PHiSHiNG

Il 95% degli attacchi informatici inizia con una e-mail di **phishing**

Pertanto, quando riceviamo un'e-mail, prestiamo sempre molta attenzione a:

Forma di saluto generica

Non veniamo menzionati per nome (non ci conoscono) ma l'email pare contenere un messaggio importante per noi. Oppure l'email potrebbe rivolgersi a noi ma in un modo anomalo rispetto al solito.

Mittente ignoto

Un mittente vago, sconosciuto o non ben chiaro.
Chiediamoci sempre: **Il mittente è uno con cui comunico di solito?**
Il mittente ha un indirizzo sospetto?

Allegato inatteso

Contiene un allegato che non stavo aspettando o da qualcuno che non conosco?

Strana forma e contenuto

Uso anomalo o strano di ortografia e grammatica.

Richiesta di dati personali

Richiedono di verificare, aggiornare o completare dati personali.

Azioni urgenti richieste

Chiedono di eseguire con urgenza un'azione, per risolvere un problema bloccante.

Link a siti sconosciuti

Ci sono collegamenti a siti web su cui viene richiesto di cliccare. Verifichiamo con attenzione la legittimità del link e a dove punta veramente.

Cosa fare se l'e-mail non ci sembra lecita o nutriamo sospetti:

Non clicchiamo su link o allegati per i quali nutriamo dubbi, anche se minimi.

Conosciamo il mittente? In caso di dubbio chiamiamolo e verifichiamo che la richiesta sia effettivamente legittima.

Segui le procedure di prevenzione e protezione della tua organizzazione per i casi di phishing.

Hai per caso cliccato su un link o aperto un file sospetto?

Contatta l'ufficio IT di competenza ed informali dell'accaduto.

Scopri i servizi Kiwa dedicati alla Cybersecurity e alla sicurezza delle informazioni (come la Certificazione ISO 27001) su www.kiwa.it

kiwa