Progetto settimanale 02/05/2025 **Davide Figus**

- Ingegneria sociale

  Simulazione di un'email di Phishing.

  Introduzione: Il Phishing è una tecnica di ingegneria sociale utilizzata dagli attaccanti al fine di estrarre informazioni alla vittima, le quali possono essere: credenziali d'accesso, dati bancari o comunque informazioni sensibili. Il processo consiste nell'inviare messaggi fraudolenti che in qualche modo porterebbero alla vittima di cliccare su un link (ingannevole), la quale a seconda del contesto troverebbe una pagina in cui inserire le proprie credenziali o comunque essere sotto minaccia in caso di allegati infetti da malware.
  In questo caso possiamo vedere un esempio di **Spear Phishing**, nel quale viene descritto il contesto, l'obiettivo dell'attaccante e le varie osservazioni che ci sono da fare riguardo la provenienza e il corpo dell'email.

  Contesto: Un influencer di TikTok diventa il bersaglio di un'email di Phishing, diventando un target esposto ad una minaccia per i suoi dati e per la sua immagine all'interno della piattaforma.

  Obiettivo: L'obiettivo principale dell'attaccante è quello di rubare le credenziali d'accesso dell'influencer, con l'intenzione di pubblicare contenuti spam, targettando l'immagine dell'influencer. Questo potrebbe portare ad una richiesta di riscatto dell'account e di conseguenza:
  - Richiesta di denaro
  - Danni all'immagine
  - Eventuale aggiunta di un link contenente un Malware per puntare a contenuti privati, così da massimizzare il ricavo in caso di estorsione.

    Email di Phishing:

    Violazione delle Linee Guida TikTok
    Oggetto: Azione urgente richiesta - Potenziale violazione delle Linee Guida TikTok
    Da: TikTok Trust & Safety <support@tiktokcommunity.review>
    A: alessia.lanza00@gmail.com

    Ciao @alessialanza,
    Il nostro sistema ha rilevato attività sul tuo account TikTok che potrebbero violare le Linee Guida della Community, in particolare in relazione a:

    - Contenuti ritenuti fuorvianti o dannosi
    - Uso non autorizzato di audio coperti da Copyright

- Promozioni esterne non verificate

Per evitare la limitazione delle funzionalità o una possibile sospensione dell'account, ti Invitiamo a completare una **verifica del tuo profilo entro 24 ore**, tramite il portale ufficiale di revisione contenuti:

>>Rivedi il tuo account qui: http://tiktok-safety-check.reviewpanel.net

L'assenza di risposta potrebbe comportare una sospensione automatica dell'account, come previsto dal Regolamento TikTok (Sec. 3.1.2)
Se ritieni che si tratti di un errore, puoi contattare il nostro team legale a:
policy.tiktok@appeals-center.info

Grazie per la tua collaborazione nel mantenere TikTok uno spazio sicuro per tutti.

TikTok Trust & Safety Team
ByteDance Ltd.

—

© 2025 TikTok/ByteDance. Questo messaggio contiene Informazioni riservate e può essere indirizzato esclusivamente al titolare dell'account menzionato.

Scenario:

- Lo scenario creato presenta una situazione che si verifica tutti i giorni, in quanto noti influencer sono esposti ad attacchi di Ingegneria sociale.
  In questo caso, Alessia Lanza (il target) riceve un'email di Phishing (non reale) ma con l'intento di manipolare e danneggiare la figura.
  L'email in questione è stata inviata dal dipartimento Safety di TikTok, che si occupa di mantenere la piattaforma priva di violazioni, in particolare:

  - La informa che uno dei suoi contenuti pubblicati risultano inappropriati o comunque sono stati segnalati per **violazione delle linee guida della community**, come l'uso improprio di contenuti protetti da Copyright o promozioni non autorizzate.
  - Nella Mail, le viene richiesto di verificare il proprio account entro 24 ore, cliccando su un link che reindirizza il target ad una finta pagina di verifica, al fine di estrarre le credenziali.

Credibilità:

- L’email apparentemente non presenta linguaggi o strutture sospette, sembra essere arrivata effettivamente dalla Safety della piattaforma.
  Inoltre, essendo una tecnica di manipolazione della vittima, nel contesto, potrebbe essere molto credibile in quanto:

    - Gli influencer utilizzano spesso audio popolari o brand, per cui l’alto tasso di pubblicazione dei contenuti potrebbe effettivamente far pensare al target di aver commesso violazioni in uno dei tanti post condivisi.
    - La paura professionale (in quanto spesso utilizzano la piattaforma come fonte di entrata principale) potrebbe creare una pressione emotiva che, dato il contesto dell’email, potrebbe portare ad una decisione affrettata e impulsiva, in quanto l’email apparentemente non risulta ingannevole ad occhi e persone disinformate riguardo l’ingegneria sociale.

Autenticità:

- L’email contiene diversi elementi che dovrebbero essere interpretati come sospetti, tra cui:

- Domin non ufficiali: Il dominio del mittente in questo caso risulta sospetto, in quanto non arriva da @Tiktok.com o comunque @bytedance.com ma presenta sottodomini che la piattaforma non utilizzerebbe mai.
- Link non ufficiali: Il link http://tiktok-safety-check.reviewpanel.net presenta un URL falso, in quanto anch’esso come i domini, non arriva da tiktok.com
- Urgenza: L’email di per se, crea pressione in quanto richiede solo 24 ore per poter cliccare sul link, una piattaforma ufficiale come TikTok raramente utilizza questa pressione.
- Errori: Nell’email non sono stati inseriti tantissimi errori, anzi, al contrario. Però con piccoli accorgimenti come il “Sec 3.1.2” riguardo il Regolamento può essere un segnale.
- Richiesta di login: Essendo che il sito e i domini non sono ufficiali e TikTok non invita il cliente ad effettuare il Login tramite un sito esterno, è un segnale molto importante.
- Email strane: Come i domini e il Link, è sospetta in quanto non proviene dal dominio ufficiale di TikTok.