CODEINMOTION

PROTECT YOUR DATA. PROTECT YOUR REPUTATION.

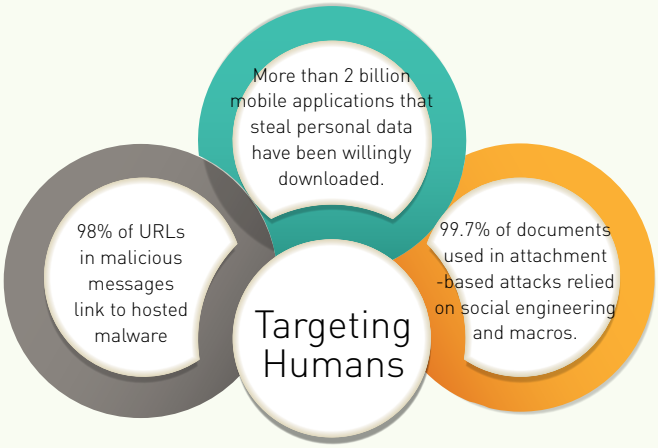
Cybersecurity: Top Tips

Filter out the noise. Focus on what's important.

Prepared for: Kildare Chamber of Commerce
Prepared by: Sam Glynn, Code In Motion Ltd

April 2017, Version 1.0

10 FUNDAMENTAL SECURITY MEASURES – PROTECTING YOU PERSONALLY AND IN BUSINESS



1. Don't be fooled

Be wary and skeptical of emails, websites and phone calls. Think before you click. Go to the website directly – Do not click the link. Hover over hyperlinks in emails – most of the time, the real URL behind the hyperlink will then appear on screen. Verify that the start of the URL is going to bring you to the site that you expect. Verify the content of the email directly with the sender (using a phone number you have on file for them).

2. Backups

Backup your phone and your computer. If you are a victim of ransomware, having a recent backup of your data will ensure you don't lose your data and don't need to pay the ransom. External USB drives are cheap. Just make sure the data is encrypted or the device is stored in a secure location. Pro tip: DropBox etc are not a good backup location, especially if they are always visible and accessible in Windows Explorer. Ransomware will encrypt these files too.

3. Account Security

Passwords need to be complex, frequently changed, not reused or shared. Use password management software to help you – e.g. LastPass, 1Pass. Set up two factor authentication wherever possible (where you receive an SMS message with a security code every time you log in).

"€630 million is the estimated annual cost of cybercrime to the Irish economy"

4. Device Security

a) On your PC, use a standard user account rather than an administrator account. Why? 94% of vulnerabilities patched in Windows in 2016 would not have been a problem for people using standard accounts!

b) Set up a PIN / lock screen on all of your devices.

c) Encrypt wherever possible.

5. Patch Regularly

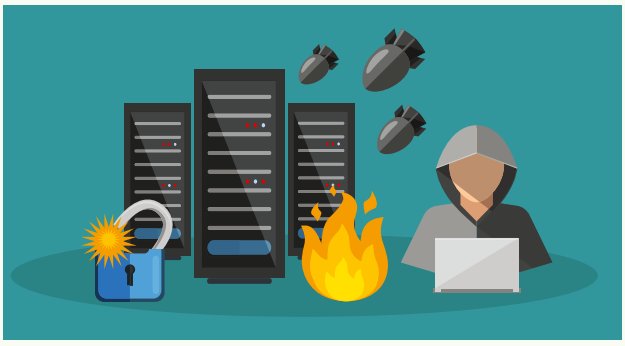
Yes, this advice is old and boring. But it helps! Make sure you download and install software patches frequently. Patches usually address vulnerabilities in software – If you don't patch, you have the vulnerability. This applies to every operating system and piece of software on your phone or PC. For example, Android, Windows, MS Office, Adobe, Flash, Java are frequent targets.

6. Secure with Multiple Layers

Ensure you are running layers of security software on your devices. On Windows, we recommend Windows Firewall, Windows Defender, plus anti-virus software (e.g. Kaspersky, Avast), as well as anti-malware software (e.g. MalwareBytes)

7. Access the Internet Securely

Using WiFi hotspots is convenient but seldom secure. If possible, use your phone's data allowance to access the web while away from the office or home. While a 3G or 4G network is not inherently secure, hacking the network involves expensive equipment that is beyond the budget or interest of the average hacker. If this is not an option, consider using VPN software on your device to encrypt your internet connection. It will secure your data away from anyone else on the WiFi network.



8. Perform Sensitive Business on a Secure Device

Only use a well-managed and fully-patched device for sensitive matters (e.g. online banking). If possible, use different devices for general web access, online gaming, video streaming etc. Unfortunately, cyber criminals are also now targeting children as they may be more likely to click on anything that pops up – So try to keep their activity separate too. And needless to say, monitor their activity for their own safety!

9. Discuss Sensitive Business over a Secure Channel

Email is not secure. It is easy for an unauthorized party to read and change your emails. Password-protected MS Office documents are slightly better but still easily cracked. Putting files into an encrypted zip file (using WinZip or 7-Zip) is secure but not always convenient. But if the matter is sensitive, secure is better than convenient.

10. USB keys – Treat them like your Toothbrush

Only use a USB key if it's yours, you know where it's been and you know it's clean!

TOP 10 CHECKLIST FOR MANAGEMENT

1. Enforce the Individual's Top 10

Everything mentioned in the earlier section should be enforced by the business.

2. Staff training

Regular sessions that seek to engage staff in the subject matter - not bore them to tears. Also, consider running simulated phishing attempts to assess staff weaknesses and address gaps.

3. Identify your important data

Every organization has important data e.g. confidential customer information, HR/Payroll information, financial records. For this important data, segregate it from other data. Secure it when stored or in motion. Limit access to it.

4. Backups

Ensure your data is backed up, both to local backup devices and remote locations (e.g. secure cloud backup services). A backup is useless if it does not work.

Ensure there is a procedure in place to regularly test the backup.

5. Secure in Motion and at Rest

Review how your important data is brought into the organization, what happens to it while it is in the organization, and where it leaves the organization. Make sure every point in the flow is secure.

6. Security from the outside

Your organization needs to be protected by a range of technology: Web filters, email filters, firewalls, monitored security services. Ensure there are security policies deployed to all PCs and laptops, applying controls on staff and devices in line with your business needs and risk appetite (e.g. locking down USB slots; auto-locking PCs after a period of inactivity; enforcement of patching / updating cycles; removal of administrator rights from staff) Don't forget your website and other systems that you have hosted 'in the cloud' (aka 'someone else's computer'). These also need to be secured and monitored.

> "€137,500 is the average cost of a security incident in Ireland"

7. BCP / Incident Response Plans

A breach will happen. Everyone needs to know their role in responding. Only working this out after a breach is not fun.

8. Policies

You need to ensure everyone is clear about what is appropriate behaviour in the business: Policies covering web use, email use, social media use, personal device use etc. all need to be clearly documented and

understood. There should also be clear statements of the sanctions of not complying.

9. Business Procedures

Given the growing risks of CEO Fraud / Payment Redirection, every organization needs to have a clear and locked-down procedure for processing payment requests and, even more importantly, setting up supplier payment details. These processes can not provide a backdoor / quick process for CEO's and other important people. You may even consider rewards for those who stick to the process despite pressure from superiors.

10. Insure the risk

Right now, for the risk and impact of a cyber attack, the cover is cheap.

Not only does it cover you for obvious financial losses, it may also provide you with access to technical / compliance / legal / communications experts in the event of a breach.

BONUS POINT: Security from the inside: - The easiest way to break a lock is with the key. While our focus is on cyber security and the threat from outside, you also need to be wary of the threats from insiders and trusted 3rd parties.

For example, there is a significant likelihood that your IT provider has full access to all of your data. Would you know if they accessed it / copied it / deleted it?

"Amateurs hack systems, professionals hack people." - Bruce Schneier, 2015.

TOP 5 BOARD CONSIDERATIONS

1. Stop burying your head in the sand & get informed

Cyber security is not management's problem. Cyber security is not IT's problem. It's your problem.

The Gardai have told you. The Data Protection Commissioner has told you. The Central Bank has told you. Data subjects waving the GDP Regulations will tell you, in court.

Follow advice from industry bodies, Kildare Chamber, and anyone who is trying to help.

Read the Central Bank's guidance, especially if you are a regulated entity or provide services to one. Read about GDPR and data protection.

2. Provide budget, drive the agenda and lead by example

Reducing the risk of cyber attack is a pain. It interrupts existing ways of doing business. It adds complexity. Unfortunately, this is required. It is less disruptive than a security breach. It reduces risk and cost. You need to champion this from the top and ensure it does not drop off the agenda due to management's 'real' work.

3. Manage the risk

Cyber crime is another risk to the organization. Like all business risks, ensure this risk is understood & documented, and being managed & mitigated.

4. Ask the right questions until you get the right answers

Ask the right questions of the management team and 3rd parties, get comprehensive answers that you can trust. Or ask again.

5. Seek outside help

This is not a tick-the-box exercise. Seek outside help to do it better and do it quicker. The organisation's data and your professional reputation are at risk.

ACKNOWLEDGEMENTS

County Kildare Chamber recognises the contribution of those involved in the preparation and production of this publication.

Code In Motion, Maynooth University, Chambers Ireland, Dooley Insurance Group, Price Waterhouse Coopers, AIB.

This guide is a Chamber best practise for business.