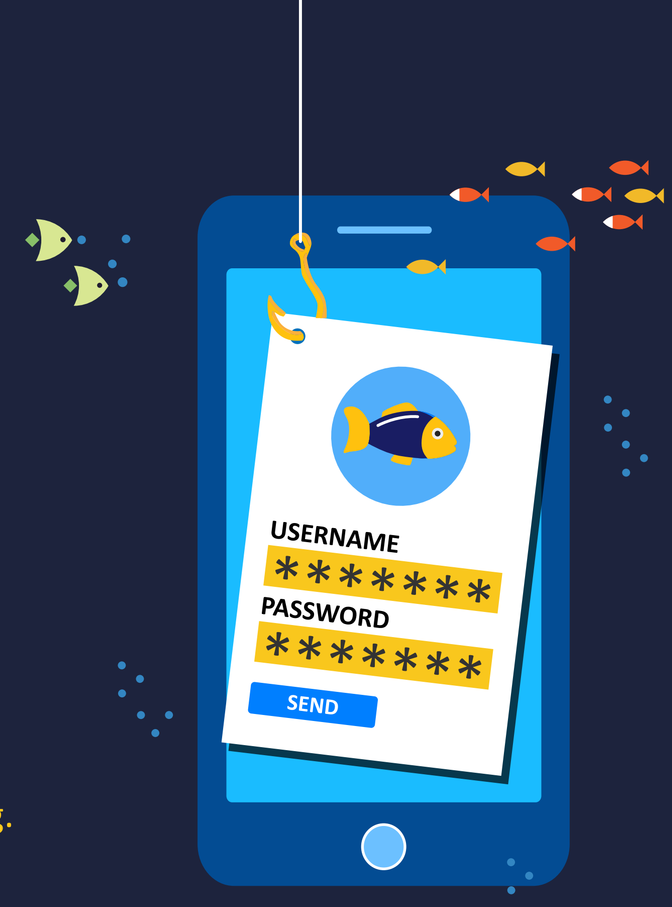
WEB-BASED THREATS

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.

https://

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.

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

^BE:%}
W@RY
*)Z#$=

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.

EUROPOL
EC3 | European Cybercrime Centre

#MobileMalware