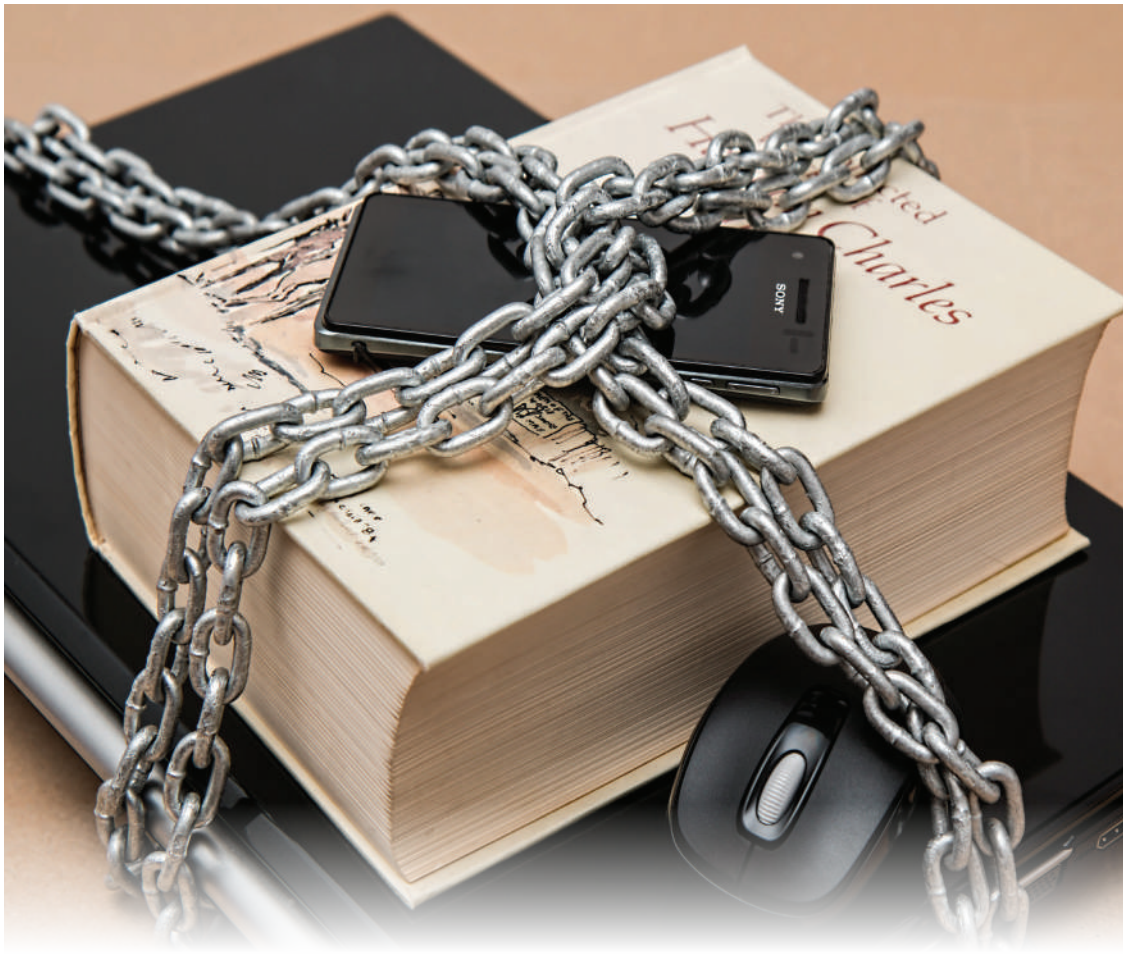


CYBERSECURITY

GOOD PRACTICE GUIDE for PUBLIC REPRESENTATIVES

Context.

We have a problem.

Every day, we are exposed to threats that originate on the Internet. In most cases, we are not even aware of the threats, or we don't respond to them. Many of us 'Don't know and Don't care', some of us 'Do know but still Don't care'. The old attitude of 'who would attack us?', tends to dominate across all sectors, even Local Government.

In the media, daily articles appear about security incidents and their impact on individuals and organizations. The reported incidents are only the tip of the iceberg. In reality, we are more exposed than we think.

Unfortunately, the risks of the virtual environment are constantly growing. Security is not taken into account and insufficient attention paid. This aspect is made worse by the complexity of new technologies.

They involve new risks that can seriously affect the individual and the organization. There are now numerous hostile actions carried out on the web. These are likely to affect the operation of your computer systems, as well as the data circulated through them.

What's the Purpose of this Guideline?

This guide aims to summarize the available information regarding existing cyber risks.

It presents some useful methods for determining behavioural reflexes for the safe use of computer systems. It provides knowledge for you as a Public Representative, a Citizen, family member and an active user of modern technology. The Guide comes in two parts – Context and detailed Notes.

It is written in simple language to avoid the communications trap that cyber experts often create for themselves. Cyber language needs to be translated, so that we can all understands the risks.

Your role as a Councillor provides access to your organizations, data, IT and communications resources.

Your dependency on this infrastructure; to provide services to the local community necessitates that you avoid cyber risks but most importantly, take the lead in raising awareness and preventing attacks

It's a Digital Age.

Our recent past and present culture is computerized. The majority of Irish people have a smart phone, tablet or laptop. The computer monitor now replaces the screens found in a cinema, a television, the walls of an art gallery, the library and even the books.

The Internet has proven to be a platform that is easy to use, cheap and flexible for providing information and communications. This has resulted in an explosion of data, both professional and amateur.

The lack of control is seen as the strongest and weakest link. The Internet hosts everyone; it is a noisy marketplace in which the craziest, immoral and ignorant person sits next to the sane, virtuous and well-informed.

The Internet has created major changes in our everyday life. We succeed in communicating with people all over the globe, to obtain information in just a few minutes. Its' search engines easily work for us, giving full pages of information in seconds.

Do all great things come to an end?

Cybercrime is the Number 1, business risk. The estimated, global cost of cybercrime is now $6Trillion per year. People's Internet behaviour has increased the risk but can also be the greatest force for decreasing it, if it can be successfully utilised.

Mass awareness and education is critical to reduce the risk for all of us. The Criminal Gangs who attack us are getting better and we are sleeping. It can all come to a very bad end, if we do not waken up and improve our people's behaviour and systems.

A cyber-attack by definition is an act or action, initiated to disrupt, deny, degrade or destroy by compromising communication, information and other electronic systems, or the information that is stored, processed or transmitted on these systems. Attacks are happening every minute of every day.

You are your data; from your driving license to your Credit Union account. Cybersecurity is inexorably linked to personal security. It is a human rights issue and a fundamental human right. Cybersecurity and human rights are complementary, mutually reinforcing and interdependent.

The global nature of the Internet, means there is increasing diversity of content. More avenues of attack are opened by being multilingual. More than 250 languages are spoken online.

English, Chinese, Japanese, Portuguese and Spanish are the top five, most used languages on the Internet. This language capability is also found in the Criminal Gangs who exploit us. Much is made of the Russians, Iranians and North Koreans. These gangs are multinational, they recruit from all over the world.

Criminality does not recognise borders, much the same as the Internet itself.

What are the Hostile Actions that the Cyber Criminal Networks use?

Cyber Criminals are maliciously disrupting, blocking, destroying, degrading or controlling information systems and infrastructure. This affects the integrity of data, its availability, confidentiality, and authenticity.

Sensitive business data that Councils work with every day, such as; employees' and citizens' data, contracts, schemes and projects can be breached by the attackers or, remotely recovered by them. They use specialized, often automated programmes or, simply steal from lost or stolen devices like your phone, or laptop.

These dangers can be significantly reduced by applying tested practices and software. These can sometimes be expensive but many are free and easy to apply. Shopping around always helps, like many aspects of life, the big brand comes at a price. The indigenous, cyber software and training sectors have many solutions on your doorstep.

Cyber risk awareness is very effective in limiting many of the issues. Your Council should have both proactive and reactive measures that include security policies, standards and guidelines.

These add-up to effective Risk Management; including training and awareness, the implementation of technical solutions to protect infrastructure, identity management and incident control.

CJHNetwork Cyber Awareness Training Programme.

Take this opportunity to get you and your staff trained on Cyber Awareness today. CJHNetwork want to let you know that you can get a voucher for a Cyber Training seat.

If you are interested in availing of this training, please contact us today and we will provide you with the details. Contact **Chris Gilson at chrisgilson@cjhnetwork.ie**

First Steps in Cyber Speak.

Your cyber security, setup should have a number of essential elements, software that protects you and you also need to be conscious of the main threats:

Cyber security software is getting better. It has to try to keep pace with the Criminals skills and organisational abilities. We are now in a better place with the next generation of software that helps to assess the risks and prevent attacks. Work is also being done on building security into the microchips that are the first layer of building blocks in IT systems.

Antivirus software.

This is a computer programme designed to detect, prevent and remove the installation of any forms of malware. These are bad software programmes often called by different names, such as; viruses, trojans, adware or spyware. They infiltrate your computers and most of the time you won't know until the Antivirus reports that it has stopped it. Hopefully! Updates are particularly important, to deal with the latest versions of the malicious programmes.

Firewall.

This is another form of protection for your computers. The Firewall monitors incoming and outgoing traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defence in network security for over 25 years.

Router.

This looks like a small box with antennae. It is a gateway that passes data between one or more local area networks (LANs). Routers use the Internet Protocol (IP) to send IP packets containing data and IP addresses of sending and destination devices located on separate local area networks.

Firmware.

Firmware updates enable hardware devices to continue operating efficiently and securely. These updates typically involve some form of programme alternation that fixes a known bug or patches against specific vulnerabilities.

Computer virus.

This type of programme can self-replicate within a system, move to other commuters on the network and propagate without your knowledge. It can ruin the functionality, integrity, and availability of the system and its data contained.

Trojan.

Thesis an example of malware; like the Trojan horse from Greek mythology that has something hidden inside. This type of programme appears to have a useful, legitimate function, but it also has the hidden one; potentially malicious which avoids security, exploiting vulnerabilities of the targeted systems. Once run, the Trojan can start malicious activities; stealing information, affecting the host computer, creating hidden, remote access paths to the affected system.

Computer worm.

This is another form of malware that can self-replicate and propagate in a computer network and beyond into other systems or networks. It worms its way in by using the existing, network resources without attaching to another programme or process.

Navigating the Internet.

The Internet is a lot like our oceans; impacted by temperatures rising, increasingly unpredictable and not following the old rules and charts. Similarly, increasing care needs to be taken while navigating the Internet.

As a result of this need for care, cybersecurity has become a frequently, discussed topic but not necessarily actioned. The virtual environment that we all experience on our computers is a dynamic one; constantly changing, the technologies used are replaced, updated and modified.

New challenges appear daily, user awareness is still low and concerned about the technical fix, rather than the right behaviour.

Vital information is targeted by the cyber criminals. This can seem, ordinary, banal and harmless. For example, they start with personal data: filling in various online forms and looking for financial, contractual data and information about employees and databases.

Online identity theft is no longer an urban legend or, the subject of a television, drama series. Access to confidential data creates strategic advantages for competitors and criminals who are working for them. Blocking user access to a set of data can bring considerable financial damage by the simple lack of access to documents at a given time. Depending on the organisation, the losses may not be only financial but reputational.

In moments of crisis, people panic and are fearful that news of a breach will be seen as a weakness. The lack of information about attacks has caused a real problem for organisations about sharing what happened and why. To beat the criminals, we need to pool the intelligence gained from all attacks to move the game towards future prevention.

The Rules for Safer Navigation.

In general, Internet users who are aware of the risks, take measures that should be enough for good protection. Far from offering the guarantee of preventable security, the following questions and comments will help you better understand the many aspects of cyber security.

It is critical to keep asking questions, as the game keeps changing. No knowledge is not an excuse.

Ask your Insurers.

Use the latest browser version.

Access to the Internet and the web comes through a browser. The most malicious applications affect Microsoft Internet Explorer which is used by more than 50% of us. Take a look at other types of browsers - Google Chrome, Opera, Firefox, Safari. When accessing possibly, unsafe web pages, try using the NotScript or NoScript option of these browsers.

- Check the contact section of the websites (address, phone number, e-mail).
- Check the actual destination of the links by passing the mouse cursor over it and viewing the real address in the lower-left part of the browser.
- Pay attention to which plugins you install, often they come with malicious software.
- Do not click on links in pop-up windows.
- Check for “https://” at the beginning of the web address before entering personal information.

Be very careful about Software Installation.

The principle is: if you aren’t looking for it in the first place, don’t install it!

Many threats online come in the form of requests to click on a specific link or, open an attachment to an email message. Others ask you to open ‘pop-ups’ asking to run a security scan or to install a player to be able to view content. Avoid complying with such requests.

If you still need to install such an application, do a pre-check on specialized and recognized websites. If it is necessary to install the software, download it directly from the website of the manufacturer and not from third-party websites.

Remove Applications that you are not using.

If you no longer need a certain software package, uninstall it!

It will then be easier to track applications that need to be updated and will allow faster run of tasks by the computer. When many small applications and add-ons are installed together, they take up memory and affect overall performance. Things slow down.

Protect your Internet Connection.

You use a router to connect to the Internet, these come to you with default passwords that must be changed. They are usually very simple like “1234”, “0000”, “admin”, “root”.

The router also updates firmware and installs safety patches. Make sure your router is configured to provide encrypted connections. WPA2 encryption technology is the most powerful formula available in most modern routers.

By following these steps, you will greatly reduce the risk of cyber mobs taking over your Internet connection. If they get in, they can access credentials to different accounts, or to use it as a proxy for carrying out other computer attacks.

Generally, a useful rule applies; the same credentials are not to be used for access to the router, electronic messaging or social networks.

Multiple Protection is needed to avoid Malware and Attacks.

You need to be on guard and use may tools to protect the Council, your-self and your systems. Combining all of the above like; risk assessments, web filtering mechanisms, antivirus applications, firewalls and anti-malware. Use antivirus and antispyware products developed by different companies, keep them updated frequently on both the operating system and the other applications used.

All of these tools must be set in the context of the Council’s security policies. Staff must be trained in cyber awareness, product training and cyber skills. This considerably reduces the risk but does not make it go away. There is an absolute to revisit regularly. Training should be an annual event for updates and better practices.

Be Careful about your Personal Data.

Remember you are your data and the bad guys want it. Do not fill in forms received via e-mail, which ask you for personal data, passwords or PINs.

When it comes to sensitive data, public bodies, banks or big companies are more conservative and don’t ask for it to be sent via email.

So most likely the message telling you that your bank wants to update customer data and needs yours; including bank card number, PIN and password connecting to the Internet Banking account... it’s NOT from the bank!

When it comes to making an online purchase, extra attention should be paid to the level of security of the page, if you opt for an online payment with a bank card. If the page requesting bank data does not use the HTTPS protocol (https://www. shopping-site/transaction completion/...), but HTTP, which facilitates the transmission of data clearly, then it is recommended to opt for cash on delivery or to go to another website that has the desired product.

Minimum Rules for Purchases.

- Purchases should only be made on recognized and secure websites.
- The value of a purchased product must not be sent before verification of its existence and functionality.
- Website verification (there are fictitious online stores that aim to attract customers and the retention of their bank data).
- Following a simple verification method, namely comparing links received through “spam” type messages with legitimate ones from banking institutions.

What is Social Engineering?

Social engineering is the term used for a range of malicious activities accomplished through connecting with People. It uses psychological manipulation to trick users into making mistakes or giving away sensitive information.

In cybercrime, these ‘human hacking’ scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.

Social engineering is also when you are notified that you have just won a sum of money, a trip or a romantic dinner, following a lottery you don’t remember entering, then you’re asked to transmit personal data or deposit some money into an account to take possession off the prize.

Regardless of the promise, social engineers will ask you for something: to open a file attached to an email or by text, to follow a link, to install software, to fill in a form with your data.

Be suspicious of such requests and don’t fall for them.

Ensuring a high level of security in the online environment is not an easy task. But the costs of insecurity can prove much harder to bear.

Phishing Attacks.

Cybercriminals often use email, text messages and even voice calls to fool their targets into giving up a password, clicking on a link to download malware or confirming a transaction—a practice known as phishing.

Phishing remains one of the most often-used and successful tricks that cybercriminals use to compromise victims.

To avoid falling for a phishing scam, always verify who is contacting you for your personal information.

Emails.

Email is one of the great gifts of computing. It has revolutionised communications but our daily use has caused increasing security issues.

Emails and their attachments play a very important role in facilitating attacks.

The Criminal Gangs are always lurking in the background looking for leaks from your system. Emails are a key entry point, sometimes directly by breaching the firewall or by accessing redundant mails. Organisations often times do not delete mail accounts when people leave. The Education Sector is vulnerable with the high turnover of students through actions of manipulating people

Social engineering regularly distributes spam mails; advertising products and services, intending to infect users.

Email Security Rules.

- Avoid sending or receiving sensitive information by e-mail.
- Avoid attempts at social engineering or phishing
- Choose an e-mail provider that offers strong anti-spam filtering.
- Do not respond to spam and avoid pyramidal e-mails.
- Correctly configure the email client.
- Do not use the same name for the personal e-mail account and the work one; the use of distinct names for these accounts lessens the risk of them being the target of an IT attack.
- Avoid storing critical information in personal e-mail accounts or other outside networks of the Council.

When you receive an email, pay attention for the following:

- The identity of the sender is not guaranteed: should check the relationship between the sender and the message content.
- Do not open attachments from unknown persons or legitimate accounts that have messages with suspicious content.
- If it is absolutely necessary to open an attachment, even from legitimate e-mails, it must be previously downloaded and scanned with an antivirus installed and opened with the associated application.
- In the case of e-mails containing links, do not directly access that link in the body of the message; possibly, that link can be copied and opened from another browser tab.
- Do not respond to e-mails containing requests for personal or confidential data (i.e., PIN code and bank card number).

Protect your Information.

Different types of data encryption are available on the market. Encryption can be on storage media or messages sent by Email.

You will know that you have been accessed by Criminals when:

- One of your contacts says they received spam emails from you.
- You receive many e-mails with errors.
- Messages appear in the “sent” folder without you sending them.
- The account location history in the login operation does not correspond to your current activity.

You can secure your Email by:

- Account recovery and password change.
- Changing security passwords, and setting verification by using the phone.
- Checking bank access accounts or online payments and notifying them about email account hacking.
- Notifying email contacts that there may be a security risk and that the email (the account) was accessed by unknown persons.
- Performing the backup operation on important files.

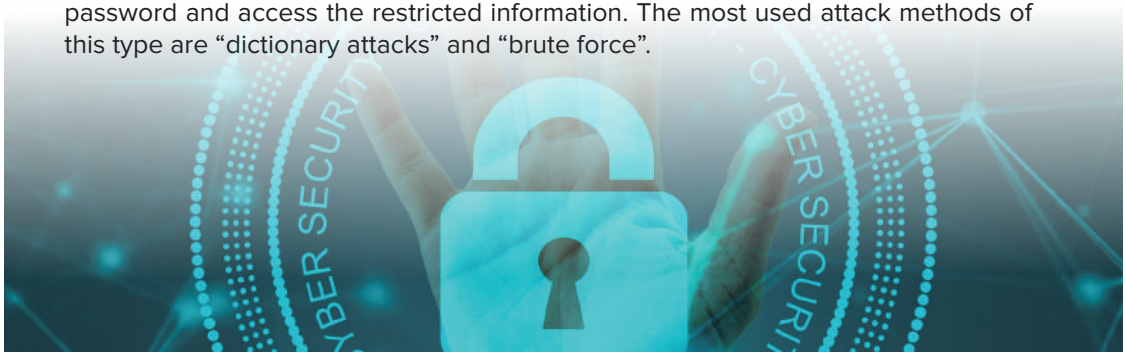
Choosing Passwords.

Password protection has now made it to the media news desks. RTE News had a piece recently where they called out the types of poor passwords that people continue to use. It was presented in a humorous fashion.

It’s not funny! A Password is an authentication tool used to gain access to a device and its data for the protection of your data.

Multifactor Authentication has become a common feature in many organisations. Check to see if its Council policy yet.

You should choose passwords that are difficult for an attacker to identify using automated, brute force tools or, by just guessing. The attacks aim to identify the password and access the restricted information. The most used attack methods of this type are “dictionary attacks” and “brute force”.



- “Dictionary attack” aims at unauthorized access to resources of IT systems, by successively trying the passwords/decryption keys in a list predefined by words or phrases.
- A “brute force” attack is a method of unauthorized access to a computer system or of decoding encrypted content, such as passwords) using “brute force” computing - via programmes that apply the trial-and-error method. The method is to try all successive possible combinations of characters, without an elaborate algorithm. It is applicable in a limited number of situations when systems are not protected with strong passwords
- Choose passwords composed of at least 12 different typical characters - uppercase, lowercase, numbers, special characters e.g. #, &, %, $, @) unrelated to you, or with the Council where you work.

Use Strong Passwords and Keep them Safe.

- Use unique IDs and passwords and do not communicate them to other users.
- The length of the password and its complexity must be chosen so that it is difficult to guess but easy to remember.
- Periodic change of passwords, at an interval of 1-3 months.
- Using different passwords for different applications.
- The use of multiple authentication methods (PIN, fingerprint, alert messages, etc.).
- Avoiding the use of similar passwords at home and work.

In short:

- Identify password-creating rules and apply them.
- Always change the initial credentials, user and password of equipment, servers, printers, routers.
- Do not keep passwords in files on the workstation or on Post-it notes.
- Never transmit passwords by e-mail or unencrypted attachments.
- Pay attention when entering passwords in the presence of other people, so as not to be observed by them.

Safe use of your Phone or Tablet.

Your Smartphone is an easy to wear minicomputers. We use them not only to make calls but also for banking, online shopping, e-mail, surfing the Internet. Most of us keep a large part of important data or personal data on mobile phones. The exponential increase in the number of apps downloaded, shared or installed is making us increasingly vulnerable to various types of malware.

Mobile banking has become increasingly popular, but without the benefit of protection mechanisms compared to those on PCs, thus encouraging computer crime. Smartphones have a low level of security. Therefore, a series of basic IT security rules must be applied:

- Only install necessary apps and check what data they have access to before downloading them (geographical positioning, contacts, phone calls, etc.). Avoid installing apps that request access to information that is not necessary for them to function.
- In addition to the PIN code that protects the SIM card, use a password or code to secure access to your phone and set it to lock automatically after (re) starting or at a shorter time interval in case of inactivity.
- Install security software specially designed for mobile devices; these can detect and remove viruses, and block multimedia spam messages or other cyber threats.
- Encrypt the internal memory of the phone or tablet if it contains sensitive information; if the mobile device is lost, the person who comes into possession of it will not have access to data.
- Make periodic data saves on an external medium in order to be able to restore them.
- Do not allow saving passwords, especially on banking applications or service providers for consumption management and bill payment.
- Periodically apply the security updates provided by the software manufacturers installed on mobile devices.

Data Protection on your Travels.

The use of mobile devices is increasingly helpful when on business trips, giving access to data and systems back home while away. Making is easier and simpler to travel.

However, there are several risks involved; data is sensitively circulated - data whose loss or theft can generate important consequences on the organization's activities.

Before Leaving.

- Only use equipment need for the trip and subsequent meetings and containing only the strict data requirement.
- Make a backup of the data to be able to restore them in case of loss.
- If you have to work during travel, use a protective filter for the screen and a secure connection for accessing company resources from a distance.
- Apply a distinctive sign to your devices to make sure that no substitution took place.
- Do not allow saving passwords.
- Delete connection history on your tablet or phone; they help one potential hacker to identify your data - locations, habits, connections.

During the Trip.

- Keep devices with you.
- Disable Wi-Fi and Bluetooth functions.
- Remove the SIM card and battery if you need to leave the phone unattended.
- Inform your Council in case of baggage inspection or seizure of devices by foreign authorities.
- Don't use equipment received as a gift if you can't check it first.
- Avoid connecting your equipment to those of other entities. If you need to extract files like presentations from the laptop, use a dedicated memory stick with the appropriate software.
- Do not allow the connection of other equipment such as a phone, USB stick, camera to those you travel with.
- Use mobile modems from mobile operators.
- In case of loss or theft, load software for remote deactivation of mobile devices and protect stored information against intrusion.

On Return Home.

- Clear call history and GPS navigation.
- Change the passwords used during the trip.
- Submit the equipment for inspection, if possible.
- Don’t use or scan memory sticks, phones, laptops and tablets with presentations where you used internet services provided to you during the trip, as they may contain malicious software.
- If necessary, for greater security, use the device reset mobile function, which allows all existing data, subsequently installed software to be deleted and destroyed, returning to the initial settings of the manufacturer.

General Recommendations.

- Avoid the publication of personal information such as birthdays, email addresses or home addresses.
- When you post photos, make sure you only do it with people you know, which do not capture exact locations.
- Never reveal information when you leave home.
- If you have children who are allowed to use the family computer, do not give them privileges of administrator on that computer.
- Install an antivirus solution with parental control, content filter and social network filter. Given the amount of pornographic content and violence online, it's a must for parents to keep their children safe.
- Inform yourself about cyberbullying and have discussions with your child.

Final Thoughts.

This document is not intended to be an absolute guide against cyber threats. It can contribute to the development of a security culture and starts to create the right behaviours. Namely;

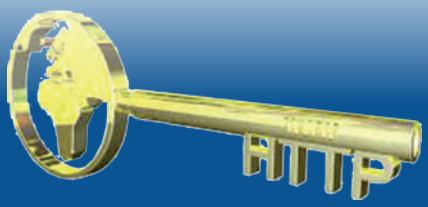
- Safe and responsible communication.
- Wise use of social networks.
- Transfer of digital content in a secure manner.
- Proper use of passwords.
- Avoiding the loss of important information.
- Ensuring that only certain people have access to information.
- Protection against viruses or other malware.

Sources to consider:

November 2023, *Best Password Managers,* **En Cybernews,**
https://tinyurl.com/yc89ywrn

Kevan Lee, July 8, 2014, *Four Methods to Create a Secure Password You'll Actually Remember,* **Lifehacker, accessed 07 November 2023,**
https://tinyurl.com/35xddm75

Paul John Spaulding, October 30, 2023, *Swiss Made Cybersecurity. Election Security. Alain Ghiai, Founder & CEO, Sekur Private Data Ltd.* **Cybercrime Magazine Podcast.**
https://tinyurl.com/5ekxv6tu



Senator
Gerard P. Craughwell

Joint Oireachtas Committee on Foreign Affairs and Defence
Joint Oireachtas Committee on Transport and Communications
Joint Oireachtas Committee on Public Petitions
Committee of Selection (Seanad Éireann)

Seanad Éireann, Leinster House,
Kildare Street, Dublin 2.
Tel: +353 1 618 3323 Mob: +086 022 9855
Email: Gerard.Craughwell@Oireachtas.ie
Web: www.gerardcraughwell.ie
Twitter: @GCraughwell
Facebook:www.facebook.com/Senator-Gerard-Craughwell-1520429548255015/