ELI NET

04.Cyber Security

6 SUGGERIMENTI PRATICI PER CONTRASTARE IL CYBER CRIME ADOTTANDO COMORTAMENTI CONSAPEVOLI

ATTENZIONE AL PHISHING
Banche, assicurazioni, P.A. non vi chiederanno mai informazioni personali via e-mail.
Attenzione, se qualcuno vi chiede tali informazioni potrebbe trattasi di un tentativo di phishing.

ATTENZIONE AI LINK E AGLI ALLEGATI
In una e-mail dall'aspetto sospetto vi viene chiesto di fare clic su un link o di scaricare un allegato?
Attenzione, potreste scaricare inavvertitamente un malware o dare accesso alle vostre informazioni sensibili.

DIFFIDARE DELLE RETI NON PROTETTE
Se riuscite ad accedere ad una rete wi-fi aperta, anche un cyber criminale può farlo.
Fate attenzione alle reti non protette, se le utilizzate potreste consentire ad un malintenzionato di accedere ai vostri dati.

AGGIORNATE GLI ANTIVIRUS
La scelta migliore per proteggersi è avere una difesa forte.
Mantenete il vostro software antivirus sempre aggiornato, sia su desktop che sugli apparati mobile.

AGGIORNATE SOFTWARE & APP
Gli hacker sono costantemente alla ricerca di una via d'accesso... e spesso la trovano. **Chiudete tutti gli accessi mantenendo sempre aggiornati i software e le app** alle versioni più recenti.

UTILIZZATE PASSWORD COMPLESSE
"123456" potrebbe essere una password semplice da ricordare, ma decifrabile in pochi secondi.
Utilizzate password articolate e uniche, non riciclatele e non utilizzatele su più account e app.

4 BEST PRACTICE PER UN USO PIU CONSAPEVOLE DEI TUOI ACCOUNT SOCIAL

SEPARA I CONTESTI!
Quando usi i social, mantieni separata la sfera personale da quella professionale.
Ogni volta che condividi contenuti, rendi pubblica una parte interpretabile della tua identità. **Uno dei rischi più seri è quello di vedere compromessa la tua immagine e la tua reputazione**, lasciando tracce nel tempo che potrebbero comportare danni per te e per la tua organizzazione.

IMPOSTA LA PRIVACY
Scegli con cura quali informazioni rendere pubbliche o private quando imposti la privacy dei tuoi post sui social.
I criminali utilzzano "l'ingegneria sociale", un attacco su base psicologica, per ottenere informazioni utili alla loro "attività". Limitando l'esposizione dei contenuti pubblici, limiterai la possibilità di cadere vittima degli attacchi.

PROTEGGI LA MAIL!
Non utilizzare mai l'indirizzo e-mail aziendale per registrarti a social-media con finalità di carattere personale, potresti compromettere il livello di sicurezza dei tuoi sistemi o di quelli della tua organizzazione, aumentando la probabilità di diventare inconsapevoli vittime del cyber crime.

ATTENZIONE A QUEL CHE CONDIVIDI!
Stai attento ai contenuti che vuoi diffondere, un selfie scattato a lavoro e postato con leggerezza potrebbe contenere informazioni confidenziali e vanificare le politiche aziendali di prevenzione rispetto ad una possibile perdita di dati. **Agendo in modo ragionato e consapevole, eviterai la perdita di dati e informazioni riservate a vantaggio di criminali o concorrenti**.

via Alfieri 2, 30038 Spinea (VE) info@elinet.it (+39) 041 5084911 www.elinet.it