LOOK TWICE BEFORE YOU CLICK

You could lose your money, your personal information and even your stored data, if the device stops functioning. Don’t get hooked!

HOW COULD IT HAPPEN?

- **Phishing Attacks**: They trick users into giving up personal information by posing as a trustworthy entity. They spread through email, text message or social media platforms.

- **Website Browsing**: Your mobile device might get infected simply by visiting an unsafe website.

- **File Download**: Malicious links and attachments can be directly embedded within an email.

WHY IS IT EFFECTIVE?

- Mobile devices are **constantly connected** to the internet.

- The **reduced size of the device’s screen** is a general constraint. Mobile browsers display URLs on limited screen space, making it difficult to see if the domain is legitimate.

- **Implicit user trust** in the personal nature of a mobile device.

WHAT CAN YOU DO?

- Be suspicious if you receive an SMS or a phone call from a company asking for personal information. You can verify that the message/call is legitimate by directly calling the company on their official number.

- Never click on a link/attachment in an unsolicited email or SMS. Delete it immediately.

- When browsing the web on your mobile device, make sure your connection is secured through HTTPS. You can always check it out at the beginning of the URL.

- Be wary if you land on a site that contains poor grammar, misspellings or a low-resolution.

- If available, install a mobile security app which will alert you of any suspicious activity.