

# CORSO INGEGNERIA SOCIALE



01

Epcodesecurity  
[www.Epcodesecurity.it](http://www.Epcodesecurity.it)  
Epcodesecurity@semoforti.com

## CHE COS'E' INGEGNERIA SOCIALE?

L'ingegneria sociale è una forma di manipolazione psicologica in cui gli attaccanti cercano di ottenere informazioni sensibili o indurre le persone a compiere determinate azioni attraverso l'inganno.

In sostanza, si tratta di sfruttare gli aspetti sociali e psicologici per raggiungere scopi malevoli, come l'accesso non autorizzato a informazioni riservate o sistemi informatici.

## INGEGNERIA SOCIALE: VERI E PROPRI ATTACCHI

Gli attacchi di ingegneria sociale sono veri e propri attacchi, la maggior parte delle volte ha a che fare con i PHISHING, email malevole.

## MA PERCHE' SONO COSÌ PERICOLOSI?

**Fiducia e Autorità:**

**Scarsa Consapevolezza:**

**Difficoltà nella Difesa  
Tecnologica:**

**Flessibilità e  
Adattabilità:**

## ALCUNI ESEMPI DI PHISHING:

E-mail o  
Messaggio Ingannevole

Richiesta di Azioni  
Immediate

Contenuto Ingannevole

Raccolta di Informazioni  
Sensibili

## QUINDI COME CI SI PUO' DIFENDERE?

Consapevolezza:

Verifica delle Fonti

Uso di Filtri  
Anti-Phishing:

Autenticazione  
Multifattore (MFA)

In particolare  
i filtri

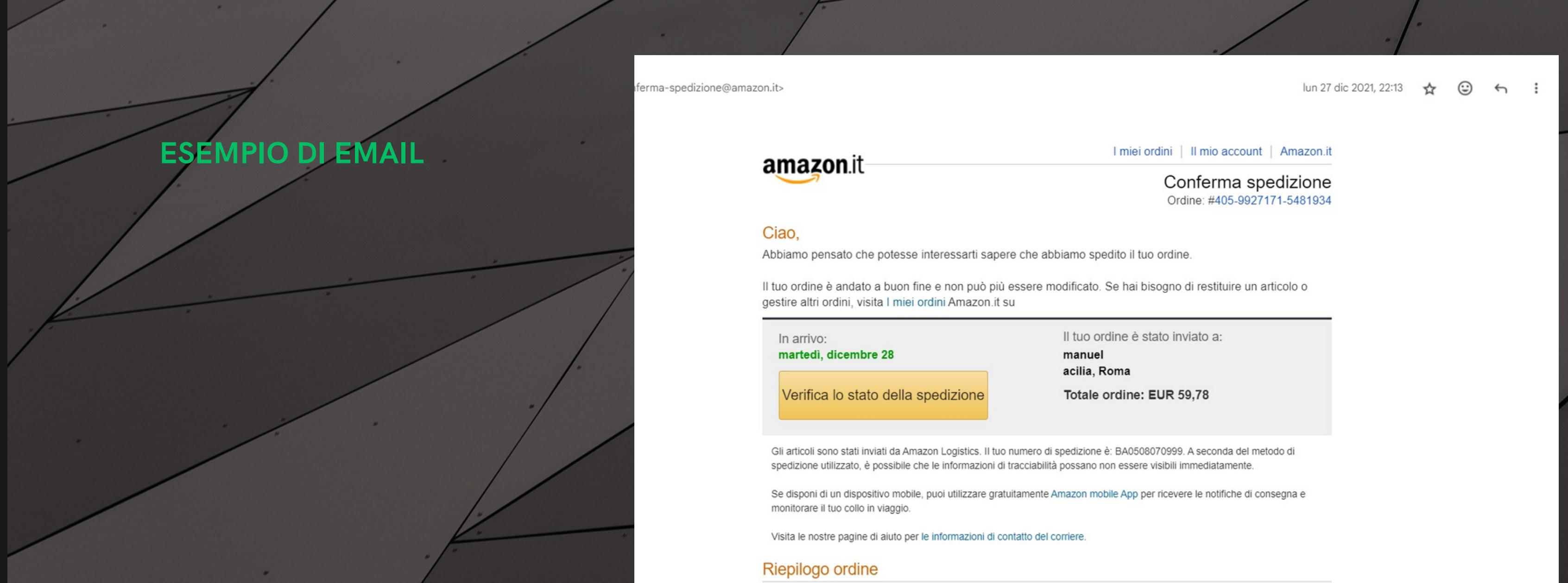
VEDIAMO I FILTRI IN PARTICOLARE:

● SPF (Sender Policy Framework).

● DKIM (DomainKeys Identified Mail).

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

# SIMULAZIONE DI PHISHING



## ESEMPIO DI EMAIL

### Messaggio originale

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 <a href="#">Ulteriori informazioni</a>
DKIM:	'PASS' con il dominio amazon.it <a href="#">Ulteriori informazioni</a>
DMARC:	'PASS' <a href="#">Ulteriori informazioni</a>

Vedremo che tutti i filtri avranno una scritta affianco con "PASS" il che significa che l'email ha superato il filtraggio.

## ESEMPIO DI EMAIL

### 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..."
```

**E' possibile notare che i filtri non sono presenti. E l'email del mittente è sospetta: l'email dovrebbe essere inviata da Amazon ma vediamo invece un indirizzo totalmente diverso.**

## METTIAMO ALLA PROVA I DIPENDENTI

(Il direttore mi ha conferito il permesso di creare un phishing controllato per mettere alla prova i dipendenti)

Simulerò un PHISHING all'azienda di EpicodeSecurity e invierò una email ai dipendenti.

In esso viene offerto un bonus di 500 euro per il "lavoro svolto con successo", cliccando sul link.

Tale email sarà sicuramente molto simile all' originale, ad esempio "Epicodesecuriti@semoforti.it" (Dominio diverso, quindi verificare bene) e il link sarà simile a "<https://www.bonus500dipendenti.it/>"

Nella mail ci sarà un link che indirizza sulla pagina copiata del sito che offre il bonus, e chiederò di inserire i dati di accesso.

Ovviamente se un dipendente dovesse sbagliare non ci saranno gravi conseguenze.

**OBIETTIVO:** Far sì che i dipendenti siano coscienti delle loro azioni, e di prevenire danni da PHISHING

**NOTE: Se si dovesse aprire l'email malevola in questo caso non succederebbe nulla, in quanto autorizzato a creare un "PHISHING innoquo". Tuttavia un PHISHING vero costituisce un pericolo. Sempre attenzione alle email che aprite!!**