I PERICOLI DI INTERNET

Flavio Casertano 4D/SC.

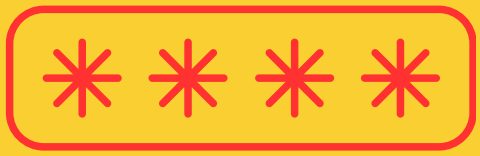
I VIRUS

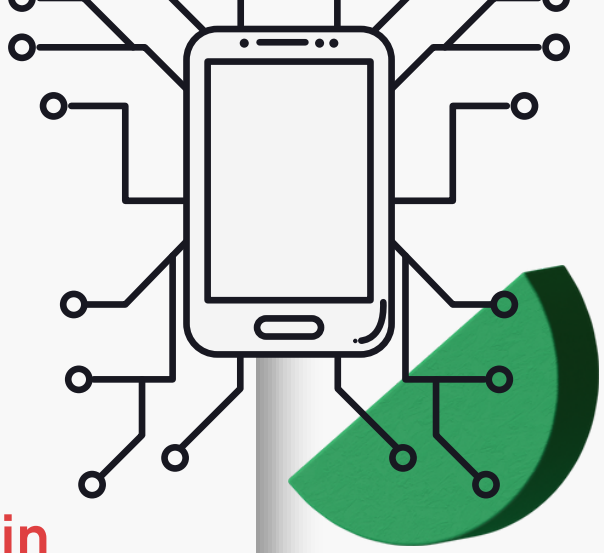
Ecco i tipi di virus più diffusi al giorno d'oggi

- MALWARE
- WORM
- ADWARE
- SPYWARE
- RANSOMWARE
- BOT
- ROOTKIT
- TROJAN
- BUG

Falsi miti sui virus

-Se il computer dà un messaggio di errore, è presente un virus? NO, potrebbe anche avere problemi con software sani e/o con file puliti. -Allegati mail da mittenti sicuri sono affidabili al 100%? NO, il file potrebbe essere corrotto e/o infetto anche se inviato da un mittente sicuro. -Gli antivirus eliminano sempre il 100% delle minacce? NO, anche il migliore antivirus non garantisce il 100% della sicurezza. -I virus causano danni hardware? NO, a meno che il PC non sia talmente carico e/o sforzato da fondere il processore o la RAM a causa della troppo elevata temperatura.





Qual è il browser migliore per navigare in sicurezza?

Il browser migliore per navigare in modo sicuro è Firefox. Questo perché Firefox ha la possibilità di applicare delle estensioni Ad-Blocker, ovvero delle estensioni del browser in grado di bloccare gli annunci dannosi, i quali rappresentano la maggiore fonte di virus nel web. Per citare un'estensione valida, che non gravi troppo sulla velocità della CPU, possiamo chiamare in causa "uBlock Origin". Anche altri browser possiedono questa tecnologia, ma molte volte è inaffidabile, oppure contiene essa stessa un virus.

Quali sono le maggiori fonti di virus?

ANNUNCI SU SITI NON SICURI

Insieme ai giochi, i programmi e la musica piratata (si ricorda che scaricare contenuti a pagamenti in modo gratuito è illegale) che potrebbero contenere file infetti.

E-MAIL

Molte e-mail contengono link falsi che portano a pagine o siti tramite i quali i pirati informatici possono carpire i nostri dati. Quest'ultimo metodo è chiamato 'Phishing'.

COME AVVIENE UN ATTACCO DI PHISHING?

Con un attacco di phishing gli hacker tentano di indurre la vittima a condividere informazioni sensibili. Il loro obiettivo è sottrarre login, numeri di carte di credito e informazioni aziendali sensibili. Potrebbero anche cercare di infettare il computer della vittima con dei malware.

Come difendersi dai virus?

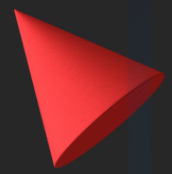
Esistono molti rimedi contro i virus, primo fra cui l'uso di un antivirus funzionante e valido, che sappia riconoscere i file dannosi per il PC.

Il miglior antivirus è Malwarebytes, che fornisce un servizio di scansione completo del computer e elimina, o mette in quarantena i file infetti.

Inoltre è raccomandabile scansionare i file prima di scaricarli da internet. Un sito che permette di fare questo è VirusTotal, che analizza i file in questione con circa 70 antivirus differenti. Se la maggior parte di questi classifica il programma o documento come virus, non è raccomandabile lo scaricamento. Per quanto riguarda i programmi già presenti sul PC, è consigliabile l'uso di ProcessExplorer, che fornisce un sistema di monitoraggio di tutti i processi in atto nel PC.

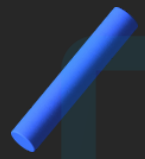
TRUFFE

Un altro pericolo del web è rappresentato dalle truffe online, che hanno visto un rapido incremento a causa della pandemia. Qui sono riportati gli esempi più comuni di truffe online:



FALSI ANNUNCI PUBBLICITARI

FRODI NEGLI ACQUISTI TRAMITE PREZZI VANTAGGIOSI



MESSAGGI DA MITTENTI NON IDENTIFICFATI

EMAIL PUBBLICITARIE DI SPAM O PHISHING

Come difendersi da una potenziale truffa?

Difendersi dalle truffe online non è semplice, alcuni segnali però, ci possono aiutare:

- Prezzi di vendita nettamente inferiori rispetto all'effettivo prezzo di mercato;
- Durante l'acquisto il venditore richiede oppure rivela molti dati personali;
- Utilizzo di mezzi di pagamento non tracciabili;
- Errori di ortografia nelle email.


FURTO DI DATI

Come prevenire o accorgersi di un furto di dati?

Il furto di dati è una problematica meno diffusa rispetto ai virus o alle truffe, ma rappresenta ugualmente un pericolo preoccupante da cui difendersi.

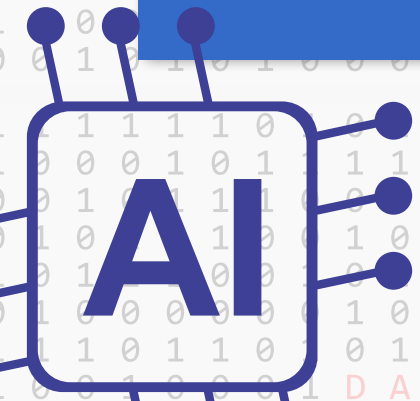
Navigare su siti protetti dal criptaggio dati; possiamo definire un sito affidabile quando accanto al link del sito stesso ritroviamo l'immagine di un lucchetto , ma ciò non vale quando accanto al link viene indicato "non sicuro".

Per le password le uniche due pratiche che la rendono sicura sono:

- la creazione di password contenenti lettere, numeri e simboli;
- l'abilitazione deella verifica a due fattori 2FA.

Altri segni che possono aiutarci sono:

- l'accesso risulta impossibile anche con credenziali corrette;
- le impostazioni sulla privacy o condivisione di dati risultano alterate;
- ci viene richiesto di accedere nonostante l'opzione di accesso rapido sia attiva.



Conclusioni

Abbiamo:

- analizzato i principali pericoli del web e come difenderci da essi. dedotto che per essere cittadini digitali si deve avere
- una guida e dei diritti che vanno conosciuti.

Quindi, una persona che si approccia ad internet va educata e avvertita sui pericoli.

Avete delle domande?