

23.03.2020

Do your banking from home - but securely!

Because of the corona virus, the Federal Council is recommending you stay at home if at all possible. Thanks to e-banking, there is generally not a problem with this. Some matters however require face-to-face contact with a customer consultant. Still, there are safe and secure alternatives for this, too.

To contain the spread of the corona virus, the Swiss have been asked to not leave their homes if at all possible. Many financial transactions, e. g. remittances, can be processed comfortably and securely via e-banking. Some matters however need to be discussed with your personal point of contact at your bank. How can you achieve this both safely and securely?

In many cases, a telephone conversation with your customer consultant is feasible and sufficient. In case there is a need however to present documents, such as contracts, or to explain some software, this might prove difficult. To this end, banks are currently sometimes offering video conferencing or remote support sessions. Please note our tips on [how to securely handle remote support \(https://www.ebas.ch/remotesupport\)](https://www.ebas.ch/remotesupport) on this issue.

Increased caution is called for in case of unexpected e-mails, SMS or Messenger messages or telephone calls - even if these seem to originate from a person or company you know. There are currently some deceptively authentic-looking phishing e-mails doing the rounds, purportedly sent by a German bank, which ask customers to enter their contact details on a bogus website. The closure of certain bank branches is stated as the reason for sending these mails. Similar phishing attempts are also to be expected in the name of Swiss financial institutions.

Criminals are generally exploiting the current situation involving the corona virus, sometimes quite shamelessly:

- Bogus e-mails sent out in the name of the Bundesamt für Gesundheit (BAG, Public Health Office) last week were meant to induce the recipients to install a piece of malware sent in the annex, disguised as a harmless document. This would have given the attacker total access to the victim's PC.
- The very next day, fraudsters, once again posing as the BAG, tried to obtain sensitive information with the help of telephone calls.
- Shortly after, e-mails emerged purporting to include a memo card on the spread of the corona virus, or an e-book on how to protect yourself against it in the annex. In reality, this was a Trojan.
- Since the last week-end, ransom mails have been circulating, with criminals threatening to infect the recipient with corona virus, since allegedly they know of his or her exact whereabouts.
- Last but not least, there is an increasing number of web shops offering hard to obtain products such as protective masks for sale. Once paid, they don't however then deliver.

Protect yourself against fraudsters by treating all electronic messages with great caution. Don't open any annexes or links included in them, unless you are able to check on the sender's authenticity for certain first. And don't entrust just any third party or unknown provider with your sensitive data about yourself and your online access details, neither via the Internet nor the telephone.

Information on further protective measures can also be found in our articles on [phishing \(https://www.ebas.ch/phishing\)](https://www.ebas.ch/phishing)

and [fraudulent support calls \(https://www.ebas.ch/en/fraudulent-support-calls/\)](https://www.ebas.ch/en/fraudulent-support-calls/).