Info Blatt

Information sheets on economic security

How to protect against phishing

German trade and industry as well as the science sector, but also the political sphere and administration are worthwhile targets for cyber attacks. One of the most frequent methods of attacking is phishing. Cyber and phishing attacks are techniques also used by foreign intelligence services for the purposes of espionage and sabotage.

However, you are able to minimise possible threats. This may also involve the support of the security agencies. BfV is in charge of countering espionage activities carried out by foreign intelligence services. Therefore, we are available as a confidential point of contact.

Most cyber attacks start with an email.

9 020021 542847

1 What is phishing and why is it so dangerous?

DEFINITION

- As part of a phishing attack, the addressee receives an ostensibly authentic email. The email often contains an attached document or links to ***other websites***.
- Attackers deliberately exploit **curiosity, stress or anxiety**. Their aim is to make you click on malicious documents or reveal sensitive information such as passwords.

PHISHING

- *Phishing is composed of the words "password" and "fishing", i.e. fishing for passwords.*

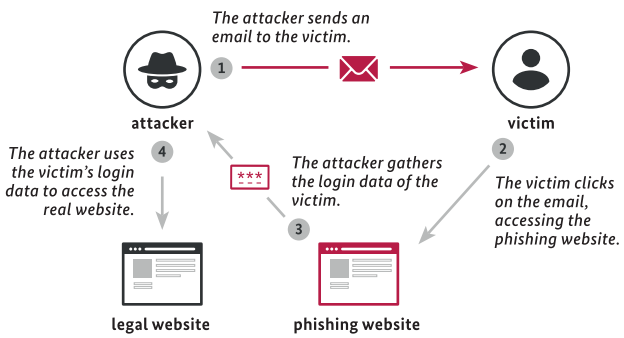
- ***Other websites***
  *Attackers reconstruct **login websites** etc. that look almost identical to the original ones. The data divulged by the victim in the login process is secretly captured by the attacker. Afterwards, the victim is usually redirected to the correct website to avoid them becoming suspicious.*

DANGER

***Login data captured** my means of phishing can be used in various ways against you.*

- *Accessing other **services and accounts** used by you*
- *Reading out your **correspondence and contacts***
- ***Sending false emails** with malicious attachments or links to colleagues, for example*
- ***Blackmailing or damaging your reputation** by means of captured personal information or images*
- ***Disseminating fake news** in your name, in social media, for example*

Orchestration of a typical phishing attack



*Especially **email accounts** are of interest to attackers because they contain much personal information.*

- *Images/videos, contact details and calendar entries*
- *emails and documents*
- *Information on personal social media accounts and other online services*

Many online services are linked to an email account. The 'forgot password' functionality enables the attacker to hack other accounts too.

SN-22094280.0*1**0

2 How to recognise phishing emails

- The sender's address is usually manipulated by way of email-spoofing. Phishing emails often purport to be from your email provider, from social media platforms or a bank.

> ***Email spoofing***
> *By manipulation of the email header, a false sender address is displayed to you. So have a closer look at it if you are unsure. For more information on how to verify the email header, please visit* ***www.verbraucherzentrale.de*** *(„Header").*

- **An urgent need to take action** is suggested to you, e.g. by announcing 'deactivation of your email account in two days'. **Threats** further increase the pressure, example: "If you do not take action now, then ...".
- There are **links or files contained in the email** which you are supposed to open. They **request sensitive data**, such as PINs, TANs or passwords.
- Frequently, there are **spelling errors or inconsistencies in language** in the text, such as forms of word that are at odds with the sender. The **salutation** is often impersonal, such as "Dear customer". There is no **site notice**, or it is incomplete.

> ***SPEAR PHISHING***
> *Spear phishing is similar in procedure (malicious link or attachment, capture of login data etc.). The attack, however, is usually targeting a specific organisation or individual person or a specific category of persons. The attacker's email is individually tailored to the concrete target, being the most frequent way of infection in targeted cyber attacks.*

9 120021 542847

3 How to protect yourself

PERSONAL PRECAUTIONS

- Be wary of any emails asking you to take urgent action. **Never provide your passwords**. This is also true for emails from family members, friends or the employer. Their **email accounts might be hacked too**.
- If you receive suspicious emails, ask yourself what **relation you really have to the sender** and whether the **request to take action** is really **plausible**.
- Never click **on links or attachments** of suspicious emails. Be particularly cautious when confronted with attachments having formats like .exe or .scr. Use your **browser** to search for a website and, if required, to authenticate yourself there.
- Activate – whenever possible – the **Two-Factor Authentication** for online accounts.
- Use a mouseover to verify the **links contained** in the email. Which **website address** (URL) is shown there?
- In case of doubt, contact **the sender**, for example by phone, **to ask for confirmation** that the email was sent by them.
- You may also **conduct an internet search** based on the **email content**. This is to check whether other persons have also received the same email and reported it.
- Install **anti-virus programmes and update software and operating system** always immediately.
- Use **different and strong passwords** (***safe passwords***).

> ***Safe passwords***
> - *Passwords such as "12345" or "password" can be cracked quickly by attackers. Safe passwords consist of at least 8 characters including capital and small letters as well as at least one special character and a number.*
> - *Use different passwords for different online accounts. This is a better way to protect them against access by third parties. Use, for example, the "password note" method (Passwort-Merkblatt) suggested by the Federal Office for Information Security (BSI).*
> - *Further tips, in addition to those of BSI, to compose and administer safe passwords are offered by the consumer centres:*
> ***www.bsi-fuer-buerger.de***
> ***www.verbraucherzentrale.de***

SN-22094280.0*1**0

3

HOW TO REDUCE THE RISK IN YOUR COMPANY

- Minimise **potential possibilities of accessing** the system (so-called attack vectors). Consider carefully which of the digital processes and systems are absolutely essential to daily work and which of them can be **separated from the network**.
- Make **backup copies** at regular intervals and then keep them separate from the systems concerned.
- Close known security gaps by **installing existing patches** and regularly load the **most recent updates**.
- Use **up-to-date operating systems and programmes**. Consider to set up **anti-spam and anti-phishing-programmes**.
- Regularly check user accounts, authorisations and users on systems. Remove **unknown or spare users** (e.g. former employees) and reduce the number of **usage authorisations to a minimum**.
- Consider to install a so-called **intrusion detection system (IDS) or intrusion prevention system (IPS)**. Such systems are able to detect and block many sorts of malware.
- For safeguarding your email traffic, make use of a **transport or an end-to-end encryption**. The use of **digital signatures** helps ensure the integrity of data and of the senders of emails.

EMPLOYEES AS "HUMAN FIREWALLS"

- *By means of phishing, attackers intend to circumvent the increasing technical precautions such as firewall or spam filter. So you as the members of an organisation have a particular responsibility. Always be wary and never open suspicious emails or attachments carelessly.*

HOW TO PROTECT YOUR EMPLOYEES

- **Conduct regular awareness raising measures for all of your employees** warning them to stick to precautions. Inform them promptly about **new methods of attacking**.
- Facilitate dealing with potentially dangerous emails for your employees by issuing **clear email guidelines including checklists**.
- **Phishing tests** may possibly identify further need for training or awareness raising measures. This involves the sending of imitated phishing emails to the employees.

HOMEOFFICE

- *In homeoffice, there is an increased risk of cyber attacks: a clear code of conduct, training and the appropriate technical equipment are indispensable measures to reduce this risk.*

9 020021 542847

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

*BfV (Bundesamt für Verfassungsschutz) and the 16 domestic intelligence services of the federal states are the domestic intelligence community. They cooperate closely in the field of preventive economic security. Thus a strong network is formed that extends to where your company is based. Please visit **www.verfassungsschutz.de** to find a list of contacts at the federal state authorities.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

*The Economic Security Initiative (Initiative Wirtschaftsschutz) is an initiative by BfV, BKA, BND and BSI. On their information platform **www.wirtschaftsschutz.info** they offer their expertise in the field of economic security together with various partners. This includes the issue of cyber crime as well as economic and scientific espionage or IT security.*

Your direct contact to economic security

SN-22094280.0*1**0