SCENARIO:

Antonio Longhi è un utente regolare di ***Epic Games*** e utilizza frequentemente il suo account per giocare e gestire i suoi acquisti. Recentemente, Epic Games ha implementato nuovi strumenti di monitoraggio per migliorare la sicurezza degli account e rilevare accessi non autorizzati. Gli attaccanti approfittano di questa situazione inviando un'email che sembra provenire dal team di sicurezza di Epic Games, informando Antonio di un accesso non autorizzato da un indirizzo IP sconosciuto e cercando di ottenere le sue credenziali di accesso.

EMAIL:

Oggetto: Attenzione: Attivita' sospetta nel tuo account Epic Games
Da: support@epicgames.com

Gentile [Antonio Longhi],

Abbiamo rilevato un accesso non autorizzato al tuo account Epic Games da un indirizzo IP sconosciuto. L'attività sospetta è stata registrata il [Data e ora] da un dispositivo che non riconosciamo.

Per proteggere il tuo account e impedire ulteriori accessi non autorizzati, ti invitiamo a **verificare immediatamente** questa attività.

Cosa devi fare:

- **Clicca sul seguente link** per accedere al tuo account Epic e verificare l'attività recente: Verifica attività ora
- Dopo aver effettuato l'accesso, controlla e **chiudi tutti gli accessi** da dispositivi o luoghi che non riconosci. Vai alla sezione "Sicurezza" e seleziona "Chiudi tutti gli accessi non autorizzati". Questa azione assicura che eventuali sessioni non autorizzate vengano terminate immediatamente.
- **Modifica la tua password** per prevenire ulteriori accessi non autorizzati e assicurati di utilizzare una password complessa e unica.

Importante:

Se non completi la verifica entro 24 ore, per motivi di sicurezza, il tuo account sarà temporaneamente bloccato per prevenire accessi non autorizzati. Se ritieni che questo sia un errore, o se hai bisogno di ulteriore assistenza, contattaci immediatamente rispondendo a questa email o visitando il nostro **Centro Assistenza**.

Cordiali saluti,

Il Team di Sicurezza di Epic Games
[Logo Epic Games]
support@epicgames.com

Relazione:

Perché un utente ci cascherebbe:

- **Tono professionale e urgente:** L'email utilizza un tono formale e credibile, comune nelle comunicazioni ufficiali. La menzione di un blocco temporaneo crea un senso di urgenza e paura di perdere l'accesso, una tecnica tipica per spingere l'utente ad agire rapidamente senza pensarci troppo.
- **Link ingannevole:** Il link "Verifica attività" sembra legittimo, ma indirizza l'utente a un sito falso che replica l'interfaccia di Epic, inducendolo a inserire le proprie credenziali. Il dominio, " support@epicgames.com ", è progettato per sembrare autentico, utilizzando parole chiave come "Epic", "support".
- **Dettagli personalizzati:** L'inserimento di dettagli come la data e l'ora dell'accesso sospetto (anche se falsi) e l'indirizzo IP rende l'email più credibile. Un utente poco esperto potrebbe pensare che sia una comunicazione ufficiale, poiché appare convincente e tecnica.
- **Imitazione del formato aziendale:** L'uso del logo di Epic e di un indirizzo email apparentemente legittimo, come " support@epicgames.com ", aiuta a confondere l'utente, che potrebbe non notare la piccola differenza rispetto ai veri indirizzi Epic (ad esempio, EpicGames.com). Anche la firma e la struttura dell'email imitano perfettamente lo stile delle comunicazioni ufficiali.

Motivi psicologici dietro l'efficacia di questo phishing:

- **Senso di urgenza:** L'idea che il loro account possa essere bloccato o compromesso induce panico, portando l'utente a compiere azioni impulsive senza riflettere.
- **Fiducia nelle autorità:** L'email simula una comunicazione ufficiale da un ente di fiducia, il che riduce le difese dell'utente. Molti utenti tendono a fidarsi delle email che sembrano provenire da servizi che utilizzano quotidianamente.
- **Paura di danni futuri:** La possibilità di accessi non autorizzati o perdite economiche spinge le persone a voler risolvere la situazione il più rapidamente possibile.

Come evitare di cadere in questo tipo di phishing:

- **Controllare attentamente il dominio:** Gli utenti dovrebbero sempre controllare attentamente l'indirizzo email del mittente e l'URL del link.
- **Non cliccare immediatamente sui link:** È meglio accedere a Epic Games manualmente dal sito ufficiale invece di cliccare su link nelle email.
- **Abilitare la 2FA (autenticazione a due fattori):** Questo può prevenire compromissioni anche se un attacco di phishing ha successo.

Elementi dell'Email che Dovrebbero Far Scattare un Campanello d'Allarme:

1. **Dominio del Link:**
    - Il link fornito, "http://epicgames-security-check.com/login", contiene un dominio che non è ufficiale di Epic Games. I veri domini di Epic Games sono "epicgames.com" o "fortnite.com". La presenza di un dominio diverso è un chiaro segnale di phishing.
2. **Richiesta di Inserimento delle Credenziali tramite Link:**
    - L'email richiede all'utente di accedere e inserire le proprie credenziali tramite un link, anziché guidarlo a farlo tramite il sito ufficiale di Epic Games. Questo è un metodo comune di phishing per raccogliere informazioni sensibili.
3. **Minaccia di Blocco dell'Account:**
    - La minaccia di bloccare l'account se le azioni non vengono completate entro 24 ore è un'altra tattica di phishing comune, progettata per spingere l'utente a reagire rapidamente senza riflettere sulla veridicità dell'email.
4. **Verifica dell'Indirizzo del Mittente:**

- Anche se l'indirizzo del mittente sembra ufficiale, è importante verificarlo attentamente. Le comunicazioni legittime di Epic Games dovrebbero provenire da un dominio ufficiale e non da un indirizzo generico come "support@epicgames.com" che potrebbe essere facilmente falsificato.

5. **Controllo di Errori e Incongruenze:**
   - Anche se l'email è ben strutturata, gli utenti dovrebbero prestare attenzione a errori grammaticali o stilistici, che potrebbero indicare un tentativo di phishing. Una comunicazione ufficiale è solitamente priva di tali errori.

EMAIL ORIGINALE:

Di' NO alle truffe!

Fai attenzione ai siti truffa che offrono V-buck gratuiti o scontati. Gli unici siti ufficiali di Fortnite sono **epicgames.com** e **fortnite.com**.

Informazioni account

Non condividere la tua password con altri. A meno che tu non voglia effettuare l'accesso, Epic non ti chiederà mai la tua password, né altre informazioni sul tuo account. I truffatori sono abili nel replicare l'aspetto di un sito web di EPIC ufficiale, perciò controlla sempre l'URL!

Autenticazione a due fattori

Mantieni al sicuro il tuo account. Visita **fortnite.com** --> Account --> Password e sicurezza. Attiva autenticazione a due fattori. Facilissimo!

Per maggiori informazioni su come mantenere al sicuro il tuo account, **visita la nostra Informativa sulla sicurezza degli account**.

EMAIL MODIFICATA:

DI' NO ALLE TRUFFE!

Abbiamo rilevato un accesso non autorizzato al tuo account Epic Games da un indirizzo IP sconosciuto. L'attività sospetta è stata registrata il [Data e ora] da un dispositivo che non riconosciamo. Per proteggere il tuo account e impedire ulteriori accessi non autorizzati, ti invitiamo a verificare immediatamente questa attività.

COSA DEVI FARE?

• Clicca sul seguente link per accedere al tuo account Epic e verificare l'attività recente:
Verifica attività ora
• Dopo aver effettuato l'accesso, controlla e chiudi tutti gli accessi da dispositivi o luoghi che non riconosci. Vai alla sezione "Sicurezza" e seleziona "Chiudi tutti gli accessi non autorizzati". Questa azione assicura che eventuali sessioni non autorizzate vengano terminate immediatamente.
• Modifica la tua password per prevenire ulteriori accessi non autorizzati e assicurati di utilizzare una password complessa e unica.

ATTENZIONE:

Se non completi la verifica entro 24 ore, per motivi di sicurezza, il tuo account sarà temporaneamente bloccato per prevenire accessi non autorizzati. Se ritieni che questo sia un errore, o se hai bisogno di ulteriore assistenza, contattaci immediatamente rispondendo a questa email o visitando il nostro **Centro Assistenza**.

Per maggiori informazioni su come mantenere al sicuro il tuo account, **visita la nostra Informativa sulla sicurezza degli account**.