ELI NET

01.Phishing

Il Phishing è il cyber attacco più comune e più pericoloso.
La prima regola per difendersi è imparare a riconoscerlo "a colpo d'occhio".
I criminali spediscono e-mail dal contenuto ingannevole e al destinatario viene richiesto di compiere un'azione per ottenere un vantaggio o evitare una situazione spiacevole.

Se l'azione richiesta viene eseguita i criminali ottengono un vantaggio fraudolento provocando un danno al destinatario o alla sua organizzazione.

3 TIPOLOGIE PIÙ COMUNI DI ATTACCO PHISHING

PHISHING VIA E-MAIL
Richiesta di un'azione da compiere con urgenza.
Richiesta di informazioni sensibili.
Presenza di link o allegati da scaricare.

SMISHING - PHISHING VIA SMS
Offerta imperdibile o intervento di sblocco.
Urgenza per non perdere l'occasione o per intervenire.
Presenza di un link che indirizza a un sito malevolo.

VISHING - PHISHING VIA TELEFONO
Chiamata da un'organizzazione conosciuta (es. banca).
Senso di urgenza legato a un possibile rischio.
Richiesta di informazioni sensibili (pin, numeri carte, ecc).

5 REGOLE PER PREVENIRE UN ATTACCO PHISHING

EVITARE CLICK IMPULSIVI
Verificare la fonte e confermare il mittente prima di visitare i link o scaricare gli allegati.

SOSOPETTARE DEI LINK
Verificare con attenzione gli eventuali link contenuti nelle e-mail, evitando di cliccare su link che risultano sospetti.

PROTEGGERE SE STESSI
Riflettere sempre con attenzione davanti a una richiesta di informazioni personali.

NON CEDERE ALL'URGENZA
Diffidare delle e-mail in cui viene richiesto di intrapendere rapidamente un'azione. Non reagire d'istinto ma verificare l'autorevolezza del messaggio.

DUBITARE DI MAIL INATTESE
Fare attenzione alle e-mail inattese, sopratutto se il contenuto sembra sospetto o troppo bello per essere vero.

5 SUGGERIMENTI PER RICONOSCERE IL PHISHING

INDIRIZZO DEL MITTENTE
L'indirizzo del mittente contiene spesso anomalie, compresa quella di appartenere ad un domino di tipo generico oppure straniero.

COMUNICAZIONE INSAPETTATA
L' e-mail spesso contiene una comunicazione inaspettata con una richiesta insolita.
La forma risulta inusuale anche quando arriva da un mittente apparentemente conosciuto.

ERRORI ORTOGRAFICI
Le e-mail massive (Spray Phishing) contengono spesso errori ortografici, frutto di traduzioni approssimative. Le formule di apertura sono generiche, del tipo "gentile cliente".

SENSO DI PRESSIONE E URGENZA
I cyber criminali fanno normalmente leva su un criterio di pressione e urgenza per indurre un'azione istintiva e immediata.

LINK MALEVOLI
Le e-mail di phishing inducono a cliccare su link con anomalie.
Il link "visibile" spesso non coincide con il link "reale" e il link reale punta su siti diversi da quelli "attesi".

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