26/03/2021

la Repubblica.it
il mondo in diretta 24 ore su 24

EAV: € 14.429
Utenti unici: 3.706.667

Argomento: Exprivia: si parla di noi

https://www.repubblica.it/native/economia/2021/03/26/news/truffe_vie_internet_attenzione_all_home_banking-293603477/?ref=search

Truffe via Internet, attenzione all'home banking

Pochi e semplici, ma importanti accorgimenti possono aiutarci a proteggere i nostri risparmi

26 MARZO 2021 2 MINUTI DI LETTURA

Secondo l'Osservatorio Cybersecurity, lo studio sui crimini informatici elaborato da Exprivia, negli ultimi tre mesi del 2020 in Italia sono stati registrati 237 crimini informatici. Di questi, oltre il 60% ha provocato il furto dei dati. Fra le tecniche più sfruttate dai cyber-criminali attivi nel nostro Paese primeggia il "phishing-social engineering" (43%), le cui vittime preferite sono gli utenti distratti o poco avvertiti sui modi di adescamento tramite mail o social network. Seguono gli attacchi cosiddetti "sconosciuti" (24%), cioè le metodologie inedite sperimentate dagli hacker per non essere rilevati dai meccanismi di difesa tradizionali, e i malware (23%), il cui utilizzo è quadruplicato nel corso dell'anno. Tutto questo mentre cresce, sia ai danni dei consumatori che alle imprese, il numero delle truffe o dei tentativi di truffa che mirano a sottrarre soldi o informazioni. Complice la pandemia, il numero di transazioni online o con strumenti di pagamento elettronici è aumentato, mentre si sono evolute, in parallelo, le tecniche utlizzate dai truffatori (tra cui quelle nelle quali un soggetto si spaccia per un operatore della banca).

Chiunque utilizzi strumenti di pagamento deve essere a conoscenza dei potenziali pericoli e delle modalità con le quali i truffatori cercano di carpire informazioni e soldi e allo stesso tempo devono adottare tutte le precauzioni per difendersi. È utile in primo luogo monitorare con regolarità il conto corrente e fare attenzione alle piccole anomalie che potrebbero presentarsi come spese per piccoli importi sul proprio home banking. Fare anche attenzione a video o dalle gif inattese che riceviamo sulle app di messaggistica istantanea, dagli errori di sintassi contenuti nelle mail sospette, dai domini non veritieri degli indirizzi di posta o dall'improvvisa velocità con cui navighiamo sul pc.

In genere, si fa riferimento a tutte queste minacce con delle definizioni in lingua inglese, ormai entrate nel gergo comune Ricapitolarle può essere utile.

Phishing. Fare attenzione alle e-mail in cui si richiede l'inserimento di dati riservati tramite un link e che contengono errori ortografici e grammaticali (la vostra banca non richiederà mai informazioni via e-mail, quindi non cliccate su eventuali link).

Pharming. Navigando su Internt si può incappare in un sito clone creato per carpire i nostri dati personali. Indispensabile perciò controllare sempre che l'URL del sito visitato sia scritto in modo corretto (deve cominciare con "https://" e non con "http://").

Leggi anche

Coronavirus: per combattere la crisi economica delle pmi arriva il lease

Le pensioni integrative come salvagente in un mare di precariato. Lanciato anche dalle banche

Energia: case più ecologiche grazie al Superbonus. E le banche aiutano

Truffe via Internet, attenzione all'home banking

Pochi e semplici, ma importanti accorgimenti possono aiutarci a proteggere i nostri risparmi Secondo l'Osservatorio Cybersecurity, lo studio sui crimini informatici elaborato da Exprivia, negli ultimi tre mesi del 2020 in Italia sono stati registrati 237 crimini informatici. Di questi, oltre il 60% ha provocato il furto dei dati. Fra le tecniche più sfruttate dai cyber-criminali attivi nel nostro Paese primeggia il "phishing-social engineering" (43%), le cui vittime preferite sono gli utenti distratti o poco avvertiti sui modi di adescamento tramite mail o social network. Seguono gli attacchi cosiddetti "sconosciuti" (24%), cioè le metodologie inedite sperimentate dagli hacker per non essere rilevati dai meccanismi di difesa tradizionali, e i malware (23%), il cui utilizzo è quadruplicato nel corso dell'anno. Tutto questo mentre cresce, sia ai danni dei consumatori che alle imprese, il numero delle truffe o dei tentativi di truffa che mirano a sottrarre soldi o informazioni. Complice la pandemia, il numero di transazioni online o con strumenti di pagamento elettronici è aumentato, mentre si sono evolute, in parallelo, le tecniche utlizzate dai truffatori (tra cui quelle nelle quali un soggetto si spaccia per un operatore della banca). Chiunque utilizzi strumenti di pagamento deve essere a conoscenza dei potenziali pericoli e delle modalità con le quali i truffatori cercano di carpire informazioni e soldi e allo stesso tempo devono adottare tutte le precauzioni per difendersi. È utile in primo luogo monitorare con regolarità il conto corrente e fare attenzione alle piccole anomalie che potrebbero presentarsi come spese per piccoli importi sul proprio home banking. Fare anche attenzione a video o dalle gif inattese che riceviamo sulle app di messaggistica istantanea, dagli errori di sintassi contenuti nelle mail sospette, dai domini non veritieri degli indirizzi di posta o dall'improvvisa velocità con cui navighiamo sul pc. In genere, si fa riferimento a tutte queste minacce con delle definizioni in lingua inglese, ormai entrate nel gergo comune Ricapitolarle può essere utile. Phishing. Fare attenzione alle e-mail in cui si richiede l'inserimento di dati riservati tramite un link e che contengono errori ortografici e grammaticali (la vostra banca non richiederà mai informazioni via e-mail, quindi non cliccate su eventuali link). Pharming. Navigando su Internt si può incappare in un sito clone creato per carpire i nostri dati personali. Indispensabile perciò controllare sempre che l'URL del sito visitato sia scritto in modo corretto (deve cominciare con "https://" e non con "http://"). Smishing. Se si riceve un messaggio da un numero sospetto, potrebbe trattarsi di un falso SMS inviato per ottenere informazioni personali. Non cliccare su eventuali link. Vishing. Se si riceve una telefonata da un presunto operatore della banca o da una voce pre-registrata che richiede informazioni e dati riservati, non comunicarli assolutamente al telefono. Nel caso si venga contattati da un soggetto che chieda informazioni sul conto corrente o comunichi una situazione sospetta invitando all'azione, è meglio prima contattare il proprio gestore in banca, senza dare seguito

a solleciti poco chiari. Se si viene contattati telefonicamente, è invece consigliabile terminare la comunicazione e chiamare il numero verde della propria banca per verificare l'effettiva situazione. Val la pena infine ricordare che, quando si sottoscrivono servizi in banca, occorre leggere con attenzione la documentazione pre-contrattuale e contrattuale. Questa infatti, oltre a riepilogare le caratteristiche del servizio/prodotto sottoscritto, riporta anche le procedure e le tempistiche da seguire per la gestione di eventuali controversie, dal reclamo fino all'eventuale ricorso all'Arbitro Bancario Finanziario. Il Gruppo Bancario Cooperativo Iccrea riunisce oltre 130 Banche di Credito Cooperativo (BCC) presenti con oltre 2600 sportelli su tutto il territorio nazionale. Da sempre è al fianco delle imprese, delle famiglie e dei liberi professionisti.