superhighways
harnessing technology for community benefit

GDPR - Are we getting it right?

about Superhighways

Helping small charities do more with digital for 20 years

- Training (current offer)
- Tech support
- Consultancy & Websites
- Digital inclusion
- Training
- Impact Aloud
- Datawise London

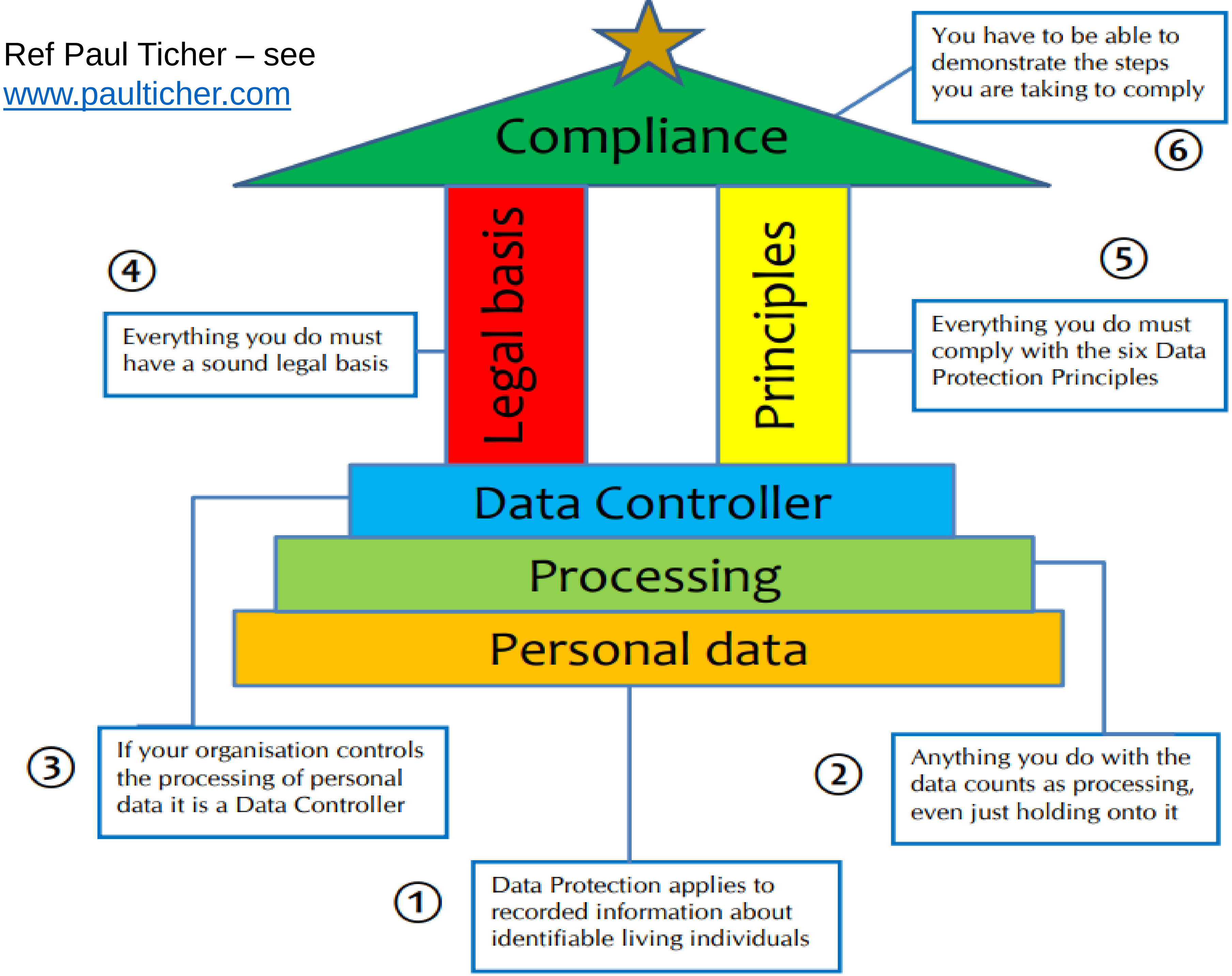
E-news sign up https://superhighways.org.uk/e-news

What we'll be covering today

- Key components of GDPR
  - Principles
  - Data audits
  - Privacy statements
  - Data protection policies

- Data security

Ref Paul Ticher – see
www.paulticher.com



Compliance

⑥ You have to be able to demonstrate the steps you are taking to comply

Legal basis

Principles

④ Everything you do must have a sound legal basis

⑤ Everything you do must comply with the six Data Protection Principles

Data Controller

Processing

Personal data

③ If your organisation controls the processing of personal data it is a Data Controller

② Anything you do with the data counts as processing, even just holding onto it

① Data Protection applies to recorded information about identifiable living individuals

Data protection

Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

See also the Data protection self assessment – getting ready for GDPR

Personal data definition

Special categories

Data processing…

- How are you processing personal data?

The 6 GDPR Principles

1. Process lawfully, fairly and in a transparent manner
2. Collect for specified, explicit and legitimate purposes
3. Only keep what is adequate, relevant and limited to what is necessary
4. Store accurate information and keep up to date
5. Retain only for as long as necessary
6. Process in an appropriate manner to maintain security

7. *Accountability* the controller shall be responsible for, and be able to demonstrate, compliance with the principles

Legal basis for processing…

Has to meet at least one of the following 6 Conditions…

- **Consent** – the individual has given clear consent for you to process their personal data for a specific purpose
- **Contract** - the processing is necessary for a contract you have with the individual
- **Legal obligation** - the processing is necessary for you to comply with the law (not including contractual obligations)
- **Vital interests** - the processing is necessary to protect someone's life
- **Public task** - the processing is necessary for you to perform a task in the public interest or for your official functions
- **Legitimate interests** - the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Legitimate interests

- Applying the three part test:
  - **Purpose test** – is there a legitimate interest behind the processing?
  - **Necessity test** – is the processing necessary for that purpose?
  - **Balancing test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?

- If your data processing is based on legitimate interests – be careful about extending your use beyond the original purpose

Consent

- Review how you are seeking, obtaining & recording consent
- GDPR references consent & explicit consent (especially re special categories)
- Both need to be:
    - Freely given
    - Specific
    - Informed
    - Unambiguous
- A clear positive indication of agreement to personal data being processed has to be given
- GDPR clear that Controllers must be able to demonstrate consent was given

Organisational Accountability

Raising awareness

- Update trustees, staff & volunteers
- Identify areas where you may have compliance issues
- Look at your risk register?

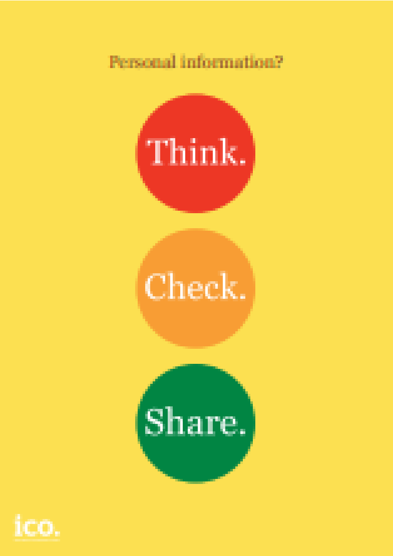
Review the information you hold

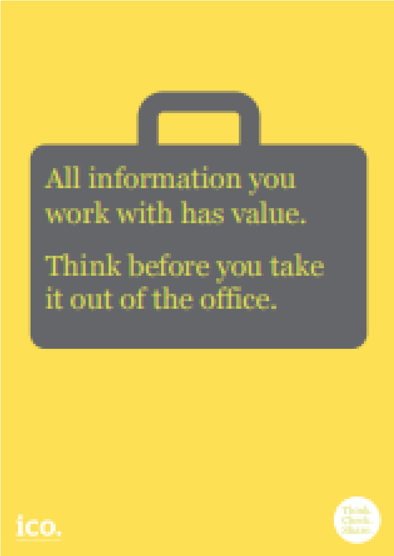
- Document the personal data you hold
- Where it came from
- Who do you share it with - you are expected to be able to update an organisations you've shared data with about an inaccuracy which needs correcting

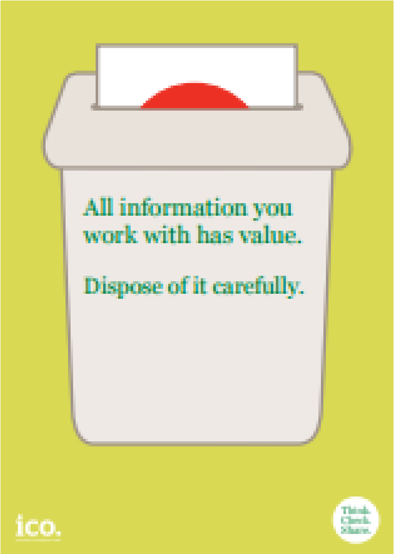
Communicating privacy information

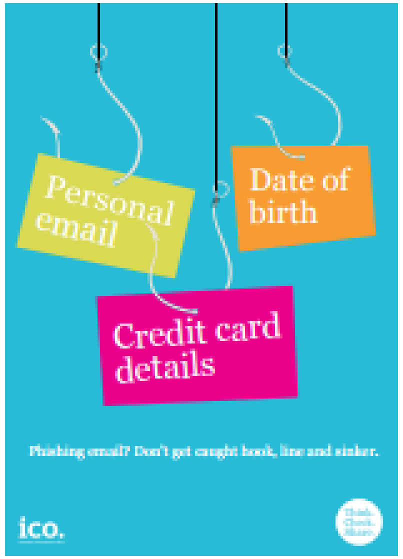
- Review current privacy notices *(what you tell people when you collect their personal data e.g. your identity + how you intend to use their data)*
- GDPR requires additional things to communicated:
  - Explain your purposes + legal basis for processing the data
  - State data retention periods
  - Point out people have a right to complain to the ICO if they think there is a problem with how you are handling their data
- Consider a layered approach - key points to be presented at point of data capture – e.g. paper or online forms
- Full details included in an accessible and understandable privacy policy or statement

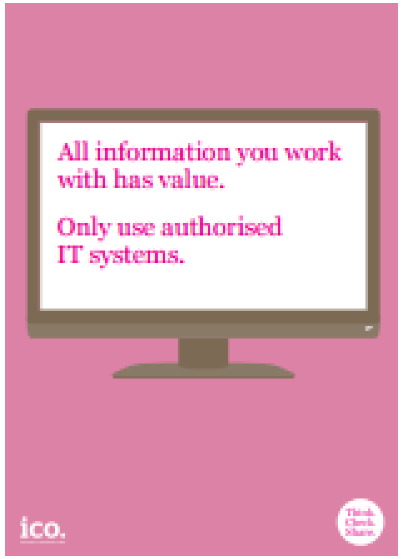
Think. Check. Share toolkit

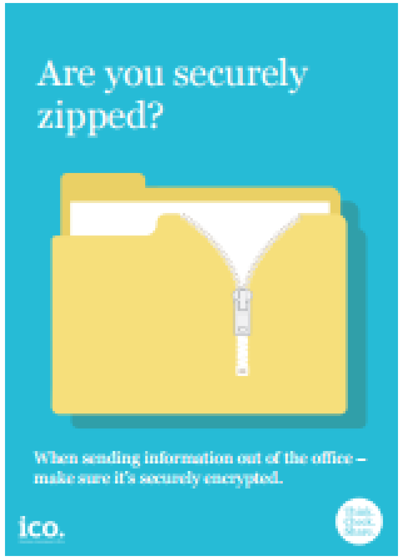


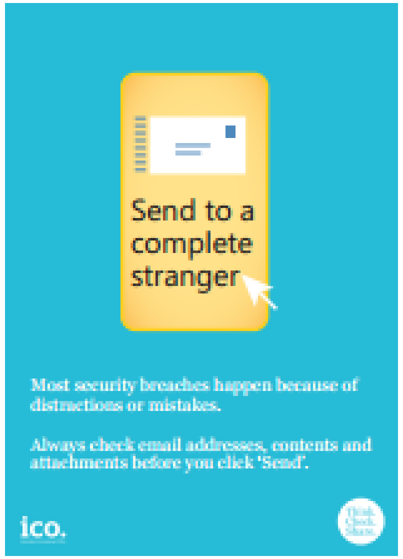

All information you work with has value.
Think before you take it out of the office.
ico.

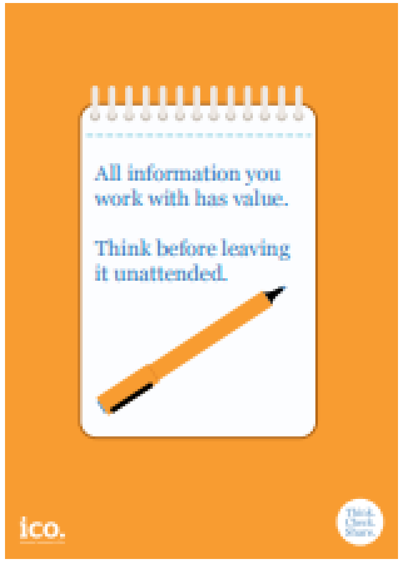


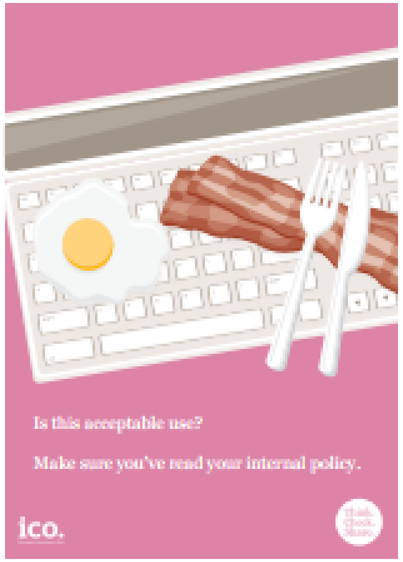


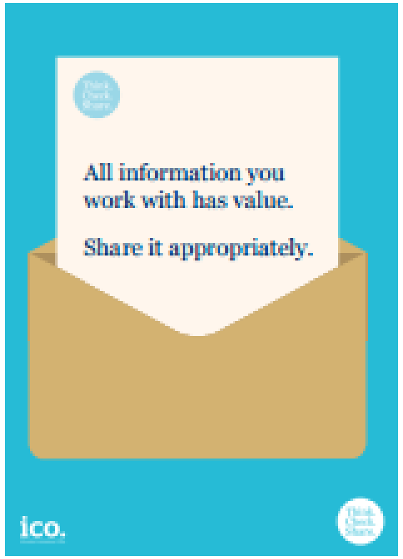

All information you work with has value.
Only use authorised IT systems.
ico.


Are you securely zipped?
When sending information out of the office – make sure it's securely encrypted.
ico.


Send to a complete stranger
Most security breaches happen because of distractions or mistakes.
Always check email addresses, contents and attachments before you click 'Send'.
ico.


All information you work with has value.
Think before leaving it unattended.
ico.





Getting ready for the new UK data protection law

Eight practical steps for micro business owners and sole traders

ico.
Information Commissioner's Office

1 **Know** the law is changing – which you now do, so that's one thing you've done already!

2 **Make sure you have a record** of the personal data you hold and why.

3 **Identify** why you have personal data and how you use it.

4 **Have a plan** in case people ask about their rights regarding the personal information you hold about them.

5 **Ask yourself: before I collect their data**, do I clearly tell people why I need it and how I will use it?

6 **Check your security.** This can include locking filing cabinets and password-protecting any of your devices and cloud storage that hold your staff or customers' personal data.

7 **Develop a process** to make sure you know what to do if you breach data protection rules.

8 **Don't panic: we're here to help.** For example, you can click here to see some frequently asked questions and their answers for several different business sectors.

ICO’s 5 top tips for small charities

- **Tell people what you are doing with their data**
  People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

- **Make sure your staff are adequately trained**
  New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

- **Use strong passwords**
  There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

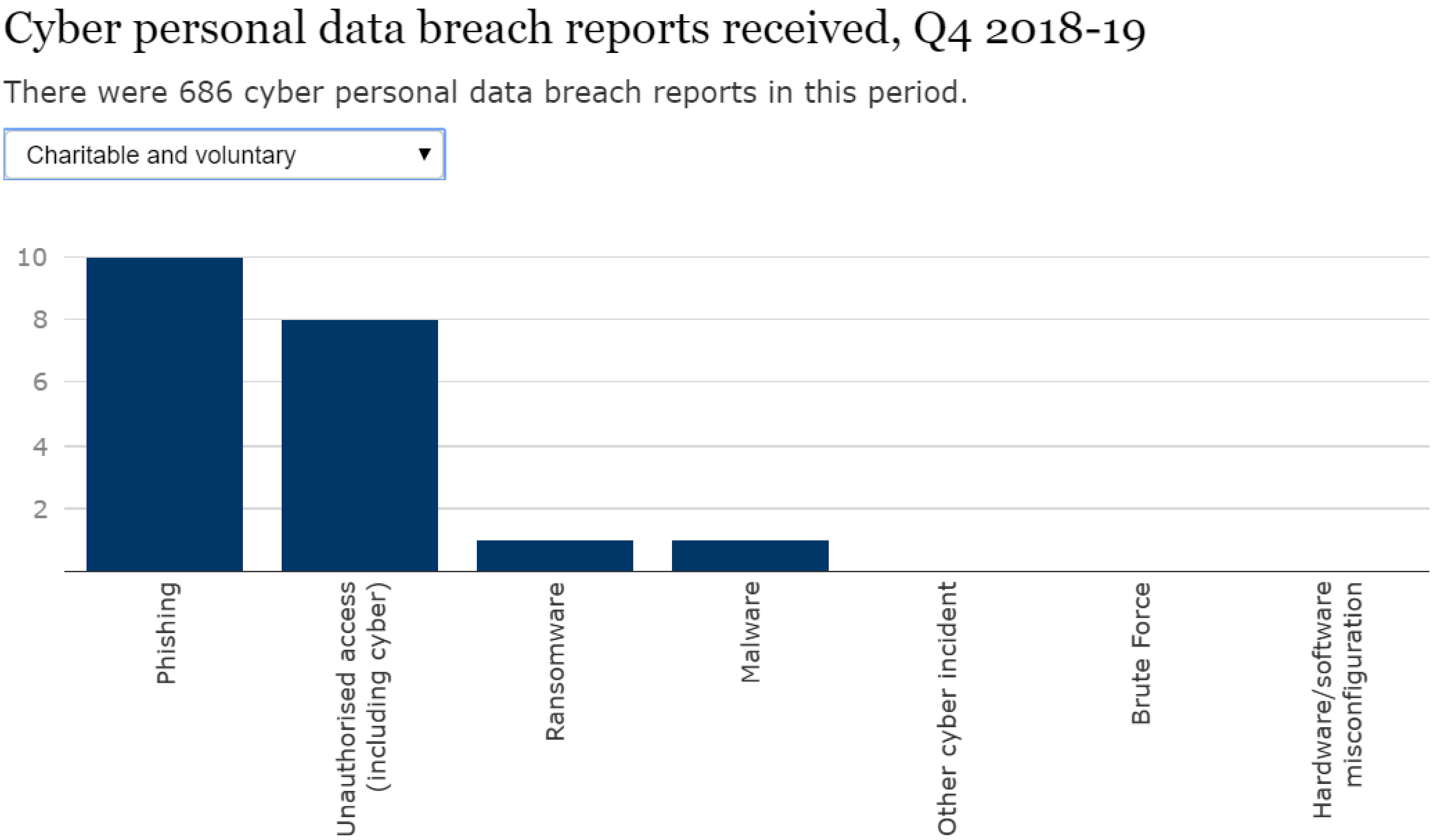
- **Encrypt all portable devices**
  Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

- **Only keep people’s information for as long as necessary**
  Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

superhighways
harnessing technology for community benefit

Maintaining security

Data security incident trends



Cyber personal data breach reports received, Q4 2018-19

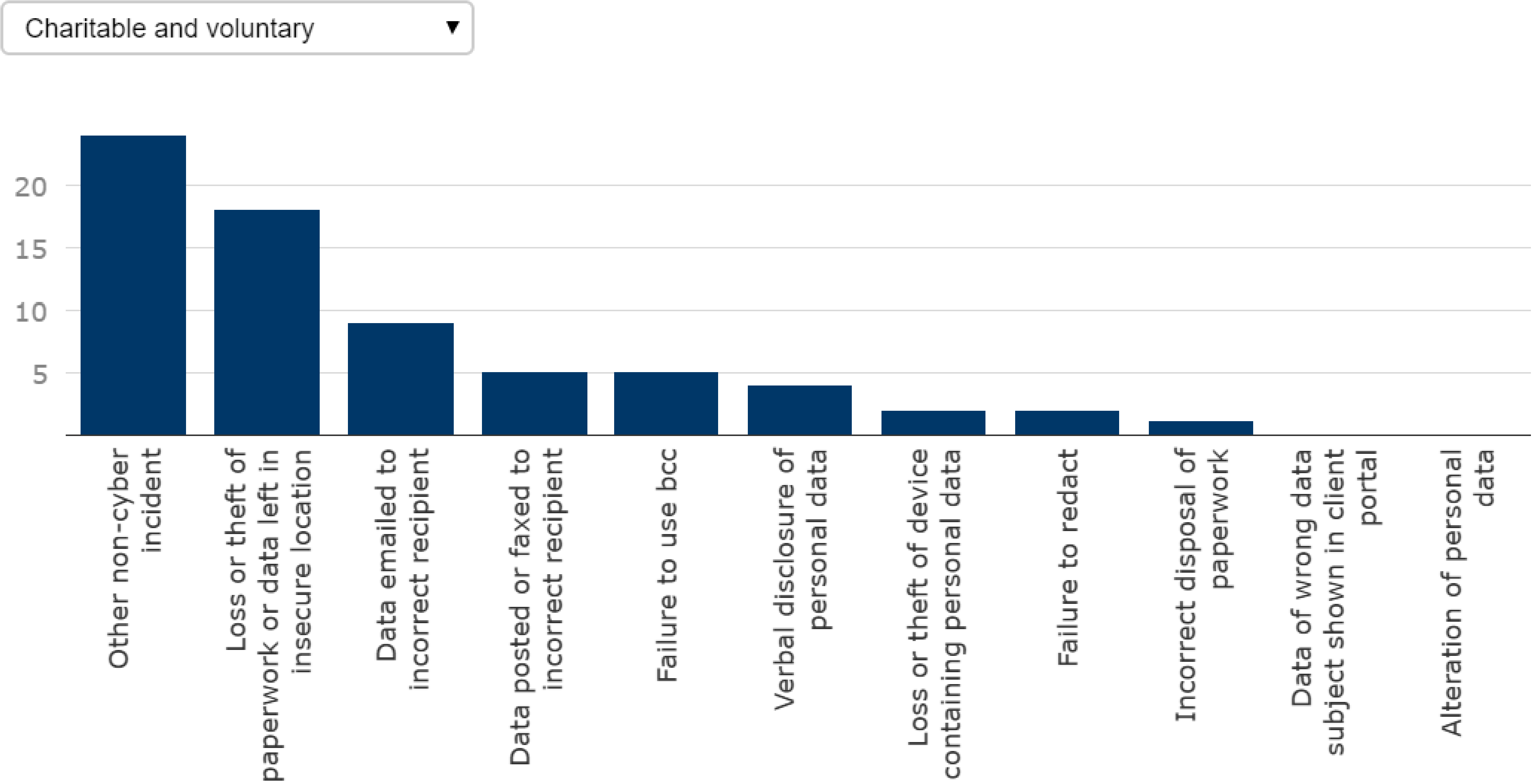
There were 686 cyber personal data breach reports in this period.

Charitable and voluntary ▼

10
8
6
4
2
Phishing
Unauthorised access (including cyber)
Ransomware
Malware
Other cyber incident
Brute Force
Hardware/software misconfiguration

Non-cyber personal data breach reports received, Q4 2018-19

There were 2,577 non-cyber personal data breach reports in this period, including 384 where the cause was "not provided", which are not displayed in this chart.



Charitable and voluntary ▼

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities 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/charity** .

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, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.

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 charity 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*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

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. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

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

https://youtu.be/TFICLREWxfU

Home working

Someone has had an operation and needs to work from home for one month.

Risks?

Mitigations?

Outreach service delivery

You take a laptop to a number of community venues around the borough to provide outreach advice sessions.

Risks?

Mitigations?

Referring clients

You make and receive client referrals from local statutory and voluntary sector organisations.

Risks?

Mitigations?

Staff turnover

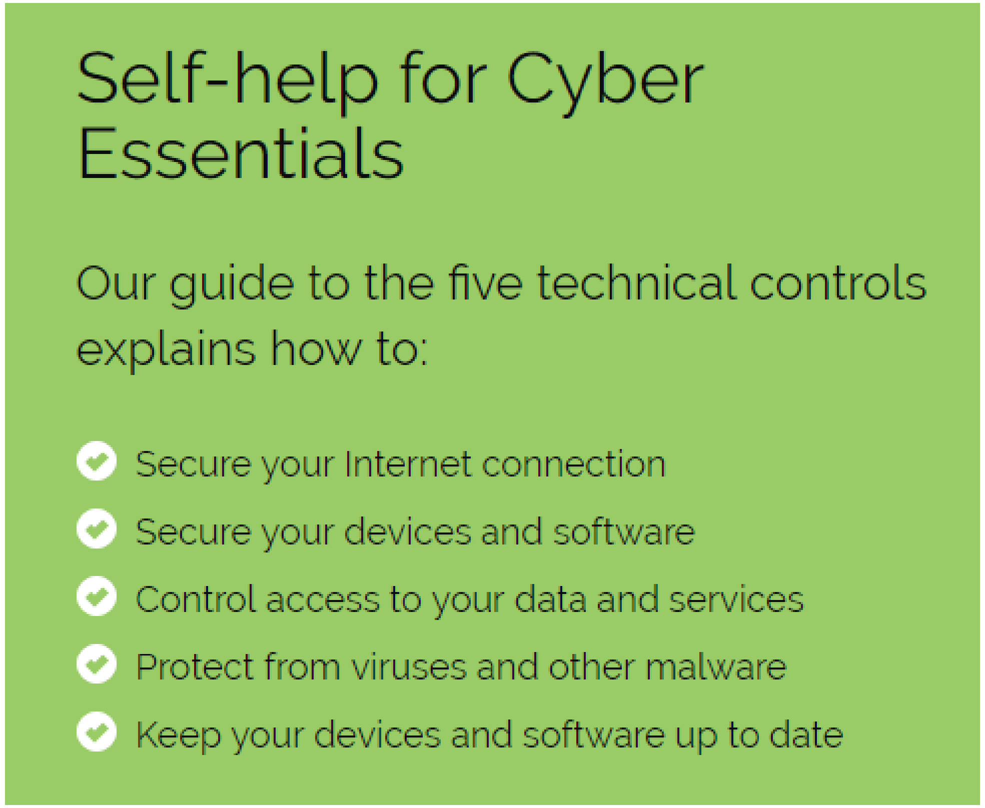
A member of staff who’s been with you for 10 years leaves your organisation.

Risks?

Mitigations?

Cyber Essentials

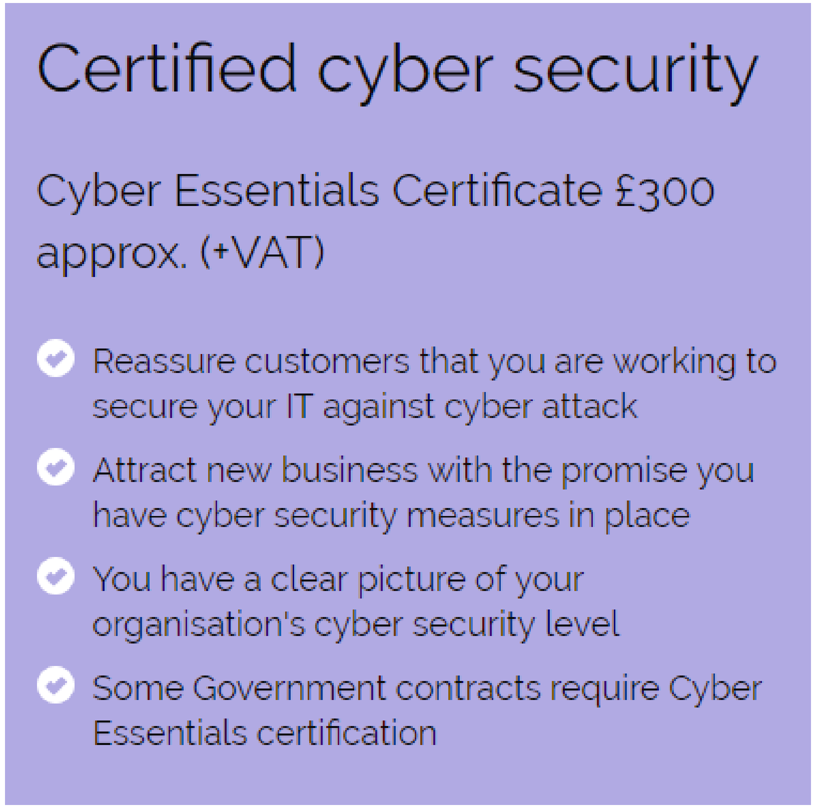
- Govt backed scheme - https://www.cyberessentials.ncsc.gov.uk



Self-help for Cyber Essentials

Our guide to the five technical controls explains how to:

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



Certified cyber security

Cyber Essentials Certificate £300 approx. (+VAT)

- ✓ Reassure customers that you are working to secure your IT against cyber attack
- ✓ Attract new business with the promise you have cyber security measures in place
- ✓ You have a clear picture of your organisation's cyber security level
- ✓ Some Government contracts require Cyber Essentials certification

National Cyber Security Centre

Stay Safe Online

Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand why you might be vulnerable to cyber attack, and how to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

Who is behind cyber attacks?

Online criminals

Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.

Foreign governments

Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.

Political activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.

Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.

Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.

Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.

Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings, and think about what you post.

Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.

Phishers often seek to exploit 'normal' business communications and processes. Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.

Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.

Secure your devices

The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.

Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.

Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for an attacker to exploit a device if it is left unlocked, lost or stolen.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.

If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option. 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

Reporting incidents promptly - usually to your IT team or line manager - can massively reduce the potential harm caused by cyber incidents.

Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

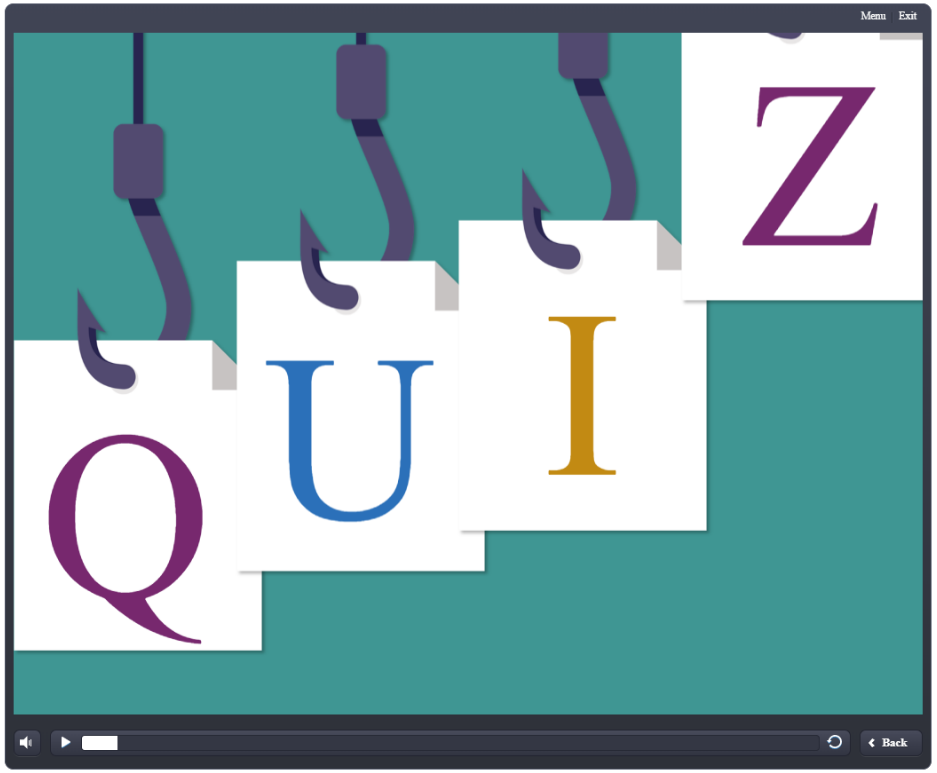
Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.

www.ncsc.gov.uk @ncsc National Cyber Security Centre

NCSC's new cyber security training for staff now available

The NCSC's new e-learning package 'Top Tips For Staff' can be completed online, or built into your own training platform. www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html



superhighways

harnessing technology for community benefit

Useful GDPR links

info@superhighways.org.uk

www.superhighways.org.uk

@SuperhighwaysUK