Phishing, AI e l’arte dell’inganno

Guida rapida per comprendere le minacce digitali e le strategie di difesa

Questo documento approfondisce alcuni dei temi affrontati durante le attività di divulgazione realizzate con HoneyPeople. Attraverso una panoramica su phishing, social engineering, intelligenza artificiale generativa e strategie di difesa, offre strumenti utili per comprendere meglio le minacce digitali e sviluppare una maggiore consapevolezza nell’utilizzo quotidiano delle tecnologie.

Cos’è il social engineering?

Il social engineering comprende tutte le tecniche di manipolazione psicologica utilizzate per influenzare il comportamento delle persone.

Gli attaccanti sfruttano emozioni e comportamenti umani come fiducia, urgenza, paura, curiosità e abitudine per ottenere informazioni, accessi o altre azioni utili all’attacco.

Per questo motivo il fattore umano continua a rappresentare uno degli elementi più critici della sicurezza informatica.

Cos’è il phishing?

Il phishing è una tecnica utilizzata per convincere una persona a compiere un’azione che favorisce un attacco informatico, come condividere credenziali, aprire allegati pericolosi o effettuare pagamenti fraudolenti.

Può avvenire attraverso email, SMS, applicazioni di messaggistica, telefonate o codici QR. L’obiettivo non è colpire direttamente la tecnologia, ma indurre la vittima a fidarsi e ad agire senza verificare.

Le red flags del phishing

Alcuni segnali possono aiutare a riconoscere un possibile tentativo di phishing:

- mittenti con domini simili ma non identici a quelli ufficiali;
- richieste urgenti o pressioni emotive;
- messaggi generici o incoerenti;

- link sospetti o allegati inattesi;
- richieste di password, codici o dati personali.

Con l'uso dell'AI generativa, molti attacchi sono oggi più realistici e credibili rispetto al passato, rendendo sempre più importante verificare la fonte e il contesto del messaggio.

L'impatto dell'AI generativa

Gli strumenti di AI generativa consentono di creare rapidamente campagne di phishing personalizzate, credibili e grammaticalmente corrette.

Questo permette agli attaccanti di aumentare la qualità e la quantità dei messaggi inviati, riducendo molti dei segnali che in passato rendevano più semplice riconoscere una truffa.

Dopo il click: il phishing è spesso solo l'inizio

Il furto di una password o di una credenziale rappresenta spesso soltanto il primo passo di un attacco più ampio.

Le informazioni ottenute possono essere utilizzate per accedere ad altri servizi, raccogliere dati sensibili, compromettere ulteriori sistemi o supportare attività di estorsione e ransomware.

Cos'è la cyber deception?

La cyber deception è un approccio difensivo che utilizza sistemi esca, dati fittizi e ambienti simulati per osservare il comportamento degli attaccanti, rallentare le loro operazioni malevole e raccogliere informazioni utili alla difesa.

Cos'è la gamification?

La gamification consiste nell'applicare elementi tipici dei giochi, come sfide, obiettivi e feedback immediati, a contesti educativi e formativi.

In cybersecurity permette di apprendere concetti complessi attraverso simulazioni pratiche, aumentando coinvolgimento, partecipazione e capacità di ricordare quanto appreso.

Come difendersi

Buone abitudini

- Fermarsi e riflettere prima di cliccare.
- Verificare sempre mittente e link.
- Diffidare da richieste urgenti o insolite.
- Verificare informazioni e richieste tramite un canale diverso.
- Segnalare messaggi sospetti.

Strumenti utili

- Password uniche per ogni servizio.
- Password manager.
- Autenticazione a più fattori (MFA).
- Passkey quando disponibili.
- Aggiornamenti regolari di dispositivi e applicazioni.
- Filtri antispam e antiphishing.

Tre cose da ricordare

Non avere fretta. L'urgenza è uno degli strumenti più utilizzati dagli attaccanti.

Verifica sempre. In caso di dubbio, controlla prima di agire.

Proteggi i tuoi account. Password robuste, MFA e aggiornamenti regolari riducono significativamente il rischio di compromissione.

FONDAZIONE BRUNO KESSLER
CENTER FOR CYBERSECURITY

DAISY
DISTRIBUTED AI FOR DEPENDABLE CYBERSECURITY

UNIVERSITY OF TRENTO