03.08.2020

A new wave of phishing

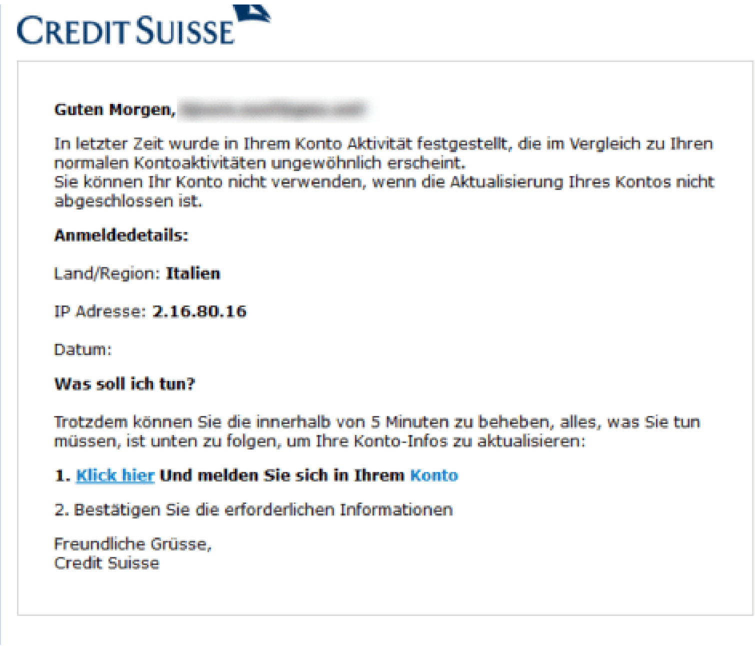
Currently, there is an increase in fraudulent e-mails from financial institutions. These are trying to lure e-banking customers to banking websites which are just as fake.

Fraudsters are currently stepping up their efforts once again to lure bank customers to imitation e-banking websites with purported e-mails by financial institutions such as the Credit Suisse. This current phishing wave is aiming to steal access data and credit card information.

In the process, fraudsters try and put pressure on bank customers: They are misled into clicking a link leading to a faked e-banking website under some pretext or other - for instance that customers will have to update their personal information.

In contrast to earlier waves of attacks, these e-mails and faked websites look deceptively genuine both visually and also as far as their contents are concerned, using near-perfect German and original bank logos. In addition, these websites have a valid security certificate (SSL certificate), therefore displaying a secured connection including https:// and a lock symbol in the browser address line to potential victims.

However, you can recognise such fakes by their address which does not agree with the one of the actual financial institution, e.g. «https://entry.credit-suisse.services» or «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?

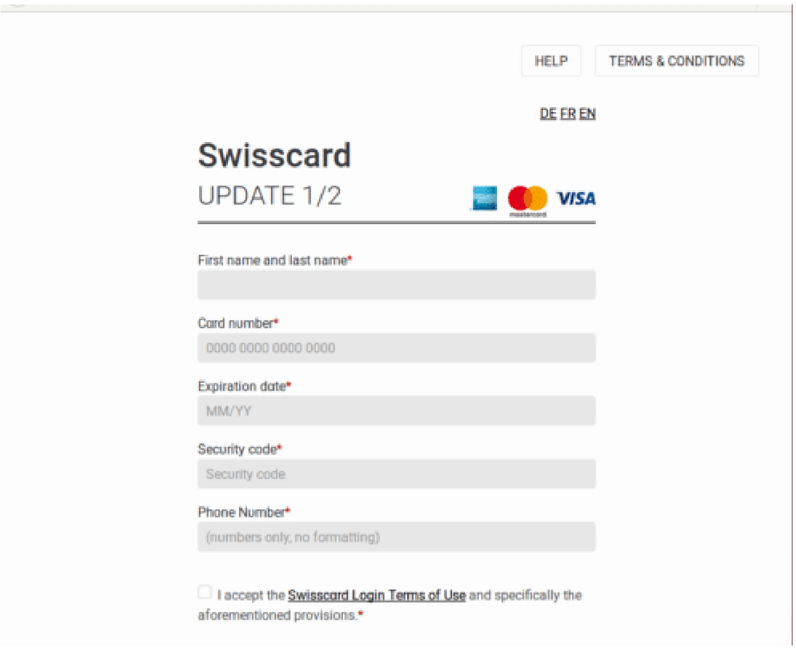
Trotzdem können Sie die innerhalb von 5 Minuten zu beheben, alles, was Sie tun müssen, ist unten zu folgen, um Ihre Konto-Infos zu aktualisieren:

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)



HELP TERMS & CONDITIONS

DE FR EN

Swisscard

UPDATE 1/2

First name and last name*

Card number*

0000 0000 0000 0000

Expiration date*

MM/YY

Security code*

Security code

Phone Number*

(numbers only, no formatting)

□ I accept the Swisscard Login Terms of Use and specifically the aforementioned provisions.*

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

You can protect yourself against phishing by observing the following rules of conduct:

- Please be careful when handling e-mails. Don’t ever open any annexes straight away or click on any links, even if the sender looks familiar. In case of doubt, ask the purported sender for verification via a different channel (e.g. the official telephone number of a bank). **Financial institutions will never ask you to log into their site or enter your access data by e-mail!**
- Don’t let anybody put pressure on you (“Your account will be blocked”, etc.).
- Always make sure to enter the address for your financial institution’s log-in page manually into your browser’s address line.
- Check the SSL connection (green lock, domain name, certificate).
- In case of doubt or error, please contact your financial institution immediately.
- Create a basic level of protection using our “5 steps for your digital security” (https://www.ebas.ch/5steps) : Create back-up copies regularly, use antivirus software and firewall, keep operating system and programs up to date, exercise care and remain alert.

Further information on the subject of phishing can be found here (https://www.ebas.ch/phishing) .