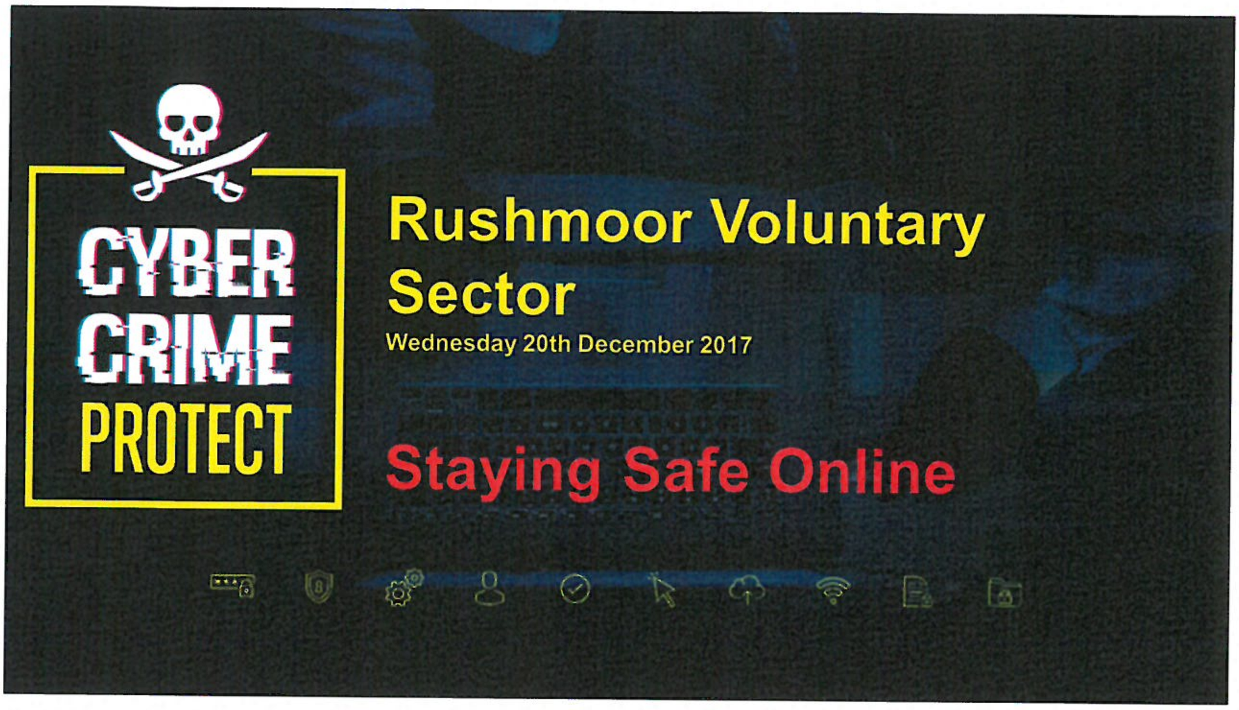
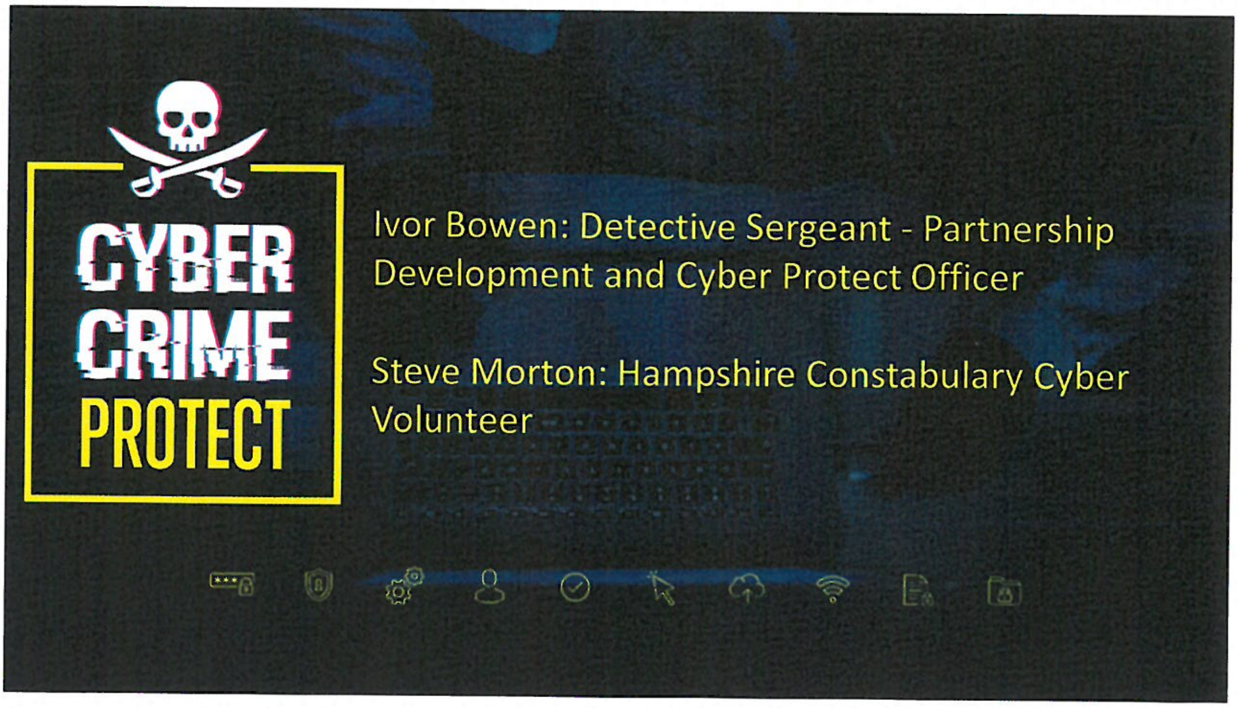


CYBER CRIME PROTECT

Rushmoor Voluntary Sector

Wednesday 20th December 2017

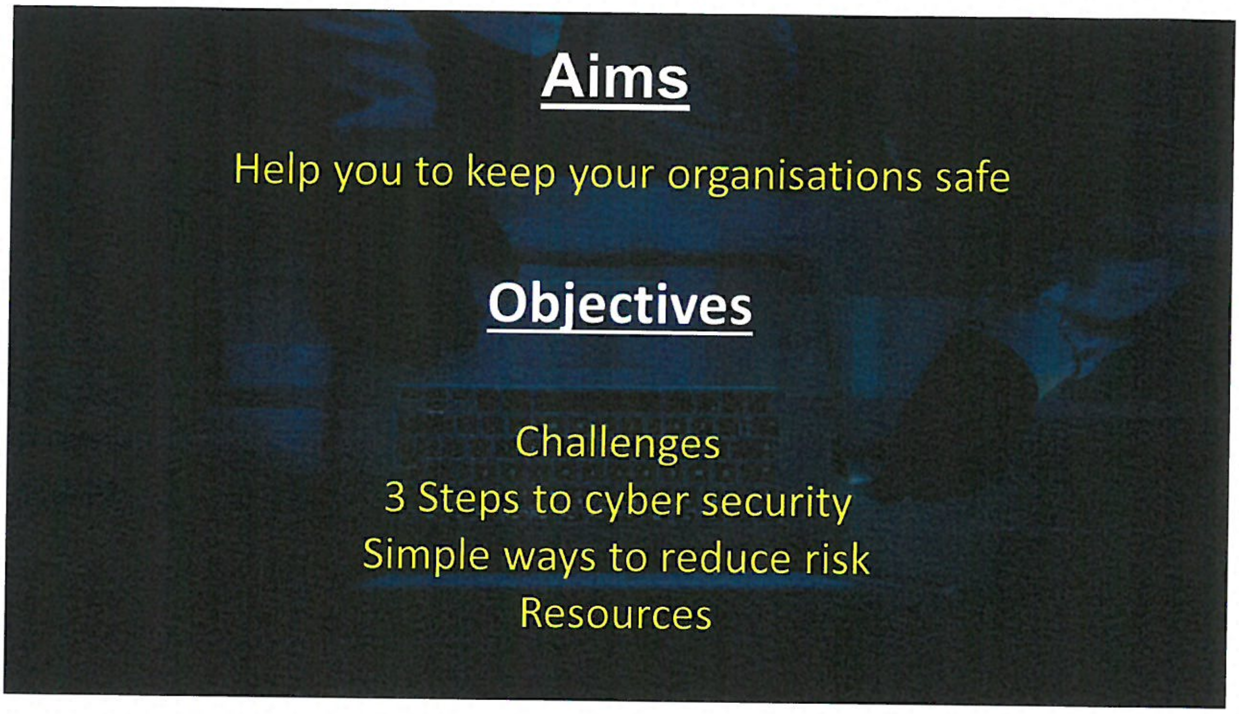
Staying Safe Online



CYBER CRIME PROTECT

Ivor Bowen: Detective Sergeant - Partnership Development and Cyber Protect Officer

Steve Morton: Hampshire Constabulary Cyber Volunteer

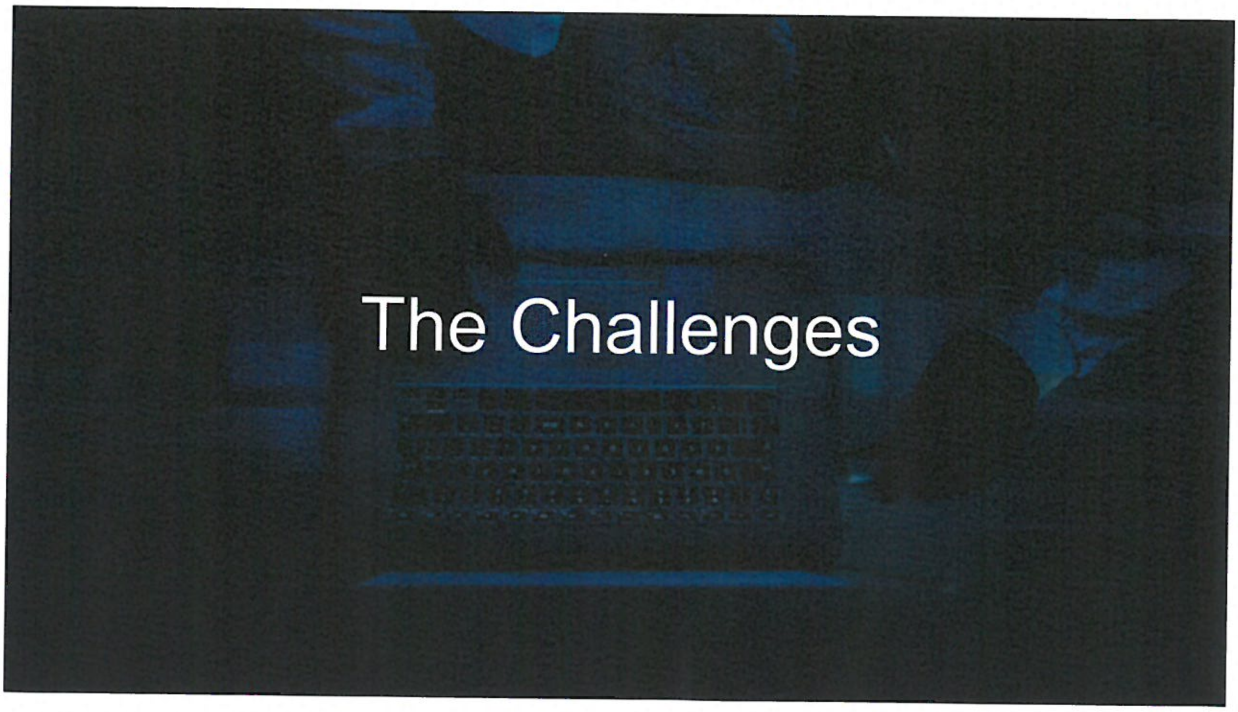


Aims

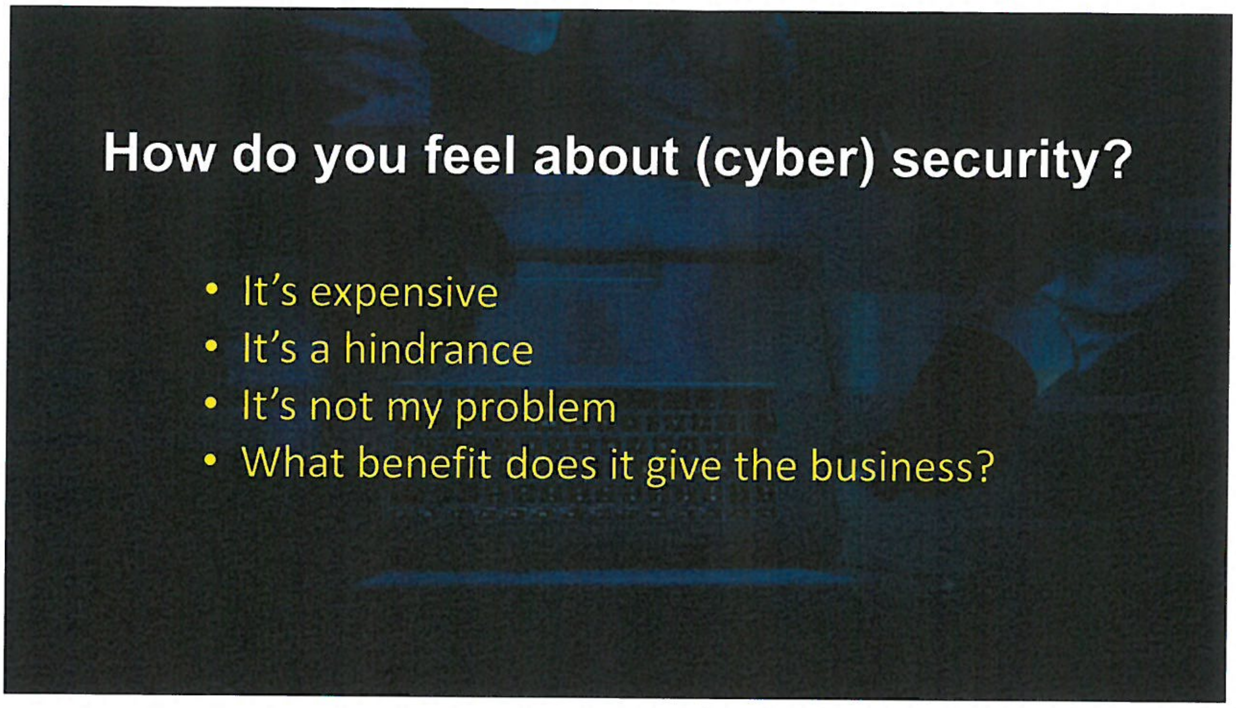
Help you to keep your organisations safe

Objectives

Challenges
3 Steps to cyber security
Simple ways to reduce risk
Resources

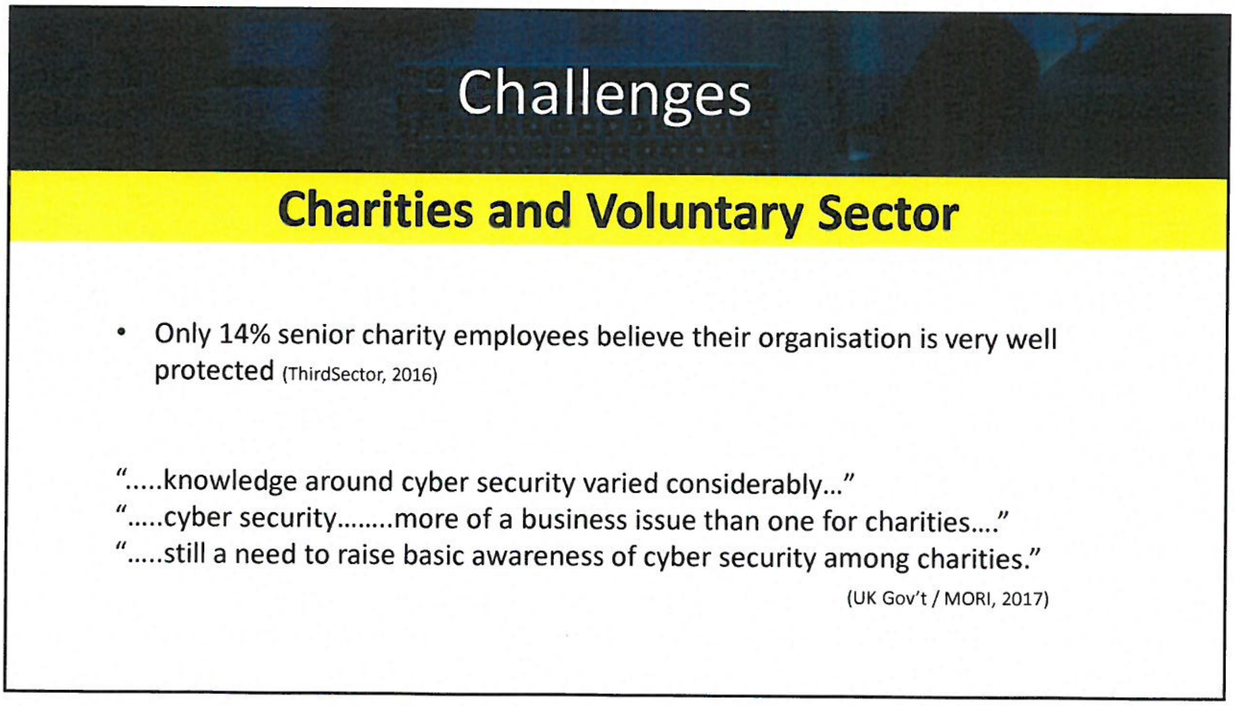


The Challenges



How do you feel about (cyber) security?

- It's expensive
- It's a hindrance
- It's not my problem
- What benefit does it give the business?



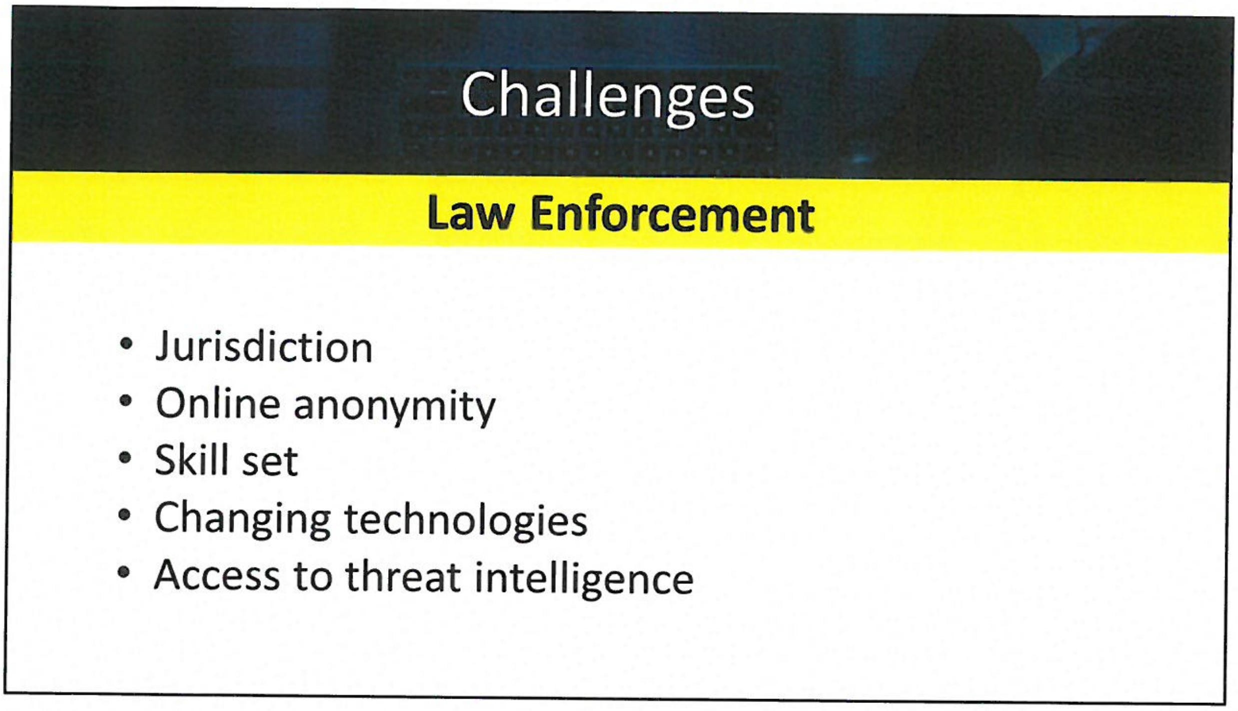
Challenges

Charities and Voluntary Sector

- Only 14% senior charity employees believe their organisation is very well protected (ThirdSector, 2016)

".....knowledge around cyber security varied considerably..."
".....cyber security........more of a business issue than one for charities...."
".....still a need to raise basic awareness of cyber security among charities."

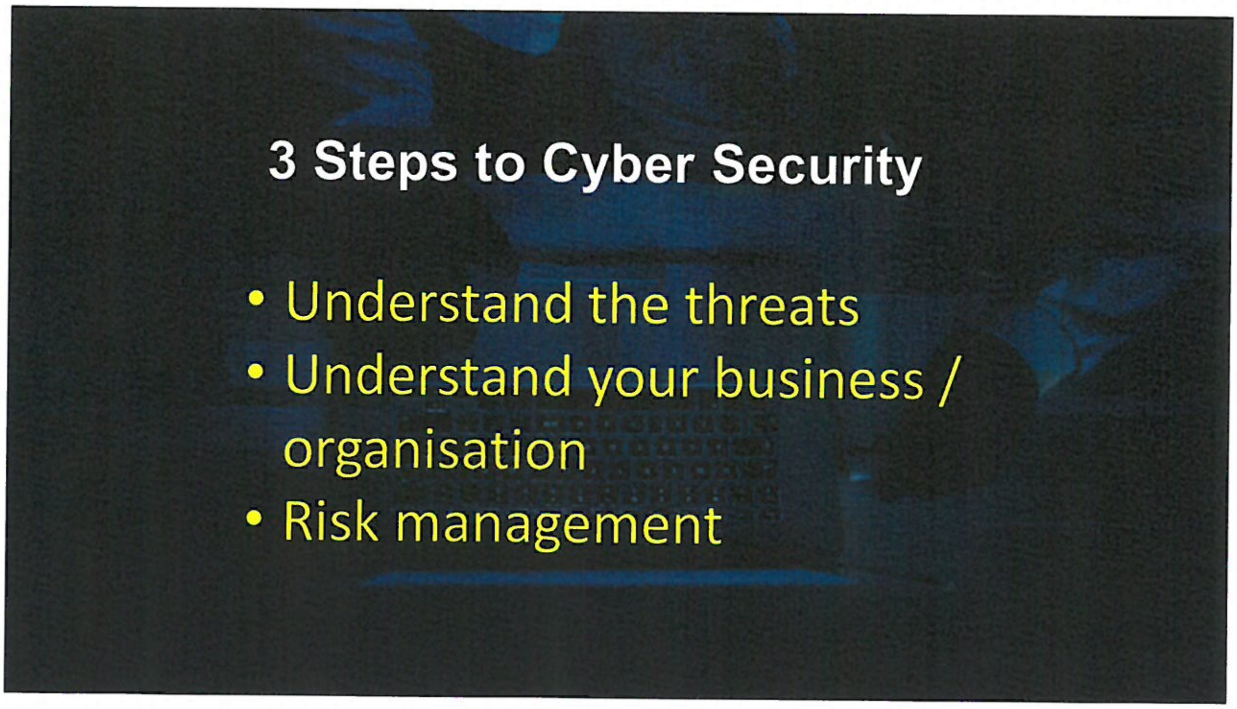
(UK Gov't / MORI, 2017)



Challenges

Law Enforcement

- Jurisdiction
- Online anonymity
- Skill set
- Changing technologies
- Access to threat intelligence



3 Steps to Cyber Security

- Understand the threats
- Understand your business / organisation
- Risk management

Common charity fraud risks

The true cost of fraud to UK charities is unknown. But could be as high as **£2bn** a year.

Gift aid
Cyber crime
Investment
Banking
Phishing
Identity
Grant
Staff
Fundraising
Payroll
Credit card
Accounting
Expenses
Procurement

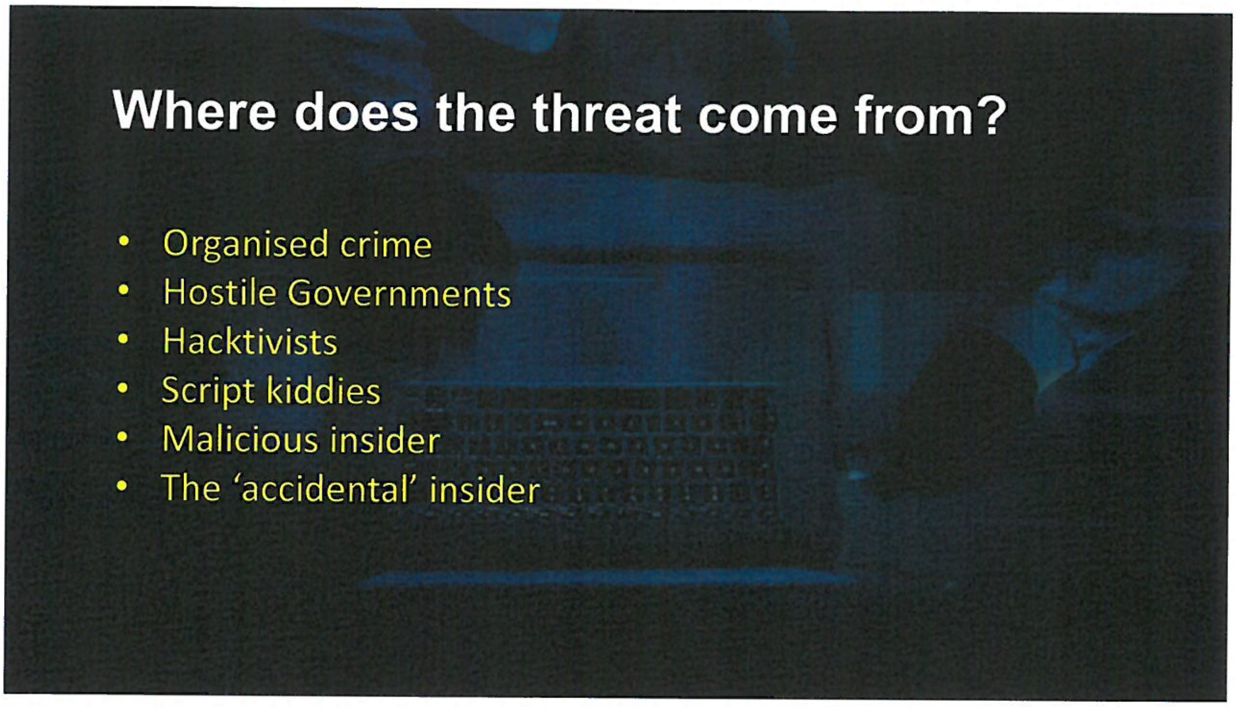
Fraud Advisory Panel

Understand the threats

Many types of crime affecting charities

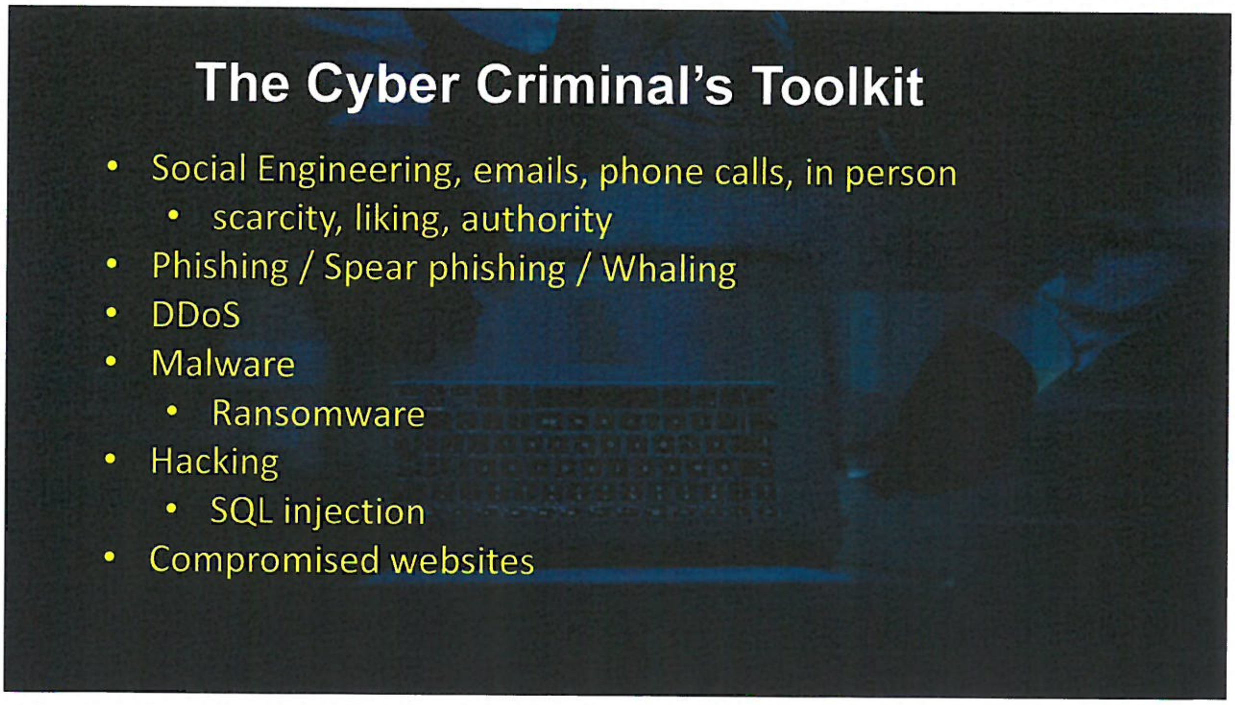
Understand the threats

- Approx 5 million fraud and computer misuse crimes year ending June 2017 (ONS)
- Approx 50% crime is fraud
- £11 billion lost through cybercrime/fraud 2015/16 (Action Fraud)
- £29 billion in 2016 (Beaming)
- 1.3 million businesses it by phishing
- 1.3 million (viruses), 1 million (hacking), 390,000 (ransomware)
- £7.4 million (ransomware), £5.9 million (phishing)



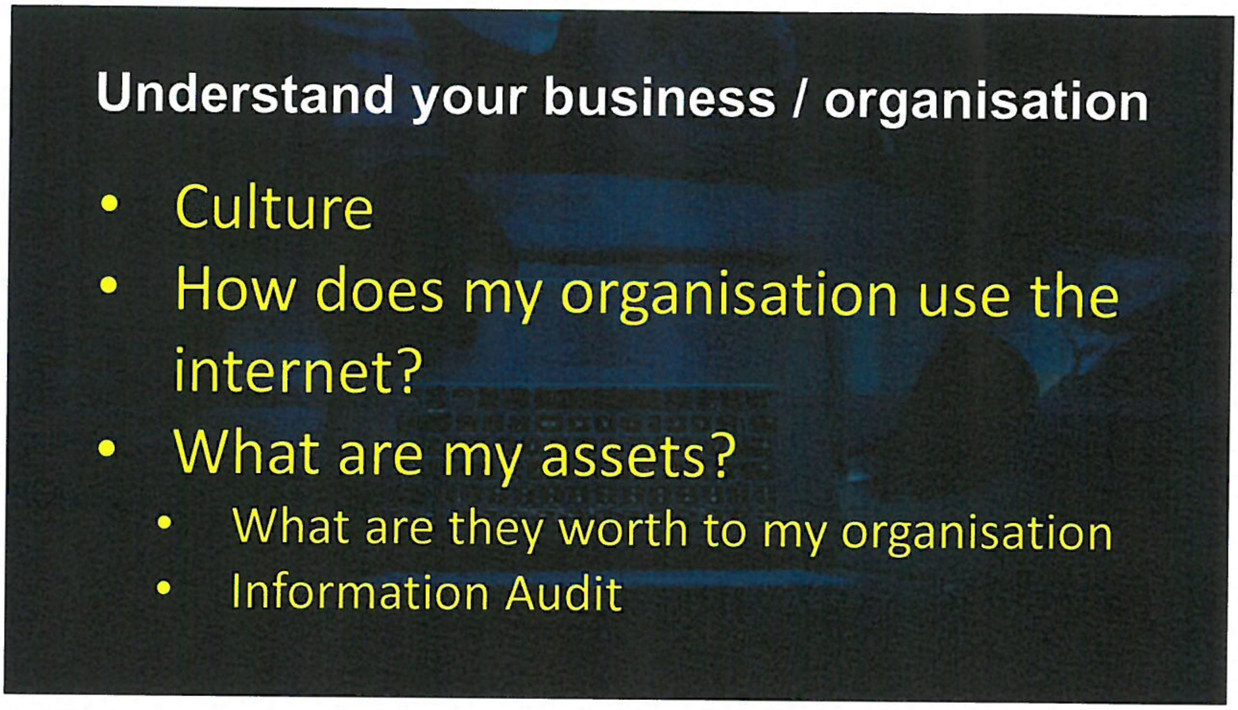
Where does the threat come from?

- Organised crime
- Hostile Governments
- Hacktivists
- Script kiddies
- Malicious insider
- The 'accidental' insider



The Cyber Criminal's Toolkit

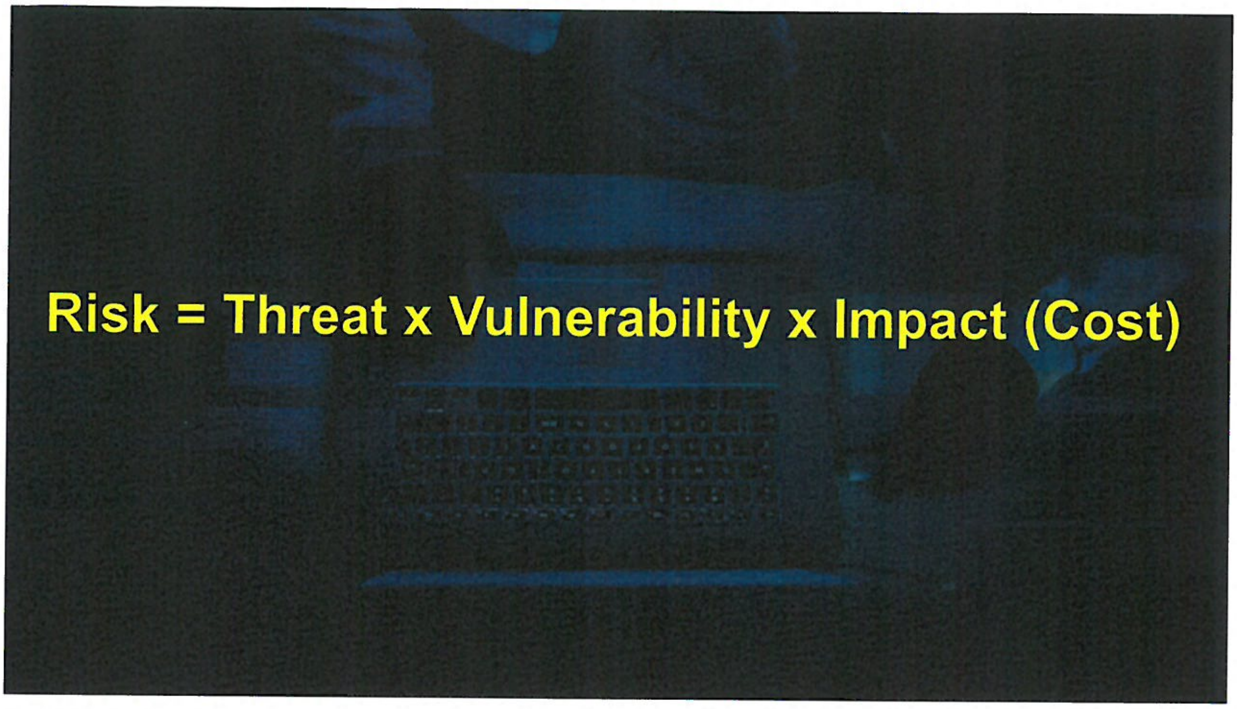
- Social Engineering, emails, phone calls, in person
  - scarcity, liking, authority
- Phishing / Spear phishing / Whaling
- DDoS
- Malware
  - Ransomware
- Hacking
  - SQL injection
- Compromised websites



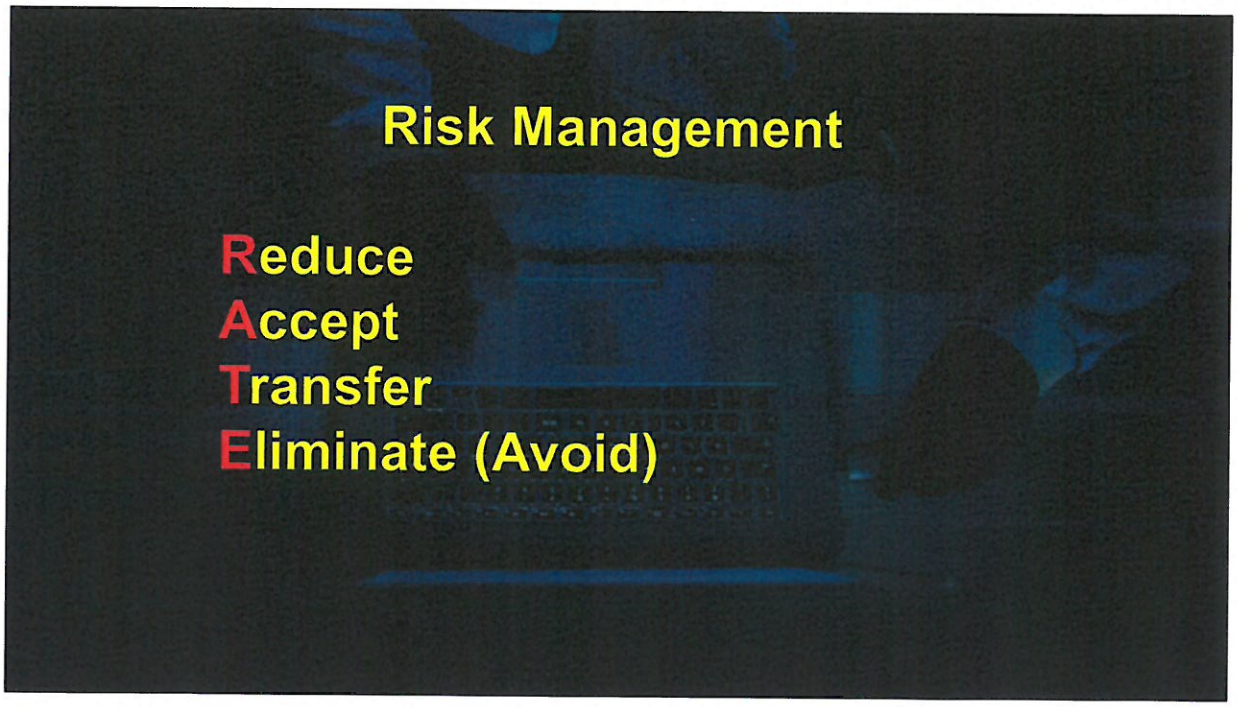
Understand your business / organisation

- Culture
- How does my organisation use the internet?
- What are my assets?
  - What are they worth to my organisation
  - Information Audit

What would be the impact if you lost those assets?

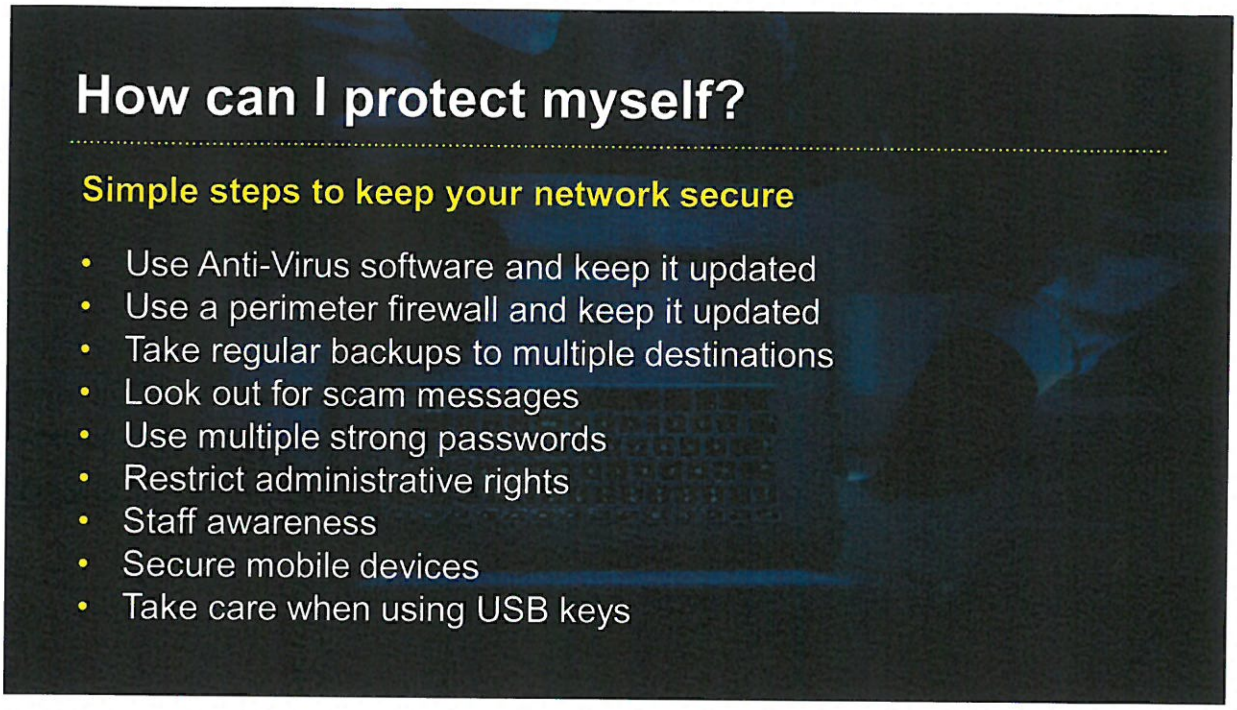


Risk = Threat x Vulnerability x Impact (Cost)



Risk Management

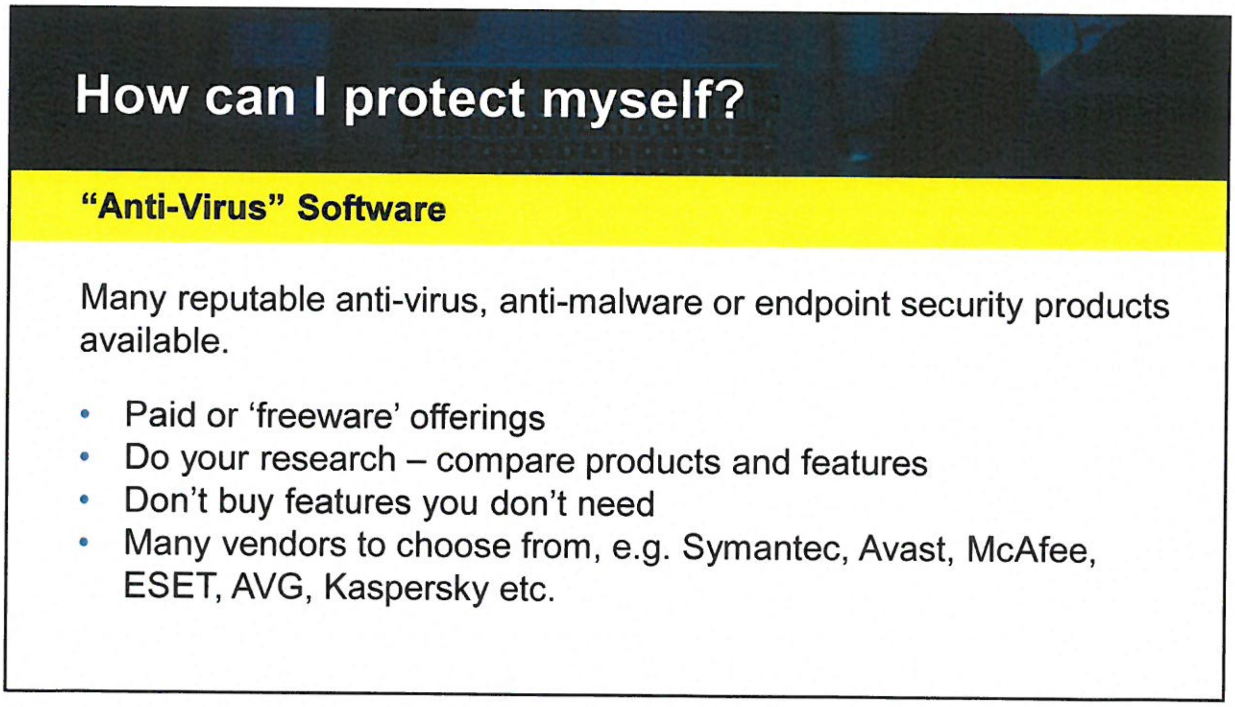
Reduce
Accept
Transfer
Eliminate (Avoid)



How can I protect myself?

Simple steps to keep your network secure

- Use Anti-Virus software and keep it updated
- Use a perimeter firewall and keep it updated
- Take regular backups to multiple destinations
- Look out for scam messages
- Use multiple strong passwords
- Restrict administrative rights
- Staff awareness
- Secure mobile devices
- Take care when using USB keys

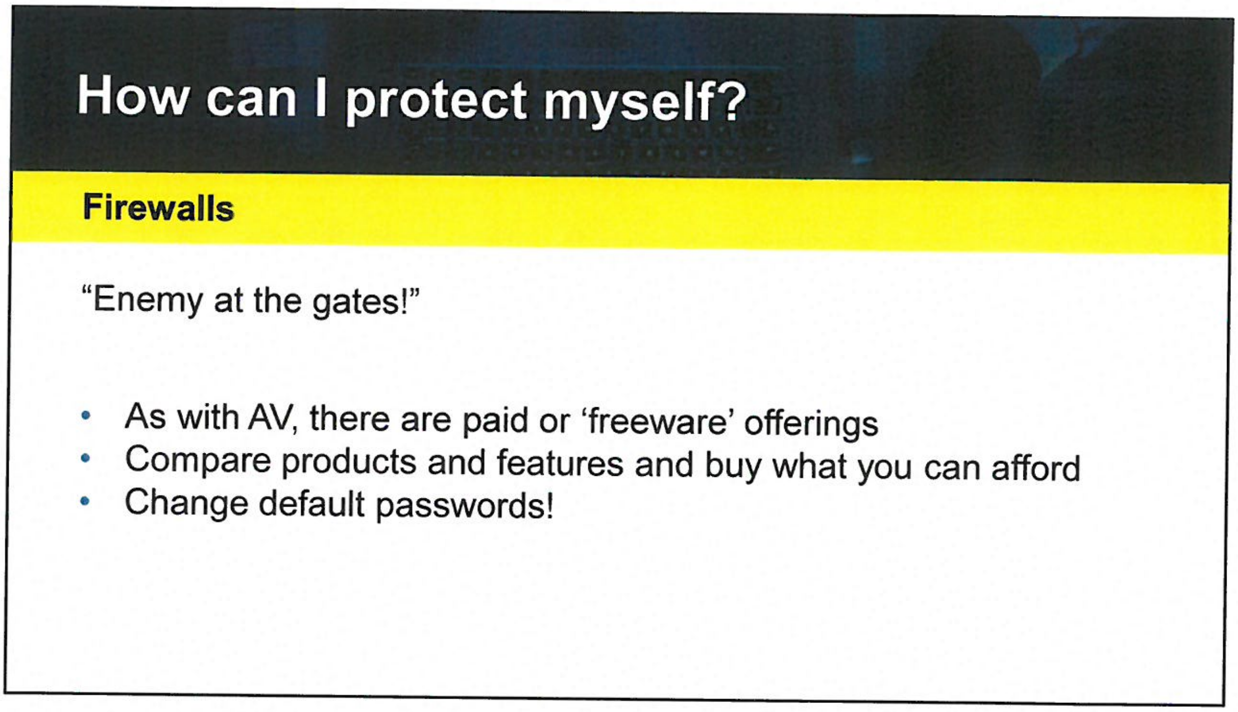


How can I protect myself?

“Anti-Virus” Software

Many reputable anti-virus, anti-malware or endpoint security products available.

- Paid or ‘freeware’ offerings
- Do your research – compare products and features
- Don’t buy features you don’t need
- Many vendors to choose from, e.g. Symantec, Avast, McAfee, ESET, AVG, Kaspersky etc.

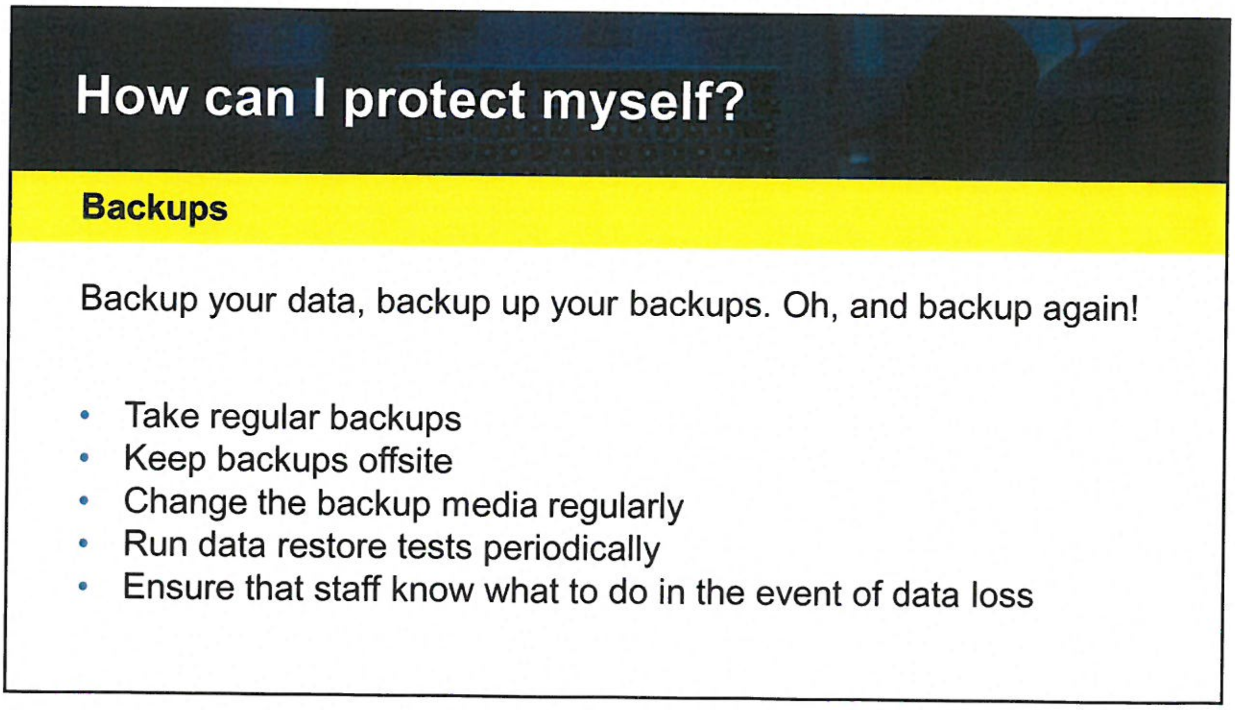


How can I protect myself?

Firewalls

“Enemy at the gates!”

- As with AV, there are paid or ‘freeware’ offerings
- Compare products and features and buy what you can afford
- Change default passwords!



How can I protect myself?

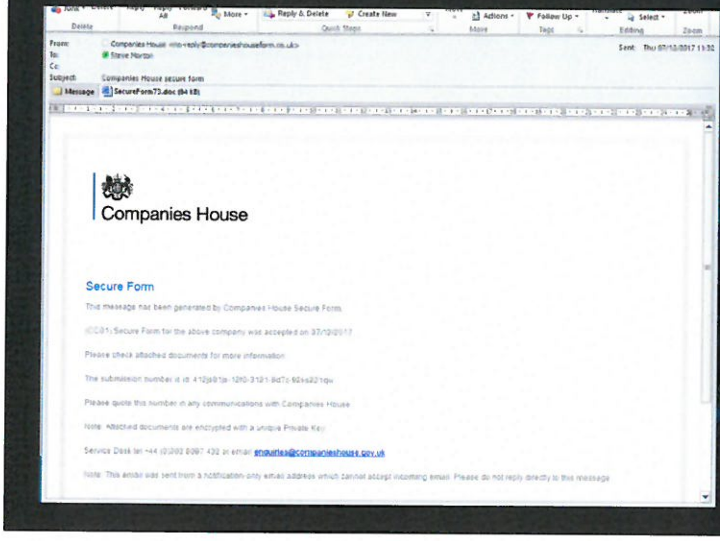
Backups

Backup your data, backup up your backups. Oh, and backup again!

- Take regular backups
- Keep backups offsite
- Change the backup media regularly
- Run data restore tests periodically
- Ensure that staff know what to do in the event of data loss

How can I protect myself?

Phishing messages



From: Companies House <no-reply@companieshouseform.co.uk>
To: Steve Morton
Cc:
Subject: Companies House secure form
Sent: Thu 07/12/2017 11:32
Message | SecureForm73.doc (84 KB)

Companies House

Secure Form

This message has been generated by Companies House Secure Form.

(CC01) Secure Form for the above company was accepted on 07/12/2017

Please check attached documents for more information

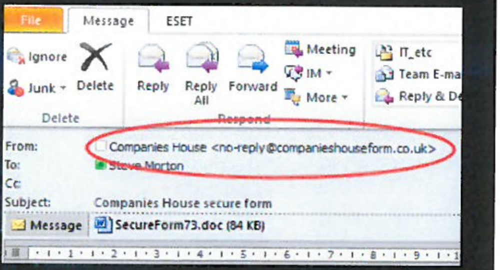
The submission number is id: 412jb01a-12f0-3121-9d7c-92xs221qw

Please quote this number in any communications with Companies House

Note: Attached documents are encrypted with a unique Private Key

Service Desk tel +44 (0)303 8097 432 or email enquiries@companieshouse.gov.uk

Note: This email was sent from a notification-only email address which cannot accept incoming email. Please do not reply directly to this message

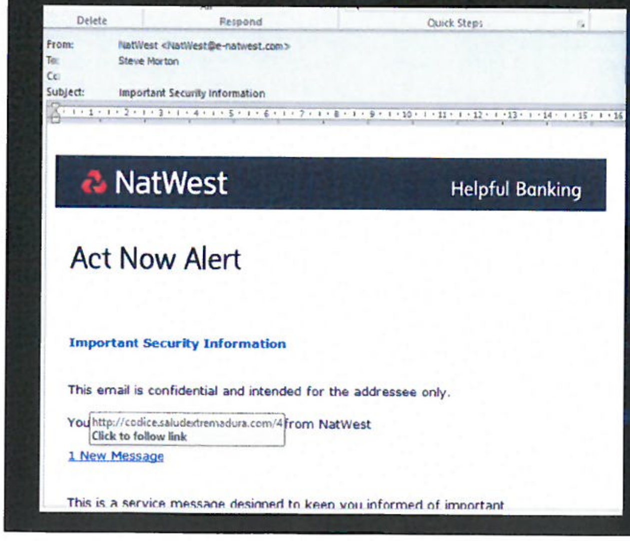


From: Companies House <no-reply@companieshouseform.co.uk>
To: Steve Morton
Cc:
Subject: Companies House secure form
Message | SecureForm73.doc (84 KB)

- Why?
- Salutation correct?
- Sender Address Ok?
- Are there attachments?
- Are links genuine?

How can I protect myself?

Phishing messages



From: NatWest <NatWest@e-natwest.com>
To: Steve Morton
Cc:
Subject: Important Security Information

NatWest Helpful Banking

Act Now Alert

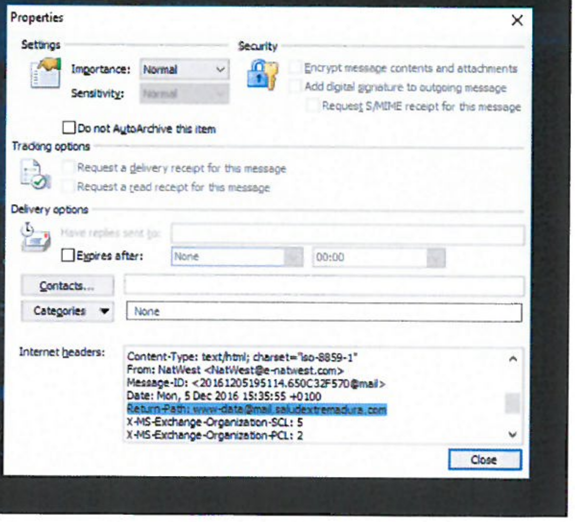
Important Security Information

This email is confidential and intended for the addressee only.

You http://codice.saludextremadura.com/4 Click to follow link from NatWest

1 New Message

This is a service message designed to keep you informed of important

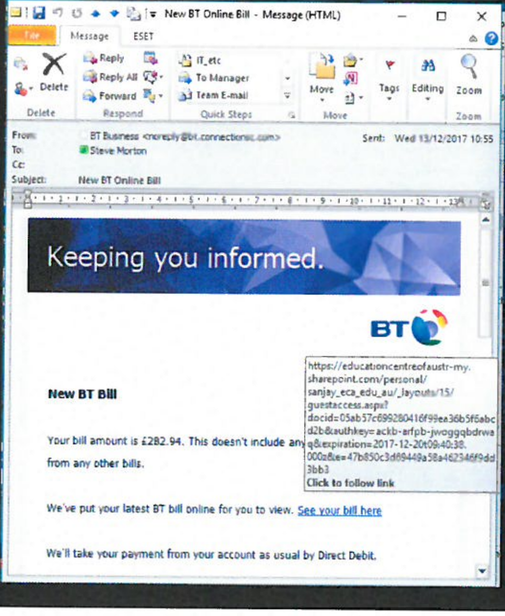


Importance: Normal
Sensitivity: Normal
□ Encrypt message contents and attachments
□ Add digital signature to outgoing message
□ Request S/MIME receipt for this message
□ Do not AutoArchive this item
□ Request a delivery receipt for this message
□ Request a read receipt for this message
Have replies sent to:
□ Expires after: None 00:00
Categories: None

Internet headers:

```
Content-Type: text/html; charset="iso-8859-1"
From: NatWest <NatWest@e-natwest.com>
Message-ID: <20161205195114.650C32F570@mail>
Date: Mon, 5 Dec 2016 15:35:55 +0100
Return-Path: www-data@mail.saludextremadura.com
X-MS-Exchange-Organization-SCL: 5
X-MS-Exchange-Organization-PCL: 2
```

How can I protect myself?



From: BT Business <noreply@bt.connectionsc.com>
Sent: Wed 13/12/2017 10:55
To: Steve Morton
Cc:
Subject: New BT Online Bill

Keeping you informed.

BT

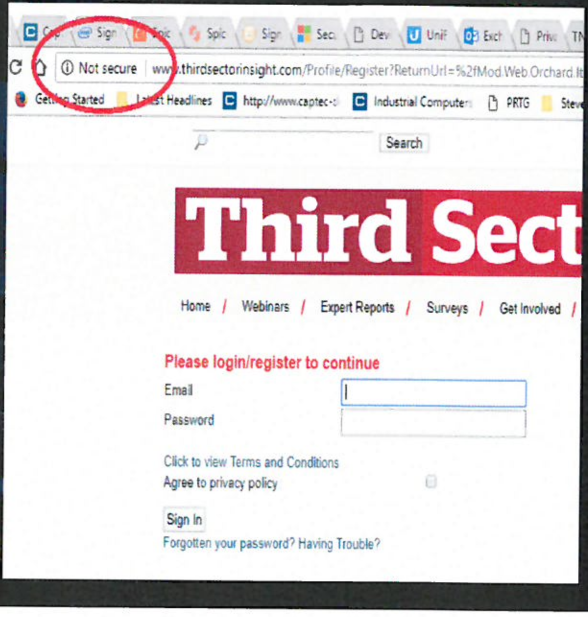
New BT Bill

Your bill amount is £282.94. This doesn't include any ... from any other bills.

https://educationcentreofaustr-my.sharepoint.com/personal/sanjay_eca_edu_au/_layouts/15/guestaccess.aspx?docid=05ab57c699280416f99ea36b5f6abcd2b&authkey=ackb-arfpb-jwoggqbdrwaq&expiration=2017-12-20t09:40:38.000z&e=47b850c3d69449a58a462346f9dd3bb3
Click to follow link

We've put your latest BT bill online for you to view. See your bill here

We'll take your payment from your account as usual by Direct Debit.



www.thirdsectorinsight.com/Profile/Register?ReturnUrl=%2fMod.Web.Orchard.It

http://www.captec-

Third Sect

Please login/register to continue

Email

Password

Click to view Terms and Conditions

Agree to privacy policy □

Sign In

Forgotten your password? Having Trouble?

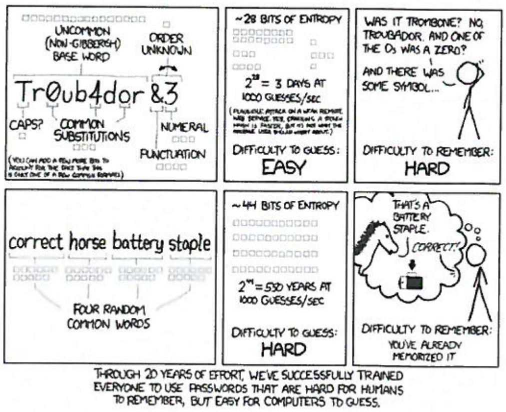
How can I protect myself?

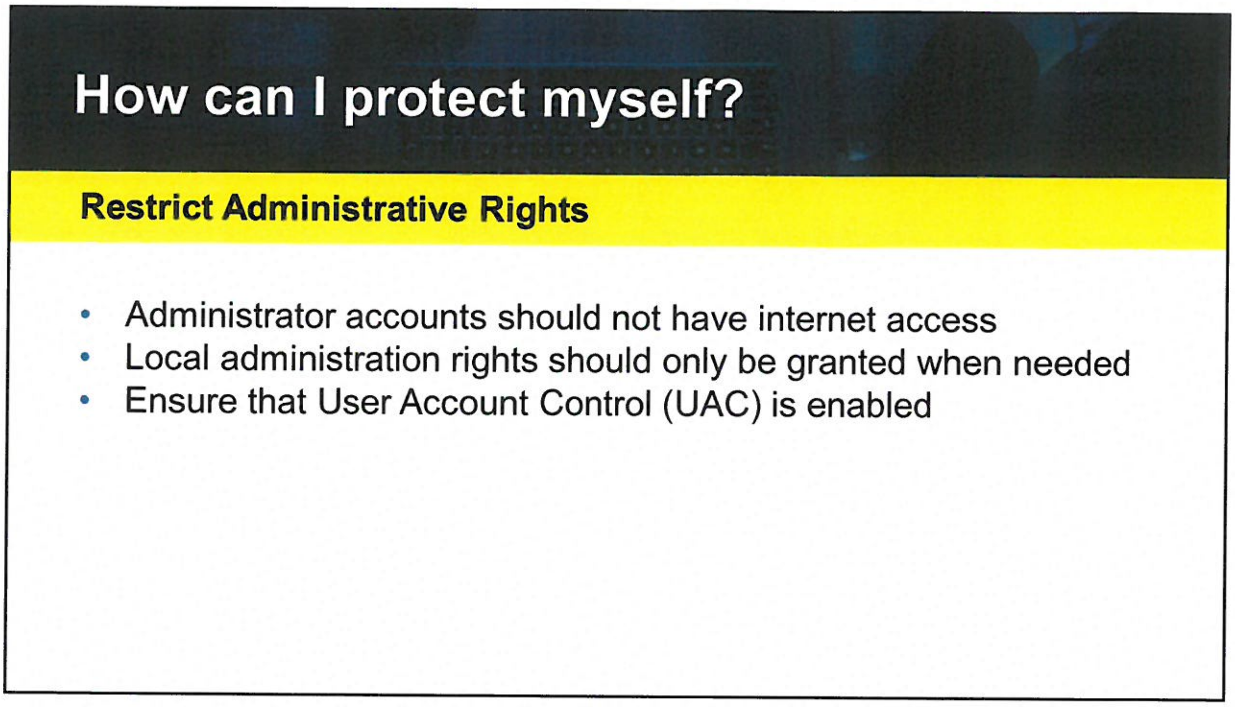
Passwords

"You don't use the same key for every lock, why use the same password for every account?"

- Use multiple strong passwords
- Use phrases or chains of words

- *Cartoon courtesy of xkcd.com*

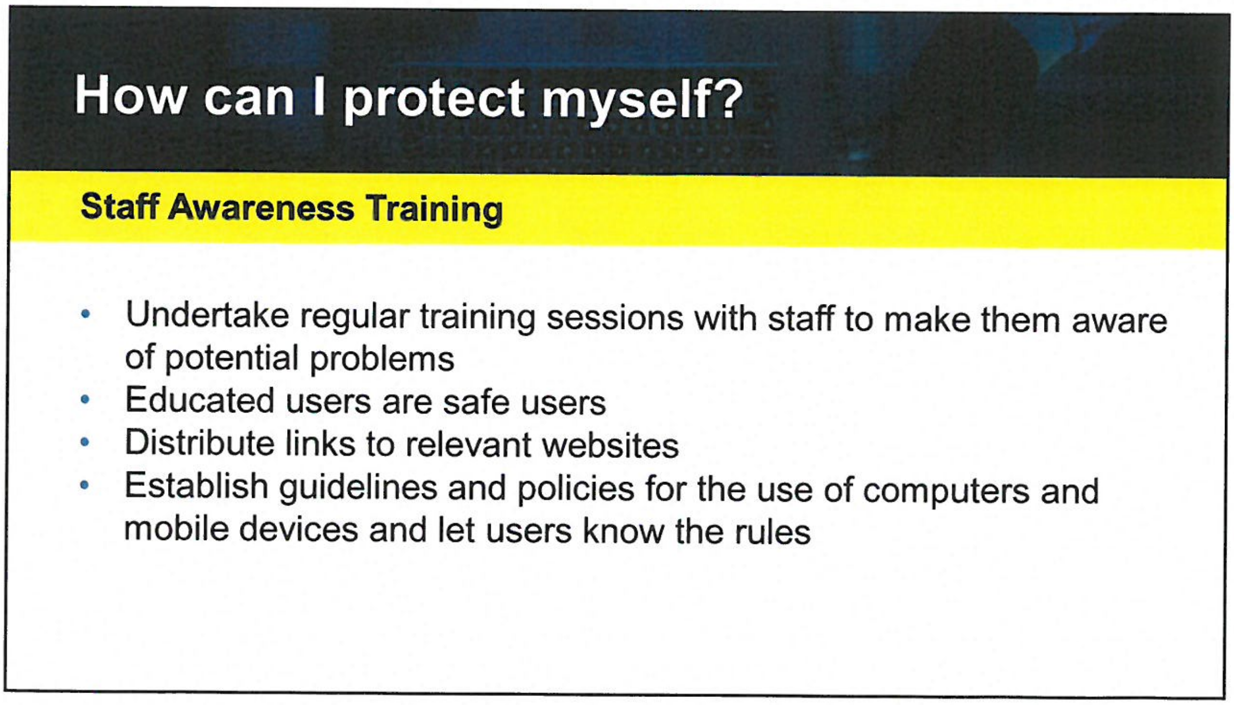

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



How can I protect myself?

Restrict Administrative Rights

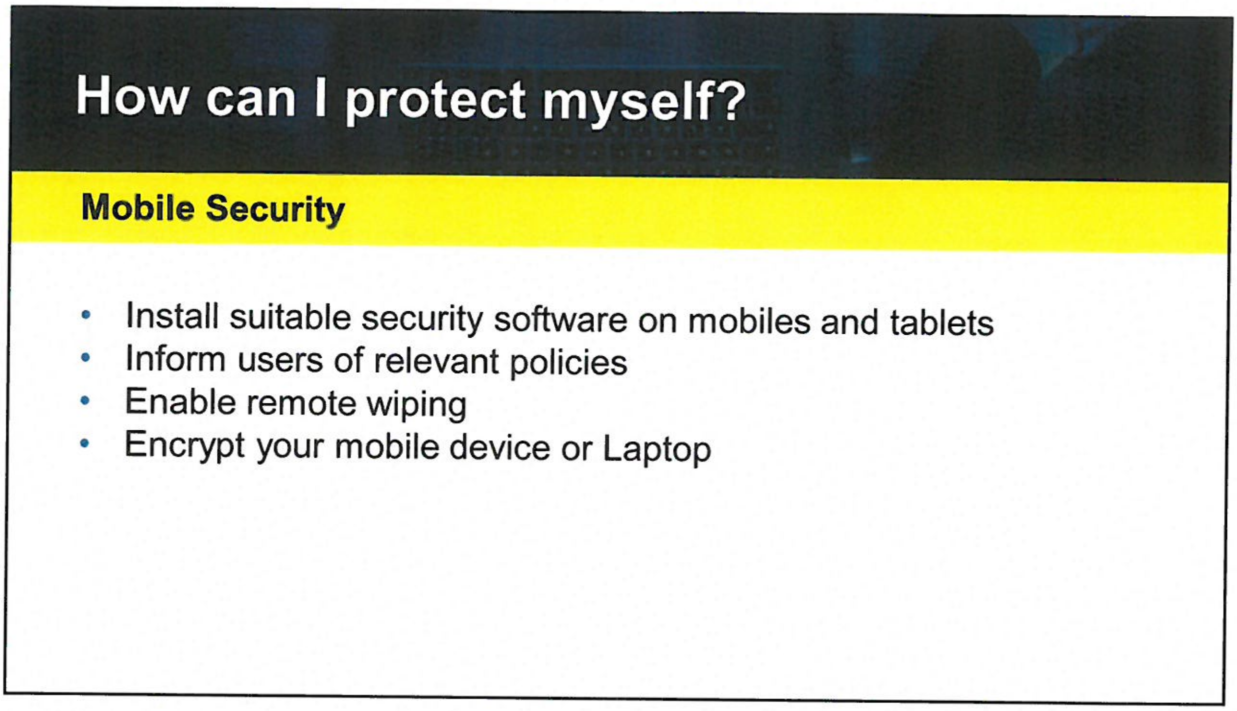
- Administrator accounts should not have internet access
- Local administration rights should only be granted when needed
- Ensure that User Account Control (UAC) is enabled



How can I protect myself?

Staff Awareness Training

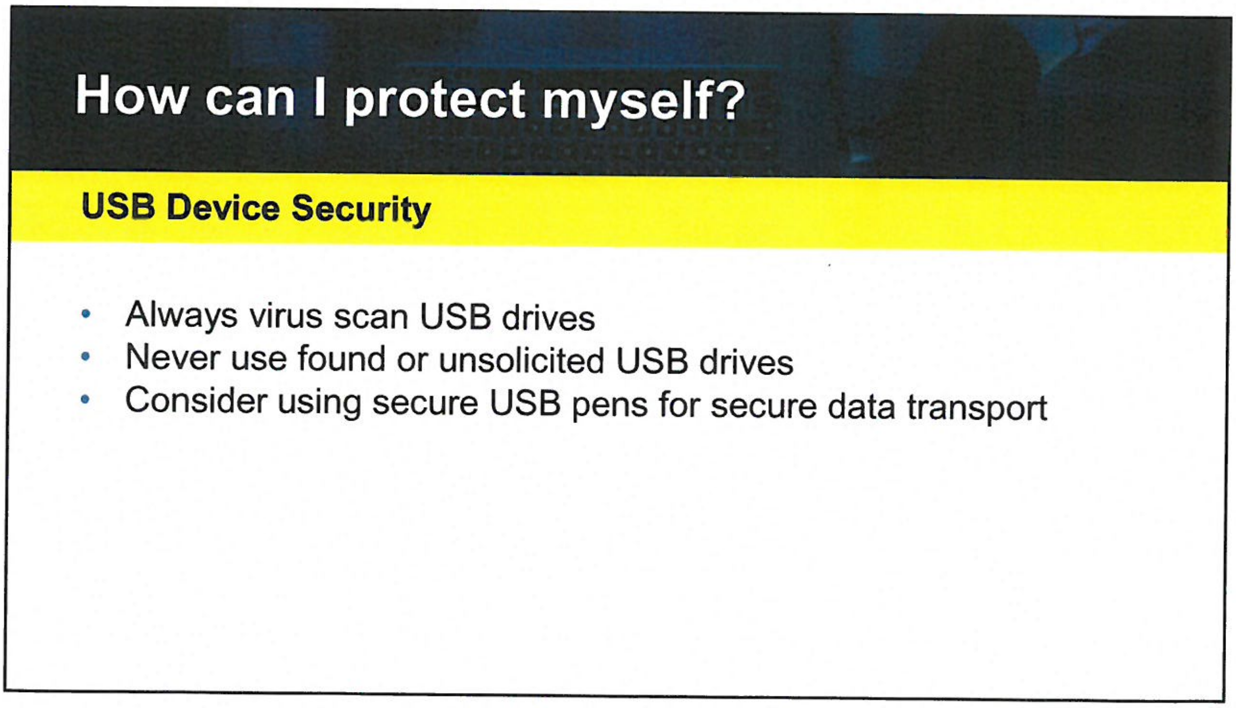
- Undertake regular training sessions with staff to make them aware of potential problems
- Educated users are safe users
- Distribute links to relevant websites
- Establish guidelines and policies for the use of computers and mobile devices and let users know the rules



How can I protect myself?

Mobile Security

- Install suitable security software on mobiles and tablets
- Inform users of relevant policies
- Enable remote wiping
- Encrypt your mobile device or Laptop



How can I protect myself?

USB Device Security

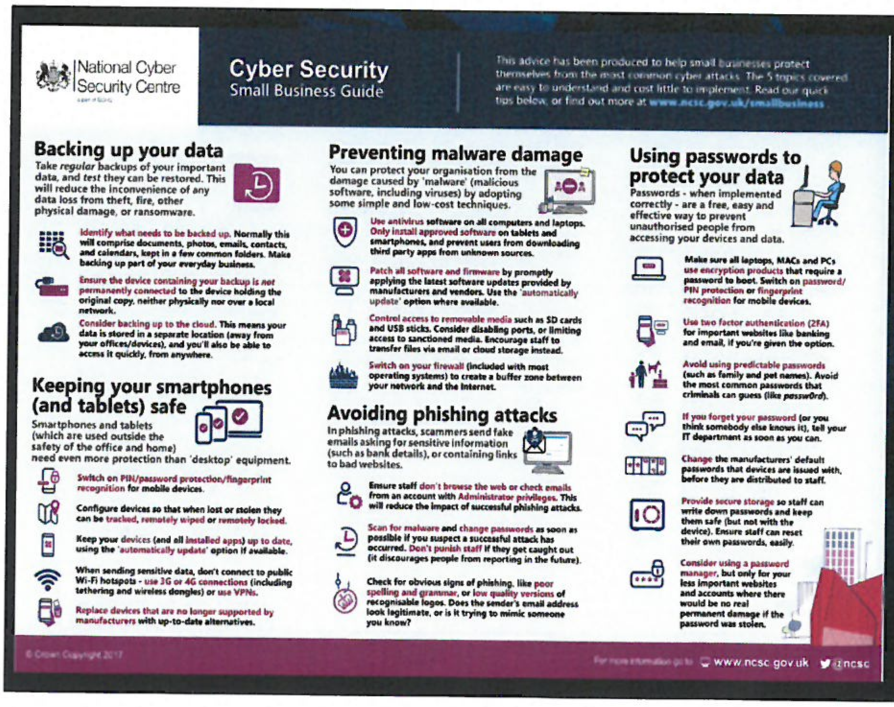
- Always virus scan USB drives
- Never use found or unsolicited USB drives
- Consider using secure USB pens for secure data transport

Resources

NCSC (National Cyber Security Centre) Small Business Guide Video Collection

www.ncsc.gov.uk/smallbusiness/video

- Backing up your data
- Protecting your organisation from malware
- Keeping your smartphones and tablets safe
- Using passwords to protect your data
- Avoid phishing attacks



National Cyber Security Centre

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/smallbusiness.

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.

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.

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.

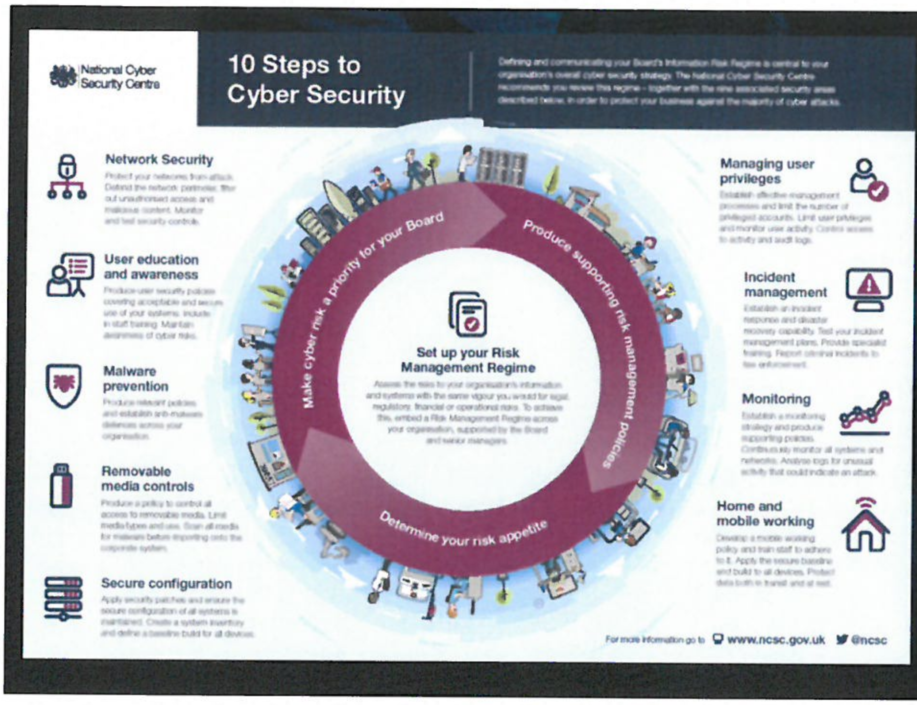
Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

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.

For more information go to www.ncsc.gov.uk @ncsc

NCSC Small Business Guide

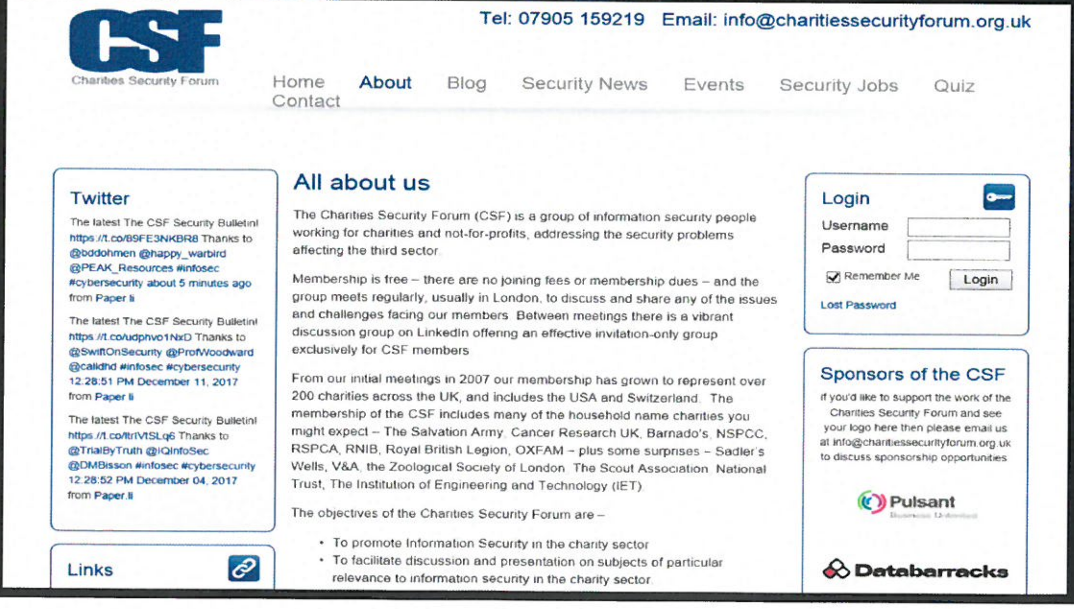
https://www.ncsc.gov.uk/smallbusiness


National Cyber Security Centre
10 Steps to Cyber Security
Network Security
User education and awareness
Malware prevention
Removable media controls
Secure configuration
Managing user privileges
Incident management
Monitoring
Home and mobile working
Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite
Set up your Risk Management Regime
For more information go to www.ncsc.gov.uk @ncsc

Ten Steps to Cyber Security and others

https://www.ncsc.gov.uk/guidance/10-steps-executive-summary

https://charitiessecurityforum.org.uk/



Tel: 07905 159219 Email: info@charitiessecurityforum.org.uk

All about us

The Charities Security Forum (CSF) is a group of information security people working for charities and not-for-profits, addressing the security problems affecting the third sector.

Membership is free – there are no joining fees or membership dues – and the group meets regularly, usually in London, to discuss and share any of the issues and challenges facing our members. Between meetings there is a vibrant discussion group on LinkedIn offering an effective invitation-only group exclusively for CSF members.

From our initial meetings in 2007 our membership has grown to represent over 200 charities across the UK, and includes the USA and Switzerland. The membership of the CSF includes many of the household name charities you might expect – The Salvation Army, Cancer Research UK, Barnado's, NSPCC, RSPCA, RNIB, Royal British Legion, OXFAM – plus some surprises – Sadler's Wells, V&A, the Zoological Society of London, The Scout Association, National Trust, The Institution of Engineering and Technology (IET).

The objectives of the Charities Security Forum are –

- To promote Information Security in the charity sector
- To facilitate discussion and presentation on subjects of particular relevance to information security in the charity sector

Twitter

The latest The CSF Security Bulletin! https://t.co/89FE3NKBR8 Thanks to @bddohmen @happy_warbird @PEAK_Resources #infosec #cybersecurity about 5 minutes ago from Paper.li

The latest The CSF Security Bulletin! https://t.co/udphvo1NxD Thanks to @SwiftOnSecurity @ProfWoodward @calidnd #infosec #cybersecurity 12:28:51 PM December 11, 2017 from Paper.li

The latest The CSF Security Bulletin! https://t.co/trIVtSLq6 Thanks to @TrialByTruth @IQinfoSec @DMBisson #infosec #cybersecurity 12:28:52 PM December 04, 2017 from Paper.li

Links

Login

Username

Password

☑ Remember Me Login

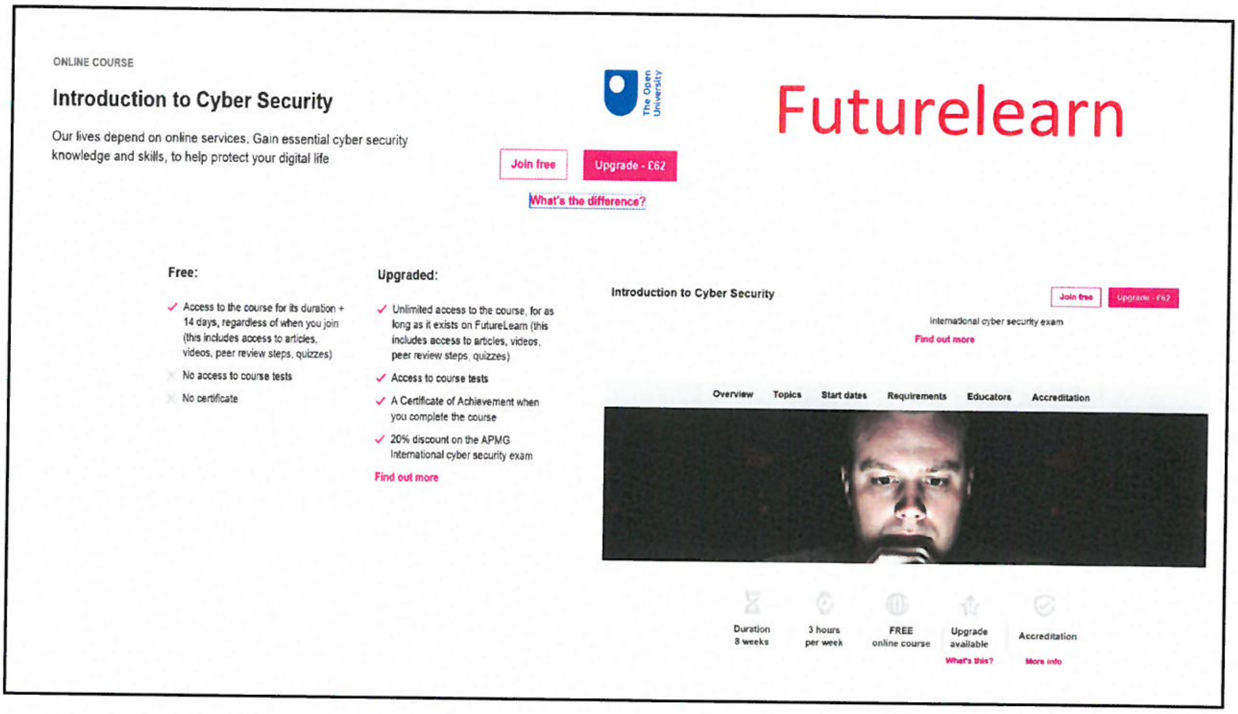
Lost Password

Sponsors of the CSF

If you'd like to support the work of the Charities Security Forum and see your logo here then please email us at info@charitiessecurityforum.org.uk to discuss sponsorship opportunities.

Pulsant

Databarracks



ONLINE COURSE

Introduction to Cyber Security

Our lives depend on online services. Gain essential cyber security knowledge and skills, to help protect your digital life

Join free | Upgrade - £62

What's the difference?

Futurelearn

Free:

- ✓ Access to the course for its duration + 14 days, regardless of when you join (this includes access to articles, videos, peer review steps, quizzes)
- ✗ No access to course tests
- ✗ No certificate

Upgraded:

- ✓ Unlimited access to the course, for as long as it exists on FutureLearn (this includes access to articles, videos, peer review steps, quizzes)
- ✓ Access to course tests
- ✓ A Certificate of Achievement when you complete the course
- ✓ 20% discount on the APMG International cyber security exam

Find out more

Introduction to Cyber Security

Join free | Upgrade - £62

International cyber security exam

Find out more

Overview | Topics | Start dates | Requirements | Educators | Accreditation

Duration 8 weeks | 3 hours per week | FREE online course | Upgrade available What's this? | Accreditation More info

Cyber Essentials Scheme

5 Technical Controls

- Securing your internet connection
- Secure your devices and software
- Control access to data and services
- Protect from viruses and other malware
- Keep devices and software up to date

ISO 27000 Series

Information Security Management Standards

- Risk based
- International standard
- Standards on risk management, business continuity, cyber security
- Compliance without accreditation

ActionFraud

National Fraud & Cyber Crime Reporting Centre

0300 123 2040

www.actionfraud.police.uk

CYBER
CRIME
PROTECT

Questions?

THANK YOU FOR LISTENING

@HCCyberProtect DIIProtect@hampshire.pnn.police.uk