



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 camuffare 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.

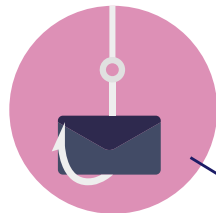


VULNERABILITÀ

- Possibilità di attacchi alle vulnerabilità della nostra azienda.

Esempi di Tecniche di Phishing

Messaggi di
emergenza



Richieste di
aggiornamento
password



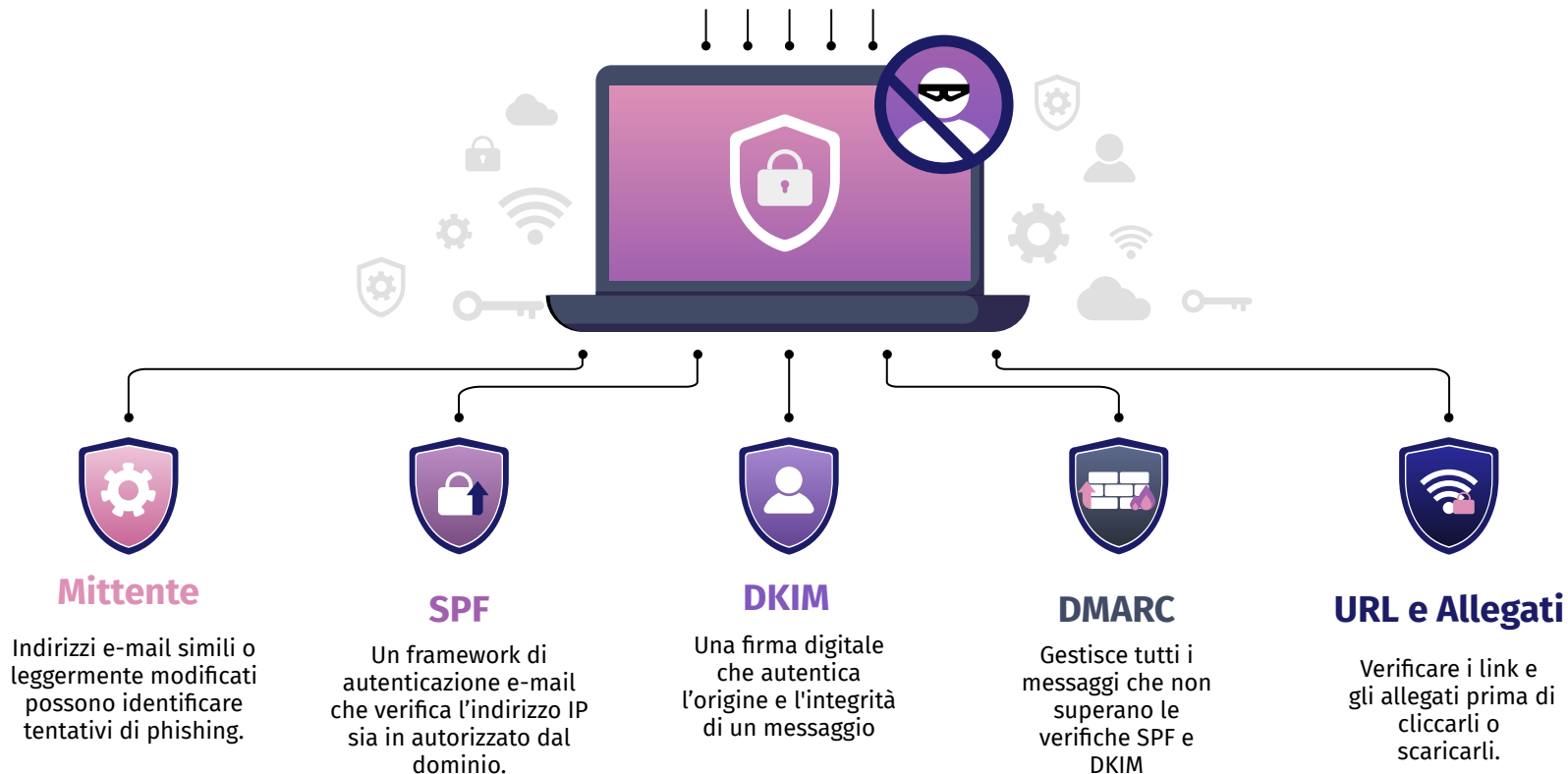
Falsi Premi



Link e File
Malevoli



Riconoscere il Phishing



Esempio di E-mail Sospetta

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

Il tuo ordine Amazon.it che include “TP-Link TL-WPA7517 Kit...” Posta in arrivo

pcroad1408@gmail.com
a me

gio 14 dic, 07:36 (1 giorno fa)

amazon
prime

I miei ordini | Il mio account | Amazon.it

Ricezione ordine
Ordine n° 405-9927171-9481934

Gentile Manuel,

Grazie per il tuo ordine. Ti invieremo un'e-mail quando i tuoi articoli saranno spediti. La tua data di consegna prevista è indicata in basso. Puoi consultare la sezione [I miei ordini](#) su Amazon.it per visualizzare lo stato del tuo ordine o apportare delle modifiche.

Arriverà: **martedì, dicembre 28**
La tua modalità di spedizione è: **prime Premium**
La tua preferenza di spedizione: **Spedisci gli articoli non appena disponibili**

L'ordine sarà spedito a: **manuel acilia, Roma Italia**

Totale Ordine: EUR 59,78
Metodo di pagamento selezionato: **Mastercard**

[Visualizza i dettagli dell'ordine](#)

TP-Link TL-WPA7517 Kit Powerline WiFi AV1000 Mbps su Powerline. 750 Mbps su WiFi Dual Band. 1 Porta

EUR 59,78

Messaggio originale

ID messaggio	<1702535764885356600.6332.8543051994045262048@Amm01>
Creato alle:	14 dicembre 2023 alle ore 07:36 (consegnato dopo 2 secondi)
Da:	pcroad1408@gmail.com Tramite gophish
A:	Manuel Pinto <pcroad1408@gmail.com>
Oggetto:	Il tuo ordine Amazon.it che include “TP-Link TL-WPA7517 Kit...”



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



Return-Path: <pcroad1408@gmail.com>
Received: from Amm01 ([51.179.99.168])
by smtp.gmail.com with ESMTPSA id w30-28028a05600c474a0b0b040b2:195523sm25514850wmo.31.2023.12.13.22.36.07
for <pcroad1408@gmail.com>
(version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
Wed, 13 Dec 2023 22:36:07 -0800 (PST)
From: pcroad1408@gmail.com
X-Google-Engineer: From: c0g8@gmail.com
MIME-Version: 1.0
Date: Thu, 14 Dec 2023 07:36:05 +0100
X-Mailer: gophish
Subject: TP-Link TL-WPA7517 Kit Powerline WiFi AV1000 Mbps su Powerline. 750 Mbps su WiFi Dual Band. 1 Porta
To: Manuel Pinto <pcroad1408@gmail.com>
Content-Type: multipart/alternative; boundary=caa11f6bf88367a405310ba87ac30a3a6c277708ba66861a27670f6ff4d

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 legittimità 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 segnalazione degli incidenti per informare tempestivamente l'azienda di eventuali tentativi di phishing.



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 è più esperto.



Partecipa attivamente a questo tipo di lezioni



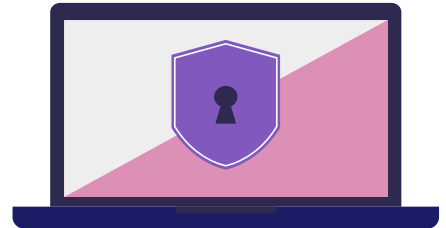
Internet e la tecnologia possono sembrare pericolosi ma con la giusta consapevolezza non bisogna avere paura



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.***



***I feedback
sono piu che
graditi***



Contatti

***Kamenica.Kristiano@SecEpicode.
com***