Sicurezza informatica online

Minaccia informatica: I tuoi dati personali sono in pericolo

Un problema comune quando sei online è una "violazione dei dati". Immagina che le tue informazioni private vengano divulgate. È simile a ciò che accade online durante una violazione dei dati.

Una violazione dei dati si verifica quando informazioni sensibili o personali vengono consultate, esposte o rubate senza autorizzazione.

Negli acquisti online, possono includere nomi, indirizzi, dati di pagamento o ciò che hai acquistato.

I criminali informatici vogliono queste informazioni.

Le violazioni dei dati possono portare al furto d'identità e causare problemi ai negozi online. È un problema serio per tutti.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minacce online

Le minacce online sono potenziali pericoli che possono compromettere la sicurezza dei nostri dispositivi e dei nostri dati quando siamo online. Alcune minacce online comuni includono:

Spyware

Phishing

Spoofing

Malware

Ransomware

… e altro ancora.

Possono portare ad accessi non autorizzati, furto di dati e danni ai sistemi.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica: Spyware - Il ladro silenzioso

Una minaccia a cui prestare attenzione è lo "spyware". È subdolo e si nasconde nei tuoi dispositivi.

Lo spyware è un tipo di malware che monitora segretamente le attività su un dispositivo.

Può raccogliere informazioni come la cronologia di navigazione, le password e i dati finanziari.

Alcuni tipi possono anche registrare ciò che digiti sulla tastiera, acquisire lo schermo o accedere ad altre funzioni del dispositivo.

I criminali informatici utilizzano queste informazioni per rubare denaro o identità.

Lo spyware è un pericolo silenzioso. Proteggiti facendo attenzione ai download e utilizzando software di sicurezza affidabili.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica:
Phishing - Messaggi falsi e ingannevoli

Il phishing è un attacco informatico in cui i criminali informatici fingono di essere una persona o un'organizzazione affidabile per rubare le tue informazioni personali.



Come ti attirano nella trappola:

Email di phishing: queste email spesso creano un senso di urgenza e utilizzano loghi e nomi familiari per spingerti a cliccare su link o a rivelare informazioni personali.

Smishing e Vishing: truffe simili avvengono tramite messaggi di testo (smishing) e telefonate (vishing). Utilizzano urgenza o tattiche intimidatorie per ingannarti.

Siti web falsi: i criminali informatici creano siti web che sembrano reali e rubano le tue informazioni di accesso quando provi ad accedere.

© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica:
Phishing - Messaggi falsi e ingannevoli

Segnali d'allarme a cui fare attenzione:

Urgenza: messaggi che ti spingono ad agire immediatamente.

Richieste inaspettate: richieste di password, pagamenti o informazioni personali.

Mittente sospetto: l'indirizzo email o il numero di telefono non corrisponde a chi il mittente afferma di essere.

Link o allegati sospetti: link inaspettati, URL abbreviati o file.

Linguaggio insolito: una grammatica scorretta o errori di ortografia possono ancora essere un segnale d'allarme, anche se i moderni messaggi di phishing possono sembrare molto professionali.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica: Spoofing - Camuffamenti online

Lo "spoofing" si verifica quando gli aggressori camuffano le informazioni in modo che sembrino provenire da una fonte affidabile.

Lo spoofing è una tecnica di inganno informatico utilizzata per ingannare persone o sistemi. È come indossare un travestimento per sembrare qualcuno di familiare. Gli aggressori possono falsificare:

Indirizzi email: le email possono sembrare provenire dalla tua banca o da un'azienda conosciuta, invitandoti a cliccare su un link o a scaricare un allegato contenente malware.

Numeri di telefono: potresti ricevere chiamate che sembrano provenire dalla società della tua carta di credito o dall'assistenza tecnica, nel tentativo di rubare i tuoi dati personali.

Indirizzi IP: gli aggressori possono manipolare le informazioni IP per far sembrare che provengano da una posizione affidabile.

Fai attenzione! Non fidarti delle informazioni online solo perché sembrano familiari. Verifica sempre le richieste importanti attraverso i canali ufficiali.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica:
Spoofing - Camuffamenti online

Proteggersi dallo spoofing:

Controlla attentamente le informazioni del mittente: non fidarti degli indirizzi email o dei numeri di telefono solo in base a ciò che vedi. Verificali attraverso i canali ufficiali.

Fai attenzione alle richieste urgenti: le aziende legittime raramente ti spingono ad agire immediatamente. Fai attenzione alle email o alle chiamate che richiedono un'azione rapida.

Verifica i link prima di cliccare: non cliccare sui link presenti nelle email o nei messaggi. Digita manualmente nel browser l'indirizzo del sito web legittimo.

Verifica le richieste importanti: se un messaggio o una chiamata richiede denaro, password o informazioni sensibili, contatta l'organizzazione utilizzando un numero ufficiale conosciuto o il suo sito web.

Password sicure e MFA: utilizza password uniche e attiva l'autenticazione a più fattori (MFA) per aumentare la sicurezza dei tuoi account.

Restando vigile e seguendo questi passaggi, puoi rendere più difficile per chi utilizza lo spoofing riuscire a ingannarti.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica:
Malware - I pericoli dei software dannosi

Malware significa "software dannoso".

Il malware è un software progettato per danneggiare i sistemi, rubare dati, interrompere le operazioni o ottenere accessi non autorizzati. I criminali informatici utilizzano il malware per raggiungere diversi obiettivi dannosi:

Rubare informazioni: il malware può rubare dati sensibili come password, numeri di carte di credito o file personali.

Interrompere le operazioni: il malware può bloccare il sistema, danneggiare i file o impedirti di accedere al computer.

Diffondersi ulteriormente: il malware può replicarsi e infettare altri dispositivi presenti sulla tua rete.

Prendere il controllo: nei casi più estremi, il malware può dare agli aggressori accesso remoto al tuo computer, permettendo loro di controllarlo.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica:
Malware - I pericoli dei software dannosi



Proteggersi dal malware:

Software antivirus e anti-malware: installa e mantieni aggiornati software antivirus e anti-malware affidabili che possano rilevare e rimuovere le minacce malware.

Fai attenzione ai download: scarica software solo da fonti affidabili. Evita di cliccare su link sospetti o di aprire allegati provenienti da mittenti sconosciuti.

Mantieni aggiornato il software: i software non aggiornati possono avere vulnerabilità di sicurezza. Aggiorna regolarmente il sistema operativo, il browser web e le altre applicazioni.

Password, passkey e MFA: utilizza password uniche con un password manager, attiva l'MFA e utilizza le passkey dove disponibili.

Fai attenzione alle offerte gratuite: se qualcosa online sembra troppo bello per essere vero, probabilmente lo è. Evita di cliccare su annunci pop-up o di scaricare software gratuito da fonti non affidabili.

© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica:
Ransomware - Dati tenuti in ostaggio

Il "ransomware" è un tipo di malware particolarmente pericoloso. Blocca i tuoi file e richiede denaro per sbloccarli.

Il ransomware cripta i tuoi file, rendendoli inutilizzabili.

I criminali informatici richiedono il pagamento di un "riscatto", spesso in criptovaluta.

Senza un backup funzionante o un metodo di recupero, potresti perdere l'accesso ai tuoi dati.

Gli attacchi ransomware possono compromettere seriamente la logistica e gli acquisti online.

Non pagare il riscatto. Perché? (Discussione)



Il ransomware può essere devastante. Esegui regolarmente il backup dei tuoi dati. Il pagamento non garantisce il recupero, sostiene le attività criminali e in alcuni casi può creare problemi legali. Segnala gli attacchi alle autorità.

© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Minaccia informatica:
Ransomware - Dati tenuti in ostaggio

Proteggersi dal ransomware:

Backup regolari: conserva backup recenti dei file importanti, includendo almeno una copia a cui il ransomware non possa accedere facilmente o che non possa modificare.

Aggiornamenti software: mantieni aggiornati il sistema operativo, le applicazioni e i software di sicurezza per correggere le vulnerabilità sfruttate dagli aggressori.

Fai attenzione ad allegati e link: presta attenzione agli allegati e ai link nelle email, soprattutto se provengono da mittenti sconosciuti. Non cliccare su link sospetti e non scaricare file non richiesti.

Software anti-malware: utilizza un programma anti-malware affidabile in grado di rilevare e potenzialmente bloccare gli attacchi ransomware.

Non pagare il riscatto: pagare non garantisce il recupero e può incoraggiare ulteriori attacchi. Segnala l'incidente e chiedi assistenza a professionisti o alle forze dell'ordine.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Altre minacce online
E altre a cui prestare attenzione

Oltre a queste minacce principali, ci sono molti altri pericoli online di cui essere consapevoli quando si fanno acquisti online.

…e altro ancora: il mondo delle minacce informatiche è in continua evoluzione.

Continuano ad apparire nuovi tipi di malware e di attacchi.

Anche il furto degli account e delle credenziali di accesso sono rischi comuni.

Essere vigili e prudenti è fondamentale per la sicurezza online.

Ricorda sempre che le minacce online si evolvono. Rimani aggiornato sulle notizie di sicurezza informatica e sulle migliori pratiche per proteggerti.

Tieniti aggiornato visitando regolarmente siti come StaySafeOnline.org e GetSafeOnline.org.



© Global Digital Web di Roberto Bianchi - globaldigitalweb.com

Sicurezza informatica online

Altri modi per restare al sicuro online

Oltre agli strumenti di cui abbiamo parlato, ci sono anche altre misure di sicurezza! È come avere molte serrature sulla porta, non una sola.

La crittografia protegge i tuoi dati rendendoli illeggibili senza la chiave corretta.

Utilizza la 2FA o l'MFA ogni volta che è possibile.

Utilizza password lunghe e uniche, un password manager oppure le passkey dove disponibili.

La formazione sulla sicurezza informatica ti aiuta a riconoscere le minacce.

Gli aggiornamenti e i controlli regolari aiutano a mantenere i sistemi più sicuri.



Utilizzare insieme diversi metodi di sicurezza è il modo migliore per restare al sicuro online. È come un lavoro di squadra!

© Global Digital Web di Roberto Bianchi - globaldigitalweb.com