Dental Good Practice Guide – How to avoid Malicious software

Background

This guide has been written in response to there being a number of Malicious Software incidents within Dental Practices.

Malicious Software is the generic term for computer Viruses, Trojans, Spyware, Worms and so on. These infections can cause a significant amount of damage and can be very costly. Vital data can be lost, business processes can take longer due to down time as well as financial penalties for breaches of the Data Protection Act 1998 involving loss of Person Identifiable Information.

Using antivirus software such as McAfee, Sophos and Kaspersky with the latest “Virus Definitions” is still important, but this alone is not enough to prevent being infected with malicious software. Antivirus software only works once an infection has been captured in a lab and a “Virus Definition” has been produced. This definition is like an antibody and enables the infected computer to identify and quarantine the infection.

Malicious Software that has not been analysed and a definition produced for it is called a “Zero Day”. New malicious software is very common as cyber criminals use it to run very lucrative illegal businesses. A type of Malicious Software called “Ransomware” can encrypt all your data and then demand a ransom that you might have to pay to get your data back.

Malicious software can also obtain your personal information enabling a criminal to steal your identity, or turn your computer into a “Zombie” which can be used by a criminal to commit crimes without your knowledge.

Malicious Software infections are common and many using an infected computer do not even realise they are infected, however the risk of being infected can be significantly be reduced by following some good practice guidelines.

Internet

Browsing the internet (Surfing), and just visiting an infected website can be enough to get your computer infected, as malicious software can be embedded in the web page and placed on your machine as you browse. However, inappropriate and non-work related websites are much more likely to be infected than legitimate work related ones.

Examples of inappropriate websites include those offering illegal / copyright content such as free movies or MP3’s, where the links that you click on may start a malicious software download. To reduce the risk of infection from websites of this type, it’s important to keep work and personal internet use separate, by not using the internet for personal use at work.

- Only visit appropriate work related internet sites, keep it for work purposes only
- Do not visit inappropriate websites which offer illegal / copyright content
- Do not use internet browsers such as “TOR” which is commonly used to anonymise users access to inappropriate websites or the “Dark Web”
- Be mindful of the risk of inadvertently visiting inappropriate websites, particularly when searching for streaming audio / video or downloadable content

Email

Email is another potential source of infection. This is referred to as Phishing, where a person with malicious intent will send out emails, disguised to be legitimate but in actuality contain files or website links designed to steal information or install malware.

Take care when receiving email that you are not expecting or from a sender that you don't recognise, and never open an attachment or follow a website link unless you are confident about the origins of the email.

Cybercriminal's can easily craft an email that contains legitimate company logos and appears as if they came from a person that you know, so always be wary.

- Disable the use of macros in MS Office/Excel or applications (if possible disable macros for all users at an enterprise level via "Group Policy" – which your IT Supplier may be able to setup for you)
- Keep work email for work purposes only
- Do not click on links or open attachments within emails where you are unsure of its origins
- Beware of phishing and other scam emails which use scare tactics in order to get you to click on a link, for example "your account has been frozen, click on the link and login to re-enable"

Work & Personal Devices

Mixing devices for work and personal use increases the risk of malicious software spreading to work systems and affecting your ability to complete important activities.

If you use a laptop for example, it is advisable you have one laptop for work and one for your own personal use. The same can be said for other equipment such as Smartphones and USB memory sticks etc.

- Ensure that you have separate devices for work and personal use

Social Networking & Passwords

Some cybercriminals are able to obtain usernames and passwords from hacking into services such as Facebook or Twitter. High profile hacking cases with customer data stolen includes TalkTalk and Ashley Madison. If you use the same password for work as you use for things that you access on the internet you increase the likelihood of a criminal having the credentials to access your work account. As well as stealing your password criminals can guess your password by repeatedly entering similar or random password combinations until they get the right one. Just like you look after the key to your home you should look after your password by;

- Creating a password that you can remember easily so you don't have to record it anywhere, but avoiding using a password that someone could easily guess

- Password should be strong using letters, numbers and special characters (!"£$%) and should be at least 8 characters in length

- Use a different password for work and personal use, and for your own safety use different passwords for websites across the internet, and never reuse internet banking passwords on other websites

- If you do need to record your passwords somewhere, use a secure alternative for managing accounts and passwords through the use of a password manager application

System / Software Configuration & Maintenance

In addition to what you can personally do to avoid malicious software there are also a few things that you can ask your IT supplier to help implement.

File shares

File shares enable infections to spread, these are connections that you have to another computer or server storing computer files. To reduce the risk of cross-infection, access to file shares on other computers or servers should be restricted to only those required to enable practice systems to run and for you to complete normal business activities.

- Ask your IT provider to identify any computer / server file shares, and remove any that are not required

Note: Care should be taken when amending / removing file shares as in some cases these may be used by practice systems

Vulnerabilities & Patching

Malicious software exploits vulnerabilities present within useful and legitimate software such as Microsoft Windows, Adobe and specialist dental related proprietary software you may use.

A vulnerability is a weakness which has previously not been identified, either during the software's original development (creation) or after the software has been updated to add additional features / functionality.

As most modern software is made up of millions of lines of computer code it is impossible for software developers to identify all these weaknesses before the software is used by the customer. To address this problem, once a weakness is identified a fix called a "Patch" is issued by the software developer, however patches are only created for software that is still supported, for example Microsoft no longer supports and provides patches for Windows XP and as a result Windows XP is considered vulnerable and should not be used.

Once weaknesses have been identified and patches created by the developer, these should be installed onto your computers and servers as soon as possible to reduce the likelihood of infection.

- Ask your IT provider to regularly deploy system and software patches
- Ask your IT provider to identify unpatched / unsupported systems and software
- Only obtain software from legitimate sources who can offer continued support
- Only allow software to be installed by staff who have been specifically authorised and trained, or ideally your IT provider
- To prevent the installation of illegitimate software, remove "Local Administrative Privileges" on Practice PC's
- Ensure that you have automatic, regular, reliable off-site backups which support document history and versioning
- Sensitive data such as Person Identifiable Information should be encrypted wherever it is stored, whether local PC, Server, Practice system or Cloud Service such as Microsoft Office 365

Note: Care should be taken when updating / patching systems and software, as specific software versions and/or patch levels may be required in order for practice systems to operate