Come riconoscere un’email di phishing

Christian Cantinelli - 2026-04-13 - Supporto Tecnico

Nonostante l’efficacia delle misure di sicurezza automatiche, spesso si cade nel tranello di una falsa e-mail che richiede di visitare un link, ad esempio per **bloccare la sospensione di un servizio** o verificare un conto corrente. Ecco perché è importante capire come riconoscere un’email di phishing e proteggere il tuo account di posta elettronica.

Quello che dobbiamo sapere è che i **link nelle email di phishing** sono una truffa digitale: si aprirà una pagina identica a quella di un servizio, come le Poste o una banca. Una volta inseriti i dati, questi saranno acquisiti da hacker che potrebbero utilizzarli per svolgere operazioni a tuo nome. Nessuno è veramente al sicuro da queste minacce digitali.

A volte vengono attivate delle campagne di phishing con Serverplan come obiettivo e può capitare che alcuni clienti ricevano e-mail con avvisi di sospensione e link sui quali vengono richiesti dati di accesso per l'attivazione dei servizi. Non bisogna cliccare, ma è anche giusto a questo punto capire **come smascherare** un’email di phishing prima che faccia danni.

Controlla i link senza visitarli

Questo è il primo consiglio che possiamo dare a chi ha bisogno di riconoscere un’email di phishing. Come fare un controllo rapido? **Fai clic con il tasto destro** sul collegamento ipertestuale sospetto 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.

Ad esempio, se hai ricevuto un’email con sospetto phishing di Serverplan che ti suggerisce un’ipotetica scadenza di un dominio o di un altro servizio, non accedere al tuo account facendo clic sul link che ti è stato proposto. Apri un browser e visita il sito serverplan.com. In questo modo effettui tutti i controlli del caso e bypassi i **rischi di un’email phishing**.

Non svolgere azioni senza verifica

Nelle email di phishing ti chiederanno di svolgere delle azioni. Capita anche nelle email che simulano le richieste di Serverplan: se l’e-mail riguarda il ripristino della password del tuo account, assicurati che sia stato tu a inviare la richiesta. In caso contrario, **cestina la mail**. Non cliccare su nulla: né link, né tantomeno allegati (possono contenere malware).

La maggior parte dei servizi professionali (come ad esempio quelli di Serverplan) non richiede mai username/password per l’accesso ai servizi o riferimenti ai pagamenti. Inoltre, fai attenzione a toni minacciosi o urgenti come "*Il tuo account verrà sospeso entro 24 ore*", "*Rilevato accesso non autorizzato: clicca qui per bloccarlo*", "*Hai vinto un premio, riscattalo subito!*". Se un'email ti mette fretta o ti minaccia, fermati e **valuta bene cosa fare**.

Ci sono dati personali?

Vuoi riconoscere le e-mail di phishing? Nel messaggio che ti è arrivato nella casella di posta elettronica dovrebbe esserci un testo standard e poco specifico. Spesso viene indicato soltanto un **problema generico**, senza indicare neanche di quale servizio si tratti. Inoltre, il testo non ha formule di saluto all’inizio o alla fine e neanche tutti i dettagli utili:

- Nome e 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 una comunicazione generica indirizzata a più persone. La tecnica è quella della pesca a strascico: **mandiamo tante email generiche**, qualcuno cadrà nella trappola. E, considerati i numeri, c'è un buon margine di profitto dal phishing via email.

Verifica chi manda l'email

Controlla con attenzione l'indirizzo e-mail del mittente, non il nome, ma proprio la stringa composta dal **nome dominio** e dall'user. Le aziende serie usano il proprio dominio (ad esempio @serverplan.com o @amazon.it); noi inviamo e-mail esclusivamente da indirizzi con dominio/sottodominio serverplan.com concessi tramite SPF. Ovvero Sender Policy Framework, un metodo di autenticazione su record DNS che elenca gli IP autorizzati.

Fai un check degli errori del testo

Fai un check per assicurarti che ci siano i classici errori di sintassi e ortografia: spesso vengono utilizzati **testi standard tradotti** automaticamente dall'inglese che lasciano a desiderare. Anche se con gli strumenti dell'intelligenza artificiale il livello si è alzato in modo indicativo, spesso le traduzioni automatiche sono poco affidabili e facilmente riconoscibili.

Queste semplici accortezze ti aiuteranno a restare al sicuro da frodi e accessi non autorizzati identificando in tempi utili la presenza del phishing. Se ricevi un'email sospetta che ha come obiettivo Serverplan, 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 provvederà a inviare gli abuse ai provider per **terminare l'attività malevola**.

Per approfondire:

- Cosa fare se hai ricevuto email phishing Serverplan?
- Come eliminare definitivamente lo spam
- Gestione Antispam - Servizio di Supporto Serverplan