CYBERSECURITY AWARENESS MONTH

RICONOSCI TE STESSO NELLA CYBERSICUREZZA (SEE YOURSELF IN CYBER)

Tutti fanno la loro parte nella cybersicurezza...a prescindere dal ruolo che ricoprono.

Fai la tua parte per mantenere te stesso e la nostra Azienda al sicuro compiendo quattro azioni chiave.

ABILITA L'AUTENTICAZIONE MULTI-FATTORE

Nota anche come autenticazione a due fattori e verifica in due passaggi, l'autenticazione multi-fattore è una misura di sicurezza che richiede a tutti coloro che accedono a un account di eseguire una procedura a due passaggi per comprovare la loro identità. Questo raddoppia le difficoltà per chi cerca di violare l'accesso a un account online. Aggiungendo un unico semplice passaggio al momento dell'accesso a un account, l'autenticazione multi-fattore ne aumenta notevolmente la sicurezza.

USO DI PASSWORD FORTI

Le password sono importanti se desideri mantenere le informazioni al sicuro. Ecco alcuni semplici modi per mantenere al sicuro i tuoi account attraverso migliori pratiche relative alle password. A prescindere dall'account, tutte le password devono essere create tenendo in mente queste tre parole

- Lunghezza – Almeno 12 caratteri.
- Unicità – Ogni account ha bisogno della sua password esclusiva.
- Complessità – Usa una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali. Alcuni siti Web permettono perfino di includere gli spazi.

SOFTWARE AGGIORNATI

Esegui sempre gli aggiornamenti dei software, quando disponibili, e non li rimandare mai. Questi aggiornamenti risolvono problemi generali del software e offrono nuovi patch di sicurezza in cui i criminali informatici potrebbero entrare. Quando si scarica un aggiornamento del software, è necessario riceverlo unicamente dall'azienda che lo ha creato. Non usare mai versioni hackerate, piratate o prive di licenza del software perché spesso contengono malware e causano più problemi di quanti ne risolvano.

RICONOSCIMENTO E SEGNALAZIONE DEL PHISHING

I segnali possono essere impercettibili, ma dopo aver riconosciuto un tentativo di phishing, puoi evitare di cascarci. Ecco alcuni suggerimenti rapidi su come individuare chiaramente un'e-mail di phishing falsa: contiene un'offerta troppo vantaggiosa per essere veritiera; il linguaggio è immediato, allarmante o minaccioso; è scritta male e contiene molti refusi ed errori di grammatica; i saluti sono ambigui o molto generici; richiede l'invio di informazioni personali; invita con urgenza a fare clic su un link ipertestuale o un allegato sconosciuto; contiene richieste lavorative strane o repentine; l'indirizzo e-mail del mittente non corrisponde a quello dell'azienda da cui proviene.

MAUSER
Packaging Solutions