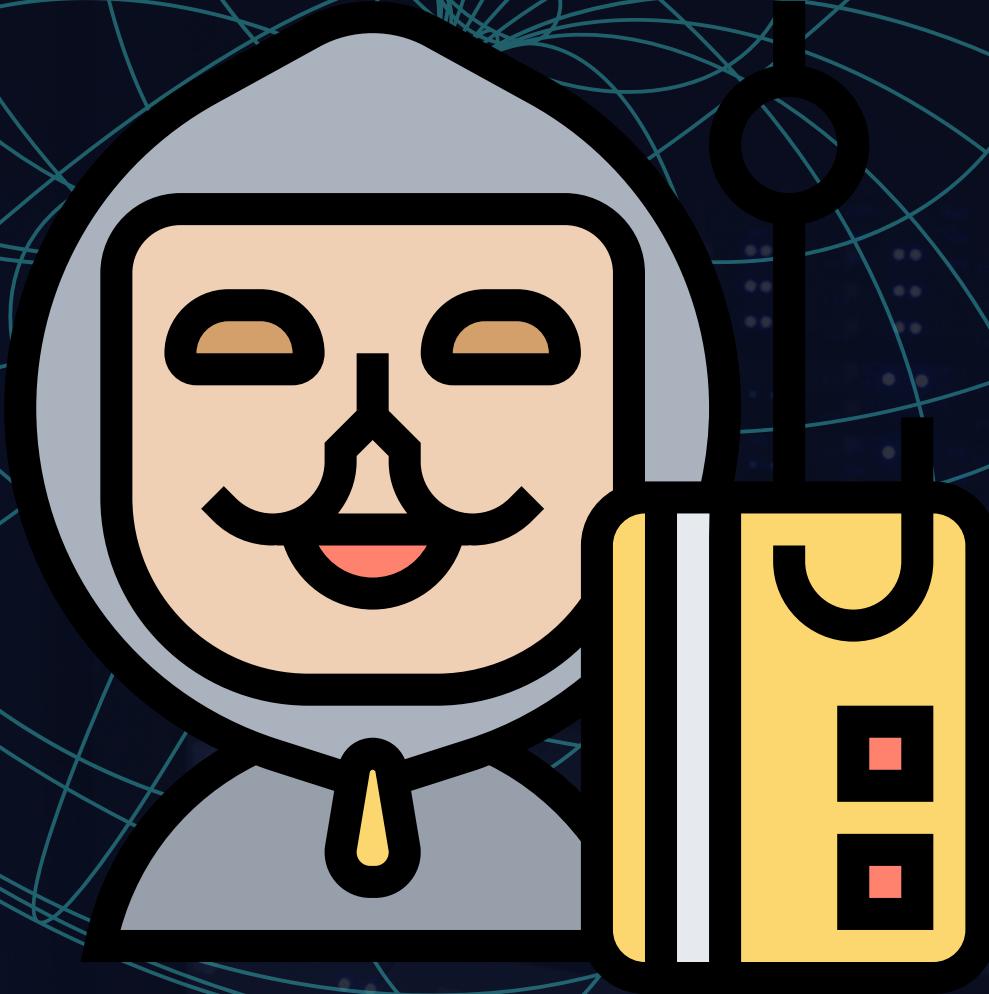


Ingegneria Sociale & Phishing





Quando pensiamo alla cybersecurity, pensiamo soprattutto a come difenderci da hacker che sfruttano le vulnerabilità tecnologiche per attaccare reti di dati.

*Ma c'è un altro modo per penetrare in organizzazioni e reti:
Sfruttare le debolezze umane.*

Questa pratica è nota come ingegneria sociale e si basa sul convincere qualcuno a divulgare informazioni o a concedere l'accesso a reti di dati. Ad esempio, un malintenzionato potrebbe fingersi un tecnico del servizio di assistenza ai clienti per farsi dare informazioni come nome utente o password.

È sorprendente quante persone non riflettano prima di rivelare simili informazioni, soprattutto se la richiesta sembra particolarmente convincente. In parole poche, l'ingegneria sociale è l'uso dell'inganno per manipolare gli individui e convincerli a divulgare informazioni o dati, oppure a garantirvi l'accesso.

INGEGNERIA SOCIALE

L'ingegneria sociale è pericolosa perché rappresenta una forma di manipolazione che sfrutta la psicologia umana per ottenere informazioni riservate, accesso a sistemi informatici o per indurre le persone a compiere azioni indesiderate.

Questa pratica si basa sulla manipolazione delle interazioni sociali e psicologiche piuttosto che sulla violazione diretta dei sistemi informatici.

Ecco alcune ragioni per cui l'ingegneria sociale è considerata pericolosa:

Accesso non autorizzato: Gli attacchi di ingegneria sociale possono portare a un accesso non autorizzato a sistemi, dati o informazioni sensibili. Ad esempio, un attaccante potrebbe fingersi un dipendente aziendale o un amico per ottenere accesso a informazioni riservate.

Violazione della privacy: Gli ingegneri sociali possono manipolare le persone per rivelare informazioni personali o aziendali sensibili. Queste informazioni possono essere utilizzate per scopi dannosi, come il furto di identità o il sabotaggio aziendale.

1. **Diffusione di malware:** Gli attacchi di ingegneria sociale spesso coinvolgono l'invio di contenuti dannosi, come link o allegati, per compromettere i dispositivi delle vittime con malware. Questo può portare al furto di informazioni, al controllo remoto del sistema o ad altri danni.
2. **Induzione di comportamenti dannosi:** I truffatori possono utilizzare l'ingegneria sociale per convincere le persone a compiere azioni dannose, come effettuare trasferimenti di denaro, condividere password o eseguire azioni che compromettono la sicurezza di un'organizzazione.
3. **Minaccia alla sicurezza aziendale:** Le organizzazioni possono essere vulnerabili agli attacchi di ingegneria sociale se i dipendenti non sono consapevoli delle tecniche utilizzate dagli attaccanti. La formazione sulla sicurezza informatica è fondamentale per mitigare questo rischio.
4. **Difficoltà di rilevamento:** Gli attacchi di ingegneria sociale possono essere difficili da rilevare poiché spesso coinvolgono manipolazioni psicologiche piuttosto che azioni tecniche. Le vittime potrebbero non rendersi conto di essere state manipolate fino a quando non è troppo tardi.

Per mitigare il rischio associato all'ingegneria sociale, è importante sensibilizzare le persone riguardo a queste minacce, implementare misure di sicurezza robuste e promuovere buone pratiche di sicurezza informatica all'interno delle organizzazioni.

PHISHING

Il phishing si presenta in vari modi, tra cui e-mail, telefonate, post sui social media e messaggi di testo.

I messaggi di phishing racchiudono tattiche di ingegneria sociale, applicando la finzione, la fiducia e la voglia di cliccare per incoraggiare i destinatari a divulgare informazioni personali, come password e dati della carta di credito.

Gli attacchi phishing sfruttano un'e-mail o un messaggio di testo, apparentemente provenienti da una fonte fidata, che richiedono informazioni.

Un classico sono le mail che sembrano provenire da una banca, che chiede ai propri clienti di "confermare" le informazioni di sicurezza, dirottandoli così su un falso sito dove le credenziali di accesso verranno registrate. Lo "spear phishing" prende di mira una singola persona all'interno di una azienda, inviando una mail che pare provenire da un dirigente di alto livello, che richiede informazioni confidenziali.

E-mail o Messaggio Ingannevole:

Gli attaccanti inviano e-mail o messaggi che sembrano provenire da fonti affidabili, come istituzioni finanziarie, servizi online popolari o aziende con cui la vittima potrebbe avere una relazione.

Contenuto Ingannevole:

Il contenuto del messaggio spesso contiene elementi ingannevoli, come loghi ufficiali, testi persuasivi o richieste di azioni immediate. L'obiettivo è convincere la vittima che il messaggio è autentico.

Richiesta di Azioni Immediate:

Le vittime vengono sollecitate a compiere azioni immediate, come fare clic su un link, inserire informazioni di accesso o scaricare allegati. Queste azioni portano le vittime verso siti Web o risorse controllate dagli attaccanti. ●

Raccolta di Informazioni Sensibili:

Una volta che le vittime seguono le istruzioni, gli attaccanti possono raccogliere informazioni sensibili come nomi utente, password, dati finanziari o altre informazioni personali.

Difese contro il Phishing:

Consapevolezza:

L'istruzione delle persone sulla rilevazione delle e-mail di phishing è fondamentale. Le persone devono essere consapevoli dei segnali di un potenziale attacco, come errori di ortografia, indirizzi e-mail sospetti o richieste di informazioni sensibili.

Verifica delle Fonti:

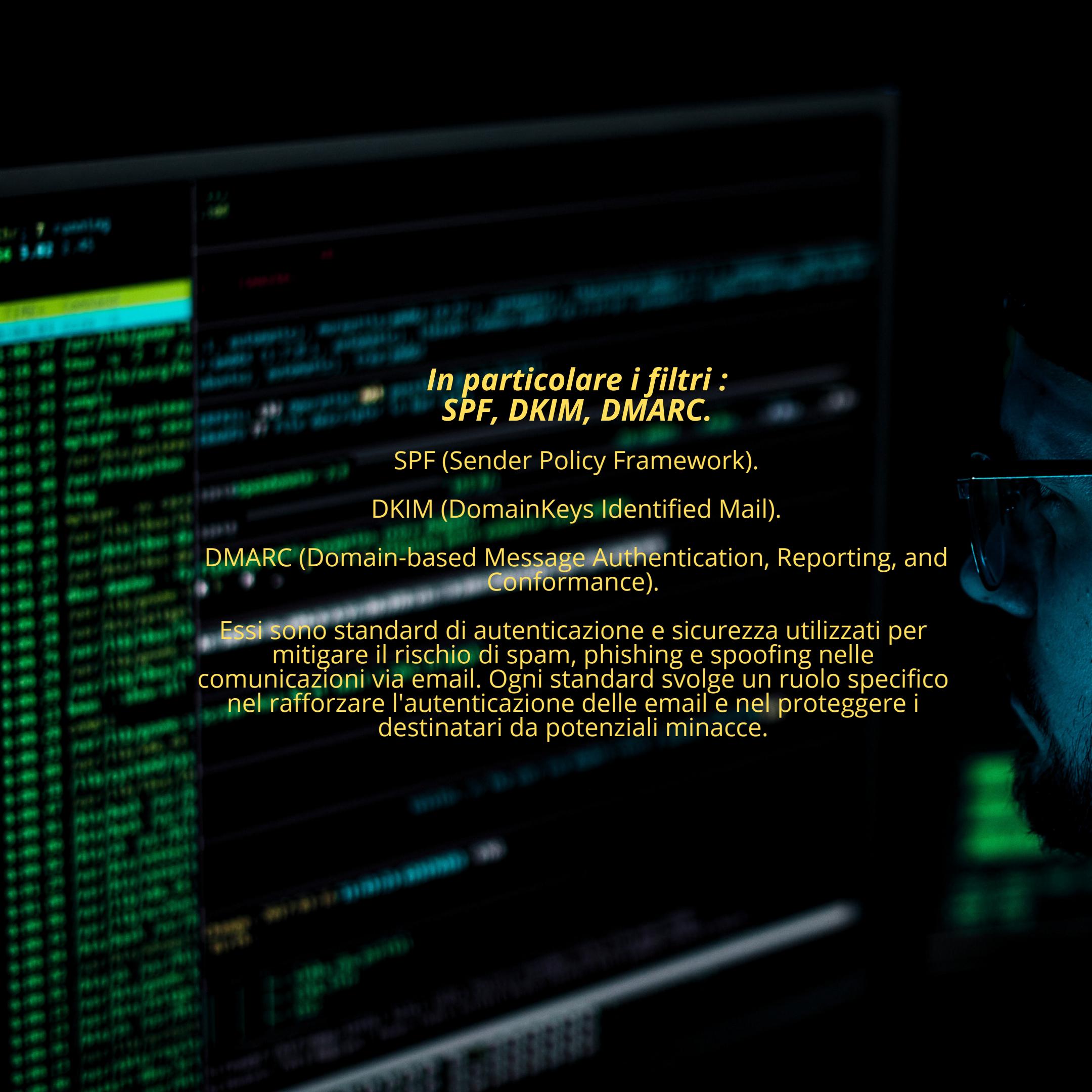
Le vittime devono verificare attentamente la fonte del messaggio, specialmente quando si tratta di richieste di informazioni sensibili. La verifica può includere contattare direttamente l'azienda o l'organizzazione apparentemente coinvolta.

Uso di Filtri Anti-Phishing:

L'utilizzo di filtri anti-phishing può aiutare a bloccare e-mail sospette prima che raggiungano le caselle di posta degli utenti.

Autenticazione Multifattore (MFA):

L'implementazione di MFA può aggiungere uno strato di sicurezza, anche se le credenziali vengono compromesse.

A close-up photograph of a person's face, partially obscured by dark sunglasses, looking intently at a computer monitor. The monitor displays a grid of green and blue text, likely code or log entries, which is slightly blurred. The overall lighting is low, creating a focused and mysterious atmosphere.

In particolare i filtri : SPF, DKIM, DMARC.

SPF (Sender Policy Framework).

DKIM (DomainKeys Identified Mail).

DMARC (Domain-based Message Authentication, Reporting, and Conformance).

Essi sono standard di autenticazione e sicurezza utilizzati per mitigare il rischio di spam, phishing e spoofing nelle comunicazioni via email. Ogni standard svolge un ruolo specifico nel rafforzare l'autenticazione delle email e nel proteggere i destinatari da potenziali minacce.

SPF

Sender Policy Framework

è un'e-mail metodo di autenticazione che garantisce che il server di posta mittente sia autorizzato a originare la posta dal dominio del mittente dell'e-mail. Questa autenticazione si applica solo al mittente dell'e-mail elencato nella "busta da" campo durante la connessione SMTP iniziale.

DKIM

(DomainKeys Identified Mail)

è un metodo di autenticazione e-mail standard che aggiunge una firma digitale ai messaggi in uscita. I server di posta riceventi che ricevono i messaggi firmati con DKIM possono verificare che i messaggi provengano effettivamente dal mittente e non da qualcuno che si spaccia per il mittente.

DMARC

(Domain-based Message Authentication, Reporting, and Conformance).

Autenticazione, reporting e conformità dei messaggi basati sul dominio (DMARC) è un Protocollo autenticazione e-mail. È progettato per offrire ai proprietari di domini di posta elettronica la possibilità di proteggere il proprio dominio dall'uso non autorizzato, comunemente noto come spoofing di posta elettronica. Lo scopo e il risultato principale dell'implementazione di DMARC è proteggere un dominio dall'utilizzo in attacchi di compromissione della posta elettronica aziendale, phishing_email, truffe via email e altre minacce informatiche attività.

INIZIAMO CON IL TEST !!!

Dopo essermi messo d'accordo con il direttore , metteremo alla prova i dipendenti mandando loro una mail di phishing creata da noi

Invieremo loro una e-mail dove cercheremo di trarre in inganno i dipendenti, ad esempio comunicheremo loro che per un aggiornamento appena effettuato , dovranno ripetere l'accesso alla loro piattaforma. useremo una mail quasi uguale a quella loro , ovvero useremo Epicodesecurity@semofort.com l'unica differenza con quella originale è la mancanza una lettera nella seconda parte della e-mail . nella nostra falsa e-mail ci sarà un link che li porterà presso la loro schermata login , a primo impatto la pagina web risulterà identica all'originale.

La differenza sta nel URL , perché quello creato da noi , risulterà non sicuro . Lo scopo del test è dimostrare ai propri dipendenti come prevenire un phishing . Quindi , l'obiettivo dovranno verificare la provenienza dell' e-mail tramite "mostra originale " , capiranno che non si ha l'autorizzazione dell' SPF e neanche da DKIM e Dmarc.

(Ovviamente non ruberemo i dati di accesso di nessun dipendente , servirà solo a scopo formativo e a prevenire determinati attacchi informatici)

Foto di repertorio:

ID messaggio	<0102017dfdbd8244-985293aa-0b28-4ff9-a95e-06a42f49964f-000000@eu-west-1.amazonaws.com>
Creato alle:	27 dicembre 2021 alle ore 22:13 (consegnato dopo 0 secondi)
Da:	"Amazon.it" <conferma-spedizione@amazon.it>
A:	manuelpinto1408@gmail.com
Oggetto:	Il tuo ordine Amazon.it di "TP-Link TL-WPA7517 Kit..." è stato spedito.
SPF:	PASS con l'IP 54.240.1.118 Ulteriori informazioni
DKIM:	'PASS' con il dominio amazon.it Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

[Scarica messaggio originale](#)

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..."

[Scarica messaggio originale](#)

[Copia negli appunti](#)

```

Return-Path: <pcroad1408@gmail.com>
Received: from Amm01 ([51.179.99.160])
by smtp.gmail.com with ESMTPSA id w10-20020a05600c474a00b0040b2c195523sm25514056wmo.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-Original-From: test@gmail.com
Mime-Version: 1.0
Date: Thu, 14 Dec 2023 07:36:05 +0100
X-Mailer: gophish
Message-Id: <1702535764885356600.6332.8543051994045262048@Amm01>
Subject: Il tuo ordine Amazon.it che include "TP-Link TL-WPA7517 Kit..."
To: Manuel Pinto <pcroad1408@gmail.com>
Content-Type: multipart/alternative; boundary=aa11febf883667e105310ba87ac20e2ee62277d8b0a69861a4262f9eff1d

```