Identity theft

Identity theft (also called identity fraud) is a scam involving someone's user account – i.e. their identity – being misused by a third party. In the process, attackers either hack a personal account or create a new one in the name of their victim. Their aim is to illegally gain from their actions, or to damage someone's reputation.

This is how you protect yourself against identity theft:

- Be economical with any personal data you disclose and wary when doing so.
- Use secure passwords (https://www.ebas.ch/en/4-protecting-online-access/) .
- If possible, also activate your so-called two-factor authentification (https://www.ebas.ch/en/4-protecting-online-access/) options.
- Never forward any PIN codes received, and don't confirm any SMS or Messenger messages.

You may receive an e-mail with "Urgent" in the subject line, saying something like: "Dear John, I urgently need your help. I am currently abroad. I was robbed, and my credit card and smartphone have been stolen. I now need CHF 500 for my return flight home. Could you possibly remit this sum to my Western Union account as soon as you can, please? I will of course repay you as soon as I get back."

E-mails like that are not uncommon. Fraudsters hack an e-mail account or a social network account (e. g. Facebook) and go begging contacts for money.

The above e-mail is one potential shape identity theft could take – but there are many others in today's digital world, too: Fraudsters open and/or take over a social network account and entice "friends" to click links. They open a PayPal account in a false name and start shopping. They shop using strangers' credit cards. They fraudulently access e-banking facilities and siphon off money.

If you suspect a fraudulent identity

On the Internet, it is no problem at all to pretend you are someone else. Your name, date of birth, address, telephone number – in our digital age, it is not always easy to check the spread of such information. A healthy dose of distrust (https://www.ebas.ch/en/5-exercising-care-and-remaining-alert/) is therefore appropriate.

If you notice a potentially forged user account or a false identity, you should follow the recommendations below.

This is how to proceed in suspicious cases:

- To verify someone's identity, ring the person in question and ask them a couple of questions which only that particular person could answer.
- In case someone fraudulently pretends to be a person you know: Let the real person know immediately.
- Notify the platform provider of any potentially faked account. The more people report such an account, the quicker it will get deleted.

Copyright – All rights reserved. Lucerne School of Information Technologies

Stolen identity

If you find that you are affected yourself and that someone is abusing your identity, you should take immediate action. Some indications this is the case could be:

- Inexplicable transactions on your bank account
- Spurious payment requests
- Passwords correctly entered into user accounts which are not accepted
- Messages by friends or acquaintances stating they have received unusual e-mails, SMS or Messenger messages from you which you never sent

This is how to proceed in fraud cases:

- Immediately change your password for the account involved, or block it.
- Notify the platform provider of this fraud case.
- Let your friends and acquaintances know about this fraud case.
- Let the National Cyber Security Centre (NCSC) know using their report form (https://www.report.ncsc.admin.ch/en/) , and also file charges with your local police station.

A digital identity consists of data describing a real person on the Internet. These are usually linked to a personal user account. A real person can have several such user accounts (e. g. e-mail, Facebook, e-banking, etc.) on the Internet. Some data making up part of your digital identity are for instance your name, date of birth, address, e-mail address, account number, etc.

Copyright – All rights reserved. Lucerne School of Information Technologies