centro criptológico nacional

Phishing

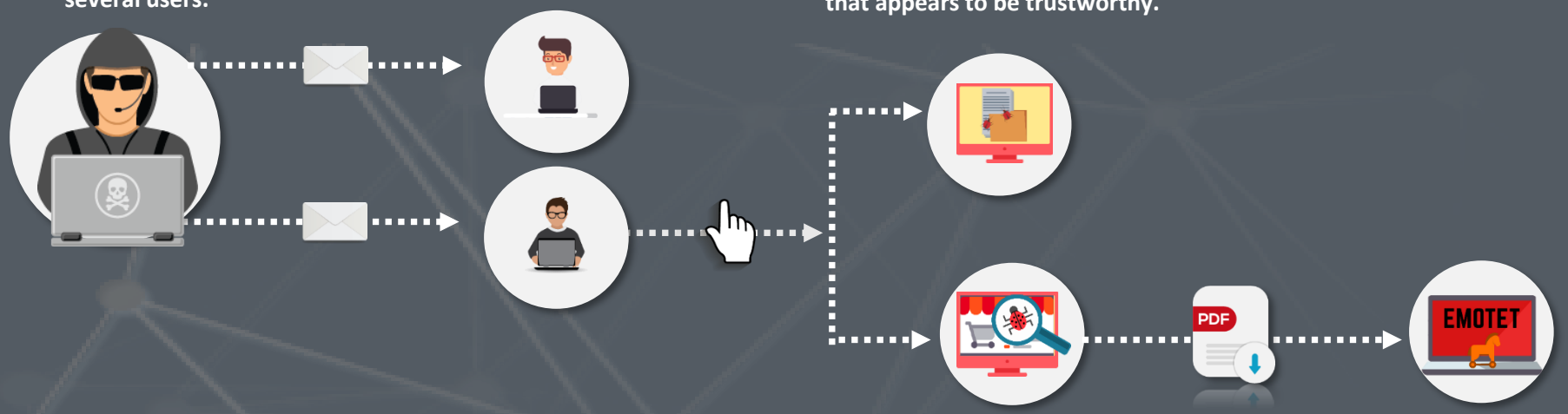
Phishing attacks use social engineering to fraudulently acquire users' personal information. Sending e-mails that appear to be reliable and that often lead to fake websites, they try to trick users into providing personal information (bank account details, passwords, social security numbers, etc.).

1 **The attacker sends fraudulent emails to several users.**

2 **A user opens the email**

3 **The e-mail contains a malicious attachment or a link to a website that appears to be trustworthy.**

4 The user downloads a file that executes a malware.



How to avoid being a phishing victim

Check the **domain of the sending e-mail** and that its name matches its e-mail account (name and domain).

Do not trust e-mails with **badly written or misspelled text.**

Avoid opening attachments if you do not know the sender or do not expect the document.

Pay attention to the **syntax of the websites' links** that are sent to you by e-mail. One letter can make a difference.

If you access websites through search engines, before entering personal data, always **check that it is the official website and not a secondary site** that collects the information you are interested in.

If you notice any anomaly in an e-mail**, contact the sender through another channel** (e.g. telephone) to check the authenticity of the message.

Enable **the second authentication factor** in all digital media available (banking applications, social networks, e-mail, etc.).

Do not enter personal data on websites whose **link has been shortened** (cort.as, bit.ly, etc.).

Use one browser for banking and official transactions, and a different one for regular navigation.

Keep the browser **updated**, as well as its extensions and plug-ins (Flash, Java, etc.).

centro criptológico nacional