Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCC
NATIONAL CYBERSECURITY
COORDINATION AND
DEVELOPMENT CENTRE
IRELAND

Cyber security for small business

Guidance on cyber security measures for Irish business

www.ncsc.gov.ie

Table of Contents

Introduction

Cyber security is not just an information technology problem, but an integral part of an overall business strategy. Even a minor cyber security incident can have devastating impacts on a small business in Ireland.

This guidance document includes practical and evidence-based security measures to help protect your business against some of the most common threats in the area. While implementing the best practices outlined in this guide won't guarantee complete protection from all possible cyber-attacks, it will help improve your business's cyber security defence. As a starting point for protecting your business data, assets, and reputation, we recommend the following six measures:

1	Identify what matters most
2	Keep devices and software up to date
3	Implement basic protections
4	Turn on multi-factor authentication
5	Back up your information
6	Create strong complex passwords

We have provided a cyber security checklist as part of this guidance document that can serve as an aid for evaluating your current cyber security status. This guide may include steps that are not applicable to your business, or your business may require more advanced security measures thatn are outlined here. Once you've completed this guide, we suggest that small businesses consider implementing the additional 12 steps recommendations provided by our earlier document 12 Steps to Cyber Security.

Rialtas na hÉireann
Government of Ireland
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

The potential damages of a cyber-attack to a small business in Ireland

Cyber-attacks can significantly affect your business, leading to financial losses from data theft, ransom payments, and recovery costs. Additionally, damage to your reputation can have a lasting financial impact on your business, even if the initial breach didn't cause immediate losses. It's important to note that cyber incidents can occur accidentally and may not always be criminal in nature, while cyber crimes are intentionally harmful to your business, their volume and impact are increasing each year. To the right is a report from ENISA, the EU cyber security agency, which outlines the cyber threats facing businesses across the EU.

Case study #1

Importance of cyber-awareness training

An employee at a print company received an email from their manager asking that they purchase 3 x €500 Visa prepaid credit cards. The manager told her to keep the cards confidential as they would be gift vouchers for staff members. Once purchased, the employee was asked to photograph both sides of the cards and send them to the manager as proof of purchase.

As instructed, the employee went to a post office and used her credit card to purchase the gift cards. She replied to the manager's email and sent photos of the gift cards as proof. After returning from the post office, the employee gave the physical cards to the Manager, who did not know of them. On review, all emails about the gift cards came from a random email address and were not from the manager's legitimate email account. It had been a scam.

Impact:

Financial loss to the employee and the business.

Lessons learned:

Cyber security awareness training helps employees understand and implement best practices for business security. Ensure all employees undergo at least basic cyber security training.

Always check email addresses and website URLs. Use an alternative communications method (eg. phone call to manager) to double-check, especially when credit cards are involved.

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Overview

Businesses in Ireland should take steps to ensure they apply appropriate cyber security controls

Identify what matters most

Safeguarding your business' assets against threats is paramount to its success. Given that most small businesses have moved online and often rely on technology to deliver their services, a significant threat is that of a cyber-related incident. Asset identification involves recognising and recording all the valuable assets within your company, ranging from data and systems to infrastructure and personnel.

Keep devices and software up-to-date

Updating your software and systems is one of the best ways to protect your business from a cyber-attack. Updates can fix security flaws in your operating system and other software, making it harder for a cyber-criminal to break in. Regularly updating your software and devices will reduce the chance of a cyber-criminal using a known weakness to run malware or hack your devices. Also, ensure that you understand your business obligations around updating your business systems if you use externally managed services such as cloud-hosted services.

Implementing basic protection

As a business owner or manager, you hold the key to protecting your business from financial loss, regulatory fines, and reputational damage. Cyber-criminals can exploit vulnerabilities in your IT systems, but you can take steps to prevent this by ensuring you have basic anti-virus protection in place. In many cases, successful cyber-attacks on businesses are a result of a lack of these basic protections. Most exploits require an IT system that has not been updated with security patches and has an out-of-date malware protection system in place. By

taking the initiative to deploy basic protections, including regular updates, turning on firewalls, and installing anti-malware and encryption, you can secure your IT systems and your business.

Turn on multi-factor authentication

Using multi-factor authentication (MFA) significantly enhances password security by adding an additional layer of protection, making it much harder for hackers to gain access to your IT systems. According to Microsoft, implementing MFA can prevent 99.9 percent of account attacks. See the link below. MFA requires anyone logging into an account to provide not only their username and password but also something else, such as a unique code sent via text message or generated by an authenticator app. It is important to enable MFA on all systems and services whenever possible, including cloud services, email accounts, and personal accounts. For more detailed guidance on MFA, please refer to our previously published advice on it - see below.

Benefits of MFA
Microsoft

NCSC-MFA-Guide
NCSC

Back-up your information

One of the most effective ways to safeguard your data is by backing it up regularly. The main reason for a data back-up is to ensure that you don't lose any of your important business or customer information. Ensure you are backing up all critical data, including documents, databases, and configurations. Ensure that this back-up is kept separate to the original data. It would help if you also considered the frequency of your back-ups. How often you need to back up will depend on how frequently your data changes.

Create strong complex passwords

Remember, one of the easiest and most effective ways to safeguard your business data is by using strong passwords or passphrases. Cyber-criminals employ different techniques to crack weak passwords and passphrases to gain unauthorised access to your business accounts. Once they infiltrate your accounts, they can misuse your business and personal information, steal your identity and customer data, or even gain access to your bank account.

Detailed guidance

1. Identify what matters most

Understanding what and where your digital assets are is essential to protecting them. After all, if you don't know what you have and where it is, how can you even start to protect it? Your first step is to identify your essential data—the information that your business couldn't function without. It means creating, establishing, and maintaining authoritative and accurate information about your assets that enables both day-to-day operations and efficient decision-making when you need it. It will help you track and control devices as they're introduced into your business. Steps which organisations should consider include:

Record and maintain list of all your assets

First, make sure to list all your assets, such as phones, laptops, and other equipment.

Important tip #1

You can't secure something if you don't know it exists. Not knowing your IT assets can lead to unmanaged vulnerabilities, potential breaches, and significant financial and reputational damage.

That's why cyber security asset management is a critical component to the foundation of cyber security across businesses of all types.It is the process of identifying, on a continuous, real-time basis, the IT assets your business owns and the potential security risks or gaps that affect each.

Identify your business objectives

Then, outline your business objectives by identifying the key elements necessary for the operation of your business, including products, services, and processes that support your people, customers, operations, and technology.

Don't forget your third-party suppliers

This should also include any third-party suppliers, such as cloud providers who manage systems and data on your behalf.

Remember! Be sure to maintain an updated list of all your assets and make any necessary amendments as and when needed.

2. Keep devices and software up-to-date

One of the most effective ways to manage cyber security risk is to manage the updates for the software and devices in your business. Today's cyber security threats are varied and constantly changing. Software and app developers focus daily on keeping their products secure, developing updates to patch vulnerabilities and better secure their products. Installing those updates as soon as they are available reduces the risk of cyber-criminals exploiting those vulnerabilities and targeting your business. If the manufacturer stops offering support for either the hardware or software you are using in the business, it is time to replace it with a more up-to-date alternative.

Automatic updates

Set up automatic security updates so that new updates are downloaded and installed as soon as they are available from the vendors. You may have to restart your device for the updates to install fully. Installing updates as soon as possible is best but can be scheduled outside of business hours to minimise interruption and downtime.

Important tip
#2

Do you use a point-of-sale (POS) system?

Many small businesses use cloud-based POS systems, which offer versatility and security. Security is crucial because businesses regularly manage sensitive data.

Are you regularly updating your software, or is your software supplier managing the security of your POS software?

Ensure a safe source for updates to devices and software

Know the source before downloading anything, especially software and app updates. Ensure you only download software to your business devices from verified sources and apps from an official app store. Never use pirated, hacked, or unlicensed software, which can spread malware, viruses, or other cyber security threats to your network.

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

3. Implement basic protections

Implementing basic protections, such as installing anti-virus software and training your staff to regularly back-up systems, can significantly reduce the risk of your business becoming a victim of a successful cyber-attack. This is especially the case with unsophisticated cyber-criminals who are only capable of exploiting basic vulnerabilities. Scam messages and phishing attacks are still some of the most prevalent cyber-attacks in 2024.

Important tip
#3

Is your staff aware of the risk that cyber-attacks pose to your business?

Most cyber-attacks now rely on human interaction to facilitate their success, typically early in the attack lifecycle, whereby a legitimate system user is tricked into providing the attacker with access to or a foothold into the system. This comes in many forms of social engineering, such as phishing emails and phone calls or physically bypassing security controls to access your business systems. It's critical to ensure your staff are aware of the dangers. Employees with good cyber security practices are your first defence against cyber-attacks. By providing cyber security awareness training, you help mitigate against cyber-attacks.

Scam calls and messages

Scam calls and messages are a common way that cyber-criminals target small businesses. Their goal is to trick you or your staff into sending money or gift cards, or to convince you to click on malicious links or attachments to obtain sensitive information, such as passwords or banking details. Cyber-criminals may try and scam your business through email, text messages, phone calls and social media. They will often pretend to be a person or organisation you trust.
Please contact your local Garda station or visit Garda.ie if you are concerned you have fallen victim to a scam, or if you have come across something you suspect to be a scam.

Phishing attacks

These scams often contain a link to a fake website where you are encouraged to log in to an account or enter confidential details. Phishing attacks typically compromise your account passwords. Cyber-criminals often use this method to "take over" the social media accounts of small businesses and hold them to ransom. Use caution if a message is from a known entity and yet seems suspicious. Contact the person or business separately to check if the message is legitimate.

NCSC_Quick_Guide_Phishing
NCSC

NCSC_Quick_Guide_Ransomware
NCSC

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Ways to mitigate cyber-threats by implementing basic protections

Anti-virus

A centrally managed anti-virus solution should be implemented on all types of devices and kept up-to-date to ensure continuous protection from cyber-threats. Anti-virus software, often included for free within popular operating systems, should be used where possible on all computers, phones, and laptops.

Ensure data is encrypted

Protect your business data by encrypting it. Data encryption is important as it involves converting data into a secure, unreadable format using cryptographic algorithms so even if the data does fall into the wrong hands, it cannot be used. You should ensure the data stored on mobile devices such as laptops, smartphones, and tablets are encrypted. For data transferred over public networks, such as hotel or airport Wi-Fi networks, ensure that data is encrypted by employing a virtual private network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Email encryption helps to protect personal information from hackers by only permitting certain users to access and read your emails.

Think before you click. Always be wary of emails, links or attachments from unknown or suspicious sources.

Important tip
#4

How does your business connect to the internet? Are your staff members safe when they are online?

Enabling a firewall on your systems and devices can enhance your systems' security. Think of firewalls as a protective barrier between your network and the vast world of the internet. Most modern operating systems come with this security feature, so it's usually just a matter of activating it.

Email and protection tools

Employ solutions to block spam emails, emails containing links to malicious websites, emails containing malicious attachments such as viruses, and phishing emails. Most email providers now include many features to ensure spam is blocked, enabling them across all your business devices will help prevent cyber-attacks on your business.

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

4. Turn on multi-factor authentication (MFA)

MFA typically works by requiring one or more verification factors, such entering a code received by phone in addition to a traditional user ID and password. For example, when you receive an authentication code by SMS text message after entering your password to log into an online account. MFA makes user accounts and computer systems much more secure, and it makes it harder for cyber-criminals to take over your account, by adding extra layers of protection.

MFA requires you to use a combination of two or more of the following factors to access your accounts:

- something you know (e.g. a PIN, password, or passphrase)
- something you have (e.g. a smartcard, physical token, authenticator app, SMS, or email) and
- something you are (e.g. a fingerprint, facial recognition, or iris scan)

MFA helps to defends against the majority of password-related cyber-attacks. For example, MFA protects against credential stuffing, where cyber-criminals use previously stolen passwords from one website and try to reuse them elsewhere to gain access to more accounts. It provides an extra layer of protection from cyber-criminals attempting to break in. Even if they break through one layer by guessing your password, they must break a second barrier to access your account.

MFA is a versatile tool that often goes by different names. You may come across it as two-factor authentication (2FA) or two-step verification. Understanding these different terms and their applications can help you make the most of MFA. For more detailed information, please refer to our previously published MFA guide.

NCSC-MFA-Guide

NCSC

Some further examples of MFA could include:

- SMS verification codes (2FA via SMS):
  - Users log in using their standard username and password
  - After entering credentials, a one-time verification code is sent to their mobile phone via SMS
  - Users must enter this code to complete the login process
- Biometric authentication (Fingerprint):
  - Scans and matches unique fingerprint patterns to authenticate identity
  - Convenient for users (no need to remember complex passwords or carry tokens)
  - Difficult for attackers to impersonate users due to fingerprint uniqueness

Rialtas na hÉireann
Government of Ireland

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Case study #2

The Importance of multi-factor authentication

Background: A mid-sized financial services company experienced a data breach when an employee fell for a phishing email, revealing their username and password. Without multi-factor authentication (MFA), the attacker gained full access to sensitive customer data.

Impact: Financial losses amount to €3.5 million in fines and recovery costs. There was a 20% loss of clients within six months, resulting in reputation damage. Additionally, the organisation faced regulatory penalties and increased scrutiny due to inadequate security measures.

Lessons learned

1. MFA is essential. Passwords alone are too vulnerable to phishing and other attacks.
2. Employee awareness matters. Regular training can help prevent credential theft.
3. Pro-active security pays-off. Implementing MFA and layered defences minimises risk and protects sensitive data.

5. Back-up your information

Data back-ups are copies of data that can be recovered later typically after a cyber-attack, accidental deletion, or another event that compromises the integrity or availability of data. Back-ups are a critical component of a recovery plan, making it easy to retrieve essential files and resume your business operations quickly after an incident. It's crucial to understand the difference between cloud storage and cloud back-ups, especially if you use a Security partner to provide these services. This knowledge will keep you informed and in control.

- Cloud storage stores data and files in an offsite location, which means your data is stored in a remote server maintained by the cloud service provider, making them accessible from any device or location.
- Cloud back-up creates a secure snapshot, a copy of your files and data at a particular point in time. This provides a way to restore them in case of a data disaster, as it acts as an uncorrupted copy.

Case study #3

Importance of cloud back-ups / Cloud hosting company

Background: A code hosting and software collaboration platform experienced a devastating cyber-attack. The attacker gained access to their cloud service control panel and demanded a ransom. When the company refused to pay, the attacker deleted most of their data and back-ups.

Impact: The attack led to the complete shutdown of the organisation. They lost customer data, project files, and their entire business infrastructure. This incident highlights the critical importance of having secure, off-site back-ups that are not accessible through the same credentials as the primary data.

Lessons Learned:

1. Regular back-ups: Ensure regular back-ups of all critical data.
2. Off-site storage: Store back-ups in a separate, secure location.
3. Access controls: Implement strict access controls and multi-factor authentication to protect back-ups.

Ways to back-up your data

Your business back-ups should be kept in a secure location, not directly connected to the business network. Such locations can be an external hard drive or a cloud-based back-up service. After gaining access to your network, or devices, threat actors may deliberately try to tamper with data back-ups to cause further damage. You can stop attackers from doing this by keeping your back-ups air-gapped (separated from the original data it is a snapshot of), which makes them physically isolated and unable to establish external connections. It's important to note that there are many approaches to data back-ups, giving you the flexibility to choose the one that best suits your business needs. A few of the more common ways to back up data are via:

Cloud-based storage

A good cloud storage service comes with a file management system for simplified access and can offer several advantages for your business.

- **Data security:** cloud storage keeps your data secure on remote servers, reducing the risk of data loss due to local server failures. Even if one server goes down, your data is backed up elsewhere.
- **24/7 access:** cloud storage liberates you from the constraints of physical storage, allowing you to access your data anytime, anywhere, from any device, be it a desktop, laptop, mobile phone, or tablet. This flexibility empowers you to work on-the-go without compromising data accessibility.
- **Unlimited capacity:** unlike physical hard drives, cloud storage provides virtually infinite space for your data.
- **Reduced IT costs:** cloud storage can significantly reduce the need for high-specification office computers; a simple internet connection is all you need. This cost-effective solution can provide relief, knowing you're making smart financial decisions for your business.
- **Enterprise-level security:** cloud providers implement robust security measures to protect your data.
- **Scalability:** easily add or remove storage space as your business.

Back-up services

Using a dedicated back-up service can significantly enhance data security for your business. These specialised services can be tailored for individual users, providing a comprehensive and secure data recovery solution in the event of a data breach or loss. Should you encounter a situation like a malware attack that renders your files inaccessible, restoring your data is a simple process that often just involves clicking a restore button. However, it's essential to understand that most of these back-up services require a monthly subscription fee, which can vary depending on the features and storage capacity you choose. This investment, while periodic, can prove invaluable in safeguarding your critical business information.

Best back-up strategy for your business

Be sure to ask the right questions before deciding on a back-up solution.

It's important to consider the following:

- Whether you store your back-up in a hard drive off-site, or in a cloud solution off-premises.
- Where the data is stored, e.g. is it in the EU?
- What physical access controls are in place?
- Who has access to the data?
- Is your sensitive customer data stored in the solution?

6. Create strong complex passwords

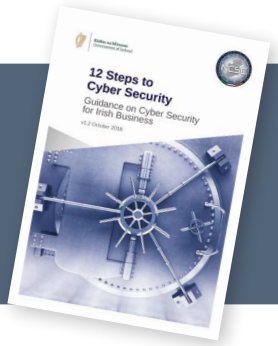
By using passphrases or strong passwords you can protect your devices and information from cyber-criminals. Many Irish SMEs face cyber-attacks because of poor password usage behaviour. For example, re-using the same password on multiple accounts. One of the most common mistakes is not changing the manufacturers' default passwords that smartphones, laptops, and other types of equipment are issued with. Change all default passwords before devices are distributed to staff. You can use both password managers and passphrases to create strong passwords.

Some suggestions for creating strong complex passwords

- Passwords should be at least 12 characters in length.
- Consider using passphrases; these are easier to remember and help in creating longer more complex passwords.
- Use random and unrelated words. The greater the complexity the better.
- Use words that do not appear in the dictionary.
- Use words from different languages.
- Use a combination of random numerical and special characters throughout the passphrase.
- Do not use common phrases or quotes.
- Do not use personal words like family names, pets, local football club or anything associated with your personal life.
- Do not use words or abbreviations associated with your organisation or industry.
- Consider using a password manager.
- Do not reuse passwords across multiple accounts.

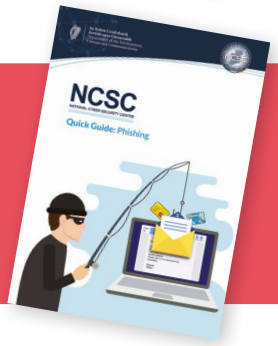
Links to NCSC guidance documents

Cyber security 12 steps

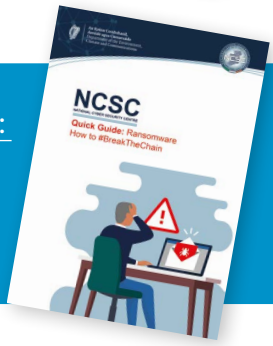


NCSC-MFA-Guide

NCSC - Quick Guide: Phishing



NCSC - Quick Guide: Ransomware



WFH Advisory

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Cyber security checklist

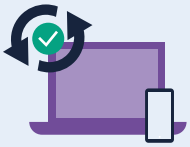
Best practices

- Identify your business objectives and document your inventory assets.

- Make sure to regularly update and patch applications and systems.

- Install anti-virus software on all devices to protect against malware and viruses.

- Enable automatic updates for all devices, including smartphones, tablets and laptops.



- Make sure to use a reliable source for software updates to ensure cyber safety.

- Enable multi-factor authentication.

- Back-up your information, and make sure to keep back-ups of your systems. Regularly update these backups to ensure they are current.

- Make sure to test your back-ups regularly.

- Make sure to enable firewalls on all devices and use VPN services to ensure secure communications.

- Ensure that your staff receives cyber security awareness training.

- Activate email protection to safeguard your information and enhance your security.

- Ensure that mobile phones and IT devices are encrypted, password-protected, and equipped with anti-virus software.

- Establish an asset management program to monitor your devices and data effectively.

- To protect your accounts, always use strong passwords or passphrases and refrain from re-using any of them.

- Make sure that encryption is implemented for all your data at rest (data stored) and in transit (data transport across a network such as the internet).

- Make sure to implement security controls for cloud services, such as multi-factor authentication (MFA).

- It is essential to understand the security responsibilities associated with utilising cloud services for your business.

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Glossary of cyber security terms

Anti-virus	Software designed to detect, stop, and remove viruses and other kinds of malicious software.
Anti-malware	Software that is designed to detect, stop, and remove malicious software (*malware*).
Authentication	Authentication is the process of confirming the correctness of the claimed identity.
Auditing	Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.
Asset management	Identifying and recording of a businesses physical assets, software, data, essential staff, and utilities.
Authenticator app	An authenticator app is a desktop or mobile application that secures accounts, apps, financial transactions, and more with time-based, one-time passwords (TOTPs)
Cloud computing	Utilisation of remote servers in the datacentre of a cloud provider to store, manage, and process your data instead of using local computer systems.
Cyber-awareness training	Designed to help users understand the role they play in combatting security breaches, teaches proper cyber-hygiene, security risks, and how to identify cyber-attacks.
Cloud storage	Stores data and files in an offsite location, which means your data is stored in a remote server maintained by the cloud service provider, making them accessible from any device or location.
Cloud back-up	Creates a secure snapshot of your files and data at a particular point in time. This provides a way to restore them in case of a data disaster, as it acts as an un-corrupted copy.
Cyber security	The protection of devices, services, and networks - and the information on them - from unauthorised access, theft, or damage.
Cyber-attack	An attempt to damage, disrupt or gain unauthorised access to computer systems, networks, or devices.
Cyber-threat	The threat of a cyber-attack to a user or organisation, and the unauthorised access, theft or damage that could result.
Credential stuffing	Is a cyber-attack method where attackers use stolen usernames and passwords.
Data owner	A data owner is the entity having responsibility and authority for the data.
Data in transit	Data as it is transferred from one location to another, either through a private network or the internet.

Digital signature	A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message has not changed since transmission.
ENISA	Is the EU agency dedicated to enhancing cyber security in Europe.
Encryption	Protection of information by making it unreadable by everyone except those with the key to decrypt it.
Firewall	Hardware or software used to prevent unauthorised access to or from a network.
Malware	Derived from 'malicious software', malware is any kind of software that can damage computer systems, networks, or devices. Includes viruses, ransomware and trojans.
Multi-factor authentication (MFA)	Is a security measure that protects individuals and business by requiring users to provide two or more authentication factors to access an application, account, or virtual private network (VPN).
NCSC	The National Cyber Security Centre, Ireland's national technical authority on cyber security.
Patching	Patching is the process of updating software to a different version.
Passphrases	A sequence of words or other characters longer than a normal password, used to verify the identity of a user, usually to gain access to an account, website, or system.
Phishing	The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website.
Ransomware	Is a type of malware that encrypts the victim's personal data until a ransom is paid.
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
Social engineering	A technique an attacker uses to manipulate people into carrying out specific actions, or divulging information.
Virtual private network (VPN)	A set of cryptographic technologies used to encrypt data as it travels over a network between two fixed endpoints.
Virus	A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program.

Contact details

National Cyber Security Centre,
Department of the Environment, Climate and Communications,
29-31 Adelaide Road, Dublin, D02 X285, Ireland.

info@ncsc.gov.ie

+353 1 6782333

https://twitter.com/ncsc_gov_ie

www.ncsc.gov.ie

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre