STANDARD PRECAUTIONS

Following the steps below will help in minimising the risk of a cyber-attack and, in particular the risk of misappropriation of the practice's finances:

1. Secure your computer and keep it up to date

Security software is essential, regardless of what you use your computer for. Ensure all computers in the practice (PCs, file servers, and mail servers) are protected by trustworthy internet security **business** products and are using the latest updates. Consumer solutions (paid or free) are not sufficient to provide adequate coverage and visibility for the security of your business. Also, ensure you have a firewall turned on.

Ensure that your operating system and all other software are up-to-date to ensure that there are no security holes present. You should also ensure that the software is update automatically/regularly so that it is maintained up to date.

2. Backups

It is essential that regular backups of all data are taken, preferably on a daily basis. You should also ensure that you backup to different locations, such as the cloud and an external portable drive. Ensure that you disconnect the external drive after backing up on every occasion.

Regularly check to ensure that your backup is working and its integrity is maintained.

3. Avoid clicking through emails

The majority of cyber-attacks originate with phishing emails. These e-mails either request that you respond directly or include infected attachments that will, if opened, install malware onto your computer.

Ensure that you open and close each email individually, rather than flicking through them, so that you can ascertain whether the email is from a trusted source before opening it.

Be skeptical of unexpected emails, particularly those with attachments. If in doubt, do not open the email and contact the sender to ensure its veracity.

Remember, financial institutions will not send you an email asking you to provide any of your login details. If you receive an email that appears to be from your bank that asks for such details then treat it with suspicion as it may well be a phishing attempt to trick you into handing your credentials over.

Likewise, be aware of links in emails that appear to be from your bank – this is a trick often employed to get you onto a website that looks like your bank. When you log in to 'your account' they will steal your username and password and, ultimately, your money.

It is always safer to access your online bank account by typing the address into your browser directly rather than following a link.

Also, be aware of unsolicited phone calls that purport to be from your bank. While your financial institution may require you to answer a security question, they should never ask for passwords or PINs (they may ask for certain letters or numbers from them, but never the whole thing).

If in doubt, do not be afraid to hang up and then call your bank back via a telephone number that you have independently confirmed as being valid.

4. Create a strong password

Ensure that you use strong passwords. A different password should be used for every account and should be changed regularly. The best way to achieve this is by making it long and a mix of upper and lower case letters, numbers, and special characters.

Consider using passphrases instead of passwords, for example: “androids dream of electric sheep” can be converted into a passphrase as “@NDR()!DSdmofecSH33P”.

Always avoid using any common words or phrases and never create a password that contains your name, initials, or your date of birth. Also, do not write down your passwords or store these in a document on the computer.

When setting up online banking, if your bank asks you to provide answers to some standard security questions remember that the answer you give does not have to be the real one, so make it something else, as if it was a password. Use a password manager if you are concerned about how to remember everything!

5. Train employees

Educate your employees on the dangers of opening files from unknown sources.

Educate your employees on how to verify hyperlinks by hovering over the hyperlink and checking the file path before clicking – this is particularly important for websites that do not use the 'https://' protocol (look for the padlock icon on your URL bar),

Ensure that all employees are aware of the risks and the steps outlined above to decrease the level of risk involved.

6. Access/Hardware/Encryption

Ensure that staff only have access to files which they require access to. If a member of staff leaves the practice ensure that their account is closed and their access rights are revoked. Also, ensure that inappropriate websites cannot be accessed from the practice's systems.

Try to adopt a system that will eliminate the use of removable media such as USB memory sticks and minimise the use of e-mail attachments. If required, ensure that the removable media and e-mails are scanned for viruses and malware. Ensure that unapproved devices are not connected to the practice's system.

Consider encrypting any information stored on removable media devices or any external device. Ensure that any files containing confidential data are secured before transferring to or from the practice's system.

7. Risk Management policy

Ensure that an appropriate risk management policy is put in place. Ensure that all staff are aware of the policy and that any breach of it is considered a disciplinary matter. Cyber security and the associated risks should be on the agenda for each management meeting, where the effectiveness of the procedures implemented and the degree to which staff are adhering to the controls are reviewed.

A plan should be put in place to identify the resources that will be needed in the event of a cyber security attack. The practice should also consider the repercussions of an attack for the practice and its clients, so that any loss of trust is kept to a minimum.