DRIZZA LE ANTENNE

Progetto realizzato in collaborazione con la Direzione di CBCM di Intesa Sanpaolo.

MdR
MUSEO DEL RISPARMIO

MdR
MUSEO DEL RISPARMIO

Come navigare su Internet in sicurezza?

- Non credere a tutto ciò che leggi su Internet, ma verifica sempre che la fonte sia affidabile.
- Chiedi il permesso ai tuoi genitori prima di registrarti su un sito.
- Non installare su tablet o smartphone app provenienti da store non ufficiali.
- Sui Social Media (es. Facebook), aggiungi solo persone che conosci realmente.
- Non caricare online foto di persone, senza prima aver chiesto il loro consenso (principio del consenso).
- Attenzione a fare clic! Quando clicchi su un banner, potresti essere indirizzato su un sito fake che potrebbe tentare di truffarti tramite il phishing.

MdR
MUSEO DEL RISPARMIO

La password

- Una password è un modo per accedere «da qualche parte», e può essere utilizzata come mezzo per identificare una persona. Poiché la password è l'unico modo per identificare una persona, deve essere mantenuta segreta.

- Le password sono composte da caratteri, lettere e numeri. È consigliabile cambiare la propria password una volta all'anno, o anche più spesso, per prevenire i fenomeni di hacking.

- Ecco qualche suggerimento utile:
  1. Una persona potrebbe essere in grado di indovinare una password se è troppo facile: crea password complesse utilizzando una combinazione di lettere, numeri e caratteri speciali. Usa almeno 8 caratteri (14 è l'ideale).
  2. Non utilizzare la stessa password per più account.
  3. Non utilizzare il tuo nome in una password .
  4. Non condividere le password con nessuno oltre alla famiglia .

MdR
MUSEO DEL RISPARMIO

Mondo virtuale e mondo reale

Regole generali

- Pensa sempre a chi c'è dietro lo schermo.
- Mantieni segrete le informazioni personali.
- Non chattare o inviare foto a sconosciuti.
- Mantieni al sicuro gli account dei social media.

Cosa condividere nei profili social

- Nome, nickname o pseudonimo.
- Hobby e interessi ma senza troppi dettagli.
- Foto da cui non è possibile ricavare dettagli (es. foto della scuola, delle uniformi di società sportive, ecc.).
- «Mi piace» su film, libri o cibi.

Cosa non condividere nei profili social

- Nome e cognome.
- Nominativi di amici e familiari.
- Data di nascita.
- Nome della scuola.
- Foto da cui è possibile ricavare dettagli e informazioni personali.
- Indirizzo di casa e numero di telefono.

MdR
MUSEO DEL RISPARMIO

Malware e antivirus

- Quando si uniscono le parole «malicious» (che in inglese significa "dannoso") e «software» si ottiene la parola «malware». Il malware è un tipo di software che i malintenzionati sono in grado di installare su un computer senza il consenso del proprietario.

- Esistono diversi tipi di malware che possono danneggiare i computer: i più famosi sono forse i virus informatici, ma ce ne sono anche molti altri. Tutti questi programmi cattivi possono rubare password, eliminare file, raccogliere informazioni personali o persino impedire il funzionamento di un computer.

- Se è installato correttamente su un sistema informatico, il software antivirus può bloccare i programmi indesiderati.

- Se non è installato alcun software antivirus, gli hacker potrebbero essere in grado di accedere alle informazioni presenti nel computer.

- Installare più di un antivirus non è una buona idea. I diversi software antivirus installati insieme possono interferire tra loro.

MdR
MUSEO DEL RISPARMIO

Definizioni di alcuni malware

Virus
I virus sono tra i malware più importanti e conosciuti. Si tratta di programmi che infettano un computer o un sistema informatico per tentare di distruggerne i dati, danneggiarne i file o modificarne le prestazioni. A differenza di altri malware, i virus sono in grado di auto-replicarsi e di diffondersi in altri computer, tablet o smartphone sfruttando la connessione Internet o anche altri sistemi di comunicazione.

Spyware
Il nome nasce dall'unione delle parole inglesi «spy» ("spiare") e «ware» (diminutivo di software). Si tratta di un malware che infetta computer, tablet, smartphone e sistemi informatici con l'obiettivo di spiare chi li usa, rubando le informazioni presenti nella memoria di questi dispositivi per inviarle ad altri dispositivi gestiti dagli hacker che hanno creato lo spyware.

Ransomware
Tra i malware più pericolosi e recenti, i ransomware (tradotto: software del riscatto) sfruttano il phishing per infettare un dispositivo e infiltrarsi in una rete informatica. Una volta che sono entrati all'interno del computer, del tablet o dello smartphone, il proprietario può fare ben poco: i ransomware nascondono immediatamente tutti i dati presenti nella memoria e riavviano il dispositivo. Alla riaccensione, il proprietario visualizza un messaggio di riscatto ("ransom" in inglese) che gli chiede di pagare una somma per poter accedere di nuovo ai suoi file.

MdR
MUSEO DEL RISPARMIO

Definizioni di alcuni malware

Worm
Il worm (parola inglese che significa "verme") è un malware che sfrutta i dispositivi infettati per replicarsi e diffondersi su altri dispositivi; nella stragrande maggioranza dei casi, lo fa auto-inviandosi tramite posta elettronica. Il worm, solitamente, non viaggia da solo, ma apre la strada ad altri malware, per esempio gli spyware.

Cavallo di Troia
Come Ulisse entrò a Troia sfruttando un cavallo di legno, così gli hacker spesso superano i sistemi di difesa di computer, tablet, smartphone e sistemi informatici proprio utilizzando un «Trojan horse» (tradotto dall'inglese: "cavallo di Troia"). Si tratta di un software che, una volta entrato, crea un accesso remoto usato dai criminali sia per rubare dati, sia per controllare a distanza il dispositivo.

Adware
Probabilmente, gli adware sono tra i malware meno pericolosi, perché si tratta di programmi malevoli che entrano in computer, tablet e smartphone solo per mostrare video pubblicitari e banner. Lo scopo, in questo caso, non è rubare dati o distruggerli, ma semplicemente guadagnare sulla visualizzazione di pubblicità da parte dei proprietari dei dispositivi infettati.

MdR
MUSEO DEL RISPARMIO

Consigli per i genitori

- Non lasciate che i vostri figli piccoli navighino senza supervisione! Impostate i dispositivi domestici in modo che i bambini dimentichino la password della rete Wi-Fi e, così, non possano andare online senza di voi. Allo stesso tempo, controllateli nel download delle app, nell'attività sui social media, ecc.

- Parlate ai vostri figli della sicurezza online! È importante che i bambini comprendano le implicazioni di ciò che pubblicano (ciò che viene messo online rimane online...), i rischi connessi alla condivisione di informazioni personali, il cyberbullismo, l'esistenza di «cattivi» e il modo in cui si nascondono su Internet (il principio del «non parlare con gli sconosciuti» vale anche virtualmente), ecc.

- Utilizzate motori di ricerca adatti ai bambini.

- Controllate le impostazioni sulla privacy nei dispositivi utilizzati dai vostri figli.

- Impostate il web browser per bloccare i popup e disabilitare Java.