Avviso di sicurezza -Phishing poste italiane

Sono in corso **nuove campagne di phishing malevolo** veicolate attraverso il servizio di posta elettronica di Ateneo il cui obiettivo **è quello di sottrarre ai loro destinatari le credenziali normalmente utilizzate per accedere ad alcuni servizi erogati in rete delle Poste Italiane**.

Le email in esame, di cui riportiamo un esempio, **vengono inviate da test@ttara[.]ir> e hanno come oggetto "inviata su SMS sarà progressivamente disabilitato per i nostri clienti"**

Si fa presente che sia l'oggetto che il testo delle email potrebbero presentarsi con alcune modifiche e che la società Poste Italiane non ha alcuna responsabilità in merito a questo tentativo di truffa.

Gentile Cliente,
Ti comunichiamo che, nel rispetto dei pi`u aggiornati standard di sicurezza, abbiamo recentemente apportato alcune variazioni alle modalit`a di utilizzo del servizio di PosteID abilitato a SPID.
Ricorda che:
come previsto dall'art. 12 delle Condizioni Generali del Servizio, puoi recedere dal contratto entro 30 giorni dal ricevimento della presente comunicazione;
continuando ad utilizzare il Servizio, accetterai le modifiche contrattuali;
restano immutate le condizioni economiche del Servizio.
COSA CAMBIA PER TE?
Per semplificare le modalit`a di utilizzo della Tua Identit`a Digitale, l'accesso tramite password temporanea inviata su SMS sar`a progressivamente disabilitato per i nostri clienti.
Potrai continuare ad accedere con questa modalit`a ancora per 30 giorni. Successivamente riceverai una e-mail che ti confermer`a la disattivazione e potrai continuare ad accedere a tutti i servizi abilitati utilizzando l'APP PosteID.
COSA DEVI FARE?
Se non l'hai gi`a fatto, installa subito l'APP PosteID. `E disponibile sull'App Store (per i dispositivi iOS) o sul Play Store (per i dispositivi Android). Saranno sufficienti pochi minuti per attivarla: ti basta inquadrare il QR code visualizzato sulla pagina di login e utilizzare la tua impronta digitale e facciale (su terminali abilitati) per accedere a tutti i servizi abilitati, senza dover ricordare la tua password.
HAI BISOGNO DI PI`U INFORMAZIONI?
Per maggiori informazioni puoi visitare la pagina clicca qui

Image

Image

Messaggio di posta elettronica generato automaticamente. Ti preghiamo di non scrivere/rispondere all'indirizzo mittente. Per metterti in contatto con noi contatta il nostro Servizio Clienti al Numero Verde 803.160.

Poste Italiane ti ricorda di non rispondere ad e-mail, lettere o telefonate in cui si richiedono codici personali, dati delle carte di credito o della carta Postepay, perch`e Poste Italiane non utilizza mai queste modalit`a per richiedere tali dati.

Ci troviamo di fronte ad un tentativo di truffa informatica per contrastare il quale invitiamo gli utenti interessati a:

- **non cliccare sui link riportati nell'email ricevuta;**
- **non rispondere all'email ricevuta;**
- **non compiere alcuna delle azioni suggerite;**
- **non effettuare / aprire eventuali allegati.**

Cosa fare

L'Ufficio di Staff Sicurezza ICT, venuto a conoscenza della campagna di phishing in esame, ha attuato tutte le misure tecnologiche utili ad impedire dall'interno della rete di Ateneo la raggiungibilità del sito web malevolo linkato nel testo delle email in esame.

Tuttavia, non è possibile escludere che, tra gli utenti a cui è stata consegnata la mail fraudolenta nella casella INBOX, ve ne sia qualcuno che abbia cliccato sui collegamenti malevoli da una rete esterna ad Unimi (ad es. reti cellulari/domestiche o reti di altri enti o fornitori di connettività a Internet).

Chiunque avesse ricevuto l'email fraudolenta e inserito le proprie credenziali sul sito malevolo deve:

- **segnalarlo all'Ufficio di Staff Sicurezza ICT** inviando un'email a:sicurezza@unimi.it;
- **effettuare un cambio repentino della password dell'account di Poste Italiane** e **contattare il servizio di assistenza Poste Italiane** per segnalare l'accaduto e seguire le loro istruzioni;
- **nel caso in cui la password fosse utilizzata anche su altri sistemi (ad esempio quello di Ateneo), si richiede di cambiarla immediatamente su tutti**, utilizzando un dispositivo diverso da quello con cui si è cliccato sul link di Phishing.

Per coloro i quali avessero riconosciuto la mail fraudolenta come sospetta e dunque non abbiano cliccato sul link in esse riportato e inserito le credenziali sul sito malevolo, non è richiesta alcuna azione.

Si raccomanda in generale a tutti gli utenti di utilizzare:

- password per ciascun account univoche e robuste (almeno 8 caratteri, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente);
- di impostare come domanda di controllo per il cambio password, una domanda la cui risposta non sia facilmente indovinabile o desumibile da informazioni disponibili in rete;
- cambiare le password regolarmente e con frequenza almeno ogni 6 mesi;
- non riutilizzare la stessa password a breve distanza di tempo;
- mantenere sistema operativo e antivirus aggiornati.

Al fine di poter gestire al meglio i tentativi di phishing e di malspam, chiediamo agli utenti che ricevono email sospette di:

- non cliccare sui link riportati nell'email;
- non rispondere e non eseguire alcuna delle azioni suggerite;
- non scaricare / aprire eventuali allegati.

Inoltre, si invitano gli utenti ad inviare le future segnalazioni di spam a spam@unimi.it, mettendo in copia sicurezza@unimi.it solo nel caso in cui si ricevano email che possano rappresentare rischi di sicurezza, e quindi afferibili al nostro ufficio.