Wumbel®

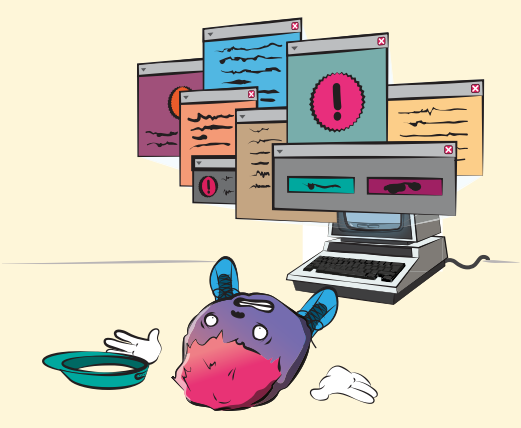
Cyberattacks then what?

DR. BITTNER GROUP

Imagine IT support receives a call: **"My password no longer works—please reset it."** However, behind the voice is an attacker who has gained access to a phone number through SIM swapping. This is exactly how employees of British companies were deceived.

Or another scenario: You are in a video conference, and a supposed executive gives you clear instructions to transfer tens of thousands of dollars. Everything seems real. But the participants are AI-generated deepfakes. **Only you are real.**

These examples show that cyberattacks have long been playing on the human level. They no longer rely solely on technical vulnerabilities, but on **deception, trust, and time pressure.**

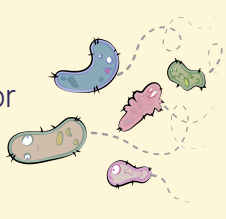


What classifies as a cyberattack?

Cyberattacks come in many forms. In addition to classic hacking using malware or exploiting security vulnerabilities, there are increasingly attacks that target people directly.
Typical methods include:

Phishing and spear phishing:
Deceptively genuine emails or messages that request sensitive data or contain malicious links.

Vishing (voice phishing):
Fraudulent calls in which attackers pretend to be support or bank employees.

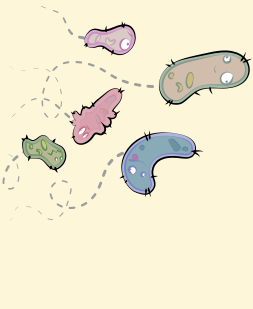


Smishing:
Manipulative SMS or messenger messages with links or requests to share data.

SIM swapping:
Attackers take over your mobile phone number by activating a replacement SIM card in their name.

Business Email Compromise (BEC):
Fake emails sent on behalf of executives with the aim of obtaining bank transfers or sensitive information.

Deepfakes:
AI-generated voices and videos that appear deceptively real and are used in meetings or calls.



What makes a cyberattack really dangerous?

1. Social manipulation instead of classic hacking:
Firewalls and antivirus programs can be tricked when people are manipulated.

2. Focus on data protection: Even seemingly harmless data such as phone numbers, email addresses, or membership numbers are considered personal data under the GDPR and are worthy of protection.

3. Immediate consequences: Stolen data, disrupted supply chains, and millions in losses are not uncommon.

An Overview of typical attack vectors

Helpdesk manipulation:
Attackers convince IT support to reset passwords, supported by SIM swapping.

Fake support calls: Attackers pose as IT staff to trick victims into downloading malware.

Deepfake fraud: AI-generated video conferences in which executives were imitated to obtain fraudulent transfers.

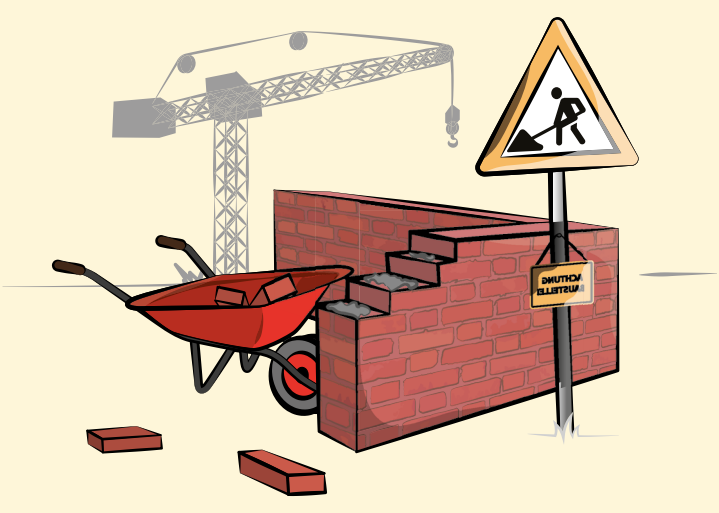
How can you protect yourself?

1. Clear verification processes: Password resets only after strict verification, e.g., by callback via known numbers or multi-factor authentication via independent channels.

2. Regular awareness training: Training on social engineering, deepfakes, and fake support requests—practical and repeated.

3. Clear internal communication: Firmly establish and publicize:
We never ask for passwords by phone, Teams, or text message.
Official requests are made exclusively through defined support channels.

4. Quick action in an emergency: Immediately report suspicious calls, messages, or video conferences to IT security and document all details.



Conclusion: You are the last line of defense!

Cyberattacks have long been part of everyday life—and they target the weakest link: people. They rely on trust, deception, and time pressure. **Establishing clear processes, continuously raising awareness among employees, and securing official communication channels makes an organization resilient.**

This prevents a seemingly harmless phone call or a deceptively genuine video conference from turning into a security incident costing millions.

Dr. Bittner Consulting GmbH & Co. KG

Podbielskistraße 386
30659 Hannover

Servicenumber: 0800 88446688
Email: office@drbg.de

DR. BITTNER GROUP