Cyber security guidance for those using their own IT devices

When using your own personal computer and email account to look after volunteers' and members' data, it's important to follow these guidance steps to prevent data breaches of security.

- ✓ Don't ignore software updates - they contain patches that keep your device secure. If you're prompted to install any, make sure you do.
- ✓ Always lock your device when you're not using it and use a PIN, password, or fingerprint/face id. This will make it harder for an attacker to exploit a device than if it is left unlocked and lost or stolen.
- ✓ 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 If you don't have a password to access your home computer, it's important to set one up. Make sure your passwords are strong - using three random words together is a good way to ensure this.

  And of course, never share your passwords with anyone else, or use the same password multiple times.

- ✓ Password protect key documents. Make sure that any electronic files that contain personal data are password protected or put somewhere secure so only people that need them can access them.
- ✓ Make sure all electronic files that contain personal data are properly deleted when no longer needed, for example, deleted from both the hard drive and recycle bin. This is important to ensure you're adhering to UK GDPR regulation too.
- ✓ Use Multi factor authentication (MFA). If you use email accounts such as Yahoo or Gmail, there's functionality to increase the protection of your account. The main benefit of MFA is that it enhances the security of your account by requiring anyone wishing to access your account to have more than a username and password. When you sign into your online accounts - a process we call "authentication" - you're proving to the service that you are who you say you are. Traditionally that's been done with a username and a password. Unfortunately, usernames are often easy to discover and sometimes people tend to pick simple passwords, or use the same password at many different sites.

  That's why almost all online services - banks, social media, shopping have added a way for your accounts to be more secure. You may hear it called "Two-Step Verification" or "Multifactor Authentication". When you sign into the account for the first time on a new device or app (like a web browser) you need more than just the username and password. You need a second thing - what we call a second "factor" - to prove who you are.

- ✓ Using social media - Beware of who you are engaging with on social media, you may never be certain of a person's identity or intentions. Criminals may use publicly available information from social media and other websites to appear convincing.

  Review your social media privacy settings, and think about what you post on online. Criminals take a lot of time researching their victims and the organisations they work for to gain a lot of information about them before launching their scams.

- ✓ Be vigilant if you visit a website that is declared "untrusted". If a web browser states that you are about to enter an untrusted site, be very careful – it could be a fake website that has been made to look genuine. Google may display a red padlock or a warning message stating 'Your connection is not private'.

- ✓ If you have inadvertently responded to a phishing email:

  The most important thing to do is not to panic. There are number of practical steps you can take: Open your antivirus (AV) software, and run a full scan. Follow any instructions given. If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk. If you've been tricked into providing your password, you should change your passwords on all your other accounts.

- ✓ Make sure your AV product is turned on and up to date.

  Windows and iOS have built-in tools that provide suitable AV. Make sure your AV software is set to automatically scan all new files, such as those downloaded from the internet or stored on a USB stick, external hard drive, SD card, or other type of removable media.

- ✓ If you receive a phone call offering help to remove viruses and malware from your computer, hang up immediately (this is a common scam). If you think your computer has been infected, open your AV software, and run a full scan. Follow any instructions given. Set all software and devices to update automatically, including your AV software.
- ✓ New computers often come with a trial version of additional AV software. You may want to carry out your own research to find out if these products are right for you. You should consider replacing devices that are no longer supported by manufacturers with newer models. You can search online to see how long your current device will be officially supported.
- ✓ When disposing of your electronic device ensure that any personal data held on it is entirely deleted before you dispose of the device and the device is securely disposed of. If you are disposing of your device but not destroying it, ensure that you have deleted the charity's data from the folder in which it was kept and the recycle bin to which it is moved when you deleted it from the original folder.

- ✓ When people receive emails, the 'To' and 'CC' (carbon copy) fields at the top will show who else has received the email. This may pose a problem when ensuring you're keeping people's data safe.

  If you send emails to people using the BCC (blind carbon copy) field, instead of the 'To' or 'CC' fields, people receiving the email will not be able to see the people it was sent to, so keeping everyone's data safe.

  In one example of the repercussions of failing to BCC an email sent to multiple recipients, the ICO fined a public enquiry £200,000 for failing to 'BCC' an email, thereby identifying possible abuse victims. The fine would nowadays be far higher, following a change in the penalties.

  Volunteers' most common data breach is failing to BCC the email addresses of multiple recipients of an email. So, remember, when emailing multiple recipients, before you press 'Send' check recipients' email addresses are in the BCC box in the header (unless the recipients already have each other's contact details e.g. members of a committee or group who are regularly working together and communicating via email and/or those who are listed in the members directory).

All data breaches must be treated seriously, for example if personal data we hold is stolen, lost, destroyed or seen by an unauthorised third party, we have an urgent responsibility to investigate the breach and to report a serious breach to the Information Commissioner's Office (ICO) within 72 hours. Please let the Principal Officer know if you are concerned about a data breach sarah.barker@ceagm.org.uk

Spring 2024