bankenverband

Companies under attack: **cybercrime**

Berlin, October 2019

Foreword

Companies are increasingly being targeted by cybercriminals. They are first spied on via the internet, with attempts at fraud then focusing on an individual employee who is cleverly manipulated to unwittingly divulge confidential company information or make payments to designated accounts. This new type of fraud, referred to collectively as ‘social engineering’, is not easy to detect. Learn here what forms it can take and how to protect your company.

Content

How do **cybercriminals operate?**

Social engineering covers malicious phone calls, emails or other kinds of manipulation intended to induce company employees to perform certain acts or divulge information. Many of the following scams are launched after information about the company has been collected beforehand (e.g. from its website, public registers, and social media used privately and professionally). While the strategies attackers adopt vary, what they all have in common is that they exploit human qualities such as helpfulness, trust, fear or respect for authority. Employees are manipulated so that they act in good faith but unsuspectingly damage their company in the process.

'Bogus boss' scam ('CEO' scam)

An employee authorised to make payments (e.g. in the book-keeping department) receives a fake message supposedly from the company's CEO or CFO. This may not only be in writing: cases have been reported where a voice is impersonated on the

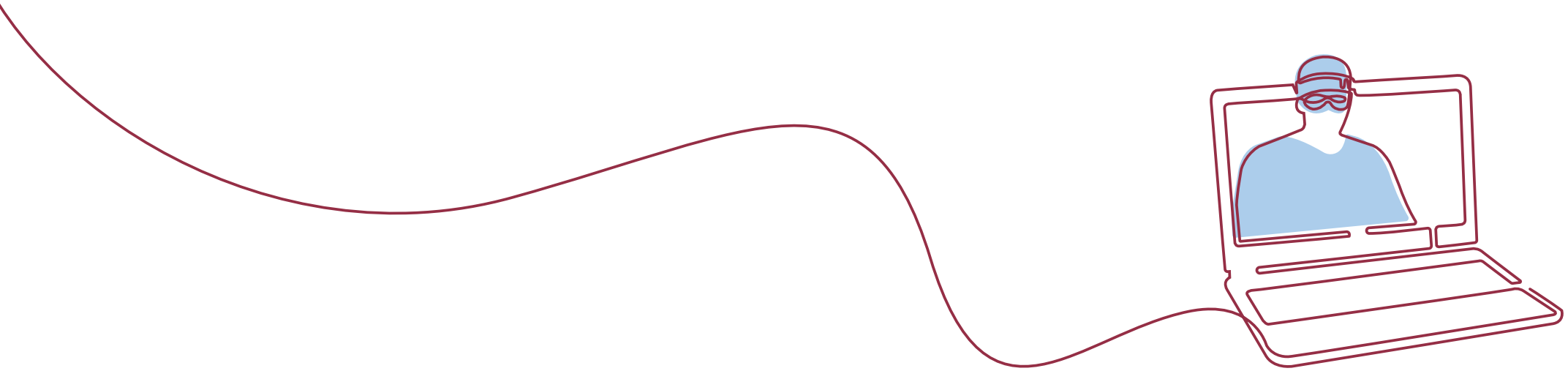
phone using AI-based software. Here, a machine-learning algorithm mimics the way the supposed boss speaks. The fraudster asks the employee concerned to conduct an urgent, confidential financial transaction. Criminals adapt the reasons they give for this to fit the company targeted: these can be, for instance, a takeover deal, payment of a fine, or the like. The employee is, at any rate, instructed to keep absolutely quiet about the whole transaction within the company. After contact is initially established, phone calls or emails ostensibly from advisors or lawyers hired by the company may then follow. Often such transactions are given added credibility through fake documents, e.g. invoices or notarised deeds. Their purpose is to get the employee to make a seemingly urgent large-value payment to a designated bank account that is often located abroad. This type of scam may be repeated again and again until the company concerned notices it.

‘Mandate’ scam

The criminal’s aim this time is to divert payments to another bank account by replacing a legitimate payment mandate with a fake payment mandate of their own. They can do so using a simple email informing the recipient about a new bank account number ostensibly on behalf of a business partner, e.g. a supplier. Cases have also been reported, however, of supposed changes to salary account details being notified or of notices being put up in blocks of flats about a purported change of landlord. A particularly devious way of implanting a new bank account is hacking into existing email communication. The scam is usually only detected when the legitimate payee points out that they haven‘t received the expected amount.

‘Fake invoice’ scam

In this case, criminals send fake invoices for imaginary services that may well be very similar in content and amount to an invoice that is expected. In some cases, replicated letterheads featuring different bank account details are used in real business partners’ email format. Internal control mechanisms may be bypassed by, for example, disguising the email with attached invoice as one supposedly forwarded by the head of the company with a request for immediate attention without the need to obtain clearance.



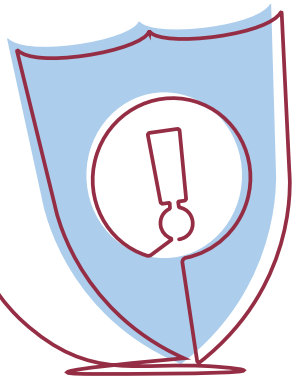
‘Overpayment’ scam

In this case, the victim receives funds that they cannot identify. Later, they are contacted by someone and asked to return part of the money. This someone may be a supposedly new business partner who brings a much lower amount into play. Though the overpayment was made direct to a bank by cheque, the fraudster talks about an error by their book-keeping department. If the victim then decides to repay the excess amount, the cheque bounces shortly afterwards. Cases have also been reported where the subsequent victim is given fraudulent payment channels or account numbers to correct the supposed book-keeping error.

‘Remote access’ scam

Criminals pretending to be bank technical support staff sometimes contact a company, claiming that its banking software needs to be updated and that all the company’s authorised signatories have to be on hand for this. In the fake support calls they subsequently receive, the company’s authorised signatories follow the criminals’ instructions (e.g. they plug in authorisation media, enter banking or signature PINs or allow remote access to the company’s computer). Then access data is altered and payments, even those involving distributed signatures, are authorized electronically. To disguise the attack, the company is told that, because of the supposed software update, online banking will not be available for the next day or two. Cases have also been reported where account statements are downloaded using a company’s access data, manipulated and then sent to customers. This prevents such a scam from being detected quickly.

Tips on **how to protect** your company



1. Check risk-prone processes

Where could there be a gateway for such scams in your company? Not just entering or authorizing payments are security-sensitive processes. Changes to master data (account numbers, mailing addresses) should also be monitored by way of specific checks or clearly defined processes (also for salaries).

2. Create an open corporate culture and allow queries

Where employees notice unusual transactions or dealings, they should always be able to query these as far as management level: obtaining confirmation personally or over the phone from a dedicated contact person or a superior in the company can prevent fraud.

3. Encourage careful social media management

Contact solicited by unfamiliar persons via social media networks shouldn't just be casually accepted. Make your employees aware that they need to always check whether information they post on such social networks could be used against them, e.g. to commit identity theft.

4. Call for caution with emails from unfamiliar senders

Make your employees aware that they should handle emails carefully. Even if the purported sender appears to be genuine, the email address should still be checked. If the email address used fits the sender, the email can be opened. If not, the email should be deleted. Generally speaking, the content of every email should be checked for credibility or plausibility. That goes likewise for all links and images in the email. If the links don't fit the sender, the email should be forwarded to the IT support unit and then deleted.

5. Make sure your IT system is secure

Safeguard your systems: install firewalls and anti-virus software, have updates installed automatically and ask employees to change passwords regularly, also for your telephone system and in all systems connected to the internet. Don't install software that other persons try to foist on you.

6. Check how you grant user rights and ensure secure authorization processes

Grant user rights only to the extent that users need them to perform their tasks. Too many user rights pose a higher risk. When granting authorization rights, apply the 'four eyes' principle at the very least (and the 'six eyes' principle if necessary where large-value payments are involved). Avoid, on the other hand, granting employees individual power of attorney.

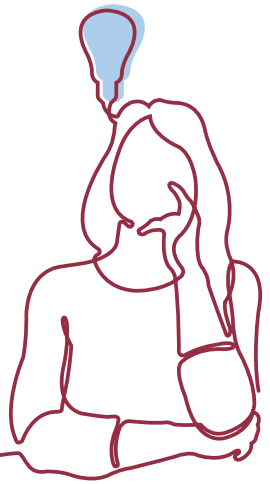
7. Educate your employees on cybercrime

Hold regular training sessions on any new scams to sensitise your employees to these. Explain to employees how fraudsters operate and what they should look out for.

8. Encourage a common sense approach

Urge your employees to always use their common sense in everything they do. Increased vigilance is the best safeguard for your company.

What should you do if you are nevertheless **the victim of cybercrime?**



Contact your bank immediately, particularly if the payment is still 'fresh', since funds are only returned if they haven't yet been credited to the payee's account, but possibly also if they haven't yet been touched on the account. Even if you managed to thwart a scam in time, give your bank details of the account to which the fraudulent payment was supposed to be made. We advise you to always report fraud – and attempted fraud – to the police.

For more information, contact the Zentrale Ansprechstelle Cybercrime (ZAC) (Central Cybercrime Office) at **www.allianz-fuer-cybersicherheit.de**.

General information on cybersecurity is also available at **www.bsi.bund.de**.

We wish to thank the following panel of experts for
their support in producing this publication:

Michael Alber
Managing Director
Federation of German Wholesale Trade, Foreign Trade and Services

Dr Alexander Barthel
Head of Department, Economic and Environmental Policy
German Confederation of Skilled Crafts

Dr Christian Fahrholz
Head of Department, Financial and Monetary Policy,
Business Finance, Business Continuity
Association of German Chambers of Commerce and Industry

Stephan Jansen
Managing Director
Association of German Guarantee Banks

Albrecht von der Hagen
General Manager
Association of German Family Businesses

Fabian Wehnert
Head of Department, SMEs and Family Businesses
Federation of German Industries

The Association of German Banks can be contacted at:

Bundesverband deutscher Banken
Postfach 040307
10062 Berlin
+49 30 1663-0

bankenverband@bdb.de
bankenverband.de

Published by:
Bundesverband deutscher Banken e. V.
Legally responsible:
Oliver Santen
Design:
ressourcenmangel an der panke GmbH
Printing:
Buch- und Offsetdruckerei H. Heenemann GmbH & Co. KG

Berlin, October 2019