Ref. Dott.ssa Anna CIMA
Tel. 328.8923614

Alla C.A.
del Dirigente Scolastico, del DSGA
e del personale amministrativo

Comunicazione n.05/2024: email phishing…sembra autentica ma non lo è!

Come avrete notato, nelle ultime settimana arrivano quotidianamente email apparentemente autentiche soprattutto da parte di Aruba, nelle quali si sollecita il pagamento del dominio del sito della scuola o pagamenti relativi a rinnovi email e/o PEC. Le email hanno un contenuto che appare identico a quello normalmente inviato da Aruba e che, dunque, possono trarre in inganno l'utente. Non solo finte email Aruba, ma anche comunicazioni da Poste, GLS e altri corrieri per consegna merce, PayPal oppure da Banche o gestori delle utenze, tutti mittenti ritenuti affidabili e che conosciamo; messaggi che riceviamo abitualmente per le nostre attività quotidiane e che ci fanno pensare che anche quelli fraudolenti possano essere effettivamente autentici.

Si chiama **phishing** (dall'inglese "fishing", pescare) ed è una tipologia di truffa realizzata tramite la rete internet che mira ad ingannare gli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica che imitano quelli autentici e nei quali si comunicano problemi di pagamento, di consegna merce, di accesso a qualche sito su cui si è registrati con l'invito a cliccare su un link riportato nel testo del messaggio.

Se l'utente si lascia trarre in inganno e "abbocca all'amo" cliccando sul link, ecco che si concretizza la truffa: sul pc potrebbe essere scaricato un malware o si viene ricondotti a qualche sito identico a quello originale su cui l'utente inserisce i propri dati, che entreranno così nella disponibilità dei truffatori.

Bisogna adottare alcune accortezze per imparare a riconoscere questi tentativi di truffa:

- **Controllare l'indirizzo email del mittente**: a volte è quasi identico a quello originale, ma c'è sempre qualche lettera in più, qualche parola aggiuntiva, uno spazio, numeri e caratteri speciali;
- **Controllare l'URL di destinazione del link**: quando in una email è presente un link del tipo CLICCA QUI, andando sopra il link con il cursore SENZA cliccare, si dovrebbe vedere in basso nell'angolo sinistro del monitor (o nei pressi del collegamento) l'URL effettivo a cui punta quel link. Nel caso di collegamenti fraudolenti, quasi sicuramente si vedrà un indirizzo strano e di dubbia attendibilità.

E' importante quindi imparare a riconoscere i segnali e agire responsabilmente quando arrivano queste email, senza farsi prendere dal panico per il tono urgente della comunicazione.

Segue un esempio di tentativo di phishing che falsifica un avviso da parte di Aruba per mancato rinnovo, in cui si chiede al destinatario di cliccare per rinnovare il dominio:

Ref. Dott.ssa Anna CIMA
Tel. 328.8923614

Resto a disposizione per eventuali chiarimenti.

Data 15/02/2024

Cordiali Saluti
Dott.ssa Anna CIMA