**Progetto per Epicodesecurity**

Siete stati chiamati da un'azienda di nome **Epicodesecurity,** questa azienda ha un sito web suo personale con il nome di dominio **www.Epicodesecurity.it**. un server email con l’email aziendale Epicodesecurity@semoforti.com

Il progetto prevede la formazione dei dipendenti dell’azienda attraverso un corso online che verrà sottoposto a tutti i dipendenti nello stesso momento. Al termine del corso verrà eseguito un test per verificare le competenze che hanno appreso i dipendenti.

Nei mesi successivi verranno proposti a campione dei test ai dipendenti (a loro insaputa) per verificare che la formazione intercorsa sia stata utile e recepita.

Il corso prevede questo tipo di percorso:

* Che cosa sono gli attacchi di ingegneria sociale
* Quali sono i tipi di attacchi di ingegneria sociale
* Come identificare gli attacchi informatici di ingegneria sociale
* Test di verifica delle competenze apprese

Successivamente, come da accordi con il direttore di Epicodesecurity verranno effettuati i test controllati per verificare che i dipendenti abbiano recepito le nozioni presentate

Programma del corso:

* Definizione di **ingegneria sociale** e di attacchi di 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, la manipolazione e l'uso delle relazioni umane. 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

Il tipo di attacco più importante e diffuso è quello del **phishing**.

Il phishing coinvolge l'invio di e-mail o messaggi ingannevoli che cercano di indurre le persone a rivelare informazioni personali, come nomi utente, password o dati finanziari.

Questo attacco sfrutta la fiducia della vittima, convincendola erroneamente che il messaggio provenga da una fonte affidabile o legittima.

* 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.

Le migliori difese contro il phishing ad oggi sono:

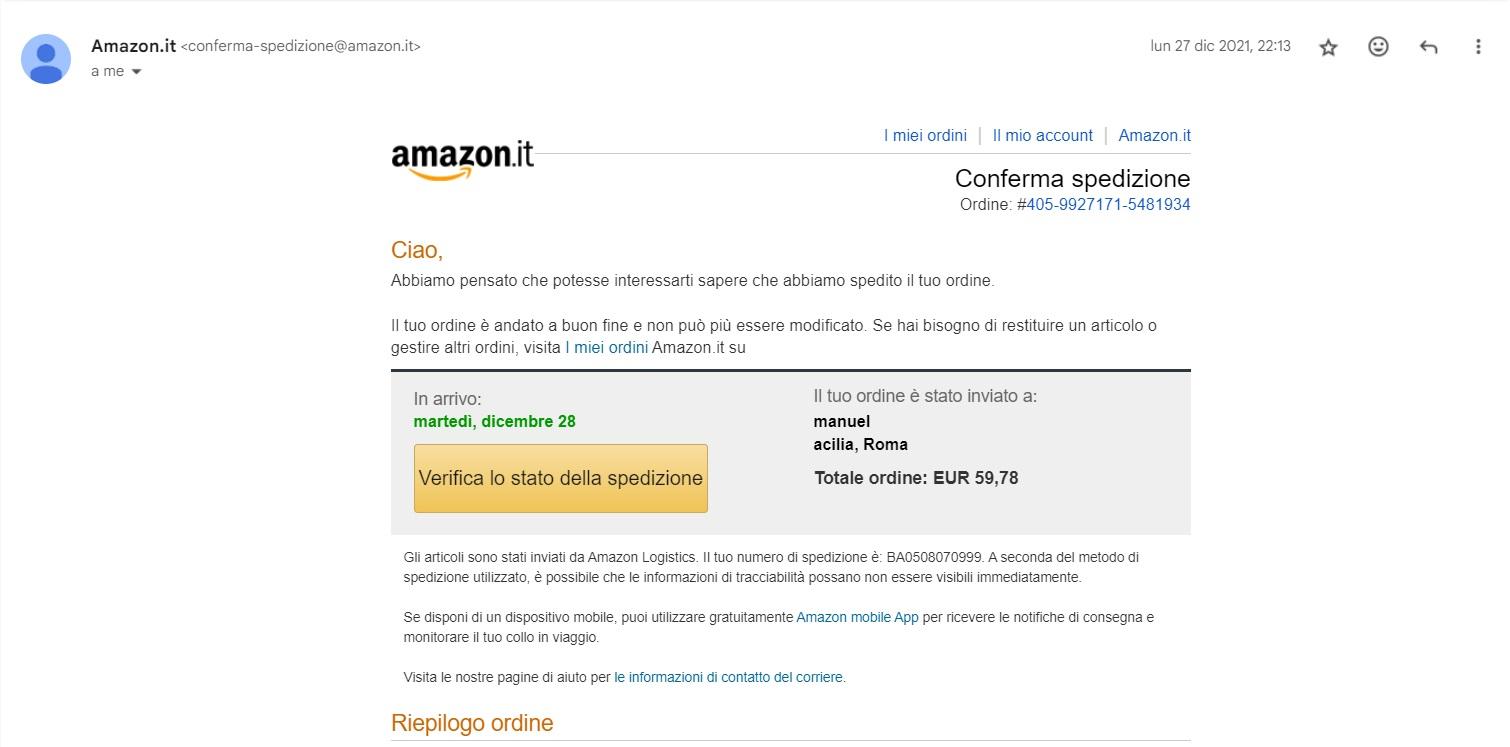
* Consapevolezza:L'istruzione delle persone sulla rilevazione delle e-mail di phishing è fondamentale. Le persone devono essere consapevoli dei segnali di un potenziale attacco, come errori di ortografia, indirizzi e-mail sospetti o richieste di informazioni sensibili.
* Verifica delle Fonti: Le vittime 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.
* In particolare i filtri : ○ SPF, DKIM, DMARC.

Ora che sono stati spiegati i concetti principali riguardanti l’ingegneria sociale andremo a vedere un esempio pratico.

L’esempio che prenderemo in considerazione oggi è la ricezione di un pacco da parte di amazon.

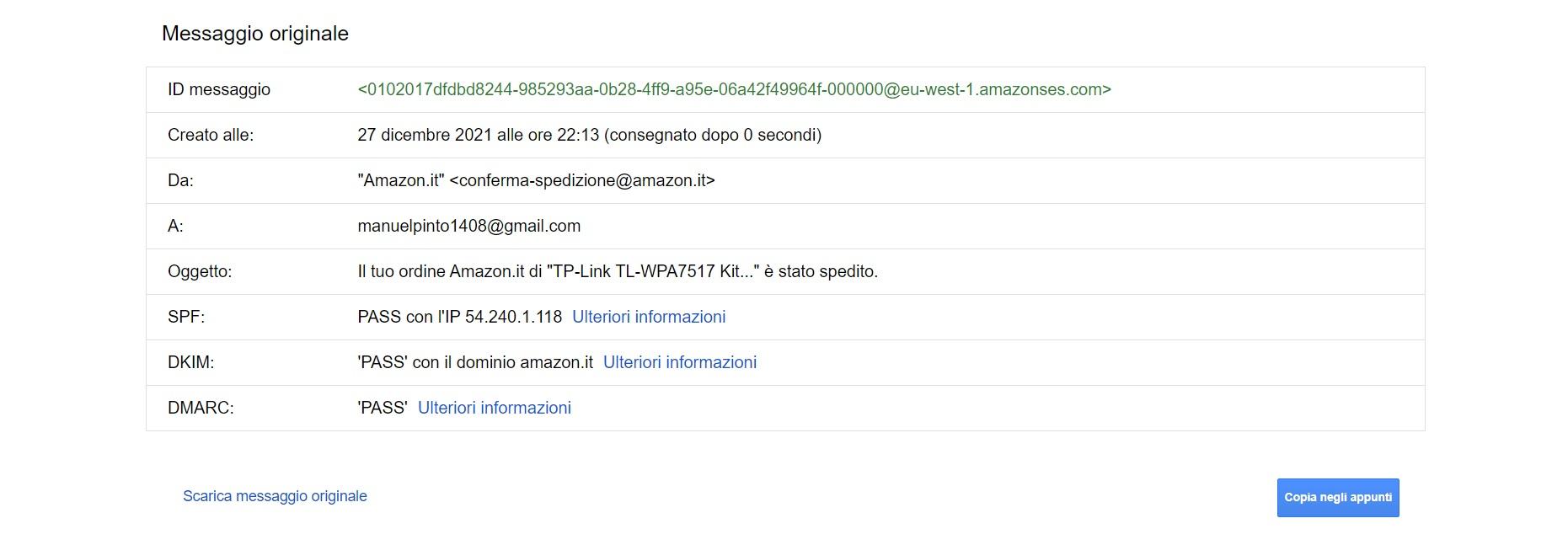
Il metodo più indicato per verificare e prevenire il phishing è verificare determinati parametri o filtri quali SPF, DKIM, DMARC.

Questa è la mai che prenderemo in considerazione:



E’ un semplice ordine di amazon; per verificare i parametri occorre cliccare in alto a destra i tre puntini e cliccare “mostra originale”

Qui verrà mostrata una schermata di questo tipo:



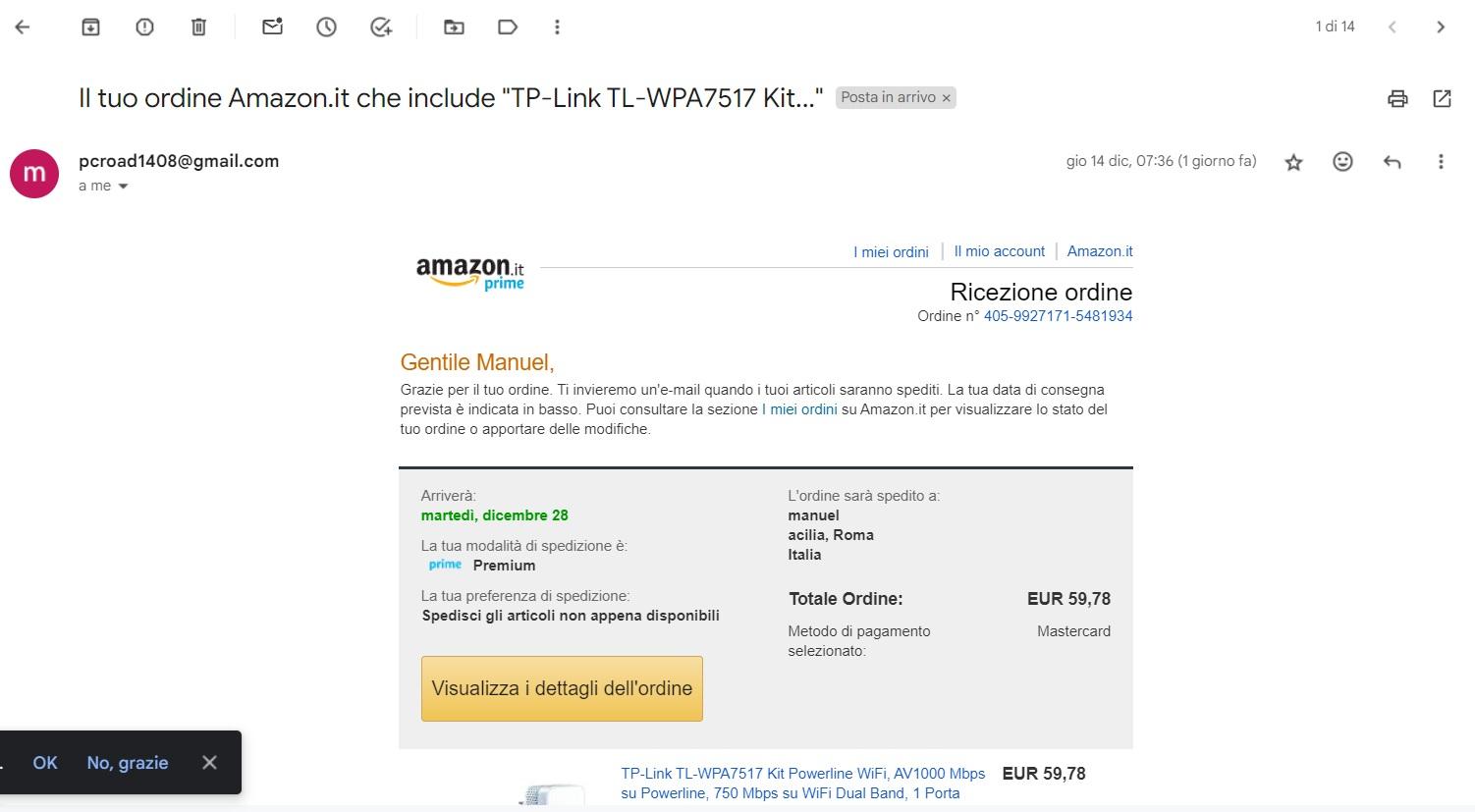
Come è possibile notare, ci sono i 3 filtri che abbiamo visto in precedenza:

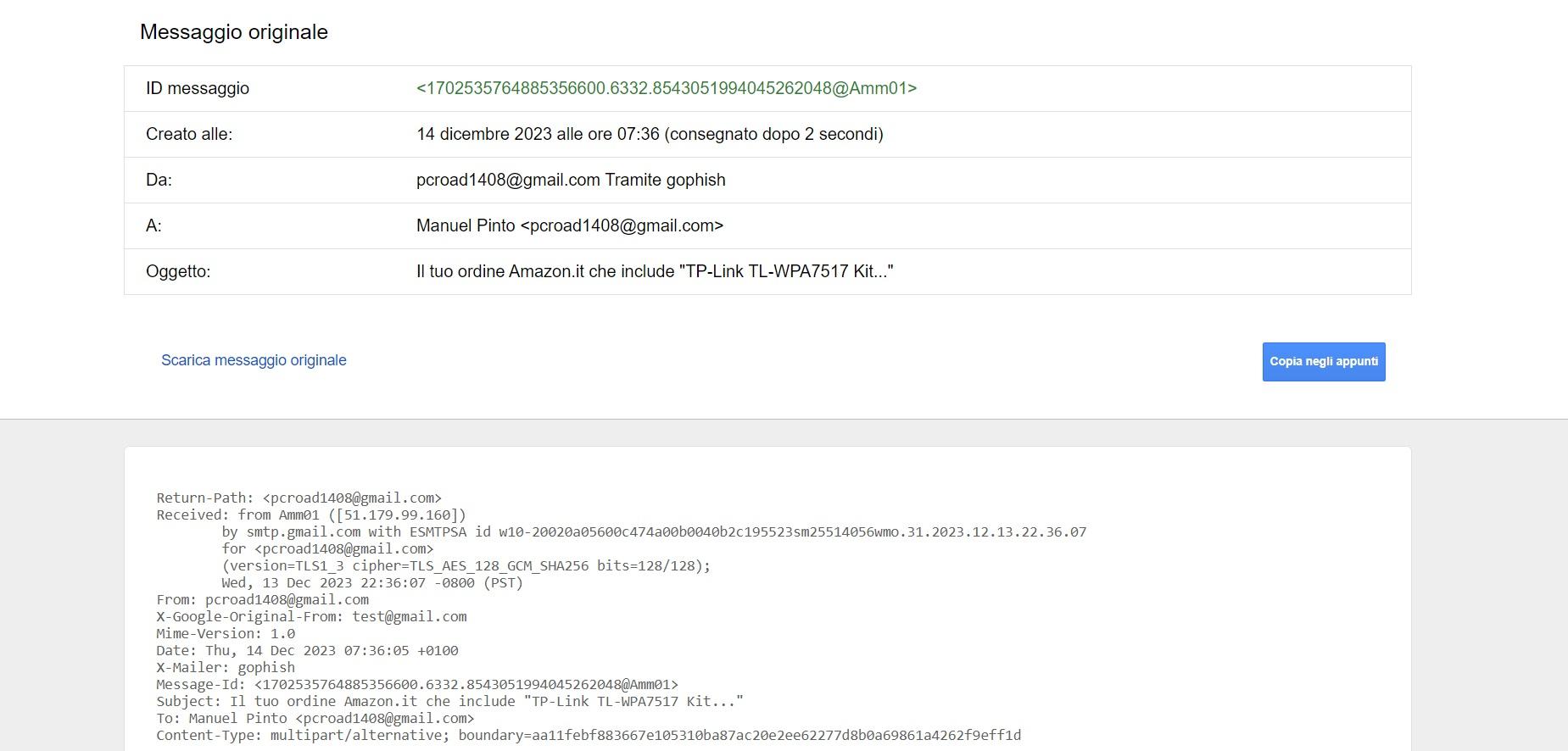
sono standard di autenticazione e sicurezza utilizzati per mitigare il rischio di spam, phishing e spoofing nelle comunicazioni via email. Ogni standard svolge un ruolo specifico nel rafforzare l'autenticazione delle email e nel proteggere i destinatari da potenziali minacce.

I due filtri più importanti sono l’SPF, verifica che l'indirizzo IP che invia un'email sia autorizzato a farlo per conto del dominio specificato e il DKIM che va a garantire l'integrità e l'autenticità del contenuto di un'email mediante la firma digitale.

La prima verifica da fare è che il mittente sia davvero quello che vi sta scrivendo, in questo caso amazon è confermato perchè stiamo ricevendo un mail da amazon.

Adesso vediamo un esempio di un’email di phishing e vedremo le varie differenze.





Come possiamo notare le due mail sono completamente uguali graficamente, ma come abbiamo visto con il metodo precedente, andando ad analizzare il codice sorgente notiamo che i 3 filtri sono mancanti.

La mancanza di questi 3 filtri e il nome del mittente diverso dalla mail ricevuta bastano per dichiarare un’email come poco sicura e potenzialmente pericolosa o affetta da malware.

In questo caso occorre eliminare immediatamente la mail senza cliccare su nessuna parte o link della mail e segnalare come phishing.

Successivamente a questo corso sugli attacchi dell’ingegneria sociale il personale verrà testato con un quiz a scelta multipla.

Nei mesi successivi verrà invece sostenuto un test a campione, questo test sarà una finta mail di phishing.

Il progetto di questa campagna sarà basato su un ipotetico “rinnovo” delle credenziali per accedere alla piattaforma online dell’azienda.

La mail sembrerà una mail inviata dall’azienda stessa (ovviamente sotto copertura), così da verificare che all’invio di dati sensibili come credenziali di accesso alla piattaforma aziendale, ci sia una soglia di attenzione più elevata da parte del personale dell’azienda stessa.

Il programma utilizzato per la gestione del phishing è Gophish, un software particolarmente sicuro pensato proprio per questo tipo di test.

L’obiettivo è quello di creare una mail e osservare che il domain che invia la mail non appartiene al server di posta dell’azienda, ovvero:[**www.Epicodesecurity.it**](http://www.epicodesecurity.it).

Una volta verificato questo, occorre verificare se i filtri sono presenti o meno.

Il direttore deciderà a sua volta che tipo di provvedimenti instaurare con il personale che non supera il test.