Maggio 2025

REGIONE MOLISE

Sistemi Informativi - Cyber Security Brochure

Il Phishing

Come proteggersi dalle trappole digitali

Regione Molise - Servizio Sistemi Informativi e Transizione al Digitale

Progetto PNRR: M1C1I1.5 “Cybersecurity” formazione tecnica

Cosa troverai in questa brochure

Sommario

Introduzione

Nel contesto attuale, caratterizzato da una crescente digitalizzazione delle Pubbliche Amministrazioni, il **Phishing** rappresenta una minaccia ampiamente diffusa, nonostante la sua apparente semplicità.

Si tratta di un attacco informatico che, attraverso **e-mail, SMS, telefonate** e **link fraudolenti**, mira a indurre le vittime a fornire **informazioni personali** e **sensibili**, oppure a installare inconsapevolmente software dannosi sui propri dispositivi.

Lo sapevi?

Percentuale di crescita degli attacchi di Phishing e Ingegneria Sociale, dal **2023** al **2024**.*

Questa tipologia di attacco risulta particolarmente efficace perché sfrutta tecniche di **ingegneria sociale** (social engineering): strategie mirate a manipolare psicologicamente l'utente, facendo leva su **fiducia**, urgenza o timore per spingerlo ad agire contro il proprio interesse.

Le Pubbliche Amministrazioni Regionali gestiscono un'enorme mole di dati personali, che include **dipendenti**, **cittadini** e **studenti**, rendendole un bersaglio privilegiato per i cybercriminali. La complessità e l'estensione delle loro reti informatiche ne aumentano la **vulnerabilità** e rendono più difficile garantire un'adeguata **protezione**.

Le fasi di un attacco Phishing

01 **Analisi** del **contesto** organizzativo di riferimento e/o degli utenti *target.*

02 **Creazione** delle e-mail e/o del software malevolo da utilizzare per eseguire l'**attacco** di Phishing verso la platea di soggetti individuati (invio massivo di e-mail).

03 **Invio** delle e-mail dal contenuto malevolo (es. **link** e/o un **allegato**) con la finalità di attrarre gli utenti *target* ad interagire con le stesse.

04 **Furto di dati** riservati e/o installazione di **software malevoli** sul dispositivo dell'utente caduto vittima dell'attacco di Phishing.

***Fonte:** CLUSIT Report - Sicurezza ICT in Italia 2024

Attento a quel link!

Di seguito, vengono riportati e descritti i principali **rischi** degli attacchi Phishing.

Installazione di programmi malevoli

Gli attacchi di phishing sono spesso il punto di ingresso nei **sistemi informatici**, sfruttando **software dannosi**, (come i malware) veicolati attraverso l'**interazione** della vittima con **link** o **allegati**. Questi programmi, una volta attivati, possono infettare i dispositivi, monitorarne le attività e compromettere la **sicurezza** e la **riservatezza** di dati e informazioni

Violazione dei dati e delle informazioni

Attraverso il Phishing, gli attaccanti mirano a **sottrarre dati sensibili**, come credenziali di accesso, numeri di carte di credito, etc. Questi dati possono poi essere utilizzati per compiere **altre attività illecite**, come furti d'identità e frodi, mettendo a rischio non solo la **privacy** della vittima, ma anche la **sicurezza complessiva** degli **utenti** nel contesto digitale.

Perdite economiche e finanziarie

Nel primo semestre del 2024, la Polizia Postale per la sicurezza cibernetica ha registrato un aumento delle somme sottratte a seguito di frodi online. Quando un **attacco di phishing** va a segno, infatti, può provocare ingenti **perdite finanziarie** per le vittime, permettendo ai criminali informatici di effettuare **transazioni fraudolente**.

Principali Contromisure:

Prima di interagire con l'e-mail, cliccando sul link in allegato, **verifica attentamente l'URL** di reindirizzamento esterno, assicurandoti che appartenga a siti web ufficiali e/o legittimi.

Diffida da chi ti richiede di condividere informazioni personali con urgenza **verificando l'identità del mittente**: adottare comportamenti consapevoli online è una responsabilità sociale condivisa.

Poni attenzione a siti e/o persone che inducono a condividere i **dati** della tua **carta di credito**. Gli Istituti bancari, non richiedono **mai** la condivisione di informazioni sensibili.

Come difendersi?

Gli attaccanti di Phishing fanno spesso leva sull'effetto **sorpresa** e sul senso di **urgenza** per spingere le vittime ad agire impulsivamente. È fondamentale **restare calmi** e **controllare con attenzione** ogni comunicazione ricevuta, sia in ambito professionale che personale.

Controlla sempre il **sito che stai per visitare:** con il mouse, passa sopra il link (senza cliccare) e verifica che inizi con https://, mai con http://.

Verifica sempre con attenzione l'**indirizzo e-mail** del mittente. I truffatori informatici spesso utilizzano indirizzi simili a quelli ufficiali: controlla che il **dominio corrisponda effettivamente all'organizzazione** da cui sembrerebbe provenire la comunicazione.

Se hai **dubbi** sull'email ricevuta o sul sito web indicato, usa strumenti online gratuiti (come ad esempio **Virus Total**) per verificarne l'affidabilità.

I messaggi di phishing presentano frequentemente degli errori **grammaticali**, di **sintassi** oppure **stilistici**. Fai attenzione a eventuali anomalie nel linguaggio o a un tono poco professionale, che potrebbero indicare un **tentativo di frode**.

In caso di **dubbio** sulla **legittimità del mittente**, verifica attraverso canali ufficiali la sua veridicità e autenticità.

Per proteggere in modo ancora più sicuro l'accesso a **portali** e **siti web che utilizzi** frequentemente, attiva laddove possibile **l'autenticazione a due fattori**, un livello aggiuntivo di sicurezza che rende più difficile agli attaccanti ottenere l'accesso alle tue **informazioni personali**.

Per salvare i tuoi accessi con doppio fattore, ricordati di utilizzare sempre **applicazioni verificate** come **Google** o **Microsoft Authenticator**.

Security Trends

gennaio 2024

Promessa di finto rimborso per prestazioni sanitarie in Italia

Con comunicato diffuso nel mese di gennaio 2025, il CERT-AGID ha segnalato una campagna di **Phishing finanziario** attualmente attiva, condotta sfruttando impropriamente il nome e il logo del **Ministero della Salute**.

I criminali informatici, tramite l'invio di e-mail fraudolente apparentemente riconducibili al Servizio Sanitario Nazionale, hanno indotto gli utenti a cliccare su un link malevolo con la **promessa di un rimborso** di €265,67 per prestazioni sanitarie. L'email, conteneva un collegamento ad una pagina web ingannevole in cui venivano richiesti alla vittima **dati personali** e **bancari**, tra cui nome, indirizzo, numero di telefono e dati della carta di credito. In alcuni casi, veniva chiesto un doppio inserimento dei dati, per ridurre il rischio di errori e massimizzare la sottrazione di informazioni sensibili.

Il dominio malevolo, utilizzato dai criminali informatici per l'attacco, è stato oggetto di attività di contrasto da parte del **CERT-AGID**, che ha prontamente segnalato l'abuso e informato il Ministero della Salute dell'accaduto.

Fonte: CERT-AGID Phishing Finanziario

aprile 2025

L'Intelligenza Artificiale al servizio dei criminali informatici

Con comunicato pubblicato nel mese di aprile 2025, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha segnalato l'attività di una campagna di **Phishing Adattivo**, individuata grazie alle osservazioni del CERT-AGID.

In tale contesto, è stato rilevato l'utilizzo da parte degli attaccanti, di tecniche sofisticate capaci di **generare dinamicamente pagine di login fraudolente**, personalizzate in base al dominio e-mail dell'organizzazione bersaglio.

Le pagine in questione, costruite tramite servizi di **Intelligenza Artificiale (AI)**, riproducevano fedelmente loghi e contenuti dei **portali istituzionali**, ingannando gli utenti e inducendoli all'inserimento delle proprie credenziali riservate.

L'impiego combinato di loghi dinamici e **repliche precise dei siti reali** ha reso la truffa particolarmente credibile, aumentando il **rischio di compromissione** di account aziendali e istituzionali.

A seguito dell'individuazione della minaccia, il **CERT-AGID** ha attivato le procedure necessarie per la rimozione dei domini malevoli e informato prontamente gli enti pubblici accreditati, al fine di prevenire ulteriori violazioni.

Fonte: CERT-AGID Phishing Adattivo

In arrivo nei prossimi Journal

Social Network

I pericoli e le insidie che si nascondono dietro ai social media

Ransomware

Il Malware che attacca e tiene in ostaggio i tuoi dati

Per segnalare possibili minacce o problemi di sicurezza, od eventuali temi che vorresti approfondire scrivi a:

sistemi.informativi@regione.molise.it

Il presente Cyber Security Journal e tutti gli altri contenuti informativi a tema sicurezza informatica, sono disponibili all'interno dell'intranet di Regione Molise al seguente link:

"PERSONALE"