

IT Security

Password Sicure

- Utilizzare una combinazione di almeno otto caratteri con lettere maiuscole, minuscole, numeri e caratteri speciali.
- Evitare l'uso di informazioni personali come nomi, date di nascita o numeri di telefono.
- Assegnare una password unica per ogni account.
- Utilizzare un gestore di password per memorizzare in modo sicuro e generare password complesse.
- Abilitare l'autenticazione multifattore (MFA) quando possibile.

Metodi di Furto di Identità

- Phishing: invio di e-mail o messaggi falsi per ottenere informazioni personali.
- Social Engineering: manipolazione psicologica per ottenere accesso a informazioni riservate.
- Raccolta di informazioni da fonti pubbliche o violando la sicurezza dei dati.
- Furto di documenti fisici come carte d'identità o carte di credito.
- Skimming: installazione di dispositivi illegali per raccogliere informazioni di carte di credito o debito.

Tipologie di Malware

- Virus: programmi progettati per replicarsi e danneggiare i file di sistema.
- Trojan Horse (Trojan): programmi che sembrano legittimi ma eseguono operazioni dannose.
- Spyware: software che raccoglie informazioni sulle attività degli utenti senza il loro consenso.
- Ransomware: blocca l'accesso al sistema o ai dati e richiede un pagamento per ripristinarli.
- Adware: software che mostra annunci indesiderati o pop-up sui dispositivi degli utenti.

Cyberbullismo

- Messaggi Offensivi: Invio di messaggi minacciosi o molesti.
- Diffamazione Online: Spargere false informazioni o pettegolezzi.
- Esclusione Digitale: Escludere intenzionalmente qualcuno da gruppi online.
- Furto di Identità: Usare l'identità di qualcuno per danneggiarne la reputazione.
- Diffusione di Immagini/Videos: Condividere immagini o video imbarazzanti senza consenso.

Sicurezza nei Social Network

- Evita di pubblicare foto o video di bambini.
- Sii consapevole che i social network possono vendere i tuoi dati personali.
- Proteggi la tua privacy evitando di condividere informazioni sensibili.
- Presta attenzione al rischio di furto di identità e alle truffe online.
- Usa le impostazioni di privacy per controllare chi può vedere le tue informazioni.

Tecniche di Protezione

- Utilizzare software antivirus e antimalware aggiornati per rilevare e rimuovere minacce.
- Mantenere il sistema operativo e le applicazioni aggiornati per proteggere da vulnerabilità note.
- Implementare autenticazione a più fattori per un accesso più sicuro agli account.
- Educazione e consapevolezza degli utenti per riconoscere e evitare tecniche di phishing e altre truffe online.
- Backup regolari dei dati critici per garantire la disponibilità in caso di attacco ransomware o perdita di dati.
- Utilizza **AdBlock** o altre estensioni di Google Chrome per bloccare le pubblicità moleste.