Formazione sulla Sicurezza Informatica: Combattere il phishing

Docente: Kamenica Kristiano

INTRODUZIONE

Scopo della formazione:

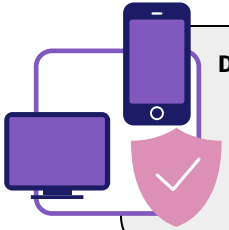
- Proteggere i dipendenti e l'azienda.
- Creare consapevolezza e competenze.

Importanza della Sicurezza Informatica

- La nostra azienda gestisce dati sensibili.
- Una violazione della sicurezza potrebbe compromettere la reputazione dell'azienda.

Collaborazione Necessaria

- Lotta di squadra contro il phishing. Tutti i dipendenti devono adottare pratiche sicure.



Durata della Formazione

- Investire tempo nella formazione aiuterà l'azienda e i suoi membri a proteggersi.

Obiettivo della Formazione

- Rendere i dipendenti consapevoli.
- Fornire conoscenze pratiche.
- Promuovere una cultura aziendale consapevole.

Coinvolgimento Attivo

- Se avete dubbi chiedete!
- Importante condividere informazioni tra colleghi.

Cos'e il Phishing?

Il phishing e un tipo di attacco informatico che mira a ottenere informazioni sensibili, come password e dati finanziari, fingendosi di essere una fonte affidabile e/o conosciuta.

TIPI DI PHISHING:

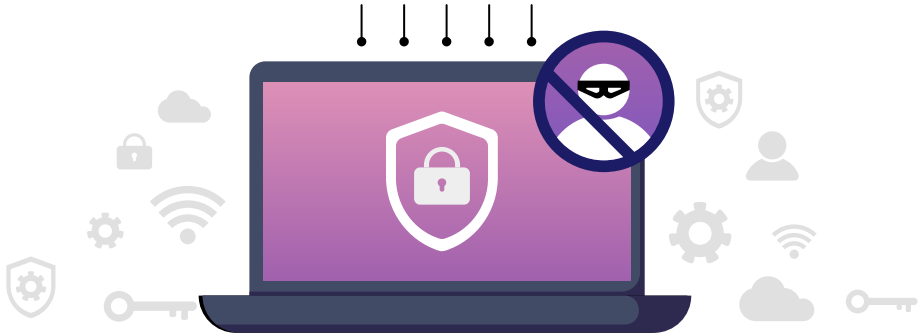
1. ***Phishing via email*** ovvero la forma più comune e che approfondiremo oggi.
2. ***Vishing(chiamate) e smishing(Sms)***, nel caso delle chiamate vengono utilizzate IA per cammufare la voce.
3. ***Sniffing trami Siti Web Contraffatti***

Rischi per l’azienda

CONSEGUENZE	• Perdita di dati aziendali sensibili. • Danno alla reputazione aziendale. • Accessi non autorizzati ai sistemi aziendali.
DIPENDENTI	• Rischio di furto di identità. • Compromissione delle credenziali. • Potenziali conseguenze finanziarie.
COSTI	• Spese e costi legati ad un attacco. • Possibili sanzioni e recupero di dati.
VULNERABILITA	• Possibilità di attacchi alle vulnerabilità della nostra azienda.

Esempi di Tecniche di Phishing

Riconoscere il Phishing



Mittente

Indirizzi e-mail simili o leggermente modificati possono identificare tentativi di phishing.

SPF

Un framework di autenticazione e-mail che verifica l'indirizzo IP sia in autorizzato dal dominio.

DKIM

Una firma digitale che autentica l'origine e l'integrità di un messaggio

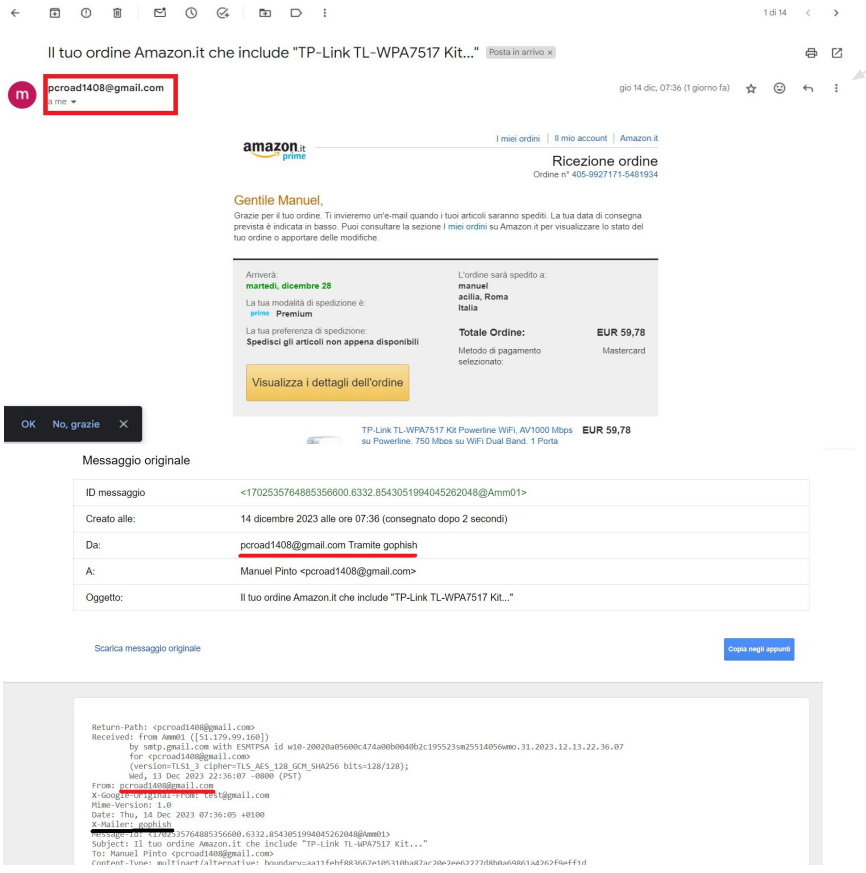
DMARC

Gestisce tutti i messaggi che non superano le verifiche SPF e DKIM

URL e Allegati

Verificare i link e gli allegati prima di cliccarli o scaricarli.

Esempio di E-mail Sospetta



Tramite questo messaggio possiamo accedere al “messaggio originale” in modo da analizzare e-mail sospette.

Mittente

Nonostante l’e-mail possa sembrare legittima notiamo subito che l’indirizzo e-mail del mittente non corrisponde con quello amazon.

Tramite gmail e possibile visionare il “messaggio originale” e quindi “spogliamo” l’e-mail e notiamo che non e presente il SPF

SPF

DKIM

Anche in questo caso notiamo che nella seconda immagine manca il DKIM e ciò deve farci insospettire.

In questo caso specifico magari non abbiamo mai effettuato questo ordine e quindi dovremmo iniziare a sospettare.

CONTENUTO

Consigli per evitare Il Phishing

Esaminare attentamente gli indirizzi e-mail dei mittenti, evita di aprire messaggi sospetti o provenienti da fonti non affidabili.

Non cliccare su link sospetti. Passa il mouse sopra il link per verificare l'URL effettivo prima di fare click.

Verifica la legittimita di richieste di informazioni sensibili attraverso canali ufficiali.Non condividere informazioni tramite email non sicure.

Partecipare regolarmente a sessioni di formazione sulla sicurezza informatica e rimanere aggiornati sulle tecniche di phishing.

Utilizza il sistema di segnalazion degli incidenti per informar tempestivamente l'azienda d eventuali tentativi di phishin

Mantieni una sana consapevolezza soprattutto davanti a messaggi che ti danno un senso di urgenza e/o emergenza

Hai qualche dubbio? Non avere paura e chiedi!

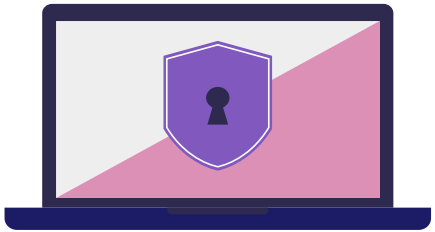
Chiedere a chi e piu esperto.

Partecipa attivamente a questo tipo di lezioni

Internet e la tecnologia possono sembrare pericolosi ma con la giusta consapevolezza non bisogna avere paura

Davanti ad un problema non farti prendere dal panico

“Ricordate sempre che la sicurezza informatica deve essere una priorità per tutti noi! Siate vigili e responsabili!”



GRAZIE!

Grazie per aver partecipato al corso.

Contatti

Kamenica.Kristiano@SecEpicode.com

I feedback sono piu che graditi