An Introduction to Cyber Security

Version 5

Published
First published: 01/12/2017 Last updated: 27/08/2019
Author:
Keith Strahan

1. FOREWORD

Thank you for taking the time to read this guidance, which has been written for Care Providers and for anyone else who would find it useful.

It has significant contributions from many, including the Digital Social Care team and the National Cyber Security Centre.

For extra information about cyber security, the guidance includes links to a variety of web pages from government approved organisations e.g. Stay Safe Online: Top Tips for Staff Infographic.

If you have feedback about the websites used in this guidance, please contact the organisation concerned.

2. TECHNOLOGY AND BENEFITS

There are fantastic benefits to embracing technology and working securely online in health and social care.

Technology can enhance integration and enable greater and faster information sharing. This allows us to improve the quality of care and support provided. Examples include,

- Personalised care planning
- Transfers of care
- Viewing medications, etc.

The individuals we support can also fully participate and have better access and input into their records.

However, as we use technology more, we must continue to do all we can to keep people's information safe and secure. Particularly, ensuring that disruption to care and support at best is avoided or that any disruption is minimised.

3. WHAT IS CYBER SECURITY?

Cyber security is how individuals and organisations reduce the risk of cyber-attack, whether on computers or mobile devices. It covers not only safeguarding confidentiality and privacy, but also the availability and integrity of data. This is vital for ensuring the quality and safety of care and support.

Implications for Citizens

The National Cyber Security Centre's first UK Cyber Survey in April 19 showed 42% of citizens in the UK expect to lose money to online fraud. Moreover, the key findings from the survey show only 15% know a great deal about how to protect themselves from harmful activity.

This is why all citizens should be aware of basic cyber security safeguards for personal use from the time they start using the internet. The same applies when participating in the management and coordination of their care and support.

Implications for Care Providers

Security breaches can occur in many ways including 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. This is because substantial amounts information can be distributed more easily and to a far wider audience.

The impact of a cyber breach or attack can be significant and costly: there's the time lost through having to fix your website or systems, the potential loss of customers, damage to your reputation and all the other potential consequences of a hacker getting their hands on your data.

According to the Department for Digital, Culture, Media and Sport's Cyber Breaches Survey 2019, 32% of businesses and 22% of charities have identified breaches or attacks. Among these organisations, the most common types of breaches or attacks are:

- Phishing (scam) emails (80% of businesses and 81% of charities who experience breaches or attacks)
- Others impersonating their organisation online (28% and 20%)
- Viruses or other malware, including ransomware (27% and 18%).

This is why cyber security is a high priority for business and why all staff must be aware of how to implement protective measures and know what steps to take if a cyber incident take place.

4. IMPROVING CYBER SECURITY

Cyber security is a constantly changing area and sometimes can seem quite confusing. However, there are many effective and relatively simple steps that can be taken to protect information and protect you and your organisation. Taking some simple actions and practising safe behaviours will help reduce the risk of falling victim to a cyber-attack.

The most important steps to improve online security are ensuring you:

A. INSTALL THE LATEST SOFTWARE AND APP UPDATES

Over time, software e.g. operating systems such as Windows, also apps, web browsers, etc. may no longer be updated by the supplier.

Although the software will continue to work, it may no longer protect against online threats. If a security weakness is discovered, software can be compromised and become vulnerable to a cyber-attack.

The global ransomware attack in May 2017, which in the UK particularly affected the NHS, reminds us all that it is worth taking necessary precautions. Many organisations whose systems were infected had unpatched or unsupported operating systems. However, whether organisations had patched their systems or not, taking action to manage their firewalls facing the internet would have guarded organisations against infection.

However, for benefits to be gained from up-to-date security measures, only use supported software on your systems and devices. This includes downloading and installing software updates as soon as possible as it will help keep your devices secure.

You can set desktops, laptops, smartphones and tablets to automatically install software updates when an update is available. You can choose to install updates overnight or you can set your device to automatically update when you are connected to Wi-Fi.

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

Your computers and mobile devices can easily become infected by small pieces of malicious software, often called malware. Common types include viruses or spyware and ransomware.

To help protect your organisation, install internet security software, like anti-virus and/or anti-malware on your devices and keep it up-to-date.

C. USE STRONG PASSWORDS

Passwords should be easy to remember and difficult to guess.

Recent analysis outlined by the National Cyber Security Centre found that 23.2 million victim accounts worldwide used 123456 as a password! It's also a good idea not to use words such as your child's name, pet's name or your favourite sports team. This type of information might be easily viewed on your social media page e.g. Facebook. Numbers and symbols can still be used but it is advised that three random words is the key to creating a strong password.

Use a strong, separate password for your email and other important accounts. This means if hackers steal your password for one of your less important accounts, they cannot use it to access your most important ones. This includes your main email account. Hackers can potentially use your email to access many of your personal accounts and find out personal information. If this is your bank details, address or date of birth, you might be left vulnerable to identity theft or fraud.

For your most important accounts, if it's available, you should use Two-Factor Authentication. This means involving a second step after entering your password e.g. providing a fingerprint, using Eye/Face identification, answering a security question, or entering a unique code sent to your device. To find out how to enable Two-Factor Authentication on your online accounts visit TurnOn2FA

Remember – always keep your passwords secret

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

Email is an excellent communication tool but is frequently used to deliver unwanted or unwelcome material. This is often referred to or spam or junk email. At best this is annoying and at worst it can be malicious, causing considerable harm to your computer and organisation.

Delete suspicious emails. Do not click on links or open attachments in these fake emails as they may contain fraudulent requests for information or contain links to viruses.

A phishing email is a scam where criminals typically send fake emails to thousands of people. Do not respond to them even if they seem to come from a company or person you may know. Responding can confirm that your address is legitimate to the sender. If you're not sure if an email is genuine, try calling the sender on a phone number you know to be correct.

E. BACK UP YOUR DATA

If your device is infected by a virus or accessed by a hacker, your data may be damaged, deleted, stolen or even held to ransom. This means you won't be able to access it. 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. in the Cloud, follow all appropriate data protection measures and government standards and guidance that relate to health and social care organisations.

F. PROTECT MOBILE DEVICES (AND TABLETS)

Mobile devices (including smart phones and tablets) are increasingly being used by care providers to access and manage care data. These devices are now as powerful as traditional computers, and as they leave the safety of a fixed working environment, they often need additional protection. There are a number of steps you can take to protect mobile devices and tablets:

- Switch on screen lock protection – Make sure mobile devices are locked when not in use, for example with a suitably complex PIN or built-in fingerprint scanner.
- Make sure lost and stolen devices can be tracked, locked or wiped – Staff are more likely to have their tablets or phones stolen (or lose them) when they are out and about. Fortunately, many devices have free web-based tools that are invaluable should a device be lost or stolen.
- Keep devices and apps up to date – Just like a 'desktop' computer mobile devices and apps need to be kept up to date to ensure that critical security updates are applied.
- Only connect to trusted Wi-Fi networks – when you use public Wi-Fi hotspots (for example in coffee shops), there is no way to easily find out who controls the hotspot. If you connect to these hotspots, somebody else could access or what you're working on whilst connected your private login details.

Some care providers allow staff to use their own devices to access and manage data. A Bring Your Own Device (BYOD) approach can increase flexibility and reduce costs when compared to providing devices for staff.

However, it also creates several legal and security risks and issues that need to be carefully considered and managed. Thought should be given to what data can be accessed from the device, how that access is managed, and agreeing a policy with staff for the use of personal devices for work purposes.

G. 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. Due to the rapid development and changes in digital technology it is a good idea to add cyber security to your annual training plans.

The National Cyber Security Centre has produced a new e-learning training package. It's free and takes less than 30 minutes to complete. The Stay Safe Online: Top Tips for Staff training is primarily aimed at small and mediums sizes organisations, charities and the voluntary sector, but can be applied to any organisation, regardless of size or sector. You can either direct your staff to the NCSC website, or if you have your own online learning portal you can easily integrate it into it.

H. MANAGE SECURITY RELATIONSHIPS WITH SUPPLIERS AND PARTNERS

As your organisation grows you become a link in a supply chain; a network consisting of an organisation and its suppliers to produce and distribute a specific product or service to the customer.

Being a desirable, trustworthy organisation or suppler includes observing good practice (and in many cases, compliance) when it comes to cyber and information security. If good practice is not followed, it may not only place your own organisation at risk, but also others within the 'supply chain'.

If you use third-party managed IT services, check your contracts and service level agreements. Ensure that whoever handles your systems and data has security controls in place.

One way to demonstrate that you have the security controls in place is to undertake a basic assessment and achieve a Cyber Essentials certificate. You can ask your suppliers to do the same.

5. RESOURCE LIBRARY

The information below lists some of the organisations who offer advice about the best ways to protect devices and data.

Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cybercrime. You can report it and/or phone 0300 123 204 if you have been scammed, defrauded or experienced cybercrime.

Cyber Aware

The Cyber Aware website aims to support simple secure online behaviours to help protect themselves from cyber criminals. It is delivered by the Home Office alongside the National Cyber Security Centre.

Get Safe Online

The Get Safe Online website provides practical advice on how to protect yourself and your business. There is also a Jargon Buster.

Information Commissioner's Office (ICO)

The ICO is a UK independent body set up to uphold information rights. It provides access to official information and guidance about topics such as GDPR.

National Cyber Security Centre (NCSC)

The NCSC site is the authority on cyber security and has some useful advice and guidance and resources.

NHS Digital

NHS Digital is the national information and technology partner to the health and social care system. Its systems and services include the Data Security and Protection Toolkit and NHSmail. Its Social Care Programme commissioned this guidance and the Digital Social Care website.

SASIG

The Security Awareness Special Interest Group (SASIG) is a subscription-free networking forum. Its aim is for professionals to be able to safely and freely exchange views and concerns about the issues of cybersecurity. Membership includes hundreds of organisations from all sectors; public and private.

Take Five

Take Five is a national campaign that offers advice to help everyone protect themselves from preventable financial fraud.

APPENDIX 1

The Department for Digital, Culture, Media and Sport's Cyber Breaches Survey 2019 outlined organisations experience of breaches in the last 12 months: