VOLUNTARY
ACTION
CAMDEN

# Introduction to Cybersecurity Guide

## Cyber Essentials – what is it and why does it matter?

https://www.ncsc.gov.uk/cyberessentials/overview

### What is it?

- Government industry backed scheme to help UK organisations improve their awareness of cybersecurity and guard against threats. It offers self-help, online guidance about threats; as well as some resources, templates and frameworks, which can be downloaded or accessed online.
- Essentially, Cyberessentials defines a set of standards based on best and recommended IT practice.
- Certification (i.e. an independent assessment that you meet the standard requirements) is available to organisations who need or want to prove they are meeting the standards.
- Certification is required for some government approved contracts; some funders may also request you have it before releasing funds.
- Even if you don't certify it, it is still important to adhere to the standards.

### Key Standards

#### Administrator Privileges

- One of the most important standards is about **separation of administrative privileges from standard user accounts.**
- Admin accounts should only be used for administrative purposes e.g. ability to make changes to the system itself: downloading / updating software, creating new users, registry changes etc.
- If you work under a system admin profile, then attacks that do find their way into your systems can affect the whole computer as as an administrator can write to core portions of the computer that are out of bound for a standard user.
- If users are set up with a standard profile, this helps limit how far an attack can penetrate through your systems, as any major changes would require administrative privileges, and these changes are blocked from running automatically under a Standard account.
- You can avoid a lot of damage by setting up staff under a Standard Profile and setting up a separate Administrator profile for administrative only purposes.

### Minimum Access

- This is also an important standard and dovetails with the above guidance on user accounts.
- **You should only give each person the access they need to do their job**
- **Extra permissions should only be given to those who need them** (and understand the responsibilities and risks that come with the additional permissions).

## Maintenance and updates

- Over time, software and hardware becomes out of date. The provider may release updates to fix it, or they may bring out new products and stop providing updates for older products.
- For example, Windows 7 came to its 'end of life' in January 2020 which means updates are no longer released by Microsoft. If this is the software you use (or earlier editions such as Windows XP or Vista) then your system is vulnerable to attack.
- Similarly, Office 2010 is no longer supported by Microsoft.
- Flash is also redundant and should be removed from all computers.
- Outdated software, whether you use it or not, could become a risk.
- Hackers and criminals will look to exploit vulnerabilities through outdated software.
- Windows 10 updates should be installed unless there is good reason not to. They can be set to run automatically in the background.
- **Updates exist to fix bugs or vulnerabilities in the system.**
- **Software should always be kept up to date, removed if not used any more or replaced with the latest version.**
- Get help from your IT support if you need the software but it can't be updated.

## Backups

### Copying vs. Backup

- Copying files is not the same at all as a backup!!
- Copying is as it sounds – it literally copies what you have from one pace to another.
- Backing up should create multiple complementary copies of your data, which would enable you to recover all of your data to the point of the last backup if the worst happens.
- Use proper backup software where possible.
- Most products available are ok for basic backup. E.g. Windows 10
- For increased resilience you can add another external backup drive.
- For bigger organisations with software in the cloud you should look at alternatives.

### Windows 10 Backup

- Windows + I
- Find a setting > Backup

### Cloud to cloud back ups

If you have more than 10 staff then it is recommended to use proper back up software

- **Idrive** – Inexpensive and simple to use, but only useful for basic needs.
- **Sharepoint** – Pricing varies on two things – how much data you have, number of mailboxes

- OBM, from VSL (aka Vitanium Systems Limited) is the more robust one, particularly recommended for Sharepoint and 365 mailboxes. That's the one which costs around £70 + VAT per month on average, but prices vary according to the amount of data and the number of mailboxes.

### Testing Backups

- Your IT support company can help with this but if you don't have one then:
- Testing your backups is essential. It is also advisable to check that you can restore from the backup.
- Check your backups weekly, i.e. make sure you get a confirmation from your software that it has worked, but also try a test restore at least once a year, to make sure you are actually able to use those backups.
- External drives have a useful life of about 4-5 years. They should also be tested regularly to make sure the drive is still functioning.
- Take the drive and plug it into another machine to see if you can see it in the list of devices.
- Do not format it.
- If it is not visible in disk manager. Some drives are configured not to be assigned a drive letter by default., then it should be replaced.

## Anti-virus and Firewall

Antivirus and firewall are not the same thing!!

### Antivirus

- Antivirus is an application or software which provides security from the malicious software coming from the internet. An antivirus generally performs three actions:
  - Detection
  - Identification
  - Removal
- Antivirus deals with both external threats and internal threats.
- The best anti-virus at the moment is Kaspersky (1st) and Bitdefender Gravity Zone (2nd best). Kaspersky get near perfect scores from all independent testing labs.
- Some discounts may be available for Bitdefender Gravity Zone through Charity Digital Exchange. This is a platform for registered charities to purchase discounted software and applications.
- There are cheaper anti-virus solutions out there but they do not score as highly as the above recommendations.
- You can also download the free version of Bitdefender. This isn't as good as the paid for version but is still better than some paid for products.
- Any antivirus is better than none.
- Windows Defender is not as good as Bitdefender but it is better than nothing.
- **Everybody should have anti-virus installed on their system and it should be updated regularly.**
- **You should only have one anti virus product on your system.** The best products will scan everything they come onto contact with. Only one system should do this otherwise the

system will grind to a halt. You may have a dormant Anti-Virus running in the background but if not used it is best to uninstall it.

### Firewall

- A firewall is a hardware or software devices which filters network traffic according to pre-defined rules. Most antivirus products contain a software firewall. So does Windows. So does your router. A firewall will protect you against most worms (a type of virus which moves along network nodes) but it will do nothing to protect you from other forms of malware, e.g. crypto lockers, password stealers, etc. which are more prevalent these days. To protect you against those, you need a proper antivirus.
  A firewall monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Firewall will do nothing to protect you from other risks like malware, ransomware.
- Most anti-virus software contains a software firewall – along with Windows 10 and your internet router.

### Antispam filters

- Most spam filters do not include anti-virus scanning, therefore the tool to protect you for spam will not protect you from viruses.
- Anti-spam filtering is usually the job of your IT support people or email provider.
- If you publish email addresses on your website or in auto-response emails, then this is likely to result in spam.
- Some anti-virus products also utilize spam filtering.

### In Summary

- Alertness is the best defense.
- A good antivirus is not the same as staying vigilant.
- Even if you tick all the boxes for cyber essentials you still have to be alert and on top of the risks.

## Managing Risk

- Training, supervision and appraisals can help embed cybersecurity within your organisation.
- Most charities may not have a budget for training staff on cyber security but there are some good free resources that can help (see below). These are really a starting point.
- Training should be provided for any stakeholders using IT systems, including staff, trustees and volunteers.

### Training

- https://www.ncsc.gov.uk/training/cyber-security-for-small-organisations-scorm-v2/scormcontent/index.html#/
- https://www.ncsc.gov.uk/collection/charity
- https://www.youtube.com/watch?v=i0iLy8racHIS

## Policies and Procedures

- It is important to have policies and procedures in place so you have a framework to know what or what not to do in the event of a cyber-attack.
- This helps to show that you understand what the cyber security risks are and how to mitigate them.
- Depending on the size of your organisation and complexity of your IT configuration, you may have several policies, or they may be incorporated into one single IT Policy. Common policies include:
    - Acceptable use of IT
    - Password policies
    - Bring Your Own Device (BYOD)
- You can download our template for small organisation if you need a basic policy.
- You can also find template policies online if you need something more detailed.

## Multi-Factor Authentication

Is where you receive a code on your phone, email or via an authenticator app to double check you are who you say you are. You will be asked to enter the code into the system you are logging into so it can verify you are the right person.

- Can help to prevent unwarranted access to systems. However:
    - Most small charities don't do this.
    - It can be a little bit over the top for some people – particularly if on a personal device.
    - Not a bad thing to have, except that criminals know that people have to do this so it becomes another route for them to target you.
    - If you opt to receive messages by SMS (or us ean app based authentication) and your device is inaccessible or stolen, you may not receive your code and will not be able to access the system you were trying to get on to.

## Password Policies

The question of how often to change a password is a balancing act of risk.

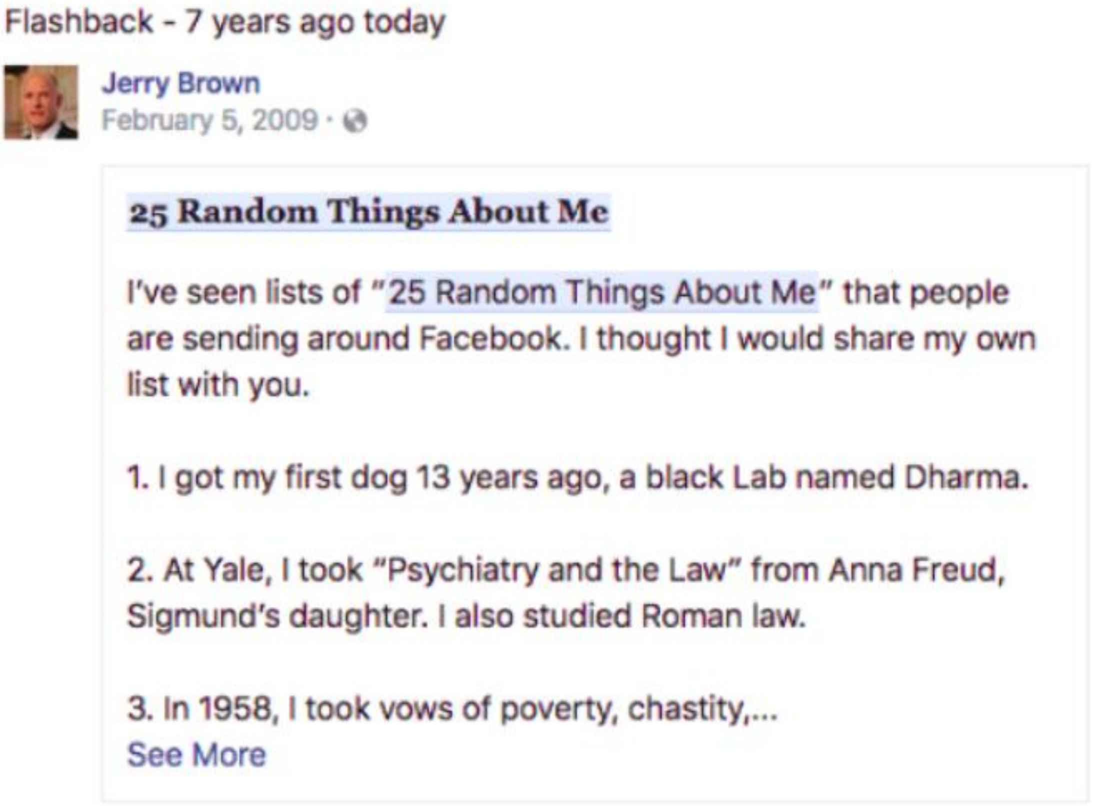
- **Very important to have different passwords for different systems.**
- It is less important to change the password frequently if you do use multiple passwords.
- The risk of changing the password too frequently is that people will end up using the same one over or writing it down!
- Writing the password down in a coded way that only you understand is ok.
- Password managers can help you keep track of your passwords, but they rely on you having your password manager available on the device you are using. If this is stolen and the gain access, it is a bit of a double edged sword.
- If you are certain that the device is secure then these are quite good.

    - Keypass.
    - Dashlane
    - Lastpass

# The 2021 threat landscape

## Social Engineering

- "Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps."
- Research is usually put in to this e.g. Looking up on Facebook, e.g.  names of children, checking websites for details of staff e.g.  finance coordinator, name and email.
- It isn't a huge leap from working out someone's name, to then find their email address and username; or name of a child and year of birth for the password.
- Be careful of questions, quizzes and surveys on social media asking for personal or security information. This is likely to be the first part of a targeted attack



Flashback - 7 years ago today

Jerry Brown
February 5, 2009 ·

**25 Random Things About Me**

I've seen lists of "25 Random Things About Me" that people are sending around Facebook. I thought I would share my own list with you.

1. I got my first dog 13 years ago, a black Lab named Dharma.

2. At Yale, I took "Psychiatry and the Law" from Anna Freud, Sigmund's daughter. I also studied Roman law.

3. In 1958, I took vows of poverty, chastity,...
See More

## Common Fraud

- Often involves some back and forth between the hacker and the target as well a sense of urgency.
- Might start with simple request then progress to more sophisticated ask e.g. to make a purchase, change bank details etc.
- Less common attack but damage can be significant if you inadvertently make payments to the fraudster.
- Anti-virus won't protect you from fraud.
- These attacks are getting more sophisticated.

- You need to be able to recognize this type of email for what it is. Prevention against this also involves having strong finance protocols which cannot be bypassed by anyone under any circumstances. If something looks a little odd, check the originating email address, call the person on the phone. Always check the real destination of links by hovering your mouse cursor over them. **But above all, follow protocol and stay attentive.**

- You should have strong financial policies and procedures to prevent attacks like this circumventing your normal processes, particularly around changing bank details, supplier details or changes to payments.

**Example**

1. User receives an email asking them to do something e.g. click on this document, image, some sort of link.
2. User clicks on the link which takes them to a fake website or similar asking for their details.
3. The user enters their credentials.
4. Now the hacker has stolen the username and password!!
5. From here they can recreate your mailbox profile and get into your account and start causing problems e.g. creating rules to divert emails from your attention to a hidden folder, changing bank details, copy your contacts and attack them too.

## Spoofing

- This is where an email address pretends to be from the genuine person, but on closer inspection, the email address is wrong and did not originate from the genuine contact.
- It is easy to change the display name of who an email is from but less easy to hide the actual email domain.
- In Outlook, you can check the email headers to see if is genuine:
- To check, the email: Open the email, file > properties > look for hidden sending address.

### How to read a URL

- A URL consists of a **Protocol**, the **Host and Domain Name** and the rest of the path:
- https://jobs.theguardian.com/
- the hostname (jobs.theguardian.com) consists of more than just the domain name (theguardian.com) and people's ignorance of how to read that can be exploited by criminals, for instance by registering the domain name "jobsinlondon.com" and creating a website which includes a hostname of theguardian, thus creating a URL of https://theguardian.jobsinlondon.com which many people would think belongs to the Guardian, but has nothing to do with them.

- Https is the protocol here; that always comes first, and is followed by a colon and two slashes.
- Then comes the hostname, which is in between the two slashes of the protocol and the next slash.

- Host names are read by browsers from right to left, and can consist of many parts, separated by full stops. The only parts that matter are the last two parts (or 3 if it's a .something.uk) before the next slash. They are the domain name.

**Example: is this a genuine email from DHL?**

https://DHL.yourparcel.com/deliverytimes

1. Protocl = https://
2. Host = DHL.
3. Domain name is yourparcel.com

The part that really matters is~~ what follows after the Host. E.g.'DHL.'~~. In this case the domain is Yourparcel.com

4. The domain name is yourparcel.com
5. This is not from DHL!!

## What to do if you're unsure

- Never click on a link if you are uncertain it is genuine.
- PAUSE before you get a link asking you to type in your password from a link!
- Hover your mouse over the email address or link to get more information about the domain name and URL.
- Ask questions – why am I getting this information? What are they asking for? Do I know this person? feel comfortable giving this information out?
- If you're still not sure, google the company and check the real domain
- If something looks a little odd then always challenge it – don't just click without thinking.
- Call to verify.

## Spam

- "Unsolicited and email sent in bulk": means that the Recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content.
- Usually trying to sell you something.
- Generally ~~fraudulent~~ but generally not dangerous
- However, some spam does contain viruses!!!

## Phishing

- Tries to trick you into providing information.
- Typical phishing will contain a link (email, image etc.) that looks like a familiar website but is actually a fake.
- The user then enters their details which opens up the way to the actual attacks e.g. encrypting files,
- These are the first step of something that can turn out quite nasty

- Some of these will rummage through your contacts, steal these and then use your email to send out more phishing attacks to your contacts.

### How to spot a dodgy email, phone call or SMS

- May purport to be from a trusted provider e.g. HMRC, BT, your bank.
- Spelling mistakes are a dead give away
- Outdated logos
- Strange jargon
- Adding pressure or a sense of urgency to respond or provide information.
- Asking for personal information, banking information, security info, generic address e.g., dear colleague, or to visit a website should ring alarm bells.

### Pawned Passwords

- You can check if your passwords have been stolen:
- https://haveibeenpwned.com
- 509million passwords stolen in Facebook data breach!!!
- If you always use the same password you should check that they haven't already been pawned.

### Malvertising

- This is usually a pop up on your PC.
- Most browsers have inbuilt blockers.
- Some anti-virus software has this too. Includes a feature that allow feature to block adverts and pop-ups from opening on your PC.
- Notifications can evade AV's as some people may want to receive notifications from websites e.g. Amazon e.g. impending deliveries.
- Use browser setting to stop online notifications.
- Settings > notifications > fine tune which websites can send you notifications.

### Phone malware

- If you have ever installed an app onto your phone or tablet, did you scan it with your phone antivirus first? Do you even have an antivirus on your phone? Most people don't. They rely on the app store scanning the apps for them. However, most phone malware evades the app store's defences by having an initial release without any malicious code. Users install that on their phone. Only later does the malicious code appear in the app, following an update. Phone malware can send SMS messages, make in-app purchases etc. It is particularly nasty.

## What to do in the event of an attack?

This really depends on the nature of the attack; however the following general guidance is useful:

- Files encrypted – restore from back up.

- Passwords – change password
- Financial damage – phone the police and report the scam as fraud.
- Check anti-virus reports / run anti-virus
- Get advice!