REMINDER: AWARENESS KIT
TIPS ON KEY POINTS

- Do not use the same **credentials** (passwords) to access corporate applications for personal use.
- Do not click on suspicious links. In case of doubt type the URL address in the **browser bar**.
- Do not **store sensitive information** on external devices. If you need to do so, encrypt the information on the device.
- Learn how to detect social engineering attacks and how to defend yourself. **Warn IT** if you notice an abnormal behavior on your PC.
- Block the PC session when you leave **your desktop**.
- Do not change your **device settings** nor install unauthorized applications.
- Avoid using **non-corporate computers** to access corporate services. If you access your corporate email from your personal computer, do not download files to your computer, or be sure to delete them.
- Be careful with the use of **email**. Avoid chain letters.
- Use only official stores to download the apps on your mobile.

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
Tips on key points

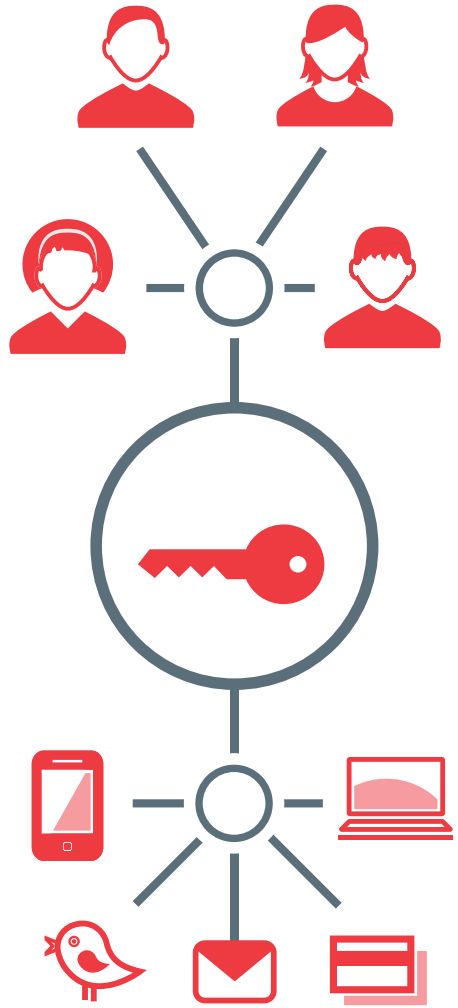
We must be aware of the **MOST IMPORTANT KEY POINTS** about cybersecurity and implement appropriate **SECURITY MEASURES** for the adequate protection of the information when performing our professional tasks.

SOCIAL ENGINEERING is focused on the employees of our organization and seeks to obtain confidential information to organize fraud. You must always stay alert.

It is recommended to set a password and the automatic locking option on your **MOBILE DEVICE.**

Do not use **CLOUD HOSTING SERVICES** not approved by IT (e.g. Dropbox) to store company data.

Make sure your **ANTIVIRUS** is enabled and working properly on both the PC and mobile.



PASSWORDS must be secret and unique, we must NOT write down, share or reuse them.

You **MUST** surf the Internet securely and avoid access to untrusted web pages.

Use **EMAIL** securely and delete or inform your IT department of suspicious mails you receive.

Protect company **INFORMATION** and make sure your backup system works properly.

When **TRAVELING**, do not send sensitive information via untrusted WiFi networks.

You **MUST NOTIFY** your IT department if you detect any suspicious activity.