

Occhio alle truffe telematiche!

Inviato da GriGio - 20/03/2020 10:48

Dato che passiamo molto più tempo in casa e davanti a computer e smartphone, siamo bersagli perfetti per truffe telematiche/telefoniche varie ed eventuali.

Un tentativo è arrivato anche all'indirizzo mail di questo forum, dove si fantasticavamo generici problemi di fatturazione e che dovevo con urgenza cliccare un link per sistemare la cosa.

Male, molto male.

In generale:

- a pagare e a morire si fa sempre in tempo
- non vi regala niente nessuno
- diffidare, sempre, degli sconosciuti

Quindi state attenti prima di cliccare e inserire dati sensibili:

- controllate sempre il mittente, sia il nome che l'indirizzo mail (col forum son stati molto bravi, quindi controllate se quell'indirizzo vi aveva già spedito mail in passato)
- diffidate delle urgenze e dell'uso incondizionato di imperativo e punti esclamativi (paga subito, problema!, ecc...)
- diffidate anche della promessa di premi o sconti mirabolanti: non vi si caga e non vi vuole regalare niente nessuno, tranquilli, soprattutto se sconosciuti
- se ci sono errori d'ortigrafia, cancellate immediatamente
- se appunto è una mail che non vi aspettate, cancellate immediatamente

Questo vale anche al telefono: nessuno, NESSUNO, vi chiederà MAI codici d'accesso al telefono. Se insistono o se avete dubbi: riagganciate (anche senza salutare, che si offenda pure) e chiamate il numero che avete sempre usato. Se la telefonata era vera andate avanti con l'operatore che VOI avete chiamato, se era falsa, beh, vi terranno al telefono e vi chiederanno chi era, cosa gli avete dato, insomma, un paio di info per denunciare l'accaduto internamente.

Dato che non siamo invincibili, può capitare di fare la cazzata (è capitato anche a me) e cliccare sul link bastardo: dopo aver mangiato la foglia, fate un bel respiro e **chiamate subito il servizio clienti** per spiegare con calma. Sistemano loro la cosa e di solito non fate in tempo a chiamare che avevano già

sgamato la truffa.



Vi lascio il link di Aruba dove spiegano meglio il phishing e dove potete vedere i printscreen delle mail: www.aruba.it/magazine/email/come-riconos...oni-email-aruba.aspx

=====

Re: Occhio alle truffe telematiche!

Inviato da Domenico80 - 20/03/2020 13:07

Cyber Champions! 🏆🏆🏆



=====

Re: Occhio alle truffe telematiche!

Inviato da Marcodeli - 20/03/2020 14:44

Ed io che volevo sottoscrivere l'abbonamento online per "servizio a domicilio di pulizie a fondo tutto compreso";...

=====

Re: Occhio alle truffe telematiche!

Inviato da ninomiao - 20/03/2020 20:55

vuoi dire che il servizio di Troie multinazionalita' a domicilio che mi hanno proposto a 19.90 euro al mese potrebbe essere una truffa ?

vuoi dire che la mia prenotazione per "insaziabile ninfomane moldava" potrebbe non avere seguito ?

vorresti insinuare che la mia GS 1250 full optional nuova , famoso concessionario Bielorusso , a 2999 euro potrebbe arrivare con qualche giorno di ritardo ?

...non posso crederci...

=====

Re: Occhio alle truffe telematiche!

Inviato da GiBi - 21/03/2020 01:02

Beh, prima consigli di non cliccare e poi metti un link da cliccare 🤖

E chi lo conosce???

E siamo sicuri che il messaggio lo ha messo Gio? 🤖

=====

Re: Occhio alle truffe telematiche!

Inviato da muccopezzato - 21/03/2020 12:56

per mè se ci clicchi sopra esce il Maresciallo che ti dice.....STO KAZZO!!!!!!! 🤖

=====

Re: Occhio alle truffe telematiche!

Inviato da Franz3000 - 22/03/2020 09:56

In realtà qualche regalo in rete si trova.

Sul sito

solidarietadigitale.agid.gov.it/#/

ci sono un sacco di cose offerte gratuitamente. Per il momento ho fatto solo l'abbonamento a infinity gratuito per due mesi.

Ma ci sono corsi di lingue, ebook, programmi, etc..

Molto interessante

=====

Re: Occhio alle truffe telematiche!

Inviato da GriGio - 22/03/2020 11:16

Franz, queste sono lodevoli iniziative distribuite da un sito governativo, che appunto, in evidenza segnala (copio&incollo):



ATTENZIONE AGLI SCIACALLI

Facendo leva sull'emergenza coronavirus, circolano e-mail e PEC che promuovono prodotti dalle dubbie funzionalità, a volte veri e propri malware. È necessario adottare misure extra di sicurezza ed una maggiore attenzione alle truffe. [Leggi](#) come fare.

Vi invito a leggere tutte le avvertenze qui:

www.cert-pa.it/notizie/coronavirus-attenzione-agli-sciacalli/

=====

Re: Occhio alle truffe telematiche!

Inviato da Franz3000 - 22/03/2020 12:28

Si esatto, concordo, ho segnalato il sito governativo perchè almeno quello pare sicuro. 🇮🇹

=====

Re: Occhio alle truffe telematiche!

Inviato da MarchesedelGrillo - 22/03/2020 23:33

Giò....clicca e inserisci i dati del Maresciallo!!!! È lui il padrone del forum!!!!

=====

Re: Occhio alle truffe telematiche!

Inviato da GriGio - 26/03/2020 11:24

In momenti di emergenza come quello che stiamo vivendo è ancora più importante prestare attenzione ai tentativi di frode informatica attuati attraverso l'invio di email (phishing), SMS (smishing), messaggi su app di messaggistica (WhatsApp) che contengono link o allegati dannosi, ma anche tramite chiamate telefoniche.

Per Crédit Agricole, sicurezza vuol dire anche protezione dei propri Clienti e delle loro informazioni. Per questo è importante per noi ricordare che la Banca non invia email o SMS per chiedere di confermare o inserire numeri telefonici e/o codici personali.

Segnaliamo quindi alcuni semplici accorgimenti per riconoscere i tentativi di frode online:

 prestare attenzione al dominio dell'email ricevuta. I messaggi di Crédit Agricole arrivano da @creditagricole.it

 ascoltare interamente il messaggio Securecall prima di inserire il PIN^{STB} Dispositivo per confermare le operazioni

 leggere attentamente le notifiche push di conferma delle operazioni online su app **Nowbanking** prima di procedere all'autorizzazione

 verificare la presenza del certificato di sicurezza del sito al quale si fa accesso, controllando che nella barra dell'indirizzo compaia "https" (tutti i siti Crédit Agricole lo prevedono)

 ignorare l'eventuale richiesta presente nell'email di accedere all'Home Banking: vai sul browser e digita direttamente www.creditagricole.it

 non comunicare credenziali e codici via email, SMS, chat o telefono. Crédit Agricole non contatta i propri Clienti per richiederli.

Per qualunque dubbio o sospetto sull'attendibilità del messaggio ricevuto, invitiamo a contattare il Servizio Clienti al Numero Verde **800771100** per verificarne la veridicità.