



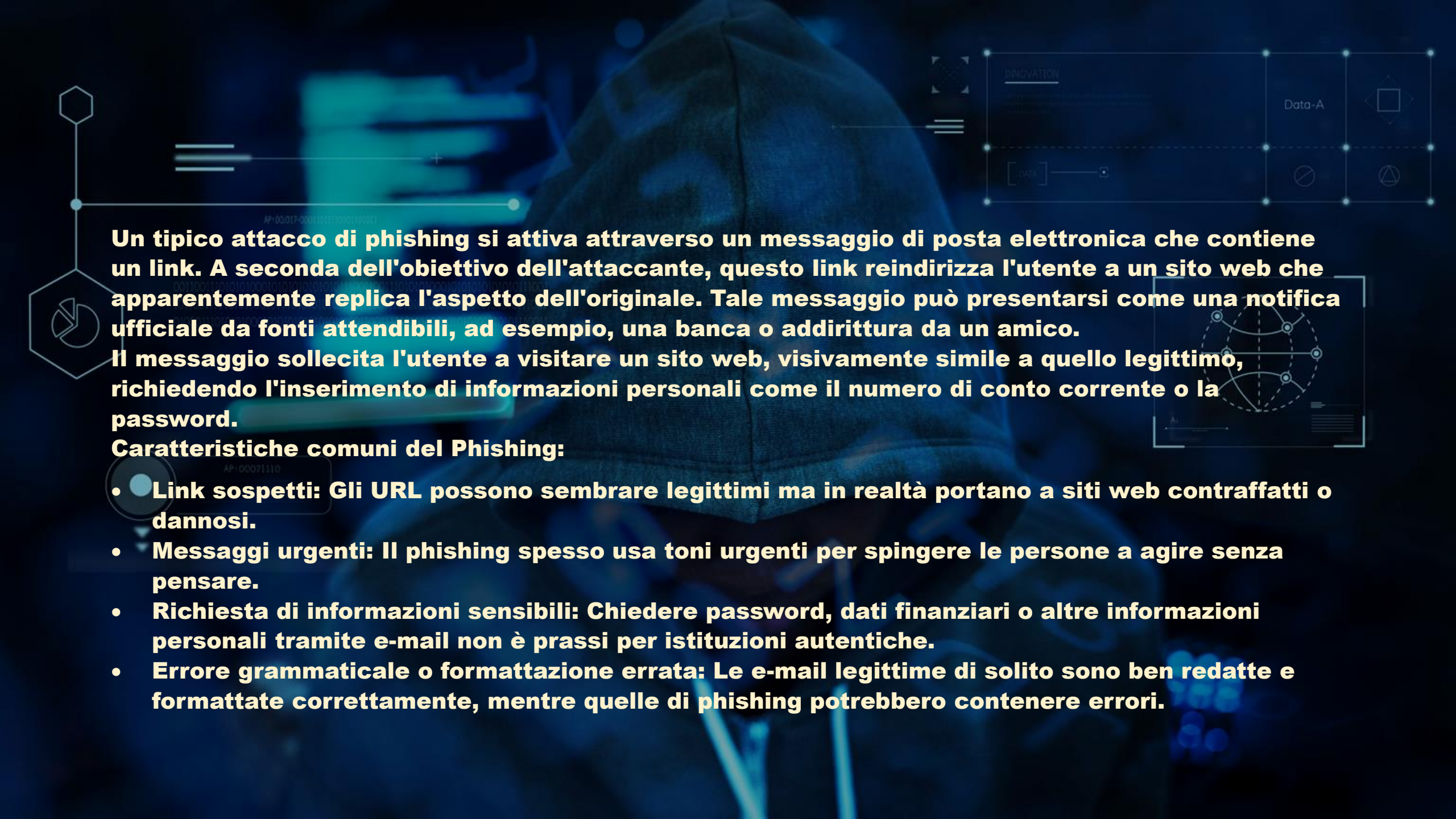
PHISHING

Cyber Security & Ethical Hacking -
Ingegneria sociale

Cosa è il phishing

Il phishing è una forma di attacco informatico che coinvolge l'inganno e l'ingegneria sociale per ottenere informazioni sensibili, come password, dati finanziari o altre informazioni personali, rubandole dall'utente incauto. Di solito avviene attraverso e-mail contraffatte, siti web fasulli o messaggi di testo.





Un tipico attacco di phishing si attiva attraverso un messaggio di posta elettronica che contiene un link. A seconda dell'obiettivo dell'attaccante, questo link reindirizza l'utente a un sito web che apparentemente replica l'aspetto dell'originale. Tale messaggio può presentarsi come una notifica ufficiale da fonti attendibili, ad esempio, una banca o addirittura da un amico. Il messaggio sollecita l'utente a visitare un sito web, visivamente simile a quello legittimo, richiedendo l'inserimento di informazioni personali come il numero di conto corrente o la password.

Caratteristiche comuni del Phishing:

- **Link sospetti:** Gli URL possono sembrare legittimi ma in realtà portano a siti web contraffatti o dannosi.
- **Messaggi urgenti:** Il phishing spesso usa toni urgenti per spingere le persone a agire senza pensare.
- **Richiesta di informazioni sensibili:** Chiedere password, dati finanziari o altre informazioni personali tramite e-mail non è prassi per istituzioni autentiche.
- **Errore grammaticale o formattazione errata:** Le e-mail legittime di solito sono ben redatte e formattate correttamente, mentre quelle di phishing potrebbero contenere errori.

Per identificare un potenziale tentativo di phishing, i dipendenti dovrebbero prestare attenzione a diversi parametri e indicatori che possono suggerire la legittimità o la dubbia autenticità di un messaggio. Ecco alcuni elementi chiave da considerare:

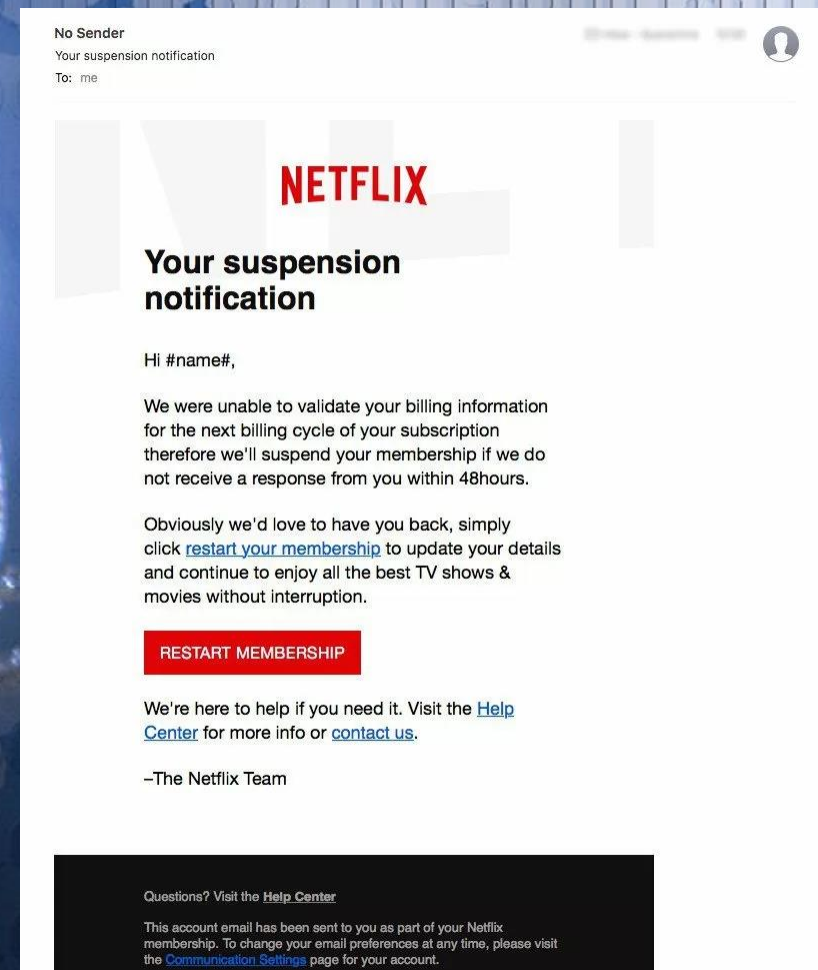
Controllare attentamente l'indirizzo email del mittente. verificare se corrisponde all'indirizzo ufficiale dell'azienda o dell'organizzazione presunta mittente.

Prestare attenzione alla grammatica e all'ortografia nel testo del messaggio. Spesso i phishing contengono errori evidenti o frasi mal formulate.

Diffidare da richieste di informazioni personali o sensibili via email. Le comunicazioni legittime non chiedono mai password, numeri di conto o altre informazioni personali tramite email.

Alcuni messaggi legittimi includono autenticazioni come SPF, DKIM, o DMARC. Questi possono essere indicatori di autenticità, ma non sono una garanzia assoluta.

Educare i dipendenti su questi criteri e incoraggiarli a essere vigili e a segnalare qualsiasi sospetto può aiutare a prevenire con successo attacchi di phishing all'interno dell'azienda.



Phishing Controllato

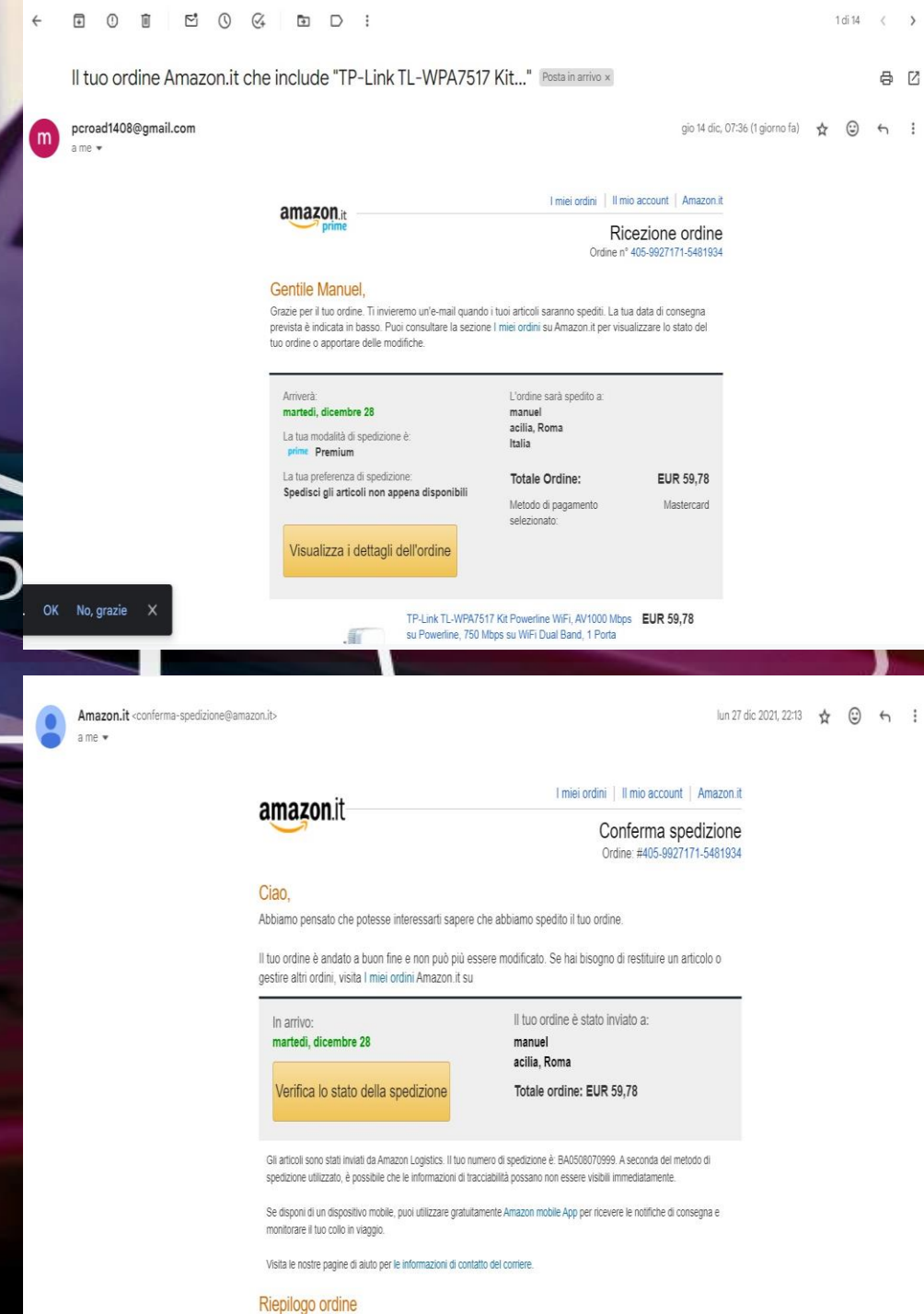
Identificare il tipo di messaggi che potrebbero attirare i dipendenti. Ad esempio, potrebbe essere una falsa richiesta di cambio password o un avviso di accesso non autorizzato.

Utilizzare uno stile simile a quello aziendale, ma con sottigliezze (come piccole discrepanze nel logo o nell'indirizzo e-mail) che possano essere identificate se prestate attenzione.

Utilizzare un tono urgente o un motivo credibile per spingere alla risposta.



Un esempio tipico potrebbe mostrare due e-mail sovrapposte: una rappresentante un tentativo di phishing e l'altra la reale comunicazione. A una rapida occhiata o a un utente meno esperto, le due potrebbero sembrare identiche. È in situazioni del genere che si nasconde il rischio: la somiglianza visiva può fuorviare e ingannare, portando a cliccare o interagire con messaggi fraudolenti.



Il mio metodo di approccio è stato quello di creare una mail fasulla, dove all'interno ci sarà un file contenente un virus (ransomware è un tipo di malware progettato per criptare i dati su un dispositivo o una rete, rendendoli inaccessibili all'utente. Una volta che i file sono criptati, il ransomware richiede un pagamento in cambio della chiave per sbloccare i dati).



A epicodesecurity@samoforti.com

Cc Ccn

Nuovo Antivirus da scaricare entro fine giornata!

Buongiorno,

Vi informiamo che abbiamo cambiato l'antivirus per garantire maggior sicurezza. In allegato troverete un documento con istruzioni dettagliate su come scaricare il nuovo antivirus.

Grazie a tutti e buon lavoro.

Cordiali saluti,

Gian Marco

[Video per installare l'antivirus.docx \(12K\)](#)

×