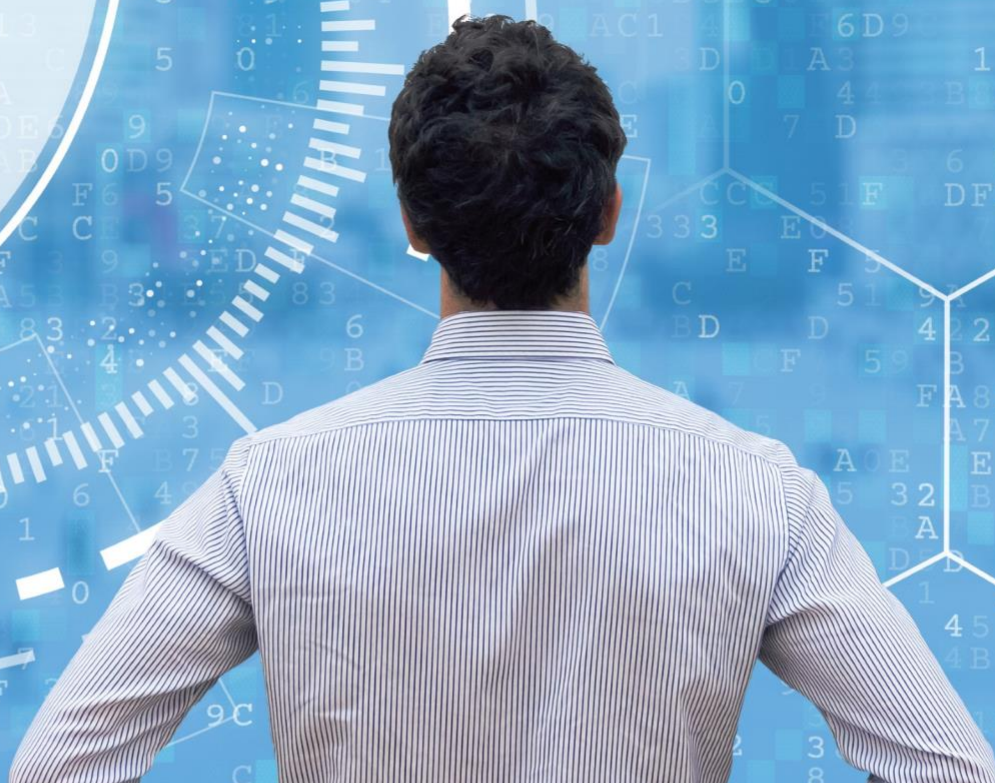




FORTIFY
Institute

CYBERSECURITY

What SMEs Need to Know



CYBER TOOLKIT

Jan Carroll - Fortify Institute - jan@fortify.ie

CONTENTS

Where to start?



Hit by Ransomware!



Email, Text & Call Scams Cyber



Awareness Training Cyber Incident



Response Plan



Has Your Email been in a Breach?



Cyber Awareness Videos Further



Resources

WHERE TO START?

ENISA (European Union Agency for Cybersecurity)



This guide provides SMEs with practical 12 high level steps on how to better secure their systems and their businesses.

Link

<https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>

Further resource

Gov of Ireland – 12 Steps to Cyber Security over 12 months

Link

https://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf

HIT BY RANSOMWARE?

If your organisation has been infected with malware, these steps may help limit the impact:

- 1.Immediately disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based.
- 2.In a very serious case, consider whether turning off your Wi-Fi, disabling any core network connections (including switches), and disconnecting from the internet might be necessary.
- 3.Reset credentials including passwords (especially for administrator and other system accounts) - but verify that you are not locking yourself out of systems that are needed for recovery.
- 4.Safely wipe the infected devices and reinstall the OS.
- 5.Before you restore from a backup, verify that it is free from any malware. You should only restore from a backup if you are very confident that the backup and the device you're connecting it to are clean.
- 6.Connect devices to a clean network in order to download, install and update the OS and all other software.
- 7.Install, update, and run antivirus software.
- 8.Reconnect to your network.
- 9.Monitor network traffic and run antivirus scans to identify if any infection remains.

Incident Reporting:

Contact the National Cyber Security Centre and An Garda Siochana to report the incident – guidance here:

<https://www.ncsc.gov.ie/incidentreporting/>



Further Resources:

[https://www.ncsc.gov.ie/pdfs/NCSC Quick Guide Ransomware.pdf](https://www.ncsc.gov.ie/pdfs/NCSC%20Quick%20Guide%20Ransomware.pdf)

<https://www.nomoreransom.org/en/index.html>



PHISHING - SCAMS, EMAILS, TEXTS & PHONECALLS

Email:

Be wary of any requests to update or verify account information.

Be wary of any sense of urgency.

Trust your gut!

Call the person if you're unsure.

Do the test below



Text:

Don't install an app from a text link. What if you do?

<https://cyberawarenessireland.com/flubot-infographic>

Calls:

Avoid unknown or blocked numbers.

If you answer, they ask for sensitive information or know some of your information, call them back from a number you sourced.

Trust your gut.

Resource: <https://www.caici.eu/hse-cyber-attack-9-steps-to-take>



[Can you spot when you're being phished?](#)

This is an excellent resource from Google

CYBER AWARENESS TRAINING

Resources



Why Awareness training is vital. <https://www.caici.eu/what-we-know-so-far>



Free, quality training and certification
<https://cyberreadinessinstitute.org/>



Introduction to Cybersecurity

Free course from CISCO Skills for All

<https://skillsforall.com/course/introduction-to-cybersecurity>

Recent article detailing cybersecurity training in Ireland.



Cybersecurity Training and Education in Ireland - Where do I start?

There is a global shortage of cybersecurity professionals and with data breaches and ransomware attacks on the rise, the industry is crying out for quality individuals to fill the roles. In...

<https://www.fortifyinstitute.com/blog/cybersecurity-training>



CYBER INCIDENT RESPONSE PLAN

Excellent resources recently published by CyberScotland. Can be easily adapted.

Developing an incident response plan is a critical step towards preparing a robust and effective incident management and technical response capability.

Good incident management will help reduce the financial and operational impact on your business.

Cyber Incident Response Plan Template



Developing An Incident Response Plan

Developing an incident response plan is a critical step towards preparing a robust...

 Cyber Scotland

<https://www.cyberscotland.com/developing-an-incident-response-plan/>

The documents will compliment any existing Incident Response Plan or assist you in creating one.



HAS YOUR EMAIL BEEN IN A BREACH?

Go to this link:

<https://haveibeenpwned.com/>

- Check your emails to see if they have appeared in a breach.
It's a safe site.
- If your email has been included in a breach – change your password.
- Sign up for alerts so if your email appears in future you will be notified.
- Register your domain, so any if any emails with your domain appear in future breaches, you will be notified.



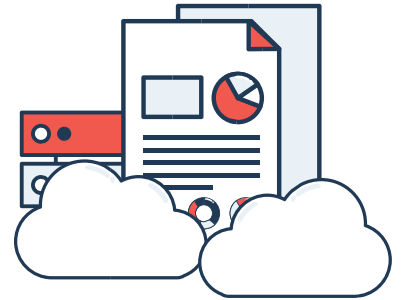
CYBER AWARENESS VIDEOS

Resources

- Social Engineering
<https://www.youtube.com/watch?v=BEHl2IAuWck>
- Ransomware
https://www.youtube.com/watch?v=j0EZpH_elsY
- Passwords – This one is funny!
https://www.youtube.com/watch?v=z_HmDP3IKMI



FURTHER RESOURCES



Resources

- Excellent awareness resources and infographics
<https://www.caici.eu/>
- Ireland's National Cyber Security Centre
<https://www.ncsc.gov.ie/>
- UK National Cyber Security Centre <https://www.ncsc.gov.uk/>
- Ireland's Cybersecurity cluster.
<https://cyberireland.ie/>
- Cyber Incident Response Plan Template
<https://www.cyberscotland.com/developing-an-incidentresponse-plan/>