DELL Technologies

Riepilogo sulla sicurezza informatica

In questo mondo sempre più virtuale, è naturale che il crimine informatico aumenti a ritmi allarmanti. In effetti, **il crimine informatico ha generato all'incirca $ 6 bilioni di entrate nel 2021**, cifra che l'ha reso la terza economia nel mondo, alle spalle solo degli Stati Uniti e della Cina.[1] I malintenzionati aumentano ogni giorno il loro livello di astuzia e sofisticazione, ma è semplice proteggersi online se si conoscono le minacce più recenti e si adottano le misure di protezione necessarie. **Ecco alcune delle minacce che gli esperti di sicurezza informatica Dell si impegnano a prevenire e alcuni suggerimenti per la protezione del tuo ambiente professionale o domestico.**

Compromesso rapido

I malintenzionati ottengono l'accesso al tuo sistema quando incappi in un sito web non protetto o compromesso.

Come accorgersene:

Riscontro sul sistema di nuovi file o connessioni di rete che non hai aggiunto tu

Richieste indesiderate di informazioni sulla configurazione

Hardware non sicuro

I malintenzionati immettono le vulnerabilità direttamente nell'hardware e negli accessori.

Come accorgersene:

Offerte troppo convenienti per essere veri

Social engineering

I truffatori manipolano le persone spacciandosi per un ente giuridico o altre autorità per rubare loro **informazioni personali** o **finanziarie** sensibili ("phishing"). L'invio del codice malevolo avviene tramite link o allegati a e-mail, messaggi diretti e SMS.

Come accorgersene:

E-mail o SMS indesiderati in cui si chiedono informazioni personali con la richiesta di aprire link e allegati

Anomalie nell'indirizzo e-mail del mittente, nel testo o nell'ortografia

Attacco malware tramite USB

I criminali utilizzano dispositivi di storage rimovibili, come unità USB, dischi rigidi portatili, smartphone, lettori musicali, schede SD e supporti ottici (CD, DVD, BluRay), per infettare un computer o una rete.

Come accorgersene:

Accesso imprevisto ai file o creazione di nuovi file sul dispositivo

Rapporto di fiducia

Un hacker viola una terza parte affidabile, come uno studio medico, e ne utilizza la reputazione per sfruttare i pazienti.

Come accorgersene:

Comportamento di accesso insolito

Come salvaguardare la sicurezza informatica:

COSA FARE

Utilizza l'autenticazione a più fattori e password complesse e univoche per i vari account.

Tutti i dispositivi connessi a Internet sono esposti agli attacchi.
Tieni aggiornati i software.

Tieni alti l'attenzione e lo scetticismo. Impara a riconoscere le tattiche dei truffatori.

Fatti sentire. Segnala gli attacchi al dipartimento IT e informa colleghi, familiari e amici.

COSA NON FARE

Evita la pigrizia. Attieniti sempre a tutti i protocolli di sicurezza.

Non cliccare su link contenuti in e-mail o messaggi diretti indesiderati.

Non ignorare gli avvisi del browser, ad esempio "La connessione non è sicura" o "La connessione non è privata".

SUGGERIMENTO:
Per maggiori informazioni, visita il sito:
Dell.com/Endpoint-Security

DELL Technologies

[1]Cybersecurity Ventures: 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics