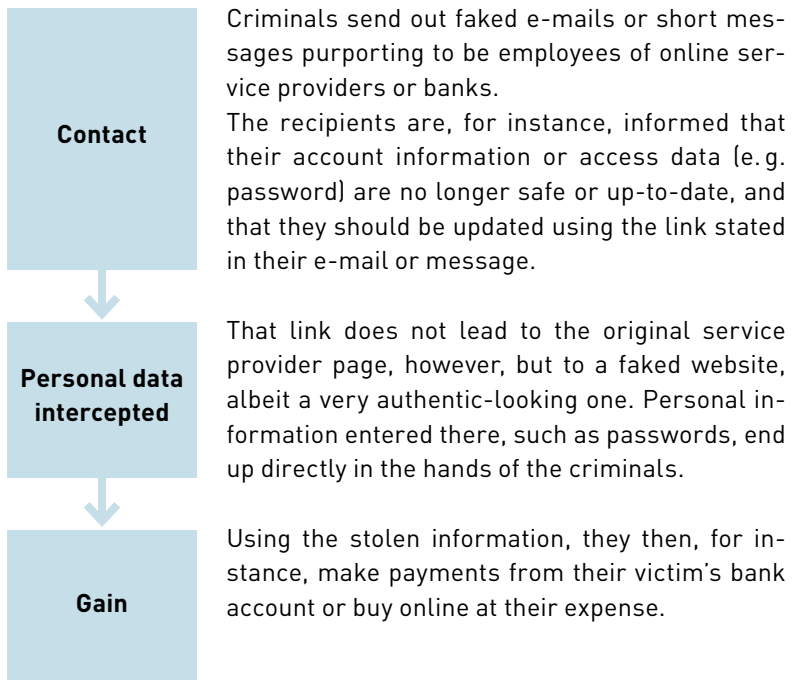# Phishing

How to protect yourself against phishing attacks

Police and Swiss Crime Prevention –
an office supported by the cantonal
ministries of justice and police,
in co-operation with the University of
Lucerne and "eBanking – but secure!"
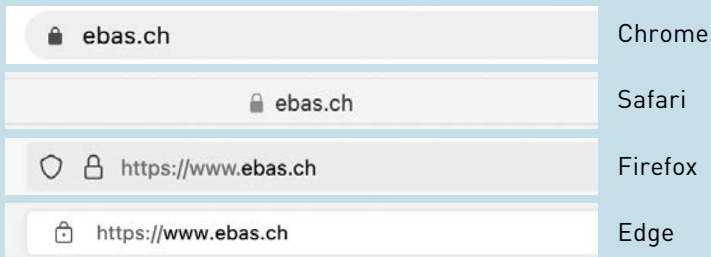
# If just one wrong click is enough ...

**Phishing is a made-up word that means sending out e-mail lures to fish for data. This involves theft of personal and sensitive information – usually passwords.**

When phishing, criminals will try to obtain passwords and other confidential information, such as credit card numbers, with the help of faked e-mails and websites. Attackers try to gain access to confidential information this way for financial gain. Usually, such criminals target log-in information for online service providers such as financial institutions (e-banking), online auction houses or online shops. Short message technology such as texts, MMS and WhatsApp are also being used increasingly for phishing. The sneaky thing about "smishing" (SMS+phishing) is that most of the criteria that filter out phishing e-mails are not used for this sort of messaging.

**Contact**

Criminals send out faked e-mails or short messages purporting to be employees of online service providers or banks.
The recipients are, for instance, informed that their account information or access data (e. g. password) are no longer safe or up-to-date, and that they should be updated using the link stated in their e-mail or message.

**Personal data intercepted**

That link does not lead to the original service provider page, however, but to a faked website, albeit a very authentic-looking one. Personal information entered there, such as passwords, end up directly in the hands of the criminals.

**Gain**

Using the stolen information, they then, for instance, make payments from their victim's bank account or buy online at their expense.

**Protect yourself against phishing and smishing by:**

- never clicking on any link sent to you via e-mail or short message, or scanned in via QR code to log into any online service provider or financial institution site.
- never filling in any forms received by e-mail or short message that ask you to enter log-in information.
- always entering the address for your online service provider or bank's log-in page manually via the browser address line.
- checking there is an TSL connection (http**s**://, lock symbol) when calling up a log-in page, and verifying that the internet address shown in the address bar of your browser actually indicates that you have reached the correct page.

| | |
|---|---|
| 🔒 ebas.ch | Chrome |
| 🔒 ebas.ch | Safari |
| ◯ 🔒 https://www.ebas.ch | Firefox |
| 🔒 https://www.ebas.ch | Edge |

- contacting your online service provider or bank if you are not quite sure or something is not clear.

Test your knowledge of phishing with our phishing quiz by "eBanking – but secure!" at **www.ebas.ch/phishingtest**

Received a phishing mail or a smishing message, or found a phishing page? Report these at **www.antiphishing.ch**

Further information:
**www.ebas.ch/phishing**
**www.skppsc.ch/phishing**

# SKPPSC

Swiss Crime Prevention (SCP)
House of Cantons
Speichergasse 6
CH-3001 Bern

www.skppsc.ch

This leaflet was created in co-operation with the
University of Lucerne and "eBanking – but secure!"

www.ebas.ch | www.ebankingbutsecure.ch

**HSLU** Lucerne University
of Applied Sciences
and Arts

**eBanking** but secure!