Vademecum

Come riconoscere email false

A cura del ***CED***
Centro Elaborazione Dati
Seac Confcommercio
Umbria

Una serie di pratici consigli per evitare di cadere vittima di messaggi di posta creati per ingannarvi!

Anche se i tempi sono cambiati, il classico "messaggio di posta" è sempre il mezzo preferito dai malintenzionati per trarre in inganno ignari utenti ed indurli a rivelare informazioni sensibili, mettendo in pericolo aspetti più o meno importanti della propria vita, **o scaricare e/o installare programmi assolutamente nocivi.**

Ecco allora una serie di indicazioni per riconoscere email false nel minor tempo possibile, analizzando i vari aspetti del messaggio.

In verità non esiste una scienza esatta che aiuti a comprendere se un messaggio di posta elettronica sia genuino o fasullo, ma basta allenare un po' 'occhio per essere in grado, dopo qualche tempo, di rendersi conto al volo di un eventuale tentativo di spam o phishing.

Prima di continuare, vi raccomandiamo fortemente di tenere il mouse lontano dal corpo del messaggio e dalla sezione "allegati" e di non scaricare file o visitare pagine web elencate nel messaggio prima di aver verificato la sua effettiva veridicità.

Il mittente

L'analisi del mittente può rappresentare da subito un metodo per cestinare immediatamente l'email falsa.

Uno degli attacchi che viene condotto prevalentemente con le email è il cosiddetto **tentativo di phishing,** nel quale i malintenzionati tentano prevalentemente di:

- **fingersi la vostra banca** (o il vostro istituto di credito in generale) per rubare le vostre credenziali d'accesso;
- **fingersi un portale web celebre** (ad esempio Google) per rubare le vostre credenziali d'accesso;

- **fingersi un gestore password** (ad esempio Lastpass) per rubare le vostre password…

o tentativi simili.

La prima cosa che dovete fare è guardare bene l'indirizzo del mittente e cercare di comprendere a colpo d'occhio se si tratta di un indirizzo fasullo.

Facciamo un esempio: *il sito di riferimento per l'istituto di credito Banca Sella è "bancasella.it", tuttavia potreste ricevere una email da qualcosa come verifica@banca-sella.it. Quel trattino tra le parole "banca" e "sella", che non dovrebbe esserci, vi dice immediatamente che si tratta di un messaggio di posta fasullo e potrete cestinare il messaggio.*

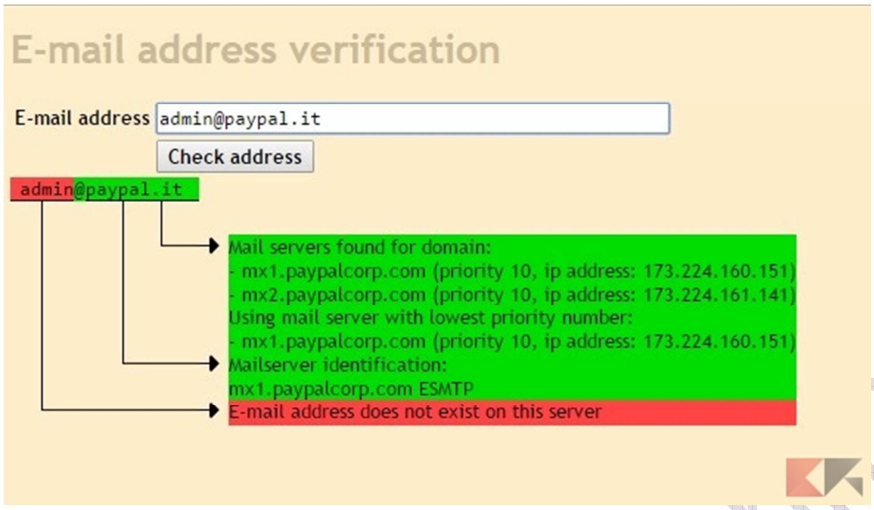
Nell'immagine a seguire, il messaggio (che continueremo a prendere in esame) vorrebbe farci credere di provenire da Intesa Sanpaolo ma in realtà arriva da un certo "admin@focogroup.com", visibilmente differente. Si tratta certamente di un tentativo di phishing, anche perché Intesa Sanpaolo non è il mio istituto di credito né lo è mai stato.

Altri domini che i phisher usano per inviare email false sono:

- **@contobancoposta.it** e tutte le sue varianti (falso, poiché le comunicazioni ufficiali arrivano esclusivamente dal dominio @poste.it);
- **@paypal.it** (falso, in quanto le comunicazioni da PayPal arrivano usando il dominio commerciale @paypal.com);
- **@poste-italiane.it**, **@xxx-poste.it** e simili.

Purtroppo esistono metodi per falsificare il mittente di un messaggio di posta poiché non sempre vengono effettuati i controlli del caso in fase di ricezione, dunque **potreste ritrovarvi un messaggio di posta falso che sembra vero**.
Se avete questo sospetto, allora **potrete verificare l'effettiva esistenza del mittente utilizzando il servizio online Mailtester.**

http://www.mailtester.com/testmail.php

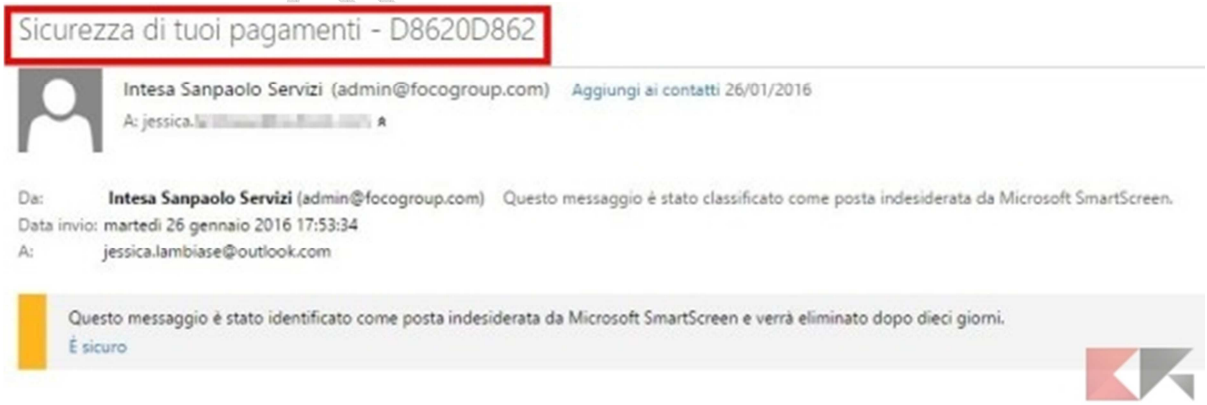


Se qualsiasi altro campo dovesse essere in giallo, cestinate comunque il messaggio.

L'oggetto del messaggio

I falsari usano spesso degli oggetti d'impatto per attirare gli ignari utenti nelle loro trappole: se parla di un'eredità ricevuta da un lontano parente di cui non avete mai sentito parlare, se vi viene offerta una somma in denaro, se vi parla di reimpostare una password (senza che voi lo abbiate mai chiesto) ed altre informazioni o richieste bislacche, magari in una lingua diversa dalla vostra lingua madre, nel 99% delle probabilità si tratta di spam o phishing.

Nell'esempio in basso, "Sicurezza di tuoi pagamenti" non è di certo una frase scritta in italiano corretto.



Il corpo del messaggio - La forma

Prima di tutto, leggete ciò che c'è scritto **(senza cliccare in alcun posto)**: se l'email è scritta nella vostra lingua madre analizzate il corpo del messaggio alla ricerca di errori

grammaticali, richieste assurde o qualsiasi altro elemento che vi insospettisca. **Solitamente, i messaggi di spam o phishing sono scritti usando un linguaggio scorretto,** spesso risultato di una traduzione da altra lingua. Se è il vostro caso, cestinate senza andare avanti.

Il corpo del messaggio - Il contenuto

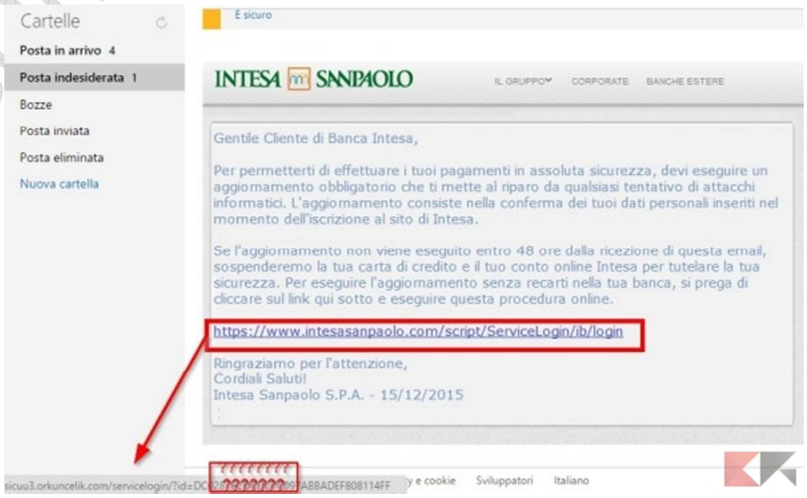
A questo punto arriva **la prova del 9** e dovete chiedervi:

- questo messaggio mi chiede di cliccare da qualche parte per verifiche o reimpostazioni di password, credenziali o altro?
- questo messaggio mi chiede di scaricare un allegato che io non ho mai richiesto e che non mi aspettavo?
- questo messaggio mi chiede un indirizzo o gli estremi del conto in banca o della carta di credito affinché io possa ricevere merce inattesa o denaro?

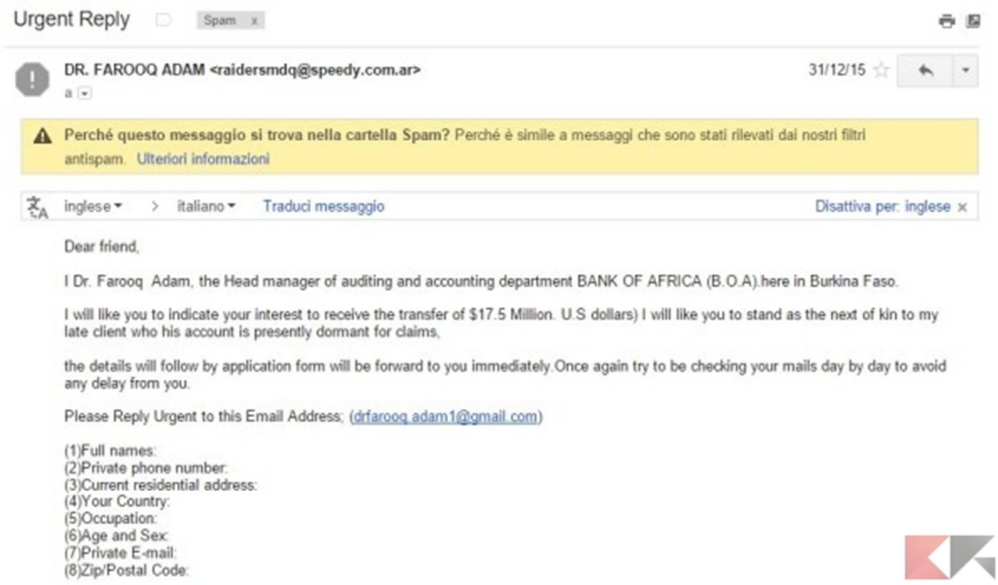
Se almeno una di queste risposte è si, cestinate il messaggio immediatamente: a questo punto le probabilità che si tratti di un tentativo di phishing sono altissime.

Nella foto in basso, ad esempio, la presunta Intesa Sanpaolo vorrebbe farmi credere che dovrei aggiornare il mio conto per evitarne la chiusura, una procedura che MAI un istituto di credito svolgerebbe telematicamente ma richiederebbe la presenza fisica del titolare del conto.

Inoltre, l'avviso mi chiede di inserire le mie credenziali su un sito web che sembra portare ad Intesa Sanpaolo, ma basta soltanto posizionare il mouse sul link cliccabile (SENZA farci click) e guardare in basso a sinistra per rendersi conto che il link ci porterà ad una pagina ben diversa da quella di Intesa Sanpaolo, pagina piuttosto strana.



Il messaggio in basso vuole invece farmi credere di dover ricevere dei soldi da una banca sita in Burkina Faso e richiede delle informazioni per iniziare la transazione. Si tratta ovviamente di un messaggio di phishing, come specifica anche Google.



Infine, se il messaggio è scritto in una lingua diversa dalla vostra e/o ha un tono confidenziale (ad esempio: "Ciao, ti ricordi di me?" oppure "Sono in cerca di amicizie, vogliamo socializzare?" o ancora "Ho bisogno di aiuto per questa causa, mi mandi il tuo indirizzo?") **cestinatelo senza remore.**

Un esempio è quello in basso, che mi son ritrovata nella cartella spam e che… beh, è abbastanza eloquente!

Ho ricevuto una email falsa, cosa faccio dopo averla cestinata?

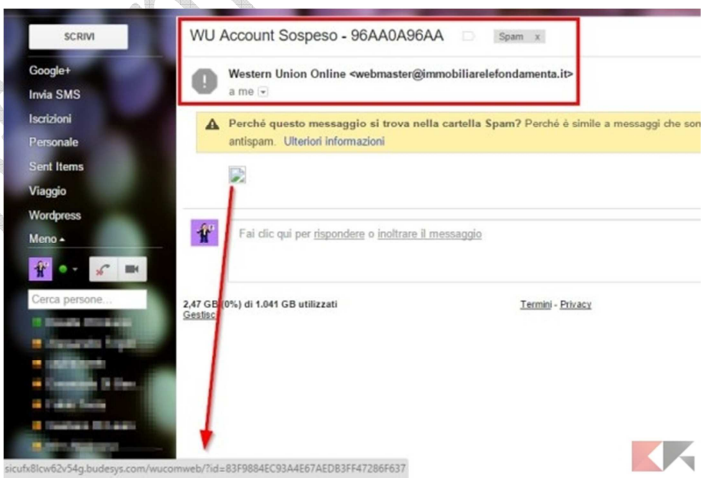
Aiutandovi con le funzionalità del gestore di posta o del programma usato per leggerla, vi

consiglio di **bloccare il destinatario e dirottare i suoi messaggi direttamente nel cestino o, meglio ancora, aggiungerlo ad una lista nera per non ricevere più suoi messaggi.**

Mi sono accorto tardi di esserci cascato. E ora ?

A seconda del tipo di messaggio falso, **le conseguenze della vostra distrazione potrebbero essere più o meno gravi.** Vediamo come comportarci:

- se avete scaricato ed eseguito un allegato, riavviate immediatamente il computer in
- modalità provvisoria ed effettuate una scansione con un antivirus che sarà in grado di rilevare ed annullare eventuali minacce, dopodiché assicuratevi di cambiare la password di sistema e qualsiasi altra password abbiate digitato dopo l'infezione;
- se avete scaricato ed eseguito un allegato e contratto un ransomware, ovvero vi ritrovate con una richiesta di riscatto per ri-ottenere i vostri dati, rivolgetevi immediatamente ad un esperto;
- se avete inserito nome utente, password o altre informazioni in una pagina web sospetta, contattate immediatamente il vostro istituto di credito o il servizio di cui avete svelato le credenziali e raccontate l'accaduto al team di assistenza; loro sapranno come limitare i danni delle vostre azioni.



Concludendo…

Come si accennava ad inizio articolo, **stare lontani dai tentativi di phishing e dai messaggi di spam non rappresenta una scienza esatta ma, col passare del tempo, saranno il nostro buon senso e la nostra esperienza vissuta a permetterci di riconoscere email false dando**

loro soltanto uno sguardo fugace.
Ricordate sempre che con l'evolversi della tecnologia si evolvono anche i metodi usati dai malintenzionati, che col passare del tempo diventano sempre più fini e sofisticati: quindi, occhi sempre aperti e dita sempre lontane dai click o dai tap potenzialmente nocivi!