Cybersecurity Tips

DID YOU KNOW?

- **Human error accounts for 95% of all cybersecurity breaches**
- **77% of organisations do not have a cybersecurity plan**

HOW DO I APPROACH CYBERSECURITY AS A BUSINESS, SCHOOL, OR INDIVIDUAL?

As cyber-attacks and their consequences grow, the imperative for cybersecurity awareness has become increasingly evident to businesses, schools, and individuals. Attackers use a variety of vulnerabilities and phishing attacks to compromise the security of your networks and devices. To approach this threat effectively and protect your networks, it is vital to become familiar with the cyber essentials of your business and personal accounts, such as email, social media, and more so that you can better secure your information and identity online! October is Cyber Security Month #CyberSecMonth and here are some simple tips to help keep you safe online.

IT ie

Unit 35, Finglas Business Centre, Jamestown Road, Finglas Dublin 11, D11 EP86

hello@it.ie

(01) 8424114

SIMPLE CYBER TIPS FROM IT.IE

Be aware of risk. Be aware of possible risks such as malware viruses, ransomware, and phishing. It's also important for everyone in your organisation to be aware of the possible risk and threats that could occur should your systems become affected by any of these threats. To help you to evaluate your employee or human risk we are currently offering businesses a Free Human Risk assessment, whereby we scan your employee email addresses for dark web breaches and run a simulated phishing campaign on your behalf. This allows us to then provide you with a Free Human Risk Report. To get a better idea of what's involved please view this Sample Risk Report.

Train your employees. Employees and emails are the foremost cause of data breaches for small businesses because they are a direct path into your system. Train and inform your employees and on basic Internet practices. This will go a long way in preventing cyber-attacks. Check out our Cyber Awareness Training page to find out how you can help build a strong cyber awareness within your business.

Keep antivirus software updated. Make sure all your computers, Internet-connected devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.

Secure your networks. Secure your network by using a firewall and encrypting information. This is also useful for the individual. If you have a Wi-Fi network, secure it by hiding the network, by setting up a wireless access point or router so it doesn't broadcast the SSID service set identifier and network name. Protect the router and put the password on.

Use strong passwords. Creating strong passwords is an easy win in terms of improvements to your cyber security. Always use different passwords for different accounts and make it a requirement that strong passwords include one uppercase letter, one lowercase letter, at least one number and 10 or more characters. Use trusted password managers to generate and remember different, complex passwords for each of your accounts.

Backup your data. Routinely back up data on all computers and digital devices. The only sure-fire way to guarantee that you won't lose vital data is to have it backed up in the cloud.

Control physical access. Control access to backup data as well as school or business computers by unauthorised individuals. Make sure to use separate user accounts for each employee or student and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel. If you have a lot of mobile devices, then it is recommended that you use a Mobile Device Management service. Mobile Device Management (MDM) is the process of enhancing corporate data security by monitoring, managing, and securing mobile devices such as laptops, smartphones and tablets that are used in education and business settings.

Play hard to get with strangers. Links in emails and online posts are often the way cybercriminals compromise your computer. If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email. Be cautious of generic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.

Think before you act. Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organisation but still looks "phishy," reach out to them external to the email. What we mean by this is, don't click on a "contact us" link in the email or call back a number contained within the email. It is very easy to verify contact information with a simple internet search.

Protect your personal information. If people contacting you have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols. Over 3.2 billion email credentials have also been released online and chances are that at least one of your email addresses has been compromised. "Have I been Pawned" is a great, free online service that allows you to check if any of your business or personal accounts have been compromised.

• Be wary of hyperlinks. Avoid clicking on hyperlinks in emails and hover over links to verify authenticity. Also ensure that URLs begin with "https." The "s" indicates encryption is enabled to protect users' information. If you don't trust 100%, **Don 't Click**

Double your login protection. Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read our Multi-Factor authentication guide.

Contact Us: IT.ie Unit 35, Finglas Business Centre,Jamestown Road, Finglas Dublin 11, D11 EP86
Email hello@it.ie | Call (01)8424114