CITTÀ DI VENEZIA

ACLI VENEZIA

PROSSIMI^
Digitale, Sostenibile, Inclusivo

SAFER INTERNET DAY

GIORNATA MONDIALE SULLA SICUREZZA IN RETE

REGIONE DEL VENETO

AGENDA DIGITALE 2025 DEL VENETO

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

REPUBBLICA DIGITALE

Finanziato dall'Unione europea NextGenerationEU

PUNTO DIGITALE FACILE

CYBER SECURITY

PERCHÉ È IMPORTANTE?

La cyber security serve a proteggere sistemi, reti, programmi e dati da attacchi informatici. Questi attacchi hanno di solito lo scopo di accedere, modificare o distruggere informazioni sensibili; estorcere denaro agli utenti; o interrompere normali processi aziendali.

A livello individuale, un attacco informatico può comportare di tutto, dal furto d'identità, ai tentativi di estorsione, alla perdita di dati importanti come le foto personali e di famiglia.

E tu? Sai come adottare un comportamento responsabile su internet? Quali sono i pericoli più comuni in rete?

TRACCIAMENTO

SPAM

FUGHE DI DATI

FURTO D'IDENTITA'

PHISHING

DOXING

Le **spam** sono mail indesiderate che, oltre ad essere un elemento di disturbo per via delle pubblicità in esse contenute, possono anche costituire una tentativo di trasmissione di malware (virus) e di accesso ai tuoi dati personali.

Meno conosciuto è il **doxing**, cioè la diffusione malevola di informazioni personali o private online, spesso con l'intento di danneggiare la vittima in modi diversi.

WIFI pubblico sì, ma con prudenza

- Assicurati che **l'hotspot sia legittimo**
- Scegli solo siti con il **protocollo HTTPS**
- Non condividere **informazioni sensibili**
- Se non sei sicuro usa la **rete mobile**

LO SAPEVI CHE?

Lo sapevi che?
*Il **phishing** è il cyber attacco più utilizzato, perché è quello **più economico e più efficace;** basta che l'utente "si fidi" e inserisca i dati nel sito fraudolento.*
Una volta che le informazioni personali sono in loro possesso, possono essere usate per rubare l'identità della vittima.

IL FURTO D'IDENTITÀ DIGITALE COSTITUISCE REATO DI SOSTITUZIONE DI PERSONA

COME RENDERE SICURO IL TUO SMARTPHONE

Non cliccare sulle pubblicità

Potrebbero contenere un **particolare tipo di virus** in grado di attivare la pubblicità indesiderata, e talvolta dannosa, sullo schermo del tuo dispositivo così come registrare le tue preferenze ed interessi tramite la profilazione dei dati.

Non aprire link o messaggi sospetti!

Il tentativo di phishing può arrivare anche tramite **SMS** (smishing) con lo stesso scopo di acquisire informazioni personali con scopi illegali.

Proteggi i tuoi dati in modo sicuro

Imposta una **password complessa** (con caratteri alfanumerici e speciali). Più è complessa, più è forte! Se scegli un **PIN** assicurati di inserire una sequenza lunga. È più difficile da indovinare! Oppure opta per l'**impronta digitale** o il **riconoscimento facciale**. È più sicuro e pratico!

COME RICONOSCERE SE TI HANNO HAKERATO?

- *Pubblicità e pop up*
- *Smartphone lento*
- *Aumento del consumo dati*
- *Le app si chiudono improvvisamente*
- *App installate senza motivo*
- *Consumo batteria eccessivo*

Come denunciare alla Polizia Postale

Le modalità di denuncia sono due:
1) **online** direttamente sul sito della Polizia Postale;
2) recandosi **di persona** all'Ufficio di Polizia più vicino.

Per **compilare una denuncia di truffa** online servono:

- **dati anagrafici** della vittima, compresi i dettagli della carta d'identità;
- una **descrizione dettagliata** dell'evento fraudolento specificando la tipologia di truffa subita
- il **nome del sito web** o dei siti coinvolti nell'incidente.

Centro Operativo per la Sicurezza Cibernetica (C.O.S.C.) del Veneto, con sede a Venezia in Via Cappelletto, 11
Tel. - 041/2907311

PRIVACY E SOCIAL NETWORK:
ATTENZIONE A CHI E COSA PUBBLICHI!

Se utilizzi i social network sei quotidianamente sottoposto ad una serie di rischi che possono influire sulla tua sicurezza, la tua privacy ed il tuo benessere.

La presenza di una gran quantità di dati in un unico luogo (foto, nomi, posizione gps), fa sì che i social network siano tra i target preferiti dagli hacker.

VIOLAZIONE DELLA PRIVACY

Chi pubblica una foto su Instagram con un amico, se quest'ultimo non ha dato il suo consenso specifico alla pubblicazione, sta commettendo una violazione della privacy.

MINACCE E STALKING

Lo **stalking**, ovvero la sistematica reiterazione della **persecuzione di un individuo**, le **minacce** e le **molestie** reiterate via social sono punibili per legge. **[Art. 612 bis del Codice Penale italiano; reato di cyberstalking]**

Questo può includere: monitoraggio dei profili altrui, invio ripetuto di messaggi o commenti non richiesti, e la raccolta di informazioni personali.

CYBERBULLISMO

Con questo termine si indicano tutti i comportamenti dannosi ed offensivi ripetuti nel tempo, mirati ad una vittima, e perpetrati attraverso canali di comunicazione online e virtuali. La **legge del 2017** prevede che il minore vittima di cyberbullismo (se ha più di 14 anni; altrimenti i genitori) può richiedere l'oscurazione, la rimozione ed il blocco dei contenuti diffusi in Rete oggetti della pratica direttamente al gestore del sito internet, o del social media, o al titolare del trattamento.

COSA FARE QUINDI NELLA PRATICA?

CONDIVIDI... MA CON CAUTELA

- Non diffondere informazioni altamente personali e potenzialmente preziose.
- Crea della password uniche, complesse e difficili da indovinare per ciascun account.
- Evita di condividere informazioni sensibili come indirizzi, numeri di telefono o dettagli personali.
- Accetta solo le richieste di amicizia o i follower da persone che conosci o che ti sembrano autentiche.
- Attenzione alle email o ai messaggi che sembrano sospetti.
- Controlla e personalizza le impostazioni della privacy sui tuoi account.
- Segnala eventuali comportamenti inappropriati.
- Verifica chi può leggere i tuoi post, chi può inviarti messaggi e chi può taggarti nelle foto.

OCCHIO ALLE FAKE NEWS!

Per "**fake news**" si intendono tutte quelle **informazioni non veritiere o fuorvianti** che vengono diffuse attraversi vari mezzi di comunicazione con l'intenzione di ingannare, disinformare, calunniare, creare scandalo o spesso anche con il fine di generare click su Internet (clickbaiting).

Vengono presentate in **forma** di **articoli, libri o pubblicazioni** e tradizionalmente diffuse attraverso i mezzi di comunicazione di massa, come le emittenti televisive e le testate giornalistiche, tuttavia, con l'ascesa di Internet e la diffusione dei social media, la loro proliferazione è aumentata in modo significativo.

LA DIPENDENZA DA INTERNET

La costante **accessibilità a Internet** ed in particolare ai social media ha creato una società estremamente iperconnessa, nella quale hai la possibilità di utilizzare la rete attraverso svariati dispositivi in qualsiasi momento e da qualsiasi luogo ti trovi.

Se da un lato questo ha portato a vantaggi indiscutibili, non si può trascurare l'esistenza di alcuni risvolti negativi, talvolta gravi, come la **FOMO** (Fear of Missing Out) e lo sviluppo di una **vera e propria dipendenza da Internet**, che sia essa legata alle informazioni, allo shopping, ai videogiochi e ai giochi d'azzardo online oppure la più nota **dipendenza dai social media**, cui si affianca la dipendenza da messaggistica istantanea (WhatsApp, Messenger o Telegram).

In generale, tutte queste forme di dipendenza sono caratterizzate da un'**incapacità di controllare l'uso di Internet**, nonostante le conseguenze negative sulla vita quotidiana (ansia, depressione, stress, vere e proprie crisi di astinenza).

Ricorda che il **riconoscimento dei sintomi** e la **ricerca di aiuto** sono due passi fondamentali per il recupero psicologico ed il ripristino di uno stile di vita sano ed equilibrato.

LO SAPEVI CHE?

Hikikomori *(lett. "stare in disparte) è un termine giapponese che indica* ***l'isolamento sociale volontario*** *di alcuni giovani (tra i 12 e 30 anni), i quali decidono di rinchiudersi nella propria camera per lunghi periodi e di* ***limitare il più possibile i contatti con il mondo esterno****.*

GLI 8 PASSI PER PREVENIRE LA DIPENDENZA DA INTERNET

Informati e sii consapevole
Comprendere i rischi associati all'uso di Internet è il primo passo per prevenirli. Bisogna essere consapevoli dei sintomi della dipendenza e dei suoi effetti negativi sulla salute mentale e fisica.

Stabilisci dei limiti di tempo
Programmare regolarmente delle "pause digitali" in cui staccare completamente dalla tecnologia, può aiutarti a ripristinare la connessione con il mondo reale e a ridurre il rischio di dipendenza.

Pratica l'autodisciplina
Impara a gestire l'impulso di utilizzare Internet in modo eccessivo. Cerca di essere consapevole delle tue abitudini e di interrompere le sessioni online quando hai raggiunto il limite stabilito.

Bilancia con attività off-line
Bilancia l'uso di Internet con attività della vita reale, praticando uno sport o una tua passione, partecipando ad incontri con i tuoi amici e alle attività all'aperto.

Stabilisci le priorità
Definisci chiaramente le tue priorità nella vita. È essenziale! Identifica obiettivi personali, familiari, accademici o professionali e assicurati che l'uso di Internet non li ostacoli. La priorità dovrebbe essere data alle relazioni personali, alla salute fisica e mentale e alle responsabilità quotidiane.

Coinvolgi amici e familiari
Condividere le tue preoccupazioni con amici e familiari può portare a un supporto sociale positivo e ad un maggiore impegno per ridurre l'uso eccessivo di Internet.

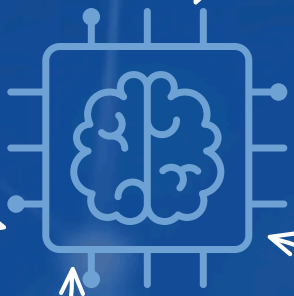
Riconosci le red flags
Presta attenzione ai segnali di avvertimento della dipendenza da Internet. Se noti un aumento del tempo trascorso online, l'isolamento sociale o l'incapacità di concentrarti su altre attività, è importante affrontare questi problemi in modo proattivo.

Cerca l'aiuto di un professionista
Se sospetti di avere una dipendenza da Internet o fai fatica per ridurre l'uso eccessivo nonostante gli sforzi, è fondamentale cercare l'aiuto di un professionista della salute mentale specializzato nella gestione delle dipendenze.

L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE

Accantonando i timori legati all'Intelligenza Artificiale, come tutti gli strumenti, non è né buona né cattiva: tutto dipende dall'uso che ne fai.

Gli aspetti positivi si traducono nella sostituzione del lavoratore umano per mansioni di tipo pesante e ripetitivo (mediante l'utilizzo di macchinari automatizzati), l'aumentato livello di sicurezza dei dispositivi (con meccanismi di blocco/sblocco mediante l'identificazione di dati biometrici).



Il suo obiettivo è quello di sollevare l'essere umano dallo svolgimento delle mansioni più pesanti e ripetitive, che nulla portano alla qualità delle nostre vite.

Una parentesi a parte deve essere fatta per le **intelligenze artificiali di tipo generativo**, come Alexa e Chat GPT, le quali sono in grado di generare testo, immagini, video, musica o altri media in risposta a delle richieste, dette **prompt**.

CHAT GPT

Attraverso il **Machine Learning**, che permette alle macchine di apprendere dall'esperienza, e il **Deep Learning**, che sfrutta i vari strati di reti neurali per calcolare i valori di quelli successivi, Chat GPT può **apprendere autonomamente**, attraverso gli input che riceve dai propri utenti.

L'Intelligenza Artificiale ha un ruolo determinante nell'**analisi della grande quantità di dati** e nella **personalizzazione** dei risultati delle ricerche, utente per utente. Ma può fare di più.

L'Intelligenza Artificiale sta dando un notevole impulso a sistemi che apprendono o migliorano le performance in base ai dati utilizzati e gli algoritmi alla base dei motori di ricerca evolvono con l'obiettivo dichiarato di **riuscire a fornire agli utenti le informazioni più pertinenti e complete.**

Sono molte le occasioni in cui **condividiamo informazioni personali online**, spesso senza la consapevolezza che ogni nostra attività in rete viene "registrata" e tutte le informazioni che ricerchiamo e digitiamo vengono "memorizzate".