

03.08.2020

Nouvelle vague de phishing détectée

On assiste actuellement à une recrudescence des faux emails provenant d'instituts financiers. L'objectif est d'attirer les clients des services d'e-banking vers des sites bancaires piratés. Ne vous laissez pas tromper !

Des criminels s'emploient en ce moment à attirer les clients de différentes banques sur des copies de sites d'e-banking en utilisant des emails imitant les communications officielles des instituts bancaires. Le but de cette vague de phishing est de voler aux victimes leurs données d'accès.

Pour arriver à leurs fins, les escrocs font pression sur les clients en les incitant, sous un prétexte quelconque – telle que la mise à jour de leurs données personnelles sous la menace de voir leur compte verrouiller – à cliquer sur un lien conduisant vers un faux site d'e-banking.

Contrairement aux précédentes vagues d'attaques, les courriels de phishing et les faux sites Internet sont pratiquement identiques aux originaux, d'un point de vue graphique (avec les logos officiels) mais aussi au niveau des contenus, exprimés dans un français presque parfait.

Par ailleurs, les sites sont dotés d'un certificat de sécurité en cours de validité (certificat SSL) et s'affichent dans la barre d'adresse comme une connexion sécurisée en <https://> avec le symbole du navigateur. Mais la tromperie se reconnaît dans l'adresse, qui diffère de celle de l'institut financier (par ex. « <https://entry.credit-suisse.services> » ou « <https://entry.swisscard.services> »).



Guten Morgen, [Nom]

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?

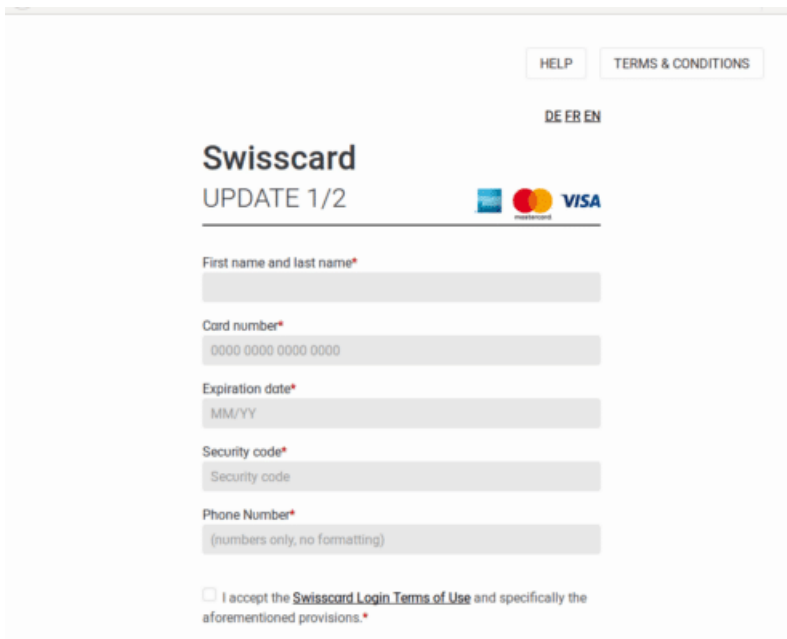
Trotzdem können Sie die innerhalb von 5 Minuten zu beheben, alles, was Sie tun müssen, ist unten zu folgen, um Ihre Konto-Infos zu aktualisieren:

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 ER EN

Swisscard
UPDATE 1/2

  **VISA**

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>)

Les règles de conduite suivantes permettent de se protéger efficacement contre le phishing :

- Faites preuve de prudence et de vigilance au moment d'ouvrir vos emails. Ne vous précipitez pas sur les pièces jointes ou sur les liens contenus dans le message, même lorsque l'expéditeur vous semble connu. En cas de doute, contactez l'auteur prétendu du courriel par un autre moyen (en utilisant par ex. le numéro de téléphone officiel de la banque). Les instituts financiers ne vous demanderont jamais de vous identifier ou de communiquer vos données de connexion via un link transmis par courriel.
- Ne cédez pas à la pression exercée par les menaces (par ex. : « votre compte sera verrouillé »).
- Tapez toujours manuellement l'adresse de la page de connexion de l'institut financier dans la barre d'adresse de votre navigateur.
- Vérifiez la connexion SSL (cadenas vert, nom de domaine, certificat).
- En cas de doute ou d'incertitude, contactez immédiatement votre banque.
- Assurez votre protection de base dès aujourd'hui avec nos « [5 règles pour votre sécurité numérique](https://www.ebas.ch/5steps) » : établissez régulièrement des copies de sauvegarde, utilisez une protection antivirus et un pare-feu, procédez régulièrement à la mise à jour de votre système d'exploitation et de vos programmes, faites preuve de prudence et de vigilance.

Pour en savoir plus sur le thème du phishing (ou hameçonnage), cliquez [ici](https://www.ebas.ch/phishing) (<https://www.ebas.ch/phishing>).