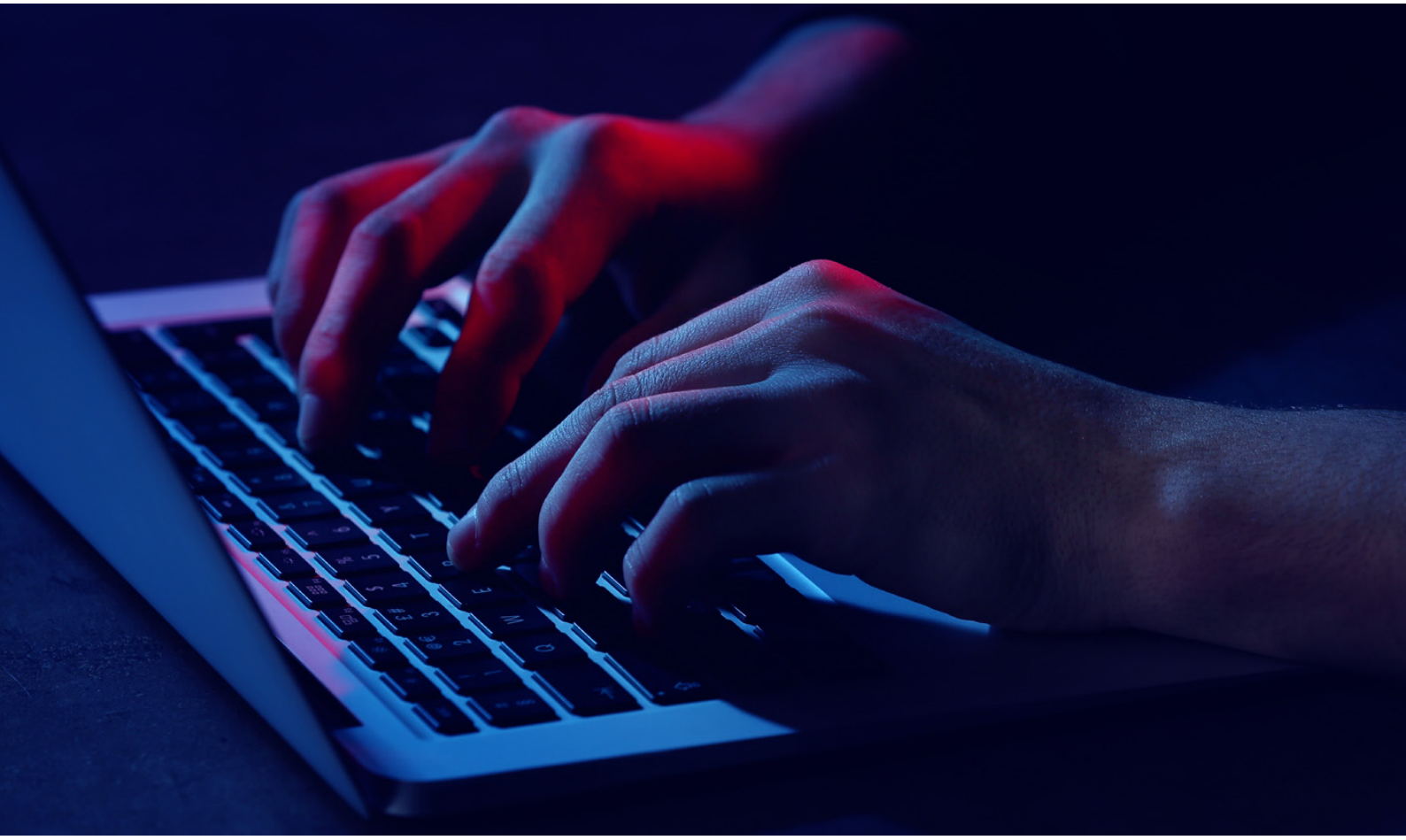
sosafe

Working Securely from Home

The Risks of Mobile Work
and How to Stay Safe



Home Office as a Target

→ Damages in the billions

In Germany alone, home-office based cyberattacks cause over 50 billion euros in damages every year.

→ Increased risk of losses

Data security incidents cost organizations an average of 4.42 million USD, and an additional 1.07 million USD when remote work is included.

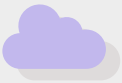
→ Insufficient monitoring

Only 38% of organizations secure work devices with a connection to the company network.

What are the Risks of Working from Home?

Phishing

Cybercriminals are merciless in their use of topical issues for manipulative cyberattacks (e.g., over the phone or by email).



Use of cloud tools

Cloud tools are often used for remote work, but they are not always officially authorized. Attackers use these tools as a potential gateway to company systems.

Uncertainty

New working conditions make the potential for risk even greater. Half of all employees click on phishing emails sent during the implementation of collaboration tools.

No grapevine

Employees working remotely click on phishing emails at three times the rate of employees working from the office. This could partially be due to the lack of direct communication with coworkers.

Bring-your-own-device

Many employees make up for the lack of company devices by using their personal end devices, such as laptops or smartphones, for work purposes. The company's IT department cannot inspect these devices for irregularities.

Insufficiently protected workplaces

If workplaces are not sufficiently protected against third-party access, criminals are able to obtain company data.

5 Tips for Working Securely from Home

- ☑ Store documents and portable data storage media in a location where even your family or guests cannot access them.
- ☑ Always lock your screen or computer if you are not right in front of it. Also ensure that your screen is not visible to others (e.g., through your window).
- ☑ Only use password-protected WiFi and, for example, connect to your company network via a VPN. Only use (cloud) tools approved by your IT department.
- ☑ Never connect uninspected, external data storage media (e.g., USB flash drives) to your work device.
- ☑ Render confidential documents unrecognizable and illegible before disposing of them.

Learn more about information security in the home office on our awareness blog