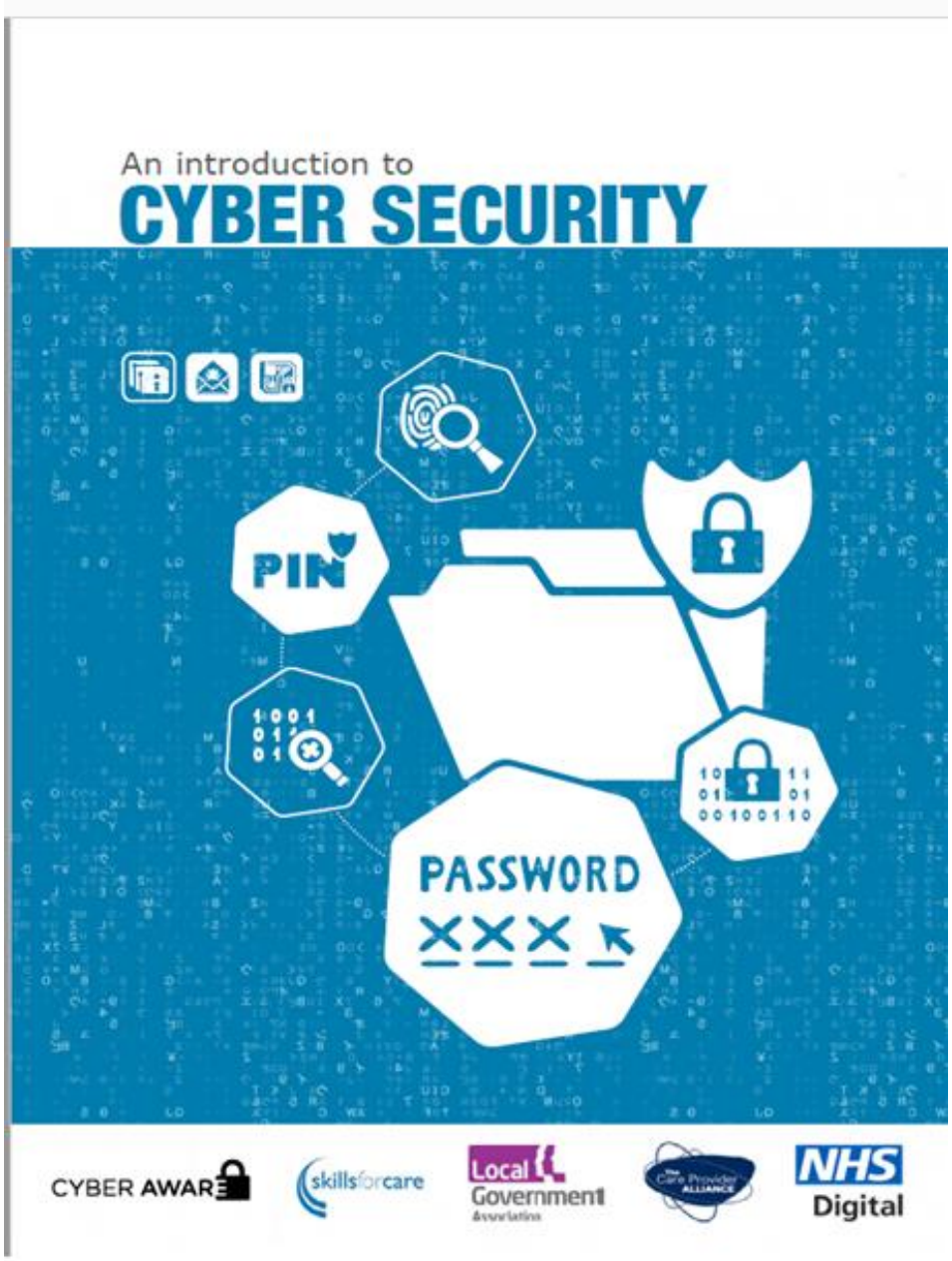
Essentials in Cyber Security.

- What is cyber security?
- How do I make sure I am keeping data safe?
- Who needs to know?
- What do they need to do?
- How can I access learning in this area?

skillsforcare



‘An introduction to Cyber Security’.

Find it here; www.skillsforcare.org.uk/digital

Can also be found on the Care Providers Alliance website.

What is Cyber security?

Cyber security is the name for the safeguards taken to avoid or reduce any disruption from an attack on data, computers or mobile devices.

Security breaches can occur when we use paper records, send information using fax machines and even verbally. However, the consequences of security breaches with digital information are potentially far more severe, as information can be distributed more easily and to a far wider audience.

Attacks are becoming more common.

In a Government Cyber Breaches Survey in 2017, 46% of businesses reported a cyber-breach or attack.

Wannacry ransomware attack, May 2017; At least 6,900 NHS appointments were cancelled as a result of the attack.

BUT investigation found it could have been prevented by following cyber security guidelines (National Audit Office).

9 steps to improving cyber security.

1. MOVE AWAY FROM USING UNSUPPORTED SOFTWARE

This is when software e.g. operating systems such as Windows, apps, web browsers, etc. are no longer updated by the supplier. Although the software will continue to operate, it will no longer protect against online threats through updates or patching (a software update, often relates to improving security).

2. ALWAYS DOWNLOAD AND INSTALL THE LATEST SOFTWARE AND APP UPDATES

Software updates are designed to fix weaknesses in software and apps which could be used by hackers to attack your device. Installing them as soon as possible helps to keep your device secure.

3. RUN UP-TO-DATE ANTI-VIRUS SOFTWARE

Your computers, tablets and smartphones can easily become infected by small pieces of software known as malware. Common types include viruses or spyware and ransomware. To help prevent infection, install internet security software, like anti-virus and/or anti-malware on your devices and keep it up to date.

4. USE STRONG PASSWORDS (and don't share them).

Passwords should be easy to remember and difficult to guess.

Use 3 random words to create a strong password.

Passwords should not be shared on written down somewhere easily accessible.

5. DELETE SUSPICIOUS EMAILS AND AVOID CLICKING ON UNKNOWN ATTACHMENTS OR LINKS

Delete suspicious emails and do not click on links or open attachments in these emails before you delete them as they may contain fraudulent requests for information or contain links to viruses. If in doubt, check verbally with the sender that the email is genuine.

6. BACK UP YOUR DATA

You should therefore safeguard your most important data by backing up to a secure external hard drive or storage system based in the Cloud. You should also ensure you regularly test your back-ups and, if you are saving confidential data off-site e.g. the Cloud, follow all appropriate data protection measures and government standards and guidance that relate to health and social care organisations.

7. TRAIN YOUR STAFF TO BE CYBER AWARE

Make sure staff are trained to know the benefits of operating digitally, but are also aware of cyber security threats and how to deal with them.

8. MANAGE SECURITY RELATIONSHIPS WITH SUPPLIERS AND PARTNERS

As your organisation grows and works with more suppliers and partners, you become a link in one or more complex supply chains. If you use third-party managed IT services, check your contracts and service level agreements, and ensure that whoever handles your systems and data has security controls in place.

Improving awareness and safety within your organisation.

- Consider gaining Cyber Essentials certification.
- Consider the role of the Data Security and protection toolkit.
- Consider policies and procedures; what is in place if there were to be a cyber attack? Is it fit for purpose? Is everyone aware of it?

Improving awareness and behaviours of your staff (at all levels)

- Access and implement awareness training for all.
- Make cyber awareness just one of the many aspects of keeping data safe (see http://www.skillsforcare.org.uk/Documents/Topics/Digital-working/Information-sharing-collection-and-storage-guide-1.pdf)
- E-lfh level 1 course; free to social care employers. Supports the DSandP toolkit but can be used outside of this.

E-Learning for Health; level 1 Data Security and awareness module.

Access to e-LfH content; available to all social care professionals in England whose employers are registered with the Skills for Care National Minimum Data Set for Social Care (NMDS-SC). (*others routes to access are available.)

Every employer providing NMDS-SC workforce information to Skills for Care has been given a user registration code for their staff. This code enables them to self-register for access to e-LfH resources.

For information about registering an organisation with the NMDS-SC the employer should access www.nmds-sc-online.org.uk or contact the Skills for Care Support Service on 0845 8730129.

Help and guidance is available.

- ‘An introduction to Cyber Security’. LGA, NHSd, Skills for Care, CPA.
- Cyber aware website; https://www.cyberaware.gov.uk/ (The National Cyber Security Centre)
- Get Safe on Line website; dedicated section for businesses https://www.getsafeonline.org/business/
- Information Commissioners Office; https://ico.org.uk/
- NHS Digital; has a Data Security Centre which has live reporting on cyber security threats in health and care. By going to the website, anyone can sign up to receive updates on the latest threats. https://digital.nhs.uk/cyber-security