



Educazione digitale per una migliore cybersecurity

#beaware #cybersecurity

Vita digitale



Vita digitale

Viviamo in una **società digitale** che ci permette di essere costantemente **connessi** tramite dispositivi e tecnologie con i quali **interagiamo** quasi ininterrottamente durante la nostra giornata

Vita digitale e vita reale

Le nostre vite fisiche e le nostre vite digitali si **incontrano e sovrappongono**, creando un'esperienza inscindibile e unica.

Pericoli della vita digitale

In questo universo digitale siamo esposti a diversi **rischi** che incidono sulla nostra **sicurezza**, proprio come nel mondo fisico.

Ma spesso non siamo **consapevoli dei pericoli** che corriamo durante la navigazione in rete.

Quali sono i pericoli del web?



- Il **furto** dei tuoi **dati**
- Il **furto** della tua **identità**
- **Phishing**
- Le **app** sanno sempre dove sei con la «**posizione**» **attiva**
- **Diffusione** dei tuoi **contenuti personali** **senza** il tuo **permesso**
- Essere vittima di una **truffa**
- Fare il **download** di programmi malevoli senza volere (malware, virus, spyware e ransomware)

Cos'è la cybersecurity?

La **Cybersecurity** è la capacità di proteggere e difendere il cyber spazio dai cyber attacchi

- Comportamenti
- Strumenti



Come puoi navigare in Internet in sicurezza

1

Non credere a tutto ciò che leggi su Internet. **Verifica sempre che la fonte sia affidabile**

2

Non installare app su tablet o smartphone **provenienti da store non ufficiali**

3

Non dare mai il tuo numero di telefono a sconosciuti, **né informazioni personali** come indirizzo, età, foto

4

Prima di pubblicare qualcosa in internet, pensaci: non postare nulle che consideri personale o riservato e di cui potresti pentirti in futuro

5

Sui Social Media **aggiungi solo persone che conosci realmente e controlla le impostazioni del tuo profilo**

6

Non caricare online foto di persone, senza prima aver chiesto il loro consenso (principio del consenso)

7

Attento ai falsi e fai attenzione a ciò su cui fai clic: messaggi allarmistici, richieste d'aiuto, offerte, richieste di dati, segnalazioni di virus spesso sono dei trucchi, sii diffidente. Quando clicchi su un banner potresti essere indirizzato su un sito fake che potrebbe tentare di truffarti tramite il phishing.

La Password è come la chiave di casa

- La **password** rappresenta la **chiave di accesso** ai nostri luoghi digitali.
- Scegliere **password sicure** e custodirle in modo efficiente **è il primo passo per proteggersi** dai rischi della rete e dagli attacchi informatici.



PASSWORD EFFICACE

COMPLESSA (numeri, lettere maiuscole e minuscole, simboli)

LUNGA (più di 8 caratteri)

DIVERSA per ogni account

AGGIORNATA (cambiare spesso)

SEGRETA (non comunicare a nessuno!)

Malware e antivirus

Il **malware** è un software che viene installato su un computer senza l'approvazione del proprietario. Si tratta di **programmi cattivi** possono **rubare password, eliminare file, raccogliere informazioni personali o persino impedire il funzionamento di un computer.**



PROTEGGITI CON L'ANTIVIRUS!

Il **software antivirus**, se installato correttamente su un sistema informatico, **può impedire l'accesso ai sistemi informatici da parte di altri programmi indesiderati.** Se non è installato alcun software antivirus, **gli hacker potrebbero essere in grado di accedere alle informazioni** presenti nel computer.

Definizioni

Worms

Letteralmente "verme", è una famiglia di malware che sfrutta le macchine infettate per replicarsi e diffondersi su altri PC (nella stragrande maggioranza dei casi, il worm si "auto-invia" sfruttando la posta elettronica). Il worm, solitamente, non viaggia mai solo: funge infatti da "apripista" per altri malware, come keylogger, backdoor o spyware.

Spyware

Il nome è piuttosto evocativo: lo spyware nasce infatti dall'unione dei termini inglesi spy (spiare) e ware (per software). Si tratta di un malware che infetta PC, smartphone e sistemi informatici con l'obiettivo di spiare l'utente, trafugare informazioni presenti nella memoria del dispositivo e inviarle un server remoti gestiti dagli stessi hacker - oppure organizzazioni criminali - che hanno creato il malware.

Ransomware

Tra le famiglie malware più pericolose, è anche una delle ultime ad aver fatto la sua comparsa. I ransomware, o software del riscatto, sfruttano una combinazione di Social Engineering e phishing per infettare un computer e infiltrarsi in una rete informatica. Una volta che il virus è all'interno del PC o dello smartphone, l'utente può ben poco: il ransomware crittografa immediatamente tutti i dati presenti nella memoria e riavvia il dispositivo. Alla riaccensione, l'utente visualizza un messaggio di riscatto ("ransom" in inglese) da pagare solitamente in bitcoin.

Virus

I virus sono una delle famiglie malware più importanti e conosciuti. Si tratta di programmi che infettano un PC o un sistema informatico per tentare di distruggerne i dati, corromperne i file di sistema o alterarne le prestazioni. A differenza di altri malware, i virus sono in grado di autoreplicarsi e diffondersi in altri computer o smartphone sfruttando la connessione a Internet o altri sistemi di comunicazione.

Cavallo di Troia

Come Ulisse entrò a Troia sfruttando un cavallo di legno, gli hacker sono soliti crearsi delle "aperture" nei sistemi di difesa di PC, smartphone e altri sistemi informatici utilizzando i trojan horse (letteralmente "cavallo di Troia"). Si tratta di software che, una volta all'interno del dispositivo, crea un accesso remoto che un cybercriminale può utilizzare sia per trafugare dati, sia per accedere al device e prenderne possesso a distanza.

Adware

A differenza di moltissime altre famiglie di malware, quella degli adware è probabilmente tra le meno pericolose. Si tratta di programmi malevoli che infettano il PC o lo smartphone per mostrare video pubblicitari e banner. Lo scopo, in questo caso, non è quello di rubare dati o distruggerli, ma semplicemente di guadagnare sulla visualizzazione di pubblicità da parte degli utenti.