IT Best Practices

CYBER SECURITY

ie UNIVERSITY

Software

KEEP UPDATED YOUR SOFTWARE AND ANTI-VIRUS ALWAYS

Check that you are using the latest version of apps and anti-virus on your devices.
For that, access "Windows Update".

USE MICROSOFT ONEDRIVE

In the event of loss or theft, this helps to minimize data loss and leakage.

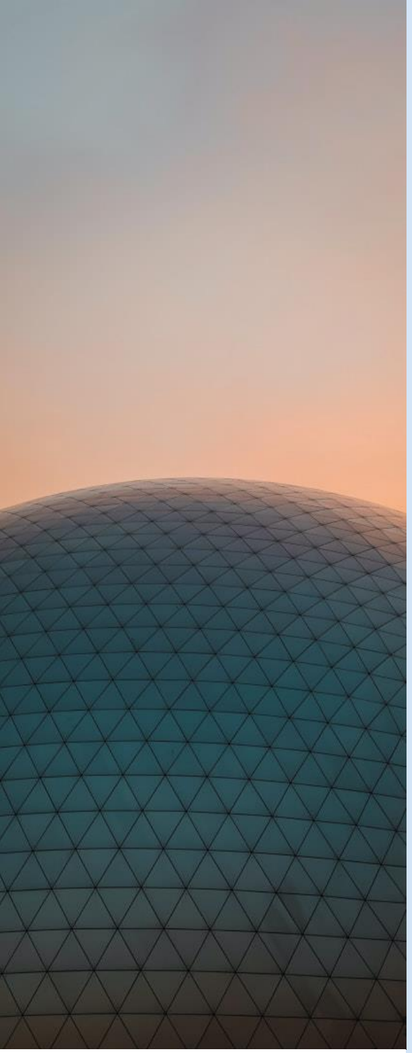
FOLLOW THE RECOMMENDATIONS WHEN USING VIDEO- CONFERENCE AND MEETINGS APPS.

Doing so will avoid unwanted access when using the likes of Zoom and Microsoft Teams.

DON’T DOWNLOAD APPS THAT ARE NOT AUTHORIZED BY IT.

Keep your device safe and IE information confidential.

ie UNIVERSITY



Hardware

AVOID SHARING YOUR COMPUTER.
Don’t lend your computer or leave it unattended.

SHUT DOWN YOUR COMPUTER EVERY DAY.
When you are not using it, both in the office and at home when you are teleworking. Don't leave it locked up overnight or on weekends.

BEWARE OF STRANGE PENDRIVES.
First check them with the antivirus (Cortex).

SET A SECURE PASSWORD ON YOUR MOBILE DEVICES.
Don't use the same ones on all applications and sites.

ie UNIVERSITY

Connection

USE THE VPN PROVIDED BY IE.
Keep a secure connection through the VPN software, Forticlient, with this profile defined: IE_Staff_Split: general usage.
Keep in mind that wireless networks can be abused by malicious actors.

AVOID ACCESSING PUBLIC SPACES WITHOUT VPN. There are programs that facilitate the jamming of platforms and store keystrokes.

STAY SAFE BY USING YOUR MOBILE DATA ON SECURE AND TRUSTED NETWORKS.

BEWARE OF PUBLIC WIFI NETWORKS.
Public WiFi networks, for example at hotels and restaurants, are not always secure. It's best to carefully read the provider's terms and conditions and, as much as possible, limit your site visits and sharing your data. When using these networks, do not make payments or access your bank account.

ie UNIVERSITY

Mail

BE CAREFUL WITH THE SUSPICIOUS MAILS ON YOUR MOBILE

Check the sender, subject and authenticity. Be careful when reading mails on cell phones, which do not display in their entirety.

BEWARE OF CEO FRAUD

If you receive a request for personal or financial data, verify its authenticity before doing anything else. We will not send you an email that asks for your credentials (nor will a bank for that matter!) or about retained emails or lack of space in your inbox.

AVOID FAKE WEBSITES

Before clicking on a shortened link (e.g., *bit.ly, goo.gl, ow.ly*), check the source that posted the link.

HOW TO RECOGNIZE A PHISHING MAIL

- Non-personalised emails. E.g. "Dear Customer".
- "An offer you can't refuse": in the case of tempting offers, you can and must refuse them.
- They ask you to act immediately: phishers love to play with urgency.
- On shortened links, check for hidden malicious links by hovering over them.
- Attached files: if they don't come from someone you trust, stay away from them. Scammers can even hide malware in rich content files such as PDFs.
- Links with deliberate typographical or spelling errors. They might be fake urls.
- Incorrectly written messages: with spelling and grammar mistakes.
- Requests for personal information: if you are asked for personal information by mail, it is likely that it is a scam. Should you are asked to access a URL, make sure it begins with "https" instead of "http". The "s" means "secure".

ie UNIVERSITY

Mail

Phishing

Phishing is a cyber crime in which one or more targets are contacted by email or text message by someone posing as a legitimate institution to obtain confidential data such as banking details and passwords.

You can report such emails to Microsoft for analysis through the Outlook add-in called "Report Message".

Social Network

THINK BEFORE YOU SHARE

We all like to share pictures of our feet in the pool... This is fine so long as you don't share too many details on your public profiles. Don’t give clues to criminals who might try to impersonate you, or worse.

REVISE YOUR PRIVACY SETTINGS

Configure your devices so that photos do not contain geolocation information and remove this option from your postings on social networks.

Review your contacts and privacy settings on social networks.

If you do not want to be tagged in photos or have photos of you uploaded, let your friends know!

ie UNIVERSITY

Password

BE ORIGINAL AND CREATIVE

Don’t use personal information: dates, places or any data that can be investigated.

Don’t use your username.

Don’t use common words or groups of words.

Don’t use the same password for two or more sites.

TOP 10 WORST PASSWORDS

“123456”, “123456789”, “qwerty”, “password”, “1234567”, “12345678”, “12345”, “iloveyou”, “111111”, “123123”.

CHANGE IT FRECUENTLY

Update the passwords frecuently.

KEEP IT SECRET

Don’t share passwords. Try not to write them down anywhere.

Try to avoid using the "remember password" option of the browsers.

Avoid accessing at public spaces without VPN. There are programs that facilitate the interference of the platforms and store the keystrokes.

ie UNIVERSITY

Password

MAKE IT HARD TO GUESS...

By its length: include at least 12 characters.

By its randomness: combine numbers, symbols, uppercase and lowercase letters.

... AND EASY TO REMEMBER

Choose the first letter of each word in an easy to remember sentence (sayings, songs, quotes, or even some personal custom): "Bacon double cheddar cheeseburger with caramelized onions": “BdCcBwCo".

Replace vowels with numbers: "BdCcBwCo".

Personalize the passwords based on the same pattern: "HelpMeobiWanKenob1@FB" (Facebook), or "HelpMeobiWanKenob1@AMZ" (Amazon).

ie UNIVERSITY

In the end, the best thing you can do is use your common sense and remember that, on the Internet, the best security system is you!

ie UNIVERSITY

Thank you!