Crescere digitali

Ludoteca

Registro.it

Il metodo LUDOTECA del Registro .it

Percorsi formativi
per primarie e secondarie
di primo grado

Registro.it
L'ANAGRAFE DEI DOMINI .IT

IIT ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

Sommario

Premessa

L'obiettivo di questa pubblicazione è fornire a docenti e formatori una panoramica sui contenuti e gli strumenti del progetto Ludoteca del Registro .it, dedicato all'educazione digitale nelle scuole e attivo dal 2011.

La decennale esperienza sul campo, frutto di un'intensa e proficua collaborazione con una rete di scuole distribuita su tutto il territorio nazionale, ci ha permesso di mettere a punto e testare un "metodo" per introdurre i temi del digitale, evidenziando le tante opportunità ma mettendo in luce anche i potenziali rischi.

Il nostro approccio didattico si basa sull'unione tra conoscenze e competenze, per trasmettere ai piccoli utenti della Rete le indispensabili nozioni tecniche ma anche gli strumenti per imparare "a fare qualcosa", con la giusta consapevolezza.

Il viaggio nel metodo Ludoteca inizia quindi con una **parte introduttiva** in cui descriviamo le finalità e gli strumenti del progetto, cercando di collocarlo all'interno di teorie metodologiche oggi molto utilizzate nella didattica del digitale: la gamification e il framework DigComp.

Segue una **prima parte** dedicata ai **contenuti,** con approfondimenti su temi fondamentali che riguardano Internet, il web e il digitale (come, ad esempio, i protocolli, i nomi a dominio, i social network, i cloud, l'internet delle cose, i big data, la cybersecurity, i rischi legati alla sfera sociale), per dare ai docenti una visione il più possibile completa e capace di cogliere tutte le implicazioni.

Nella **seconda parte,** entriamo più nel merito degli **strumenti,** con una rassegna delle principali risorse didattiche messe a disposizione sui nostri canali, tutte basate sull'idea di unire apprendimento e divertimento, per stimolare il più possibile l'interesse e il coinvolgimento della classe. Ogni strumento del kit didattico è presentato nelle sue principali caratteristiche ma soprattutto attraverso le modalità per utilizzarlo in classe, riportando esempi di percorsi e attività. Una "cassetta degli attrezzi" ricca e variegata, frutto di quello che abbiamo imparato in tutti questi anni, anche grazie alla collaborazione di tanti e tante docenti che hanno voluto condividere con noi questa bellissima avventura.

Introduzione al progetto Ludoteca del Registro .it

1. Il Registro .it

Il Registro .it è l'anagrafe dei domini .it, la targa Internet dell'Italia.

La registrazione dei nomi a dominio di Internet sotto il country code top level domain .it (ccTLD .it) è un'attività svolta dall'Istituto di Informatica e Telematica (IIT) del Consiglio Nazionale delle Ricerche (CNR) fin dalle sue origini. Già nel dicembre del 1987, con la nascita del primo dominio della rete italiana (cnuce.cnr.it), IANA (Internet Assigned Numbers Authority), oggi ICANN (Internet Corporation for Assigned Names and Numbers), riconobbe il ccTLD .it, assegnandone la gestione al CNR in virtù delle competenze tecniche e scientifiche maturate dai suoi ricercatori, tra i primi in Europa ad adottare il protocollo IP[1].

Questo servizio, assolto dal CNR, è in realtà strettamente correlato a una più generale funzione di salvaguardia della stabilità operativa della rete, cui il Registro provvede attraverso lo sviluppo del Domain Name System (DNS)[2] e delle politiche a esso connesse, di concerto con gli organismi internazionali di riferimento.

Il Registro è gestito dall'Istituto di informatica e Telematica del Consiglio Nazionale delle Ricerche (IIT), che riveste un ruolo di punta nei settori dell'Internet e delle tecnologie dell'informazione e della comunicazione. Nello IIT ricerca e applicazioni si integrano fra di loro in maniera bilanciata e sinergica: i risultati della ricerca di base trovano nelle applicazioni un momento di verifica, mentre dalla gestione delle applicazioni nascono nuovi spunti per le attività di ricerca. Di particolare interesse per la crescita scientifica e tecnologica dell'Istituto è anche la cooperazione con altre istituzioni. Questa strategia è attuata mediante la collaborazione con associazioni nazionali e internazionali come ad esempio Ecso[3], Eurid[4] ed Ercim[5].

Il Registro è dunque parte attiva di un più generale processo di diffusione, partecipato e condiviso, di una nuova cultura della Rete: ispirata alla libera competizione degli attori, all'uso consapevole e alla neutralità e nella quale debbono trovare ampia rappresentanza anche le comunità globali di Internet.

In questa ottica il Registro ha, ormai da anni, messo in atto un'ampia azione, utilizzando molteplici strumenti, rivolta agli studenti e studentesse dalla scuola primaria alla scuola secondaria di secondo grado. Laboratori, giochi, web app, peer education, seminari, pubblicazioni, fumetti, contest, eventi che hanno messo in contatto il Registro con migliaia di ragazzi e ragazze, insegnanti, genitori in un circolo virtuoso di trasferimento di conoscenze, che rispecchia in pieno lo spirito e gli obiettivi della ricerca e quindi del CNR stesso.

1. Indirizzo IP: Numero che identifica in modo univoco un dispositivo collegato alla rete Internet secondo lo standard IP (Internet protocol)
2. Domain Name System: il sistema utilizzato per la conversione dei nomi a dominio in indirizzi IP e viceversa
3. European Cyber Security Organisation - ECSO (https://ecs-org.eu)
4. Registro per i nomi a dominio .eu (https://eurid.eu)
5. European Research Consortium in Informatics and Mathematics (https://www.ercim.eu)

2. La Ludoteca

La Ludoteca è un progetto del Registro .it, che porta nel nome stesso il concetto positivo di gioco: l'intento è sì fornire informazioni, conoscenze e soprattutto strumenti per sviluppare "buone pratiche" di navigazione, sempre però nell'ottica del divertimento. Anche l'approccio al tema della Rete è positivo: pur trattata nella sua complessità e facendo riferimento ai rischi che si possono incontrare, i giochi e il materiale didattico proposto tendono sempre a evidenziare le enormi risorse e potenzialità.

La caratteristica principale e uno dei punti di forza del progetto è proporre strumenti eterogenei di formazione, spaziando da giochi in presenza a prodotti interattivi e multimediali. I contenuti e le informazioni sono trasmessi utilizzando mezzi a loro familiari, che appartengono alle abitudini della vita extra scolastica (come nel caso dei videogiochi) e che, per questo motivo, riescono a innescare da subito un atteggiamento ricettivo e partecipe.

Il target privilegiato per mettere in atto questa "missione" è il mondo della scuola, inteso come corpo docente, studenti e studentesse, ma la Ludoteca si rivolge anche alla famiglia, includendo iniziative dedicate a genitori e parenti.

Incorporare l'insegnamento dei fondamenti della rete Internet e della cybersecurity nei programmi educativi è una scelta di grande rilevanza nell'era digitale. Internet si è affermato come una componente essenziale nella vita quotidiana, permeando la comunicazione, l'accesso alle informazioni e le prospettive professionali. I laboratori della Ludoteca si propongono di fornire una comprensione approfondita di queste tematiche, per preparare ad affrontare le sfide e sfruttare le opportunità del mondo digitale.

Le competenze acquisite attraverso i materiali didattici della Ludoteca non solo consentono agli studenti e alle studentesse di navigare in modo consapevole sulla Rete, ma anche di partecipare attivamente alla società digitale. Comprendere i meccanismi di comunicazione online, l'accesso alle informazioni e i principi fondamentali della rete Internet li dota di strumenti essenziali per l'approccio alle carriere tecnologiche in continua evoluzione.

La Ludoteca riconosce anche l'importanza cruciale della cybersecurity nell'ambiente digitale sempre più complesso. La cybersecurity non è solo una questione di protezione dei sistemi informatici, ma riguarda anche la sicurezza delle informazioni personali e sensibili. Le classi, attraverso laboratori dedicati, non solo apprendono le pratiche di sicurezza fondamentali, ma sviluppano anche una consapevolezza e responsabilità digitale. La protezione dei dati personali, la risposta alle minacce digitali, la prevenzione degli attacchi informatici e la comprensione delle normative sulla privacy diventano pilastri della formazione, preparando a navigare non solo in un ambiente tecnologico in costante evoluzione ma anche a farlo in modo etico e conforme alle normative.

L'insegnamento di queste competenze non solo è una risposta alle esigenze pratiche della società moderna, ma è anche un investimento per il futuro, poichè trasmette alle giovani generazioni le competenze e la consapevolezza necessarie per affrontare un mondo sempre più connesso e digitale.

3. Il progetto: target e obiettivi

La Ludoteca ha l'obiettivo di diffondere la cultura di Internet, partendo dalla conoscenza funzionale delle tecnologie digitali. Il progetto è rivolto a tutti i livelli di scuola, dalle primarie alle secondarie di secondo grado, anche se questo libro è particolarmente dedicato alle attività riservate alle primarie e alle secondarie di primo grado

Il tema della Rete Internet è introdotto a partire dalle basi tecniche (linguaggio binario, trasmissione dei dati, nomi a dominio, indirizzo IP, protocolli), per trattare, in seguito, le principali problematiche legate all'utilizzo del web, come ad esempio la tutela della propria identità digitale, l'attendibilità dei contenuti e la sicurezza informatica (cybersecurity).

L'obiettivo è migliorare conoscenze, atteggiamenti e comportamenti di utilizzo della Rete Internet, così da favorire l'adozione di buone pratiche legate alla conoscenza dei rischi.

Per le primarie e secondarie di primo grado il progetto è proposto nell'ambito dei percorsi di cittadinanza digitale previsti all'interno delle ore di educazione civica, mentre per le scuole secondarie di secondo grado questo percorso formativo si svolge in modalità PCTO (Percorsi per le Competenze Trasversali e l'Orientamento); per le scuole secondarie di primo grado è previsto un percorso di approfondimento specifico basato sul videogioco *Nabbovaldo e il ricatto dal cyberspazio*, per le primarie un percorso centrato sull'uso della web app *Internetopoli* e su alcuni giochi dedicati alla cybersecurity.

L'introduzione dei laboratori sulla cybersecurity nasce nel 2018 dall'esperienza diretta nelle scuole, da cui è emersa, in tutte le fasce d'età, una scarsa e inadeguata conoscenza delle cyber minacce, associata a un uso molto frequente di varie risorse e servizi online, come ad esempio app, piattaforme di gioco, siti web.

Aspetto, questo, evidenziato dall'indagine 2023 del Telefono Azzurro-Doxa Kids, dalla quale emerge che il 93% dei ragazzi e ragazze tra i 12 e 18 anni utilizza quotidianamente lo smartphone e dunque è connesso. Il rischio ritenuto più probabile è quello di essere contattati/e da estranei adulti (65% dei casi, percentuale che si innalza al 70% se si prendono in esame solamente le ragazze e i più piccoli, dai 12 ai 14 anni). Seguono il bullismo (57%), oversharing di dati personali (54%), la visione di contenuti violenti (53%) o sessualmente espliciti (45%), l'invio di contenuti di cui ci si potrebbe pentire (36%), le spese eccessive (19%), il gioco d'azzardo (14%). Per quanto riguarda la fascia dei bambini sotto i 12 anni, secondo un recente rapporto della società Italiana delle Cure Primarie Pediatriche Lombardia in collaborazione con l'Università di Milano-Bicocca, se nel 2020 i bambini e le bambine tra i 6 e i 10 anni "possessori" di uno smartphone erano il 23,5%, questo numero sale addirittura al 58,4% nel 2021: praticamente un bambino su due ha nello zainetto la porta d'accesso per navigare, entrare nei social, accedere a siti web e dunque fruire di contenuto.

Questi dati evidenziano quanto sia urgente intervenire con azioni formative che diffondano la consapevolezza nell'uso delle risorse digitali, partendo dalla conoscenza delle basi tencniche per affrontare poi i temi legati alla sicurezza, come ad esempio la tutela dei dati e della propria identità online.

Internet rappresenta per i ragazzi e le ragazze un contesto di esperienze e "social networkizzazione" irrinunciabile: si usa per mantenersi in contatto con amici e conoscenti, cercare informazioni, studiare, ecc. Le nuove tecnologie, quindi, sono in grado di offrire, a chi ne fa uso, grandi opportunità, specialmente nel campo comunicativo-relazionale, ma nello stesso tempo espongono a nuovi rischi. È importante parlare di consapevolezza e corretta informazione nella prevenzione di questi episodi, soprattutto nel contesto scolastico. La scuola, infatti, non è un ente e struttura educativa a sé stante, ma rappresenta la più moderna e contemporanea visione di ogni aspetto di crescita, educazione e cultura e proprio per questo la Ludoteca ha scelto di strutturare la propria offerta formativa in base ai cicli scolastici, svolgendo i laboratori all'interno delle scuole in collaborazione con i/le docenti.

4. Gli strumenti: la didattica ludica

Il progetto Ludoteca, fin dal suo avvio, si è focalizzato sull'utilizzo del gioco come strumento di acquisizione di conoscenza, come testimonia anche il primo claim della Ludoteca: 'Internet è un gioco'. Il gioco ha costantemente rivestito un ruolo di veicolo educativo e di crescita.

Per il pedagogista Jean Piaget[6], consente nell'età dell'infanzia di migliorare abilità preesistenti, sviluppando al contempo una consapevolezza delle proprie capacità di influire sulla realtà esterna. In particolare, le competenze cognitive possono essere affinate attraverso l'attività ludica, che richiede la gestione dell'incertezza, l'adattamento a situazioni mutevoli e la valutazione critica di condizioni variabili. Ciò stimola il problem solving, il ragionamento flessibile e attiva la memoria di lavoro.

Pedagogisti illustri come Piaget, Vygotskii, Rogers[7] e altri riconoscono l'importanza formativa del gioco nel promuovere la curiosità e la scoperta. La Ludoteca, seguendo una strategia laboratoriale, enfatizza l'aspetto euristico della didattica e la pratica del fare, incoraggiando l'apprendimento attraverso l'esperienza diretta. Questo metodo favorisce lo sviluppo dell'autostima, della riflessione cognitiva e dell'autonomia di scelta. Gli strumenti e i giochi della Ludoteca promuovono il lavoro di gruppo, il learning by doing e la peer education, trasferendo l'attenzione dall'insegnamento all'apprendimento, con l'educatore che assume il ruolo di facilitatore.

Nei percorsi laboratoriali proposti dalla Ludoteca si incontrano vari tipi di gioco, (come, ad esempio, attività di gruppo, cruciverba, quiz), studiati per età diverse perché, citando Piaget, lo sviluppo cognitivo è a stadi e il gioco cambia la sua forma di pari passo alla sua crescita.

I serious game, o giochi seri, rappresentano un approccio innovativo nell'ambito della didattica, progettati non solo per intrattenere, ma anche per educare e formare. La storia dei serious game risale almeno agli anni '70, ma la loro popolarità e diffusione si sono notevolmente ampliate negli ultimi due decenni. Questi giochi stanno emergendo come una forma innovativa e coinvolgente di didattica, poiché offrono una vasta gamma di benefici, che possono migliorare significativamente l'esperienza di apprendimento e hanno dimostrato di avere un impatto positivo su diversi aspetti dell'educazione.

L'elemento comune tra gamification e serious game è l'utilizzo di elementi di gioco, mentre la gamification integra tali elementi in contesti non ludici per migliorare l'esperienza, i serious game sono giochi completi progettati per scopi educativi o formativi specifici. In altre parole, la gamification può essere considerata una strategia di progettazione più ampia che incorpora elementi di gioco, mentre i serious game sono giochi educativi creati per insegnare in modo specifico.

6. "La formazione del simbolo nel bambino" - Piaget
7. "Pensiero e linguaggio" - Lev Vygotskij; "L'età pre-scolare" - Lev Vygotskij; "La mente in sviluppo" - Lev Vygotskij; "L'apprendimento esperienziale" - Carl Rogers

La gamification può migliorare l'esperienza di apprendimento e motivare gli studenti e le studentesse. Gli elementi di gioco, come punti, badge, e livelli, stimolando la loro motivazione e la possibilità di raggiungere obiettivi specifici contribuisce a mantenere alta l'attenzione. Sfide, quiz interattivi e simulazioni, aiutano ad acquisire conoscenze in modo più pratico e coinvolgente e stimolano pensiero critico, collaborazione e creatività. Gli studenti e le studentesse sono spinti a cercare soluzioni innovative e a lavorare insieme per raggiungere obiettivi comuni. I sistemi "gamificati" possono offrire una tracciabilità dettagliata delle prestazioni agli/alle insegnanti che possono utilizzare questi dati per valutare il progresso individuale e apportare eventuali modifiche al programma didattico.

I serious game riescono a catturare l'attenzione in modo straordinario. Attraverso il gioco si è coinvolti attivamente nella risoluzione di problemi, nella simulazione di scenari realistici e nell'applicazione pratica di concetti. Un elemento fondamentale dei serious game è la restituzione di un feedback istantaneo che consente di capire immediatamente gli errori e di correggere il percorso di apprendimento.

5. Le competenze digitali e DIGCOMP: una mappa per i contenuti della Ludoteca

L'educazione digitale prevede il saper programmare e utilizzare gli strumenti, ma non può limitarsi a questo, servono competenze per la cittadinanza digitale per fare in modo che ogni individuo possa sentirsi incluso, attivo, critico, libero e possa esercitare i suoi diritti nella società attuale. L'avvento del digitale ha portato dei cambiamenti anche per le istituzioni educative, che si trovano oggi a doversi confrontare su nuovi temi, come, appunto, la formazione dei futuri cittadini e cittadine digitali e a dover gestire problematiche nate dalla vita social (hate speech, cyberbullismo, sexting, ecc) per garantire il benessere dei minori.

Tutte le attività e gli strumenti didattici della Ludoteca sono stati pensati per aiutare l'educatore a soddisfare i vari aspetti che concorrono alla formazione del nuovo cittadino digitale e per fronteggiare problematiche tipiche della frequentazione della Rete.

I temi e i percorsi proposti dalla Ludoteca trovano conferma nel framework di autovalutazione - elaborato dal Joint Research Centre europeo (JRC-IPTS) - DIGCOMP che è stato creato per concorrere allo sviluppo e al miglioramento delle competenze digitali dei cittadini, declinandole in conoscenze, abilità e atteggiamenti.

DigComp è stato sviluppato da JRC come progetto scientifico e con il forte contributo degli stakeholder, inizialmente per conto di DG EAC e più recentemente per conto di DG EMPL. Pubblicato per la prima volta nel 2013, DigComp è diventato un riferimento per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali, sia a livello europeo sia nei singoli stati membri dell'Unione. A giugno del 2016, JRC ha pubblicato DigComp 2.0, aggiornando la terminologia e il modello concettuale e presentando esempi di implementazione a livello europeo, nazionale e regionale.

L' Agenzia per l'Italia Digitale (AGID) ha pubblicato la traduzione ufficiale in italiano del DigCom 2.1.

Il DigComp 2.1 è organizzato in cinque aree di competenza, ciascuna suddivisa in livelli crescenti di complessità. Le aree sono:

1. **Informazione e alfabetizzazione dati:** Capacità di cercare, valutare e gestire informazioni e dati.
2. **Comunicazione e collaborazione:** Abilità nella comunicazione, collaborazione e partecipazione attraverso piattaforme digitali.
3. **Creazione di contenuti digitali:** Capacità di creare e modificare contenuti digitali in modo critico e creativo.
4. **Sicurezza:** Consapevolezza delle minacce digitali e adozione di comportamenti sicuri online.
5. **Problem Solving:** Risoluzione di problemi utilizzando strumenti e risorse digitali.

In sintesi, il DigComp 2.1 rappresenta una guida dettagliata e strutturata per valutare e sviluppare le competenze digitali, promuovendo l'alfabetizzazione digitale a diversi livelli e contesti.

Fra le varie competenze citate nel framework, le attività e risorse della Ludoteca rientrano in questi punti:

- Area di competenze 1: Alfabetizzazione su informazioni e dati (intera Area)
- Area di competenze 2: Comunicazione e Collaborazione.
    - **Punto 2.5 Netiquette:** il conoscere e il sapere applicare norme di comportamento per l'interazione in ambiente digitale; l'essere consapevoli degli aspetti connessi alla diversità culturale; l›essere in grado di proteggere sé stessi e gli altri da possibili pericoli in rete (tra i quali il cyberbullismo); l'essere in grado di sviluppare strategie attive per individuare comportamenti inappropriati.
    - **Punto 2.6 Gestire l'identità digitale:** saper creare, modificare e gestire una o più identità digitali, essere in grado di proteggere la reputazione in rete; essere in grado di trattare i dati che un soggetto produce nell'utilizzo di account e applicazioni.
- Aree di competenza 4: Sicurezza
    - **Punto 4.1 Proteggere i dispositivi:** saper proteggere i propri strumenti e avere consapevolezza dei rischi in rete e delle minacce; conoscere le misure di protezione e sicurezza.
    - **Punto 4.2 Proteggere i dati personali:** il soggetto comprende i termini di servizio comuni; protegge in modo attivo i dati personali; rispetta la privacy di altri soggetti; si protegge dalle frodi in rete, dalle minacce e dal cyberbullismo.

Questo elenco di competenze può servirci da mappa per il raggiungimento di questi importanti obiettivi di cittadinanza digitale tramite l'utilizzo di strumenti e giochi proposti dal progetto Ludoteca.

6. Presente Digitale: formazione gratuita per gli insegnanti

L'emanazione da parte del Ministero dell'Istruzione delle "Linee Guida per l'Insegnamento dell'Educazione Civica" ha evidenziato la necessità di coinvolgere le giovani generazioni in una riflessione su principi come il rispetto dell'altro e dell'ambiente che li circonda e, di conseguenza, sui comportamenti che ne derivano, anche quando si utilizza la Rete Internet; per questo motivo, 4 delle 33 ore di formazione obbligatoria, sono dedicate all'educazione alla Cittadinanza Digitale.

Nell'ottica di soddisfare questo nuovo bisogno formativo, la Ludoteca del Registro .it ha progettato percorsi formativi finalizzati a trasmettere conoscenze e competenze per l'utilizzo critico della Rete.

Per favorire la diffusione della cultura digitale nella scuola, la Ludoteca ha pensato anche alle/agli insegnanti, che devono disporre di strumenti culturali adatti per trasferire le nuove competenze e ha realizzato il portale "Presente digitale", in collaborazione con l'Istituto di Tecnologie Didattiche del CNR, per la formazione online gratuita. Il portale offre anche dei percorsi di riflessione da proporre nelle classi e rende disponibili materiali di approfondimento. I/le docenti hanno a disposizione contenuti di base e trasversali e contenuti più specialistici. Il materiale prodotto è pubblicato con licenza che ne assicura il pieno uso a scopi didattici (Open Educational Resources).

I contenuti sono stati organizzati ed erogati in modo da essere conformi ai requisiti previsti dal MIUR per la formazione dei/delle insegnanti.

I principali temi affrontati sono i seguenti:

- Sicurezza informatica.
- Internet per scopi didattici (ad es. Risorse educative aperte, Corsi online aperti di massa).
- Pensiero computazionale e programmazione informatica.

L'insegnamento è realizzato tramite Moodle, un Learning Management System (LMS) e ogni corso può essere fruito liberamente: i corsi sono basati su video lezioni, articoli di approfondimento, materiali di riferimento.

I corsi online a disposizione sulla piattaforma abbracciano trasversalmente i vari aspetti della cultura digitale e offrono strumenti e competenze per affrontare tali temi in classe con maggiore sicurezza e consapevolezza, aggiungendo alla conoscenza (che in parte anche gli studenti hanno) l'esperienza didattica e di adulto.

Questo processo può favorire il trasferimento degli elementi di cultura digitale, non necessariamente attraverso percorsi didattici "standard" ma più facilmente attraverso riflessioni guidate dal docente sulla vita in Rete, che per i "millennials" è scontata quanto quella "reale" o collocando i concetti di cultura digitale come messaggio "nascosto" nei contenuti oggetto della didattica.


1090
Nabbo
Non si preoccupi, signor Hashtag! Ci sono qua
NABBOVALDO TUTTOFARE! Rimuovere i vir
me è uno scherzo...

Il metodo Ludoteca: i temi

1. Che cos'è Internet?

Internet è una rete globale di computer interconnessi che consente la comunicazione e lo scambio di informazioni tra loro. Questa vasta infrastruttura permette ai dispositivi collegati, come computer, server, smartphone e altri dispositivi, di comunicare tra loro attraverso una serie di protocolli di comunicazione standard, il più noto dei quali è il protocollo TCP/IP (Transmission Control Protocol/Internet Protocol).

Il concetto di Internet è basato su alcuni principi chiave:

- **Decentralizzazione:** Internet non ha un'entità centrale che controlla l'intera rete. Al contrario, è costituita da una vasta distribuzione di server, router e dispositivi, consentendo una maggiore resilienza e flessibilità.
- **Accessibilità globale:** Internet collega milioni di reti e miliardi di dispositivi in tutto il mondo. Questo permette alle persone di accedere a risorse, informazioni e servizi da qualsiasi luogo connesso.
- **Protocolli standard:** I protocolli di comunicazione standardizzati, come il TCP/IP, garantiscono che i dispositivi eterogenei possano comunicare tra loro in modo coerente.
- **Accesso aperto:** Internet è aperto a tutti coloro che hanno accesso a una connessione e ai dispositivi appropriati. Questo principio di accesso aperto ha favorito l'innovazione e la diffusione delle informazioni.
- **Varietà di servizi:** Oltre alla semplice comunicazione, Internet supporta una vasta gamma di servizi, tra cui il World Wide Web (WWW), la posta elettronica, la condivisione di file, il VoIP (Voice over Internet Protocol), i social media e molto altro.
- **Evoluzione continua:** Internet è in costante evoluzione per adattarsi alle nuove tecnologie, esigenze e sfide. Nuovi protocolli, standard e tecnologie emergono costantemente, contribuendo a plasmare la sua crescita e sviluppo nel tempo.

Tutte queste caratteristiche mettono in luce la complessità di Internet e la sua capacità di trasformare radicalmente la comunicazione, l'accesso alle informazioni, il commercio, l'istruzione e molti altri aspetti della nostra vita.

1.1. Come funziona Internet

La Rete Internet permette di collegare computer, telefoni, tablet e altri tipi di oggetti lontanissimi tra di loro e di inviare e ricevere informazioni, come dati, testi, immagini, video e così via da un punto all'altro del mondo. Ma come avviene tutto questo?

1.2. Indirizzo IP e protocolli

INDIRIZZI

Nella Rete Internet un indirizzo è composto solo da numeri. Se il computer di casa è collegato alla Rete gli viene assegnato un numero, come succede per i telefoni e i numeri telefonici. Questo numero si chiama indirizzo IP.

Gli indirizzi Internet sono chiamati 'indirizzi IP' (IP significa Internet Protocol, ovvero protocollo Internet) e sono formati da 4 gruppi di massimo 3 cifre separate da un punto, ad esempio: 192.12.193.252. Ciascun gruppo può andare da 000 a 255, quindi gli indirizzi IP vanno da 000.000.000.000 a 255.255.255.255 e sono in totale oltre 4 miliardi (per l'esattezza 4.294.967.296!). Questo modo di numerare gli indirizzi va sotto il nome di IPv4 (che vuol dire Internet Protocol versione 4). La versione più recente dell'Internet Protocol è la 6 (detta IPv6) che può arrivare a miliardi di miliardi di indirizzi! È stata introdotta proprio perché gli indirizzi della versione 4 erano diventati insufficienti rispetto al numero dei dispositivi da connettere. Gli indirizzi della Rete sono un po' complicati perché i computer collegati sono tantissimi e non ci possono essere due indirizzi uguali, come non ci possono essere due case con lo stesso numero civico e due telefoni con lo stesso numero!

PROTOCOLLO

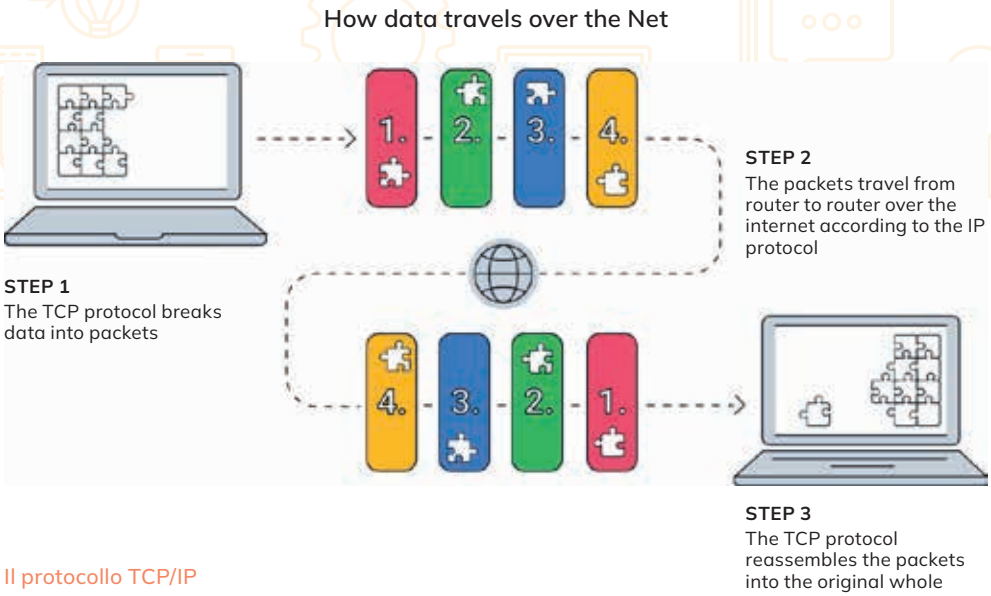
Nella Rete il termine 'protocollo' indica un insieme di regole stabilite per avere una comunicazione corretta tra apparecchiature elettroniche collegate tra loro. In base a queste regole sono raggruppati e viaggiano i dati.

Una volta che i dispositivi collegati in Rete (computer, tablet, cellulari, elettrodomestici, smartphone per citarne alcuni) riescono a trovarsi grazie agli indirizzi IP, come fanno a parlarsi, a inviare e ricevere dati? Usando un protocollo, chiamato TCP (Transmission Control Protocol – protocollo di controllo delle trasmissioni).

IL PROTOCOLLO TCP/IP

Per trasmettere i dati, i protocolli IP e TCP vengono usati insieme, per questo di solito si parla di protocollo TCP/IP.

Per scambiarsi dei dati, due dispositivi devono necessariamente essere univocamente identificati tramite il loro indirizzo IP (entra, quindi in gioco, il protocollo IP, che, lo ricordiamo, è composto da quattro blocchi numerici di tre cifre).



Il protocollo TCP/IP

Il protocollo IP individua con esattezza il dispositivo elettronico collegato alla rete e fornisce al mittente l'indirizzo di destinazione a cui può inviare i dati, proprio come avviene per l'indicazione del destinatario quando inviamo una lettera. Il TCP, invece, gestisce l'organizzazione dei dati e il controllo della trasmissione degli stessi. Standardizza la grandezza dei dati da inviare, spezzettandoli in sottoinsiemi più piccoli, di dimensioni fissate, chiamati pacchetti. Questi vengono poi ricomposti nella forma originale nel momento in cui arrivano al destinatario. Per spostare i pacchetti di dati tra mittente e destinatario, il protocollo TCP ha bisogno delle informazioni fornite dal protocollo IP (ecco perché "protocollo TCP/IP"), cioè ha bisogno di sapere con certezza l'indirizzo del mittente e quello del destinatario, informazione che gli viene fornita dal protocollo IP.

2. Nomi a dominio

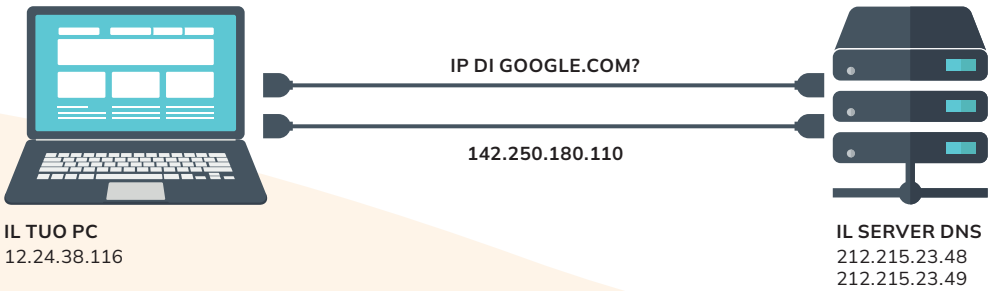
Ricordare l'indirizzo IP del destinatario del messaggio, per un umano, sarebbe pressoché impossibile, quindi si ricorre a un "sinonimo": a un indirizzo IP può essere associato un nome, che è più facile, per noi, da ricordare; come nella nostra rubrica telefonica, cercheremo il nome per trovare il numero associato ad esso. In questo modo, alcuni tipi di dispositivi collegati in rete possono essere identificati con il nome invece che con l'indirizzo IP. È fondamentale che la corrispondenza tra nome e numero sia univoca, cioè a ogni numero corrisponde un solo nome e viceversa. Quali sono questi nomi? Sono, per esempio, quelli che digitiamo nella barra del motore di ricerca (Uniform Resource Locator) quando vogliamo collegarci a un sito e si chiamano "nomi a dominio" (domain names). La loro composizione segue regole precise, che sono uno standard in tutto il mondo. Nei prossimi paragrafi vedremo come funziona.

2.1. La Mappa dei nomi e il DNS

Se Internet è una grande città, i nomi a dominio sono gli indirizzi di case, negozi e uffici. Ce ne sono miliardi, ma ciascuno ha il suo e non esistono duplicati.

Un indirizzo, nel linguaggio della Rete e dei computer, è solo la sequenza di numeri su cui si basa il protocollo IP. I calcolatori possono memorizzarli senza problemi; gli esseri umani, invece, hanno bisogno di associare agli indirizzi parole o espressioni semplici da ricordare. I nomi a dominio non sono altro che sequenze di lettere e/o numeri, combinate dagli utenti secondo fantasia ma in modo che possano essere facilmente memorizzate e che "traducono" gli indirizzi IP in una forma adatta alla memoria umana.

Anche i nomi a dominio, come gli indirizzi veri e propri, sono unici e non possono essere duplicati: a ogni sequenza di numeri corrisponderà sempre un solo nome a dominio, e viceversa. A "tradurre" i nomi in numeri - l'unico linguaggio delle macchine - ci pensa il DNS, Domain Name System, in modo del tutto invisibile e trasparente.



Il Domain Name System

Il DNS associa in modo certo e univoco un indirizzo IP (la sequenza di 4 gruppi di numeri) a una stringa alfanumerica facilmente memorizzabile (come nella rubrica telefonica).

Ad esempio, l'indirizzo IP di www.ludotecaregistro.it è 192.12.192.39. Questo sistema è cruciale per rendere Internet accessibile e comprensibile per tutti noi. Inoltre, con l'avvento dell'Internet delle cose (IoT), dove ogni oggetto ha il suo indirizzo IP, la disponibilità di indirizzi sufficienti diventa ancora più importante.

2.2. Top Level Domain (TLD)

Le estensioni dei nomi a dominio, anche conosciute come top-level domain (TLD), sono l'ultimo segmento di un nome a dominio, la parte che si trova dopo l'ultimo punto. Servono a identificare il tipo di organizzazione o l'area geografica a cui appartiene il dominio e sono fondamentali per l'organizzazione e la classificazione dei siti web su Internet. Esistono diverse tipologie di estensioni, ognuna con uno scopo specifico:

Generiche (gTLD): queste estensioni non sono associate a una specifica area geografica ma possono fare riferimento a particolari categorie, come ad esempio il settore commerciale per il .com e le organizzazioni per il .org.

Geografiche (ccTLD): ccTLD significa Country Code Top Level Domain. Queste estensioni sono associate a una specifica area geografica o territorio. Ad esempio, .it per l'Italia, .fr per la Francia, .uk per il Regno Unito, .de per la Germania, ecc.

Specializzate (sTLD): queste estensioni sono riservate per specifici settori o comunità e sono spesso utilizzate per indicare una particolare attività o interesse. Alcuni esempi sono .edu per istituti educativi, .gov per enti governativi, .mil per le forze armate, .museum per musei, .aero per l'industria aeronautica, .coop per le cooperative, ecc.

Nuove estensioni (new gTLD): queste sono estensioni introdotte nel 2013 e includono una vasta gamma di suffissi che coprono interessi, settori e comunità specifiche. Alcuni esempi sono .blog, .shop, .app, .guru, .photography, .music, .club, ecc.

2.3. I domini di secondo livello

I domini di secondo livello sono composti da un nome di riconoscimento ed è la parte del nome, a sinistra del punto. La struttura di un dominio di secondo livello è cioè "nomedominio.estensione".

Un esempio di dominio di secondo livello è ludotecaregistro.it dove ".it" è l'estensione (dominio di primo livello ed è un ccTLD, perché .it identifica l'Italia) e "ludotecaregistro" è il nome a dominio di secondo livello.

I domini di terzo livello hanno una struttura così composta: nomesottodominio.nomedominio.estensione (es. comune.pisa.it).

2.4. Come si sceglie un nome a dominio

Nel vasto contesto della metropoli di Internet, rappresentata dai nomi a dominio specifici di ciascun Paese (tramite le relative estensioni ccTLD) e dalle diverse attività commerciali (mediante le estensioni generiche come .com, .biz, .pizza, ecc.), gli individui e le imprese possono spostarsi liberamente senza incontrare ostacoli né richiedere visti sui loro "passaporti digitali". Ogni entità è identificata e si distingue grazie al proprio nome a dominio, il quale, in un certo senso, ne riflette la natura e le caratteristiche.

Ad esempio, una società commerciale potrebbe trovare vantaggioso registrare il proprio nome sotto l'estensione .com, anche se ciò comporterebbe la perdita della connotazione geografica. Tuttavia, se tale aspetto è rilevante (ad esempio, nel caso della valorizzazione del marchio "made in Italy"), potrebbe essere più appropriato scegliere un nome a dominio con l'estensione del proprio Paese (come, ad esempio, il .it nel nostro caso). In un ambiente senza confini fisici, evidenziare la propria provenienza geografica può costituire un valore aggiunto, sia per la qualità dei prodotti offerti, sia per la tipologia di servizi erogati, oppure per ragioni puramente affettive.

Una volta registrato il nome a dominio, si crea una sorta di "nuova casa" digitale, che richiede un'adeguata cura e personalizzazione. Si può decidere di gestire autonomamente l'allestimento, seguendo il proprio gusto personale, oppure delegare l'incarico a professionisti esperti, proprio come avviene nella vita reale.

L'utilizzo più comune di un nome a dominio è per la creazione di un sito web (ad esempio, ricordiamo ludotecaregistro.it) e l'associazione di un indirizzo email personalizzato. Questo fornisce una vetrina virtuale con visibilità globale e un'identità digitale personalizzata. Una famiglia può scegliere di registrare il proprio cognome come nome a dominio e assegnare un indirizzo email personalizzato a ciascun membro. Negozianti e professionisti possono sfruttare il proprio nome commerciale o settore di attività per promuovere prodotti e servizi o ampliare la propria presenza online.

Le opportunità offerte da Internet sono virtualmente infinite e dipendono principalmente dalla creatività e dall'ingegno degli individui e delle imprese.

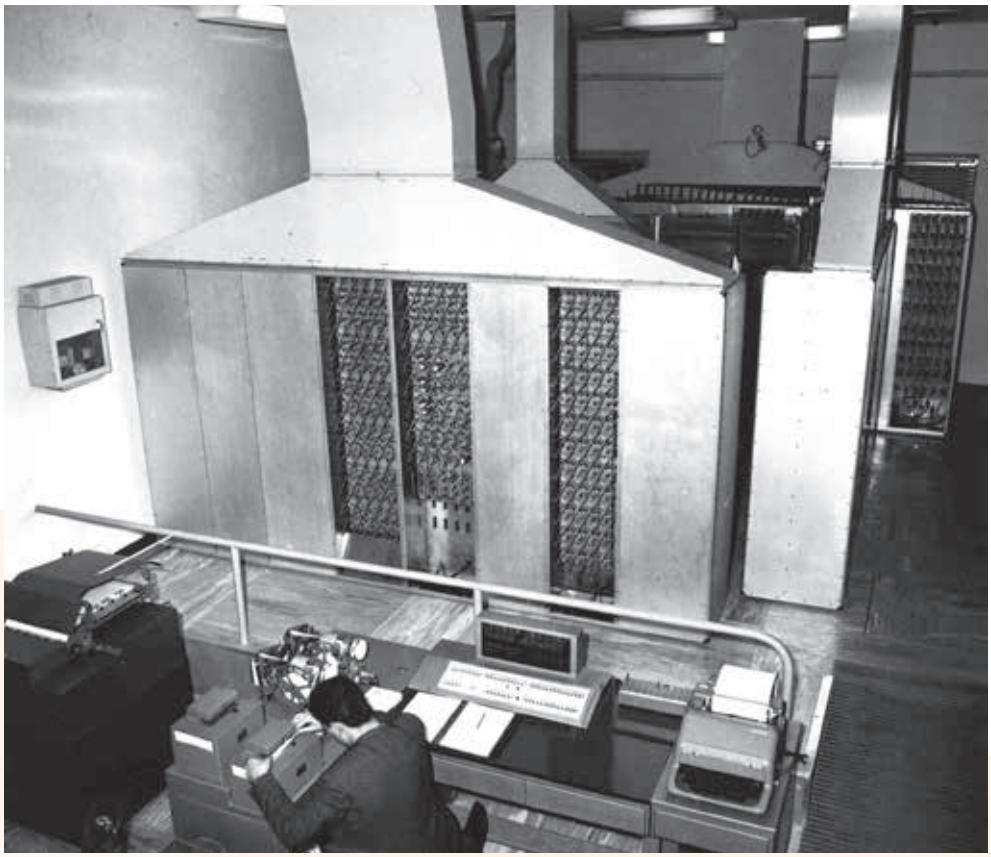
3. Storia della Rete in Italia: dai primi calcolatori elettronici alla prima connessione

ANTEFATTO: PISA, LA CULLA DEL CALCOLO ELETTRONICO ITALIANO

La storia del primo collegamento alla Rete Internet in Italia è strettamente legata alla storia dei progressi tecnologici nel campo dell'informatica. Pisa in questo senso ha rappresentato, a partire dagli anni '50, il fulcro di ricerche pionieristiche che hanno portato a traguardi importanti.

Nel 1953, il fisico Enrico Fermi, ex studente della Scuola Normale di Pisa e ancora legato al gruppo di fisici della città, scrive al rettore dell'Università di Pisa, Enrico Avanzi, per promuovere la realizzazione di una macchina calcolatrice all'avanguardia. Questo strumento era essenziale per gli scienziati impegnati nelle loro ricerche nella città.

Tra il 1955 e il 1958, nasce il progetto della CEP (Calcolatrice Elettronica Pisana), inizialmente sviluppato come "macchina ridotta" per scopi di prova e infine, il 13 novembre 1961, la CEP viene inaugurata nella sua forma definitiva dal Presidente della Repubblica, Gronchi.



CEP

1958 LA GUERRA FREDDA E LA NASCITA DI ARPANET

Il Ministero della Difesa americano lancia DARPA (Defence Advanced Research Projects Agency), un progetto di finanziamento al mondo universitario per lo sviluppo di soluzioni tecnologiche di difesa. Il Governo americano cerca così di rispondere al lancio del satellite Sputnik I effettuato dai russi alla fine del 1957 e alla paura che l'URSS compia un balzo in avanti decisivo nella scoperta di nuove tecnologie belliche. Tra le prime attività di ricerca finanziate da ARPA, quella dedicata alla messa in rete dei calcolatori elettronici, di vitale importanza per lo scambio d'informazioni tra i centri di ricerca americani e molto utile anche in caso di guerra. Il progetto prende il nome di ARPANET.

1969 ARPANET E IL PRIMO TRASFERIMENTO DI DATI

Il 29 ottobre 1969 segna il primo trasferimento di dati su ARPANET, collegando l'Università di Los Angeles e lo Stanford Research Institute. Nel marzo del 1970 la rete attraverserà l'America per collegare anche la East Coast. Entro il 1971 saranno 13 i computer collegati, 46 entro il 1976, 213 alla fine del 1981.

1986 COLLEGAMENTO CNUCE CON ARPANET E LA SVOLTA TECNOLOGICA

Con un semplice scambio di "Ping" e "OK" avviene il primo collegamento tra il CNUCE a Pisa e Telespazio al Fucino, dopo essere rimbalzato attraverso l'antenna verso il satellite Intelsat V e da lì a Roaring Creek, Pennsylvania. Questo è il segnale della prima connessione stabilita con Arpanet in Italia, la quarta in Europa dopo Inghilterra, Norvegia e Germania.

1987 ASSEGNAZIONE DEL DOMINIO .IT AL CNR

Il 23 dicembre 1987, IANA (Internet Assigned Numbers Authority) ufficializzò il ccTLD .it, affidando la gestione al Consiglio Nazionale delle Ricerche (CNR) in riconoscimento delle sue competenze tecniche e scientifiche avanzate, essendo tra i pionieri in Europa nell'adozione del protocollo IP. È in questo contesto che venne registrato il primo dominio della rete italiana: cnuce.cnr.it.

Dalla metà degli anni 2000 in poi, la storia di Internet ha subito una serie di evoluzioni significative che hanno plasmato il modo in cui interagiamo, comunichiamo e conduciamo affari online.

L'avvento degli smartphone e dei dispositivi mobili ha reso Internet sempre più accessibile ovunque. Le applicazioni mobili, insieme alla navigazione web su dispositivi portatili, hanno portato a un cambiamento radicale nelle abitudini di consumo e di ricerca. Piattaforme come Facebook, Twitter, Instagram e LinkedIn hanno rivoluzionato il modo in cui le persone si connettono e interagiscono online. La condivisione di contenuti, la creazione di reti e l'influenza sociale sono diventati elementi fondamentali della vita digitale. Piattaforme di e-commerce come Amazon, eBay e Alibaba hanno cambiato il modo in cui facciamo acquisti e l'avvento del cloud computing ha trasformato il modo in cui archiviamo, gestiamo e distribuiamo dati e risorse online.

4. La governance di Internet e Il Registro .it

La cosiddetta “governance”, di Internet si occupa di creare e applicare le regole, le politiche e i processi che guidano l’uso e lo sviluppo della rete in modo sicuro, equo, aperto e trasparente. Sono numerosi i soggetti che entrano in gioco, con ruoli e compiti diversi, che vengono brevemente descritti nel seguito.

4.1. ICANN e altri enti internazionali

La governance di Internet si riferisce al modo in cui Internet è gestito, regolato e organizzato a livello globale. È un processo complesso che coinvolge una vasta gamma di attori, tra cui governi, organizzazioni internazionali, settore privato, società civile e comunità tecnica. La governance di Internet si basa su un modello multilaterale e decentralizzato che cerca di bilanciare la necessità di apertura, accessibilità, sicurezza e stabilità della rete.

I principali temi che vengono discussi a livello globale sono:

- **Standard tecnici:** Internet è basato su una serie di standard tecnici che definiscono il modo in cui i dispositivi e i protocolli di comunicazione interagiscono sulla rete. Questi standard sono sviluppati principalmente da organizzazioni come l’Internet Engineering Task Force (IETF) e il World Wide Web Consortium (W3C).
- **Assegnazione degli indirizzi IP:** gli indirizzi IP, che identificano univocamente ogni dispositivo connesso a Internet, sono assegnati da organizzazioni regionali come l’Internet Assigned Numbers Authority (IANA) e i loro operatori di servizi (Regional Internet Registry) regionali come American Registry for Internet Numbers (ARIN), Réseaux IP Européens - Network Coordination Centre (RIPE NCC), Asia-Pacific Network Information Centre (APNIC), ecc.
- **Nomi a dominio:** i nomi a dominio, che forniscono un’etichetta mnemonica per risorse specifiche su Internet, sono gestiti da varie organizzazioni, inclusi i registri dei domini di primo livello (TLD) come Verisign per .com e il Registro .it per .it, e registrati tramite i Registrar accreditati.
- **Governance tecnica:** la governance tecnica di Internet coinvolge organizzazioni come l’Internet Corporation for Assigned Names and Numbers (ICANN), che coordina il sistema dei nomi a dominio e gli indirizzi IP, e l’Internet Governance Forum (IGF), che facilitano il dialogo su questioni di governance di Internet tra vari portatori di interesse.

ICANN, fondata nel 1998, è un'organizzazione no-profit del settore pubblico internazionale, impegnata nel mantenimento della sicurezza, della stabilità e dell'interoperabilità di Internet. Ha l'incarico di assegnare gli indirizzi IP e di identificare il protocollo e la gestione del sistema dei nomi a dominio di primo livello (generic Top Level Domain) e di quelli nazionali (i country code Top Level Domain - ccTLD). La funzione di ICANN è quella di coordinare questi identificatori univoci in tutto il mondo. Senza questo coordinamento, non esisterebbe una rete Internet globale.

4.2. Il Registro italiano dei domini .it

Nel contesto della governance di Internet, l'assegnazione dei nomi e dei numeri segue regole e standard tecnici ben definiti. I nomi e gli indirizzi devono essere univoci per evitare possibili confusioni e garantire il corretto funzionamento della Rete. Per questo motivo, per ogni estensione di primo livello (p.es. .com, .org, .net, .it, .fr, ecc.) esiste un registro centrale, attivo 24 ore su 24, che vigila sulla corretta assegnazione dei nomi a dominio.

In Italia questo ruolo è svolto dal Registro .it. Con oltre tre milioni di nomi a dominio registrati, il "quartiere" italiano di Internet gode di una notevole popolarità e riceve costantemente nuove richieste di registrazione.

È importante sottolineare che il Registro opera esclusivamente come ente di registrazione ufficiale e non si occupa direttamente della fornitura di servizi Internet o della gestione dei prezzi dei servizi forniti dai Registrar. Queste funzioni sono invece delegate ai Registrar, che sono fornitori di servizi Internet, tra cui la registrazione dei nomi a dominio, la connettività, lo spazio web, servizi di posta elettronica ecc., le cui attività relative alla registrazione dei nomi a dominio, sono regolate da specifici accordi con il Registro.

4.3. Regole nella scelta del dominio

La registrazione di un nome a dominio nel ccTLD.it è consentita soltanto a soggetti maggiorenni che abbiano cittadinanza, residenza o sede nei paesi dello Spazio Economico Europeo (See), nello Stato del Vaticano, nella Repubblica di San Marino, nella Confederazione Svizzera e nel Regno Unito.

Di seguito alcune regole da seguire nella scelta di un nome a dominio:

- Un nome a dominio .it può essere composto solo da lettere dalla "a" alla "z", numeri da 0 a 9 e il simbolo "-" (trattino) e tutti i caratteri NON ASCII appartenenti a un insieme di caratteri indicati nelle "Linee Guida tecniche". Semplificando molto i caratteri NON ASCII sono caratteri speciali che non si trovano sulla tastiera di un computer.
- Non deve iniziare e finire con il simbolo "-" (trattino) né iniziare con la sequenza di caratteri "xn--"
- Un dominio .it può essere composto da un minimo di 3 caratteri fino ad un massimo di 63.

5. Risorse e servizi della Rete

Le risorse e i servizi della Rete Internet sono gli elementi fondamentali che compongono il mondo online. Le risorse sono tutto ciò che è disponibile online e può essere accessibile tramite la rete internet, come ad esempio le pagine web, le immagini, i video e molto altro ancora.

I servizi della rete internet sono le piattaforme e gli strumenti che consentono agli utenti di accedere e utilizzare queste risorse (social media, servizi di email, negozi online e così via).

In sostanza, le risorse costituiscono il contenuto disponibile online, mentre i servizi sono gli strumenti e le piattaforme che permettono agli utenti di accedere, condividere, e interagire con questo contenuto.

5.1. Motori di ricerca

I motori di ricerca sono strumenti online progettati per aiutare gli utenti a trovare informazioni sulla rete. Svolgono una funzione cruciale nell'organizzazione e nella catalogazione delle immense quantità di dati disponibili su Internet. Tra i più noti possiamo citare Google, Bing, Yahoo ma ce ne sono molti altri.

Il funzionamento dei motori di ricerca avviene attraverso una serie di passaggi che potremmo così sintetizzare:

- **Indicizzazione:** è il processo mediante il quale i motori di ricerca raccolgono, analizzano e memorizzano informazioni dettagliate su tutte le pagine web che riescono a scoprire durante la loro attività di crawling. L'obiettivo è creare un indice organizzato e facilmente consultabile.
- **Crawling:** la fase di crawling precede l'indicizzazione. In questa fase, i motori di ricerca utilizzano dei programmi chiamati "crawler" o "spider" per esplorare il web alla ricerca di nuove pagine e aggiornamenti su pagine esistenti. Questi crawler seguono i link da una pagina all'altra, costruendo una mappa della struttura del web.
- **Recupero del contenuto:** durante il crawling, i crawler recuperano il contenuto delle pagine web, inclusi testi, immagini, link e altri elementi. Questi dati vengono estratti dalle pagine web visitate dai crawler.
- **Analisi del contenuto:** dopo il recupero del contenuto, i motori di ricerca analizzano il testo e altri elementi presenti nelle pagine. L'analisi può includere l'identificazione delle parole chiave, la comprensione del contesto e la valutazione della rilevanza del contenuto.
- **Tokenizzazione e creazione di un indice:** i motori di ricerca suddividono il testo delle pagine web in unità più piccole chiamate "token". Un token può essere una singola parola o una sequenza di caratteri con significato. Gli indici vengono quindi creati associando ogni token alle pagine web che lo contengono. Questo processo consente di recuperare rapidamente le pagine pertinenti quando un utente effettua una ricerca contenente determinati termini.

- **Algoritmi di ranking:** vengono utilizzati per assegnare un punteggio di rilevanza alle pagine indicizzate in base alle query degli utenti. Questi algoritmi considerano diversi fattori, come la presenza delle parole chiave, la qualità dei contenuti, la struttura dei link e altri indicatori di autorevolezza.
- **Aggiornamenti periodici:** gli indici dei motori di ricerca vengono aggiornati regolarmente per riflettere le modifiche nel web. I motori di ricerca continuano a eseguire il crawling e l'indicizzazione in modo costante per mantenere aggiornati i loro database.
- **Risposta alle query degli utenti:** quando un utente inserisce una query di ricerca, il motore di ricerca consulta il suo indice e restituisce una lista di pagine web ritenute più rilevanti. La precisione di questa risposta dipende dalla qualità dell'indicizzazione e dalla pertinenza delle pagine nel database.

L'indicizzazione è quindi il processo mediante il quale i motori di ricerca organizzano e rendono accessibili i contenuti web, consentendo agli utenti di trovare informazioni pertinenti attraverso le loro ricerche.

5.2. Strategie per una ricerca efficace

Quando interroghiamo i motori di ricerca non sempre riusciamo a trovare quello che vogliamo e ci perdiamo nella miriade di risultati che ci vengono restituiti. Per ovviare a questo problema e procedere con una ricerca mirata possiamo usare alcuni strumenti.

- **Sintassi di ricerca avanzata:** si possono utilizzare operatori come "AND", "OR", "NOT" per affinare i risultati. Ad esempio, "tecnologie AND sostenibili" restituirà risultati che contengono entrambe le parole chiave.
- **Uso delle virgolette:** per cercare una frase esatta, si possono inserire le parole chiave tra virgolette. Ad esempio, "intelligenza artificiale".
- **Utilizzo di operatori wildcard:** l'asterisco (*) può essere usato come segnaposto per parole sconosciute. Ad esempio, "tecnologia * avanzata".
- **Limitazione della ricerca a siti specifici:** per limitare i risultati di ricerca a un determinato dominio si può utilizzare il prefisso "site:". Ad esempio, "site:example.com".
- **Utilizzo dei filtri di ricerca avanzati:** molti motori di ricerca permettono di filtrare i risultati per data, tipo di contenuto e altre categorie.
- **Ricerca inversa dell'immagine:** per cercare informazioni su un'immagine, si può utilizzare la ricerca inversa dell'immagine su motori come Google Images: caricando un'immagine il motore di ricerca ne trova la o le fonti da cui è stata presa

5.3. Enciclopedie online

Le enciclopedie online sono risorse digitali che forniscono informazioni su una vasta gamma di argomenti. A differenza delle enciclopedie tradizionali stampate, le enciclopedie online sono aggiornate regolarmente e spesso consentono la partecipazione degli utenti alla redazione di contenuti.

Queste enciclopedi consentono un accesso rapido alle informazioni, spesso con una struttura di navigazione intuitiva e offrono una vasta gamma di argomenti, dalla scienza alla cultura popolare, e sono soggetti a continui aggiornamenti per riflettere gli sviluppi più recenti nelle rispettive discipline.

Wikipedia è la più famosa ma esistono diverse risorse di riferimento digitali, come ad esempio:

- Enciclopedia Britannica Online: una versione digitale che offre articoli accurati e approfonditi su una vasta gamma di argomenti.
- Encyclopedia.com: un sito che fornisce accesso a più di 100 enciclopedie e risorse di riferimento, coprendo argomenti che vanno dalla scienza all'arte.
- Enciclopedia Treccani: una versione online della famosa enciclopedia con informazioni dettagliate su storia, arte, scienza e cultura.
- Stanford Encyclopedia of Philosophy (SEP): autorevole enciclopedia online di filosofia, curata da esperti nel campo e con articoli approfonditi su temi filosofici.
- HowStuffWorks: non è una vera e propria enciclopedia, però fornisce spiegazioni dettagliate su vari argomenti, dalla tecnologia alla scienza e alla cultura.

Oltre alle enciclopedie, in Rete ci sono molte altre fonti di informazione online che vanno dai siti di notizie ai blog, dai forum specializzati alle pubblicazioni accademiche.

5.4. Wikipedia e fonti di informazione online

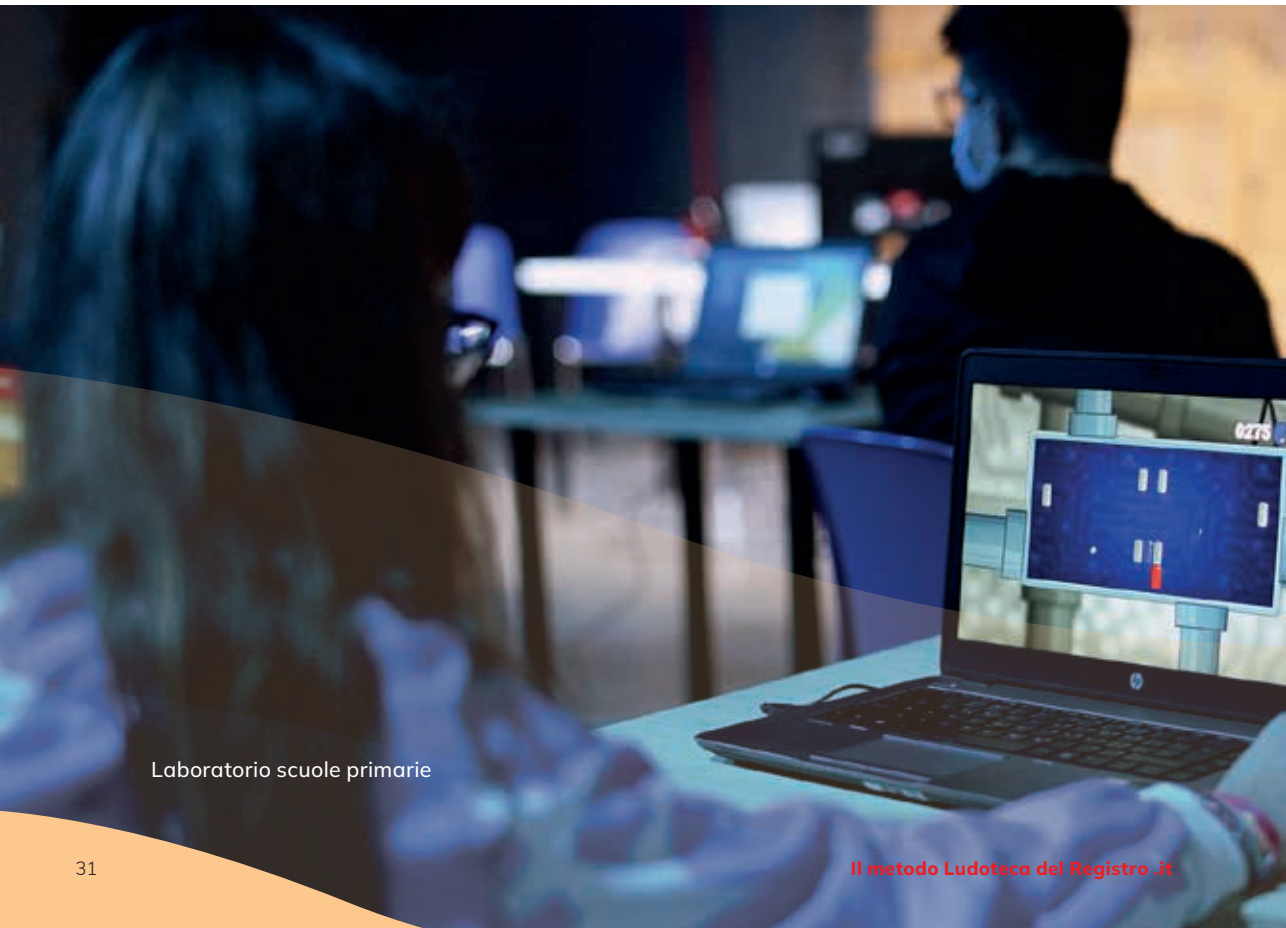
A proposito delle enciclopedie online, la più usata e conosciuta è sicuramente Wikipedia. Fu lanciata ufficialmente a inizio 2001, in lingua inglese, sul sito Wikipedia.com. Innanzitutto, Wikipedia si autodefinisce «libera e collaborativa», ogni utente infatti può aggiungere o modificare una voce. L'adozione di licenze libere per testi e immagini (in particolare delle licenze Creative Commons) consente il riutilizzo dei contenuti per ogni scopo. Il «libera» fa anche riferimento all'indipendenza che il progetto rivendica rispetto a influenze esterne: per una maggiore autonomia Wikipedia è uno dei pochi siti ad alto volume di traffico a non avere inserzioni pubblicitarie, è gratuita e aperta a chiunque abbia accesso a Internet ed è disponibile in numerose lingue, consentendo l'accesso a una vasta comunità globale.

Per consultare al meglio Wikipedia e ottenere informazioni accurate e affidabili, ecco alcuni suggerimenti:

- verificare le fonti: occorre sempre controllare le fonti citate negli articoli. Wikipedia incoraggia la citazione di fonti attendibili, ma è sempre meglio confermare la loro validità consultando le fonti originali.

- leggere l'intero articolo: è importante non basarsi solo sulla parte iniziale di un articolo di Wikipedia, gli articoli spesso forniscono dettagli e approfondimenti più avanti.
- controllare la cronologia delle modifiche: se si stanno cercando informazioni aggiornate o si hanno dei dubbi sulla validità di un articolo è bene consultare la cronologia delle modifiche per capire come l'articolo è stato modificato nel tempo.
- attenzione agli avvisi: Wikipedia pubblica avvisi quando ci sono preoccupazioni sulla neutralità, sulla completezza o sulla veridicità delle informazioni.
- sottoporre a valutazione le informazioni: Wikipedia può essere un ottimo punto di partenza, ma è sempre consigliabile cercare fonti aggiuntive per convalidare i dati e poter valutare criticamente le informazioni presenti.
- esplorare le categorie e i collegamenti: Wikipedia organizza gli articoli in categorie e fornisce collegamenti tra argomenti correlati ed è bene esplorare queste connessioni per ottenere una visione più ampia e approfondita dell'argomento che ci interessa.

Occorre ricordare che, come abbiamo già detto, Wikipedia è un'enciclopedia collaborativa quindi le informazioni possono variare nella loro completezza e precisione.



Laboratorio scuole primarie

5.5. Il Cloud

Un servizio internet molto utile per archiviare file e dati è il cloud (che vuol dire "nuvola"), uno spazio di memoria a cui l'utente può accedere tramite Internet. L'utilizzo ha vari scopi: conservare file di grandi dimensioni, fare copie di sicurezza di dati (il cosiddetto back up), condividere documenti con altri utenti. I servizi cloud oggi sono sempre più numerosi, Google Drive, Dropbox, OneDrive sono sicuramente quelli più famosi e offrono anche la possibilità di utilizzare il servizio gratuitamente fino ad un massimo di spazio in GB (gigabyte). Esistono però moltissimi altri cloud ma è importante sceglierli con attenzione, considerando che in questi spazi sono conservati i nostri file.

5.6. Utilità e rischi del Cloud Computing

Si parla anche di "cloud computing" per indicare un servizio che consente di sfruttare la rete internet per distribuire e accedere a risorse software e hardware da remoto, come nel caso in cui aziende e organizzazioni abbiano bisogno di potenze di calcolo elevate.

Il cloud computing offre una serie di vantaggi, primo tra tutti il fatto che le risorse possono variare in base alle esigenze dell'utente senza la necessità di investimenti in hardware aggiuntivo e che sono sempre raggiungibili da qualsiasi luogo con una connessione Internet, consentendo il lavoro remoto e la collaborazione distribuita. Innegabili anche i vantaggi economici: spesso si paga solo per le risorse utilizzate, evitando i costi fissi associati alla gestione di infrastrutture. Inoltre, i servizi cloud spesso offrono ridondanza e backup automatici per garantire l'affidabilità e la disponibilità continua delle risorse.

Oltre ai numerosi vantaggi occorre considerare anche alcuni rischi informatici che devono essere affrontati e gestiti adeguatamente.

Quando i dati sono archiviati nel cloud, l'utente perde un certo grado di controllo diretto su di essi con preoccupazioni sulla privacy, sulla conformità normativa e sulla protezione dei dati sensibili anche se le aziende che archiviano dati sensibili nel cloud devono garantire la conformità con le leggi e i regolamenti pertinenti, come GDPR[1] e altri. La mancata conformità può portare a sanzioni legali, multe e danni alla reputazione dell'azienda.

Da considerare anche il fatto che il fornitore di servizi cloud potrebbe subire interruzioni o malfunzionamenti dei server e i servizi e le risorse ospitati nel cloud potrebbero non essere disponibili. Questo può causare perdite finanziarie, interruzioni delle operazioni aziendali e insoddisfazione degli utenti.

Per mitigare questi rischi, le organizzazioni devono adottare misure di sicurezza robuste, come l'implementazione di crittografia dei dati, l'adozione di autenticazione multi-fattore, l'implementazione di controlli di accesso rigorosi, l'addestramento del personale sulla sicurezza informatica e la valutazione regolare dei rischi. Bisogna quindi prestare molta attenzione prima di affidare i nostri dati al cloud e selezionare fornitori che offrono alti standard di servizio conformi alle normative di sicurezza e privacy vigenti.

1. General data protection regulation (https://www.garanteprivacy.it/regolamentoue)

6. Social network

Nell'era digitale in cui viviamo, i social network e la messaggistica istantanea giocano un ruolo fondamentale nella costruzione delle nostre interazioni sociali e comunicative. Questi strumenti digitali hanno trasformato radicalmente il modo in cui condividiamo informazioni e manteniamo relazioni personali e professionali.

Un social network è una piattaforma online che permette di creare profili personali, mettersi in contatto con altre persone e condividere contenuti come testi, immagini, video, mettendo a disposizione una vasta gamma di funzionalità che consente agli utenti di interagire tra loro.

Tra i social network più popolari possiamo citare Facebook, Twitter, Instagram, LinkedIn e TikTok, ognuno con la propria enfasi su tipi specifici di contenuti e interazioni. Ad esempio, Instagram si concentra principalmente sulla condivisione di foto e video, mentre LinkedIn è orientato alla connessione professionale e alla ricerca di opportunità lavorative.

La messaggistica istantanea è un'altra forma di comunicazione digitale che consente agli utenti di scambiarsi messaggi in tempo reale attraverso Internet. Questo tipo di comunicazione è diventato estremamente popolare per la sua immediatezza e praticità, si possono infatti inviare e ricevere messaggi di testo, immagini, video e file in tempo reale.

Piattaforme di messaggistica istantanea come WhatsApp, Facebook Messenger, Telegram, Signal e Discord sono diventate parte integrante della nostra vita quotidiana, consentendoci di comunicare facilmente con amici, familiari, colleghi di lavoro e altri contatti, sia a livello personale che professionale.

L'avvento dei social network e della messaggistica istantanea ha avuto un impatto significativo sulla società e sulla cultura. Costituiscono un nuovo paradigma di comunicazione, non ne sono soltanto uno strumento; hanno cambiato il modo di relazionarci con gli altri, dove "gli altri" possono essere vicini o lontani, amici, conoscenti o perfetti sconosciuti; hanno cambiato il luogo dove ci relazioniamo: non esiste più solo la piazza del paese, o il tradizionale faccia a faccia, ma il luogo virtuale, dove potenzialmente la platea degli ascoltatori è enorme. Eppure, alla domanda fatta ai ragazzi e ragazze: "Perché sei sui social network?" la risposta è timida e spesso vaga; molti hanno davanti a sé la (limitata) prospettiva delle proprie personali esperienze, ma i social network sono uno strumento potente per abbattere barriere spaziali, sociali e temporali.

Da un lato, questi strumenti hanno reso più facile per le persone rimanere in contatto e mantenere relazioni a distanza. D'altra parte, hanno anche sollevato questioni legate alla privacy, alla sicurezza e alla dipendenza da internet. Il problema della privacy oggi ossessiona e preoccupa un po' tutti: la Rete è certamente un amplificatore dei nostri dati e delle informazioni che inseriamo ad ogni accesso, in ogni sito web o sui social, ad esempio, e non si può negare che un margine di rischio esista.

Quest'ultimo va, tuttavia, misurato, possibilmente ridotto e in parte accettato (come accade sempre anche nella vita reale): non possiamo rinunciare alle opportunità che la Rete, la tecnologia e il progresso ci offrono. Privarsene sarebbe come scegliere di vivere sotto la famosa campana di vetro per non correre rischi affrontando la vita quotidiana.

Bisogna muoversi nella Rete come nella vita reale, con buon senso e prudenza, evitando di condividere informazioni particolarmente delicate o riservate come quelle sulla propria salute, sul proprio conto in banca e così via, a meno che non ci siano adeguate garanzie di riservatezza.

6.1. Internet e minori: cyberbullismo e altri rischi

Come già abbiamo detto, i social network insieme ai numerosi vantaggi presentano anche dei rischi, soprattutto per i navigatori più piccoli e poco esperti.

Oltre ai social network più popolari (es. Facebook, Instagram, ecc.) occorre considerare che i ragazzi e le ragazze spesso frequentano anche le piattaforme di gioco che hanno il loro modo di far comunicare gli utenti attraverso forum (es. piattaforma Steam), servizi di messaggistica (Xbox live) o servizi livestream (es. gaming YouTube, Twitch, ecc).

Agli utenti meno esperti l'ambiente dei social network può sembrare un luogo protetto, dove i rapporti sono semplici, familiari, spingendoli a rivelare con una certa facilità dati personali, immagini e informazioni che appartengono alla loro sfera privata, correndo rischi che non è il caso di sottovalutare. In realtà, bisogna sempre fare molta attenzione rispetto alla comunicazione di dati e informazioni personali, è facile perdere il controllo sulla loro diffusione. A volte, registrandosi su un social network, si può concedere al fornitore del servizio la possibilità di usare il materiale pubblicato online (foto, video, ecc.): è sempre bene, quindi, leggere con attenzione termini e condizioni di utilizzo. I rischi più comuni associati all'utilizzo dei social network da parte dei minori sono quelli di imbattersi in contenuti inappropriati, di essere vittima di episodi di cyberbullismo o peggio di predatori online, di subire o causare una violazione della privacy per aver (involontariamente) divulgato informazioni oppure di cadere in una truffa o avere interazioni con falsi profili che cercano di carpire dati personali o di coinvolgere i minori in attività illegali o pericolose. Un altro aspetto da valutare è l'uso eccessivo dei social network che può portare a dipendenza e a un impatto negativo sulla salute mentale dei minori. L'ossessione per i like, la comparazione con gli altri, la pressione sociale e la mancanza di interazioni faccia a faccia possono causare problemi come ansia, depressione e isolamento.

È importante che i genitori e gli educatori siano consapevoli di questi rischi e prendano misure per proteggere i minori, come l'educazione sui rischi e sulle pratiche di utilizzo sicuro dei social network, l'impiego di strumenti di controllo genitoriale, il monitoraggio delle attività online e il mantenimento di una comunicazione aperta con loro per affrontare eventuali problemi o preoccupazioni.

6.2. Cyberbullismo: un fenomeno diffuso

Il cyberbullismo rappresenta uno dei pericoli più gravi che bambini/e e adolescenti possono incontrare online. Si tratta di comportamenti aggressivi e dannosi che prevedono l'utilizzo di tecnologie digitali per molestare, minacciare, intimidire o danneggiare emotivamente individui o gruppi di persone. Questo comportamento è spesso ripetuto nel tempo, creando un ambiente ostile e dannoso per le vittime.

Il cyberbullismo trasporta il bullismo tradizionale dal mondo reale a quello virtuale, con la possibilità di un'ampia diffusione dei contenuti e l'anonimato che offre copertura agli aggressori. Questi possono utilizzare social network, messaggi istantanei, forum online e altri mezzi digitali per perpetrare i loro atti dannosi.

Le conseguenze del cyberbullismo possono essere gravi e durature, portando a problemi di salute mentale, isolamento sociale, ridotta autostima e, in alcuni casi estremi, anche al suicidio.

Per approfondire l'argomento del cyberbullismo dal punto di vista delle conseguenze legali, rimandiamo al paragrafo 8.11.

6.3. Doxing: la divulgazione delle informazioni personali

Un'altra minaccia online è rappresentata dal doxing, una pratica in cui gli aggressori cercano e diffondono informazioni personali e private di un'altra persona con l'intento di danneggiare la sua reputazione o esercitare pressioni su di essa. Queste informazioni possono includere nome, indirizzo, numero di telefono, e-mail e altre informazioni personali. Una volta che le hanno ottenute, gli aggressori possono diffonderle attraverso vari canali online, amplificando il danno inflitto alla vittima.

6.4. Sextortion: un pericolo in crescita

La sextortion è un'altra forma di estorsione online in cui gli aggressori minacciano di diffondere materiale sessualmente esplicito della vittima a meno che non soddisfi le loro richieste. Questo tipo di attacco sfrutta la vergogna e la paura che possono derivare dalla diffusione di materiale intimo per costringere la vittima a pagare o fornire altro materiale compromettente. Gli aggressori possono ottenere questo materiale illegalmente o attraverso l'ingegneria sociale online, ad esempio avvicinandosi alle vittime con apprezzamenti per delle foto pubblicate.

6.5. Haters

"Haters" è un termine informale utilizzato per descrivere persone che manifestano un forte e negativo disgusto o ostilità nei confronti di qualcun altro, spesso senza motivo apparente o con motivazioni superficiali. Questo comportamento può manifestarsi in vari contesti, sia online che offline, e coinvolgere una vasta gamma di situazioni e individui.

Gli hater possono esprimere il loro odio sia online, attraverso commenti negativi su social network, blog o forum, che offline, attraverso commenti sprezzanti o comportamenti ostili nella vita di tutti i giorni. Le motivazioni degli hater possono variare ampiamente. Possono essere spinti dalla gelosia, dall'invidia, dalla frustrazione personale o dalla mancanza di autostima. In alcuni casi, l'odio può essere alimentato da pregiudizi, intolleranza o semplicemente dalla volontà di danneggiare l'immagine o la reputazione di qualcuno.

Sulle piattaforme digitali, gli hater spesso si avvalgono dell'anonimato per esprimere le proprie opinioni negative senza rivelare la propria identità. Questo può portare a comportamenti più aggressivi e sfrenati rispetto a quelli che si avrebbero in situazioni faccia a faccia.

Essere il bersaglio degli hater può avere un impatto emotivo significativo. Le persone colpite possono sperimentare stress, ansia, depressione e persino effetti più gravi sulla loro salute mentale.

Le piattaforme digitali stanno cercando sempre più di combattere l'odio online attraverso politiche di moderazione, filtri anti-bullismo e la segnalazione di contenuti offensivi. Tuttavia, la sfida di gestire l'odio online rimane complessa, data la vastità e la velocità delle comunicazioni digitali.

In risposta agli hater è importante promuovere una cultura positiva online e offline incoraggiando il rispetto reciproco, la gentilezza e la consapevolezza delle parole e delle azioni.

6.6. Consigli utili

Vi è una sorta di galateo da rispettare all'interno del social network: sono norme sia di buona educazione per comportarsi correttamente all'interno di un contesto sociale, sia per rispettare la privacy altrui e tutelare la propria:

- ciò che si scrive sul profilo di un utente, è visibile da tutti gli amici di quell'utente e quindi bisogna fare attenzione a cosa si scrive. Evitare per esempio messaggi personali, o che riguardano la privacy di terze persone. Utilizzare sempre un linguaggio consono.
- evitare di pubblicare foto o filmati con persone riconoscibili senza il loro consenso, in particolare se non iscritte nel social network. Fare particolare attenzione quando si tratta di immagini che raffigurano minori. Evitare, inoltre, di ritrarre e pubblicare in un momento o in una posa imbarazzante: potrebbe risultare offensivo e avere ripercussioni sulla vita sociale, professionale e familiare della persona ritratta.
- utilizzare il proprio nome o un nickname nel profilo. Non fingersi un'altra persona o utilizzare il nome di un personaggio conosciuto, in Italia questa pratica è un reato e si chiama furto di identità.
- utilizzare con attenzione lo strumento del tag. È giusto taggare una persona in foto e video che lo raffigurano, in questo modo può decidere se comparire o no sul social network. È sbagliato taggare un altro utente in post, video o immagini a sproposito o allo scopo di metterlo in ridicolo.

7. Tecnologie emergenti: IoT, IA, Big Data

In questo capitolo, esploreremo alcune delle tecnologie emergenti che stanno ridefinendo i confini dell'innovazione. L'intersezione tra IoT, IA e Big Data promette di trasformare completamente il nostro mondo in modi che solo pochi anni fa sembravano appartenere al campo della pura fantascienza.

7.1. Internet delle cose (IoT)

L'Internet delle cose (Internet of Things) si riferisce a una rete di dispositivi fisici interconnessi che comunicano e scambiano dati tra di loro attraverso Internet. Questi dispositivi possono essere incorporati con sensori, software e altre tecnologie che consentono loro di raccogliere e scambiare informazioni. L'obiettivo principale dell'IoT è creare una rete intelligente in cui oggetti fisici possono interagire e collaborare senza necessità di intervento umano diretto.

L'IoT è una tecnologia già presente nella nostra vita di tutti i giorni, anche se spesso non ce ne rendiamo conto: ad esempio nel settore domestico, dove dispositivi connessi consentono il controllo remoto di luci, termostati, elettrodomestici e sistemi di sicurezza, migliorando il comfort e la sicurezza degli abitanti. Anche per quello che riguarda la salute, l'IoT sta rivoluzionando il monitoraggio medico, consentendo ai pazienti di tenere sotto controllo i loro parametri vitali attraverso dispositivi indossabili o sensori impiantati, mentre i professionisti sanitari possono accedere ai dati, anche da remoto, in tempo reale, per fornire cure più precise e tempestive. Nel settore retail è utilizzato per ottimizzare l'esperienza del cliente, per i trasporti è alla base del progresso verso la mobilità intelligente, nel settore industriale, è alla base della trasformazione digitale delle fabbriche, dove è utilizzato per la gestione efficiente delle risorse, l'aumento della produttività e la riduzione dei costi di produzione.

Un esempio tipico di applicazione di questa tecnologia è il suo impiego nella gestione delle smart city. L'Internet delle cose (IoT) è ampiamente impiegato nelle smart city per migliorare l'efficienza operativa, la sostenibilità ambientale, la sicurezza pubblica e la qualità dei servizi urbani. L'analisi della raccolta automatica di dati dai sensori viene utilizzata per la gestione del traffico, la riduzione del consumo energetico, la raccolta intelligente dei rifiuti, l'illuminazione pubblica, il monitoraggio della qualità dell'aria e dell'acqua, la sicurezza pubblica e molto altro ancora.

7.2. Intelligenza artificiale (IA)

L'intelligenza artificiale è l'abilità di una macchina di interpretare dati esterni, imparare da essi e utilizzare le informazioni acquisite per svolgere dei compiti e risolvere problemi. L'IA (o AI se si fa riferimento all'espressione inglese "artificial intelligence") si basa su algoritmi, ovvero sequenze di operazioni che consentono alla macchina di risolvere un problema o svolgere un compito. L'intelligenza artificiale ha oggi molte applicazioni nella vita quotidiana, basti pensare agli assistenti vocali (p. es. Google Home e Alexa), presenti negli smartphone, nelle case e anche nelle automobili.

Altre applicazioni riguardano la sostituzione dell'intervento umano in situazioni ad alto rischio o, in ambito sanitario, la sua applicazione per effettuare diagnosi sempre più precise. Recentemente è diventato molto famoso e diffuso l'utilizzo del servizio ChatGPT, un esempio di intelligenza artificiale "generativa" che permette di scrivere testi di vario tipo in base alle proprie esigenze, a partire da semplici indicazioni o domande scritte dall'utente nella propria lingua.

Naturalmente l'uso di queste tecnologie comporta alcune riflessioni di natura etica: non a caso la Commissione Europea ha emanato nel 2018 le Linee Guida Etiche sull'intelligenza artificiale sui requisiti necessari per una IA affidabile, rivolgendo il focus su argomenti quali la sicurezza, la riservatezza e la privacy dei dati e del materiale informatico.

Come abbiamo detto in precedenza, l'intelligenza artificiale ha una vasta gamma di applicazioni che rivoluzionerà numerosi settori, ma è già molto utilizzata in:

- **Medicina e assistenza sanitaria:** viene impiegata per diagnosticare malattie, prevedere epidemie, individuare anomalie nelle immagini mediche come radiografie e scansioni MRI (imaging a risonanza magnetica - Magnetic Resonance Imaging), e personalizzare i trattamenti per i pazienti.
- **Automotive:** nei veicoli autonomi, l'IA viene utilizzata per il riconoscimento di oggetti e pedoni, la pianificazione del percorso e il controllo del veicolo.
- **Finanza:** è impiegata per analizzare grandi quantità di dati finanziari, prevedere tendenze di mercato, individuare frodi e ottimizzare le decisioni di investimento.
- **E-commerce e marketing:** le aziende utilizzano l'IA per personalizzare l'esperienza degli utenti, raccomandare prodotti, analizzare i dati dei clienti e migliorare le strategie di marketing.
- **Assistenti virtuali e chatbot:** le tecnologie di intelligenza artificiale alimentano assistenti virtuali come Siri di Apple, Alexa di Amazon e Google Assistant, che forniscono risposte alle domande degli utenti, eseguono compiti vocali e interagiscono con dispositivi domestici intelligenti.
- **Produzione e robotica:** è impiegata per ottimizzare i processi di produzione, monitorare la qualità, automatizzare le operazioni e gestire i robot in ambienti industriali.

In futuro l'intelligenza artificiale promette di regalarci ulteriori sviluppi e applicazioni innovative.

L'IA generativa sta emergendo come una tecnologia rivoluzionaria che può creare contenuti originali come immagini, musica e testo e potrebbe essere utilizzata per la produzione creativa in vari settori, dall'intrattenimento alla progettazione. Con l'avanzamento dell'IA, sarà possibile anche prevedere e prevenire le malattie in modo più efficace, offrendo cure mediche personalizzate e tempestive.

I veicoli autonomi potrebbero diventare la norma, trasformando radicalmente il settore dei trasporti e riducendo il numero di incidenti stradali. L'IA potrebbe essere fondamentale anche per l'esplorazione spaziale, consentendo ai robot e alle sonde spaziali di eseguire compiti complessi autonomamente in ambienti ostili come lo spazio.

L'integrazione tra intelligenza artificiale e calcolo quantistico potrebbe portare a una nuova era di elaborazione dei dati, consentendo prestazioni e capacità di calcolo senza precedenti.

Anche il mondo del lavoro potrebbe essere travolto dall'avvento dell'IA cambiando il modo in cui lavoriamo, i lavori che svolgiamo e le competenze di cui abbiamo bisogno per avere successo. L'automazione sostituirà molte attività di routine con il risultato che saranno sempre più richieste figure che abbiano creatività, pensiero critico e capacità di risoluzione dei problemi e creando nuove opportunità di lavoro in campi come l'analisi dei dati, l'apprendimento automatico e la sicurezza informatica.

Ad esempio, si parla molto dei prompt Engineer, un nuovo tipo di professionista che sa impostare e testare gli input e gli output dei modelli generativi fornendo loro un contesto appropriato.

In Italia, i dati dell'Osservatorio Artificial Intelligence della School of Management del Politecnico di Milano del 2022 riportano che il mercato dell'intelligenza artificiale valeva 500 milioni di euro con una crescita del 32% rispetto all'anno precedente e che più di 6 grandi aziende su 10 avevano già avviato almeno un progetto nel campo dell'IA.

Immaginare le ricadute di tutto questo nella vita quotidiana ci fa capire che l'intelligenza artificiale è la tecnologia più promettente del nostro tempo e proprio per questo l'attenzione sull'etica e la responsabilità nell'IA diventerà sempre più importante.

7.3. Big Data

Il concetto di Big Data fa riferimento a un insieme massiccio e complesso di dati che richiede l'utilizzo di strumenti specializzati, diversi da quelli tradizionali, in tutte le fasi del loro ciclo di vita. Questo ciclo comprende l'acquisizione, l'elaborazione, la condivisione, l'analisi e la visualizzazione dei dati.

I Big Data sono composti da informazioni provenienti da una vasta gamma di fonti, a differenza dei dati strutturati presenti in database ordinati, possono includere immagini, email, dati GPS e informazioni provenienti dai social network. La diversità di queste fonti arricchisce ulteriormente il contesto dei dati, offrendo opportunità uniche di analisi e comprensione.

Per stimare la quantità di Big Data esistenti ad oggi occorre ricorrere agli Zettabyte, corrispondenti a miliardi di Terabyte (1 Zettabyte = 10^21 byte e un Terabyte sono 1.000 Gigabyte, cioè 10^12 byte). Questa quantità colossale di dati riflette la crescente digitalizzazione della nostra società e l'esplosione di informazioni generate dagli utenti, dai sensori, dai dispositivi connessi e da altre fonti digitali.

L'analisi dei Big Data è cruciale in molteplici settori, tra cui scienze, industria, sanità, finanza e governance. L'implementazione di strumenti avanzati di analisi, machine learning e intelligenza artificiale consente di scoprire correlazioni significative e tendenze emergenti, fornendo indicazioni fondamentali per prendere decisioni informate e ottimizzare processi complessi.

Gioco da tavolo "Internetopoli"

8. La cybersecurity

La cybersecurity è la difesa del cyberspazio, inteso come insieme di sistemi informatici, dei servizi della Rete e dei dati in formato digitale. Questa definizione fa capire quanto sia ampio l'ambito d'azione di questa disciplina. Tutto il mondo digitale oggi è potenzialmente sotto attacco: cellulari, pc, tablet, smart tv, elettrodomestici e oggetti di uso quotidiano "smart", siti web, server e data center.

8.1. I cardini della sicurezza informatica

Quali sono le caratteristiche che rendono un sistema informatico sicuro?

- **Riservatezza:** i dati e le risorse sono protetti dal possibile utilizzo o accesso da parte di soggetti non autorizzati.
- **Integrità:** i dati e le risorse non possono essere modificati o cancellati, se non ad opera di soggetti autorizzati.
- **Disponibilità:** si riferisce alla possibilità, per i soggetti autorizzati, di poter accedere alle risorse per tutto il tempo necessario e in modo ininterrotto.

8.2. Un po' di storia

La storia della sicurezza informatica è strettamente legata all'evoluzione della tecnologia e alla crescente complessità delle reti digitali ed è stata costantemente presente e in evoluzione negli ultimi 60 anni di trasformazione digitale.

I primi incidenti risalgono agli anni '50 con il phone phreaking (manipolazione dei sistemi telefonici per ottenere accesso a servizi a pagamento o per effettuare chiamate gratuite), e prosegue negli anni '60 con l'avvento dei primi computer e delle prime reti, quando le preoccupazioni principali riguardavano principalmente l'accesso non autorizzato ai sistemi. Durante questo periodo, sono state messe in atto le prime tecniche di protezione, come le password e le restrizioni di accesso, sviluppate per proteggere i sistemi mainframe.

Negli anni '80, con la diffusione dei personal computer e delle reti locali, sono emersi i primi virus informatici e worm. Gli anni '90 hanno visto la proliferazione di minacce online più sofisticate, come i malware, gli attacchi DDoS (Distributed Denial of Service) e le vulnerabilità dei software. Questo periodo ha anche assistito alla nascita delle prime aziende specializzate in sicurezza informatica e alla creazione dei primi standard e protocolli per la sicurezza dei dati.

Negli anni 2000 con l'aumento dell'uso di Internet e la diffusione globale della tecnologia digitale, gli attacchi informatici sono diventati sempre più diffusi e sofisticati. Hanno fatto la loro comparsa minacce come il phishing, il ransomware e lo spionaggio informatico, portando a una maggiore consapevolezza e alla necessità di soluzioni di sicurezza più avanzate. In questi anni si è iniziato a parlare anche di privacy online e protezione dei dati personali e sono stati introdotti regolamenti come il GDPR in Europa e leggi simili in altre parti del mondo. Questi regolamenti hanno posto un'enfasi maggiore sulla responsabilità delle organizzazioni nel proteggere le informazioni sensibili dei loro utenti.

Dal 2011 in poi la sicurezza informatica si è concentrata sulla gestione delle sfide emergenti, come la protezione delle reti IoT, la difesa contro gli attacchi IA e la crescente minaccia della cyber guerra.

Gli anni recenti, inclusi quelli a cavallo della pandemia COVID-19, e il conflitto Russo-Ucraino, hanno ulteriormente complicato il panorama della minaccia informatica. Il cybercrime ha superato altre attività illecite come lo spaccio e la prostituzione, diventando il principale mezzo di finanziamento illecito. Inoltre, il cyberspazio è diventato il luogo di scontro per la contrapposizione geopolitica, con obiettivi che mirano a destabilizzare o influenzare le opinioni pubbliche attraverso la disinformazione e la propaganda.

8.3. Vulnerabilità e attacchi

Si parla di "vulnerabilità" per indicare un punto debole di un sistema informatico, che può essere sfruttato per danneggiarlo. Un esempio di debolezza può essere, ad esempio, un sistema operativo o un antivirus non aggiornato, una password non sicura o un errore nel codice di un programma, detto bug. Il termine "bug" significa "piccolo insetto". Nel 1947 Grace Hopper, tenente della marina statunitense, stava cercando di capire per quale motivo il computer Mark II non funzionasse. Smontandolo, si rese conto che la causa era una falena incastrata tra i circuiti. Da allora il termine 'bug" per indicare un malfunzionamento di un programma è entrato nell'uso comune.

Gli attacchi informatici avvengono perché qualcuno (detto "attaccante" o più comunemente "hacker"), decide intenzionalmente di danneggiare un sistema, sfruttando, spesso, una vulnerabilità. Oggi esistono diversi tipi di hacker: quelli che scoprono le vulnerabilità e avvisano le potenziali vittime per porre subito rimedio (hacker etici) e quelli che agiscono al solo scopo di danneggiare la vittima (cracker).

I principali obiettivi degli attacchi sono:

- furto di dati (data breach)
- compromissione di un servizio/infrastruttura
- di natura politica, ideologica (si parla di "hactivism", come nel caso del movimento "Anonymous".

8.4. Le contromisure

Il processo di autenticazione nei sistemi informatici rappresenta una garanzia dell'identità di un utente e dunque uno strumento per evitare vari pericoli, dal furto di identità, al furto di dati.

Prima di accedere all'interno di un sito o di un sistema, un utente deve dimostrare la propria identità. I principali metodi per autenticarsi sono tramite username e password o tramite parametri biometrici (impronta digitale, iride, riconoscimento facciale).

La doppia autenticazione, presente ormai nella maggior parte dei servizi web e delle applicazioni, è un processo che avviene in due passaggi e, per questo motivo, è considerato ancora più robusto. La utilizziamo quando, per esempio, riceviamo un SMS sul nostro cellulare con un codice da inserire nel login per accedere a un'app o a un sito.

Altra contromisura della cybersecurity è la crittografia. La parola deriva dal greco "kryptos" che significa "nascosto" e da "graphia" che significa "scrittura". La crittografia ha origini molto antiche, veniva usata nell'antica Grecia, dai romani fino ai nostri giorni con lo scopo di rendere illeggibile un messaggio alle persone non autorizzate. La crittografia di oggi si basa su complesse tecniche matematiche e algoritmi informatici. La cifratura di un messaggio trasforma un messaggio in chiaro in uno cifrato: la sicurezza è data dalla robustezza dell'algoritmo e dalla segretezza della chiave di decifratura.

Un'altra contromisura importante è rappresentata dagli antivirus, software finalizzati a prevenire, rilevare ed eventualmente eliminare codici dannosi e malware per un computer o più in generale per un dispositivo. L'antivirus deve essere costantemente aggiornato in modo che possa riconoscere e rendere inoffensivi anche i nuovi virus.

Come ultima contromisura citiamo i firewall (letteralmente "muro tagliafuoco"), una componente hardware e/o software di difesa perimetrale che controlla il traffico di dati di una Rete in entrambe le direzioni per impedire l'entrata o l'uscita di connessioni pericolose per il sistema.

8.5. Il rischio informatico

Il rischio informatico si riferisce alla possibilità che un evento dannoso si verifichi in un ambiente informatico, causando perdite finanziarie, danni alla reputazione, interruzioni delle operazioni o compromissione della sicurezza dei dati. Questi rischi possono derivare da una serie di fattori, tra cui vulnerabilità dei sistemi, minacce esterne o interne, errori umani, mancanza di controlli adeguati e altro ancora.

Il rischio informatico non riguarda solo le organizzazioni, le aziende ma coinvolge tutte le persone che utilizzano dispositivi connessi a Internet, come smartphone, tablet, computer e dispositivi IoT (Internet of Things), come SmartTV, telecamere e elettrodomestici intelligenti.

Con il continuo aumento dell'informatizzazione e della connettività globale, le minacce informatiche sono in costante crescita, adattandosi ai progressi tecnologici per sfruttare le vulnerabilità a vantaggio degli attaccanti. Studi recenti hanno rilevato un aumento significativo degli attacchi informatici nel mondo e non solo in Italia, con un'azienda che subisce un attacco ransomware ogni 11 secondi nel 2021, rispetto a uno ogni 14 secondi nel 2019. Si prevede che la frequenza degli attacchi ransomware continuerà a crescere, arrivando a una media di uno ogni 2 secondi entro il 2031. Si stima che il costo complessivo del cybercrime nel mondo raggiungerà i 10.5 trilioni di dollari entro il 2025, rendendo il crimine informatico la terza economia mondiale.

Il World Economic Forum ha inserito il cybercrime nella lista dei 10 principali rischi mondiali per i prossimi 10 anni, sottolineando l'importanza cruciale di comprendere i rischi e le minacce informatiche che le persone affrontano ogni giorno. Questo è particolarmente importante per coloro che lavorano con bambini e adolescenti che sono cresciuti nell'era digitale e possono avere una maggiore familiarità con Internet e le app rispetto agli adulti.

È quindi essenziale educare i giovani sui rischi associati al mondo online, evidenziando che quello che accade nel mondo virtuale può avere gravi conseguenze nella vita reale. I ragazzi devono essere consapevoli dei rischi presenti su Internet e sulle applicazioni che utilizzano, perché possono essere più insidiosi e difficili da riconoscere nel mondo digitale rispetto al mondo reale.

8.6. Gli attacchi informatici e i malware

Esistono diverse modalità attraverso le quali gli attaccanti informatici possono compromettere la sicurezza dei sistemi e delle informazioni. Ecco una panoramica delle principali tipologie di attacchi informatici:

- **Phishing:** riguarda l'invio di messaggi o e-mail fraudolenti, che cercano di ingannare la vittima convincendola a fornire dati sensibili come informazioni personali, finanziarie, codici di accesso o password. Gli hacker fingono di essere entità affidabili per ottenere queste informazioni. È importante prestare attenzione all'indirizzo e-mail del mittente e all'URL dei siti web, che devono essere autentici.
- **Ingegneria sociale:** si basa sulla manipolazione psicologica delle persone per ottenere informazioni riservate o per compiere azioni non autorizzate. Gli hacker possono raccogliere informazioni sulle vittime e sui loro interessi attraverso i social media e altri canali online per personalizzare gli attacchi.
- **Forza bruta:** è il tentativo di violare la sicurezza di un sistema tramite la generazione automatica di una vasta gamma di possibili combinazioni di password fino a trovare quella corretta. È fondamentale utilizzare password sicure per proteggersi da questo tipo di attacco.
- **Denial of Service (DoS):** mira a rendere inaccessibili i sistemi o le reti sovraccaricandoli con un grande volume di richieste. In questo modo, gli utenti legittimi non riescono più ad accedere ai servizi.
- **Hacking:** gli attacchi di hacking sfruttano vulnerabilità nei sistemi o nelle applicazioni per ottenere accesso non autorizzato o per manipolare le funzionalità del sistema. Questo può consentire agli hacker di accedere a dati sensibili o di compromettere l'integrità del sistema.

Nella maggior parte dei casi gli attacchi si realizzano con l'aiuto di programmi malevoli, chiamati malware (che è la contrazione delle parole malicious e software, programma malvagio). Ce ne sono di vario tipo, e le vittime spesso non si accorgono della loro presenza. Queste sono alcune delle più comuni azioni che possono portare all'installazione involontaria di questi programmi malevoli:

- aprire file o link inviati via email o chat
- scaricare programmi, app, film ecc. da siti non ufficiali

Nel caso di mail e chat i messaggi sono scritti in modo molto convincente per spingere la vittima a fare clic.

Come capire se un dispositivo è vittima di un malware?

- si blocca e si arresta in modo anomalo;
- è più lento;
- i file si modificano o scompaiono;
- ci sono file, programmi o icone desktop sconosciuti;
- i programmi si disattivano o riconfigurano autonomamente;
- si inviano e-mail senza esserne a conoscenza.

Questi i malware più diffusi:

- Virus: una volta eseguito, infetta i file facendo copie di sé stesso;
- Trojan Horse: si nasconde dietro un programma apparentemente innocuo (come evoca il suo nome);
- Worm: si auto replica in modo automatico, senza dover infettare un file ma sfruttando la Rete Internet;
- Ransomware: prende sotto sequestro un dispositivo, rendendolo inutilizzabile, e chiede un riscatto in monete virtuali per lo sblocco dei file e dei dati;
- Spyware: spia e registra le azioni dell'utente, come ad esempio i movimenti delle dita sulla tastiera;
- Adware: apre messaggi pubblicitari indesiderati in forma di pop up.

8.7. Gestione degli account e delle password

È cruciale gestire correttamente gli account e le password nei dispositivi e online. Occorre sempre evitare di salvare le credenziali sui dispositivi e disconnettere i profili personali al termine delle sessioni di navigazione.

In ambito di protezione dei dispositivi, è consigliabile seguire queste pratiche:

- Aggiornamento automatico: configurare i dispositivi per gli aggiornamenti automatici di app e sistema operativo.
- Antivirus: installare e configurare antivirus per evitare connessioni non autorizzate al Wi-Fi pubblico.
- Crittografia per dispositivi portatili: utilizzare la crittografia per dispositivi portatili e durante la trasmissione di dati.
- Password complesse e autenticazione a due fattori: possono migliorare la sicurezza.
- Backup dei dati: effettuare regolarmente backup dei dati e utilizzare software di cancellazione per eliminare definitivamente i dati dai dispositivi obsoleti.

8.8. Cyber hygiene

La cyber hygiene, anche conosciuta come igiene digitale o sicurezza informatica personale, si riferisce alla pratica di adottare comportamenti e abitudini sicure quando si utilizzano dispositivi digitali e si naviga su Internet. È essenzialmente una serie di pratiche e precauzioni volte a proteggere la propria privacy, sicurezza e benessere online. Ecco alcuni aspetti chiave della cyber hygiene:

- **Utilizzare password sicure:** si consiglia di utilizzare password complesse e uniche per ogni account online, evitando password facilmente indovinabili come "123456" o "password". È importante anche cambiare regolarmente le password e abilitare l'autenticazione a due fattori quando disponibile.
- **Aggiornare regolarmente il software:** mantenere aggiornati sistemi operativi, applicazioni e software antivirus è fondamentale per proteggere i dispositivi da vulnerabilità e minacce informatiche.
- **Navigare in modo sicuro:** fare attenzione ai siti web visitati e evitare di cliccare su link sospetti o scaricare file da fonti non attendibili. Utilizzare connessioni Internet sicure, ad esempio reti Wi-Fi protette da password, e evitare di connettersi a reti pubbliche non sicure quando si effettuano operazioni sensibili online.
- **Proteggere la privacy:** limitare la condivisione di informazioni personali online e prestare attenzione alle impostazioni di privacy su social media e altri siti web. Utilizzare impostazioni di privacy robuste e non condividere informazioni sensibili con sconosciuti.
- **Essere consapevoli delle truffe online:** saper riconoscere e evitare truffe online, come phishing, frodi finanziarie e truffe di identità. Essere cauti quando si ricevono email o messaggi sospetti e non fornire mai informazioni personali o finanziarie a fonti non attendibili.
- **Fare il backup dei dati:** effettuare regolarmente il backup dei dati importanti su dispositivi esterni o servizi cloud affidabili per proteggerli da perdite o danni.
- **Educarsi continuamente:** mantenersi informati sulle ultime minacce informatiche, tecniche di phishing e migliori pratiche di sicurezza informatica. Partecipare a corsi di formazione sulla sicurezza informatica e seguire risorse affidabili online per rimanere aggiornati.

8.9. Ingegneria sociale

Un aspetto critico della cyber hygiene riguarda l'ingegneria sociale, ovvero la manipolazione consapevole delle persone per ottenere informazioni sensibili. Per contrastare l'ingegneria sociale bisogna stare molto attenti ai propri comportamenti, ad esempio:

- **diffidare dei contatti non richiesti:** non rispondere a telefonate, visite o email non richieste che chiedono informazioni sensibili.
- **Evitare conversazioni sensibili in luoghi pubblici:** non discutere in luoghi pubblici di informazioni personali o sensibili.
- **Limitare le informazioni sui social media:** evitare di condividere informazioni personali sui social media per ridurre la possibilità di essere una potenziale vittima.
- **Verificare richieste sospette:** non fornire informazioni personali o finanziarie senza verificare l'autenticità della richiesta.
- **Utilizzare software di sicurezza:** installare e mantenere aggiornati software antivirus, firewall e filtri email.
- **Utilizzare strumenti anti-phishing:** sfruttare le funzionalità anti-phishing dei client di posta elettronica e dei browser web.

8.10. Misure di protezione

Nel contesto aziendale o scolastico, l'ENISA ovvero l'agenzia dell'Uniore Europea per la cibersicurezza, con la pubblicazione "Review of Cyber Hygiene practices," identifica cinque principali aree di intervento per garantire la sicurezza informatica:

1. **Protezione del perimetro:** comprende la sicurezza di tutti gli ambienti digitali, inclusi dispositivi, applicazioni, hardware e software, che potrebbero essere vulnerabili agli attacchi. Oggi, con l'utilizzo del Cloud, dei dispositivi personali e dello smart working, la definizione del perimetro è diventata meno definita e più difficile da gestire.
2. **Protezione della rete:** riguarda la sicurezza dei collegamenti digitali utilizzati per accedere, gestire e lavorare con hardware e software.
3. **Protezione dei singoli dispositivi:** coinvolge l'utilizzo di software di sicurezza installato su ciascun dispositivo digitale smart per garantirne la protezione.
4. **Utilizzo sicuro del cloud:** implica l'adozione di protezione a doppio fattore per l'accesso e l'implementazione di crittografia per i dati memorizzati nel cloud.
5. **Protezione della catena di approvvigionamento:** assicura che i fornitori adottino adeguate misure di sicurezza per i prodotti e servizi forniti all'organizzazione.

Per implementare efficacemente queste pratiche di cyber hygiene, è consigliabile far gestire dalla scuola alcune attività. Buone pratiche da mettere in atto sono: mantenere un registro aggiornato di tutto l'hardware e il software per garantire una lista completa dei dispositivi da proteggere, tenere traccia di tutto il software e applicare regolarmente le patch di sicurezza, utilizzare guide di configurazione/hardening per rafforzare la sicurez-

za dei dispositivi, scansionare le email in arrivo, gestire i dati in entrata/uscita dalla rete LAN e adottare connessioni sicure durante il lavoro in smart working. Altre attività da mettere in atto sono quelle di eseguire regolarmente il backup dei dati e testare la loro ripristinabilità, stabilire un piano dettagliato di azioni da intraprendere in caso di violazione informatica, garantire controlli di sicurezza in qualsiasi contratto di servizio, inclusi quelli in ambienti cloud.

Altrettanto importanti sono le azioni in ambito di formazione e consapevolezza con la programmazione di corsi dedicati al personale sugli aggiornamenti riguardanti la sicurezza informatica che comprendano sia aspetti teorici che pratici.

8.11. Conseguenze legali delle azioni online

L'onnipresenza delle tecnologie nella nostra vita quotidiana ha reso l'accesso alle informazioni e ai servizi più facile che mai, ma ha anche esposto i minori a rischi come contenuti inappropriati, disturbi e violazioni della privacy. È importante notare che le azioni compiute online possono avere conseguenze nella vita reale e possono persino violare la legge.

Per comprendere meglio perché ciò accade, è importante considerare il modo in cui le persone percepiscono le azioni compiute attraverso le tecnologie rispetto a quelle compiute nella vita fisica. Studi di psicologia e sociologia hanno dimostrato che le azioni compiute online sono spesso percepite come meno gravi rispetto a quelle compiute offline. Ad esempio, scaricare illegalmente contenuti digitali è spesso considerato meno grave rispetto al furto di beni fisici da un negozio.

Questo fenomeno può essere attribuito a diversi fattori. Innanzitutto, esiste la falsa convinzione che l'anonimato online sia garantito. Inoltre, la facilità con cui è possibile accedere a contenuti online può far sembrare che tutto sia permesso e disponibile con un semplice clic. Le interazioni online spesso mancano del contatto diretto e immediato con le persone coinvolte, il che può ridurre la percezione degli impatti negativi delle azioni online.

Come educatori, dobbiamo quindi essere consapevoli di questo effetto potenzialmente distorsivo dei valori etici e morali e insegnare ai giovani che le azioni compiute online possono avere conseguenze serie, sia online che offline. È importante far loro capire che Internet non è un mondo separato dalla realtà, ma piuttosto un'estensione di essa, dove le azioni hanno conseguenze reali.

Nel contesto scolastico, gli/le insegnanti hanno il compito di far comprendere ai ragazzi che alcune azioni online possono essere illegali e perseguibili per legge. È importante educare le giovani generazioni sulle conseguenze delle loro azioni e promuovere un comportamento responsabile e rispettoso sia online che offline.

Solo per fare un esempio possiamo considerare quali siano le conseguenze legali derivanti da atti di cyberbullismo.

Il cyberbullismo rappresenta una forma moderna di bullismo, dove le condotte di sopraffazione e prevaricazione vengono attuate attraverso mezzi elettronici e tecnologie digitali. Questo fenomeno è stato definito per la prima volta nella legge n. 71/2017, la quale lo descrive come qualsiasi forma di pressione, aggressione, molestia, ricatto, ingiuria,

denigrazione, diffamazione, furto di identità, alterazione, acquisizione illecita, manipolazione o trattamento illecito di dati personali effettuati per via telematica, con l'intenzione predominante di isolare e danneggiare un minore o un gruppo di minori.

Le conseguenze del cyberbullismo possono essere sia penali che civili. A livello penale, anche se non esiste un reato specifico di cyberbullismo nel nostro ordinamento, le azioni del cyberbullo possono configurare diverse violazioni, come lesioni personali, diffamazione, violenza privata, minacce, stalking, molestie o disturbi alla persona, tra gli altri.

Dal punto di vista civile, le vittime di cyberbullismo hanno il diritto di chiedere un risarcimento per il danno subito. Secondo l'articolo 2043 del Codice civile, chiunque causa un danno ingiusto a un'altra persona è obbligato a risarcire il danno, sia che il fatto sia stato compiuto dolosamente che per colpa.

È importante sottolineare che, mentre la responsabilità penale è personale, sul piano civile le conseguenze delle azioni di un minore possono coinvolgere anche i genitori e gli educatori. L'articolo 2048 del Codice civile stabilisce una forma di responsabilità per "culpa in vigilando", che implica che i genitori e gli educatori possono essere ritenuti responsabili per le azioni illecite dei minori se non dimostrano di aver esercitato la dovuta vigilanza per prevenirle. In pratica, ciò significa che i genitori potrebbero essere considerati responsabili per i danni causati dai loro figli minori, mentre gli/le insegnanti e le istituzioni scolastiche potrebbero essere chiamati a rispondere per i danni derivanti da condotte illecite commesse all'interno dell'ambiente scolastico, se è dimostrato che non hanno esercitato un adeguato controllo sui minori a loro affidati.

Laboratorio scuole primarie di primo grado

9. Identità digitale

L'identità digitale comprende tutte le informazioni personali che ci definiscono in modo univoco su Internet: dai profili sui social media ai siti web personali o professionali, passando per informazioni sensibili come nomi, indirizzi email, password, codici fiscali e dati finanziari. Questo concetto include anche strumenti come lo SPID, la CIE e la CNS, che consentono l'accesso sicuro ai servizi online.

La nostra identità digitale, che include professione, interessi, opinioni e altro ancora, rappresenta ciò che gli altri possono scoprire di noi tramite una semplice ricerca online. Quando qualcuno cerca il nostro nome su Internet, l'immagine che emerge avrà un impatto significativo sulla percezione che si formerà di noi.

9.1. La memoria della rete

I dati e le informazioni che noi stessi immettiamo nella Rete costituiscono un enorme serbatoio di memoria collettiva a cui tutti attingiamo. L'esempio per antonomasia è certamente Wikipedia, ma anche le foto condivise tra amici e parenti, documenti di lavoro comuni a più gruppi e più persone, racconti e documentazione di fatti e avvenimenti, che possiamo sempre consultare, cercandoli online. In definitiva, ancora un'opportunità. Ma c'è anche in questo caso un rovescio della medaglia: in Rete non c'è diritto all'oblio. Chi immette in Rete un'informazione deve sapere che non potrà cancellarla definitivamente: qualcuno potrebbe averla memorizzata, o potrebbe aver salvato anche un semplice screenshot e potrebbe renderla di nuovo pubblica in qualunque momento. Questo aspetto deve far riflettere e suggerire prudenza nel "postare" immagini, commenti e informazioni tipicamente sui social network, ma non solo, perché, anche se dovessimo pentirci, non potremmo tornare indietro e non basterebbe semplicemente chiedere scusa. L'invito che facciamo ai ragazzi e alle ragazze è di usare con giudizio l'opportunità di condividere i propri dati, la storia personale e le proprie informazioni: non sempre teniamo completamente aperte le finestre di casa, ci sono momenti privati in cui tiriamo le tende; non sempre possiamo dire senza filtri quello che pensiamo, per non ferire o offendere chi abbiamo davanti. Dobbiamo imparare che nella Rete esistono gli stessi limiti di buon senso e civile convivenza della vita reale.

9.2. Web reputation

Nell'attuale contesto interconnesso e digitalizzato, l'identità digitale e la web reputation giocano un ruolo fondamentale per ognuno di noi. La nostra vita si dipana sia online che offline, e queste due dimensioni sono strettamente intrecciate. Nella vita di tutti i giorni, siamo naturalmente inclini a curare l'immagine che desideriamo trasmettere agli altri, sia nel comportamento che nell'aspetto, cercando di essere autentici e coerenti con noi stessi. Anche online, i nostri comportamenti, i commenti e i contenuti che condividiamo contribuiscono a plasmare l'immagine che gli altri si formano di noi, intrecciandosi inevitabilmente con quella offline.

La web reputation, o reputazione online, si riferisce alla percezione complessiva che gli altri hanno di un individuo, di un'azienda o di un marchio basata sulle informazioni e sulle interazioni presenti su Internet. Questa reputazione è influenzata da una serie di fattori, tra cui recensioni, commenti, post sui social media, articoli di notizie, blog e altro ancora.

La web reputation può avere un impatto significativo sull'immagine e sulla credibilità di un individuo o di un'organizzazione, influenzando le opinioni degli altri e le decisioni di acquisto, di assunzione o di collaborazione. Una buona reputazione online può portare a maggiori opportunità di lavoro, partnership commerciali redditizie e una maggiore fiducia da parte del pubblico. Al contrario, una reputazione online negativa può danneggiare la credibilità, l'affidabilità e la fiducia nell'individuo o nell'azienda, riducendo le opportunità e danneggiando il marchio.

È importante monitorare attentamente la propria web reputation e gestire attivamente le informazioni online per mantenere una buona reputazione e mitigare eventuali danni causati da contenuti negativi o diffamatori. Ciò può includere la gestione delle recensioni, il coinvolgimento attivo sui social media, la risposta tempestiva a commenti negativi e l'adozione di strategie di marketing online mirate a promuovere una reputazione positiva.

Presentarsi in modo positivo e coerente con ciò che vogliamo rappresentare e far conoscere di noi è essenziale per costruire una web reputation solida e affidabile.

9.3. Rischi associati all'identità digitale

Tra i principali rischi legati all'identità digitale c'è il furto di identità che è un reato grave, in cui un criminale può accedere illegalmente alle informazioni personali di un individuo per danneggiarne la reputazione o commettere frodi finanziarie. Questo può essere particolarmente dannoso per figure pubbliche, come politici o personaggi dello spettacolo, il cui prestigio dipende spesso dalla gestione accurata dell'immagine online. Il furto di credenziali può anche portare a danni economici diretti, specialmente se coinvolge informazioni sensibili come le carte di credito.

La protezione dell'identità digitale richiede un approccio proattivo da parte degli utenti. È essenziale rendere privati i propri profili online, limitare i permessi concessi alle app di terze parti, e negare il consenso ai cookie non rilevanti. Inoltre, è fondamentale condividere il minor numero possibile di dati personali e utilizzare password uniche e complesse per proteggere gli account online, aggiornare regolarmente le app e usare l'autenticazione a due fattori sono altre pratiche consigliate per migliorare la sicurezza online.

Allo stesso modo, è importante essere consapevoli dell'identità digitale degli altri e delle possibili implicazioni delle interazioni online. Prima di accettare collegamenti o interagire con persone sconosciute, è consigliabile esaminare attentamente i loro profili e valutare la coerenza dei loro contenuti e comportamenti con i propri valori e interessi. È essenziale ricordare che dietro ogni account online c'è una persona reale, con dignità e reputazione e comportarsi con rispetto e gentilezza per mantenere un ambiente civile e sicuro: a volte i profili sono privi di contenuti e questo dovrebbe farci insospettire. Fenomeni come l'odio online, il body shaming e il cyberbullismo sono gravi violazioni dell'identità digitale e reale delle persone e possono avere conseguenze devastanti, spesso configurandosi come reati punibili dalla legge. È quindi importante promuovere comportamenti responsabili e rispettosi online, riflettendo sulle conseguenze delle proprie azioni e parole nell'ambiente digitale.

Laboratorio scuole primarie

10. Comunicazione digitale

Quando parliamo di comunicazione digitale, ci riferiamo a qualsiasi contenuto testuale, visivo o audio prodotto con le tecnologie digitali (come PC, tablet, smartphone, ecc.) e diffuso tramite il web. Ciò che distingue quindi la comunicazione digitale da quella analogica o tradizionale è il mezzo utilizzato: il digitale.

I contenuti digitali possono assumere diverse forme, tra cui testi (come post sui social network, articoli di blog o di magazine online, email), immagini (come foto su Instagram o Facebook), video (come contenuti visivi su YouTube o TikTok) e audio (come podcast).

La comunicazione digitale si differenzia da quella tradizionale perché è inclusiva (chiunque può comunicare digitalmente) e bidirezionale (il ricevente può partecipare attivamente interagendo con il mittente).

Ogni volta che produciamo un contenuto digitale, lasciamo una traccia sul web, composta dalla serie di dati memorizzati derivanti da tutte le nostre attività online. Più utilizziamo Internet, più ampia diventa l'impronta digitale (digital footprint) che lasciamo, aumentando di conseguenza il rischio correlato alla sicurezza dei nostri dati.

10.1. La Netiquette

In Rete esiste un insieme di regole di condotta chiamate "Netiquette" (il documento ufficiale è il cosiddetto RFC 1885), che derivano dalla combinazione dei termini "net" (Rete) e "etiquette" (buona educazione). Queste regole ci guidano verso una comunicazione rispettosa e appropriata in Internet, promuovendo il rispetto degli altri. Alcuni esempi includono evitare l'uso esclusivo di lettere maiuscole, che corrisponde a urlare nel mondo reale, chiedere il permesso prima di condividere foto di altre persone e evitare termini offensivi o comportamenti da bullismo digitale.

10.2. Un linguaggio nuovo: il gergo di Internet

Nell'era digitale in cui viviamo, la comunicazione ha subito una trasformazione radicale. Non solo il modo in cui ci connettiamo è cambiato, ma anche il linguaggio che utilizziamo per comunicare online ha subito un'evoluzione significativa. Questo nuovo linguaggio, spesso definito come il "gergo di Internet", è diventato una caratteristica distintiva della cultura online, con una vasta gamma di espressioni, acronimi e termini che sono diventati comuni tra gli utenti di tutto il mondo.

Il gergo di Internet ha le sue radici nelle prime comunità online degli anni '90, quando l'accesso a Internet era limitato e le interazioni avvenivano principalmente attraverso forum di discussione e chat room. In queste piattaformesi è sviluppato uno stile di comunicazione unico, caratterizzato da abbreviazioni, emoticon ed espressioni idiomatiche.

Una delle caratteristiche distintive del gergo di Internet è l'uso diffuso di acronimi e abbreviazioni. Queste abbreviazioni sono spesso utilizzate per risparmiare tempo e spazio di battitura e sono diventate parte integrante della comunicazione online. Ad esempio, "LOL" (Laughing Out Loud) viene utilizzato per indicare risate, "OMG" (Oh My God) per esprimere sorpresa, e "BTW" (By The Way) per introdurre un'osservazione laterale.

Oltre agli acronimi, il gergo di Internet include una vasta gamma di espressioni idiomatiche e neologismi. Questi termini possono derivare da diverse fonti, tra cui la cultura pop, il meme online e la lingua giovanile. Ad esempio, espressioni come "FOMO" (Fear Of Missing Out), "YOLO" (You Only Live Once) e "TL;DR" (Too Long; Didn't Read) sono diventate comuni nel linguaggio digitale.

Il gergo di Internet svolge diverse funzioni nella comunicazione online. In primo luogo, aiuta a facilitare la comunicazione rapida e informale, consentendo agli utenti di esprimere concetti complessi in modo conciso e diretto e può essere utilizzato per creare un senso di appartenenza e identità all'interno delle comunità online, con gli utenti che adottano e condividono termini e espressioni specifiche del loro gruppo.

Come tutte le forme di linguaggio, il gergo di Internet è in costante evoluzione. Nuovi termini e espressioni vengono costantemente introdotti e adottati dalle comunità online, riflettendo i cambiamenti culturali e tecnologici, con alcuni termini che possono diventare obsoleti nel tempo mentre altri diventano parte permanente del vocabolario digitale.

10.3. Strumenti di messaggistica

WhatsApp, Facebook Messenger, Instagram Direct, Snapchat, Telegram, Signal e altri sono strumenti di messaggistica digitale ampiamente utilizzati. È importante prestare attenzione alla sicurezza dei dati quando si utilizzano queste piattaforme, con particolare attenzione alla crittografia end-to-end per proteggere la privacy delle comunicazioni.

11. Disinformazione: analisi e contrasti

La disinformazione si riferisce alla diffusione deliberata di informazioni false o fuorvianti con l'intenzione di ingannare il pubblico. Queste informazioni possono essere create per vari motivi, tra cui scopi politici, fini economici o semplicemente per generare confusione e discordia. La disinformazione può assumere molte forme, tra cui notizie false, teorie del complotto, manipolazione dei media e propaganda.

Le cause di questo fenomeno sono molteplici e spesso interconnesse e riflettono la complessità dei fenomeni sociali, politici ed economici che lo alimentano.

Le motivazioni politiche ed economiche sono una delle principali cause della disinformazione; gruppi di interesse, partiti politici e organizzazioni con obiettivi specifici possono promuovere deliberatamente informazioni false o fuorvianti per influenzare l'opinione pubblica a loro favore. Questo può accadere ad esempio durante le campagne elettorali, in cui le false narrazioni vengono utilizzate per screditare gli avversari o per consolidare il consenso attorno a determinate idee o proposte.

Un'altra causa rilevante della diffusione di fake news è rappresentata dagli algoritmi dei social media. Questi algoritmi, progettati per massimizzare l'engagement, vale a dire il grado di coinvolgimento emotivo, e la permanenza degli/delle utenti sulle piattaforme, favoriscono spesso la diffusione di contenuti sensazionalistici, polarizzanti o fuorvianti.

Il focus sull'interazione e sulla condivisione può portare alla viralità di contenuti non verificati, contribuendo così alla diffusione della disinformazione.

Anche l'anonimato online gioca un ruolo significativo, la facilità con cui gli individui possono creare account anonimi o pseudonimi sui social media consente loro di diffondere informazioni false senza essere identificati o ritenuti responsabili per i propri contenuti.

Un altro fattore importante è rappresentato dalla mancanza di alfabetizzazione mediatica. L'incapacità di analizzare criticamente le informazioni online e la mancanza di competenze nel valutare la fonte, la veridicità e il contesto delle informazioni, può portare a una diffusa credulità nei confronti di narrazioni false o manipolate.

Infine, bisogna tener conto anche delle dinamiche di polarizzazione e divisione sociale che possono alimentare la disinformazione in contesti caratterizzati da forti divisioni politiche, sociali o culturali, dove le persone possono essere più inclini a credere e diffondere informazioni che confermano le proprie convinzioni o pregiudizi, anche se sono false.

L'argomento della diffusione delle fake news è considerato pericoloso per la democrazia, tanto da richiedere una riflessione anche a livello europeo. Una delle iniziative proposte è quella della pubblicazione di uno spazio dedicato alla raccolta di notizie false riguardanti l'appartenenza all'Unione Europea, con lo scopo di fornire chiarezza attraverso dati, fatti e informazioni verificate.

La crescente tendenza a informarsi tramite Internet e i social media ha richiesto anche una riflessione sul ruolo delle piattaforme online nel dirigere gli utenti verso punti di vista predefiniti e lontani dalla diversità di opinioni. La formazione di "eco-chambers", ovvero gruppi chiusi che amplificano informazioni unilaterali, può portare alla chiusura culturale e sociale e favorire fenomeni di incitamento all'odio.

Un'altra sfida riguarda la diffusione della disinformazione attraverso l'utilizzo del Large Language Modeling, come ChatGPT di OpenAI o Bard di Google. L'intelligenza artificiale potrebbe generare disinformazione in modo più convincente rispetto alla produzione umana, come evidenziato da uno studio su Twitter. Questo fenomeno è preoccupante poiché la disinformazione generata dall'intelligenza artificiale è economica e destinata a crescere significativamente nel prossimo futuro.

Ecco qualche consiglio per individuare una fake news: controllare le fonti, la data di pubblicazione, l'URL, l'immagine associata alla notizia e utilizzare tecniche di open source intelligence (OSINT). È poi fondamentale mantenere un approccio critico all'informazione, mettendo in discussione ciò che si legge, approfondendo prima di condividere qualsiasi contenuto.

11.1. Il problema del filter bubble

La "bolla delle informazioni" (o "filter bubble") è un termine coniato da Eli Pariser per descrivere il fenomeno in cui una persona viene esposta principalmente a contenuti online che riflettono o rafforzano le sue convinzioni preesistenti.

Le piattaforme online (motori di ricerca ma anche social network) utilizzano algoritmi che analizzano il comportamento degli utenti per fornire contenuti rilevanti o interessanti per ciascun individuo. Tuttavia, questo processo di personalizzazione può portare a una sorta di isolamento informativo, dove le persone vengono esposte principalmente a prospettive con cui sono già d'accordo riducendo la diversità delle informazioni a cui sono esposti, a opinioni e punti di vista contrastanti, limitando quindi la comprensione di questioni complesse e la possibilità di sviluppare una visione equilibrata.

È importante quindi essere consapevoli della personalizzazione degli algoritmi e cercare sempre di raccogliere informazioni da fonti diverse.

12. Gaming online: tra rischi e opportunità

I videogiochi rappresentano una forma di intrattenimento in continua evoluzione, caratterizzata da una vasta gamma di esperienze e possibilità interattive. Per comprendere appieno questo fenomeno complesso, è fondamentale definire in modo chiaro cosa s'intenda per "videogioco". Spesso si fa riferimento a questo concetto in modo generico, ma è importante considerare la diversità di meccaniche di gioco, narrazioni, modalità di interazione e piattaforme che caratterizzano i videogiochi moderni.

Secondo una definizione proposta dal D.I. MiC[2] e MEF[3] nel maggio 2021, i videogiochi sono "opere audiovisive che simulano situazioni ambientate in mondi virtuali o reali, costruiti attorno a un percorso di base che si sviluppa grazie all'interazione ludica con uno o più giocatori". Questi giochi possono essere fruiti su dispositivi elettronici tramite varie piattaforme e possono includere funzionalità di gioco online.

La crescente popolarità dei videogiochi online ha creato un vero e proprio ecosistema che include piattaforme di condivisione e streaming, facilitando l'interazione tra giocatori di tutto il mondo. Questo non solo permette di socializzare e creare comunità, ma favorisce anche lo sviluppo di competenze sociali e cognitive, come ad esempio l'apprendimento di nuove lingue.

Identificare i criteri che distinguono un videogioco da un altro può essere complesso, ma alcuni aspetti distintivi includono le meccaniche di gioco, la trama, il livello di interattività e la disponibilità di funzionalità online.

A livello normativo, sia a livello europeo che nazionale, c'è una crescente attenzione alla regolamentazione dei videogiochi, specialmente per quanto riguarda la protezione dei minori e la trasparenza nei confronti dei consumatori. Iniziative come il sistema PEGI[4] e il Digital Service Act[5] mirano a garantire una maggiore sicurezza e trasparenza nel settore.

L'Italia e altri Paesi europei hanno adottato misure per sostenere e promuovere l'industria dei videogiochi attraverso finanziamenti e incentivi fiscali. Questo dimostra il riconoscimento dell'importanza strategica e innovativa del settore e l'importanza di politiche pubbliche mirate a sostenere la sua crescita.

2. Ministero della Cultura
3. Ministro dell'Economia e delle Finanze
4. La Pan European Game Information fornisce una classificazione dei videogiochi in base all'età in 38 paesi europei. La classificazione in base all'età conferma che il gioco è adeguato agli utenti di una determinata età. PEGI esamina l'idoneità di un gioco sulla base dell'età e non del livello di difficoltà.
5. Disponibile sul sito: https://eur-lex.europa.eu

12.1. Linguaggio e comportamento nel gaming online

Il gaming online è diventato un fenomeno sociale globale, che coinvolge milioni di persone in tutto il mondo. Oltre alle dinamiche di gioco e alle strategie, una parte essenziale dell'esperienza di gioco online è rappresentata dal linguaggio e dal comportamento dei giocatori. Questo aspetto gioca un ruolo cruciale nella creazione di comunità, influenzando l'atmosfera di gioco e l'esperienza complessiva degli utenti.

Nei giochi online, ci si trova spesso a interagire con individui provenienti da diverse parti del mondo e spesso la diversità culturale si riflette nel linguaggio utilizzato durante il gioco, con possibili fraintendimenti dovuti proprio alle differenze culturali.

In passato, le chat di testo si affidavano spesso ad abbreviazioni e emoticon per esprimere emozioni, ma con l'avvento della voice chat, i giocatori hanno ora la possibilità di comunicare verbalmente, portando una nuova dimensione al modo in cui si esprimono e introducendo nuove sfide, come il rischio di abusi verbali e discriminazioni vocali.

Questi elementi di tossicità legati all'ambiente di gioco, si manifestano attraverso linguaggio offensivo, insulti, discriminazioni e comportamenti dannosi, i modi più diffusi sono:

- **Discorsi di odio (Hate Speech):** si tratta di commenti razzisti, misogini, antisemiti, omofobi e altre forme di espressione negativa che si diffondono attraverso le chat, i forum e i gruppi online;
- **Flaming:** consiste nell'invio di messaggi violenti e volgari con l'intento di provocare battaglie verbali;
- **Harassment:** coinvolge l'invio ripetuto di messaggi offensivi e molesti a una persona specifica;
- **Denigration:** si manifesta attraverso la diffusione di pettegolezzi, calunnie e offese per danneggiare la reputazione della vittima;
- **Trolling:** è una pratica di disturbo che si materializza attraverso messaggi provocatori, irritanti, fuori tema o senza senso, con l'intento di disturbare o irritare gli altri giocatori;
- **Griefing:** è l'atto intenzionale di disturbare, infastidire o danneggiare deliberatamente altri giocatori tramite sabotaggio, uccisione ripetuta degli alleati o distruzione di oggetti di gioco;
- **Exclusion:** consiste nell'escludere deliberatamente una persona da un gruppo online per suscitare in essa un sentimento di emarginazione;
- **Outing and trickery:** prevede la pubblicazione e la diffusione di informazioni riservate e imbarazzanti estorte alla vittima con l'inganno;
- **Doxing:** consiste nella diffusione pubblica via internet di dati personali e sensibili della vittima.

Le aziende di giochi online stanno adottando misure per promuovere un ambiente di gioco positivo e inclusivo. Le politiche anti-tossicità includono regole chiare sul linguaggio accettabile, sistemi di segnalazione e misure disciplinari per i trasgressori.

Il futuro del linguaggio e del comportamento nel gaming online sarà influenzato dalla continua evoluzione delle tecnologie e delle piattaforme di gioco. L'integrazione di intelligenza artificiale per la moderazione e il potenziamento delle opzioni di personalizzazione delle impostazioni di chat potrebbero contribuire a creare ambienti di gioco ancora più inclusivi e sicuri.

12.2. Rischi associati al gaming online

Numerose sono le applicazioni e i giochi gratuiti che, in varie forme, raccolgono informazioni sull'utenza, che vanno dalla navigazione alla posizione, dalle chiamate ai contatti, per poi monetizzare attraverso la vendita di tali dati. I dati personali, dunque, costituiscono la nuova valuta del mondo digitale e vengono utilizzati per acquistare contenuti e servizi digitali, come contenuti premium o periodi di prova gratuiti, offerti in cambio dell'inserimento di informazioni personali come l'indirizzo email, l'età o le preferenze di visualizzazione o acquisto.

Poiché i dati personali possono essere monetizzati, i tentativi di acquisirli, anche in modo fraudolento, sono molto diffusi, non solo durante la navigazione ma anche nel gaming. Alcuni gamer possono essere vittime di phishing, hacking o furto di account. In particolare, il furto d'identità dei minori, noto come digital kidnapping, rappresenta una sfida emergente nell'era digitale e richiede una risposta educativa e consapevole. Il digital kidnapping si verifica quando viene creato un falso profilo online o manipolata l'identità digitale di un minore al fine di ottenere le sue informazioni personali per svariati scopi, come creare personaggi finti per giochi di ruolo o adescare altri utilizzando l'identità digitale del minore.

Inoltre, il desiderio di entrare in contatto nel mondo reale con utenti sconosciuti può portare a situazioni rischiose come l'adescamento di minori su internet (grooming), con conseguenti rischi per la loro incolumità fisica e mentale, come abusi o sfruttamento sessuale.

Il gaming online presenta anche il rischio della dipendenza, noto come "Gaming Disorder". La disponibilità continua dei giochi online, l'esperienza coinvolgente e la competizione possono creare una forte attrazione, portando in alcuni casi a dedicare troppo tempo e risorse al gioco, con impatti negativi sulla salute mentale, sulle relazioni interpersonali e sul rendimento scolastico o lavorativo.

I gamer affetti da dipendenza possono provare frustrazione, rabbia o senso di fallimento quando incontrano sfide nel gioco o subiscono sconfitte ripetute, e questo può portare a comportamenti aggressivi o violenti, come il "rage quitting[6]". Le conseguenze possono ricadere anche sulla salute fisica e mentale, a causa dello stile di vita sedentario e all'esposizione a contenuti inappropriati come violenza esplicita o temi per adulti, che possono influenzare negativamente il loro comportamento.

6. Una "rage-quit" si riferisce alla fine o all'abbandono di una partita in preda alla rabbia, prima della fine regolare.

12.3. Strategie di protezione nel gaming online

È fondamentale considerare che i rischi precedentemente menzionati non si applicano a tutti i giocatori e giocatrici: una gestione consapevole del tempo, un equilibrio tra vita online e offline, e una buona igiene digitale possono contribuire a mitigarli.

Stabilire limiti di tempo ragionevoli per il gioco online e rispettarli è importante. L'uso di timer o allarmi può essere utile per controllare il tempo trascorso a giocare. Dedicare tempo ad altre attività al di fuori del mondo del gaming, come lo sport, l'hobby, lo studio o il tempo trascorso con amici e familiari, favorisce un equilibrio tra la vita online e offline e il benessere generale.

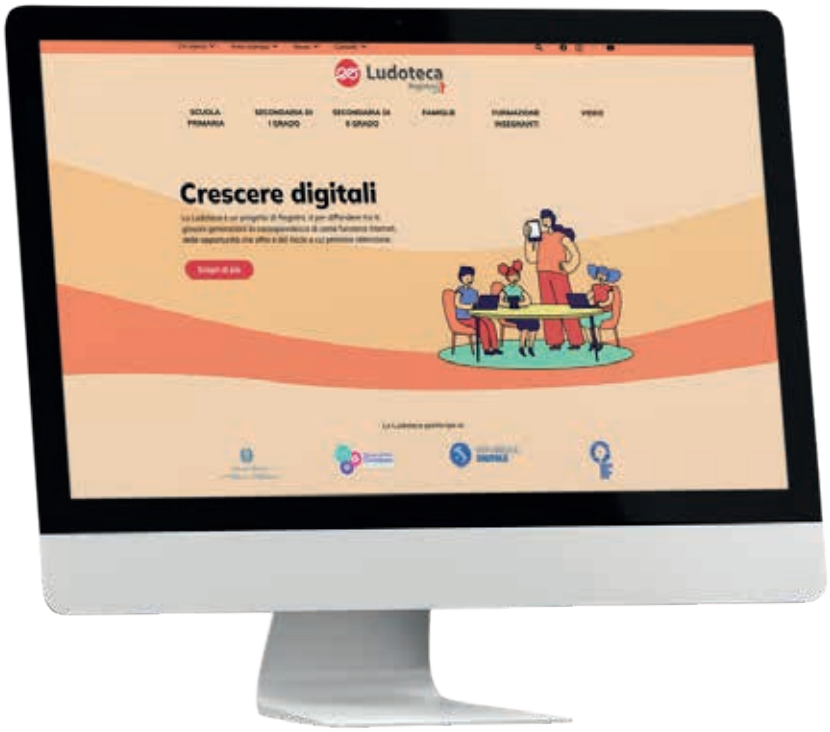
I genitori possono utilizzare strumenti di controllo parentale e limitazioni di accesso per proteggere i propri figli da contenuti inappropriati e per limitare il tempo di gioco. Tuttavia, è importante anche parlare dei rischi associati al gaming online e della necessità di una buona igiene digitale. Questo include evitare di condividere informazioni personali sensibili con sconosciuti online o su forum di gioco, utilizzare password complesse e cambiarle regolarmente, installare e mantenere attivo un buon software antivirus, effettuare aggiornamenti regolari del sistema operativo del computer o del dispositivo utilizzato, controllare e modificare le impostazioni di privacy sugli account di gioco online e giocare su piattaforme affidabili e legali, evitando di scaricare giochi da fonti non ufficiali o accedendo a siti web sospetti.

Il gaming online può essere anche un valido strumento di supporto per la formazione scolastica e per la formazione nella cybersecurity, come dimostra il videogioco 'Nabbovaldo e il ricatto dal cyberspazio' realizzato dalla Ludoteca e di cui si parlerà nei paragrafi successivi. Il gioco offre un'esperienza interattiva e coinvolgente per gli studenti e le studentesse, consentendo loro di apprendere in modo pratico e divertente.

Il metodo Ludoteca: gli strumenti

1. Il sito e il materiale

Il principale canale di comunicazione della Ludoteca è il sito www.ludotecaregistro.it, con contenuti suddivisi in base al target, news, iniziative ed eventi. Il sito si rivolge prevalentemente alle/agli insegnanti, che hanno a disposizione una panoramica completa dei contenuti formativi, dei metodi e degli strumenti utilizzati. Altro target importante sono i genitori, per i quali sono disponibili contenuti e approfondimenti dedicati a Internet e alla navigazione sicura: un modo per renderli più preparati ad affrontare l'esperienza di navigazione "condivisa" con i propri figli e figlie, dal punto di vista della conoscenza delle risorse e dei rischi.

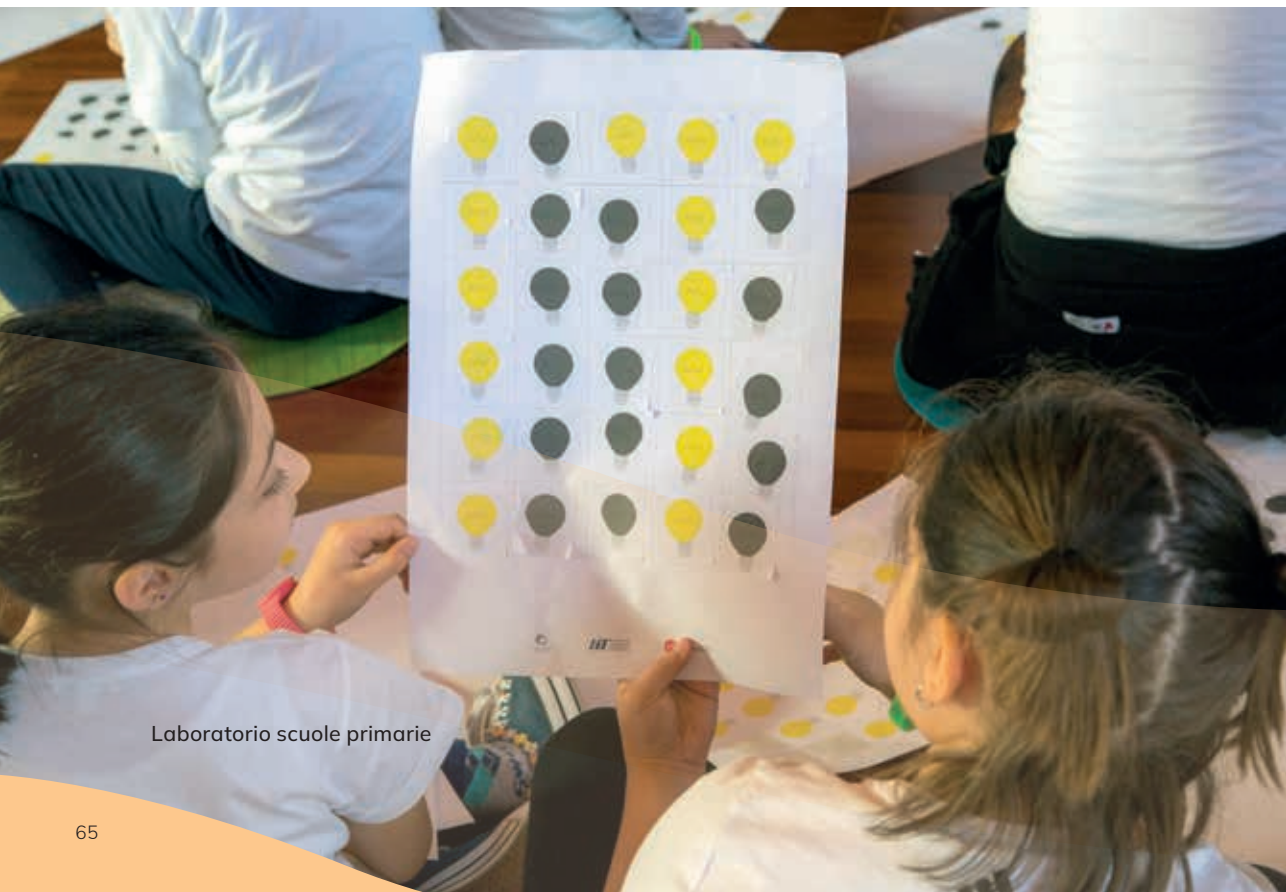


2. Materiale didattico a disposizione

I materiali sottoelencati possono essere usati come supporto ai laboratori oppure usati singolarmente per sviluppare in classe la discussione e l'approfondimento su alcuni temi.

- Internetopoli (vedi par. 4)
- Internetopoli the game (vedi par. 4.2)
- Videogioco Nabbovaldo e il ricatto dal Cyberspazio (vedi par. 5.4)
- Comics: possono essere scaricati sul sito e sono adatti a qualsiasi pubblico; i più piccoli si concentreranno sulle storie a fumetti e più grandi, compresi gli adulti, potranno approfondire con gli articoli scientifico-divulgativi compresi nei volumi.
- Carpe Digital: animazioni sul tema dell'educazione digitale: sono adatti a qualsiasi età e consentono di affrontare e commentare in classe i temi trattati
- Cyber Care: è un contenitore di video pillole dedicate al tema della cybersecurity e alla navigazione sicura in Rete. Sono "mini seminari" di 4-5 minuti, tenuti da ricercatori esperti di cybersecurity del Consiglio Nazionale delle Ricerche, destinati a ragazzi/e da 12 anni in su e adatti anche agli adulti, con brevi approfondimenti di alcuni temi.
- Webinar della Ludoteca: video di contenuti formativi della durata di 20/30 minuti ciascuno. Alcuni ricercatori ed esponenti del Consiglio Nazionale delle Ricerche di Pisa ed esperti di settore approfondiscono le tematiche relative la navigazione sicura in Rete e l'educazione digitale. Sono destinati a ragazzi/e delle secondarie di secondo grado o a un pubblico adulto (p.es. gli insegnanti).
- Gioco della rete (Classi: 4° e 5° primarie) - Un gioco per spiegare come funziona la trasmissione dei dati via Internet con una rete fatta con filo di lana e "computer umani". Tutorial disponibile qui.
- Gioco dei pixel (Classi: 4° e 5° primarie) - Il codice binario è la "lingua" utilizzata dai computer per svolgere qualsiasi tipo di operazione. Questo gioco aiuta a capire e simulare il linguaggio dei computer. Tutorial disponibile qui.
- Gioco Identità nascosta (Classi: 4° e 5° primarie e 1° secondaria di primo grado). Questo gioco è utile per spiegare quanto sia facile "mascherarsi" in Rete e quanto sia quindi importante riflettere prima di accettare l'amicizia di persone che non si conoscono. Tutorial disponibile qui.
- Gioco "Prima pensa poi condividi" (Classi 5° primarie e 1° e 2°secondaria di primo grado): per la spiegazione dettagliata si rimanda paragrafo 5.2 dedicato ai giochi per il percorso sulla cybersecurity.

- Gioco “Cyber Quiz” (Classi 5° primarie e 1° e 2°secondaria di primo grado): per la spiegazione dettagliata si rimanda al paragrafo 5.2 dedicato ai giochi per il percorso sulla cybersecurity.
- Trova differenze (Classi 5° primarie e 1° e 2°secondaria di primo grado): per la spiegazione dettagliata si rimanda al paragrafo 5.2 dedicato ai giochi per il percorso sulla cybersecurity.
- Indovina l’errore (Classi 5° primarie e 1° e 2°secondaria di primo grado): per la spiegazione dettagliata si rimanda al paragrafo 5.2 dedicato ai giochi per il percorso sulla cybersecurity).
- Memory (Classi 5° primarie e 1° e 2°secondaria di primo grado): per la spiegazione dettagliata si rimanda al paragrafo 5.2 dedicato ai giochi per il percorso sulla cybersecurity.
- Gioco cifrario (Classi 5° primarie e 1° e 2°secondaria di primo grado): per la spiegazione dettagliata si rimanda al paragrafo 5.2 dedicato ai giochi per il percorso sulla cybersecurity.



Laboratorio scuole primarie

3. La scuola primaria

3.1. Bambini della scuola primaria e abilità digitali

L'accesso precoce dei bambini e bambine, compresi quelli tra i 6 e i 10 anni, ai dispositivi e alla tecnologia è una realtà sempre più diffusa nella società contemporanea. Tuttavia, la loro effettiva evoluzione rispetto alle competenze digitali è un argomento complesso che richiede una valutazione attenta.

Da un lato, è innegabile che il porcesso di crescita avvenga oggi in un ambiente ricco di dispositivi digitali, come tablet, smartphone e computer.

Tuttavia, l'accesso ai dispositivi non garantisce automaticamente lo sviluppo di competenze digitali avanzate. I bambini e le bambine possono essere abili utenti di dispositivi per scopi ludici, come giochi e video, ma ciò non sempre si traduce in una comprensione approfondita delle tecnologie e delle loro potenzialità. Le competenze digitali primarie, come la navigazione online, la gestione di applicazioni e la comprensione di base delle funzionalità digitali, sono spesso acquisite in modo intuitivo ma possono non essere accompagnate da una piena consapevolezza dell'impatto della tecnologia.

Il ruolo della formazione e dell'insegnamento è cruciale nel plasmare le competenze digitali nelle giovani generazioni. Le scuole e le famiglie che integrano in modo proattivo l'educazione digitale nell'insegnamento quotidiano possono aiutare le giovani generazioni a sviluppare una comprensione più profonda delle tecnologie, insegnando loro non solo come utilizzare i dispositivi, ma anche come capirne il funzionamento.

3.2. I percorsi formativi della Ludoteca

L'introduzione di laboratori digitali nelle scuole primarie rappresenta un pilastro chiave per preparare le nuove generazioni a navigare il mondo di Internet in modo consapevole e sicuro.

La Ludoteca ha ideato i laboratori e la web app Internetopoli dedicati alle scuole primarie per offrire ai bambini e alle bambine una base solida per affrontare le sfide della società digitale. L'apprendimento della storia e delle nozioni di base di Internet è il punto di partenza per un viaggio alla scoperta di attività dedicate all'utilizzo responsabile dei dispositivi, alla creazione di password sicure e alla comprensione dei rischi legati alla condivisione di informazioni personali.

La sicurezza online è una componente fondamentale di questi laboratori, per insegnare a riconoscere e affrontare situazioni potenzialmente rischiose, promuovendo comportamenti etici e prevenendo il cyberbullismo. La navigazione responsabile diventa inoltre una competenza chiave per distinguere tra fonti affidabili e informazioni non verificate.

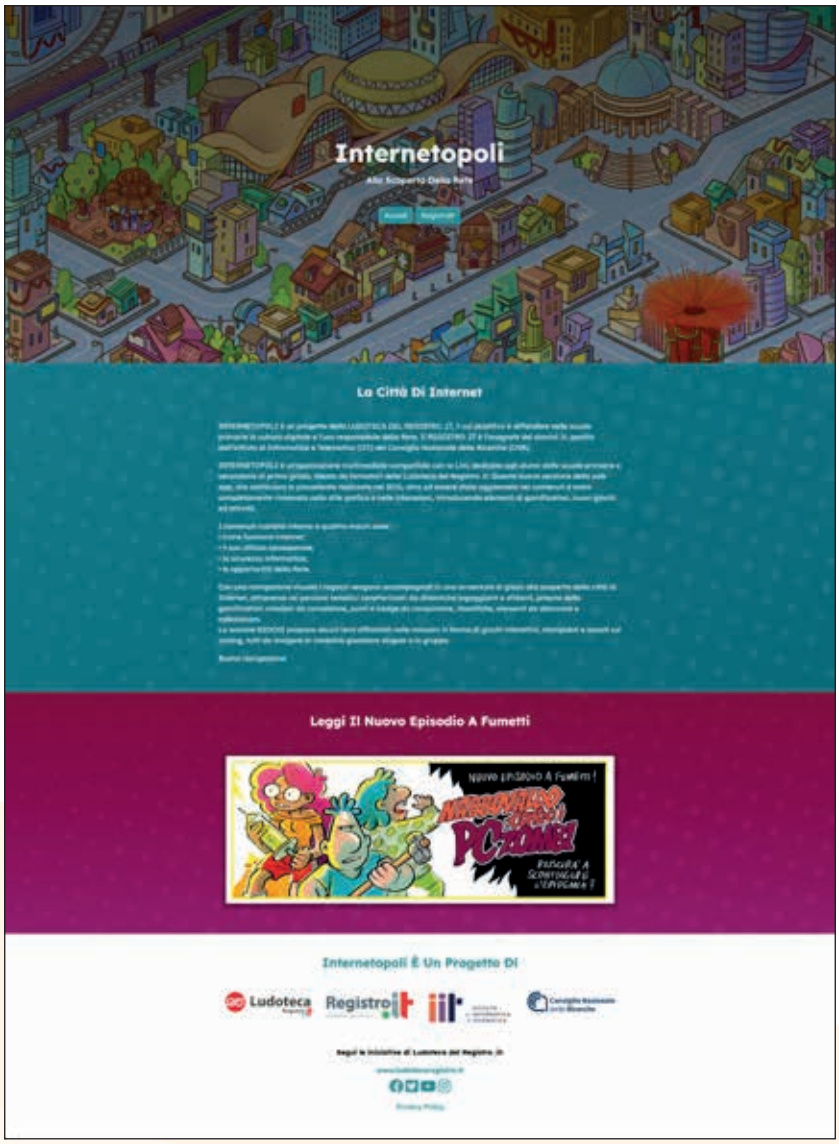
Tuttavia, l'obiettivo va oltre il semplice consumo di contenuti digitali. I bambini e le bambine vengono incoraggiati a esaminare in modo critico l'impatto di Internet sulla società, a comprendere questioni etiche legate all'utilizzo della tecnologia e a sviluppare una consapevolezza più ampia del loro ruolo nel mondo digitale, così da renderli pronti ad affrontare sfide e opportunità in un mondo sempre più orientato alla tecnologia.

Di seguito una sintesi dei principali obiettivi attesi dai laboratori proposti alle scuole primarie:

- Stimolare un atteggiamento il più possibile attivo, curioso e partecipe nei confronti della Rete;
- Insegnare le enormi possibilità offerte dalla Rete per arricchire le proprie conoscenze teoriche e pratiche, per realizzare e creare, per condividere informazioni ed esperienze;
- Far capire che anche su Internet ci sono regole e comportamenti da rispettare;
- Creare spazi ed esperienze di interscambio e condivisione tra vecchie e nuove metodologie didattiche, media tradizionali e nuovi;
- Trasmettere l'idea di Internet come esperienza di condivisione familiare;
- Trasmettere ai docenti un bagaglio di conoscenze su Internet per l'utilizzo consapevole di questo media.

4. Internetopoli

I contenuti relativi al percorso formativo dedicato a Internet convergono all'interno dell'applicazione multimediale Internetopoli (https://www.internetopoli.it), concepita come uno strumento ludico-didattico con il quale i/le docenti possono proporre in classe, in modo facile e con estrema flessibilità, tutte le tematiche della Rete. Internetopoli è un'applicazione multimediale compatibile con la Lim, dedicata alle classi delle scuole primarie a quelli del primo anno delle secondarie di primo grado, ideata dalla Ludoteca del Registro .it e realizzata da Grifo Multimedia Srl.



HP Internetopoli

L'app propone un percorso di gioco e apprendimento con contenuti di vario tipo: un vero e proprio percorso alla scoperta della Rete, interattivo e multimediale. Un modello di apprendimento digitale, aperto, polisemico e multitasking.

La prima versione dell'app è stata pubblicata nel 2015 e nel 2023 è uscita la nuova versione, aggiornata nei contenuti, nello stile grafico, nelle interazioni, introducendo elementi di gamification, nuovi giochi e attività.

Con una navigazione visuale i ragazzi vengono accompagnati in una avventura di gioco alla scoperta della città di Internet, attraverso sei percorsi tematici con dinamiche ingaggianti e sfidanti, proprie della gamification: missioni da completare, punti e badge da conquistare, classifiche, elementi da sbloccare e collezionare.

L'app prevede sei missioni, con contenuti di approfondimento e di gioco:

- Missione Isole della Rete: come funziona Internet, indirizzo IP e protocolli
- Missione Il Registro: i nomi a dominio, il Registro .it, internet governance
- Missione Il Club dei Social Network: cosa sono i social network, regole di comportamento
- Missione Agenzia Cyber Polizia: introduzione alla cybersecurity, attacchi e contromisure
- Missione La casa IoT: l'internet delle cose, smart city, big data e intelligenza artificiale
- Missione La scuola: dati e informazioni online, enciclopedie digitali, cloud.

Ogni "missione-lezione" può essere organizzata in modo flessibile sia come durata sia per la scelta degli argomenti disponibili nella app.

4.1. Guida all'utilizzo di Internetopoli in classe

Sul sito della Ludoteca è disponibile una guida all'utilizzo di Internetopoli dedicata agli insegnanti. Nella Guida proponiamo una descrizione degli argomenti introdotti nelle sei missioni del gioco, allo scopo di facilitare una "narrazione" dei vari sottotemi, legandoli alle risorse a disposizione nell'app. In alcuni casi, sono presenti anche approfondimenti esterni, per trasmettere ai docenti ulteriori conoscenze, così da facilitare la piena comprensione della materia della missione.

A titolo d'esempio di seguito riportiamo la proposta di un percorso didattico proposto nella guida

MISSIONE "LA CASA IoT"

Introduzione al tema

IoT (acronimo di "internet of things", in italiano "Internet delle cose") è un'espressione usata per indicare oggetti di uso quotidiano collegati alla Rete Internet. Questi dispositivi, definiti anche "smart" (intelligenti), sono in grado di "comunicare" tra loro e trasmettere dati con cui è possibile offrire all'utente vari servizi. Qualche esempio? Elettrodomestici, videocamere, termostati, dispositivi "wearable" (indossabili, ad esempio scarpe o bracciali per monitorare le attività sportive), applicazioni medico-sanitarie e molto altro.

In classe: per introdurre l'argomento chiedere di fare un esempio di dispositivo "smart", partendo dal significato di questa parola inglese e chiedendo che cosa rende "intelligenti" questi oggetti. Si può anche chiedere alla classe di indicare un possibile oggetto IoT presente in classe. Al termine della discussione, far vedere il video "Domenico Laforenza – Cos'è l'Internet delle Cose?" disponibile nella sezione video del sito della Ludoteca.

Esempi di alcune applicazioni

Smart home: con questa espressione si fa riferimento all'insieme di applicazioni che concorrono a realizzare la casa intelligente, in grado di conciliare le esigenze di comfort, risparmio energetico e sicurezza di chi vi abita: termostati intelligenti per regolare il riscaldamento domestico, le videocamere di sorveglianza controllabili anche da remoto, l'illuminazione degli ambienti gestita con lampadine smart, gli assistenti vocali come Google Home o Alexa.

In classe: chiedere alla classe di fare esempi di oggetti smart presenti nelle loro case, chiedendo quali sono i vantaggi.

Un'altra applicazione estremamente utile dell'IoT è in campo medico: oggi sono molti i dispositivi intelligenti usati per monitorare valori legati alla salute del paziente, come nel caso di sensori indossabili che rilevano il livello di glicemia nelle persone affette da diabete o le anomalie nei battiti cardiaci.

In classe: a conclusione di questa introduzione far vedere il video *"Cos'è l'internet of things? -What a digital world", disponibile nella sezione video del sito della Ludoteca*

Per approfondire: "Cybercare: Andrea Saracino – La casa intelligente diventa a prova di hacker"*: disponibile nella sezione video del sito della Ludoteca.*

Smart city e big data

Una smart city è una città in cui, grazie all'utilizzo delle tecnologie digitali e della Rete, è possibile ottimizzare e migliorare i servizi ai cittadini rendendoli più efficienti. È il caso, per esempio, di un trasporto pubblico completamente automatizzato e a emissioni zero, costantemente monitorato nei flussi di traffico.

Una smart city è anche una città sostenibile, in cui la tecnologia permette e favorisce il risparmio energetico, come nel caso dell'illuminazione e irrigazione pubblica gestite in modo intelligente grazie a dei sensori.

Una delle prime città a diventare smart in Europa è stata Santander, cittadina spagnola, in cui a partire dal 2013 sono stati installati circa 12.000 sensori collegati a un "cervello" centrale, gestito dall'amministrazione comunale.

Masdar City, negli Emirati Arabi, è invece una città costruita da zero con servizi e soluzioni smart: ogni edificio è cablato, il trasporto pubblico è completamente automatizzato ed è a inquinamento zero.

In classe: chiedere alla classe di citare esempi di città smart in Italia, chiedendo anche quanto la propria città possa essere definita smart e perché. Cercare su Google una recente classifica (ICity Rank) delle città più smart in Italia. Aprire Google Maps e andare a Masdar City.

Tutti i dispositivi connessi a internet, all'interno di una casa, di un'azienda o di una città, ma anche i siti internet e social network raccolgono dati sugli utenti. L'insieme di questi dati si definisce "big data". L'aggettivo "big" (grande) si riferisce al fatto che la mole di questi

dati è così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi analitici specifici per l'estrazione di informazioni.

In classe: per introdurre il tema partire dall'espressione e chiedere quale può essere il significato dell'aggettivo "big".

Per approfondire: Carpe Digital; Cosa sono i big data? *disponibile nella sezione video del sito della Ludoteca.*

Intelligenza artificiale

L'intelligenza artificiale è l'abilità di una macchina di interpretare dati esterni, imparare da essi e utilizzare le informazioni acquisite per svolgere dei compiti e risolvere problemi. L'IA (o AI se si fa riferimento all'espressione inglese "artificial intelligence") si basa su algoritmi, ovvero sequenze di operazioni che consentono alla macchina di risolvere un problema o svolgere un compito.

In classe: chiedere alla classe se qualcuno usa o ha usato assistenti vocali. Quanto sono utili, quali sono i vantaggi?

L'Intelligenza artificiale può anche sostituire l'intervento umano in situazioni ad alto rischio o essere utilizzata, in ambito sanitario, per effettuare diagnosi sempre più precise. Una delle applicazioni recenti è il servizio chatGPT, che permette di scrivere testi di vario tipo in base alle proprie esigenze, a partire da semplici indicazioni o domande scritte dall'utente nella propria lingua.

In classe: chiedere se qualcuno ha usato ChatGPT e in caso affermativo raccontare l'esperienza, evidenziando gli eventuali aspetti positivi e negativi.

Naturalmente l'uso di queste tecnologie comporta alcune riflessioni di natura etica, non a caso la Commissione Europea ha emanato nel 2018 le Linee Guida Etiche sull'intelligenza artificiale sui requisiti necessari per una IA affidabile, rivolgendo il focus su argomenti quali la sicurezza, la riservatezza e la privacy dei dati e del materiale informatico.

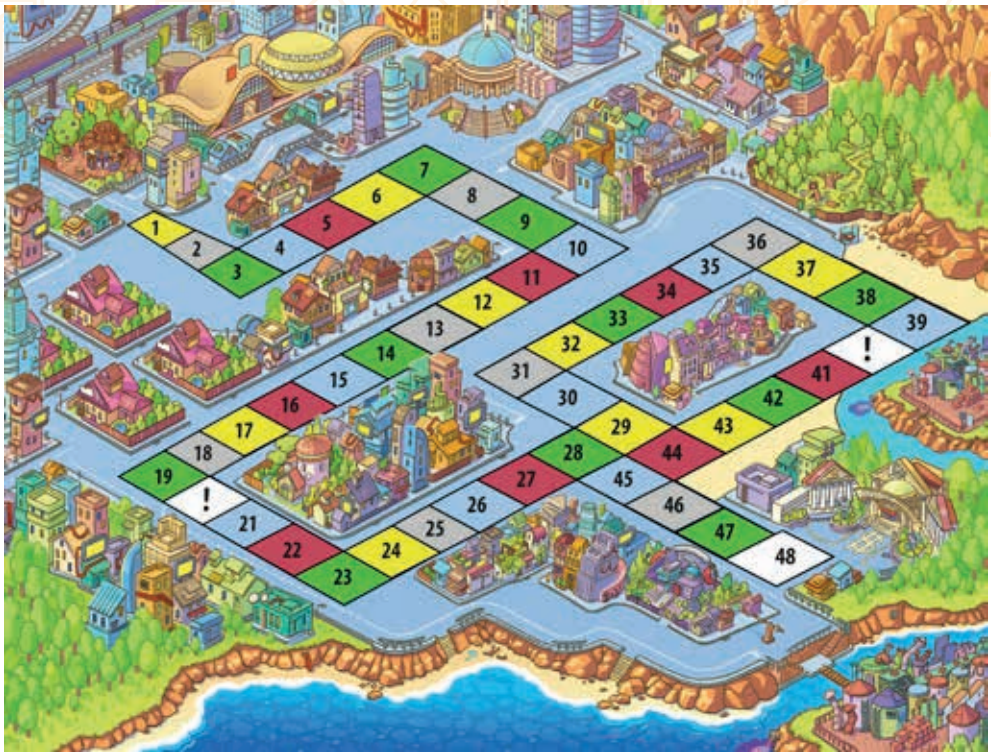
In classe: a conclusione di questo tema, far vedere video *"Intelligenza artificiale: come funziona e perché è già nelle nostre vite", disponibile nella sezione video del sito della Ludoteca*

Per approfondire:

"Cybercare: Andrea Saracino – Intelligenza artificiale: l'importanza delle implicazioni etiche"

"I webinar della Ludoteca: Fabrizio Falchi – Intuizione artificiale"

4.2. Internetopoli The Game



Web app Internetopoli

Il mondo di Internetopoli è diventato anche lo scenario del gioco da pavimento, sulla falsariga del gioco dell'oca, "Internetopoli-The Game", che si sviluppa come un percorso all'interno della città di Internet con quiz e prove pratiche a cui partecipano più squadre. Il gioco è scaricabile dal sito.

5. Percorso formativo Cybersecurity

Il tema della sicurezza informatica è di assoluta attualità, è ormai entrato a far parte della cronaca quotidiana. Ma non tutti siamo esperti e non sempre sappiamo come individuare situazioni rischiose e come comportarci. A maggior ragione, abbiamo difficoltà a mettere in guardia le giovani generazioni da situazioni a rischio e a insegnare loro comportamenti saggi e corretti. È per questo che la Ludoteca del Registro dall'anno scolastico 2018-2019 include anche attività sulla cybersecurity, con nuovi laboratori ludico-didattici destinati a bambini e bambine da 8 a 11 anni. I giochi affrontano alcuni temi tipici della cybersecurity: richieste di contatto da sconosciuti, richiesta di dati personali, compreso indirizzo e numero di telefono, download da siti sconosciuti, virus, connessioni sicure e autenticazione, ecc.

5.1. I laboratori

Nel corso dei laboratori le situazioni "pericolose" sono presentate attraverso le vignette ispirate al fumetto "Nabbovaldo e le stagioni a Internetopoli" e "Nabbovaldo contro i pc zombie", entrambi scaricabili gratuitamente dal sito della Ludoteca.

Alcuni giochi possono essere svolti a squadre, consentendo ai gruppi di "consigliarsi" tra loro prima di rispondere, favorendo quindi un comportamento di confronto e condivisione dei problemi.

I laboratori prevedono una parte dedicata alla spiegazione del tema e delle nozioni di base della sicurezza di Rete e una parte interattiva che, con l'aiuto di semplici giochi (a squadre o individuali), aiutano i/le partecipanti a verificare e fissare le regole della cybersecurity.

Maggiori informazioni sul percorso sono disponibili nel videotutorial dedicato alle risorse pubblicate nella sezione "Cybersecurity" reperibile sul canale Youtube della Ludoteca.

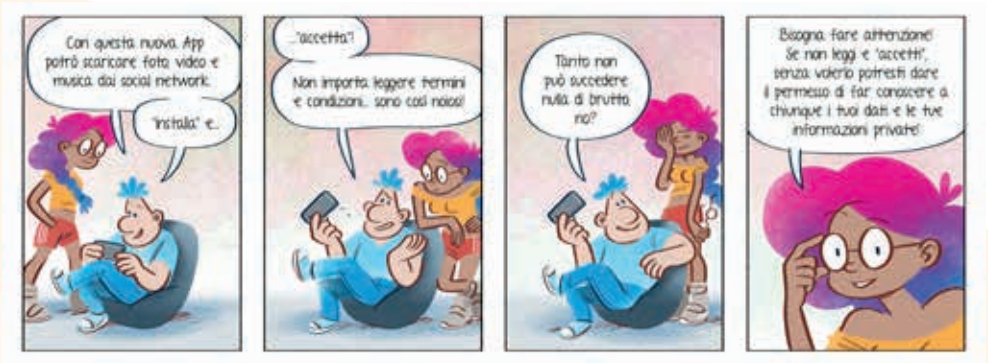
5.2. I giochi (Scuola Primaria e primo anno Secondarie di primo grado)

Tutto il materiale e i videotutorial elencati di seguito sono disponibili sul sito web della Ludoteca nella sezione 'A scuola di cybersecurity con Nabbovaldo'.

- **Tavole Cyber Quiz:** la classe, suddivisa in gruppi, legge le tavole e decide quale delle tre opzioni proposte rappresenta il migliore comportamento in termini di sicurezza informatica. Videotutorial parte 1 e parte 2.

Cyber Quiz

- **Strisce Indovina Errore:** dopo aver diviso la classe in gruppi, si distribuiscono quattro carte di una striscia chiedendo di ordinarle nella sequenza logica corretta. L'ultima carta contiene la soluzione all'errore commesso da uno dei personaggi e rappresenta quindi lo spunto di riflessione sui temi della cyber security.



Indovina l'Errore

- **Memory:** Il classico gioco per allenare la memoria diventa lo spunto per capire quando una password può considerarsi sicura. Materiale e istruzioni per il gioco sono disponibili qui.
- **Trova le differenze:** occorre trovare le differenze nelle tavole che hanno per protagonista Nabbovaldo, imparando anche qualcosa di importante rispetto alla sicurezza in Rete.

Trova le differenze

- **Cifrario segreto:** Il cifrario di Giulio Cesare è uno dei primi esempi di crittografia, letteralmente "scrittura cifrata", una delle tecniche usate in Rete allo scopo di assicurare la segretezza dei messaggi. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. Il gioco si può proporre dividendo in gruppi e dando loro una frase cifrata da risolvere entro un determinato tempo, dichiarando la "chiave", ovvero il numero di spostamenti delle lettere dell'alfabeto. È chiaro che ha solo uno scopo didattico: oggi le tecniche di cifratura sono molto più sofisticate. Sul sito della Ludoteca sono pubblicati tutti i materiali per stampare un cifrario a sostiituzione alfabetica. Materiale e istruzioni per il montaggio del cifrario sono disponibili qui.
- **Cyber bowling:** Il classico gioco del bowling rivisitato con i temi della sicurezza informatica: i birilli sono i comportamenti sbagliati, le bocce i mezzi per difenderti
- **Prima pensa poi condividi:** Un mazzo di carte con immagini divertenti diventa lo spunto per riflettere sull'opportunità o meno di condividere informazioni sui social network. A volte anche un riferimento banale alla nostra vita, "incrociato" con altri dati, può diventare un rischio per la privacy. Per ogni carta si può chiedere alla classe un parere e poi mostrare il retro con la spiegazione.

5.3. Il fumetto “Nabbovaldo contro i PC zombie

Per stimolare gli alunni e e le alunne delle scuole secondarie di primo grado a una riflessione sulle problematiche della sicurezza informatica e della privacy in Rete, si consiglia l’utilizzo di risorse che tengano vivo l’interesse della classe. Tra queste il fumetto “Nabbovaldo contro i PC zombie”, pubblicato all’interno della collana “Comics & Science” edita dal Cnr e illustrato da Gabriele Peddes.

Il comic “Nabbovaldo contro i pc zombie””

Il comic, pubblicato sul sito della Ludoteca del Registro .it, ha per protagonista il giovane tuttofare Nabbovaldo, apparentemente esperto anche di Internet ma in realtà molto ingenuo e sprovveduto di fronte al terribile virus informatico che infetta tutti i computer della città Internetopoli. Il nome richiama il concetto di “nabbo”, che nel gergo online significa appunto “scarso”, “novellino”. Il fumetto, dal taglio divulgativo e con una narrazione molto coinvolgente, può essere letto/recitato in classe, affidando a ciascun alunno un ruolo, e diventare il punto di partenza per discutere alcune nozioni base di cybersecurity, come ad esempio i malware e gli antivirus.

5.4. Il videogioco (secondarie di primo grado e ultimo anno delle primarie)

Altro strumento utilizzato per introdurre i temi della cybersecurity è il videogioco Nabbovaldo e il ricatto dal cyberspazio, un serious game "single player" pensato per avvicinare bambini e ragazzi tra gli 11 e 14 anni ai temi della sicurezza informatica. L'obiettivo del gioco, concepito come un'avventura divisa in quattro capitoli, è migliorare conoscenze, atteggiamenti e comportamenti di utilizzo della Rete Internet, in modo da favorire l'adozione di buone pratiche. Il videogioco ha per protagonista Nabbovaldo, il personaggio principale del comic "Nabbovaldo contro i PC zombie", ingenuo e poco consapevole dei possibili rischi che si corrono online.

Home page viideogioco Nabbovaldo

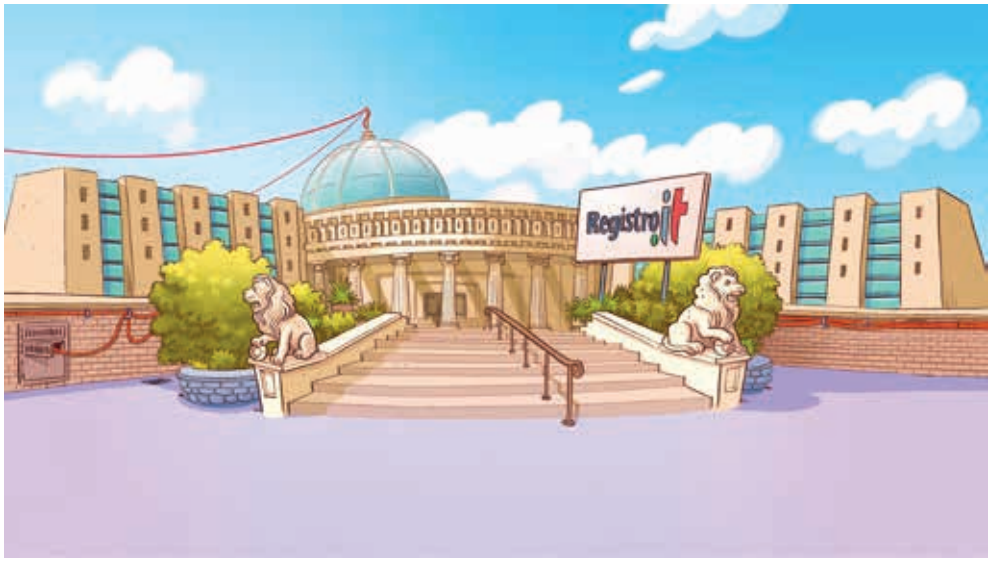
Il gioco è diviso in quattro macro-sezioni:

- AMBIENTI
- MAPPA
- DIALOGHI
- MINIGAME

A queste sezioni se ne aggiunge una quinta, chiamata Nabbopedia, un piccolo dizionario in cui sono raccolte le definizioni dei termini tecnici, per lo più legati alla cybersecurity, che il giocatore può raccogliere durante il gioco e che può consultare in qualunque momento.

Il gioco prevede una struttura ibrida tra il *percorso fisso e l'open world:* il giocatore può infatti muoversi liberamente nella Mappa, parlare con i personaggi e risolvere i minigiochi nell'ordine che preferisce, ma per arrivare alla risoluzione dell'enigma, deve necessariamente attraversare tutti i capitoli.

Tra i temi affrontati: i malware (ad esempio virus, worm, adware), gli attacchi (il ransomware che dà il titolo al gioco, il phishing e gli attacchi di forza bruta), le fake news, ma anche fenomeni come i troll e l'hate speech. Sul fronte delle contromisure tecniche, in alcuni minigame il giocatore deve imparare a utilizzare i firewall e gli antivirus ma la parte più importante è quella legata ai comportamenti. Questo aspetto emerge soprattutto nei dialoghi, incontrando i vari personaggi e trovandosi in situazioni a volte molto rischiose, si impara a riflettere sull'importanza di adottare un atteggiamento di cautela, valutando sempre le conseguenze dei propri comportamenti.



Videogiooco Nabbovaldo

5.5. I laboratori basati sul videogioco

La modalità single player del videogioco non è da considerarsi un aspetto inconciliabile con un utilizzo didattico che coinvolga l'intera classe. Sicuramente però, l'utilizzo di una risorsa di questo tipo impone l'adozione di modelli educativi innovativi, vicini alla "flipped classroom", in cui cioè si prevede un momento di apprendimento gestito in autonomia dall'alunno/a e un successivo confronto in classe sulle conoscenze acquisite.

A supporto degli/delle insegnanti che volessero proporre un percorso di approfondimento in classe in autonomia, è pubblicata sul sito anche una "Guida al Videogioco".

Per ogni capitolo la Guida propone il riassunto della trama, la presentazione dei personaggi dell'avventura e alcuni percorsi di approfondimento, richiamando risorse e strumenti didattici utilizzati dalla Ludoteca e pubblicati sul sito nella sezione Cybersecurity. Riportiamo di seguito un esempio di percorso di approfondimento da svolgere in classe, costruito a partire da alcuni spunti offerti dalla Guida stessa.

Approfondimento capitolo 1 del videogioco:

Ambiente gioco: studio del Dottor K., esperto informatico specializzato in cybersicurezza, è il posto davanti al quale Nabbovaldo incontra Troll: un ragazzo molto arrogante che, apostrofandolo come "sempliciotto", inizia a fargli delle domande sulla cybersecurity per dimostrargli di saperne molto di più.

Videogioco Nabbovaldo: Studio del Dottor K

In classe: partendo dal dialogo, dare la definizione di cybersecurity, cyberspazio, malware riprendendole dalla Nabbopedia. In particolare, nel dialogo si parla anche di spyware, un malware in grado di registrare l'attività di un utente/vittima su un particolare dispositivo digitale. Può anche essere l'aggancio per presentare l'approfondimento sui malware.

Proposta di attività: possibilmente proiettate o comunque fate leggere la tavola n. 7 delle tavole a Fumetti Cyber Quiz; fate scegliere il comportamento da tenere per alzata di mano.

Per approfondire: episodio della webserie What a Digital World dal titolo 'Cybersecurity' disponibile nella sezione video del sito della Ludoteca.

Ambiente gioco: alla Stazione centrale Nabbo incontra un poliziotto esperto in reati informatici che gli parla di alcune mail sospette: sono i tentativi di truffa effettuati tramite la tecnica del phishing.

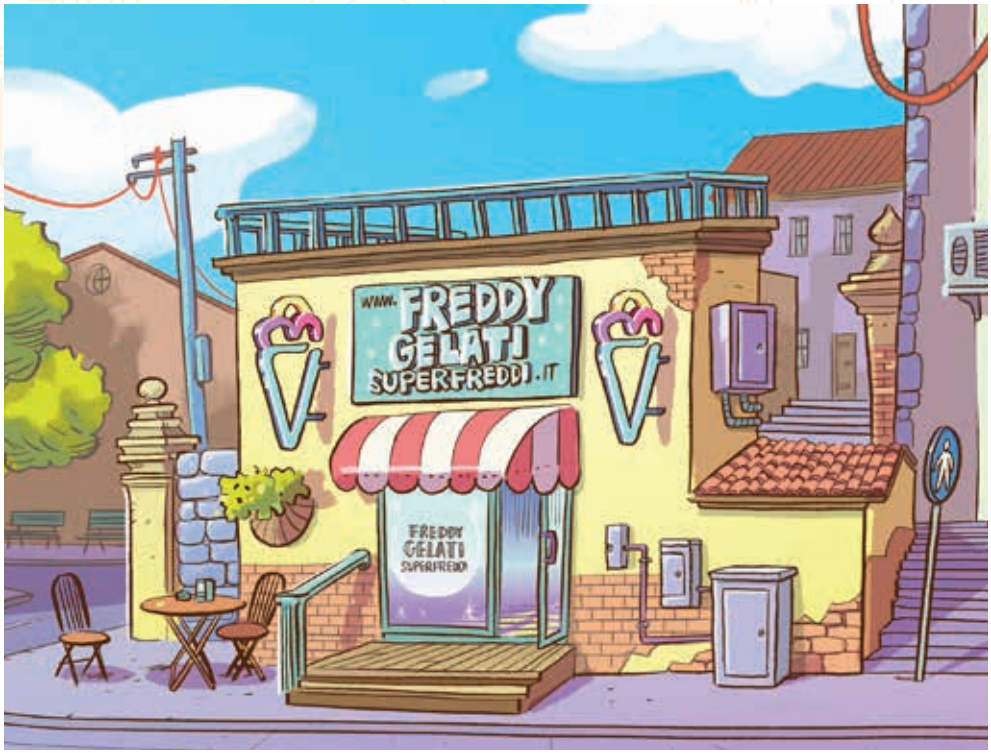
Videogioco Nabbovaldo: Stazione Centrale

In classe: partendo dal dialogo, dare la definizione di phishing (vedi sezione Nabbopedia). Approfondire il tema, soffermandosi sull'importanza delle frasi che cercano di convincere l'utente a fare qualcosa: clicca qui, metti le password e simili. Riferirsi anche alla sezione di buone pratiche: Non aprite quella posta! pubblicate nella sezione "Attenti ai pericoli" della Guida.

Proposta attività**:** divisa la classe in gruppi, si può far scrivere a ciascuno una mail di phishing su un foglio di carta. Poi ogni gruppo lo passa a un altro gruppo che cerca di individuare i punti deboli, gli errori, le ingenuità che possono insospettire chi la riceve. A conclusione dell'attività è il gruppo destinatario che legge la mail a tutta la classe ed espone gli indizi che a suo parere smascherano il tentativo.

Per approfondire: video sul tema dello spamming disponibile sul sito di RayPlay, sezione 'Domande snack' dal titolo 'In rete sicuri e informati'.

Ambiente gioco: gelateria di Freddy, il gelataio chiede a Nabbo che cos'è un trojan horse promettendogli in cambio un gelato gratuito.



Videogioco Nabbovaldo

In classe: far raccontare da qualche ragazzo la leggenda dello stratagemma di Ulisse a Troia, che dà il nome a questo tipo di malware. Riflettere sul concetto di vulnerabilità, di accettare regali da sconosciuti, di promesse ingannevoli. Riflettere poi su quali siano i link su cui non cliccare. Riferirsi anche alla sezione di buone pratiche Navigare in sicurezza (sezione "Attenti ai pericoli" della Guida).

Proposta attività: leggete la tavola n. 8 delle tavole a fumetti Cyber Quiz e fate votare per alzata di mano.

Per approfondire: video sul tema malware e spyware disponibile sul sito della Ludoteca, sezione video, serie 'Cyber Care', titolo: 'Social Engineering'.

5.6. La Guida per gamer

Per dare ai ragazzi e ragazze ulteriori spunti sul tema della sicurezza durante o dopo l'esperienza di gioco, è disponibile anche una Guida per gamer. La Guida propone brevi contenuti di approfondimento ma soprattutto giochi a quiz e cruciverba.

Tale strumento può essere consigliato alla classe per rendere più divertente l'acquisizione di alcune nozioni di cybersecurity o può diventare uno strumento didattico da utilizzare per piccole attività di gruppo.

5.7. Il manifesto sulla sicurezza online

Un'altra risorsa da utilizzare in classe, utile per stimolare l'interesse è il "Manifesto della sicurezza online", disponibile sul sito della Ludoteca, i cui contenuti sono stati curati dalla Ludoteca in collaborazione con il giornalista Giampaolo Colletti.

Il Manifesto, una guida con le dieci regole principali per navigare consapevoli e sicuri, fa riferimento, attraverso un linguaggio semplice ma non banale, a diversi temi della cybersecurity: attacchi informatici, protezione dati personali, furto di identità, meccanismi di autenticazione. In classe può essere utilizzato come ulteriore approfondimento al gioco rispetto al tema dell'"igiene informatica", intesa come insieme di comportamenti da adottare per prevenire le cyber minacce.

Manifesto della sicurezza online

Ecco i dieci punti del manifesto con un approfondimento per ogni tema:

1. **Scegli con cura.** Il primo passo è quello di adottare password alfanumeriche complesse. Quelle semplificate possono compromettere la sicurezza dei tuoi dispositivi informatici.

   Per approfondire guarda i video disponibili sul sito della Ludoteca

- "Non è mai troppo web": Le password (Ludoteca del Registro .it)
- La password del wifi (The Jackal)
- Biometria (Giacomo Giorgi Cnr-Iit)

Spesso per pigrizia o per mancanza di tempo quando ci viene richiesta una password inseriamo una "stringa" facile da ricordare: il nome di un parente o del cane, la nostra data di nascita, la sequenza 12345..., la stessa parola "password". Nord Pass ha fatto una ricerca pubblicata alla fine del 2021 che individua le password più frequenti usate in moltissimi Paesi, tra cui l'Italia. Un elenco che dovremmo consultare per verificare che le nostre password non siano in quell'elenco. È possibile anche verificare la robustezza delle nostre password, per esempio su "Quanto è sicura la mia password?" di Nord Farm o di RoboForm o in siti simili. La facilità con cui le password semplici possono essere violate, attraverso attacchi molto facili da attuare e chiamati di "forza bruta", è spaventosa e, per evitare una piccola fatica iniziale, rischiamo di consegnare la nostra vita privata e, a volte, i nostri beni a qualche malintenzionato. Certo, si dirà, ma come faccio a ricordare password complesse? Scriverle sulla propria agenda o sui post-it non è certamente una bella idea. Potrebbe convenire affidarsi a un gestore di password che oggi troviamo spesso "nativo" sia sui computer che su tablet e cellulari. Il gestore di password (Single sign on) si "ricorda" per noi le password di accesso ai siti e alle app, le conserva cifrate e ce le fa usare se immettiamo una sola password per accedere al gestore, la cosiddetta "master password". Il problema quindi si riduce a dover memorizzare una sola password, la master password del gestore delle password. Nel caso in cui non si disponga di un gestore di password disponibile nel sistema operativo del proprio dispositivo conviene scegliere con cura quello da utilizzare, eventualmente anche tra quelli a pagamento.

Un'alternativa ai classici meccanismi di autenticazione basati sul login sono i sistemi di riconoscimento biometrici, che utilizzano parametri fisici (impronte digitali, retina, volto) per identificare in modo univoco l'utente. Un altro strumento molto utile è la doppia autenticazione che si basa sulla combinazione tra il classico inserimento di nome utente e password e una chiave di sicurezza, come il codice inserito nell'sms di verifica che arriva al proprio smartphone.

2. **Custodisci gelosamente.** Password e codici di accesso non vanno condivisi con nessuno. Ricordati che corri il rischio di diventare vittima di truffe online o di hackeraggio a causa di una banale distrazione.

Per approfondire guarda i video disponibili sul sito della Ludoteca:

- Social engineering (Ilaria Matteucci - Cnr-Iit);
- Come navigare in sicurezza (Giorgia Bassi Cnr-Iit).

Abbiamo scelto password complicate, in modo che siano abbastanza sicure. Siamo stati bravi, ma bisogna porre molta attenzione alle modalità con cui le custodiamo: condividerle con amici/che, fidanzati/e o con compagni/e non è mai una buona idea, soprattutto perché, pur fidandoci, non sappiamo con quale cura la custodirà a sua volta. Senza contare che in futuro potremmo non fidarci più di quelle persone e, in questo caso, dovremmo cambiare tutte le password che avevamo condiviso con loro. Pensiamo ad esempio alle password di accesso ai nostri profili social: se cadono nelle mani sbagliate, possono farci dire online cose che non pensiamo e che non ci appartengono, creando a noi danni per la nostra reputazione o anche ad altre persone coinvolte, che magari vengono offese attraverso un nostro profilo, caduto nelle mani di una persona non più fidata. Bisogna anche evitare di appuntarle in chiaro sull'agenda del telefono o di tenere un bigliettino con le password nel portafoglio: se portafoglio o telefono cadessero in mani sbagliate, tipo in mano ad o a un ladro tutti i nostri accessi, compresi probabilmente, quelli al conto in banca, sarebbero in mano al ladro.

Attenzione anche ad effettuare il login ad applicazioni o siti critici (per esempio la nostra banca) utilizzando wi-fi pubblici e dunque reti non protette: le credenziali potrebbero essere facilmente intercettate da un hacker (sniffing).

3. **Pensa prima, condividi poi.** Prenditi il tuo tempo: prima di rilanciare un contenuto, prima di mettere un like o un cuore, prima di pubblicare un selfie o postare un video rifletti bene e poniti una domanda: ne vale davvero la pena?

Per approfondire guarda i video:

- Quando devi scegliere che foto pubblicare (The Jackal);
- Video del Manifesto della comunicaizone non ostile (Paole_Ostili).

Istintivamente, "scrollando" i social ci fermiamo su qualcosa che ci colpisce e la commentiamo immediatamente anche solo con una "faccina" o con un commento esplicito, come se il nostro intervento fosse visibile solo all'autore di quel contenuto, dimenticandoci che almeno tutta la sua cerchia di contatti potrà vederlo, come pure contatti nostri e, se abbiamo commentato per esempio negativamente il comportamento di un amico comune, quest'ultimo potrebbe rimanerci male e il commento incauto può rovinare una relazione.

Esistono anche altre ragioni per evitare di rendere pubbliche alcune informazioni: per esempio se siamo in vacanza e postiamo immagini di un posto esotico e lontano dichiarando apertamente che abbiamo chiuso casa per due settimane, stiamo automaticamente avvisando qualche ladro abile con la rete che ha campo libero per agire indisturbato in casa nostra...

4. **Fai attenzione.** Ricorda che in rete e sui social tutto è pubblico, anche quello che può sembrare privato. Perché i contenuti online hanno una viralità difficilmente prevedibile. Quindi stai attento a ciò che decidi di condividere.

Per approfondire guarda i video:

- Diventare cittadini digitali I e II parte (Luca Bechelli P4I);
- L'internet, l'io, l'oblio (Valentina Amenta - Cnr-Iit).

Spesso sentiamo parlare di "diritto all'oblio" riferito alla rete. Vuol dire che la rete ha una memoria indelebile e qualunque cosa pubblichiamo può essere ritrovata anche dopo molto tempo. La rimozione di contenuti pubblicati è praticamente impossibile perché, anche se viene rimosso quel post o quella pagina web, non è detto che non possa riapparire, ripubblicata da qualcuno che l'aveva scaricata e conservata nel suo computer o perché salvato in qualche server di backup non sincronizzato. È questa la ragione per cui dobbiamo stare attenti nel postare o pubblicare: dobbiamo essere sicuri di non avere mai ripensamenti. Questo è tanto più vero se siamo ancora giovani, portati magari a condividere sui social qualche avventura anche strana. Tra qualche anno un possibile datore di lavoro, cercando nostre notizie online, potrebbe imbattersi in situazioni che ci riguardano e che ora potrebbero metterci in imbarazzo o in difficoltà, creando un danno alla nostra di "reputazione", come nella vita reale, e con ricadute concrete nella vita reale: quel datore di lavoro potrebbe decidere che non siamo adatti a ricoprire una certa posizione.

Occorre anche prestare attenzione all'impostazione dei nostri profili social: a meno che non siamo un personaggio pubblico, conviene configurare un profilo privato, accessibile solo a persone autorizzate da noi. Questo vuol dire, come conseguenza immediata, che prima di concedere l'accesso al nostro profilo, dobbiamo verificare chi sia la persona o la pagina che ce lo sta chiedendo: è conosciuta? è affidabile?

5. **Usa la testa, non la pancia.** Non rispondere in modo impulsivo. Parla, scrivi, chatta, ma con consapevolezza. Le parole hanno un peso. Scegli di interagire in modo tale da evitare di alimentare tutto questo.

Per approfondire:

- Webinar Vera Gheno sulla comunicazione sui social media;
- Il Manifesto di Parole_Ostili;
- L'hate speech (Generazioni Connesse).

"Prima pensa, poi parla, perché parole poco pensate portano pena" è un'espressione proverbiale, che alcuni fanno risalire all'antica Grecia. Nonostante l'età, "la regola delle 10 P" è ancora attuale, anche per la nostra vita in rete. Nelle interazioni online siamo abituati a tempi brevi, risposte immediate, che ci impediscono di riflettere prima di pubblicare definitivamente il nostro pensiero o l'immagine che vogliamo condividere. Ci sembra di non poterne fare a meno, importante in una conversazione, far sapere subito cosa stiamo facendo o dove siamo. Inoltre, nello scrivere e commentare in rete manca la componente "fisica": non abbiamo davanti l'interlocutore e per lui è impossibile percepire le nostre intenzioni dalle

espressioni del corpo o del viso o dalla inflessione della voce, come per noi è impossibile percepire l'effetto di quello che stiamo dicendo o mostrando. La stessa frase, pronunciata con tono diverso, può essere ironica o seria. Nel leggerla questo effetto si perde quasi completamente, se non per la presenza di qualche «faccina» esplicativa. Nei rapporti umani, l'interazione fisica in una conversazione è una componente importante, benché istintiva. Per questo è importante riflettere sull'effetto che può avere su chi legge quello che stiamo per pubblicare, per rispetto degli altri.

I pionieri della rete si erano posti il problema dell'educazione da mantenere nella comunicazione in rete definendo la "netiquette", (la combinazione di network (rete)+etiquette (galateo)), un insieme di comportamenti corretti da adottare, che prevedevano l'isolamento e la marginalizzazione di chi non li rispettava. Non erano regole imposte ma suggerite e, a lungo, la comunità degli internauti le ha tenute in conto. Oggi, purtroppo, la netiquette è quasi completamente ignorata.

6. **Non cadere nella rete.** Perché in rete le fake news si moltiplicano su siti poco affidabili, presentati con video coinvolgenti e con titoli acchiappaclic, rilanciati spesso inconsapevolmente da profili di amici e conoscenti. Per approfondire guarda i video:

- Le fake news (Marinella Petrocchi - Cnr-Iit);
- Social media: falsi profili e bot (Marinella Petrocchi - Cnr-Iit);
- Le fake news (Generazioni Connesse).

Oggi siamo bombardati dalle informazioni, ma dedichiamo a ciascuna di esse pochissimo tempo: i tempi della rete sono sempre minimi, ogni contenuto deve essere comunicato velocemente. Questa è la ragione per cui spesso ci fermiamo a leggere solo il titolo e non l'intera notizia, non ci prendiamo il tempo per riflettere, per analizzarla con un po' di spirito critico e magari cercare altre fonti per confrontarla. In particolare, è buona norma controllare la data dei testi, cercare sempre informazioni sull'autore e diffidare di quelli pieni di errori grammaticali. Questo è il meccanismo con cui funzionano e si diffondono le bufale o "fake news": i loro autori fanno affidamento sulla velocità e superficialità con cui accettiamo i contenuti che ci vengono proposti e magari li ripubblichiamo. Chi li riceve da noi, se ci conosce e si fida, automaticamente penserà che siano affidabili e, a sua volta, contribuirà a diffonderla. È come un'ondata, che potremmo fermare dedicando un po' di tempo a verificare quello che ci viene proposto. Un buon metodo è selezionare, sulla base della propria esperienza, un insieme di fonti che nel tempo si sono dimostrate affidabili e fare riferimento a quelle in caso di dubbio (e facciamoci sempre venire il dubbio!)

7. **Aiuta chi è più in difficoltà a comprendere social e rete.** Diventa anche tu un influencer delle buone pratiche e spiega a tua mamma o a tuo papà, ai tuoi nonni e agli amici le opportunità di Internet, ma anche i rischi connessi. Per approfondire guarda i video:

- Non è mai troppo web (Ludoteca del Registro .it)
- Protocollo boomer (The Jackal)
- Aiuta un amico (Generazioni Connesse)

Si parla spesso di gap digitale tra generazioni ed è innegabile che i ragazzi siano quasi sempre più esperti degli adulti nell'uso della rete. Sarebbe auspicabile che gli adulti non si chiudessero in un rifiuto ma accettassero per una volta di essere discenti dei ragazzi invece di insegnare loro. Un'occasione per imparare a sfruttare un mezzo che offre grande opportunità e magari rinsaldare un rapporto personale che vada al di la' di chi impara e di chi insegna.

Ci sono anche casi in cui la difficoltà non è dovuta a una scarsa dimestichezza con la rete ma a qualche problema o rischio che ci troviamo ad affrontare, indipendentemente dalla nostra età: esiste il bullismo in rete, il sexting, lo stalking, il revenge porn eccetera, problemi che coinvolgono profondamente a volte incontrollatamente chi ne è vittima. Anche in questo caso, chi ne è consapevole e ne è capace, può offrire aiuto all'amico in difficoltà, denunciando, anche in forma anonima, il crimine commesso e aiutare la persona in difficoltà a comprendere come difendersi da questi rischi.

8. **Non fidarti!** I tentativi di phishing e di truffe cibernetiche vengono talvolta messi a segno attraverso account di amici e parenti, spesso hackerati. Quindi anche i tuoi contatti più stretti, senza volerlo, diventano diffusori di malware. Fidarsi è bene, non fidarsi è meglio.

Per approfondire guarda i video:

- Qual è la differenza tra virus, malware e spyware? (Fabio Martinelli Cnr-Iit);
- Lo spamming (Giacomo Giorgi Cnr-Iit);
- Social engineering (Ilaria Matteucci Cnr-Iit);
- Malware e phishing (Generazioni connesse).

La fiducia sta alla base dei nostri rapporti: accettiamo quello che ci dice un amico perché di lui ci fidiamo. Tendiamo a estendere questo comportamento anche quando siamo in rete: se un messaggio o una email ci arriva da un mittente che conosciamo, ci fidiamo e lo accettiamo. Purtroppo, in rete mascherarsi è molto più facile che nella realtà ed è quello che fanno molti truffatori: si "travestono" da un mittente che è tra i nostri contatti (un amico, la banca. l'assicurazione, l'associazione benefica) e carpiscono la nostra fiducia, inducendoci a dare loro informazioni che dovrebbero restare riservate: password, codici di accesso ecc. Si tratta di un vero e proprio attacco hacker che va sotto il nome di attacco di ingegneria sociale (social engineering). Gli attacchi di phishing sfruttano questo comportamento e inducono i destinatari di un messaggio malevolo a compiere un'azione imprudente. Questi

messaggi possono arrivare via email (e allora si tratta proprio di phishing) o per messaggio e in questo caso si parla di smishing o tramite una telefonata e prende il nome di vishing. Riconoscere un messaggio falso a volte è abbastanza facile, perché' magari è scritto male, in un italiano scorretto e questo dovrebbe insospettirci. Controllare bene l'indirizzo del mittente di una email è una buona tecnica di difesa e anche passare il mouse o il dito sul link al quale ci suggeriscono di collegarci può rivelare il vero indirizzo di destinazione che possiamo riconoscere come falso. Il phishing (e i suoi "derivati") non è l'unico tipo di truffa basata sul social engineering. Spesso ci sono siti che riproducono esattamente nell'aspetto un sito a noi noto (p.es. quello della banca) ma ne sono una copia, che noi interpretiamo come vera e accettiamo di inserire i nostri dati e le nostre informazioni private, cadendo nella trappola. Questo attacco si chiama spoofing e per evitarlo spesso è sufficiente controllare che l'indirizzo del sito sia veramente identico a quello della nostra banca.

Un'altra raccomandazione è riflettere sempre prima di scaricare applicazioni gratuite da store non ufficiali: potrebbero contenere malware in grado di registrare dati personali come password (ma non solo). Attenzione anche alla gestione dei permessi nelle app: concedere l'autorizzazione fidandosi in modo acritico potrebbe dare il via libera a varie forme di registrazione e furto di dati.

9. **Alza la mano, mai le mani.** Chiedi aiuto a chi ne sa più di te se pensi di trovarti in una situazione di rischio a causa delle interazioni in rete. Hai a disposizione un indirizzo sempre presidiato: vai su Commissariatodips.it e mettiti in contatto con gli operatori della Polizia Postale e delle Comunicazioni.

La rete offre grandi opportunità ma presenta anche zone di rischio. Gli adulti sono meno consapevoli dei meccanismi che attivano i rischi ma probabilmente avrebbero gli strumenti per affrontarli, derivanti dall'esperienza. I ragazzi, invece, quasi sempre individuano la fonte di un possibile rischio ma non sempre hanno gli strumenti per gestire il pericolo a cui si trovano esposti, proprio a causa della giovane età. In entrambi i casi è necessario un aiuto e, in alcuni casi, è proficua una interazione, uno scambio tra chi capisce da dove viene il rischio e chi è in grado di affrontarlo da un punto di vista emotivo, sociale e pratico. Per questo, in rete (come nella vita reale) è importante saper chiedere aiuto e sapere a chi chiederlo. Può essere un amico più esperto, un adulto se il pericolo riguarda un ragazzo o un giovane se chi è esposto è un adulto poco "smart". Nei casi più complicati, in cui ci si trova davanti a veri e propri reati (cyberbullismo, pedopornografia, revenge porn, stalking ecc.) è bene rivolgersi alla polizia postale, sia che siamo adulti sia che siamo ragazzi. Sul sito del Commissariato di Pubblica Sicurezza è possibile segnalare un possibile reato. Reagire direttamente, online o anche di persona, non è sempre una buona idea anche perché non sempre sappiamo chi sta veramente interagendo con noi.

10. Tieniti aggiornato sui rischi che si corrono quando si naviga. Cerca di cogliere i segnali che arrivano dagli esperti e impara ad essere prudente, a non fidarti ciecamente dei link condivisi e a ragionare prima di cliccare. Per approfondire guarda i video:

- Informarsi in rete (Sonia Montegiove, informatica, giornalista, divulgatrice);
- La Cybersecurity (Registro .it).

In rete tutto corre veloce, tutto cambia rapidamente, anche le tecniche di attacco e i tipi di truffe. Per stare al passo, bisogna tenersi aggiornati e lo si può fare proprio tramite la rete. Bisogna anche tenere aggiornati i dispositivi, dal sistema operativo, alle applicazioni, agli antivirus poiché spesso gli aggiornamenti contengono delle correzioni al codice (patch) che permettono di superare alcune vulnerabilità. È raccomandabile inoltre selezionare le fonti affidabili che, monitorate nel tempo, ci danno garanzia di essere credibili; possono essere siti di informazione, soprattutto quelli dedicati alla tecnologia e alla rete, le pagine di alcuni esperti, siano esse siti, blog, canali social ecc., siti di formazione autorevoli, su cui imparare le nozioni necessarie. L'aggiornamento è la chiave di "sopravvivenza" in rete ed è affidata per la maggior parte all'iniziativa personale: esistono alcune iniziative dedicate a diffondere la conoscenza della cybersecurity nelle scuole (come, ad esempio, la Ludoteca del Registro .it, promotrice di questo manifesto) e tra i cittadini, anche a cura di associazioni e organizzazioni no profit.

5.8. La scuola secondaria di secondo grado

Per gli istituti superiori la Ludoteca mette a disposizione, attraverso il proprio sito web una serie di risorse video che possono rappresentare degli spunti di riflessione o di approfondimento su alcuni temi legati al mondo digitale.

In particolare, le rubriche consigliate per le scuole superiori sono:

- **Carpe Digital:** pillole su alcune nozioni chiave di informatica e del mondo di Internet
- **I Webinar della Ludoteca:** interventi di esperti/e, ricercatori e ricercatrici su vari temi del digitale, dalla tutela della privacy, alle fake news, all'intelligenza artificiale
- **Cyber Care:** pillole di sicurezza informatica

Un altro utile strumento per affrontare e confrontarsi in classe il tema della sicurezza online è il Manifesto "A scuola di cybersecurity", di cui abbiamo parlato nel paragrafo 5.7.

6. La valutazione dell'efficacia dei laboratori

A conclusione di questa pubblicazione, vogliamo condividere i dati del progetto di valutazione dell'efficacia dei laboratori delle scuole primarie e secondarie di primo grado, svolto in collaborazione con il Dipartimento di Formazione, Lingue, Intercultura, Letterature e Psicologia (FORLILPSI) dell'Università di Firenze.

Questi dati offrono un'evidenza scientifica rispetto a ciò che abbiamo riscontrato sul campo in questi dodici anni: il grado di conoscenza e soprattutto di consapevolezza nell'uso dei device digitali e delle risorse della Rete è migliorato a seguito dei laboratori della Ludoteca.

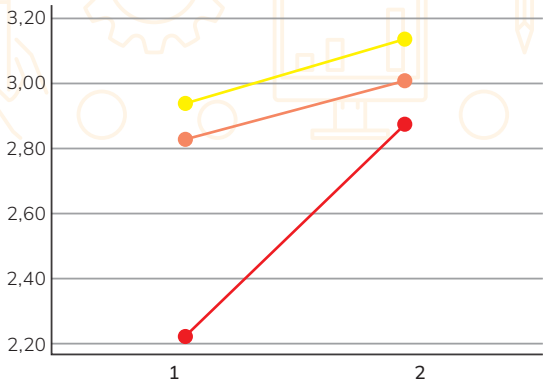
La valutazione è stata portata avanti somministrando alle classi questionari anonimi prima e dopo il percorso formativo con la Ludoteca.

I dati di seguito riportati si riferiscono all'anno scolastico 2021/22 per le classi di scuole primarie e primo anno di scuole secondarie di primo grado e all'anno scolastico 2022/23 per le classi delle scuole secondarie di primo grado. Nella valutazione di questi ultimi laboratori, oltre alle classi sperimentali, hanno partecipato al progetto anche classi di controllo.

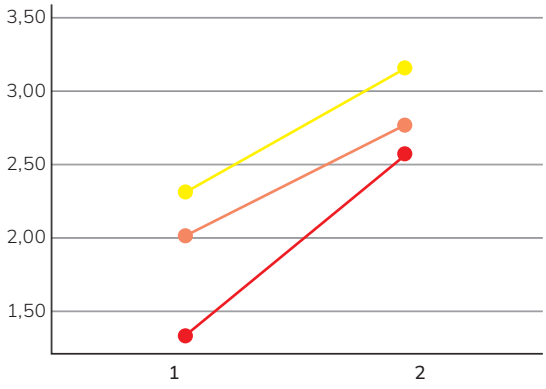
Hanno partecipato alla valutazione 274 studenti e studentesse di classi prime di scuole secondarie di primo grado (nei grafici i dati relativi sono riportati in giallo), classi quarte di scuola primaria (nei grafici i dati relativi sono riportati in rosso) e quinte di scuola primaria (nei grafici i dati sono in arancione).

I dati relativi alle scuole primarie hanno evidenziato che il livello medio di conoscenze migliora sotto tutti gli aspetti, passando da poco a molto per quanto riguarda gli aspetti relativi alla cybersecurity e alla conoscenza di tipo più generale, e da abbastanza a molto per quanto riguarda la conoscenza dei rischi di Internet. Questo miglioramento è ancora più forte per le classi quarte della primaria, che a seguito degli incontri formativi, raggiungono un livello medio di conoscenze simile a quello delle altre due classi. Gli incontri, inoltre, hanno avuto un riscontro positivo in termini di gradimento. Su una scala da 1 a 10 hanno infatti ricevuto una valutazione molto positiva, risultando divertenti (7) e interessanti (8).

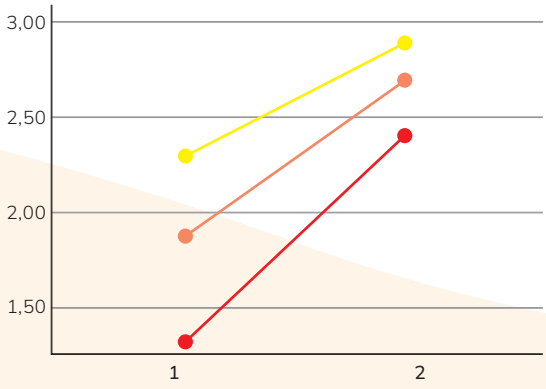
CONOSCENZE: RISCHI



CONOSCENZE: GENERALI



CONOSCENZE: CYBERSECURITY

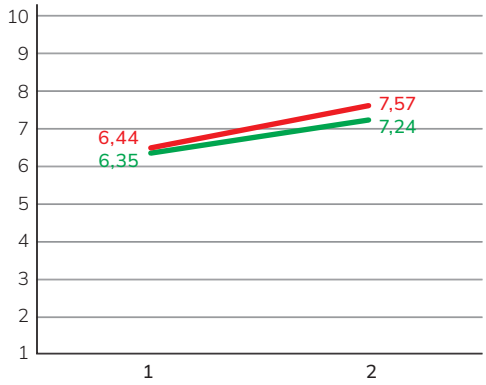


Il percorso formativo proposto alle scuole primarie produce un miglioramento significativo delle conoscenze relative al mondo della Rete. Le classi quarte, e quindi i bambini e bambine più piccoli, sono quelle che sembrano beneficiare maggiormente degli incontri. Questo risultato è molto importante perchè dimostra che la conoscenza di aspetti anche di tipo tecnico e di funzionamento della Rete e dei dispositivi digitali è un presupposto fondamentale per la costruzione di una cittadinanza digitale consapevole.

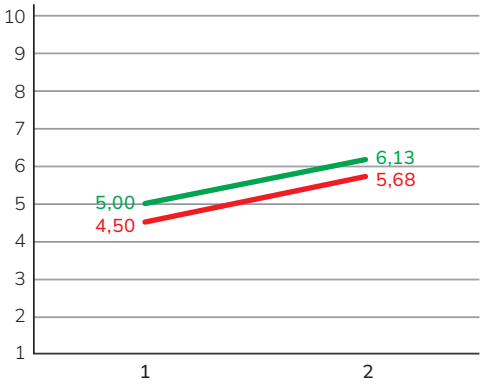
Per quanto riguarda i laboratori nelle scuole secondarie di primo grado, basati sull'utilizzo del videogioco "Nabbovaldo e il ricatto dal cyberspazio", in totale, hanno preso parte al progetto, compilando i questionari sia alla prima che alla seconda rilevazione, 204 studenti e studentesse.

A seguito del percorso formativo, il livello medio di conoscenze relative alla Rete Internet, migliora sia per quanto riguarda le conoscenze generali (Figura sotto a sinistra) che quelle più specifiche (Figura sotto a destra). Le femmine (segmento rosso), per quanto riguarda le conoscenze più specifiche, recuperano il gap nei confronti dei loro coetanei maschi (segmento verde) e, a seguito del percorso formativo, raggiungono il loro stesso livello medio di conoscenze.

CONOSCENZE: GENERALI

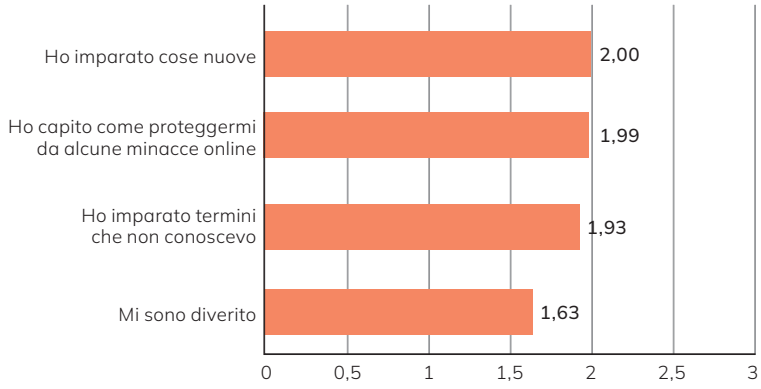


CONOSCENZE: SPECIFICHE



Inoltre, dalla valutazione è emerso che il 60% dei/delle partecipanti al progetto ha utilizzato il videogioco: la maggior parte di loro ha giocato solamente un paio di volte al mese, riuscendo a completare solamente il primo capitolo. Inoltre, i ragazzi e le ragazze hanno giocato prevalentemente a casa da soli. In generale, il videogioco è stato valutato come uno strumento utile, con meccanismi di gioco facili da comprendere e una grafica originale. Inoltre, i temi affrontati sono stati giudicati interessanti, anche grazie alla storia coinvolgente. La maggior parte ha dichiarato di aver imparato nozioni nuove, tra cui pratiche di sicurezza informatica e termini tecnici.

GIOCANDO AL VIDEOGIOCO



Glossario

A

AI
Abbreviazione di Artificial Intelligence (Intelligenza Artificiale), disciplina che si occupa dello studio di funzioni tipiche dell'intelligenza umana e della loro possibile replicazione mediante metodi e strumenti informatici.

Algoritmo
Procedimento che consente la risoluzione di problemi di carattere logico e matematico, o pratico.

Antivirus
Software che riconosce la presenza di virus informatici nei file e nelle memorie di massa e cerca di rimuoverli o di neutralizzarli.

APT
(Advanced Persistent Threat). Minaccia consistente in un attacco mirato, volto ad installare una serie di malware all'interno delle reti bersaglio, al fine di riuscire a mantenere attivi i canali impiegati per la fuoriuscita di informazioni pregiate dalle infrastrutture IT del target.

Area Controllata
Area predisposta in prossimità di un'area riservata, dove possono essere trattate solo informazioni classificate a livello RISERVATO. Deve essere dotata di misure di protezione tali da consentire l'accesso alle sole persone autorizzate per motivi attinenti al loro impiego, incarico o professione.

Attacco DDoS
Un attacco combinato di numerose macchine pensato per portare al collasso siti web o server, la maggior parte delle volte condotto per mezzo di Botnet

Avatar
Identità fittizia, soprannome, immagine virtuale in rete.

B

Backdoor
In inglese indica la porta di servizio, quella di solito sul retro di un edificio. Viene chiamato così un sistema, spesso nascosto, utilizzato per aggirare la normale procedura di autenticazione a un sistema informatico e ottenerne l'accesso. In alcuni casi le backdoor sono installate volutamente dall'amministratore del sistema per agevolarne la manutenzione in caso di problemi. Spesso però vengono installate furtivamente e utilizzate da hacker per poter continuare ad avere accesso al sistema che hanno compromesso.

Backup
Salvataggio, totale o parziale, dei contenuti di una memoria.

Blue Box
La "scatola blu" è storicamente uno dei primi strumenti usati per "violare" i sistemi telefonici, sfruttando la tecnologia e le falle di sicurezza degli stessi. Si trattava di un dispositivo elettronico che emetteva segnali sonori, o "toni", corrispondenti ai messaggi di segnalazione, e questi venivano mandati direttamente sulla linea telefonica. L'uso più comune che veniva fatto era per telefonare gratuitamente. Tramite la blue box era infatti possibile alterare la segnalazione tra le centrali telefoniche, e dirottare la chiamata verso la destinazione desiderata pur chiamando un numero differente. In questo modo veniva ingannato il sistema di tariffazione del gestore telefonico. Un famoso hacker delle linee telefoniche era "Captain Crunch", che aveva ottenuto originariamente questo risultato con un fischietto omaggio nelle scatole dei cereali Cap'n Crunch (da cui deriva il suo nickname).

Bot
Programmi che sono in grado di riprodurre il comportamento umano on-line come, ad esempio, popolare un profilo social e inviare messaggi in una chat.

Botnet
Una rete di computer utilizzata per attacchi da remoto formata da computer infetti spesso appartenenti a persone inconsapevoli e gestiti a distanza. Tali macchine infettate nel gergo vengono chiamate zombie.

Bring Your Own Device (BYOD)
Insieme di policy interne ad un'organizzazione, sia essa pubblica o privata, volte a regolare l'impiego di dispositivi digitali personali all'interno della stessa, da parte dei relativi dipendenti.

Bug
Errore in una procedura informatica.

C

Codice
Si parla di codice per indicare dati che rappresentano istruzioni che un computer può eseguire. Tutto ciò che viene eseguito da un computer o da uno smartphone, ad esempio un'app, è composto da codice!

Codice Sorgente
Il codice sorgente o semplicemente sorgente è il testo di un algoritmo scritto dal programmatore in un qualsiasi linguaggio di programmazione. Si chiama sorgente perché è da qui che si parte per ottenere il programma o l'app desiderata.

Codice malevolo
Si parla di codice malevolo per indicare una serie di dati che rappresentano istruzioni potenzialmente dannose.

Consapevolezza digitale
Prestare attenzione in maniera peculiare, piena conoscenza e capacità di utilizzo e gestione delle tecnologie IT e dei social media. Si veda la campagna e le iniziative avviate dalla Presidenza del Consiglio con il marchio "Be Aware Be Digital".

Criptovalute
Valute digitali che si basano sulla crittografia sia per la loro generazione, sia per la convalida delle transazioni.

Crittografia
Tecnica che permette di nascondere il contenuto di un messaggio. Ciò in modo che esso possa essere correttamente compreso solo da chi ne possiede la chiave di decifrazione.

Cyber-attacco
Si riferisce ad una manovra di attacco informatico da parte di uno o più individui verso un sistema, con la finalità di accedere, modificare, distruggere o rubare informazioni e dati.

Cyberbullismo

Manifestazione in rete di un fenomeno più ampio e meglio conosciuto come bullismo. Quest'ultimo è caratterizzato da azioni violente e intimidatorie esercitate da un bullo, o un gruppo di bulli, su una vittima. Le azioni possono riguardare molestie verbali, aggressioni fisiche, persecuzioni, generalmente attuate in ambiente scolastico. Oggi la tecnologia consente ai bulli di infiltrarsi nelle case delle vittime, di materializzarsi in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet. Il bullismo diventa quindi cyberbullismo. Il cyberbullismo definisce un insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici (sms, mms, foto, video, email, chat rooms, istant messaging, siti web, telefonate), il cui obiettivo e quello di provocare danni ad un coetaneo incapace a difendersi.

Cyber-crime
Qualsiasi reato o comportamento delittuoso svolto nell'ambito delle procedure informatiche.

Cyber-Defense
L'insieme della dottrina, dell'organizzazione e delle attività volte a prevenire, rilevare, limitare e contrastare gli effetti degli attacchi condotti nel e tramite il cyber- space ovvero in danno di uno o più dei suoi elementi costitutivi.

Cybersecurity
Condizione in cui il cyberspace risulti protetto rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittime ovvero nel blocco dei sistemi informativi, grazie a idonee misure di sicurezza fisica, logica e procedurale.

Cyberspace (cyberspazio)
L'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati e utenti nonché delle relazioni logiche, comunque stabilite, tra di essi. Include tra l'altro internet, reti di comunicazione, sistemi attuatori di processo e apparecchiature mobili dotate di connessione di rete.

Cyberwar
L'insieme delle operazioni condotte nel e tramite il cyberspace al fine di negare all'avversario – statuale o non – l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati. Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del cyberspace).

D

Dark Web
Contenuti del web nelle darknet (reti oscure) che possono essere raggiunti esclusivamente con software specifici.

Data Breach
Violazione dei dati: nel campo della sicurezza informatica si riferisce alla violazione della sicurezza dei dati, che può avvenire per errore o intenzionalmente, mediante la distruzione, la perdita, la modifica, la divulgazione o l'accesso ai dati personali di uno o più persone.

DEEP WEB (web profondo)
Porzione di Internet che non viene indicizzata dai tradizionali motori di ricerca.

Disinformazione
Diffusione di notizie infondate o distorte al fine di danneggiare l'immagine pubblica di un avversario e/o di influenzarne le scelte.

Distributed Denial of Service (DDoS)
Attacco DoS lanciato da un gran numero di sistemi compromessi e infetti (botnet), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse e il sovraccarico delle connessioni di rete dei sistemi server.

Doxing
Deriva dall'inglese "documents", abbreviato in "dox", ed è la pratica di diffondere pubblicamente online le informazioni private e sensibili di una persona.

E

Encryption/crittografia
E' la conversione di dati in una forma che può essere decodificato solo da chi possiede una chiave di lettura o da chi è in grado di violare il meccanismo di cifratura.

Exploit
Una porzione di "codice" che sfruttando una vulnerabilità permette, nelle dovute circostanze e con le giuste capacità, di accedere ad un sistema informatico.

F

Fattore Umano
La sicurezza informatica è caratterizzata dalla presenza di una serie di componenti hardware e software. Con la dicitura "Fattore Umano" in questo contesto ci si rivolge ad un altro importante aspetto della catena della sicurezza informatica stessa: la presenza dell'uomo. L'intervento dell'uomo è infatti presente e determinante sia dal lato di chi ha intenzioni malevole, come ad esempio un Hacker, sia da parte di chi protegge i propri dati, o scrive programmi utilizzati nell'ambito della sicurezza. In tema di difesa dagli attacchi da parte degli Hacker, l'insieme delle buone norme di condotta da adottare da parte degli individui o delle organizzazioni è un aspetto cruciale per prevenire o attenuare le conseguenze degli attacchi stessi.

Firewall
Dall'inglese "porta antincendio" è un dispositivo che permette di proteggere reti informatiche da accessi indesiderati, ma come tutte le tecnologie a volte è possibile aggirarla!

Firmware
Firmware deriva da "firm" e "software", ovvero componente software permanente, ed è un insieme di istruzioni integrate direttamente in un componente elettronico programmato, che consentono ad un dispositivo di avviarsi e di interagire con altri dispositivi. Pur trattandosi di istruzioni permanenti, i dispositivi moderni permettono l'aggiornamento del firmware.

Follower
Nei Social Network, chi decide di seguire le comunicazioni di un utente, diventandone seguace.

Flamer
Deriva dal termine inglese "flame", fiamma. Nel gergo di Internet è chi "infiamma" le discussioni online provocando litigi.

Ftp
Il File Transfer Protocol (FTP), è un protocollo Internet che facilita il caricamento o il download di file digitali.

G

GDPR
A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri europei il Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

H

Hacker
Di per sé l'hacker non è ne buono ne cattivo, si tratta solo di persone, ragazze, ragazzi estremamente curiose, capaci di studiare e scoprire cose nuove, nonché utilizzi "diversi" di ciò che si trovano davanti, in italiano potrebbero essere chiamati "smanettoni". Di solito vengono suddivisi in black o white hat a seconda se siano "hacker buoni" o "hacker cattivi", ma è una definizione che ai veri hacker non piace!

Hacktivista
Termine che deriva dall'unione di due parole, hacking e activism e indica chi pone in essere le pratiche dell'azione diretta digitale in stile hacker. Nell'ambito dell'hacktivism le forme dell'azione diretta tradizionale sono trasformate nei loro equivalenti elettronici, che si estrinsecano prevalentemente, ma non solo, in attacchi DDoS e web defacement.

Hater
Proviene dal verbo inglese "to hate", odiare. È un termine usato su Internet per indicare gli utenti che di solito disprezzano, diffamano o criticano una persona con intento distruttivo.

HTTP
L'HyperText Transfer Protocol (HTTP), ovvero il protocollo di trasferimento di un ipertesto, è un protocollo, uno standard, usato come principale sistema per trasferire informazioni sul web. L'HTTP si basa su un sistema di comunicazione tra "client" e "server": il client esegue una richiesta e il server restituisce la risposta. Nell'uso comune il client corrisponde al browser con cui si naviga su internet (ad esempio Chrome, Edge, Firefox, Opera, Safari), il server è la macchina su cui risiede il sito web.

HTTPS
Aggiungendo una "S", che racchiude il significato di Sicurezza, al protocollo HTTP, otteniamo l'HTTPS. Questo è infatti protocollo per la comunicazione attraverso una rete di computer utilizzato su Internet, all'interno di una connessione sicura, criptata. HTTPS permette di verificare che il sito visitato sia autentico, fornisce una protezione maggiore della privacy e garantisce che i dati scambiati tra l'utente e il sito web non vengano intercettati o manomessi.

I

Indirizzo IP
È un codice univoco, composto da quattro set di cifre comprese tra 0 e 255 che identifica ogni dispositivo direttamente connesso ad internet.

Ingegneria sociale (o Social engineering)
Tecniche di manipolazione psicologica affinché l'utente compia determinate azioni o riveli informazioni sensibili come, ad esempio, credenziali di accesso a sistemi informatici.

Internet of Things (IoT)
Neologismo riferito all'interconnessione degli oggetti tramite la rete Internet, i quali possono così comunicare dati su sé stessi e accedere ad informazioni aggregate da parte di altri, offrendo un nuovo livello di interazione. I campi di impiego sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'infomobilità, o all'efficienza energetica, all'assistenza remota, alla tutela ambientale e alla domotica.

IT
Information Technology (tecnologia dell'informazione), ossia l'insieme di tutte le tecnologie che afferiscono al trattamento dell'informazione, normalmente inteso come trattamento digitale dell'informazione.

K

Keylogger
È uno strumento che permette di registrare tutto ciò che viene digitato su una tastiera all'insaputa della vittima.

L

Landing Page
Landing Page È la pagina che il visitatore raggiunge dopo aver cliccato un link o una pubblicità.

Link
Un tipo di collegamento attivo, agendo sul quale si viene automaticamente rimandati a una ulteriore informazione o approfondimento.

Linux
È il più diffuso sistema operativo libero. Modificabile e distribuibile liberamente. In poche parole, il sistema operativo preferito da hacker, scienziati, smanettoni e da chiunque si occupi di sicurezza informatica, per essere precisi andrebbe chiamato GNU/Linux.

Login
Procedura con cui si accede a una sezione riservata di un sito Internet.

M

Malware
Software pirata inserito in un sistema informatico, generalmente in modo clandestino, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

Minaccia cibernetica
Espressione impiegata per indicare l'insieme delle condotte controindicate che possono essere realizzate nel e tramite il cyber-space ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici: azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare integrità e riservatezza di dati/ informazioni.

N

Netiquette
L'insieme delle regole del corretto comportamento degli utenti in rete. Mira a garantire il corretto scambio di dati e informazione nel rispetto delle norme di civiltà e dell'opinione altrui.

Noob
Abbreviazione di newbie, ovvero di chi è alle prime armi! Attenzione a non farla passare per un'offesa, tutti nella vita sono passati per essere dei noob!

O

Open Source
È quel software di cui è disponibile il codice sorgente, questo a differenza della maggior parte dei programmi commerciali. Viene chiamato più precisamente "Software Libero" perché risulta liberamente consultabile, modificabile e ridistribuibile da tutti gli utenti. Ricorda sempre: "Sharing is caring!"

P

Password
Sequenza di caratteri nota solo al legittimo proprietario: la sua introduzione consente l'accesso a parti di programmi o di siti, confermando che il richiedente ha le abilitazioni necessarie.

Phishing
Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (userid, password, numeri di carte di credito, PIN) con l'invio di false email generiche a un gran numero di indirizzi. Le email sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Il phisher utilizza i dati acquisiti per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Proxy
È un server che può essere usato per mascherare il proprio IP.

Q

QR CODE
Codice a barre bidimensionale (o codice 2D), ossia a matrice, impiegato per memorizzare informazioni generalmente lette attraverso un mobile o uno smartphone. Ma è anche uno strumento di Mobile Marketing che consente di ottenere in modo continuo nuovi flussi di contatti qualificati e targhettizzati.

R

Ransomware
Malware che cripta i file presenti sul computer della vittima, richiedendo il pagamento di un riscatto per la relativa decrittazione. I ransomware sono, nella maggioranza dei casi, dei trojan diffusi tramite siti web malevoli o compromessi, ovvero per mezzo della posta elettronica. Questi si presentano come allegati apparentemente innocui (come, ad esempio, file PDF) provenienti da mittenti legittimi (soggetti istituzionali o privati). Tale elemento induce gli ignari utenti ad aprire l'allegato, il quale riporta come oggetto diciture che richiamano fatture, bollette, ingiunzioni di pagamento e altri oggetti similari.

Reverse engineering
È un processo che letteralmente significa ingegneria inversa, e consiste nell'analizzare dettagliatamente il funzionamento di un oggetto, come ad esempio un dispositivo, un componente digitale o un software, al fine di ottenere tutte le informazioni necessarie per produrre un nuovo dispositivo o software che abbia un funzionamento simile a quello originario.

Rootkit
Software malevolo, a volte molto sofisticato, capace di accedere ad un computer e garantire l'accesso all'attaccante, aggirare il controllo da parte dell'amministratore di sistema riuscendo anche a nascondere la propria presenza.

S

Script kiddie
Pur non essendo legato direttamente all'età della persona, Script Kiddie deriva da "programma" (script), e "ragazzo" (kid) in inglese, ed è un termine dispregiativo che indica quelle persone che usano codici o appunto programmi, scritti in gran parte da altri, per far credere di essere esperti di informatica.

Sniffing
Si chiama così quell'attività che prevede di "intercettare" i dati che passano su una rete, comprese comunicazioni, password

Smartphone
Tipo di telefono cellulare che, oltre alle funzioni di telefono, integra la gestione di dati personali, il collegamento a Internet, la posta elettronica, ecc.

Social Engineering (o Ingegneria Sociale)
Arte di manipolare psicologicamente le persone affinché compiano determinate azioni o rivelino informazioni confidenziali, come le credenziali di accesso a sistemi informatici.

Spam
Messaggi di posta elettronica indesiderati, generalmente pubblicitari o malevoli.

Spear-Phishing
Attacco informatico di tipo phishing condotto contro utenti specifici mediante l'invio di email formulate con il fine di carpire informazioni sensibili dal destinatario ovvero di indurlo ad aprire allegati o link malevoli.

Spoofing
Manipolazione di dati telematici quali l'indirizzo IP o l'email del mittente, così come l'estensione di file, tali da farli apparire innocui o, comunque, provenienti da soggetti noti o che non generano sospetti.

Spyware
Tipo di software malevolo che "spia" le attività in rete di un utente per carpirne codici, azioni, ecc.

Stuxnet
È un virus informatico creato e diffuso nel 2006. Consisteva in una serie di attacchi digitali contro l'Iran. Lo scopo del software era il sabotaggio della centrale nucleare iraniana di Natanz. Il sabotaggio avveniva facendo girare le centrifughe della centrale ad una velocità eccessiva per disabilitarle, impedendo l'individuazione dell'anomalia.

T

TAG RFID
Radio Frequency IDentification: è un dispositivo senza fili e senza batterie, contenente informazioni di vario genere, lo si può trovare nelle carte di credito per pagare contact-less o nei biglietti dell'autobus. Con un opportuno dispositivo è possibile leggere e/o modificare le informazioni contenute al suo interno.

Typosquatting
Consiste nella registrazione a dominio di un nome molto simile a quello di un dominio noto. La differenza è di solito minima e concepita in maniera tale da non essere graficamente distinguibile dall'utente (ad esempio, la "l" minuscola è spesso sostituita dal numero "1").

Trojan
Tipo di software malevolo, che si annida nel PC ospite camuffandosi da programma innocuo, come il mitico Cavallo di Troia, che fu portato all'interno delle mura della città, causandone la distruzione.

Troll
Nelle leggende scandinave il troll è un abitante demoniaco di boschi, montagne, luoghi solitari: è l'equivalente dell'"orco" di altre tradizioni popolari europee.

Nel gergo di Internet, il troll è l'utente di una comunità virtuale che intralcia il normale svolgimento di una discussione inviando messaggi provocatori, irritanti o fuori tema.

U

Underground
Con tale termine si intende l'ambiente, solitamente digi- tale, frequentato per l'acquisto o la condivisione di strumenti di hacking.

Url
Sequenza di caratteri che identifica in modo univoco l'indirizzo in Internet di una pagina, di un documento o di una risorsa.

Username
Il nome identificativo dell'utente che è normalmente visibile, diversamente dalla password.

V

Virus
Software malevolo che può infestare un PC, inserendosi in un programma applicativo, causando danni diretti o indiretti, e che può propagarsi da questo ad altri PC tramite file condivisi, email, ecc.

VoIP (Voice over IP)
Protocollo che permette la trasmissione in Internet, con protocollo IP, della voce. Permette di ottenere la fonia su Internet.

W

Web
Servizio di Internet che permette di navigare e di usufruire dei contenuti multimediali della Rete.

Web defacement (defacciare)

Attacco condotto contro un sito web e consistente nel modificare i contenuti dello stesso limitatamente alla homepage ovvero includendo anche le sottopagine del sito.

Webmaster
In un sito Internet, il responsabile del corretto funzionamento del sito e dei suoi contenuti.

White - Grey - Black Hat
Viene definito "white hat", un hacker, un esperto di programmazione e sicurezza informatica, in grado di introdursi nei sistemi di reti con l'obiettivo di aiutare i proprietari di quel sistema a scoprire eventuali falle nell'accesso, valutarne l'affidabilità, e risolvere potenziali problemi di sicurezza, rispettando dunque l'etica degli hacker. Si può definire dunque a tutti gli effetti un "hacker buono". Il white hat si contrappone a chi si introduce illegalmente nei sistemi informatici con l'obiettivo di appropriarsi illecitamente di informazioni o provocare un danno, che viene definito "black hat". Una figura intermedia tra white hat e black hat è invece il "grey hat", che ha l'inclinazione a violare le leggi e l'etica, ma non ha l'intento doloso tipico del "black hat".

Wireless
Sistema di comunicazioni senza fili.

Z

Zero Day
Con questo termine (o 0-day) si indica una minaccia informatica che sfrutta vulnerabilità di applicazioni software non ancora divulgate o per le quali non è ancora stata distribuita una patch. Gli attacchi zero-day sono considerati una minaccia molto grave, in quanto sfruttano falle di sicurezza per le quali non è al momento disponibile nessuna soluzione.

Bibliografia

- Bottino R.M., et al... (2019): Digital games in primary schools for the development of key transversal skills, in Proc. of SUZA 2019
- Calvani A., (2013). I nuovi media nella scuola. Perché, come, quando avvalersene, Carocci, Roma
- Celot P., R. Franceschetti, E. Salamini, (2021), Educare ai nuovi media. Percorsi di cittadinanza digitale per l'educazione civica, Pearson Academy
- Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J. & Weintrop, D. Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. Simulation & Gaming, doi: 10.1177/1046878120933312, 2020, 51(5), 586–611
- Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T. & Boyle, J. M. A systematic literature review of empirical evidence on computer games and serious games. Computers & Education, doi: 10.1016/j.compedu.2012.03.004, 2012, 59(2), 661–686
- Ferri P., Nativi digitali, Mondadori 2011
- Ferro L.S., et al, (2020): A game-based learning experience for improving cybersecurity awareness, 4th Italian Conference on cybersecurity, Itasec 2020
- Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. Youth Internet Safety Education: Aligning Programs with the Evidence Base. Trauma, Violence, & Abuse, doi: https://doi.org/10.1177/1524838020916257, 2012, 22(5), 1233–1247.
- Haddon, L., Cino, D., Doyle, M., Livingstone, S., Mascheroni, G., & Stoilova, M. (2020). Children's and young people's digital skills: a systematic evidence review. Zenodo.10.5281/zenodo.427465
- Maglioni M., Biscaro F., (2014), La classe capovolta. Innovare la didattica con la flipped classroom, Erikson, Milano
- Prensky M., Digital game-based learning, New York: McGraw-Hill, 2001
- Ranieri, M. (2015). Linee di ricerca emergenti nell'educational technology. Form@ re-OpenJournal per la formazione in rete, 15(3), 67-83
- Rivoltella P. C., (2020), Nuovi alfabeti, Scholè, Brescia
- Zühal Okan, Edutainment: is learning at risk? British Journal of EducationalTechnology, Volume 34, Issue 3, 2003

A conclusione di questo nostro libro, desideriamo esprimere i nostri più sentiti ringraziamenti a tutti coloro che hanno contribuito alla realizzazione del metodo Ludoteca. In primo luogo, i nostri ringraziamenti vanno al Registro, ai Direttori e ai componenti del Comitato di Gestione che si sono succeduti dal 2011 in poi, i quali hanno sempre sostenuto la Ludoteca sia finanziariamente che progettualmente.

Un sincero ringraziamento va anche a tutti i ricercatori e tecnologi dell'Istituto di Informatica e Telematica, che hanno offerto il loro prezioso contributo nella produzione e revisione dei contenuti, nonché ai professionisti ed esperti che ci hanno generosamente donato il loro sapere e il loro tempo per la realizzazione delle nostre rubriche video.

Il ringraziamento più sentito è rivolto alle colleghe e ai colleghi dello staff della Ludoteca e dell'Unità Relazioni Esterne, Media, Comunicazione e Marketing del Registro .it, che fin dall'inizio e ancora oggi collaborano attivamente al progetto, portando il metodo Ludoteca nelle scuole di ogni ordine e grado e facendo dell'educazione alla cultura digitale una vera missione.

Infine, vogliamo ringraziare tutte le scuole, gli/le insegnanti, i genitori e i ragazzi e le ragazze che abbiamo incontrato nel corso di oltre 10 anni. Le loro esperienze e la loro partecipazione attiva hanno arricchito il lungo viaggio della Ludoteca.

Ludoteca

Registro.it

Registro.it
L'ANAGRAFE DEI DOMINI .IT

IIT ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche