08/04/2022

womenforsecurity.it

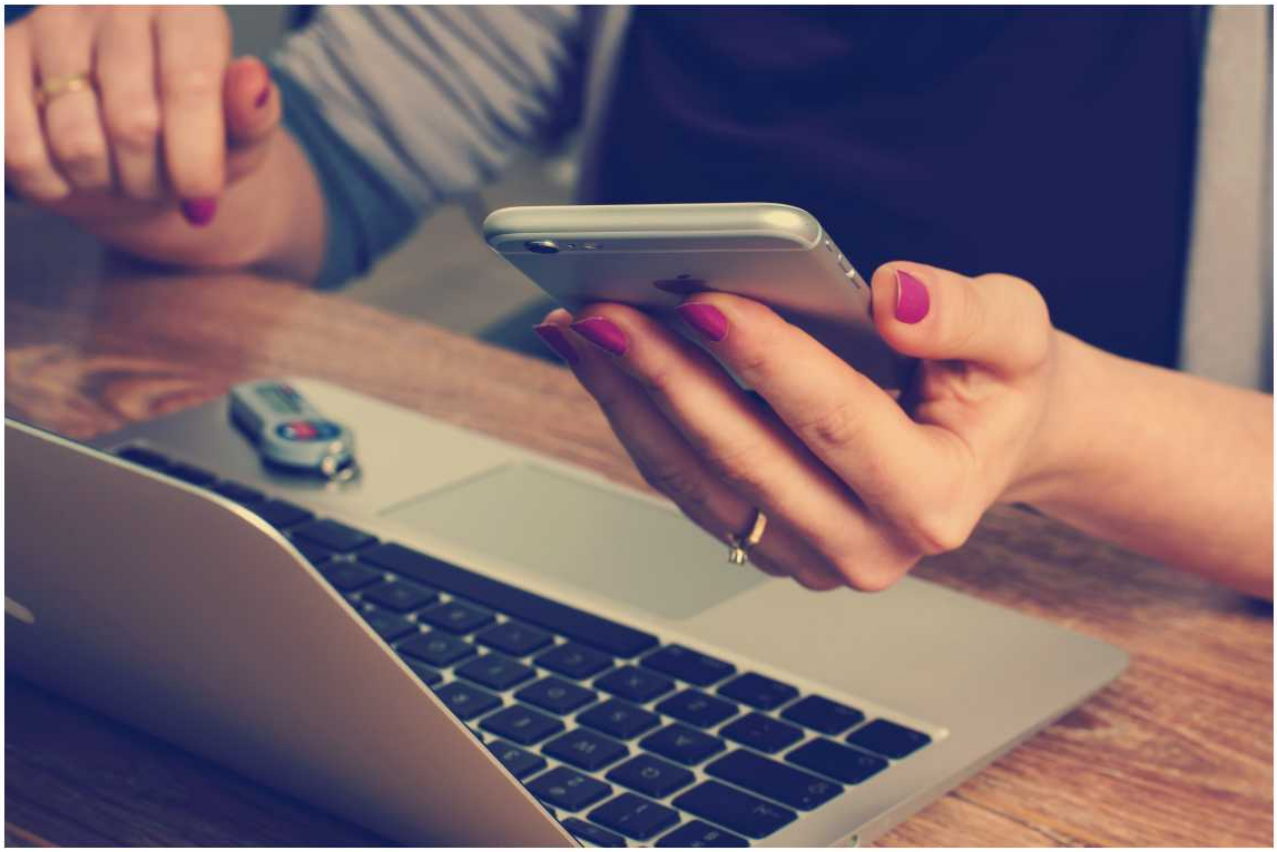
EAV: € 131
Utenti unici: 1.033

Argomento: Exprivia: si parla di noi

https://womenforsecurity.it/dettaglio/53

SMiShing, la truffa via SMS

Pubblicato da **Annamaria Gigante** | 08/04/2022



Di Annamaria Gigante, Event & Communication Specialist presso Exprivia SpA e membro delle Women for Security

L'attuale situazione politica che si riflette nella vita economica e lavorativa di tutti noi, ci impone un addestramento continuo a resistere ai sempre più frequenti attacchi Phishing.

Fenomeno, questo, che non si verifica soltanto online, via e-mail, ma anche attraverso messaggi di testo o SMS, da cui il nome "SMiShing". La parola smishing, infatti, deriva dall'unione di "SMS", ovvero i messaggi di testo che si inviano tramite cellulare, e "phishing", cioè truffa.

Lo smishing è, dunque, una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco. Il criminale compie l'attacco con l'intento di raccogliere informazioni personali, compresi il codice fiscale e/o il numero di carta di credito per rubare denaro. I cybercriminali adottano due metodi per rubare questi dati. Da una parte ingannano le vittime inducendole a scaricare dei malware che si installano automaticamente sul telefono. Questi malware mascherati da app legittime, inducono le vittime a digitare informazioni confidenziali che vengono inviate ai cybercriminali. D'altra parte, i link contenuti nei messaggi di smishing possono aprire siti falsi in cui viene chiesto di inserire informazioni personali sensibili, che i cybercriminali possono usare per rubare l'ID del malcapitato.

Lo Smishing non è frequente come il phishing, ma **è più pericoloso** perché viaggia su un canale che di solito consideriamo affidabile. Solitamente le persone considerano gli SMS e gli instant message attendibili, quindi si fidano del loro contenuto, molto più di quanto non accada per una email. In teoria, chi ci manda un messaggio via SMS o instant messaging conosce il nostro numero di cellulare; pertanto, se qualcuno ci scrive è qualcuno che conosciamo, a cui abbiamo dato noi stessi questa informazione.

SMiShing, la truffa via SMS

Pubblicato da Annamaria Gigante | 08/04/2022

L’attuale situazione politica che si riflette nella vita economica e lavorativa di tutti noi, ci impone un addestramento continuo a resistere ai sempre più frequenti attacchi Phishing.

Fenomeno, questo, che non si verifica soltanto online, via e-mail, ma anche attraverso messaggi di testo o SMS, da cui il nome "SMiShing". La parola smishing, infatti, deriva dall’unione di “SMS”, ovvero i messaggi di testo che si inviano tramite cellulare, e “phishing”, cioè truffa.

Lo smishing è, dunque, una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco. Il criminale compie l'attacco con l'intento di raccogliere informazioni personali, compresi il codice fiscale e/o il numero di carta di credito per rubare denaro. I cybercriminali adottano due metodi per rubare questi dati. Da una parte ingannano le vittime inducendole a scaricare dei malware che si installano automaticamente sul telefono. Questi malware mascherati da app legittime, inducono le vittime a digitare informazioni confidenziali che vengono inviate ai cybercriminali. D’altra parte, i link contenuti nei messaggi di smishing possono aprire siti falsi in cui viene chiesto di inserire informazioni personali sensibili, che i cybercriminali possono usare per rubare l’ID del malcapitato.

Lo Smishing non è frequente come il phishing, ma è più pericoloso perché viaggia su un canale che di solito consideriamo affidabile. Solitamente le persone considerano gli SMS e gli instant message attendibili, quindi si fidano del loro contenuto, molto più di quanto non accada per una email. In teoria, chi ci manda un messaggio via SMS o instant messaging conosce il nostro numero di cellulare; pertanto, se qualcuno ci scrive è qualcuno che conosciamo, a cui abbiamo dato noi stessi questa informazione.

In realtà questo non vero, per tre motivi:

diamo il nostro numero telefonico a diverse realtà che poi non lo trattano come dovrebbero, condividendolo con altre aziende partner. Un esempio sono le telefonate di telemarketing;
le grandi imprese sono colpite da data breach e data leak che posseggono informazioni personali come i numeri telefonici;
molte persone pubblicano online il loro numero telefonico per farsi contattare professionalmente, ma questo numero diventa pubblico, ben al di là delle iniziali intenzioni.
Oggi giorno abbiamo diversi esempi di smishing: può essere un'offerta del provider telefonico che propone uno sconto su un servizio o un aggiornamento del telefono. Il messaggio esorta a cliccare sul collegamento fornito per attivare l'offerta. Una volta raggiunta la pagina web falsificata che riproduce il sito del provider, il sito chiede di confermare il numero di carta di credito, l'indirizzo e magari anche il codice fiscale.

Per sottrarre informazioni sensibili, gli hacker tentano anche di usare misure che fanno leva sui sentimenti. Un esempio sono i messaggi riguardanti i soccorsi per calamità naturali e/o aiuti umanitari in cui i malintenzionati chiedono una donazione per beneficenza.

Il phishing effettuato utilizzando un programma di messaggistica istantanea gratuito come Facebook Messenger o WhatsApp non rientra tecnicamente nell'ambito dello smishing, ma è strettamente correlato. L'hacker sfrutta il crescente livello di comfort che gli utenti hanno nell'aprire messaggi e rispondere a sconosciuti attraverso le piattaforme di social media.

Come difendersi dallo smishing?

Sicuramente essere molto critici nei confronti dei messaggi che provengono da fonti sconosciute aiuta tantissimo. Non cliccare mai sui link nei messaggi di testo, anche se sembrano codici offerte, meglio collegarsi direttamente al sito del presunto mittente digitando manualmente il suo indirizzo web. Infine, fare buon uso della funzione di segnalazione dello spam nel client di messaggistica, di modo che i messaggi fraudolenti vengano bloccati all'origine.

A livello aziendale, se lo smishing rappresenta un problema diffuso, nel caso l'azienda per comunicazione di business faccia uso regolare degli SMS, è importante fare formazione interna sul tema. Molte aziende che si occupano di cyber security hanno sviluppato servizi di "smishing simulation" che creano attacchi simulati per verificare il grado di vulnerabilità dei dipendenti agli SMS ostili.

Personalmente trovo più semplice proteggersi da questi attacchi non rispondendo e/o non eseguendo il comando del messaggio. Ignoralo e lo renderai inoffensivo; è l'unico caso in cui si hanno risultati, semplicemente senza far nulla!

Fonti:

SecurityOpenLab - https://www.securityopenlab.it/news/1242/facebook-dati-di-533-milioni-di-utenti-esposti-online.html

Kaspersky - https://www.kaspersky.it/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Trendmicro - https://www.trendmicro.com/it_it/what-is/phishing/smishing.html

Exprivia – Threat Intelligence Report Exprivia