

Cybersecurity & Data Protection

Newsletter mensile: Novembre 2025



Questo mese parliamo di...

COME RICONOSCERE E SEGNALARE ATTACCHI DI PHISHING



Il **Phishing** è una tecnica di attacco informatico basata sull'ingegneria sociale, utilizzata per indurre le vittime a fornire informazioni sensibili, inducendolo a fare 'click' col mouse su link o allegati pericolosi. Si attua attraverso email ingannevoli che appaiono originate da fonti attendibili.



Phishing: Verifica e Segnalazione



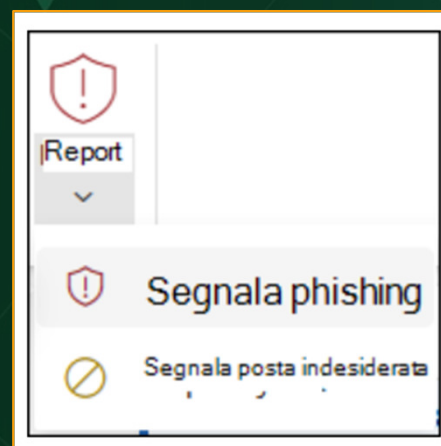
- Verificare l'**autenticità del mittente**, controllando non solo il nome ma anche l'indirizzo email.
- Verificare che i **link** siano **affidabili** prima di aprirli.
- Verificare che gli **allegati** provengano da **fonti affidabili** ed **evitare** di aprire quelli di **dubbia provenienza**.

Segnalare un'email di Phishing in Outlook

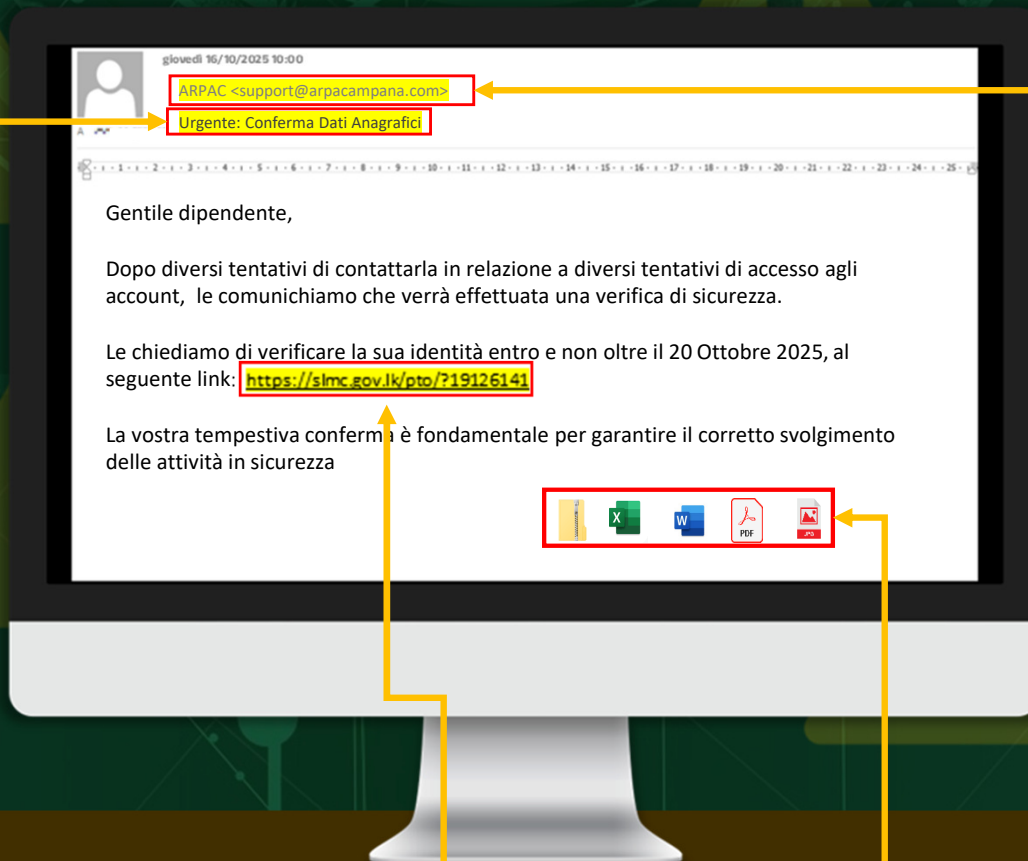
- 1 Nell'elenco dei messaggi selezionare il messaggio o i messaggi da segnalare?
- 2 All'interno del riquadro di lettura (barra superiore), selezionare «Report»?
- 3 Clicca su «Segnala phishing»?

In caso di continua ricezione o individuazione di e-mail sospette o riconducibili a tentativi di phishing, è opportuno **segnalare l'evento all'UO? Sistemi Informativi e Informatici** tramite i seguenti contatti:

☎ 0812326343 ✉ securityalert@arpacampania.it



Segnali Chiave per Identificare un'Email di Phishing



MANIPOLAZIONE PSICOLOGICA

Le email di phishing spesso iniziano con parole come "urgente" per catturare immediatamente l'attenzione del destinatario e creare un senso di urgenza. Questo approccio mira a indurre il destinatario a reagire rapidamente, senza riflettere attentamente sul contenuto dell'email.

ATTENZIONE AI LINK

Aprire esclusivamente link affidabili e verificarne l'autenticità prima di cliccarci posizionando il cursore del mouse sul link per visualizzare l'URL originale.

ATTENZIONE AL MITTENTE

È fondamentale verificare sempre l'indirizzo del mittente per accertarsi della sua autenticità.

ATTENZIONE AGLI ALLEGATI

Aprire esclusivamente gli allegati che provengono da fonti affidabili e assicurarsi di scansarli sempre con un software antivirus.