How to identify & respond to phishing

Some practical advice

SIEMENS

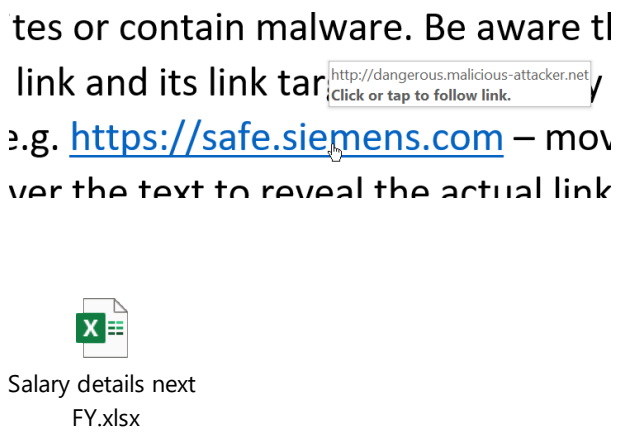
Check if the sender address matches what you expect

- In **Outlook Mobile** you may have to tap on the sender name to reveal the real e-mail address of the sender.
- E-Mails marked with **"[ext]"** in front of the sender name do come from an external sender, whatever the sender name may suggest.
- Sometimes attackers use **slight variations of existing domain names** to appear as legitimate senders (e.g. síemens.com).
- You can only be fully certain about the sender of an e-mail if it contains a **trusted electronic signature**.

SIEMENS

If it feels suspicious, it usually is!

- **Unusual wording** (incl. spelling and grammar mistakes), generic **salutations**, a lack of umlauts (e.g. "ae" instead of "ä") or other special characters used in your language, and **alleged responses** to something you did not initiate (e.g. "You won the lottery!" but did not buy a ticket) are typical indicators of phishing e-mails.
- Be extra cautious if the **e-mail contains attachments or links** - they could lead to malicious sites or contain malware. Be aware that the text of a link and its link target are two very separate things (e.g. https://safe.siemens.com – move your mouse over the text to reveal the actual link target)
- A typical psychological trick of attackers is to create a **sense of urgency** and **threaten you** with negative consequences if you do not follow the instructions in the message. Sometimes they also try to **exploit your curiosity** (e.g. access to interesting information) or offer some form of reward.
- Try not to process e-mails when **under time pressure or distracted**. This will significantly reduce your ability to recognize warning signs. Attackers take advantage of this, e.g. by sending their phishing e-mails at times when there is typically a high volume of e-mail.



SIEMENS

If unsure, get help!

- If your gut feeling tells you that an e-mail could be "phishy", **get a second opinion** - from your manager, a co-worker, an IT expert, ...
  Do not forward such e-mails, however: The recipient may accidentally click on a malicious link.
- Discussing with someone else why you found an e-mail unusual, typically quickly confirms if it was indeed malicious.
- If the e-mail claims to come from a known person, it is a good idea to call that person for confirmation using contact details from a trusted source (e.g. SCD).

You can also always reach out to
SFS Cybersecurity
sfs.infosec@siemens.com

SIEMENS

Report *every* phishing e-mail

- Use the **"Report Spam/Malware" button in Outlook** to report e-mails to the team that operates our central malware protection for e-mails. They use those reports to block malicious e-mails and links and to fine-tune the rules to detect and block phishing.
- Please **report every phishing e-mail** even if you know it has already been reported by someone else. Those multiple reports give the central team a better idea of how widespread a particular phishing attempt is. You may also have received an e-mail that slightly differs from an already reported one and it is important to identify all such variations of a phishing attack.
- If the phishing e-mail contains **a lot of context information** (e.g. refers to actual projects you are working on, sender seems to know a lot more about you than just your e-mail address) or if the e-mail asks you to **perform critical actions** (e.g. approve payments, send confidential information, enter data in an application) then please always get in touch with **SFS Cybersecurity** (sfs.infosec@siemens.com) because this could be a **targeted attack** that needs to be investigated.

SIEMENS

Additional resources to learn more…

- The **Siemens Cybersecurity Card "Fraudulent E-Mail"** (also available in additional languages) provides practical guidance on how to identify phishing e-mails and how to react.
- Google has an **interactive quiz** (in English, German and many other languages) to teach some of the most common tricks phishers use.
- This provider of malware protection maintains a **gallery of current phishing e-mails** – some very simple but effective, some very creative…
- While most of us work from home, we face additional Cybersecurity threats. The **SFS "COVID-19 Cybersecurity Special"** outlines what we can do to secure our office away from the office.
- For any question on Cybersecurity, please do not hesitate to contact the SFS Cybersecurity Team.

SIEMENS

Thank You

SIEMENS

Contact

SFS Cybersecurity (SFS CYS)

E-mail SFS.InfoSec@siemens.com

Intranet SFS Cybersecurity Wiki
SFS CYS department homepage

Yammer SFS Cybersecurity #sfscybersecurity

SIEMENS