Attenzione alla tua sicurezza! Diffida da e-mail di phishing e proteggi il tuo account

Christian Cantinelli - 2023-05-30 - Supporto Tecnico

Nonostante l'efficacia delle misure di sicurezza automatiche, troppo spesso si cade nel tranello di una falsa e-mail (**phishing**) che richiede di visitare un link, ad esempio per bloccare la sospensione di un servizio. Purtroppo quel link porterà a una pagina identica a quella del tuo account ma, una volta inseriti i dati, questi saranno acquisiti da hacker senza scrupoli che potrebbero utilizzarli per svolgere operazioni a tuo nome.

Alcune volte vengono attivate delle campagne di phishing con Server Plan come obiettivo e può capitare che alcuni dei nostri clienti **ricevano e-mail con avvisi di sospensione e link** sui quali vengono richiesti dati di accesso per la riattivazione di servizi.

Quello che ci teniamo a precisare è che si tratta di e-mail completamente fraudolente.

Quando ricevi una email da Server Plan:

- **controlla con attenzione l'indirizzo e-mail del mittente**, non il nome, ma proprio l'indirizzo e-mail! Noi inviamo e-mail esclusivamente da indirizzi con dominio/sottodominio serverplan.com concessi tramite SPF;
- verifica la presenza di eventuali errori di sintassi e ortografia: spesso vengono utilizzati testi standard tradotti automaticamente dall'inglese che lasciano alquanto a desiderare! Le traduzioni automatiche sono poco affidabili e facilmente riconoscibili;
- **controlla se ci sono dati personali**: nelle e-mail di phishing il testo è standard e poco specifico. Spesso viene indicato soltanto "Il tuo servizio è stato sospeso", senza specificare neanche di quale servizio si tratti. Inoltre, in genere il testo non comprende formule di saluto all'inizio o alla fine oppure nome, cognome, numero di partita iva, codice cliente e così via. Questi sono tutti segnali che suggeriscono che l'e-mail non sia indirizzata direttamente a te, ma che sia più probabilmente un'e-mail generica indirizzata a più persone;
- **controlla i link senza visitarli**: fai clic con il tasto destro sul link e seleziona "Copia link", quindi apri il Blocco note e incollalo lì. Con tutta probabilità farà riferimento a siti web che nulla hanno a che fare con il sedicente mittente;
  anche se l'e-mail è ben fatta e sembra lecita, non accedere al tuo account facendo clic sul link che ti viene proposto: apri un browser e visita il sito serverplan.com. Potrai effettuare l'accesso direttamente da lì;

- se l’e-mail riguarda il ripristino della password del tuo account, assicurati che sia stato tu a inviare la richiesta: in tal caso, il link che inviamo ha una durata di soli 30 minuti; in caso contrario, cestina la mail il nostro personale non richiede mai username/password per l’accesso ai servizi o riferimenti ai propri metodi di pagamento (es. numero di carta di credito).

Queste semplici accortezze ti aiuteranno a restare al sicuro da frodi e accessi non autorizzati.

Se ricevi una mail di **phishing** che ha come obiettivo Server Plan, salva la mail in formato eml (quindi con tutto il sorgente) e apri un ticket al Supporto Tecnico indicando la data e l'ora di ricezione e allegando il file.

Il nostro Staff procederà ad inviare gli abuse necessari ai provider per terminare l'attività malevola.