CYBERCRIME

RISKS & PREVENTION TIPS

AN GARDA SÍOCHÁNA

Garda National Cyber Crime Bureau

GARDA NATIONAL
CYBER CRIME BUREAU
Walter Scott House
Military Road
Dublin 8
D08 PTX6

01 6663496/7

GNCCB@garda.ie

Please report all cybercrimes to:
YOUR LOCAL GARDA STATION

CYBERCRIME

RISKS & PREVENTION TIPS

CYBERCRIME...

Barry Walsh

Detective Chief Superintendent, Garda National Cybercrime Bureau.

It is my privilege to publish this booklet titled **Cybercrime Risks & Prevention Tips** for use by all our stakeholders. As the Detective Chief Superintendent with responsibility for the Garda National Cyber Crime Bureau (GNCCB) it is my desire to engage with all users of electronic devices about some of the most dominant risks that are currently a reality of operating in the cyber environment.

Online connections and devices now exist in over 90% of our homes and businesses, and there are now a greater number of mobile devices in use in this country than there are inhabitants.

The current climate sees more and more people using the online world as their primary means of interacting; both in private and professional capacities. ICT Technology is increasingly important in all our lives as Irish society continues to embrace the blended home/office environments, and it has resulted in immense quality of life benefits.

However, the criminal community has also embraced the global reach that this technology and the internet provide. They provide those who have criminal intent with a universally available platform to access any network or computer from any other part of the globe. In the same way that this has huge benefits, there are associated risks. Preventing that access is a key enabler in reducing those risks.

It is my experience that education and awareness are two critical elements in preventing cyber criminality. The capacity of cyber criminals to launch a devastating cyber-attack is no longer dependent on having high-levels of specialist skills and knowledge.

Developments in the cybercrime landscape now mean that those with criminal motivation can purchase cyber-attacks as a service (CaaS). In a world where potential victims are globally accessible 24/7 at the click of a mouse; all that is required is a computer, an internet connection and the intention to attack. Unfortunately, the latter is an all-too-frequent reality in today's cyber domain.

This booklet, setting out cybercrime risks and prevention tips, is intended to enhance awareness in relation to the types of cybercrimes that exist along with providing cyber security advice to support to IT system owners and users in developing and implementing appropriate prevention techniques.

Because of the dynamic nature of cyber criminality, the content of this booklet should not be regarded as an exhaustive list. Rather, it seeks to highlight some of the core information that will enable you, the reader, to implement the appropriate cyber security precautions that every internet and network user can take, themselves, whether you are an IT system owner or user.

Our work here in the Garda National Cyber Crime Bureau is continually focused on helping people and companies proactively combat cybercrime by delivering enhanced awareness to support effective prevention. This booklet is delivered with this ambition resolutely to the fore. It recognises that we can only be successful if we all work together to Keep People Safe online.

Barry Walsh

CYBERCRIME

RISKS & PREVENTION TIPS

CYBERCRIME WHAT IS IT?

Cybercrime is the use of a computer to further or commit illegal acts. The cost of cybercrime continues to grow as its illicit benefits are recognised by criminals and organised crime gangs and it falls under two primary categories.

Cyber Dependant Crime

These are crimes that cannot be committed without a computer being involved because the computer is the target of the crime. Offences such as unauthorised accessing of data, interference with computer systems or data and data interception of examples of these types of crimes. These include deliberately injecting viruses or encryption malware (ransomware) into a system or denial of service attacks where a system is bombarded with requests and unable to function properly. These types of crimes are prohibited by the Criminal Justice (Offences Relating to Information Systems) Act 2017.

Cyber Enabled Crime

These are traditional crimes such as frauds or harassment that are committed over a computer network. The Internet and computers have increased the reach and victim base of these crimes and over 70% of frauds are now committed online.

The apparent anonymity of sitting behind a computer is not a protection from fraudulent emails, fake friend requests or offers that seem too good to be true.

PREVENT TO PROTECT

'There are two types of companies, those that have been the target of a cyber attack and those that will be'.

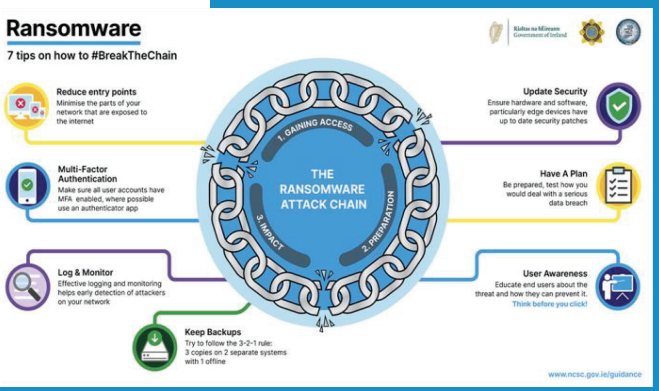
Recent times have seen cyber attacks against critical national infrastructures with those in the areas of health and education being subject to publicity over the past few years.

At the same time, SMEs have increasingly found themselves on the end of unwanted cyber attention from criminals and curious hackers.

The cost of a cyberattack can be significant. Reputational damage, data loss, recovery costs and the possibility of fines for breach of regulation can seriously impact a company or a sole trader.

Individuals are also targeted by hackers and online abusers with cyber frauds and fake profiles being used to deprive victims of their property and their privacy, often with devastating consequences.

A tested recovery and prevention plan is essential as is the training that should accompany every cyber security plan. Recovery is not always possible but prevention is.



CYBER DEPENDENT CRIME

Most cyber dependent crimes, or attacks against computer systems, occur through infected devices, phishing emails or unpatched outdated applications or software.

Companies

As we spend more time online, whether for work or personal reasons, we are no longer surrounded by reminders to change passwords and update systems regularly. We use the same devices to store and share documents or files between personal and work computers. We are increasingly blending work and life in our home offices surrounded by the demands of bosses and family. Over 40% of ransomware attacks arise from phishing emails where the victim clicks on a link and enables infected malware to install and encrypt the device or network.

Many companies post too much information on their public websites which is then used to connect with employees or customers and gain access to accounts or profiles. At the same time mobile devices are given to employees but are often not updated or as secure as the laptop they also have.

Personal

Passwords for social media accounts are often made up of the name of the family pet or dates of birth. This same information is then posted on profiles along with pictures of birthday celebrations at local restaurants.

We have a tendency to post personal information on our social media profiles or websites. It is not uncommon to see pictures of birthday celebrations announcing the age, and consequently the date of birth of the person involved. Or a picture of the family pet, new car or a new holiday which all provide hackers with valuable information that can be used to crack passwords or socially engineer (trick) the victim into granting access to the account and its data.

Some Effective Prevention Techniques

- Have secure and separate backups. Not on the same system but on a separate network or on the cloud.
- Don't post online what you wouldn't post offline.
- Change passwords regularly or use complex combinations of letter, symbols and numbers.
- Use a VPN to connect to a corporate network and never use public Wi-Fi to send or share sensitive information.
- Update/patch software and applications regularly from reliable official sources.
- Don't respond to unsolicited friend requests or emails asking for personal information or to update bank or other accounts.
- Use multi factor authentication for account or device access.
- Never pay a ransom demand. It may not be the final one and you may not get data back.
- Treat mobile devices like any other network device.
- Have a cyber response plan and test it regularly.
- Keep up to date with current risks and train yourself and your staff to recognise and respond.
- Monitor network traffic. Increased emails may suggest a Denial of Service (DoS) attack.
- Know your staff and contractors. Is the threat from within and can it be contained or removed?

CYBERCRIME

RISKS & PREVENTION TIPS

MALWARE

Malware, or malicious software, is used by attackers to gain unauthorised access to a computer, steal or encrypt the data or inject code onto the system allowing remote administrator control.

Malware injections can infect a computer network in many ways but the common thread in each method is that a person is involved in some way including:

- Accessing infected email attachments, clicking on links that lead to fake or infected websites or downloading files from unknown sources to external devices which are then connected to a network or a secure work system.
- Other methods of malware infection are through an unknown security vulnerability in software or in the system protections (Zero-Day) and legacy systems that are unpatched and vulnerable (Exploit).

Types of Malware

There are a number of malware types that are regularly encountered. While they carry out different functions, most have a similar purpose, to steal information and gain administrator rights (Privilege Escalation) on the targeted computer system. The most predominant forms of malware are -

ADWARE
Used to display advertisements in popup windows, the software embeds itself in the system and is mostly harmless, if not extremely annoying.

SPYWARE
Malware that spies on your activity and in particular your internet access so that it can send adware specific to your interests or searches. However, it can also be used to spy on sensitive corporate information and transmit it to another location or system.

RANSOMWARE
The most intrusive and damaging form of malware, ransomware infects a system and encrypts it to prevent access. The victim then receives a ransom demand, hence the name, which they must pay if they want to get control of their data or system again.

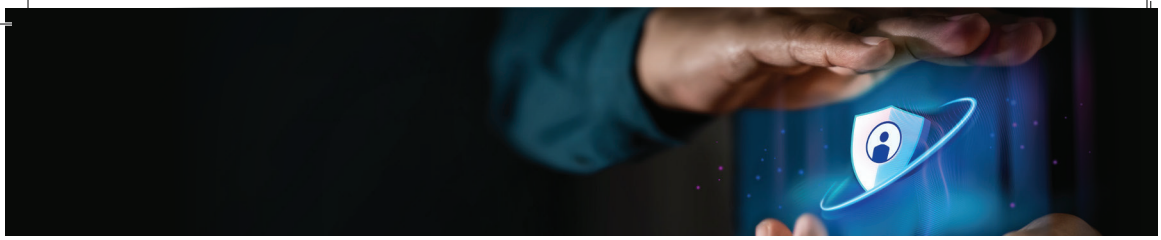
TROJAN
A virus that appears to be something completely different, they usually create a backdoor into a system which allows access to information on the victims' computer.

WORM
Viruses that can exist independently on a system and begin to replicate themselves. They do not require user interaction to begin working and also don't need a host. Their damage results from increasing the use of a network or system resource such as memory or the CPU which causes the system to crash.

VIRUSES
A virus is a malicious file that targets other files on a system and beings to infect and corrupt them. They can spread from computer to computer by attaching to an application or a file but are not capable of replication. They are also not capable of executing themselves but begin to work when the user accesses the host file or program.

KEYLOGGERS
A keylogger is a form of spyware that records all of the keys that are pressed on a keyboard but these are largely restricted to physical keyboards rather than virtual keyboards on a screen. While the keylogger is not damaging, it can be used to identify and copy sensitive data such as passwords or banking details.

All of these types of malware can equally exist and function on mobile devices and some, such as Triada, are specific to mobile phones.



MALWARE PROTECTIONS

ANTIVIRUS SOFTWARE

The primary protection against malware and virus infections is to install effective, often paid, antivirus software from reputable providers. While there are a number of free anti-virus software tools, many of these have limited functionality and their virus definitions are not updated daily as their sister paid versions mostly are. Any installed anti-virus software must be updated regularly if it is to properly protect files, memory and software on the system.

BACKUPS

While antivirus may be the primary protection, the most important is backup. It is essential that regular data backups are created to secure and separate devices such as another system or the cloud. Many users create regular backups but store these on the same system or within the corporate network. This is akin to storing the spare car keys in the glove compartment. It is advisable to create two separate backups so that at least one is available should the other fail. At the same time, the backups should be encrypted and checked regularly to ensure they still function and are accessible. However, any backup server should also have its own protections such as malware or anti-virus software, regular updates of software and user access controls.

FIREWALLS

A firewall is an electronic barrier between your network and the Internet. They control the traffic between both by filtering its content, access and keep dangerous content and traffic out while ensuring restricted access controls from your system are maintained. If you don't have one, get one from a reputable source and update it.

POLICIES

Many companies, and individuals, have policies that apply to online access and system use, password and updates. However, it some cases these policies are neither enforced nor tested and they remain words on a page. A robust cyber security policy should be risk assessed and appropriate to the needs of the network, plan for a cyber-attack and define roles and responsibilities, set out an action plan in the event of a cyber-attack, be regularly updated to take into account changes in risk and network topology, and be regularly tested to ensure it is appropriate and it is adhered to.

BYOD

External devices exist in every digital environment, as memory sticks, external hard drives or mobile phones which are used to access and store data and files that we need during the course of our work or our private online activities. Ensure a BYOD policy is in place that ensures personal devices are scanned for viruses or malware before being connected to any network or laptop computer. At the same time, devices should not be used for shared personal and work related activities to prevent the possibility of cross infections.

EMAILS AND ATTACHMENTS

Infected email attachments are a primary source of cyber-attack using infected links or attachments that download viruses or link to infected sites and files. Have a policy about opening emails or attachments from unknown sources. Hover over links in emails to see where it goes, check the email address is correct. If you didn't solicit the email or don't know the sender, delete it and block it if necessary. Report the email and contact the alleged sender by a known address or phone number to check if they sent it. And Report the Email to your ICT department so others can be warned.

SOCIAL ENGINEERING
WHAT AND WHY?

Social Engineering

Is the ability of a cybercriminal to trick a victim into trusting them and providing personal or sensitive information such as login details. Often they pretend to be someone else such as a friend of a friend, a representative of a company or the sender of an email from a trusted source such as police.

There are different types of social engineering which depend on the targeted victim and the device or system being used by the criminal.

Phishing

Phishing is the original social engineering method and it involves emails that appear to be coming from a trusted source such as a bank, government agency or a supplier.

The email suggests there is a difficulty with the account and asks you to verify your login details by clicking on a link and re-entering the data on a webpage that looks exactly like the genuine page.
The tone of the email is somewhat threatening and its appearance means the recipient is more likely to trust it and follow the link.

The email can come from an address that is very similar to the genuine sender's address e.g. @garrda.ie instead of @garda.ie. Or the genuine email address can be spoofed by using software that can be accessed on the Internet.

Like every crime trend, phishing is evolving and a new development sees a second email being received which also claims to be from the bank and states that the first message was fake. The second 'genuine' email offers protection if you follow the link it contains.

The data captured by the fake webpages is sold or used to access accounts and withdraw funds. The emails can also be used to install malicious software such as Ransomware with reports suggesting over 90% of this type of malware are sent in this way.

Thousands of phishing emails can be sent at the same time and the potential returns can range from €10 to hundreds of thousands of euro and, in very extreme cases, into millions.

Spear Phishing

This type of phishing targets a specific individual or role within a company so it could be sent to the finance office or to the IT department. These are potentially high value targets and their personal information is often listed on the company website.

Posting too much information on a corporate webpage makes spear phishing attacks easier and is often unnecessary data leakage.

A simple google search can show what information is available about you online. Does it all have to be out there and can you limit information to generic emails such as info@ or a central contact number? Is the same detail used for personal and corporate work or are they separate?

Smishing

The SMS version of phishing, the criminal uses a text message to convince the recipient to send them personal information or to install malicious software using a link contained in the message.

The term Smishing is a combination of the terms SMS and phishing with messages configured to look like they are from a reputable source.

The threat from Smishing attacks has increased as more people are using mobile phones for personal and work activities and these can also connect to other devices or networks.

Vishing

Vishing, or voice phishing attacks, a criminal will leave a voice message for the victim instructing them to connect to a website and, as with other attacks, provide their personal or logon details.

PREVENTIONS

All of these attacks follow three stages of obtaining trust by

- posing as a legitimate source,
- using a context relevant to the recipient such as banking or online profiles, and
- using emotion to convince the victim to respond or to follow the link.

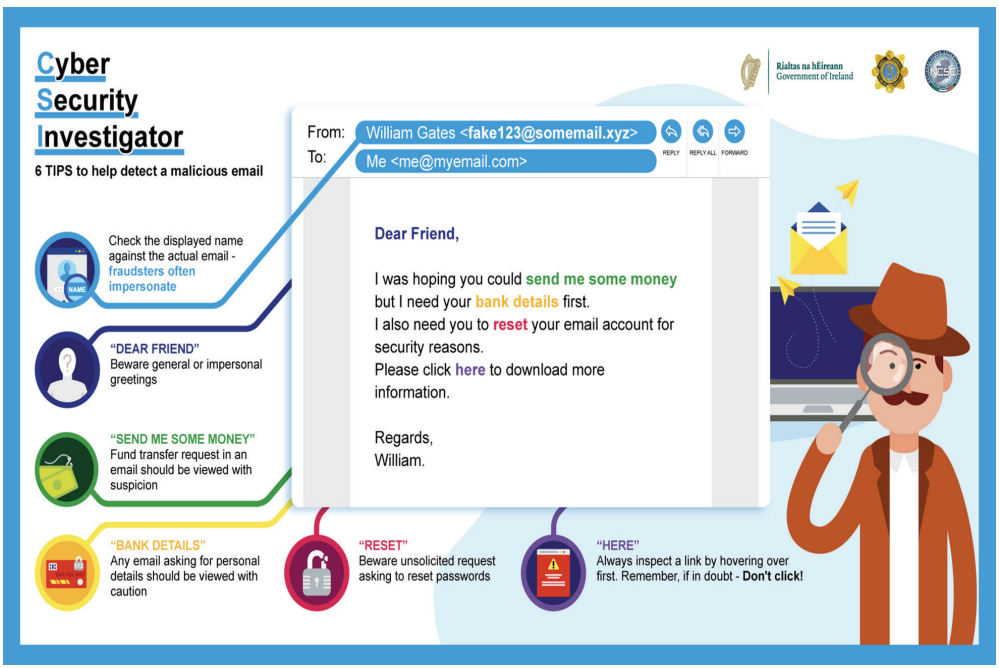
If you get an email or message like the ones above be suspicious of both the content and the sender. Your bank or other suppliers and government agencies will never send you an email asking you to supply your logon credentials by clicking on a link.

Never supply personal details by clicking on a link in an email or a text message. Hover the cursor over the link to see where it is leading you to.

Check the email address to see if it is correct and if unsure check the correct email using Google or another search engine online.

Use you antivirus software to protect against phishing emails and don't forget, the best way to check the message is to contact the company by phone.

Your greatest online protection is to be aware of the dangers and, as a result, be able to display an appropriate degree of cyber vigilance and cautiousness. If in doubt, verify by personal contact before you engage further.

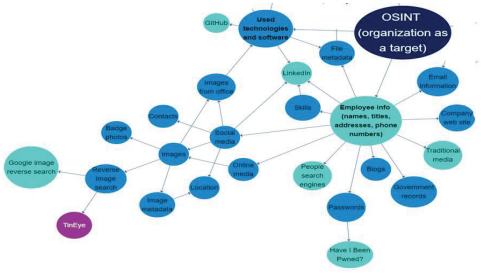


CYBER ENABLED CRIMES

Computers have made traditional crime easier, more global in its reach and accessible to anyone who owns a computer and has an Internet connection.

Cyber enabled crimes are traditional crimes that happen to occur online. The same crimes were traditionally encountered offline but with the advent of computers, they are now just as easily committed online as offline. Many of them are online frauds and these often start with the decision to post sensitive or useful information on social media or on a public website. This information can be a valuable source to cyber criminals who use this data about employment, dates of birth or educational achievements, to their own advantage. This form of data exfiltration is called data leakage and is all too common.

How often have you seen postings on social media taken at a restaurant or a hotel poolside? While this tells friends you are having a great time, it also tells criminals you are not at home. Posting an email address or a telephone number on social media can have the same effect. The cybercriminal can use these 'open source' details to create a phishing email specific to you, or that appears to come from you such as an invite to a special event or to participate in a prize draw. A simple google search for your name will give you some idea how much you have online.



In the same way that a company or employer will use an online search to find out about competitors or prospective employees, a criminal will do the same to find out about the company, its employees and potential ways to socially engineer a way in.

Protecting against data leakage

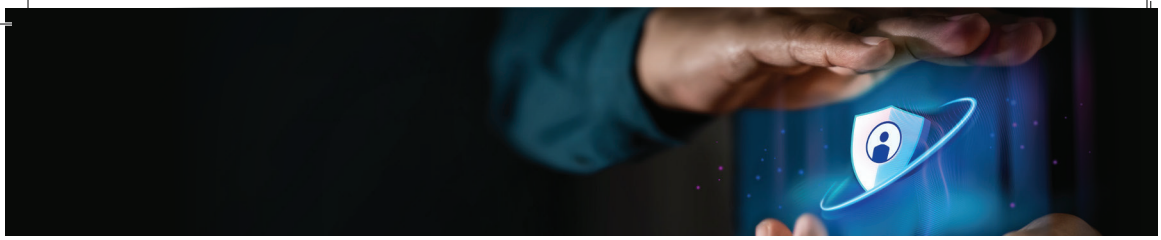
Data leakage can occur in a number of ways, all of which are avoidable or can be mitigated against. Failing to update systems regularly or poor policy implementation when it comes to user access controls all contribute to an environment where data is lost or vulnerable.

One of the greatest risks to a network is the people factor spoken about earlier where simple errors of judgement or practice can lead to the loss of data. In many cases, human errors expose a network to the risk of data loss through malware injections from opening email attachments, connecting unscanned external storage devices to systems, using the same devices for personal and business work, or deliberate actions by disgruntled employees or suppliers.

A few simple steps can enhance good cyber security awareness and practice.

- Develop, and regularly test, robust policies, procedures and guidelines on system usage, passwords and social media access usage
- Know your staff, what they can access and if they pose a risk
- Patch, backup and update systems, especially legacy systems
- Train all personnel for risks and preventions and test the training regularly.
- Restrict public facing information on the corporate website to what is needed.
- Monitor unauthorised use of the company logo or information online and check social media accounts.
- Filter email and network traffic for suspicious activity

The consequences for failing to protect data can be high. Reputational damage, financial loss, data loss, fines for breach of regulation, recovery costs. All of these are possible where customer lists, contract details, financial information or other sensitive data is exfiltrated because simple precautions were not taken.



CEO FRAUDS

CEO frauds use company executive information that is available on the corporate website such as the CEO email address. A low-ranking employee receives an urgent private email from the CEO instructing them to change the banking details of a supplier for a new 'hush-hush' contract. The tone of the message is urgent and there is a threat to tell no-one about the email or the change and only contact the sender of the email directly.

'Hi Martin…I got an email from Smichals who tell me we were late with the last 2 payments. That's not acceptable. Their new bank account is AIBIE92…… Process the new outstanding payment of €40,000 now and tell me when it is done. I will wait for your call by return and only speak with me about this.
Richard CEO'

Feeling threatened, Martin transfers the funds and replies to Richard's email at Richard.flynnn@company.com but doesn't notice its different from Richard's actual email which is Richard.flynn@company.com.
The losses in these cases can be significant but can be prevented by requiring any such change to be checked with another staff member first

UPDATE POPUPS

Another version of the fake email fraud is one which appears to come from a software provider stating that the version being used is out of date. You are asked to click on the link or the pop-up and download the latest version. The next window asks for logon details for the software or payment details to process the cost of the update. These can then be used to extract money or to access accounts and install malware such as ransomware or keyloggers. Another type of pop-up warns about a new malware threat and advises that you download protections by clicking on a link it contains.

Software providers do send out update notices, but any update should be started by your ICT provider or by using the update function on the system itself. Warning signs are vague or grammatically poor language, an increase in update requests or an urgent demand for payment from a software provider.

FLUBOT VIRUS

While Flubot was originally designed for Android phones, it has now extended to iPhones. The victim receives an SMS telling them their parcel is delayed and to track it using the link in the message. However, clicking on the link brings you to a fake data capturing webpage or to download a security or tracking application. The result of using this link is the Flubot virus is installed and grants permission to access contacts, text message and call records and services. It can also take control of the screen tap process and create fake versions of banking applications on the device.

Never click on a link whether you are expecting a parcel delivery or not. Contact the delivery company directly or via their website, or use their official parcel tracing service which is also available on their corporate website. Keep an eye on payments from your account and monitor the number of text messages being sent to contacts. And don't forget about strong updated anti-virus.

FAKE REFUNDS OR FINES

It's a modern day reality that people will receive fake emails or text messages purporting to be from Revenue informing them of a tax refund or from Gardaí telling them they have been fined for illegal online activity. These are designed to trick the person into disclosing financial details or to download malware.

Are you due a refund, is the fine accurate or do you have an appointment with the service listed? If the answer is no or you're not sure, contact the alleged sender using the entities' details that can be found in the phone book or their official website online, and Do NOT use the details in the message you received. And ensure you report the message to help An Garda Síochána prevent some other user becoming a victim of the same cybercrime.

CYBERCRIME

RISKS & PREVENTION TIPS

ONLINE HARASSMENT

Many people find themselves at the receiving end of unwanted and abusive chats or content from other social media users or totally unknown individuals. This form of harassment, prohibited under the Non-Fatal Offences Against the Person Act 1997 as amended, can be very threatening and disrupting to a person's peace of mind and welfare, especially where the sender and reasons for the abuse are unknown.

For Users: Be careful who you friend. If you don't know them or they aren't recommended, delete the friend request and block them. Don't post anything online that can be used to abuse or embarrass you. Never go off platform to continue a chat or a conversation. If you're not sure search for the profile image to see if it is used on another account. If you are abused online, save copies of the message or chat and block the sender. Report abuse to someone, a friend, family member and Gardaí. Remember you are the victim.

For Parents: Talk to your child about the risks of online activity such as abuse or exploitation and know the warning signs that something is up. Is your child missing school or has their mood changed, especially after being online, and are they not eating or sleeping properly? Are they staying indoors and not meeting friends like before? Encourage children to tell you if something is wrong, that they know they are a victim. Tell the school and Gardaí. It's a crime

ONLINE STALKING

Stalking is another side to online harassment and was added to the Harassment prohibition by the amending Criminal Justice (Miscellaneous Provisions) Act 2023. It occurs where a person develops an obsession with another to such an extent that they persistently follow or contact them. As a consequence the victim fears for their safety, regardless of whether harm is the intention of the stalker or not.

The measure of stalking is behaviour that is Fixated, Obsessive, Unwanted and Repeated or F.O.U.R.
If you experience any of the following you should report it to your local Garda station.

- Loitering around your home or spying on you.
- Following or making unwanted approaches to you or families about you
- Threats to harm you or others if you don't response to their advances
- Sending inappropriate content or messages or unwanted gifts and calls
- Making false complaints or taking false legal claims against you

SEXUAL EXPLOITATION

In some cases, online abuse can take the form of sexual exploitation. The contact starts the same with a friend request, usually from an attractive male or female and the user's age is around the same as the person they want to be friends with. Gradually the conversation gets personal and there is a request to exchange sexual imagery.
Once that happens, the conversation changes completely and becomes threatening, demanding more explicit content or payment to prevent the images being sent to all the victim's contacts. Victims can be children with offences under the Child Trafficking & Pornography Act 1997 or adults with offences of coercion under the same Non-Fatal Act as above or blackmail under the Criminal Justice (Public Order) Act 1994.

Again, the advice is the same. Only friend known or recommended profiles. Be suspicious of unsolicited requests and if it looks too good, it probably is. Never

exchange sexual imagery online and block any suspicious or abusive contacts. Save a copy of the messages or chat and report it to a friend, family and Gardaí. It's a crime.

REVENGE PORNOGRAPHY

Many relationships don't end well or by mutual consent and one party can feel aggrieved to the extent of seeking revenge. The online world provides an anonymous place to seek revenge by posting intimate images or videos taken during the relationship in order to embarrass or harm another person's reputation and peace of mind.

Posting intimate imagery of another person without their consent with the intent to cause them harm or ignoring the potential for harm is an offence under Coco's Law, or the Harassment, Harmful Communications and Related Offences Act 2020. The same is true for recording intimate images or content of another without their consent and publishing them, even if there is no intent to cause harm.

If someone does post intimate images, regardless of when or where they were taken, report it as it's a crime. The same is also true for sending offensive or threatening messages by text, online chat or email to another person, or publishing those types of messages about another person. If you didn't consent, it's a crime.

ROMANCE SCAMS

Other people are searching for relationships and use online platforms or dating apps to meet someone new. But these platforms are also used by scammers and fraudsters who only have eyes for your money.

- If he/she looks too good, they probably are.
- If they are much younger than you, tread carefully.
- If they express their love for you quickly, beware.
- If they ask for money, bank account or bank card details for any reason, it's almost certainly a scam.
- If they ask for money for a sick friend, an operation, it's a scam.
- If they ask for money for a business venture or to travel to meet you, it's a scam.
- If the amounts start small and then get larger, it's a scam.
- If they quickly ask to move the conversations off the platform and onto messaging or phone, beware.
- If they ask you a lot of questions but give you vague answers to yours, beware.
- If they ask for your phone number but seem reluctant to give theirs, beware.
- If the grammar and spelling in their messages is poor but they went to university, beware.
- If they avoid using video chat or meeting in person, it's a scam.
- If you search for their profile picture using Google Image Search and find it used elsewhere, IT'S A SCAM.

Commonly known as cat-phishing, these types of crimes are all too common and the losses can be significant. If you are a scammed, don't be embarrassed as you are the victim of a skilled fraudster. Tell a friend and tell the Gardaí.

FAKE ONLINE GAMING SITES

Online gaming is a thriving community made up of skilled players and newbies who learn on the fly from their peers.

However, some gaming platforms are prowled by the same scammers that join social media to defraud or abuse

other players. They can also be used to download malware or bully other users. The same protections apply on both and will help gamers keep safe.

- Only use official sites to purchase games and updates.
- Don't respond to emails or direct message requests.
- Don't accept requests to chat off platform
- Don't share personal or private information, no matter who.
- Don't accept requests to meet up unless you know the other gamer or it's with a group.
- Don't agree to meet or give out your phone number unless you know the other player personally.
- Use strong passwords for your account and multi-factor authentication to be doubly sure, especially for purchases.
- Be careful of links to offers for great games or software. Hover over the link first to see where it is going. It could be malware or a scam.

The online gaming world is a very select group but predators can use the platforms to find new victims for sexual and financial exploitation. The community is also competitive and this can open it up to bullying. If that happens, stop the contact and report it.

INVESTMENT SCAMS

Investment scams are increasing with offers of quick profits or high interest returns. Many of these schemes advise investment in unregulated cryptocurrencies, which are subject to significant fluctuations in value. The promise of great returns is a temptation that is hard to resist. But is many cases, the only one making a profit is the one making the offer. Losses can range from €2000 to hundreds of thousands. The Central Bank keeps a register of licenced investment brokers and has published some very useful advice to anyone looking to invest.

- Beware of get rich quick offers and investment popup adverts, there is no such thing.
- Always seek independent investment advice before parting with any money
- Avoid investment schemes with celebrity endorsements. It's unlikely they are legitimate.
- Never make a quick or uninformed decision, especially when it comes to investing in cryptocurrency.
- Only use regulated investment brokers. Check the Central Bank website for the broker's name. If they aren't listed, report them and avoid.
- Do a quick Google search for the broker. You may be glad you did before investing.
- Never disclose personal or banking information.
- Beware of any suggestion to download software to your system.

SAFE ONLINE SHOPPING

Many people are now using online platforms to shop while most high street retailers have an online presence offering the same goods and bargains you can find in-store. The attractions are convenience, all year round availability and home delivery services with the same return policy you would expect instore.

But additional risks arise online because you aren't in the store and the seller is not in front of you. Fake websites and 'bargains' can be avoided if you take proper precautions when shopping online. Other risks are unique to online shopping and knowing these can keep you and your money safer.

- New sites with excellent reviews are a warning sign
- Sites offering once in a lifetime bargains

- Payments for goods by money transfer only
- Sites or profiles offering second or last chance purchases of sold out goods
- Shopping sites that aren't encrypted with https:// in their address
- Retailers beware of bulk orders, especially from new or overseas customers
- Check that the delivery and billing address are the same or that postcodes link to a business or home

E-Commerce sites can be hijacked and the stolen user details used to create duplicate accounts. Adverts can be faked with cloned pictures of previous sold goods. Reviews are easily duplicated or faked.

WORKING FROM HOME...

As more and more employees work from home or in a blended home/office environment, companies are expected to provide a strong connection to the corporate network. Staff should be able to send and receive email, access company files and accounts and upload contracts, materials or reports securely.

However, where the supporting ICT infrastructure is not supported all data is open to unauthorised access or hacking and that can be especially true where the system is available to staff remotely.

Virtual Private Networks or VPNs

Used to establish a secure network connection over the Internet, VPNs encrypt online data and disguise a user's identity. This double layer of security makes it more difficult to determine who the user is and track their activity or steal their data. The data is encrypted 'on the go' while also sending your IP or Internet Protocol address (see below) through a separate server which strips this identifier away and replaces it with a generic one instead.

So essentially, using a VPN allows remote access to the company network over the Internet but is hides the data traffic unless you have the decipher or decryption key. It also hides your location by stripping away your unique IP address (a numeric sequence) which you need to go online and can be used to identify who you are.

Another feature of a VPN is the 'kill switch' facility which stops your connection if the VPN is insecure or interrupted.

Wi-Fi

Wire Fidelity or Wi-Fi is a term used to define a group of network protocols or standards used to connect devices across a network. It is also used to connect to the Internet and send data by using radio wave transmission. In many cases the Wi-Fi is publicly available in stores, libraries, coffee shops or other retail premises. These Wi-Fi hotspots offer paid or free connection for sending email, accessing accounts or searching online for anything you need.

However they also pose a serious security risk as they don't require user authentication to connect to there is no protection from data sniffing or malware injections.

Man in the Middle attacks happen when a hacker sits between your device and the Wi-Fi router or server that connects you to the Internet and beyond. So, while you are sending data to the server, you are also sending it to the hacker who can see all of your information in plain text and use it as they want.

Malware infections can arise where the Wi-Fi router itself is infected and this in turn infects the connecting devices. A common method is where the user is sent fake pop-up messages suggesting they download software or update their existing operating system. Clicking on the pop-up enables malware to download and install which allows the hacker to steal or, at best, copy data, encrypt the device or hide until you connect to your corporate network and install there.

Publicly available Wi-Fi connections are notoriously insecure and it is possible to eavesdrop on traffic sent from a device to the Wi-Fi server or router. This is called **Sniffing** and can extend to the data send and received or just the browsing history and activity of the user all of which is possibly useful to a hacker.

Evil Twin attacks occur where a hacker sets up a fake or duplicate Wi-Fi hotspot with a similar name to the one expected, or an attractive sounding name which lures users to connect. The hacker then monitors and records useful traffic and data.

Free public Wi-Fi is available to everyone including cyber criminals who are capable of exploiting your use of the network to capture your log-in ID and credentials for their next criminal enterprise. Be careful or you could end up paying a high price for the free access in the end.

CYBERCRIME PROTECTIONS

Most cyber protection initiatives are generic such as antivirus, but some can also be specific depending on the type of network involved and whether it personal or corporate.

There are a number of generic protections that apply to every environment and these form the basic level approach to cyber security. The nature of the business will determine the value of its data and who might target it for intrusion.

State agencies may be targeted by State sponsored hackers. Large corporations may be targeted by competitors or organised crime groups. Smaller companies such as SMEs may be the target of ransomware groups, a trend seen by both the Garda National Cyber Crime Bureau and the National Cyber Security Centre.

A survey by IBM found that less than 8% of companies that paid a ransom recovered all of their data. The same survey found that over 40% of ransomware attacks started with a phishing email, while another survey by Grant Thornton found that only 25% of companies reported a cyber attack.

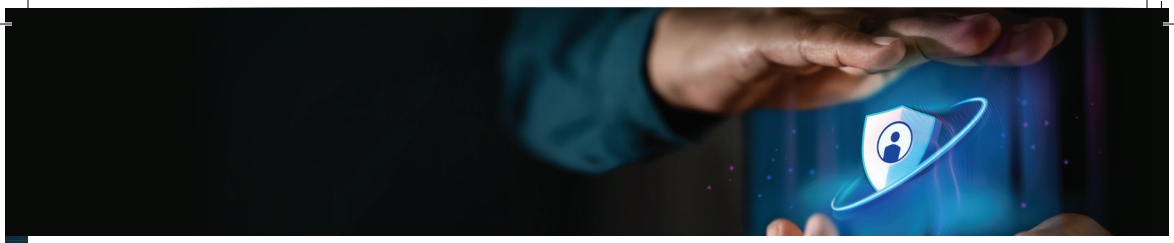
Protecting against cybercrime is an essential part of any corporate, and personal, strategy. Its worth repeating these protections

Update and backup

This can't be stated often enough. A network is only as secure as its ability to recover from a cyber-attack. Any effective recovery is centred on the ability to replace lost data with a working backup that is up-to-date. So backup your data regularly and separately, and ensure systems and software are updated from trusted sources, every day if necessary. Software, like any other product, goes out of date with time. We wouldn't eat food that is out of date so why would we trust software or antivirus products from last year to be fully effective? So update and backup you data regularly but always to a secure and separate system.

Understand your business

A robust review of the business and its functions should include looking at how a cybercriminal may attack the network and exploit its weaknesses whether they are electronic, human or process based. This form of cyber



resilience based approach will ensure that any potentially damaging gaps are identified and closed. It will also set the roles and responsibilities that should be part of any response for a cyber responses.

All of this should be part of an overall cyber culture where staff and managers collaborate to protect the company and their stake in it from attack. That culture is based on investment in testing and training that is ongoing and subject to continuous review.

Train for an attack and prepare a response

At the core of a cyber culture is risk based training that engages staff and management in responding to the risks that exist and learning from simulated cyberattacks. In that way any response can be modified where necessary, unidentified risks or Zero-day vulnerabilities flagged so that they can be prevented from having an impact.

While some training may be specific to one group, core training should involve everyone who has an incident response and prevention role. It should include lessons learned from previous events and any resilience testing that took place.

Test and test again

Testing cyber resilience can take many forms. A good cybersecurity partner will run penetration tests against a system to identify vulnerabilities and test mitigations that are in place. It will also bring new technologies and risks into play and identify where gaps that need to be plugged exist. But not every company can engage a cybersecurity company so know you own system so you recognise risks.

Know your system

That's where knowing your system comes into play and where internal tests can be used to identify gaps in processes and responses. Sending pretend phishing emails to all employees with a secure link can identify if you need to retrain staff on the correct responses and how to identify these types of emails. This should not become a blame mechanism. People will make mistakes and any test should be a learning process which encourages reporting, vigilance and trust.

OSINT

Employees should be able to use every available resource and department to identify and flag any suspicious activity or correspondence they receive. While we tend to post too much online on social media and other sites, these platforms can provide a valuable source of publicly available intelligence on email addresses, people, websites and other topics. A quick search can bring up warnings or flagged accounts that will tell users to steer clear of the offer, the friend request or the message they have received.

Know your staff and their access controls

At the same time, every company should know their staff and the roles they have, especially when it comes to sensitive corporate or customer data. And staff should also know, verbally and contractually, the limits to their access and roles, with appropriate controls to remind them such as user restrictions and rights.

Use multi-factor authentication.

Multifactor authentication is used to confirm identity and sees a message being sent to an email address or a mobile device asking the user to confirm they are trying to send funds or access a personal account. Confirmation can be in the form of a PIN code, a password, a fingerprint or a message from the provider asking for confirmation.

Passwords

Using passwords to access accounts is no longer safe but and it can be difficult to remember many different passwords for all the platforms or apps we use. So if you use a limited number of passwords they should be strong with a mixture of letters, numbers, symbols, capital and small letters. There are also a number of password management applications that can be used to store and recover passwords. However using a biometric passwords is more secure.

Other supports

A corporate newsletter is a useful resource and can be a good platform to list any risks that exist, cyber or not. There are also a number of online resources which can help a company or individual stay safe, and in many cases recover from a cyber-attack. Websites such as **https://Check.cyberskills.ie** allow you to check if a webpage is legitimate or a known phishing or scamming site.

You can check your own email address to see if it has been compromised using **https://haveibeenpwned.com**. Most cyber attackers tend to advertise their successes by posting compromised email addresses online. If yours is listed, don't panic and just change the password. Of course, you shouldn't use your email to store banking or other sensitive details in a message.

And if you are attacked with ransomware, check out **www.nomoreransom.org** which is a site maintained by Europol and cyber security companies. The site lists decryption solutions to many of the current ransomware types.

Even though it is aimed at students, **www.webwise.ie** has a number of useful resources suggesting how to stay safe online. And it would be remiss of us to not mention the **www.garda.ie/cybercrime** page that contains advice on cyber dependant and cyber enabled crimes and protections.

S	**SAFE**	Restrict public facing information to what is necessary. Must you share the CFO's personal email?
M	**MULTI**	Have policies for multifactor authentication, passwords, banking a/c changes, online meetings.
A	**ACCEPT**	Don't accept emails, links, attachments, friends requests or messages from unsolicited sources.
R	**RELIABLE**	Update software/systems from reliable sources. Have separate and secure backups available.
T	**TELL**	Always tell someone about threats, online abuse, phishing emails, mistakes made or online exploitation. You get one chance to fix.

Reporting cybercrime events

Every cybercrime event is a potential learning opportunity for the individual or company and for those involved in cyber policing and security roles. Data Protection rules like GDPR require companies to report data breaches where personal data may have been compromised.

Similar rules exist when it comes to reporting cybercrime events to law enforcement. Section 19 Criminal Justice

Act 2011 contains a mandatory reporting provision for relevant offences which include cybercrime offences of hacking and data interference. The section states that any person who has material information regarding the commission of a relevant offence is guilty of an offence if they fail to disclose it to Gardaí and can be prosecuted for same.

Every cybercrime event provides a potential learning opportunity, not only for the individual or company, but also for those involved in cyber policing or security roles.

In many cases, the only time cybercrimes are reported to Gardaí are when an insurance company requires it or the Data Protection Commissioner compels the company to do so.
While this is an understandable situation for companies who rely on their reputation to remain in business, it creates a significant gap in potential learning for everyone, including the Gardaí.

Reporting cyber-attacks to law enforcement should be an integral part of a corporate cyber culture and not one that is forced or compelled through fear of prosecution or penalty for data breach. After all, it is only through collaboration that the risk of cyberattacks can be minimised. It takes a network to defeat a network.

- REPORTING ALLOWS FOR CRIMINAL INVESTIGATION & VICTIM SUPPORT
- GNCCB HAS EXPERIENCED EXAMINERS & INVESTIGATORS
- HELPS IDENTIFY CURRENT & EMERGING CYBERCRIME TRENDS
- UNIFORMS OUR ADVICE TO THE PUBLIC AND CORPORATE SECTORS
- HELPS REINFORCE CUSTOMER CONFIDENCE IN YOUR RESPONSE
- HELPS GARDAI SUPPORT ALL VICTIMS OF CRIME
- FULFILS YOUR STATUTORY OBLIGATIONS FOR MANDATORY REPORTING

NOTES

GARDA NATIONAL
CYBER CRIME BUREAU
Walter Scott House
Military Road
Dublin 8
D08 PTX6

01 6663496/7

GNCCB@garda.ie

Please report all cybercrimes to:
YOUR LOCAL GARDA STATION

AN GARDA SÍOCHÁNA

Garda National Cyber Crime Bureau