

Cyber Resilience in a world of increasing Cyber Risk

www.gov.scot/cyberresilience



Keith McDevitt
Cyber Resilience Integrator
Scottish Government

The Internet – The greatest enabler of our time

Just because the technology works doesn't mean its safe by design or the user is sufficiently knowledgeable to use it safely



Over time we made rules for manufactures and users to make vehicles and roads safer.

Digital opportunities bring Risk

Remarks by the President on securing our nations cyber infrastructure

It's the great irony of our Information Age, the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And the paradox – seen and unseen – is something that we experience every day.

29 May 2009



With new opportunities come new threats – growing in capability and sophistication

WannaCry ransomware 'from North Korea' say UK and US



Scottish Government hit by two ransomware cyber attacks



Ransomware attacks encrypt sensitive files before demanding money from the user for their release (Photo: Getty)



Cyber attack on Scottish Parliament 'could last many days'



No Rest after Wannacry

- Not Petya was different;
- It masked as Ransomware;
- It used the same stolen weapons grade exploit as Wannacry;
- Its target appears to have been the Ukraine;
- **Its intention was not to extort but to destroy.**
- **The unintended consequences was that it could have infected, any business, any size, anywhere, corner shop to multi national, and this is the risk we now face, but are we prepared for it?**

Security

28

NotPetya ransomware attack cost us \$300m – shipping giant Maersk

IT crippled so badly firm relied on WhatsApp

By Iain Thomson in San Francisco 16 Aug 2017 at 22:15

SHARE ▼



The world's largest container shipping biz has revealed the losses it suffered after getting hit by the NotPetya ransomware outbreak, and the results aren't pretty.

The malware surfaced in Ukraine in June after being spread by a malicious update to MeDoc, the country's most popular accounting software. Maersk picked up an infection that hooked into its global network and shut down the shipping company, forcing it to halt operations at 76 port terminals around the world.

You are important and worth protecting

BBC Sign in News Sport Weather iPlayer TV Radi

NEWS

Home UK World Business Politics Tech Science Health Family & Education

Scotland Scotland Politics Scotland Business Edinburgh, Fife & East Glasgow & West

Self-catering worth £300m to Scots economy

© 21 April 2017 | Scotland business

f t v Share



Get the Basics Right and prevent 80% of the threat



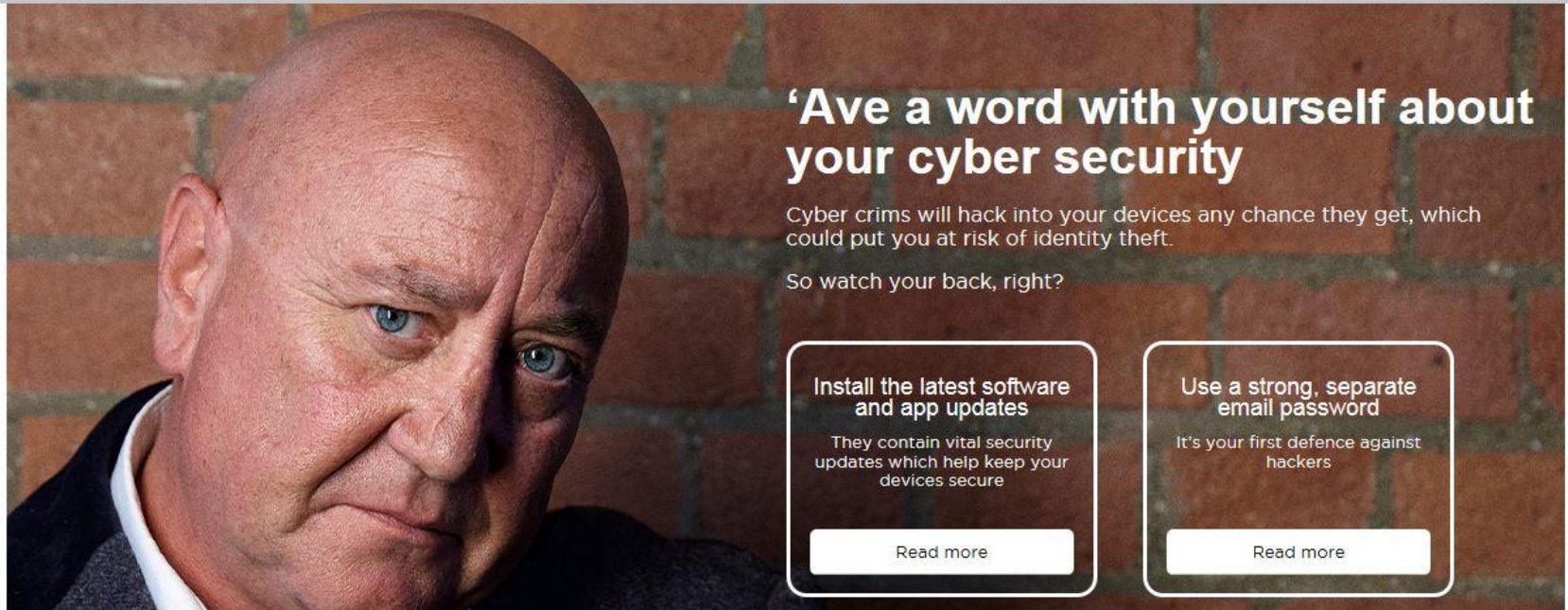
CYBER AWARE 



Protect your device

Protect your data

Protect your business



'Ave a word with yourself about your cyber security

Cyber crims will hack into your devices any chance they get, which could put you at risk of identity theft.

So watch your back, right?

Install the latest software and app updates

They contain vital security updates which help keep your devices secure

[Read more](#)

Use a strong, separate email password

It's your first defence against hackers

[Read more](#)



National Cyber
Security Centre
a part of GCHQ

Search



Guidance

Threats

Incident Management

Marketplace

Education & Research

Insight

Press & Media

Topics ▼

Published guidance

Infographics

NCSC glossary

[Home](#) > [Guidance](#) > [Published guidance](#)

Guidance

Cyber Security: Small Business Guide

Created: 11 Oct 2017

Updated: 11 Oct 2017



Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.



Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.



Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).



Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.



Make sure all laptops, MACs and PCs use **encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.



Use **two factor authentication (2FA)** for important websites like banking and email, if you're given the option.



Avoid using **predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).



If you **forget your password** (or you think somebody else knows it), tell your IT department as soon as you can.



Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.



Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.



Consider using a **password manager**, but only for your less important websites and accounts where there would be no real permanent damage if the password was stolen.



<https://howsecureismypassword.net/>

HOW SECURE IS MY PASSWORD?

Please let me in

It would take a computer about

23 TRILLION YEARS

to crack your password

Dashlane can help you remember all of your secure passwords - and it's free!

[Tweet Your Result](#)

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home)

need even more protection than 'desktop' equipment.



Switch on **PIN/password protection/fingerprint recognition** for mobile devices.



Configure devices so that when lost or stolen they can be **tracked, remotely wiped** or **remotely locked**.



Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.



When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.



Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.



Use antivirus software on **all** computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.



Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.



Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.



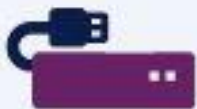
Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.



Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.



Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.



Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.



With Great Power Comes Great Responsibility – go use it wisely