Indicazioni utili a proteggersi dal Phishing

Versione 2.0

del 16/06/2021

Cos'è il *phishing*

T**entativo di truffa basato sull'invio di messaggi di** posta elettronica, il *phishing* **assume quale scopo la** sottrazione dei dati e delle informazioni personali degli utenti dei servizi erogati via web da organizzazioni affidabili solo in apparenza.

I mittenti delle email di *phishing* sembrano perseguire una finalità di tipo informativo del tutto encomiabile, e cioè riconducibile alla necessità per la potenziale vittima di risolvere un problema che riguardi uno dei suoi account attraverso l'adozione della soluzione che essi suggeriscono (es. cliccare su un link riportato nell'email ricevuta, fornire dati personali per ripristinare l'account ecc).

Come si riconosce un tentativo di *phishing*

L'obiettivo che i malintenzionati intendono perseguire, in realtà, è fraudolento: consiste nel raccogliere dati ed informazioni altrui per una qualche forma di tornaconto personale. Vengono indicate, di seguito, le tipiche caratteristiche di un'email di *phishing* **che possono presentare una o più delle seguenti caratteristiche**:

- **tono allarmistico: generalmente assumono un tono finalizzato a suscitare nella vittima pressione o "ansia".** Esempio: "Se non rispondi il tuo account verrà chiuso in 24 ore"
- **invito ad inserire informazioni personali e credenziali web su portali internet esterni al dominio "unimi.it"**
- **utilizzo di un Italiano poco corretto**

I controlli da effettuare e le precauzioni da adottare

Vengono elencati, di seguito, alcuni suggerimenti utili a difendersi da un attacco di phishing:

- tenere in considerazione il fatto che **le compagnie ufficiali non chiedono mai informazioni "importanti" via email**
- **prestare attenzione al mittente dell'email**: con tutta probabilità, avrà una forma "strana", non plausibile, non riconducibile ad un indirizzo email 'ufficiale'
- **verificare che** la pagina web di destinazione richiamata nel messaggio ricevuto:
    - **sia coerente con l'indirizzo Internet al quale il link che si suggerisce di cliccare condurrà**
    - **sfrutti un protocollo di connessione di tipo https:// e non http://**

  A tal proposito, **passare col puntatore del mouse sul link, senza cliccare.**
- **usare solo connessioni sicure**, in particolar modo quando si accede a siti "potenzialmente sensibili": non sfruttare connessioni sconosciute né i wi-fi pubblici, senza una password di protezione.

Cosa fare se ritieni di essere vittima di *phishing*

Se hai ricevuto una mail sospetta,

- **non cliccare sui link** presenti nel testo
- **non rispondere**
- **non scaricare / aprire eventuali allegati**
- **inoltra l'email malevola come allegato a: sicurezza@unimi.it**

Se hai già inserito o comunicato le credenziali, cambia immediatamente la password utilizzando un dispositivo differente da quello in uso, scegliendone una sufficientemente robusta.

Consulta la sezione "Avvisi di sicurezza" per consultare gli avvisi sulle campagne malevole in atto, visitando questa pagina internet.

Si raccomanda in generale a tutti gli utenti di:

- **utilizzare una password univoca di lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente**
- **attivare la domanda di controllo per il recupero della password**
- **cambiare le password regolarmente** e con frequenza almeno ogni 3-6 mesi
- **non riutilizzare la stessa password a breve distanza di tempo**
- **mantenere sistema operativo e antivirus aggiornati**.

Per altre informazioni relative all'utilizzo corretto delle credenziali, si rimanda alla sezione dedicata del servizio disponibile sul portale di Ateneo.