We are
Ireland online

Cybersecurity
A Guide for SMEs

2022 EDITION

Why cybersecurity matters to your business

SMEs have always had to contend with fraudsters and thieves.

Though these criminals' tactics have evolved with changing technologies, their overall goal remains the same. Only now, in addition to separating you from your hard-earned cash, today's cybercriminal is after your personal data, passwords and more.

We'll get the bad news out of the way first: Cybercrime is here to stay. In fact, you might say that it's a booming industry that's expanding every year as we continue to shop and conduct our business online.

Research by accounting firm Grant Thornton estimated the total losses of cybercrime to the Irish economy at €9.6 billion in 2020.

The purpose of this e-book is to help educate you on the basics of cybersecurity, as well as provide relatively simple – but effective – practices and tips for keeping your business safe from the most common cyberthreats you may encounter.

€9.6bn
Estimated loss to Irish economy from cybercrime

We are Ireland online

So, what exactly is cybersecurity?

Put simply – cybersecurity means protecting your computer systems, devices, programmes and networks from any type of cyberattack.

Why is it so important to secure my business?

It's incredibly easy to deprioritise and overlook cybersecurity – especially when you probably have more than enough day-to-day tasks on the go. However, not taking cybersecurity seriously could make your business a ready target.

Cybercriminals don't just target large, multinational corporations and governmental agencies. Typetec, a leading Irish IT and cybersecurity firm, discovered that **95% of more than 200 small businesses surveyed** experienced a cyberattack in the last 12 months.

Cybercriminals – like most criminals – often take the path of least resistance, and small businesses typically have lower levels of cybersecurity protection. That's not just a problem for you – but for your customers as well.

Customers expect their data – be it credit card information, home addresses, emails, shipping information, etc. - to be handled safely when shopping online. The findings of our **.IE Tipping Point Report 2022**, showed that most consumers are highly cybersecurity conscious. 75% are "very" or "somewhat concerned" about the security of their personal information online.

In the same report, we found that as many as 6 in 10 SMEs either don't take any precautions to protect sensitive customer data – or they don't know how. All the while, cybercriminals are becoming more sophisticated and continually working on ways to evade many conventional cyber defences.

Being the victim of cybercrime can ultimately mean significant losses in terms of both revenue and business-critical data. In addition, a serious cybersecurity breach can shatter customer confidence in your business or brand.

What are the benefits of cybersecurity to your business and customers?

Peace-of-mind

Good cybersecurity practices and tools help protect your business (and your employees) from falling victim to many of the most common threats, including phishing, ransomware attacks and more.

Customer data privacy and protection

Securing your business from cyber threats helps ensure you keep any sensitive customer data – including addresses, credit card information, transaction records etc. safely under cyber lock and key. Plus, when customers can clearly see that you're committed to protecting their information, they will be more likely to purchase from you.

Keep your online business up and running

Investing in cybersecurity will ensure that you protect your business and keep it online.

Avoid the devasting effects of a cyber attack

- Retain your customer's trust in your ability to keep their data safe.
- Avoid the impact on your business of lost revenue or having critical infrastructure knocked off-line.

Cybersecurity is not all doom and gloom

An important thing to note here is that we're not discussing cybersecurity or cyberthreats to terrify SMEs into staying offline for good. Quite the opposite, actually.

We want your online experience to be as positive and productive for your business as possible. Plus, the benefits to having a strong online presence can vastly outweigh the potential risks.

The fact of the matter is that most types of cyberattacks are avoidable. Burglars target physical assets with weak security. The same is true online, however, with a little education, smart security practices and the use of basic tools, such as a good quality antivirus software and password manager, you can keep your business (and customers) reasonably safe.

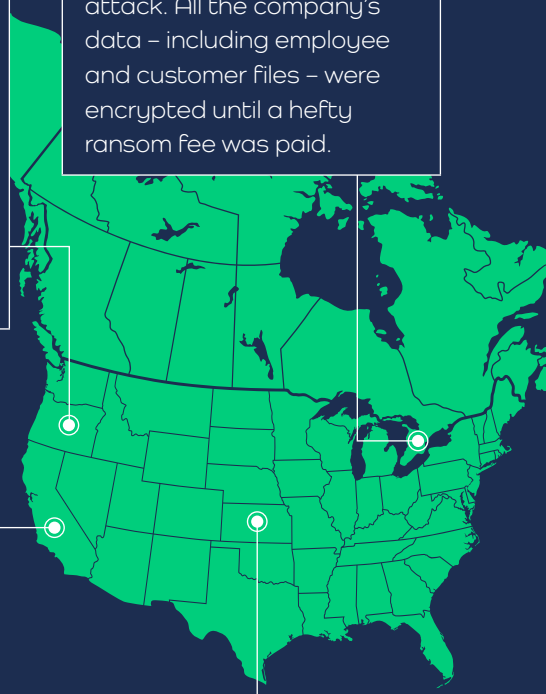
What could happen if you don't take cybersecurity seriously?

Ignoring cybersecurity as a small business owner could be one of the costliest mistakes you ever make. According to the **2021 Hiscox Cyber Readiness Report**, the median cost of a cyberattack to businesses with one to nine employees was $8,000 USD. For businesses with 10 – 49 employees, that figure jumped to $12,000 USD. Not insignificant sums by any stretch.

Here are a few real-world examples of what has happened to SMEs in the USA and Canada:

Sukhram Financial Services, a small, Toronto, Canada accounting firm, was hit by a devastating ransomware attack. All the company's data – including employee and customer files – were encrypted until a hefty ransom fee was paid.

Volunteer Voyages is a single-owner, small business based in Oregon, USA, that provides humanitarian volunteer opportunities to international travellers. After returning from a trip to Peru, the owner discovered that a cybercriminal had stolen their credit card number and ran up over $14,000 USD in fraudulent charges.



Efficient Services Escrow Group – This California-based escrow firm lost more than $1.5 million USD after hackers were able to breach their security using a form of malware. After breaking in, the hackers made several large wire transfers to bank accounts in Russia and China.

Green Ford Sales – Hackers took advantage of lax security measures and broke into this Kansas car dealership's online network. Once inside, the hackers proceeded to add nine non-existent employees to the company payroll system and make off with nearly $63,000 USD before the theft was noticed.

What exactly is a cyber threat?

Here, we outline several of the most prevalent cyber threats commonly faced by small and medium businesses:

- **Phishing:** The goal behind most phishing scams is to obtain sensitive data, like your credit card number, online banking login or access to your computer system. They most often take the form of fraudulent emails that appear to be from a legitimate source. An example of this that is fairly new and doing the rounds is "Browser in Browser attacks". You get taken to a browser within a browser to spoof a legitimate domain.
- **Smishing:** Similar to phishing, smishing is all about luring you into revealing sensitive information - but through your response to fraudulent text messages. Cybercriminals will often impersonate legitimate organisations, like a government agency, courier company or bank, then provide a link to a fake website. Once the link is clicked, victims are then prompted to enter personal information.
- **Vishing:** A.K.A. - "voice phishing." This is where cybercriminals call victims while pretending to be from a legitimate organisation - usually a bank or government agency - and demand personal information, banking details and more. A common vishing scam can involve a cybercriminal impersonating a Revenue service agent that then threatens his victim with imprisonment or stiff fines over fraudulent "unpaid taxes."
- **Malware:** This refers to any malicious or harmful software - such as spyware, viruses and other exploits - that can be used to covertly steal data from your computer system (spyware), install harmful software that can leave your system unusable (viruses) or block key parts of your network from being accessed (ransomware). Malware is commonly transmitted through fraudulent web links, or by downloading email attachments that contain viruses or other questionable software.
- **Trojan horse:** A type of malware disguised as a legitimate programme that then gets downloaded and installed onto a computer. Typically, Trojan horse malware will take the form of free-to-download software or an email attachment. Once installed, the Trojan horse releases its hidden payload to damage and steal your data, or disrupt your network.
- **Spyware:** Malware that is installed on a computer, often without the user's knowledge. Spyware can steal critical information, like banking information and login credentials, monitor your internet activity and even track your location. Often, this stolen data is forwarded to nefarious third parties.
- **Ransomware:** Ransomware can take on numerous forms, but the end goal is always the same: you must pay a fee or ransom in order to access your data and systems. A ransomware attack usually takes place after cybercriminals have already gained access to your system via malware or phishing. According to a recent global report by Hiscox Insurance, **approximately 6.5% of Irish firms have paid a ransom** following an attack.
- **Botnet:** A collection of internet-connected devices that have been compromised by malware and are being remotely controlled to send spam email, steal data and launch large-scale cyberattacks en masse.
- **Password hacking:** As the title implies, cybercriminals can use several sophisticated tools to guess a victim's password. Cybercriminals are successful when passwords are easily guessed - e.g. "123456" or contain easily discoverable personal details, e.g. a family member's name or birthday.

  A brute force attack is when cybercriminals enter as many passwords (or password combinations) as possible in the hope of guessing correctly. The graphic below shows how long it takes an experienced hacker to brute force passwords.

Time it takes a hacker to brute force your password in 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Source: Hive Systems

Keeping the .ie namespace safe

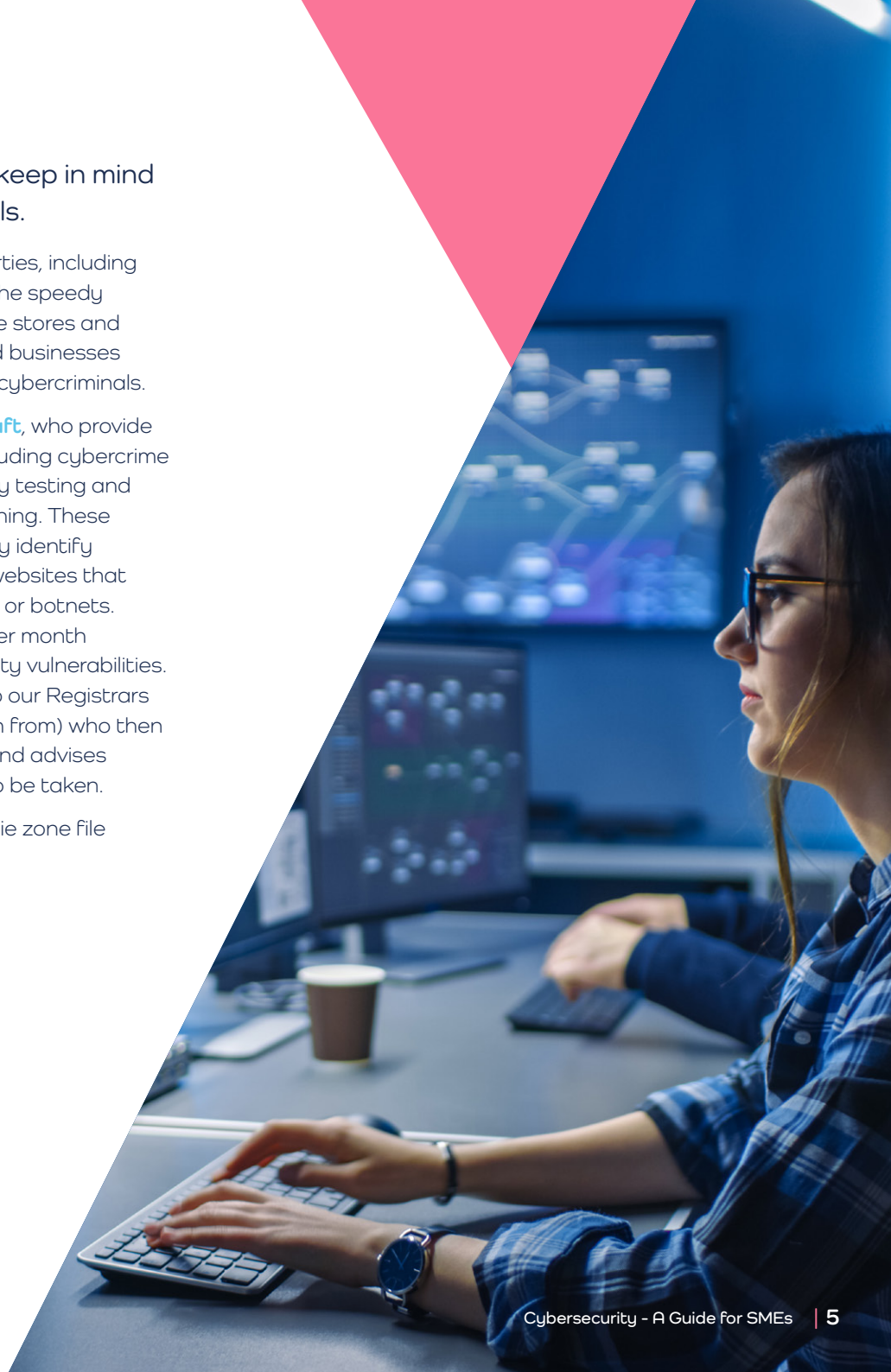
.ie domains and websites are ranked among the safest in the world. But keep in mind that nothing is completely secure from the most dedicated cybercriminals.

At .IE, protecting consumers, our customers and SMEs is important to us. We take a number of steps to keep the .ie domain as safe as possible and this ensures the level of security threat to .ie websites is much lower than .com.

Only individuals and businesses with a provable connection to Ireland can register a .ie domain, and all applications are manually reviewed to ensure that they meet this requirement. This process keeps Ireland's country domain largely free from registrations by hackers for their quick-moving scams and other illegal activities that unmanaged domains, such as .com, cannot control as easily.

Through our policies and protocols, we proactively tackle technical abuse in the .ie namespace and are dedicated to fighting malware and phishing.

- We work with several third parties, including regulatory bodies, to ensure the speedy removal of fake or illegal online stores and provide help to individuals and businesses that have been victimised by cybercriminals.
- We use the services of **Netcraft**, who provide internet security services, including cybercrime disruption, application security testing and automated vulnerability scanning. These services allow us to proactively identify online abuse issues, such as websites that are hosting malware, phishing or botnets. Approximately 50 websites per month are identified as having security vulnerabilities. We provide this information to our Registrars (who you bought your domain from) who then contacts the domain holder and advises them on what action needs to be taken.
- We do a security scan of the .ie zone file every month.



How can you keep your business safe from cyber threats?

Keep all your software up to date

Software updates are easy to ignore and put off indefinitely. But they can play a big role in ensuring your devices are secured. Yes, being repeatedly prompted to update your PC or mobile device can be irritating or intrusive, but these updates often contain the latest (and strongest) security patches. Old operating systems and software versions can be more easily exploited and accessed.

Think of it this way: Hardware and software manufacturers are constantly playing a game of cat and mouse with cybercriminals, with each trying to outwit the other. When cybercriminals find a gap or vulnerability to exploit, a company like Microsoft will swiftly develop security patches in response.

One of the simplest ways to keep your software up to date is to enable automatic updates through your device's options or settings menu. If staff's time and productivity are a concern, tell your device to perform critical updates out of hours.

Install (and turn on) antivirus tools

Modern antivirus software is designed to root out and proactively remove malware threats from your computer. That's why it's critical to have your antivirus enabled and resist the temptation to turn it off – even if periodic virus scans slow down your system.

Modern Windows and MacOS (Apple)-based systems include good, built-in antivirus software that is up to the task of handling the most common threats. Even better – this antivirus software can stay automatically up to date alongside your system.

If you'd rather bring in antivirus software of your own choosing, **Avast**, **Bitdefender**, **Sophos** and **Norton** are among the top-rated and most popular providers. Each comes with its own unique features. So, be sure to compare a couple of options before committing to a paid subscription. It's worth noting that the onus is on you to keep the antivirus software up to date, as recommended by the provider, which is an important step.

Whichever provider you choose, make sure it protects against viruses, ransomware, spyware, adware and malware.

Use strong, unique passwords

Password protection provider Nordpass recently revealed that the **most-likely-to-be hacked password** (in a study of 50 countries) was "123456." The same research showed people were also highly likely to use their own names as passwords. Even more distressing? About 84.5% of all passwords used globally can be cracked by professional hackers in under one second.

So, what qualifies as a strong password by today's standards?

A strong password should be at least ten characters in length and include a combination of upper and lower-case letters, numbers and symbols.

Avoid using any easily discoverable personal details – including names of family members, pets, your hometown or birthdays. As convenient as it might be, you should also avoid reusing the same password for multiple accounts.

For added security, Google's Chrome or Apple's Safari search engines can generate unique, impossible-to-guess passwords – made up of random numbers, symbols and letters – that will fill in automatically for you.

Lastpass and **1password** are two great password management tools that allow you to create a strong, uncrackable "master password" that the software then uses to securely log you into your accounts with one click.

Consider two-factor authentication for all your accounts

Two-factor authentication (2FA) is one of the most simple and effective ways to protect yourself online.

The biggest benefit? 2FA adds an additional barrier for cyber criminals that may have been able to get access to your primary password or credentials.

In most two-factor authentication systems, a separate, randomly generated SMS code is sent to your phone (or device of your choosing). Unless cybercriminals can access that code on your phone, your accounts stay secured against any attempted breaches. Or even better would be to use an Authenticator app, which generates a one-time code that you use to confirm that it's you logging into a website or service.

Your Google account, or Apple ID are prime examples of platforms that give you the option to enable two-factor authentication. A lot of people tend to use their Google account to sign up to other third party services so it is very important to enable two-factor authentication on it.

Protect your website and build customer trust with a security certificate

If you manage a website which processes customer information, be sure to protect it with a security certificate. Customers need to feel safe and secure when purchasing online and will look for websites whose address begins with a https (not http) and displays a lock symbol. This indicates that a security certificate is installed.

The majority of **.ie websites** have a security certificate, which ensures that consumers are protected from having their personal details stolen by cyber-criminals during an online transaction.

If you have a .ie domain, learn more about additional protections such as **DNSSEC** (this adds an additional layer of cryptographic security to a domain) and **Registry Lock** (this protects a domain from malicious or accidental changes).

Regularly backup and encrypt your data

Any essential business information, e.g. financials, customer data – should be regularly backed up to the cloud, or to an external drive in a different location. Fortunately, there are several strong, cloud and software-based solutions – like **Rewind**, **Acronis** and **iDrive** – that cater specifically to SMEs and can be easily set up and managed without needing a dedicated IT partner.

An important security measure is to encrypt your backups, as that will provide further protection for your data beyond a simple password. Many data backup solutions already offer built-in encryption tools, or the option to store encrypted backups.

Two-factor authentication in day-to-day life

Two-factor authentication-style security measures are rapidly becoming commonplace in other aspects of our daily lives – including online banking and shopping.

For example:

- Bank of Ireland requires your unique 8-digit identifier, three numbers from your passcode and date of birth. To make any transactions, you need to provide three random numbers from your passcode, plus the transaction must be authorised from your phone via the Bank of Ireland app.
- Ryanair has introduced an "online verification process" for booking flights that involves taking a photo of yourself with your passport or National Identity Card.

Google Authenticator and **Authy** are two excellent two-factor authentication apps to explore for your business. Another option to consider is **Yubikey**, which is a USB device "biometric authenticator" which uses your fingerprint to authenticate you.

Educate your employees on the most common cybersecurity risks

Security tools and passwords aside, one of your single best defences against cybercrime is security awareness and education. Enrol yourself and your employees in an **accredited cybersecurity training course** from a reputable organisation.

Investing in quality cybersecurity training can provide several benefits, including:

- **Teaching employees how to spot suspicious activity,** be it phishing emails, texts or strange pop-ups or programmes appearing on their devices.
- **Reinforcing confidentiality and security** by demonstrating the need for stronger passwords, and of being more mindful of where business critical data is stored.
- **Driving accountability** by framing cybersecurity threats and good practices in understandable, relatable terms.

Most of all, ongoing training and raising awareness can help make cybersecurity part of your business's culture and can go a long way towards making your employees far more confident and vigilant when going about their day-to-day work.

Come up with a cybersecurity incident response plan

Have a plan in place that spells out what your business is doing to prepare for, respond to and recover from cyberattacks. After all, your end goal is to get back up and running as quickly as possible!

A good incident response plan will help limit your downtime, potential disruptions to your business and customers, and data loss. Write out your plan and start by specifying who will be involved in your cyberattack response. What are their responsibilities? What resources or tools are available?

Set out detailed instructions for how you and your employees will deal with a cyberattack - e.g. identifying and reviewing the source of the attack, changing passwords/credentials, updating and patching systems and backing up data. The headings below offer a useful structure for these instructions:

Leave time for learning. What would you and your employees do differently? Where might you have made a mistake?

Stay alert against social engineering scams

The easiest way to describe social engineering is that it's a form of psychological manipulation – often involving persuasion – with the aim of tricking you into giving away sensitive information. Cybercriminals will target things like your Personal Public Service number (PPSN), passwords to your email or social media accounts and online banking information.

One of the most common forms of social engineering is phishing. In a typical phishing scenario, you may get an email that appears to be legitimate and contains a file to view, or a link to click. Often, these emails are accompanied by urgent-sounding, or sometimes threatening calls-to-action. For example, "Your account has been compromised! Click here to recover your password," or "Your package has been held at customs. Pay duty fees now."

How can you avoid phishing? Never assume an email is what it says it is until you know otherwise. For instance, **the Revenue will never send you emails** threatening fines or imprisonment over unpaid taxes. Also be wary of senders that you don't recognise, or with suspicious looking email addresses and domain names.

Secure for the future

As we mentioned earlier, cyberattacks and cyberthreats are becoming more prevalent. At the same time, an ever-growing number of your customers are conducting their business almost exclusively online.

Making cybersecurity a key priority will help keep you competitive, productive and far less vulnerable to opportunistic cybercriminals looking for an easy target.

Unlock the power of the internet with a trusted Irish .ie online identity

It's trusted

Every **.ie** applicant's identity is checked and validated at the point of registration. Consumers will have confidence in your business as **.ie** is a well-established and trusted domain. 77% of Irish consumers prefer a **.ie** website when buying online, instead of a .com.[1]

It's uniquely Irish

The official Internet country code for Ireland is **.ie** and is the only online address that is Irish. A **.ie** tells the global community that you are Irish and tells the Irish community that you are local. You can even register an Irish language name if required, fadas and all.

It's more likely to be available

There is a wider choice of available **.ie** domain names compared to .com, as significantly more of those names are already registered.

It lets your customers find you online

.ie addresses rank higher than .com addresses on Irish based search engines like Google.ie. Irish consumers are more likely to click on local website addresses.

It's the preferred online address for business in Ireland

91% of Irish consumers associate **.ie** websites with Irish businesses over other websites like .com.[1] The **.ie** domain accounts for the majority of hosted domains in Ireland.[2]

It protects your brand

Securing your **.ie** online address strengthens your brand and protects your online identity. All **.ie** domains are registered on a first-come, first-served basis.

[1] .IE Consumer Trust 2020

[2] HosterStats

PUBLIC DOCUMENT

.IE
2 Harbour Square
Dun Laoghaire
Co Dublin
A96 D6R0

Tel +353 (0)1 236 5400
Email marketing@weare.ie
Twitter @dot_IE

www.weare.ie

We are Ireland online