POSTA ELETTRONICA NELLA TUA CARTELLA SPAM

Molte volte i provider (in particolare libero.it, alice.it e altri) posizionano le mail in arrivo nella tua cartella SPAM, quindi, ogni volta che accendi il computer controlla detta cartella perché potrebbe contenere comunicazioni importanti.

MESSAGGI TRUFFA (in inglese *phishing*)

Cercano di entrare nel tuo computer per rubare i tuoi dati e sottrarti soldi e/o contattare a tuo nome coloro che sono nella tua rubrica mail per provare a derubarli: **FAI ATTENZIONE.**
Per entrare nel tuo computer i delinquenti ti inviano una mail con il mio nome e/o quello dell'associazione e/o di un tuo amico chiedendoti di scaricare un allegato oppure di cliccare su un link e/o scaricare uno zip.

BUTTALA NEL CESTINO

A volte i filtri e gli antivirus che abbiamo li bloccano e/o li inseriscono nella cartella SPAM ma nella maggioranza dei casi li trovi nella cartella POSTA IN ARRIVO.
Importante è disattivare, qualora lo avessi attivato, l'inserimento in automatico nella tua rubrica mail dei mittenti delle mail che ricevi; questo evita di avere nella tua rubrica la mail del truffatore.

INDIVIDUARLI È FACILE

Come vedi sotto, ho riprodotto un messaggio:

1. ricevuto da una persona che è nella nostra banca dati (evidenziata in verde la cancellazione della sua mail per tutelare la sua privacy),
2. dopo il **Da:** c'è il nostro nome e in calce la nostra mail che hanno copiato da qualche destinatario delle nostre mail ma la mail di provenienza che non corrisponde alla nostra (evidenziata in giallo);
3. testo sintetico e nessuna spiegazione ragionevole di cosa si tratta il link e/o il file da scaricare;
4. telefoni che non corrispondono (evidenziati in giallo).

MAIL ARRIVATA A NOSTRO NOME MA INVIATA DA UN HACKER

Da: ANCC Ciolli [mailto:k_munetou@terasoh.com]
Inviato: venerdì 25 marzo 2022 12:04
A: ... omesso per la privacy .....
Oggetto: Rv:
Inviamo in allegato le fatture del mese di marzo/2022.
CA6391982730086796594.zip
ZIP pass: dzgcv
ANCC Ciolli
E-mail: *pierluigiciolli@coordinamentocamperisti.it*
Tel. +39 8028 81 50 36
Cel. +39 010 04 62 990

PER MEGLIO ILLUSTRARE LA SITUAZIONE, A SEGUIRE IL TESTO ESTRATTO DA

https://www.fastweb.it/fastweb-plus/digital-magazine/cosa-fare-quando-si-riceve-un-e-mail-phishing/
Il mondo della **sicurezza informatica** è cambiato molto negli ultimi anni.

VIRUS, TROJAN E MALWARE sono ancora uno dei vettori principali per infettare i dispositivi degli utenti, ma con la diffusione massiccia di Internet e degli smartphone sono stati affiancati da nuovi metodi. Tra i più diffusi troviamo gli **attacchi phishing**, una particolare tipologia di attacco informatico diventato negli ultimi anni il principale veicolo di truffe online.

ATTACCHI PHISHING?

Si tratta di un attacco informatico che viene perpetuato tramite SMS ed e-mail. Il malvivente invia a un utente (nella maggior parte dei casi le vittime sono casuali, vengono inviati gli stessi messaggi a centinaia di migliaia di persone) un'e-mail nella quale lo invita a **cliccare su un link per cambiare la password** del proprio conto corrente o a inviare i propri dati personali per ritirare un premio. Per rendere più veritiero il messaggio, l'e-mail del mittente sembra essere quella di una vera azienda (Poste, banca, catena di elettrodomestici) e la URL del sito che andiamo ad aprire sembra identica a quella del portale originale. In realtà si tratta di un sito falso creato ad arte dai pirati informatici per rubare informazioni personali ai poveri utenti. Informazioni personali che possono essere utilizzate per rubare soldi dal conto corrente oppure per portare avanti altre truffe. In alcuni casi vengono addirittura **vendute sul dark web per poche decine di euro**.

COME RICONOSCERLI

E soprattutto cosa bisogna fare quando la si riceve? La maggior parte degli utenti non è in grado di **capire quando un'e-mail** è in realtà un attacco phishing. Nonostante basti poco per capire che si tratti di una truffa, molte persone non hanno gli strumenti adatti per saper **riconoscere un messaggio falso**. Per riconoscere un'e-mail phishing basterebbe fare dei semplici controlli e segnalare a chi di dovere che si tratta di un messaggio-truffa. Ecco tutto quello che possiamo fare quando riceviamo un'e-mail phishing.

Partiamo dalle basi. Per riconoscere un messaggio-truffa basta effettuare dei semplici check. Se riceviamo un'e-mail nella quale apparentemente la nostra banca ci avvisa che dobbiamo cambiare la password a causa di problemi generali di sicurezza, controlliamo attentamente l'indirizzo di posta elettronica del mittente. I pirati informatici sono abili nel costruire degli indirizzi molto simili a quelli originali, ma si differenziano per un paio di lettere. Se notiamo qualcosa di strano già nel primo controllo, possiamo essere abbastanza sicuri che si tratta di un **messaggio phishing**.

Altro controllo da fare è la **URL del link** presente nel messaggio (in un'e-mail phishing c'è sempre un link che porta su una piattaforma esterna). Anche in questo caso, la URL sembra essere identica a quella di un vero sito, ma si differenzia sempre per una o due lettere.

Basta un po' di attenzione per capire che si tratta di un sito falso creato appositamente per truffare gli utenti.

COSA FARE

Se abbiamo il sospetto che **l'e-mail** che abbiamo ricevuto dalla nostra banca nella quale ci consiglia di cambiare la password sia in realtà un **messaggio phishing**, non dobbiamo andare nel panico. Intanto bisogna capire che se riceviamo un messaggio di questo tipo, non vuol dire che il nostro computer sia infetto. Anzi. Si tratta di e-mail ricevute ogni giorno da milioni di persone.

La prima cosa da fare quando si *riceve un'e-mail phishing* è non cliccare sui link presenti all'interno del messaggio. L'infezione potrebbe iniziare proprio cliccando il link.

Altra cosa da fare è non rispondere a questo tipo di e-mail. I truffatori inviano ogni giorno milioni di messaggi di posta elettronica nella speranza che qualche utente abbocchi alla truffa. Rispondendo all'e-mail si dà la conferma al truffatore che il nostro indirizzo di posta sia "vivo e vegeto" e continuerà a inviare messaggi ogni giorno.

COME BLOCCARLI

Con la crescita degli attacchi phishing tutti i principali provider di posta elettronica hanno implementato degli strumenti per **bloccare i messaggi-truffa**.

Se un'e-mail phishing riesce a superare i filtri di protezione, gli utenti possono segnalare l'indirizzo di posta elettronica del mittente in modo che venga bloccato dal provider.

La procedura da seguire cambia a seconda dell'app e del provider di posta elettronica che utilizziamo, ma i passaggi da seguire sono molto simili tra di loro.

Nella maggior parte dei casi bisogna entrare all'interno del messaggio-truffa, cliccare sulle impostazioni e poi su "Segnala phishing". In questo modo il provider farà partire un'indagine per capire se si tratta realmente di un messaggio falso.

SEGNALARE ALLA PROPRIA AZIENDA

Uno dei **bersagli preferiti dei truffatori sono le e-mail aziendali**.
Molti dipendenti non sono in grado di riconoscere una truffa e nella maggior parte dei casi cliccano sui link presenti nelle e-mail, infettando tutta la rete aziendale.
Se ricevete un messaggio sospetto nella casella di posta aziendale, inviate un'e-mail al reparto IT segnalando il problema in modo che possano aumentare le barriere di protezione.

SEGNALARE ALLE FORZE DELL'ORDINE

Se siete caduti nella **trappola di un** attacco phishing dovete segnalare immediatamente l'accaduto alle Forze dell'Ordine.
La Polizia Postale può far partire un'indagine per risalire al mittente del messaggio e cercare di bloccare la truffa.

SEGNALARE ALL'AZIENDA VITTIMA DELLA TRUFFA

Ogni **messaggio phishing** sfrutta il nome di una vera azienda: un servizio di home banking, un brand famoso, una catena di elettrodomestici.
Queste aziende sono anche loro delle vittime della truffa: i malviventi utilizzano impropriamente il loro nome.
Se ricevete **un'e-mail phishing** avvertite immediatamente l'azienda coinvolta, in modo che possano far partire una denuncia anche loro.

CANCELLARLE

Una volta seguiti tutti questi passaggi, cancellate l'e-mail. Non c'è nessun motivo per cui dobbiate tenere sul vostro **indirizzo di posta elettronica** questo tipo di messaggi.
Ricordate che l'aver ricevuto un messaggio phishing non equivale ad avere lo smartphone infetto: non dovete eseguire nessuna scansione antivirus.

NON AVERE PAURA

Ricevere un messaggio phishing non è pericoloso. E non vuol dire che il proprio PC è infetto. I messaggi-truffa stanno diventando sempre più frequenti e può capitare di riceverne un paio. L'importante è seguire tutti i passaggi illustrati nella nostra guida ed essere sempre attenti a non cliccare su nessun link.

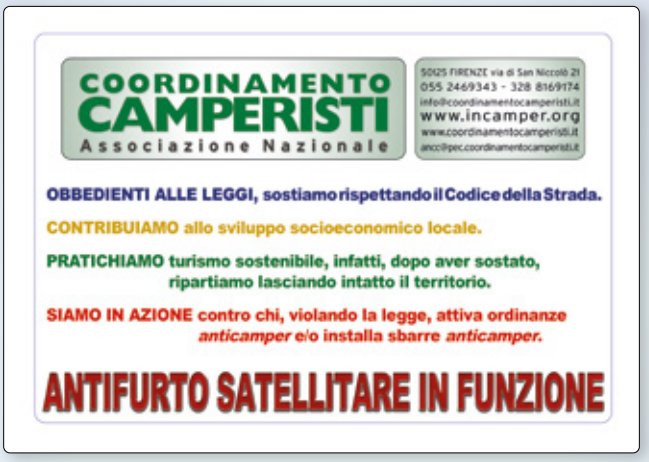
PER PREVENIRE IL DISAGIO DEL FURTO O SMARRIMENTO DEL CELLULARE

Tenere sempre nel portafoglio, in casa e in ufficio un foglio dove vi sono scritti:

- il **codice IMEI** del tuo cellulare, che è composto da 15 cifre. Se nel cellulare ci sono due codici IMEI, vanno trascritti entrambi;
- il **codice seriale univoco ICCID** della SIM. Si trova sul supporto dov'era inserita la SIM; altrimenti, essendo trascritto anche sopra la SIM, chiedere a un centro di assistenza di estrarla per rilevarlo.

COSA FARE APPENA SCOPRI CHE TI HANNO RUBATO IL CELLULARE OPPURE LO HAI SMARRITO

- Telefona al servizio clienti del tuo gestore e chiedi di bloccare la scheda SIM. Informali se intendi chiedere una nuova SIM mantenendo lo stesso numero di telefono. In tal modo i ladri non avranno la possibilità di utilizzare il credito residuo, di ricevere telefonate o messaggi dai tuoi contatti, di accedere ai dati salvati sulla scheda (rubrica, immagini, SMS o WhatsApp eccetera).
- Recatipressolacasermadei Carabinierie/odellaPoliziadiStatoconilcompilatodelladenuncia(trovideifacsimili aprendo *https://www.settimocell.it/2015/07/23/download-modulo-denuncia-smarrimento-cellulare-52928.html*). Come vedi, sul modulo devi inserire l'IMEI del telefono. Se non lo ricordi, telefona al servizio clienti del tuo gestore: potrai recuperarlo semplicemente comunicando i quattro numeri che telefoni più frequentemente.
- Dopo aver sporto al tuo gestore denuncia chiedi il blocco del telefono, allegando la denuncia. Informazioni utili aprendo *Cellulare rubato: cosa fare | Salvatore Aranzulla*.
- Prova a **bloccare il tuo cellulare da remoto** o a **cancellare tutti i dati** presenti in esso sfruttando i sistemi antifurto inclusi "di serie" da Google e Apple nei propri device *Cosa fare in caso di smarrimento o furto di iPhone, iPad o iPod touch - Supporto Apple (IT)* Per rintracciarlo sul cellulare deve essere stata abilitata precedentemente la funzione "**Trova il mio iPhone**" e i passi da fare per tentare di rintracciarlo li trovi aprendo *Furto del cellulare: cosa fare (laleggepertutti.it)*: Anche chi possiede un **Windows Phone** può utilizzare il servizio "**Trova il mio telefono**" per **rintracciare, bloccare e comandare** da un altro dispositivo. A condizione, però, che il cellulare sia acceso, connesso alla rete e, come negli altri casi, con i servizi di localizzazione attivi. Basta collegarsi ad *account.microsoft.com/devices*, scegliere il telefono che si vuole trovare e rintracciarlo sulla mappa che apparirà sullo schermo. A quel punto sarà possibile fare clic su "Blocca" e seguire le istruzioni, oppure selezionare "Cancella" per eliminare tutti i dati del dispositivo.



Ecco il tagliando che l'associato può esporre sul cruscotto durante la sosta. Per scaricarlo aprire *www.coordinamentocamperisti.it* e poi cliccare su

AGGIORNAMENTI