Scuola universitaria professionale della Svizzera italiana
Servizi centrali della Direzione
Informatica

SUPSI

Come riconoscere un attacco di phishing e come comportarsi

Cos'è il phishing?

Il phishing è una forma di ingegneria sociale: l'aggressore usa e-mail e siti malevoli che sembrano affidabili, per ottenere dalle persone informazioni riservate private o professionali.

Ad esempio un cybercriminale puoi indurti a rivelare la password facendoti credere che c'è un problema urgente con il tuo account, in seguito egli userà le informazioni ottenute per accedere illegalmente ai sistemi.

Gli attacchi di phishing si intensificano nei periodi di vacanza (perché è più difficile verificare la fonte di un messaggio ricevuto) o quando ci sono eventi particolari, ad esempio:

- calamità
- epidemie
- eventi geo-politici

SUPSI

Quali sono gli indicatori di un attacco di phishing?

1. **Mittenti sospetti:** i cyber-criminali tentano di simulare mittenti legittimi, ad esempio potresti ricevere una e-mail che a prima vista sembra provenire dal tuo superiore o da un collega, ma se verifichi l'indirizzo e-mail potresti scoprire che l'indirizzo del mittente non è un indirizzo conosciuto,

   ad esempio:  giovanni.rossi89@hotmail.com

2. **Link fasulli o siti che assomigliano a quelli reali:** se ti fermi alcuni secondi con il mouse sopra ad un link prima di cliccare, verrà visualizzato l'indirizzo che è la destinazione reale del link, in un attacco di phishing la destinazione spesso non coincide con il nome del link oppure rimanda ad un sito che assomiglia a quello reale,

   come ad esempio: http://www.supsii.ch  (nota la doppia "i").

3. **Errori grammaticali:** molto spesso le e-mail di phishing contengono errori grammaticali o di forma

4. **Allegati sospetti:** bisogna sempre dubitare di una e-mail inaspettata che ti chiede di scaricare ed aprire un allegato, i cyber-criminali nascondono malware (cioè software malevoli) all'interno di allegati apparentemente innocui, ed utilizzano tecniche di ingegneria sociale, come l'urgenza, per persuaderti ad aprirli

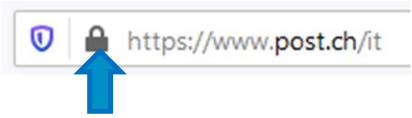
5. **Richieste inusuali:** potresti ricevere una e-mail da un collega o dal tuo superiore, che ti chiede di acquistare urgentemente delle gift-card (le carte regalo di Apple, Microsoft, Amazon ecc.) e di mandargli i codici di attivazione, naturalmente ti dirà di essere in riunione e non poter essere contattato per telefono

6. **Richieste di pagamento immediato:** potresti ricevere una e-mail da un servizio conosciuto come ad esempio la Posta Svizzera o DHL che ti chiede di pagare dazi doganali

SUPSI

Come posso proteggermi da un tentativo di phishing?

1. Sospetta sempre di e-mail o chiamate inaspettate o inusuali
2. Verifica sempre l'identità del mittente in caso di richieste sospette
3. Non fornire informazioni personali
4. Non fornire informazioni che riguardano la SUPSI, il personale o gli studenti, a meno che tu non abbia la certezza che il destinatario possa avere queste informazioni
5. Non fornire informazioni finanziarie per e-mail
6. Verifica sempre l'URL del sito al quale stai accedendo
7. Prima di inserire dati in un sito web, verifica che ci sia l'icona di un lucchetto chiuso accanto all'indirizzo del sito



SUPSI

Come faccio se penso di essere vittima di phishing?

1. Se pensi di aver fornito informazioni confidenziali che riguardano te, i tuoi account informatici oppure altre persone o la SUPSI, informa il Servizio Informatica all'indirizzo sicurezza@supsi.ch

2. Se hai fornito dati che riguardano il tuo conto bancario, contatta immediatamente la tua banca o chiedi aiuto al Servizio Informatica

3. Se hai fornito la password a qualcuno, cambiala il prima possibile e informa il Servizio Informatica all'indirizzo sicurezza@supsi.ch

Se hai domande rivolgiti al Servizio Informatica al seguente indirizzo:

sicurezza@supsi.ch