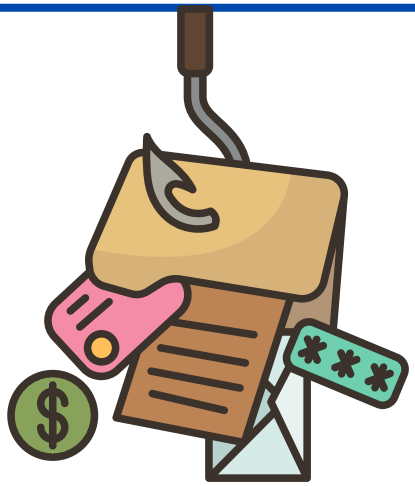
Bonus Track: #Cybersecuritymonth

Ottobre è il **Cybersecurity Month**, ideato per sensibilizzare sui rischi informatici e promuovere le buone pratiche per proteggere i dati sensibili.

Un piccolo contributo di Core Up a questa iniziativa europea: spieghiamo quali sono i diversi tipi di **PHISHING** così da riconoscerli ed evitarli.

COS'È IL PHISHING?

Il cybercriminale si spaccia per una fonte autorevole ingannando gli utenti al fine di ottenere informazioni personali come password, dati bancari, numeri delle carte di credito.



COME RICONOSCERE UN ATTACCO PHISHING?

Il SENSO DI URGENZA è la leva usata maggiormente dai criminali informatici per far sì che l'utente clicchi su un link contenuto in una e-mail di phishing.

Attenzione, quindi, alle mail che contengono frasi catastrofiche che richiedono clic o azioni immediate.
In questi casi è sempre bene fare un respiro, controllare tutti i campanelli di allarme della mail (mittente, presenza di errori di ortografia, etc), non esitare a chiedere un parere al responsabile IT, a un collega o al titolare.

Il dubbio e l'allenamento al riconoscimento del pericolo possono salvare da un attacco hacker.

I PRINCIPALI TIPI DI PHISHING

E-mail Phishing: messaggio di massa inviato per far sì che l'utente clicchi su un collegamento dannoso e inserisca le proprie credenziali.
Spear Phishing: invio di e-mail personalizzate e dannose a utenti specifici di aziende appositamente selezionate.
Whaling: l'e-mail dannosa prende di mira solo dirigenti o amministratori (i "pesci grossi) di società specifiche facendo leva su crisi urgenti da risolvere.
Smishing: attacco phishing usando i messaggi di testo sms contenenti link dannosi da cliccare.
Vishing: telefonata che, con un messaggio vocale automatico da una fonte apparentemente sicura (banca, ospedale), invita gli utenti a fornire le proprie credenziali.
Business E-mail Compromise: il criminale ottiene l'accesso all'account e-mail aziendale di un dirigente e invia e-mail ai dipendenti per suo conto per avviare bonifici fraudolenti.
Clone Phishing: replica dannosa di un messaggio ricevuto inviandolo nuovamente con collegamenti fraudolenti.
Evil Twin Phishing: creazione di una falsa rete WiFi che attira gli utenti su un sito di phishing.
Social Media Phishing: i criminali usano i social network per creare account falsi e attirare gli utenti nella trappola.
Search Engine Phishing: i cyber criminali creano siti fraudolenti e attirano gli utenti con offerte incredibili per far sì che inseriscano le loro credenziali.
Pharming: reindirizzamento degli utenti a siti web dannosi con indirizzi IP falsi.

030.4194040
info@coreup.it
www.coreup.it

Core Up Srl
Via Bruno Buozzi, 1/A
25125 Brescia (BS)

Seguici su LinkedIn:
Core Up Srl