



### **Signs of phishing attempts**

- **E-mails Demanding Urgent Action**

Emails threatening a negative consequence, or a loss of opportunity unless urgent action is taken, are often phishing emails. Attackers often use this approach to rush recipients into action before they have had the opportunity to study the email for potential flaws or inconsistencies.

- **E-mails with Grammatical and Spelling Errors**

Another way to spot phishing is bad grammar and spelling mistakes. Many companies apply spell checking tools to outgoing emails by default to ensure their emails are grammatically correct. Those who use browser-based email clients apply autocorrect or highlight features on web browsers.

- **E-mails with an Unfamiliar Greeting or Salutation**

E-mails exchanged between work colleagues usually have an informal salutation. Those that start "Dear," or contain phrases not normally used in informal conversation, are from sources unfamiliar with the style of office interaction used in your business and should arouse suspicion.

- **Inconsistencies in E-mail Addresses, Links & Domain Names**

Another way how to spot phishing is by finding inconsistencies in e-mail addresses, links and domain names. Does the email originate from an organization corresponded with often? If so, check the sender's address against previous emails from the same organization. Look to see if a link is legitimate by hovering the mouse pointer over the link to see what pops up. If an email allegedly originates from for example, Google, but the domain name reads something else, report the email as a phishing attack.

- **Suspicious Attachments**

Most work-related file sharing now takes place via collaboration tools such as SharePoint, OneDrive or Dropbox. Therefore, internal/external emails with attachments should always be treated suspiciously –especially if they have an unfamiliar extension or one commonly associated with malware (.zip, .exe, .scr, etc.).

## **Signs of Vishing attempts**

- The caller may highlight that he/she is in a rush and claim they urgently need some information to catch you by surprise with an unsolicited call.
- Causing you to react with an emotional response (such as fear or panic) to a fake scenario.
- Creating a sense of urgency so that the you ignore the little red flags or warning sounds that are going off inside your head.
- Getting you to trust or feel like the actor has your best intentions at heart.
- Making you feel like you're doing the right thing or making a good decision by cooperating.

## **How to prevent Phishing / Vishing and Smishing**

- Don't answer/reply your phone when you receive phone calls or messages from unknown numbers.
- Don't give any personal information, card details, identification details to an unknown caller.
- Don't respond to unsolicited sales, marketing, or outreach messages or calls.
- Don't click links in unsolicited messages.
- Don't call phone numbers that are provided in online ads, pop-up windows, SMSs etc.
- Register with a paid call/spam SMS blocking service.
- Educate yourself, your loved ones, about potential threats and scams. Teach them to hang up and call the person, department, or company directly using official phone numbers (such as from an official directory or from official web site).