English

What is phishing?

Phishing is a fraudulent attempt to obtain any type of sensitive information or data that can be used to attack unsuspecting users. The offender tries to disguise their self as a trust worthy entity usually via an email, or an SMS, or instant messaging and somehow extract personal information from the victims by asking them to complete a form or visit a (malicious) website.

Types of phishing (according to (Wikipedia, 2020)**)**

- Spear phishing: directed at specific individuals or companies (employees and executives)
- Whaling: specifically spear phishing executives of companies
- Catphishing: online deception involving getting to know the 'victim' personally
- Clone phishing: creating a fraudulent communication based on an intercepted original and replacing legitimate links or files with malicious ones
- Voice phishing: tricking users to call a 'bank' service in order to perform some task or update some information
- SMS phishing (or smishing): target receives an SMS with a link or being asked to call a phone number, or send an email or an SMS.

Techniques used

- Link manipulation: making a link go somewhere or do something that can compromise or extract sensitive information
- Filter evasion: manipulating e-mail contents so as to avoid filters placed on e-mail servers
- Website forgery: using web programming techniques to trick users into thinking they are visiting a legitimate site when in fact they are not.
- Covert redirect: attackers manipulate links to appear legitimate but they direct to malicious sites.
- Social engineering: users are encouraged to click on links or open attachments

How to avoid phishing

- On a big scale
  - Big mail service providers include anti-spam and anti-phishing filters to stop messages before they even reach the servers
  - System administrators can equip the mail server with anti-phishing filters
  - There are quite a few websites that report the details of phishing attempts. One example is: FraudWatch International
  - Larger companies tend to train employees to recognize popular phishing attempts

- On a user level:
- **ALWAYS PAY ATTENTION**
  - Never open emails from people you do not know
  - If you do open the email **read it carefully** and pay attention to details like, legitimacy of the sender address, proper use of the English language, existence of vague (rather than specific) information.
  - Never click on attachments from emails that you were not expecting. If the original sender appears to be legitimate, contact them directly and ask them if they sent you anything
  - Never click on email links included in emails that you were not expecting.If an email appears legitimate and is asking you to verify your details, don't click the link. Go the company's website and try and find

a page or notification about that verification process
    - Never call a number just because an email or SMS or instant message says so. Contact the main switchboard of the company and ask to be connected to whoever 'allegedly' sent you the communication
    - Any communication claiming that you have won some competition or you are the lucky draw winner can surely be considered a phishing attempt.
    - Any communication informing you of a suspension of service and an urgency to update your details in order to protect your details can surely be considered a phishing attempt.

Videos (on YouTube) for identifying phishing:

- Google's: Stay Safe from Phishing and Scams
- Atomic Shrimp: How to recognize a phishing scan message