PHISHING SIMULATO:
FORMAZIONE SÌ, COLPEVOLIZZAZIONE NO

UILCA
Gruppo
Crédit Agricole Italia

COS'È IL PHISHING

Il phishing è un tentativo di frode informatica attraverso cui soggetti malevoli cercano di indurre la persona a compiere azioni rischiose, come:

- cliccare su link fraudolenti;
- aprire allegati malevoli;
- inserire credenziali aziendali o personali;
- comunicare dati riservati;
- autorizzare operazioni non dovute.

Le tecniche utilizzate sono sempre più sofisticate e possono sfruttare urgenza, paura, curiosità, apparenza di autorevolezza, comunicazioni apparentemente aziendali o richieste che sembrano provenire da soggetti conosciuti.

PERCHÉ L'AZIENDA EFFETTUA SIMULAZIONI

Le simulazioni servono a verificare il livello di attenzione complessivo dell'organizzazione e a **rafforzare** la capacità di riconoscere comunicazioni sospette.

L'obiettivo corretto deve essere:

- aumentare la consapevolezza;
- migliorare la formazione;
- individuare aree di rischio;
- fornire strumenti pratici;
- prevenire incidenti reali.

Non deve invece diventare un sistema **per "schedare" chi sbaglia o costruire precedenti disciplinari.**

LA POSIZIONE UILCA

UILCA ritiene che la sicurezza informatica sia una responsabilità condivisa. Lavoratrici e lavoratori devono prestare attenzione, ma l'Azienda deve garantire strumenti adeguati, formazione chiara, procedure semplici, comunicazioni comprensibili e un approccio proporzionato.

Una campagna di phishing simulato deve essere costruita per formare, non per spaventare.

Per questo **chiediamo che siano chiariti alcuni principi:**

1. le campagne devono avere finalità prevalentemente **formativa**;
2. i dati raccolti devono essere trattati nel rispetto della normativa privacy;
3. eventuali report devono essere utilizzati prioritariamente in forma **aggregata**;
4. le comunicazioni individuali devono avere tono formativo e non para-disciplinare;
5. non devono essere inserite automaticamente nel fascicolo personale;
6. eventuali errori devono essere seguiti da **formazione mirata, non da lettere minacciose;**
7. deve essere chiaro chi accede ai dati, per quanto tempo e per quali finalità;
8. **nessun utilizzo per fini disciplinari.**

COSA FARE DAVANTI A UNA MAIL SOSPETTA

- prima di cliccare, controlla attentamente il mittente;
- verifica se il messaggio contiene urgenze insolite o toni allarmistici;
- non inserire credenziali dopo aver cliccato su link ricevuti via mail;
- diffida da allegati inattesi;
- verifica eventuali errori, indirizzi strani o link non coerenti;
- in caso di dubbio, segnala la mail **secondo le procedure aziendali;**
- meglio chiedere una verifica in più che esporsi a un rischio;
- considera sempre **le mail da mittente esterno (evidenziate in rosso) come sospette**

IL PUNTO PER UILCA

La sicurezza informatica non si costruisce con la paura. Si costruisce con formazione efficace, strumenti adeguati, procedure chiare, tempo per lavorare con attenzione e un'organizzazione che aiuti le persone a non sbagliare.

Il phishing è un rischio reale.
Ma la risposta non può essere la colpevolizzazione individuale: deve essere prevenzione, consapevolezza e responsabilità organizzativa.

INSIEME, PER UN LAVORO PIÙ SICURO E CONSAPEVOLE. | UILCA