MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Il Phishing

Come proteggersi dalle trappole digitali

Sommario

Cosa troverai in questa brochure

Introduzione

Il **Phishing**, oggi, rappresenta una delle minacce più pervasive nel panorama della sicurezza informatica. Il Phishing è un attacco cibernetico che, attraverso e-mail, SMS, telefonate o link fraudolenti, ti induce a **condividere** i tuoi **dati personali e sensibili** e/o **installare software malevoli** sul tuo dispositivo.

In Italia, il **settore «Università e Ricerca»** risulta essere uno dei **più bersagliati** dagli attacchi informatici; in particolare le **università** sono diventate **obiettivi privilegiati** per i criminali informatici.

L'interesse riguarda **l'enorme quantità di dati personali** conservati, che non si limitano ai soli dipendenti, ma comprendono anche gli **studenti**. Questo vasto numero di persone rende le reti più ampie, aperte e difficili da proteggere rispetto alle aziende.

Attacchi Phishing al settore «Università e Ricerca»

114 Numero di attacchi di Phishing rilevati nella Pubblica Amministrazione nel 2024

di cui:

63 Attacchi di Phishing rilevati nel solo settore dell'**Università e Ricerca** nel 2024

Le caratteristiche di un attacco Phishing

Inganno tramite ingegneria sociale: sfrutta tecniche di manipolazione cognitiva per convincerti a rivelare dati.

Alta efficacia: è uno degli attacchi informatici più insidiosi e pericolosi, oltre che estremamente efficace.

Semplicità operativa: non richiede competenze tecniche avanzate o strumenti complessi, rendendolo alla portata di molti criminali informatici.

Diversi canali di attacco: può avvenire tramite e-mail (Phishing), SMS (Smishing), chiamate vocali (Vishing) e persino social media.

Fonte: ACN - Operational Summary 2024;
Check Point Research – Cyber security report Italia 2024

Attento a quel link!

Rischi

01 Installazione di programmi malevoli

Gli attacchi di Phishing spesso costituiscono una **porta d'accesso** a **sistemi** e relative **informazioni sensibili**, sfruttando **software malevoli** (ad esempio malware) diffusi per mezzo dell'interazione con **link e/o allegati**. Infatti, detti software, sono in grado di **infettare** i **device** dell'utente, **spiando** le sue **attività**, **rubando dati ed informazioni** sensibili, ed in generale, **compromettendo la sicurezza del sistema e dei dati ivi contenuti**.

02 Violazione dati

Per mezzo degli attacchi di Phishing, i criminali informatici cercano di **esfiltrare dati sensibili**, come **credenziali d'accesso**, numeri di carte di credito, etc. Tali dati possono esser utilizzati per commettere **ulteriori illeciti,** come furti di identità, frodi finanziarie, etc., **compromettendo** non solo la **privacy dell'utente violato**, ma, in generale, la **sicurezza** degli **utenti online**.

03 Perdite finanziarie

La Polizia Postale per la sicurezza cibernetica, nel primo semestre del 2024 ha rilevato un incremento delle somme sottratte a margine di frodi online. Infatti, qualora un **attacco** di **Phishing** colpisse nel segno, potrebbe **causare** gravi **perdite finanziare** alle **vittime**, consentendo ai criminali informatici di compiere **transazioni fraudolente**.

Contromisure

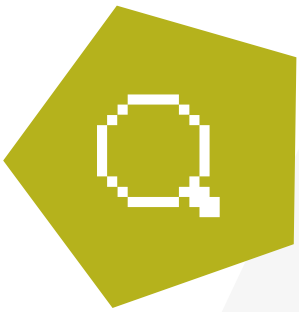
Prima di interagire con l'e-mail, cliccando sul link in allegato, verifica attentamente l'URL di reindirizzamento esterno, assicurandoti che appartenga a siti web ufficiali e/o legittimi.

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 spesso utilizzano l'elemento **sorpresa** ed il senso di **urgenza** per indurre le vittime ad agire senza pensare. **Mantieni la calma** e **verifica attentamente** tutte le comunicazioni che ricevi, sia nel **contesto lavorativo** che in quello **privato**.



Ricorda di controllare sempre **l'indirizzo e-mail** del mittente. Gli attaccanti utilizzano indirizzi che assomigliano a quelli legittimi. **Verifica attentamente la corrispondenza** tra il dominio e l'Ente apparentemente coinvolto.

Gli attacchi di Phishing spesso contengono **errori grammaticali** o **stilistici**. Presta attenzione a stranezze linguistiche o ad un **linguaggio non professionale**.

Per proteggere maggiormente l'accesso a **portali e siti web che utilizzi**, attiva **l'autenticazione a due fattori:** un livello aggiuntivo di sicurezza che rende più difficile agli attaccanti ottenere l'accesso alle tue **informazioni personali**.

Security Trend

Richiesta di aggiornamento del dispositivo utilizzato per l'home banking

Con **comunicato** di novembre 2024, **l'Agenzia** per **l'Italia Digitale (AgID)** avvisava la popolazione dell'intensificarsi di alcune campagne di Phishing, veicolate tramite e-mail, ed aventi a oggetto **l'aggiornamento** del **dispositivo** associato **all'home banking** di **Intesa San Paolo**. Il suddetto aggiornamento era finalizzato per continuare a beneficiare dei servizi digitali offerti dall'Istituto bancario.

Il **link** presente nell'e-mail indirizzava l'utente ad una **pagina web fittizia**, costruita ad hoc dai **criminali informatici**. A seguito del click sul link, si apriva la **schermata** di **accesso** alla banca online, inducendo gli utenti ad **inserire** le **credenziali**.

Successivamente all'inserimento delle credenziali di accesso, **l'utente**, con la finalità di **confermare** la sua **identità**, veniva **indotto** ad inserire il **numero** della **carta** di **credito**, la data di scadenza, il titolare ed il **codice** di **sicurezza**.

In questo modo, i truffatori hanno potuto ottenere i codici di accesso a conti online ed effettuare delle **transizioni fraudolente** recando danni economici agli utenti impattati.

novembre 2024

L'attacco di Phishing che ha preso di mira l'Università di Padova

Con **comunicato** diramato nel mese di marzo 2025, **l'Agenzia** per **l'Italia Digitale (AgID)** avvisava la popolazione della conduzione di una campagna di **Phishing** veicolata tramite **e-mail ai danni dell'Università di Padova.**

Nello specifico, i criminali informatici hanno inviato delle **e-mail** dal **contenuto fraudolento**, inducendo gli studenti ed il personale amministrativo ad accedere ad una pagina di **login form**, che riproduceva fedelmente l'aspetto del **portale ufficiale dell'Università di Padova**.

L'e-mail ha quindi indotto gli utenti dell'Università a cliccare sul link malevolo, che li ha reindirizzati su una pagina di login form creata con artificio dai criminali informatici, per carpire **e-mail** e **password di accesso**.

Da tale attacco informatico, infatti, sono state **sottratte** circa **200 credenziali** di accesso al portale universitario di studenti e dipendenti.

A valle dell'attacco subito, l'Università ha provveduto a **disattivare** le **pagine fraudolente**, impedendo, così, la possibilità che ulteriori utenti potessero inserire le proprie credenziali compromettendo le stesse.

marzo 2025

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.