Guida all'uso della posta elettronica

Sommario

Premessa

Il classico “messaggio di posta” è sempre il mezzo preferito dai malintenzionati per trarre in inganno gli utenti ed indurli a rivelare informazioni sensibili, mettendo in pericolo aspetti più o meno importanti della propria vita, o a scaricare e/o installare programmi nocivi.

In realtà non esiste una scienza esatta che aiuti a comprendere se un messaggio di posta elettronica sia genuino o fasullo. E’ però possibile prestare attenzione ad alcuni elementi di seguito illustrati per poter accorgersi di eventuali tentativi di spam o phishing (o almeno quelli più evidenti ed evitabili).

La prima raccomandazione è quella 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 l’effettiva veridicità.

Come riconoscere email false

Il mittente

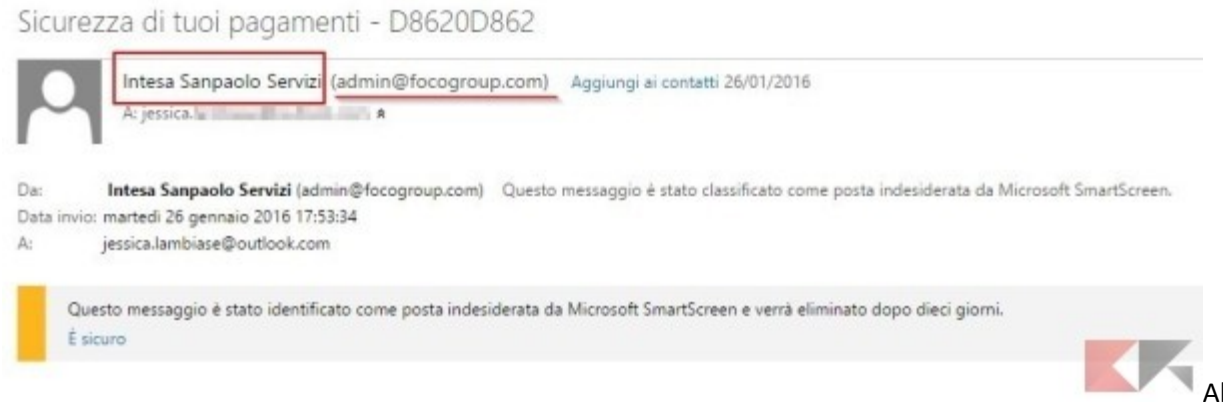
Tra gli elementi di un messaggio di posta è quello che balza immediatamente all’occhio: spesso i messaggi di spam arrivano a nome di aziende (a volte anche celebri) o persone completamente sconosciute e, in tal caso, se vi siete affidati ad un gestore di posta affidabile (ad esempio Gmail, Outlook o servizi simili), le probabilità che non vediate mai quel messaggio sono alte poiché potrebbe già essere stato spostato tra i messaggi di spam.

Il caso in cui l’analisi del mittente può rappresentare da subito un metodo per cestinare immediatamente l’email falsa 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…
- tentativi simili ai precedenti.

La prima cosa che dovete fare per riconoscere email false di questo tipo è **guardare bene l’indirizzo del mittente e cercare di comprendere** se si tratta di un indirizzo fasullo; ad 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, in tal caso vi dice immediatamente che si tratta di un messaggio di posta fasullo e potrete cestinare il messaggio.

Nella foto in basso, ad esempio, il messaggio (che continueremo a prendere in esame) vorrebbe farmi 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 di esempio 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.

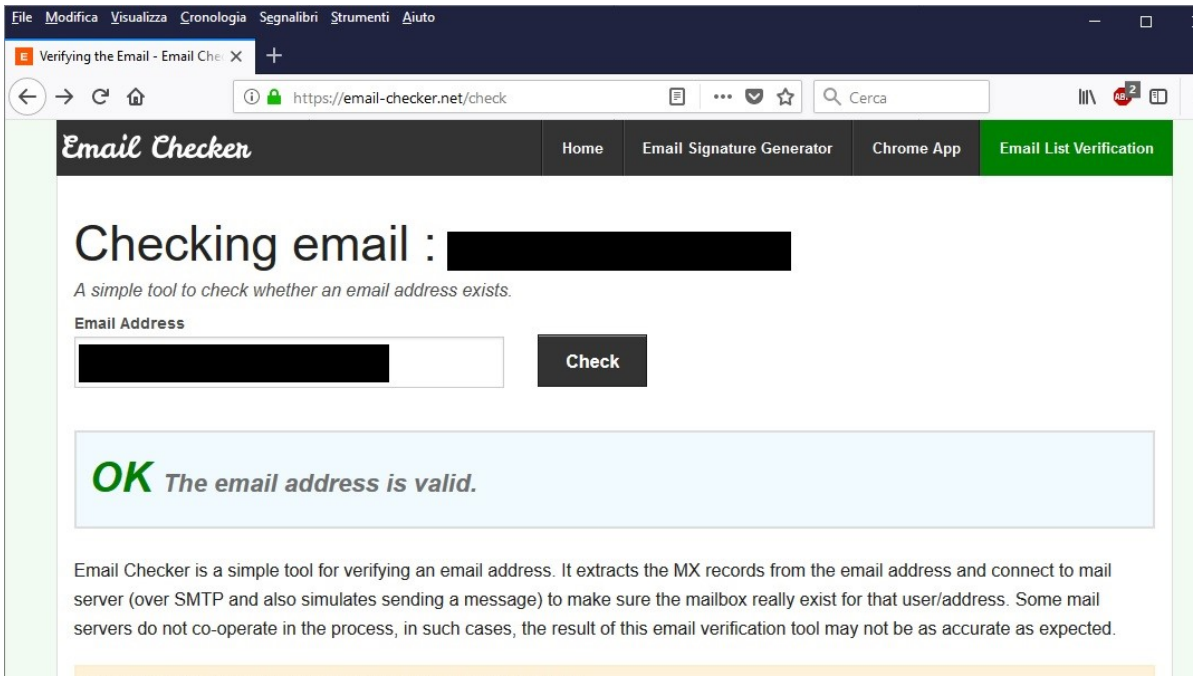
Purtroppo esistono dei metodi per falsificare il mittente di un messaggio di posta poiché non sempre vengono effettuati i controlli del caso in fase di ricezione: dunque potreste ritrovarvi un messaggio di posta falso che sembra vero.

Se avete questo sospetto, **allora potrete verificare l'effettiva esistenza del mittente utilizzando no dei servizi online per effettuare i test sull'esistenza degli indirizzi di posta.**

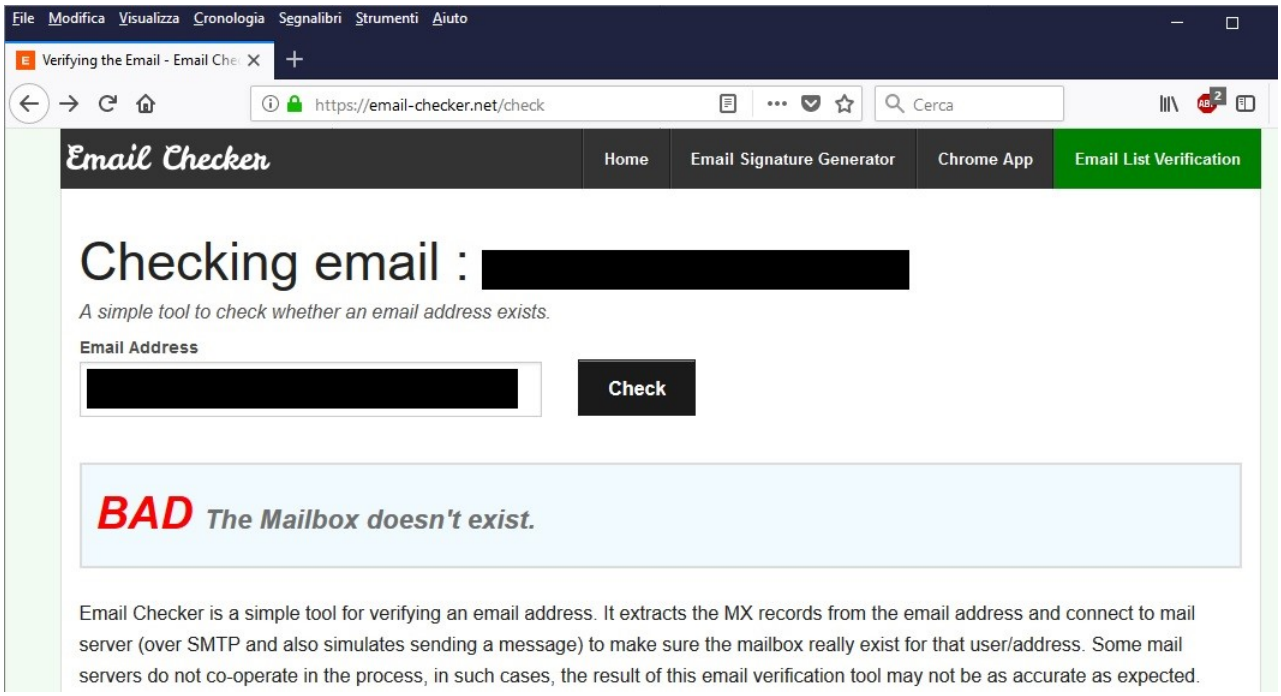
LINK | https://www.email-checker.net

Inserite il mittente del messaggio di posta nell'apposita casella di testo e cliccate su "Check".

Nel caso il mittente fosse valido e riconosciuto il risultato sarà come quello nell'immagine seguente



Caso opposto è quando il mittente risulta essere non corretto o inesistente come dall'immagine seguente



Esistono numerosi portali che offrono questi servizi di check, molti sono limitati da un numero massimo giornaliero di verifiche oltre le quali poi il servizio viene offerto a pagamento; nel caso del portale preso in esempio in questo caso ci sono 5 indirizzi all'ora verificabili gratuitamente.

A questo punto abbiamo terminato le verifiche possibili sul mittente: è probabile che abbiate già cestinato l'email falsa poiché l'analisi del mittente è già una grande scrematura ma, se siete ancora dubbiosi sulla sua veridicità o meno, andiamo a leggere l'oggetto per trovare altri elementi sospetti.

L'oggetto del messaggio

Spesso vengono utilizzati degli oggetti d'impatto per attirare gli utenti: se si parla di un'eredità ricevuta da un lontano parente di cui non avete mai sentito parlare; se vi viene offerta una somma in denaro; o se vi viene chiesto di reimpostare una password (senza che voi lo abbiate mai chiesto) ed altre informazioni o richieste anomale, 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.

Cestinate il messaggio senza remore. E se neanche l'oggetto vi avesse convinto, andiamo a guardare il corpo del messaggio.

Il corpo del messaggio – La forma

Prima di tutto, per riconoscere email false 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.

Negli ultimi tempi con il migliorare anche dei numerosi traduttori, il livello di correttezza dei documenti è quasi vicino alla perfezione. I messaggi possono essere sia informali sia estremamente personali.

Ad esempio può succedere di ricevere da persone conosciute una mail con scritto "Mi dai un parere su questo? Link a qualcosa" (linguaggio diretto e personale) oppure può capitare di ricevere un avviso di pagamento o fattura con linguaggio più formale.

Il corpo del messaggio – Il contenuto

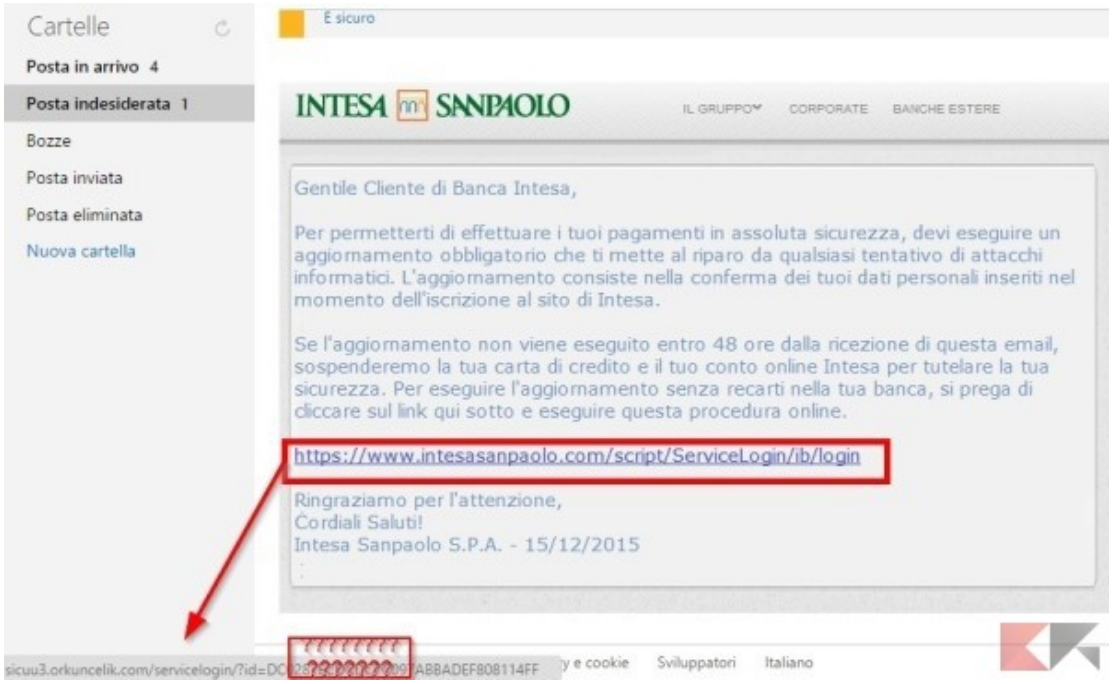
A questo punto arriva la prova del 9 e dovete chiedervi:

- 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?

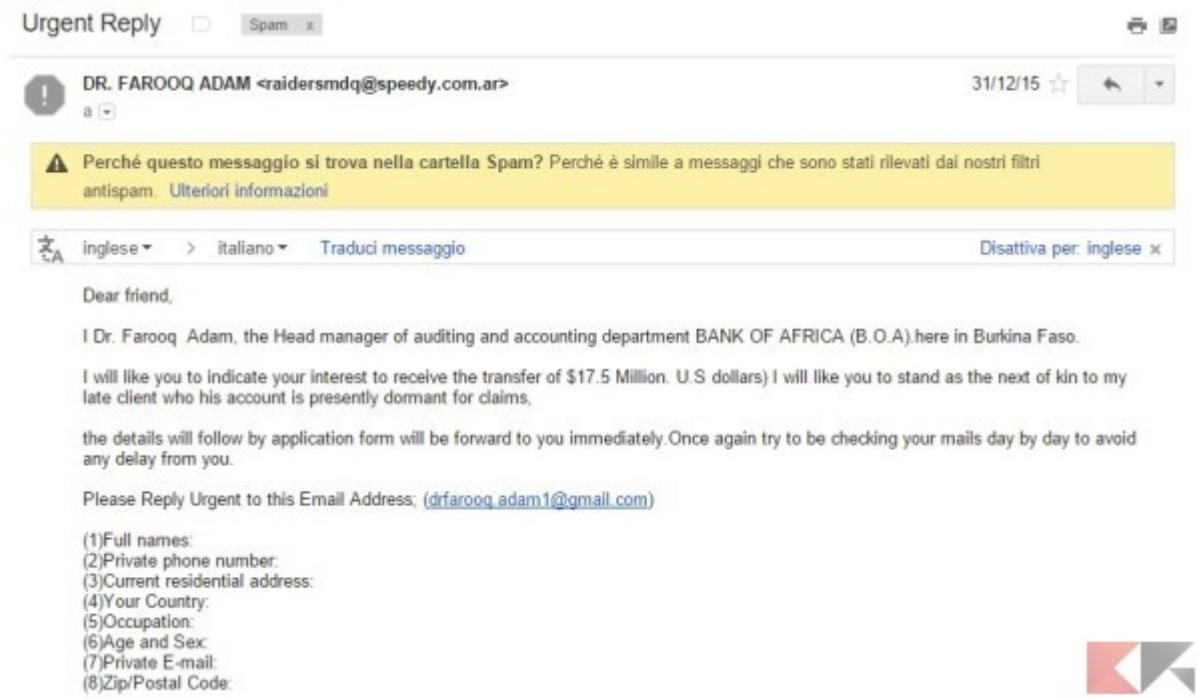
Se almeno la risposta a una di queste domande è SI, cestinate il messaggio immediatamente: a questo punto le probabilità che si tratti di un tentativo di phishing sono altissime.

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 verificare che il link ci porterà ad una pagina ben diversa da quella di Intesa Sanpaolo.



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. Questo basterebbe già per riconoscere email false di questo tipo.



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 è abbastanza eloquente; naturalmente questo messaggio è stato catalogato come spam.

L'allegato

Discorso delicato è l'allegato di posta elettronica, in ogni caso se la mail dovesse superare tutte le verifiche descritte precedentemente, ma non siamo sicuri che il file in allegato alla mail sia sicuro, potremmo avvalerci (come nel caso di verifica del mittente) di sistemi di controllo dei file.

Qualora l'antivirus presente sul computer non dovesse allertarci non è assolutamente certo che l'eventuale allegato non contenga un file infetto; quasi tutte le società di fornitura di antivirus forniscono servizi online di verifica del file. Di seguito sono riportati alcuni di questi portali:

- https://www.virustotal.com/it/
- https://virusdesk.kaspersky.com/

Il servizio è gratuito e molto intuitivo; viene richiesto di caricare il file da verificare e ne viene restituito subito il responso.

Cenni sulla PEC

La tecnologia usata per fornire il servizio di posta PEC potrebbe far credere che la sicurezza sul sistema di posta certificata siano di livello superiore rispetto a quello della posta ordinaria; in realtà (senza addentrarci in tecnicismi) la tecnologia di funzionamento della posta certificata rispetto a quella normale differisce solo dal sistema di certificazione dello scambio dei messaggi e dai protocolli di sicurezza (che tra le altre cose sono stati adottati da quasi tutte le società che vendono servizi di posta elettronica).

Fatta questa premessa è sicuramente doveroso far presente **che le situazioni descritte in questa guida possono presentarsi anche sul sistema di posta certifica e che occorre sicuramente adottare le stesse tecniche esposte nei paragrafi precedenti.**

Altri esempi di mail fasulle

Esempio avviso di pagamento con allegato

L'esempio di mail che segue riporta l'avviso di un pagamento: analizzando nel dettaglio il messaggio è chiaro che il mittente del messaggio non è affidabile (secondo quando detto precedentemente); senza esitazione non aprite l'allegato e cestinare immediatamente il messaggio.

AVVISO DI PAGAMENTO n.1486189863

Equitalia S.p.A. <1486201120pagamento@1486201120equitalia.it>
Oggi 10:45

Rispondi a tutti

fattura 3782999.zip
215 KB

ATT00001.txt
266 byte

2 allegati (215 KB) Scarica tutto

Agente della Risossione
Equitalia S.p.A.
Via Cristoforo Colombo 142 - 005161 - Roma

Art. 29 D.P.R. 07/03/1942, n. 241 e successive modifiche - Art. 29 D.P.R. 02/07/1942, n. 423, Art. 190 c.p.c.

Gentile cliente,

Il suindicato Agente della Riscossione avvisa, ai sensi delle intestate disposizioni di legge , di aver depositato in data odierna, nella Casa Comunale del Comune il seguente avviso di pagamento **"fattura 3782999"** del 04/02/2017 , composto da 3 pagina/e di elenchi contribuenti a nr. 7 atti.

SCARICA IL DOCUMENTO ALLEGATO

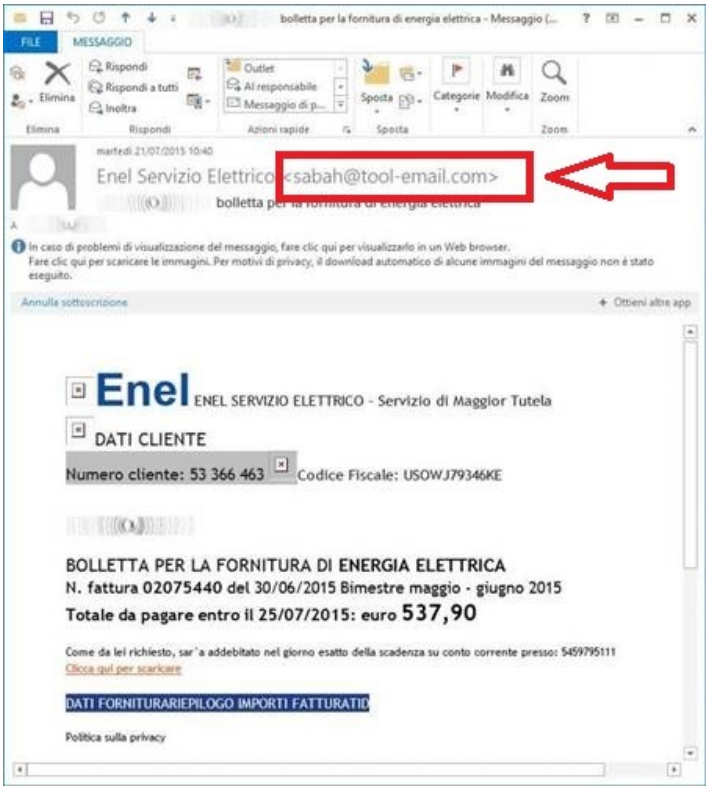
© Equitalia S.p.A. C.F. P.I. 084746643

Esempio fattura con link

Nell'esempio qui riportato non è presente nessun allegato ma siete invitati a cliccare sul link per effettuare l'operazione di pagamento; non cliccate sul link e cestinate il messaggio immediatamente.

Diffidate anche dei mittenti conosciuti; ricordate che:

1. Un contato da voi conosciuto potrebbe aver preso un virus e che sfrutta come veicolo la posta elettronica.
2. Persone molto capaci e preparate sono in grado (se le condizioni di sicurezza non sono sufficienti) di creare mail quasi perfette, comprensive di mittenti conosciuti.



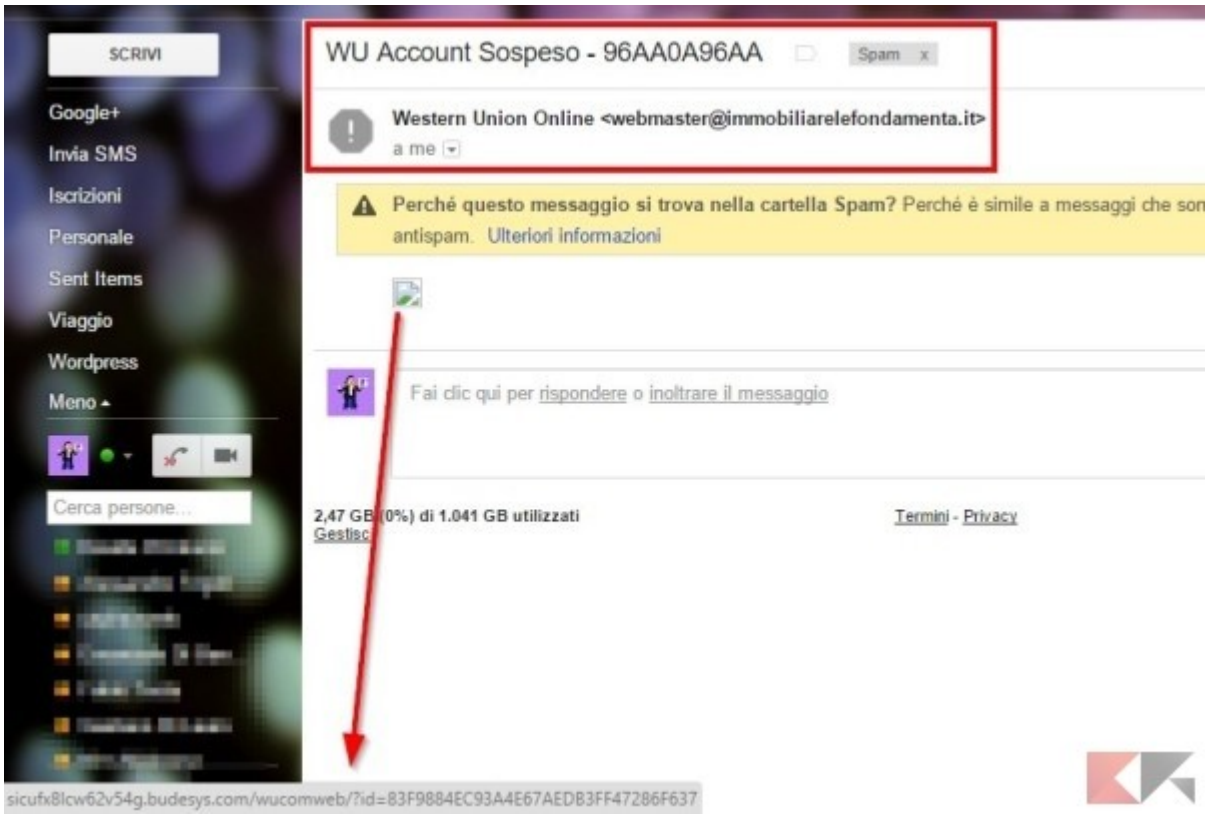
Suggerimenti

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. Cosa possiamo fare a questo punto?

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 riavere 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.

Conclusioni

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 a permetterci di riconoscere e-mail 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 aperte e dita sempre lontane dai click potenzialmente nocivi.

Un suggerimento per evitare la diffusione del proprio indirizzo di posta nei sistemi di spam è quello di non inserirlo nelle pagine web e quindi di prevedere pagine dedicate ad essere contattati (form di contatto).

Definizioni

Phisher: è colui che mette in atto le operazioni di truffa chiamate phishing

Phishing: è una truffa informatica effettuata inviando un'email con il logo contraffatto di un istituto di credito o di una società di commercio elettronico, in cui si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico. Il phishing è di norma usato per recuperare in maniera illecita credenziali di acceso ai vari siti o portali.

Ransomware: è un tipo di malware (software dannoso) installato illegalmente sul tuo computer, senza la tua autorizzazione. Tramite il ransomware, i criminali riescono a bloccare il computer o addirittura a cifrare tutti i file presenti sul computer e nella rete; a questo ne segue una procedura di riscatto per sbloccare il computer o ricevere la chiave di decifratura dei file. Il ransomware si installa generalmente aprendo o facendo clic su allegati o collegamenti fraudolenti in un messaggio email, un messaggio istantaneo, un social network o un altro sito Web. Il ransomware può entrare nel computer persino durante la semplice visita di un sito Web fraudolento.

Spam: è una pratica (anche pericolosa) che consiste nell'invio reiterato di messaggi di posta elettronica generalmente a carattere pubblicitario