22.05.2026

"Convenience" – the biggest security risk

In our modern digital world, time is the most valuable currency. Everything has to happen straight away, intuitively and with the least of effort required. Banks have reacted to this requirement and designed their e-banking facilities as user-friendly as never before. But exactly this pursuit of maximum convenience bears a danger widely underestimated. While you can currently compare financial institutions' technical security systems to well-fortified strongholds, humans still remain the one variable whose desire for convenience often serves to open the gates.

The psychological conflict between security and convenience

In information technology, security and convenience are usually diagonally opposed to each other. Real security often requires additional steps, a conscious pause and a certain cognitive effort. Yet our brains are programmed to save energy and take the path of least resistance, with the result that security measures are often considered annoying barriers, to be circumvented or done with as soon as possible.

One classic example is choosing passwords. A cryptic, long password you laboriously have to remember is rejected in favour of a simple, familiar combination – even more dangerous still if you use an identical password for all your services for the sake of pure convenience. Criminals know this: Just one successful attack on a badly secured online shop can turn into a pass key to the whole digital life of a user this way.

When speed is prioritised before diligence

The biggest threat though is created during a transaction itself. Modern scams such as social engineering (https://www.ebas.ch/en/social-engineering/) directly target our tendency to get things done quickly and without thinking too much about them. When a push message is received on their smartphone asking them to release a payment, many people tend to simply push the confirm button almost reflexively. In their haste, people often miss whether the amount, recipient or time of the request are even feasible.

Scammers deliberately exploit this "click mentality". They exert time pressure on their victims or simulate a familiar routine. If you just quickly confirm a purported security check during times of stress, that often means you already lost. In the process, it is just this short break – taking time to consciously read a text confirmation or check the URL displayed in your browser – which forms the vital barrier protecting you against loss of your money.

An argument for "conscious inconvenience"

To effectively protect themselves, users must learn to accept a certain level of inconvenience as a quality characteristic of security. Setting up a password manager, consistent use of two-factor authentification (2FA) or manual entry of a bank's URL instead of clicking on a link contained in an e-mail are small investments of time, which offer an enormous level of protection.

Technology alone is not enough. True digital resilience results only from a healthy dose of suspicion and the willingness to sacrifice a bit of convenience. Security on the Internet is not a constant state, but an active process. If you are prepared to take the "extra step", you will make it so much harder for criminals than mere firewalls alone ever could. In the end, a little effort is a small price to pay for the certainty that your money will remain safe.

Potential protection strategies

To escape from the convenience trap, even some small behavioural changes will help to significantly increase security.

- **Consciously slowing down:**
  Never take any decision when pressed for time. Take your time and check things thoroughly.
- **Strict password discipline:**
  Use unique, complex passwords (https://www.ebas.ch/en/4-protecting-online-access/) , not ever used for several services at once. A password manager will help you to keep track without security having to suffer for the sake of convenience.
- **Consistent two-factor authentification (2FA):**
  Activate this additional confirmation on a second device wherever possible. Don't consider this additional step a barrier, but important digital insurance against identity theft (https://www.ebas.ch/en/identity-theft/) .
- **Automation:**
  Don't leave security to your memory. Activate automatic updates (https://www.ebas.ch/en/3-preventing-with-software-updates/) for your operating system, your browser and apps to ensure critical security gaps are closed immediately without you having to actively think about it.
- **Keeping a critical distance to convenience features:**
  Functions such as FaceID or fingerprint log-ins are convenient, but tempt you to act reflectively. Briefly question every biometric request to ensure you don't grant strangers access by accident.