CYBERSECURITY
PHISHING

- Given the slightest doubt, do not provide any **confidential** information.
- Keep yourself **informed periodically** about the latest security news.
- It is important to use antivirus to prevent the installation of malicious code on your computer. **Scan your computer** if you are not sure about its security.
- **Verify the information.** If the source of the information is suspicious, contact by other means to verify it.
- Pay attention to **the wording, and be suspicious if** there are meaningless expressions and spelling or grammatical errors.
- Remember that this type of scam not only focuses on the banking online. **Stay alert.**
- Use **common sense** when you make any transaction over the internet, "if it's too good to be true, then it probably is".
- **Do not provide your bank account** or credit card, ID, cellphone number, unless you're actually paying for a good or service.
- If you've been a victim of a phishing attack **report** it to the company and competent authorities.

CONTACT US

http://www.it.ie.edu https://servicedesk.ie.edu/

IT Support in Pinar 15, +34 91 568 96 23 / +34 91 568 97 90

IT Support in MM 31, +34 91 787 51 99

IT Support in MM 31 bis, +34 91 787 51 39

IT Support in Segovia, +34 92 141 53 15

Cybersecurity
Phishing

PHISHING is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim, by masquerading a "trusted third party". Such attacks have become one of the external threats lurking more companies.

THE RISKS of these techniques are theft of identity and confidential data, productivity loss and consumption of resources of corporate networks. The methods used to carry out **PHISHING** are not exclusively limited to the email, but others likes SMS (**SMISHING**), IP telephony (**VISHING**), **SOCIAL NETWORKS, INSTANT MESSAGING, MOBILE, ETC.**

To avoid these risks, it is recommended to adopt good practices mainly in the use of **CORPORATE EMAIL**.

LEARN to correctly identify suspicious phishing emails. In general messages that request confidential information (passwords, bank account details, mobile number, etc..).

CHECK the source of information of your **INCOMING MAIL**. Your bank won't request your personal data or bank details via email.

Instead of using **LINKS INSIDE EMAILS**, type the address directly into the browser.

Keep **PATCHED AND UPDATED** your computer and all applications, especially the antivirus and antispam. Only apply security patches provided by the manufacturer.

Before entering sensitive information on a web page, check to **MAKE SURE THAT IT IS SAFE.** They start with <<https ://>> and have a closed padlock in the browser.

SMISHING is done through a text message trying to convince you to visit a fraudulent link.

VISHING is done through a phone call that simulates a bank asking you to verify a series of data.