

Phishing

How to protect yourself against phishing attacks

Your Police and the Swiss Crime Prevention – an office of the ministries of justice and police of the Cantons.

If just one wrong click is enough ...

Phishing is a composite word which means something like "fishing for passwords". 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 to obtain financial gains. Usually, such criminals target log-in information for online service providers such as financial institutions (e-banking), online auction houses or online shops.

Contact

Criminals send out faked e-mails purporting to be employees of online service providers or financial institutions.

The recipients of such e-mails are for instance informed that their account information or access data (e. g. user name and password) are no longer safe or up-to-date, and that they should be updated using the link stated in their e-mail.

Intercepting personal data

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

Gain

Using the stolen information, the perpetrators then, for instance, carry out remittances from their victim's bank account, buy online at their cost or place faked offers with online auction houses.

Protect yourself against phishing by:

- never clicking on any link sent to you via e-mail 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 and asking you to enter log-in information.
- always entering the address for your online service provider or financial institution's log-in page manually via the browser address line.
- checking there is an SSL connection (https://, 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.



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 found a phishing page? Report these on **www.antiphishing.ch**

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



S<??S(

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

Lucerne University of Applied Sciences and Arts **@Banking** but secure!

HOCHSCHULE LUZERN

Informatik FH Zentralschweiz Autumn 2018