Posta elettronica

Phishing

Il phishing è una strategia per rubare credenziali di accesso utilizzando tecniche di social engineering attraverso messaggi di posta elettronica più o meno mirati.

Spesso viene fatto leva su indirizzi mittente credibili o su informazioni più o meno verosimili. Oppure su richieste in scadenza o promesse di guadagno per abbassare la soglia di pericolo e invitare l'utente a fornire le proprie credenziali.

Molte campagne di phishing ai danni degli utenti @unisi.it colpiscono attraverso versioni fasulle del portale webmail:

Buona regola è quella di non cliccare MAI sui link inviati insieme alle mail e di verificare sempre che sia l'URL che la connessione protetta (lucchetto verde) siano corretti e presenti:

Posta elettronica

I nostri sistemi antispam bloccano, ogni giorno, decine di mail fasulle ma **può capitare che qualcuna sfugga ai filtri** ed arrivi nelle caselle mail degli utenti.

In caso di dubbio, evitare di inserire le proprie credenziali e contattare l'helpdesk per una verifica all'indirizzo mail helpdesk@unisi.it

Nel malaugurato caso siate cadute vittima di un simile raggiro, è necessario **cambiare immediatamente le proprie credenziali** attraverso il portale https://my.unisi.it e **contattare immediatamente il servizio helpdesk** (mail a helpdesk@unisi.it) per una verifica su eventuali accessi non autorizzati.

Per rimanere sempre aggiornati su eventuali campagne di phishing o altre minacce, vi suggeriamo di iscriversi al nostro servizio di notifica in tempo reale attraverso il BOT Unisi su Telegram (https://telegram.me/unisibot)

ID univoco: #1139
Autore: : Michele Pinassi
Ultimo aggiornamento: 2020-02-11 12:41