Email Phishing

Phishing is one of the **most common** types of cyber attacks used for gaining access and / or disclosure of information. Key indicators include a **sense of urgency, request to click links, misspellings, and poor grammar**. Cybercriminals are starting to improve their English resulting in better persuasion.

Suspicious Links: Clicking may lead to stolen user names, passwords, or malware. Popular **sites are often imitated** and may immediately request your login details or prompt for a download. The link text may also not be the actual perceived destination. Hovering your mouse over the link will reveal the actual intended site (without clicking).

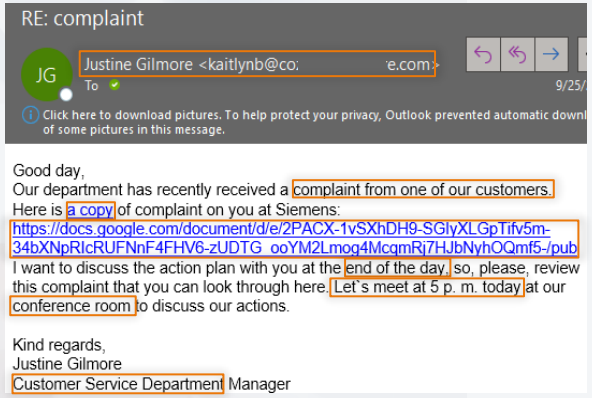
Malware Attachments: Typically these attachments contain malware which may give hackers **access your device, lock your data, log your keyboard inputs**, or other disruptions.

To report an email, select the message in Outlook and click the "**Report as SPAM / Malware**" button on the top bar. Alternatively, you can send the email as an attachment, not forward, to malware.security@siemens.com.

Can't find the button? Download it from the Software Center.
Need more help? Contact the US Cybersecurity Team (RC-US CYS).

Stay Vigilant!

Anatomy of a Phishing Email


RE: complaint

JG

Justine Gilmore <kaitlynb@co: e.com>

To

9/25/

Click here to download pictures. To help protect your privacy, Outlook prevented automatic downl of some pictures in this message.

Good day,
Our department has recently received a complaint from one of our customers.
Here is a copy of complaint on you at Siemens:
https://docs.google.com/document/d/e/2PACX-1vSXhDH9-SGlyXLGpTifv5m-34bXNpRlcRUFNnF4FHV6-zUDTG_ooYM2Lmog4McqmRj7HJbNyhOQmf5-/pub
I want to discuss the action plan with you at the end of the day, so, please, review this complaint that you can look through here. Let's meet at 5 p. m. today at our conference room to discuss our actions.

Kind regards,
Justine Gilmore
Customer Service Department Manager

Read Between the Lines

- Does the email's **context align with your role and function**? This example suggests mentions a customer complaint; if you're not in a customer facing role, how would this be possible? Always consider if the email **contents seem out of the ordinary**.
- There is **excessive use of links**, **urgency** (*"end of day", "meet at 5 pm today"*) and **attempted credibility** by referencing a familiar place (*"our conference room"*).

Know Your Sender?

- The sender's **display name** (Justine) **doesn't match the sender's email** format (Kaitlyn).
- The email body implies the sender is a Siemens employee. **All internal emails include the sender's Siemens org code**. Here there is no organization code after 'Gilmore'.
- **Check the email address domain and it's spelling**. If it's a Siemens employee, there should be an '@siemens…' address. You can also **hover over the displayed address** to confirm the recipient of a potential reply. A mismatch is a potential indicator of phishing.
- If you are still unsure about the email's legitimacy**, use a trusted source** (e.g., SCD, Company Website) to contact the purported sender to verify the request's authenticity.
- When confirming the validity of the senders request use a new email and not the original email. **Only use the confirmed directory or trusted source provided contact details**.

Want to learn more?

- Avoiding Phishing Scams (video)
- Phishing and Whaling (video)
- DHS: Security Tips - Email Attachments
- FTC: Recognizing & Avoiding Scams

#CyberSmart | The Human Sensor Network