Media release

Hacker attacks on Swiss banks – what to do?

The Swiss Internet Registration Office Switch is currently reporting that a large-scale attack against the e-banking accounts of 12 Swiss banks is afoot. A new-style Trojan called «Retefe» is the malware involved.

Lucerne, 23/07/2014 - Attacks follow this pattern: A customer opens a spam mail, and the «Retefe» Trojan contained in this mail manipulates his computer. It will change the entry to a fake name server, so that his computer will always have a fake website returned even if the address was entered correctly. The Trojan will also install a fake so-called root certificate, so that the infected computer will even certify the fake website to be purportedly «authentic». Then this Trojan will delete itself and will no longer be recognized as malware - all of which is rather insidious!

As soon as this customer now retrieves the e-banking website of his bank, he will be diverted to a fake server. He will be presented with a fake website of his bank, which will be classified as «authentic» due to the fake root certificate installed. And there we have it. Once this customer now enters his security details, they are passed on to the hackers. The customer will then be asked to install a manipulated app on his smartphone, which subsequently sends the bank's security SMS (mTAN) on to the hacker. In this way, the attackers now has full control!

What to do? - The Information Security Competence Centre of the Hochschule Lucerne recommends the following:

- The first step of the attack is a case of phishing. Such e-mails are never sent out by financial institutions and should be deleted without reading/opening them. In no case should you open any links or attachments. Further information can be found under: https://www.ebas.ch/phishing
- It is also of utmost importance that up-to-date anti-virus software is installed on every computer. This will recognize any Trojans and warns customers before they are installed.
- Should customers be asked to install an app on their smartphone during e-banking, this constitutes an attack. Now - or in case you encounter any other unusual behaviour during the log-in process - you should contact your financial institution immediately. Any fraudulent payments can be stopped this way.

Further information can be found here: https://www.ebas.ch

«eBanking – but secure!» service

The www.ebankingbutsecure.ch website is one of four services the University of Lucerne offers to their now 36 financial institution partners. In a holistic approach, «eBanking – but secure!» also runs public consumer courses. In addition, we train our financial institution partners' helpdesk staff and customer consultants in current and security-related issues, and we are also monitoring the Swiss media for any topics related to e-banking security.

Further information can be found under: https://www.ebankingbutsecure.ch/mediasection

---

University of Applied Sciences, Lucerne - Economy

The Institute for Business Informatics of the University of Lucerne - Economy operates the Information Security Competence Centre. A team consisting of lecturers and scientific staff specializes in information security. The emphasis here is on education (Bachelor and Master in Business Informatics), advanced education (e.g. Master of Advanced Studies in Information Security) plus research and services for third parties (EBAS, IT audits, etc.).

Further information can be found under: www.hslu.ch/iwi

Media contact details

University of Applied Sciences, Lucerne - Economy
Oliver Hirschi
Institute for Business Informatics
6002 Lucerne, Switzerland

https://www.ebas.ch/en/contact