# Deutschland **Digital•Sicher•BSI•**

Password Theft via Phishing

Protection against phishing

**How Can You Protect Yourself** 

**Against Phishing?** 

#### How Can You Protect Yourself Against Phishing?

#### Never send sensitive data in an e-mail

We cannot repeat it enough: No credit card company or trustworthy service provider will ever ask you in an e-mail to provide confidential access data, not even for security reasons.

Another thing to watch out for when you want to avoid having your data or passwords stolen:

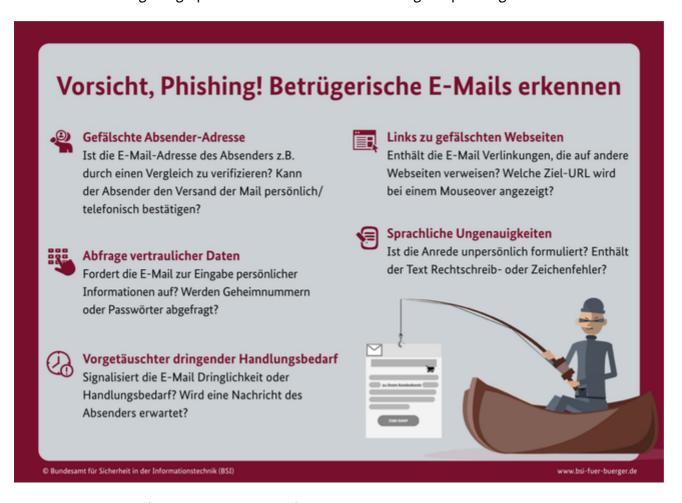
- Always check your **browser's address bar**. Bookmark the login pages you visit frequently in your browser favourites.
- Never click a **link in a suspicious e-mail**. If you are uncertain, navigate to the home page of the site mentioned in the e-mail without clicking the link in the message.
- If you want to know whether an e-mail has really been sent from the organisation and is legitimately asking about confidential information, **use the telephone to contact** the service provider or bank directly.
- Never share personal data like passwords, credit card data or transaction numbers via e-mail, no matter how trustworthy the e-mail in question appears.
- Enter your personal data only via the usual method of calling up your online banking website in a separate browser. **As soon as anything strikes you as suspicious**, break the connection immediately and contact the web host of the real website.
- Never click a download link directly from within an e-mail unless you are one-hundred per cent certain it is reliable. Always navigate to the provider's website and start the download directly from the website.
- Never open the attachment if you find the e-mail suspicious.
- Log out of each online session properly instead of merely closing your browser window.

- Regularly check your current account balance and any income or expenses you might receive or incur
  from Internet payment services. This will allow you to react more quickly if you notice unauthorised
  transactions.
- Never enter personal data on websites that do not encrypt the connection. You can tell whether a
  website is using encryption to communicate with your browser by the use of the abbreviation
  'https://' at the start of the address bar and the small padlock symbol next to the browser address
  har
- Be sure to update your anti-virus software regularly and check whether your firewall is active.

You can find more information about phishing and how you can protect yourself from it in the Sicherheitskompass (security compass) provided by the Federal police and the <u>BSI (Federal Office for Information Security)</u>. Know what you are dealing with.

### Beware of phishing! Recognising phishing e-mails

Use to the following infographic as a reminder of how to recognise phishing attacks.



Source: Bundesamt für Sicherheit in der Informationstechnik

# To the topic

download Checkliste von BSI und ProPK: Phishing (PDF)

TOrPeDo – Thunderbird-Add-on zur Erkennung von Phishing-Mails

## Similar topics



How Can I Recognise Phishing in E-mails and on Websites?



Current Examples of Phishing

Back to Password Theft via Phishing

Short URL: https://www.bsi.bund.de/dok/6599686

Legal notice
Privacy policy
Terms and conditions
Accessibility

© Federal Office for Information Security