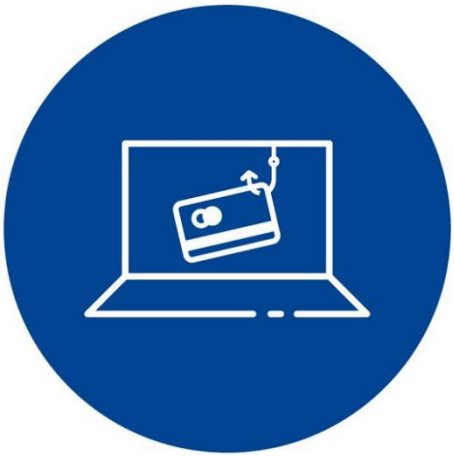
Consulenza ed assistenza per i consumatori in Europa

ECC-Net

Centro Europeo Consumatori Italia

PHISHING



A cura del

Centro Europeo Consumatori Italia ufficio di Bolzano

Via Brennero n. 3 I-39100Bolzano

Tel.+39-0471-980939 Fax+39-0471-980239

www.euroconsumatori.org

info@euroconsumatori.org

Facebook
Centro Europeo Consumatori Italia

Twitter
ECC Italy

Instagram
ecc.italy

YouTube
Centro Europeo Consumatori Italia

Cofinanziato dall'Unione Europea

Contenuti

Il Centro Europeo Consumatori Italia fa parte della Rete dei Centri Europei Consumatori, ECC-Net, è cofinanziato dalla Direzione Generale per l'Armonizzazione del Mercato e laTutelaConsumatori del Ministero per lo Sviluppo Economico, attraverso la Direzione Generale per la Giustizia, Consumo e Parità della Commissione Europea, della Provincia Autonoma di Bolzano e dalla Regione AutonomaTrentino-AltoAdige/Südtirol. Promotori sono il CentroTutelaConsumatori Utenti Alto Adige e l'Associazione Difesa Consumatori e Ambiente(Adiconsum).

Questa pubblicazione è stata finanziata dal programma per la tutela dei consumatori dell'Unione Europea (2014 - 2020). Il contenuto di questa pubblicazione rappresenta il punto di vista degli autori che ne sono gli unici responsabili; non può essere in alcun modo considerato come manifestazione del punto di vista della Commissione Europea e/o dell’Agenzia Esecutiva per i consumatori, la salute, l'agricoltura e la sicurezza alimentare o di alcun altro organismo dell’Unione Europea. La Commissione Europea e/o l’Agenzia esecutiva non accettano responsabilità per qualsiasi uso che potrebbe essere fatto delle informazioni ivi contenute.

Il contenuto e le informazioni di questa pubblicazione sono intesi come consigli pratici e non si riferiscono a casi individuali. Il Centro Europeo Consumatori Italia non può garantire la completezza, adeguatezza o aggiornamento delle informazioni contenute in questa pubblicazione.

Situazione aggiornata a marzo 2021

Phishing: che cos'è?

Il **phishing** è una **truffa** realizzata sulla rete Internet ingannando gli utenti. Il truffatore, fingendo di essere un ente affidabile e noto, invia un messaggio di **posta elettronica** con cui cerca di ingannare i destinatari per convincerli a fornire ad esempio **informazioni e password personali, credenziali** di accesso ai siti di online banking e/o dati finanziari.

Etimologia: da dove proviene il termine phishing

Il termine phishing è una variante di *fishing* (letteralmente "pescare" in lingua inglese) e allude all'uso di tecniche sempre più sofisticate per "pescare" dati sensibili di un utente. La parola può anche essere collegata al linguaggio *leet* (che sostituisce i caratteri alfabetici ad esempio con delle cifre), nel quale la lettera f è comunemente sostituita con ph.

In che modo avviene?

Si concretizza spesso attraverso **messaggi di posta elettronica ingannevoli**, apparentemente provenienti da istituti finanziari, come banche o società emittenti di carte di credito, oppure da siti web che richiedono l'accesso previa registrazione, come per esempio siti di e-commerce o web-mail. Riferendo che vi siano problemi di registrazione o di altra natura, il messaggio invita a fornire i propri dati di accesso al servizio.

Solitamente, nel messaggio, per rassicurare falsamente l'utente, è indicato un **link** che rimanda – apparentemente – al sito web dell'istituto di credito o del servizio a cui si è registrati**. In realtà il sito a cui ci si collega è stato allestito in modo identico a quello originale, ma si tratta di un falso.** Qualora l'utente inserisca i propri dati riservati, questi saranno nella disponibilità dei criminali.

Il phishing avviene a volte anche tramite **SMS** o **messaggi sui social media**, o ancora, tramite **messaggi ricevuti sulle piattaforme di messaggistica istantanea**.

Un altro pericolo connesso al phishing

Con la stessa finalità di carpire dati di accesso a servizi finanziari on-line o altri che richiedono una **registrazione**, un pericolo più subdolo arriva dall'utilizzo dei **virus informatici**.

Le modalità di infezione sono diverse. La più diffusa è tramite un **allegato al messaggio di posta elettronica**. Oltre che mediante i file con estensione .exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che possono giungere anche in formato .doc o .pdf.

Nel caso si tratti di un "*financial malware*" o di un "*trojan banking*", il virus si attiverà per **carpire dati finanziari** senza bisogno che gli siano forniti.

Altri tipi di virus, i "*keylogging*", si attivano quando sulla tastiera vengono inseriti "*userid* e *password*". In questo caso **i criminali entrano in possesso delle chiavi di accesso ai nostri account di posta elettronica o di e-commerce.**

Le caratteristiche del phishing sono tali per cui la trappola, purtroppo, è ben tesa

L'esperienza quotidiana testimonia che non riusciamo quasi mai a leggere tutte le e-mail che ci arrivano. Tante sono pubblicità e parecchie finiscono direttamente nello spam.

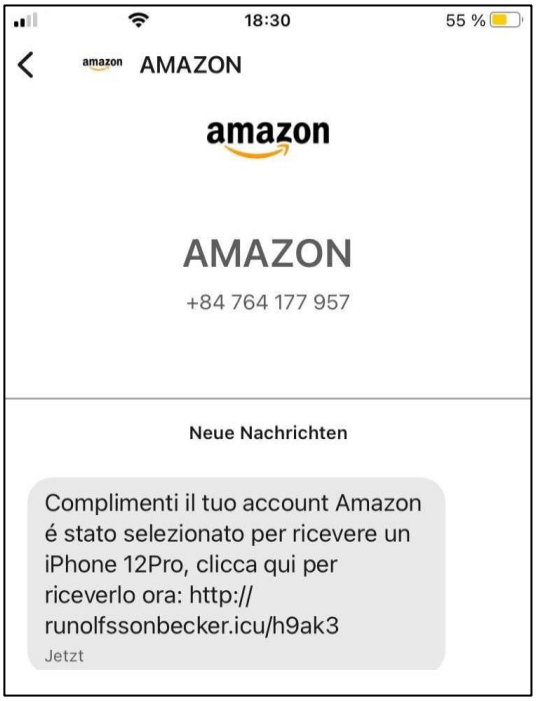
Le **e-mail** sono il vettore principale utilizzato dagli hacker criminali per condurre i loro attacchi phishing, ma prestando attenzione è possibile **riconoscere le e-mail sospette**. Si tratta quasi sempre di messaggi di posta elettronica, che riportano un **logo contraffatto** e invitano il destinatario a **visitare una specifica pagina web per fornire dati riservati**, come per esempio il numero di carta di credito o le credenziali di accesso. Queste pagine web somigliano in modo quasi perfetto a quelle vere, tanto da spingere l'utente a cliccare senza esitazione sui link posizionati opportunamente nella mail. Un esempio potrebbe essere il messaggio di un sito che si spaccia per una società di data center, come Aruba, che invita a rinnovare l'abbonamento oppure a rinnovare i dati dell'account cliccando su un link.

Per tanti di questi messaggi, **la grafica è talmente familiare** che non è difficile cadere nel tranello della loro falsificazione. Per esempio si potrebbe ricevere una mail per il rinnovo dell'account di posta elettronica da parte di un hacker che utilizza la stessa grafica e lo stesso carattere del sito clonato.

Come un pesce abbocca all'esca andando in cerca di cibo, chiunque di noi potrebbe abboccare alle richieste contenute nell'e-mail. Si potrebbe ricevere un **messaggio di posta da un da amico che racconta di essere all'estero, di avere subito il furto dei documenti**, **dei soldi e del telefono**, chiedendo l'invio di denaro via *Money Gram* o *Western Union*. Così,

cadendo in un tranello ben teso, si consegnano a siti fraudolenti i propri contatti, l'accesso ai profili digitali, denaro e, nel peggiore dei casi, le chiavi d'accesso ai propri conti bancari.

E con l'evoluzione dei **social network** e dei **programmi di messaggistica istantanea**, ormai sono spesso anche altri gli strumenti attraverso cui gli hacker criminali tentano di farci cadere nella trappola del phishing. Per esempio attraverso Telegram si potrebbe ricevere un messaggio da parte di Amazon, con il logo uguale a quello della multinazionale, che invita a cliccare su un link per ricevere un telefono nuovo, essendo stati selezionati come vincitori di un concorso… Poi, però, il numero di telefono da cui arriva il messaggio ha il prefisso di un Paese che non ci si aspetterebbe, per esempio del Vietnam, come nel caso che potete vedere in questo screen:



Come smascherare il phishing? Consigli pratici su come difendersi

Una buona notizia c'è, perché esistono dei **software utili** a smascherare questo tipo di truffe. Vi consigliamo di verificare se per il browser che utilizzate si può scaricare un'estensione che smaschera gli indirizzi sosia. Si abilitano, in certi casi, aggiungendole al browser dal web store. La loro funzione è banale, ma potenzialmente molto utile: nel momento in cui si cerca di accedere a un sito con un indirizzo "sosia", queste ci chiederanno se siamo proprio sicuri di volerlo fare. A questo punto, anche l'utente più distratto andrebbe a **leggere bene l'URL**, smascherando l'inganno.

Molti siti web che offrono servizi online ai quali ci si deve registrare (gestori di account di posta elettronica e PEC, siti di e-commerce, l'agenzia delle entrate, ecc.) informano sul pericolo di phishing e forniscono preziosi consigli su come riconoscerlo ed evitarlo.

In generale, le precauzioni da tenere a mente sono:

- **Verificare di trovarsi sul sito autentico**. Qualora dovessimo cliccare su un link, controlliamo attentamente nella barra del browser di non essere finiti su un indirizzo sospetto. Anche se simili dal punto di vista grafico alle pagine web originali, spesso il nome del sito presenta minime differenze nell'indirizzo rispetto a quello autentico.

- **Utilizzare la barra degli indirizzi del browser**. Nel dubbio, è meglio non fidarsi mai di email ordinarie che contengono link. È meglio controllare i propri account direttamente andando sui rispettivi siti ufficiali, digitandone l'indirizzo nell'apposita barra del browser.

- **Controllare l'indirizzo e-mail del mittente**. Se riteniamo sospetta una mail ricevuta, controlliamo che l'indirizzo appartenga realmente al soggetto da cui sostiene di provenire, che quindi l'indirizzo sia associabile ad esso. Per esempio, se il mittente è Apple, ma l'indirizzo e-mail è YYX@352-apple.com è il caso di stare attenti.

- **Occhio agli errori**. Nei casi di phishing più grossolano, le mail contengono errori ortografici, o piccole storpiature nel nome del presunto mittente. In ogni caso il reale indirizzo da cui provengono queste e-mail è differente da quello ufficiale. Siti come paypall.com invece di paypal.com, oppure gcogle.com anziché google.com hanno minime differenze nell'indirizzo rispetto a quelli autentici. Sono usati per ingannare gli utenti a cui sfugge il dettaglio della lettera diversa, ritrovandosi a inserire le proprie credenziali di accesso online, che vengono di conseguenza rubate.

- **Non credere alle urgenze**. È uno dei fattori su cui il phishing fa maggiormente leva: un pagamento in sospeso da saldare immediatamente, un premio da ritirare in tempi brevi o il rischio di perdere un account se non si paga subito. Quando una mail ti mette fretta, il rischio che sia una truffa è alto.

- **Attenzione agli allegati**. Quando sono presenti allegati con estensione dei file .pfd, .doc. .exe o altre estensioni più inusuali, o comunque non previsti, è bene prestare molta attenzione. In questo caso, oltre al semplice phishing, dietro quei file potrebbero nascondersi anche dei virus.

- **Nessuno regala niente**. Le e-mail che annunciano vincite di denaro, o qualsiasi tipo di premi, sono quasi sempre fasulle. Uno smartphone a 1 euro, l'eredità di un lontano parente o la vincita alla lotteria dovrebbero suonare sempre come un campanello d'allarme.