03.08.2020

Nuova ondata di phishing

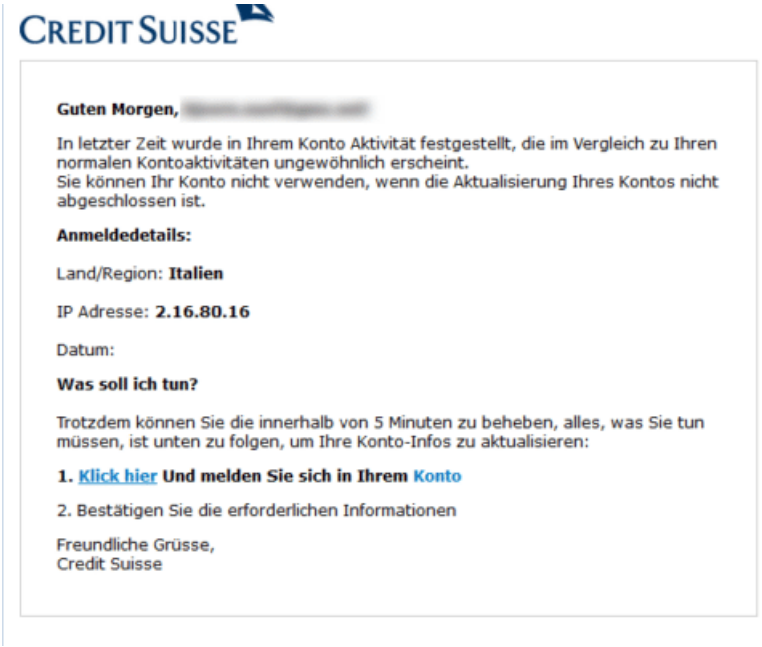
Attualmente circolano moltissime e-mail contraffatte di istituti finanziari che attirano i clienti dei sistemi di e-banking su pagine Web di banche, anch'esse contraffatte. Non lasciatevi ingannare!

I truffatori stanno provando ancora una volta, con forza, ad attirare i clienti bancari su imitazioni di siti di e-banking per mezzo di presunte e-mail di vari istituti finanziari. Lo scopo di questa ondata di phishing è appropriarsi dei dati d'accesso.

I truffatori mettono i clienti bancari sotto pressione: con un pretesto – adducendo magari che sia necessario aggiornare i propri dati personali altrimenti il sistema di e-banking verrà bloccato –vengono indotti a fare clic su un link che apre una pagina di e-banking contraffatta.

Diversamente dalle precedenti ondate di attacchi, le e-mail e i siti contraffatti hanno un grado di autenticità davvero ingannevole, sia per aspetto che per contenuti, con testi in un tedesco quasi perfetto e con i loghi originali delle banche.

Inoltre, le pagine dispongono di un certificato di sicurezza valido (certificato SSL) e si presentano alla potenziale vittima con una connessione sicura, con tanto di https:// e lucchetto nella barra degli indirizzi del browser. Le falsificazioni si riconoscono però dall'indirizzo, che non corrisponde a quello dell'istituto finanziario preso di mira (p. es. «https://entry.credit-suisse.services» o «https://entry.swisscard.services»).



CREDIT SUISSE

Guten Morgen, [redacted]

In letzter Zeit wurde in Ihrem Konto Aktivität festgestellt, die im Vergleich zu Ihren normalen Kontoaktivitäten ungewöhnlich erscheint.
Sie können Ihr Konto nicht verwenden, wenn die Aktualisierung Ihres Kontos nicht abgeschlossen ist.

Anmeldedetails:

Land/Region: **Italien**

IP Adresse: **2.16.80.16**

Datum:

Was soll ich tun?

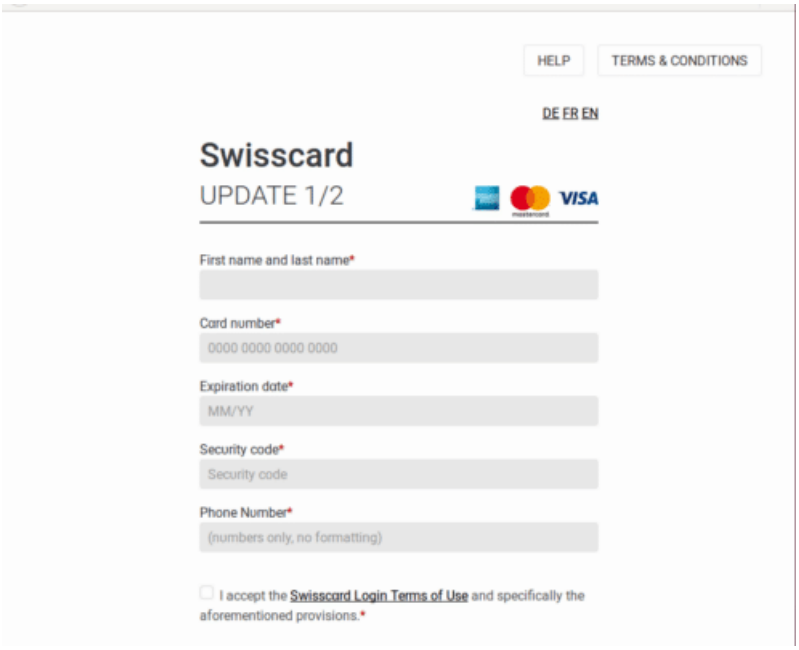
Trotzdem können Sie die innerhalb von 5 Minuten zu beheben, alles, was Sie tun müssen, ist unten zu folgen, um Ihre Konto-Infos zu aktualisieren:

1. Klick hier Und melden Sie sich in Ihrem Konto

2. Bestätigen Sie die erforderlichen Informationen

Freundliche Grüsse,
Credit Suisse

(https://www.ebas.ch/wp-content/uploads/2020/08/mail.png)



(https://www.ebas.ch/wp-content/uploads/2020/08/schritt2.png)

Con queste regole di condotta ci si può difendere dal phishing:

- Fate attenzione alle e-mail. Anche quando i mittenti sembrano noti, non aprite subito gli allegati, né fate clic sui link. In caso di dubbio, contattate il presunto mittente in un modo diverso dalla posta elettronica (p. es. chiamando il numero di telefono ufficiale della banca). **Gli istituti finanziari non chiedono mai di effettuare il login o immettere i propri dati d'accesso via e-mail!**
- Non lasciatevi mettere sotto pressione («Il vostro conto verrà bloccato», ecc.).
- Inserite l'indirizzo della pagina di accesso dell'istituto finanziario sempre manualmente, nella barra degli indirizzi del browser.
- Verificate la connessione SSL (lucchetto verde, nome del dominio, certificato).
- In caso di incertezze o dubbi contattate immediatamente il vostro istituto finanziario.
- Seguite le regole della protezione di base con le nostre «5 operazioni per la vostra sicurezza digitale» (https://www.ebas.ch/5steps) : creare regolarmente delle copie di backup, utilizzare antivirus e firewall, tenere aggiornati sistema operativo e programmi, fare attenzione ed essere vigili.

Ulteriori indicazioni sul tema del phishing sono disponibili qui (https://www.ebas.ch/phishing) .