COVID-19: PHISHING AND SMISHING SCAMS

COVID-19 Home

RECEIVED A STRANGE EMAIL OR TEXT ABOUT COVID-19?

Think twice before clicking on any links and attachments. They could be trying to phish or smish you, which is how criminals use social engineering to access your personal information.

How can I tell if a message is trying to phish/smish me?

The messages usually:

- look identical to messages from a reputable organisation (such as a medical or governmental institution);
- sound urgent;
- claim to enclose important or breaking news;
- ask you to click attachments and links.

WHAT CAN I DO?

- Spot the scam: check the address for details that wouldn't normally be present in an official email.
- Don't click links, open attachments or reply.
- Don't give out any financial information.

WHAT HAPPENS IF I CLICKED SOMETHING?

- If you open the attachment and/or click on the link, your system will be infected with malware.
- If you enter login credentials to access information, criminals will have access to those credentials.
- If you are asked to provide your bank details and you do, criminals will gain access to your finances.

TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

Source URL: https://www.europol.europa.eu/covid-19/covid-19-phishing-and-smishing-scams#comment-0