

BENVENUTI

al corso di formazione sulla

Sicurezza Informatica

Perché questo corso?

Ogni giorno siamo soggetti alla ricezione di mail, telefonate, sms indesiderati e sempre più spesso si tratta di tentativi di accesso alle nostre credenziali (IBAN, PIN, PASSWORD etc) da parte di criminali informatici.

Purtroppo negli ultimi tempi sono diventati particolarmente abili nel celare le loro intenzioni.

Per questa ragione diventa indispensabile comprendere in che modo agiscono e come potersi difendere

Cosa vedremo nello specifico:

- cos'è l'ingegneria sociale e in che modo entra in gioco negli attacchi informatici
- quali sono le principali minacce che arrivano dalla rete
- come difendersi e non cadere nella trappola di malintenzionati

Cosa si intende per ingegneria sociale?

L'ingegneria sociale è una tecnica psicologica che si basa sul manipolare una persona a fare qualcosa di vantaggioso per un criminale informatico.

E' molto pericolosa perchè sfrutta la natura umana, le emozioni e le interazioni sociali.

Il criminale informatico conosce le potenziali debolezze umane e le utilizza a proprio vantaggio.

Cosa rischia di farci abboccare al suo amo?

- Fiducia e autorità
- Difficoltà sulla difesa tecnologica
- Scarsa consapevolezza
- Flessibilità e adattabilità

Quali le principali tecniche per farci cadere in trappola?

PHISHING

VISHING

SMISHING

QUASHING

PHISHING

È in assoluto il più utilizzato e pericoloso.

Ogni volta che si riceve una mail si potrebbe incorrere in questo inganno.

Tecnicamente consiste nella ricezione di una mail in cui si viene indotti, inconsapevolmente, a fornire i propri dati.

Altri metodi di inganno

Vishing : chiamate telefoniche affidate a voci registrate

Smishing : invio di SMS

Quashing : utilizzando il QR Code (il meno frequente ma il più insidioso)

Come potersi difendere dal PHISHING

La CONSAPEVOLEZZA è la prima arma.

Essere a conoscenza di questi attacchi permette di essere più cauti e di prestare attenzione ad alcuni elementi cruciali che permettono di individuare la natura malevola della mail.

Ho ricevuto una Mail. Cosa attenziono?

VERIFICA DELLA FONTE

Conosco il mittente?

Conosco l'indirizzo di provenienza?

Nel caso di dominio, coincide esattamente con quello ufficiale?

Es. @google.it è uguale a @gooogle.it ?

Come si vede da questo esempio si tratta di escamotage subdoli, perché creati appositamente per ingannare un occhio non attento.

In questo caso è facile non accorgersi immediatamente della “o” in più.

Ho ricevuto una Mail. Cosa attenziono?

Filtri standard di sicurezza:

SPF: verifica che l'indirizzo IP sia autorizzato

DKIM: firma digitale che autentica la mail

DMARC: controlla che SPF e DKIM siano entrambe verificate

Per visualizzare questi filtri è necessario accedere al codice sorgente della mail.

I 3 filtri devono essere tutti contrassegnati con PASS affinchè la mail possa essere considerata sicura.

Come possiamo ridurre la nostra esposizione?

Utilizzando:

Filtri Anti-Phishing: App appositamente create per bloccare mail sospette

Autenticazione MultiFattore: l'associazione di più modalità di autenticazione, ancor meglio se da dispositivi differenti.

Esempio di attacco PHISHING

- Mail:

Mittente: EpidoceSecurity@semoforti.it

Destinatario: <tutti i dipendenti>

Oggetto: Estrazione per Week End in una SPA

Messaggio: La nostra Azienda mette in palio un Week End a nostre spese in una SPA.

Se voleste partecipare utilizzare questo link per l'iscrizione:

estrazioneSPA@seemoforti.it

Grazie

**Avete notato
nulla di
strano?**

Statisticamente almeno 3 persone su 10 non si saranno rese conto che l'indirizzo del mittente ha subito una modifica:

EpiDoceSecurity@semoforti.it (Mail falsa)

EpicodeSecurity@semoforti.it (Mail corretta)

Perché succede?

In questo caso il criminale ha semplicemente invertito la posizione di 2 lettere all'interno della parola, contando sulla tendenza della mente umana ad attribuire comunque un senso ad una parola scritta in maniera errata, se sono corrette la prima e l'ultima lettera.

In più, avendo cliccato sul link della mail, avranno aperto la porta di casa al criminale di turno, permettendogli di utilizzare i propri dati a suo vantaggio (IBAN, Password, C/C etc.).

Grazie per
l'attenzione e
occhio ai dati