Identity theft prevention checklist

How to protect yourself against attacks

There is no infallibly sure protection against identity theft and misuse. That's something the experts stress again and again. However, there are some security precautions that make things more difficult for attackers.

1. Passwords should be longer than eight characters and made up of digits and special characters as well as letters.

2. Allocate different passwords and usernames to different services and change them regularly. That way, you prevent your profiles being connected to create an overall profile that tells criminals what they want to know about you.

3. You can be even more secure with two-way or two-factor authentication. This involves a person wanting to log on to a computer needing a code to enable them to do that, which is sent simultaneously to their smartphone.

4. Keep your web browsers, operating system and anti-virus software up to date by downloading updates as soon as they're available.

5. When using public WLAN networks and devices that aren't your own, Facebook and similar sites should always be accessed via an "HTTPS" connection.

6. Activate the "encrypted connection" (SSL encryption) in your e-mail program.

7. Sign out of services you've been using in public networks once you've finished.

8. Avoid using online banking and other vulnerable accounts on public networks.

9. Take a look at the imprint or GTCs of a website to check that what's on it is being offered by a credible provider.

10. Never give out more details than necessary (if you have the option, don't enter them).

11. Google your own name. You can set up a Google Alert as a way of checking when and where your name gets mentioned online. An occasional image search can also be useful.

12. Don't respond to e-mails whose senders you don't know and certainly don't under any circumstances open attachments.

13. Be careful to whom you give personal details and information on social networks.

14. Set up answers to security questions that only you know.