Account hacked! What to do?

Every bank customer's nightmare: Criminals gain access to your account and clear it out. If this has already happened, the main thing is damage limitation – and to learn from this.

What to do in case of unauthorised access to your own bank account:

- If there are suspicious transactions or errors when logging into your e-banking facility, you should immediately contact your financial institution and have them block your e-banking facility, your accounts and cards.

- Disconnect any devices which could be affected by hacker or malware activities from the Internet straight away, switch them off, or set them to flight mode. You should not however reset your devices directly, since the police might request them for forensic analysis.

- Change your passwords on a separate, non-infected device. Wherever possible, activate two-factor authentication.

- In case of actual fraud, report this to the police. Note down as many available details on this fraud or attack as possible.

- In the future, protect your mobile device against unauthorised access with our "5 steps for your digital security" and our tips on secure e-banking.

How can a bank account be hacked?

Swiss financial institution e-banking portals are very well protected against hacker attacks. This should basically preclude any chance of criminals obtaining direct access to a bank's computer system.

But unwary bank customers still pose a risk: Should hackers manage to obtain someone's access data, they can use them to log into an e-banking facility unnoticed to trigger transactions or access confidential information. Some examples of the methods they use to do so are phishing attacks (https://www.ebas.ch/en/phishing/) or specific malware infections (https://www.ebas.ch/en/malware-infection/) . The only option left to victims then is to limit the damage done.

How to react appropriately in case of loss?

The most important measure first: React quickly in case of any suspicion! In case actual fraud occurred, you must immediately block your e-banking facility and all related accounts involved to prevent any further money disappearing.

In case you suspect fraud, for instance if there are suspicious transactions or error messages when e-banking, you should contact your financial institution straight away to co-ordinate any steps necessary. If your suspicion of fraud is confirmed, you should report this to the police in the first instance.

In case you cannot establish how criminals were able to obtain access to your account once you have discussed this with your financial institution, you should generally assume that foreigners have obtained your access data, and that your device has been infected by malware, for instance a banking Trojan.

To prevent any further misuse of your potentially stolen access data, you should change the password

(https://www.ebas.ch/en/4-protecting-online-access/) of your e-mail inbox plus those of all your online accounts as a precautionary measure. Please make sure though not to do so on the computer or mobile device potentially infected, but from a different device. Your e-banking access should be blocked first. You should only change your passwords later, once you have been able to clarify the situation with your financial institution.

Wherever possible, you should set up two-factor authentification – this will provide you with a much higher level of access protection.

You should disconnect your device from the Internet and switch it off, or put it into flight mode. However, please only reset (https://www.ebas.ch/en/clean-windows-10-installation/) it once any potential police investigations have been concluded.

And last but not least, you will want to protect yourself properly against any future attempts at fraud. You should therefore make sure to follow our "5 steps for your digital security" (https://www.ebas.ch/en/5-steps-for-your-digital-security/) and our tips for secure e-banking (https://www.ebas.ch/en/tips-for-secure-e-banking/) – because if you take the proper precautions, hackers don't stand a chance!

Urgent measures in case of suspicion:

- *Contact your financial institution and have your account blocked immediately*
- *Disconnect the Internet*
- *Change passwords*
- *Report to the police*

Can banks detect and stop misuse?

Individual financial institutions have a fraud detection system in place, which reports or even automatically stops suspicious transactions. These systems are becoming ever more effective, but don't offer a 100% level of protection. And fraudsters proceed ever more cleverly and unobtrusively to outwit such systems. You should therefore take personal responsibility and not just rely on your bank being able to protect your accounts against unauthorised access, for instance in case of a phishing attack, at all times.

Who is liable in the event of damage?

It is not possible to provide a general answer to the question of liability, since this has to be evaluated on a case-by-case basis. Next to the actual issue of liability, due diligence is the deciding factor here. Since attackers generally remain unknown and operate from abroad, criminal investigations often prove to be difficult. Frequently, unwary middlemen, so-called money mules (../en/money-mules-financial-agents/) , are also used to disguise such transactions. In many cases, the money transferred is lost. Both financial institutions and their customers must categorically exercise due diligence when operating bank accounts and handling the money deposited there. Courts will therefore check for any potential infringement of due diligence, something which a customer just might be guilty of – for instance, if he or she has disclosed his or her access data to a third party, whether deliberately or not. You should therefore protect your account as a preventative measure (../en/tips-for-secure-e-banking/) , so that you will not have to deal with any questions of liability in the first place!