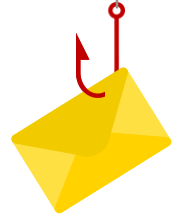


How not to: Get Phished

Everything you need to know
about phishing and how to avoid
it!



What is Phishing?

Phishing uses **manipulative emails or messages** to gather sensitive data, commit financial fraud or steal digital identities.



95%
of all cyberattacks
start with **Phishing**

How are you targeted?

Phishing messages arrive mostly through
email and messenger services.

Any highly targeted phishing attack is called
Spear phishing.




How can you protect yourself?



Have a Social Media Hygiene

- Check privacy settings of your accounts
- Be mindful about what you post
- Be aware of meta data¹

Implement technical measures

- Use multi-factor authentication²
 - Regularly update your software
- 



Communicate carefully

- Think before you click any links or buttons
- Follow the need-to-know principle
- Classify your information
- Check the email sender address



Recognize a phishing attack

- Double check unusual requests using other channels
- Be suspicious of:
 - Messages pressuring you into direct action
 - Messages from an unknown number or email address
 - Messages with call-to-action to follow a link or button
- Think twice when a message doesn't address you directly but is kept general

¹ Definition *Meta Data*: A set of data hidden in the description of a file. For example, information about location coordinates, author, time of creation and more.

You think you got phished?

Report & Support

1

You identified a phishing attack?

Use the *Report Message* button in Outlook or open a ticket for your organization.

2

You suspect a virus infection?

Disconnect your client or mobile device from the network (WLAN and LAN) and contact your local IT support through other channels (i.e. colleague)

3

You suspect a data theft (login, password, etc)?

Open a ticket to report it at your organization.



How should you handle private phishing attacks?

- **Verify the sender** using different channels and official contact details to double-check your suspicion
- **Change your passwords** (i.e. online banking, social media accounts, mobile phone, etc)
- **Block bank account**, check payment services (i.e. debit card charges, paypal, etc), contact your banking institutions
- **Possibly file charges** with the authorities
- For applications, **use their in-built report feature**