IT Security Tips for Healthcare

Reading time:
Jayson Nagpiing
Last Modified on 06/05/2024 9:33 pm AEST

All healthcare practices deal with sensitive information and almost all store information electronically. Local GP and dental practices face similar risks as other small businesses, the repercussions may be more severe given the amount of sensitive information they hold.

Ransomware has become a much higher risk for small businesses compared to large businesses that may be better able to defend attacks. Ransomware is a type of malicious software that can infect a computer and is designed to block access to a system until the victim pays a cyber criminal a fee. A ransomware virus can infect a computer when it is inadvertently downloaded through a web browser from a malicious website or when opening an attachment in a malicious email.

To protect your healthcare practice and your patients review your IT security and ensure you have software and procedures in place to protect your computers. Here are MIPS' top 10 tips for healthcare practices to protect their computers.

#Tip 1 – Install anti-virus protection

Even if you are a small practice and you think the risk is low, this is essential. Companies such as Symantec and MacAfee provide software you can purchase online. You can also download free software such as AVG or Avast, both of which offer premium products you can upgrade to.

#Tip 2 – Protect sensitive data

If you are storing patient records in files, ensure you have a software system that is password protected. Additionally, if you use a cloud computing service, check where it is hosted as you may be in violation of the Australian Privacy Principles if you are storing sensitive information outside of Australia and it is not securely stored. You should also ensure you have a back-up procedure in place. This is not only essential should records be damaged but should you fall victim to ransomware or another virus, you can delete records to purge the virus and recover records from your backup.

#Tip 3 – Manage your passwords properly

The best approach is to never write your passwords down but if you have to then use a password management application such as Dashlane, LastPass, Zoho or Sticky Password to assist you. Avoid duplicating passwords for any sites but especially key sites such as your Gmail and Facebook as these are common hacking targets.

Avoid ‘dumb’ passwords such as ‘password’ or ‘pass123’ and keyboard patterns such as ‘qwerty’ as hackers use libraries of common passwords to access systems. Including two uncommonly linked words combined with a mix of upper and lower case letters, number and special characters can make a strong password, for example ‘High Beast’ could become Hi12GHbea&*sT.

#Tip 4 – Always use ‘automatic updates’

Windows and Mac operating systems are set by default to download automatic updates. You should leave this on and do the same for other software to ensure you download and install security updates. Any vulnerabilities that are identified in software are often patched quickly by suppliers such as Microsoft and Apple to ensure their customers do not fall victim to viruses or hacking. It’s best to take advantage of this and update frequently.

#Tip 5 – Add two-factor authentication

Two factor authentication is an added layer of security for logging in to online services or executing online services. Generally, this means that in addition to your password you will be asked for an additional piece of information, for example, your mother’s maiden name or a pin number sent via SMS to your mobile. Two factor authentication is available for online banking, My Gov and other websites.

#Tip 6 – Get a professional

Whether it's establishing a network or reviewing your security sometimes it pays to get a professional in rather than trying to do it all yourself. IT firms can provide on demand services charged by the job or hour to assist. Some may charge a monthly retainer (more suitable for larger practices) while others may be contracted for jobs as you go.

#Tip 7 – Keep your wits

It's sounds simple but it's often the human element not the technology that is the weak spot in a healthcare practice's security. Clicking malicious links in unsafe emails or downloading free software from websites are common ways for viruses, malware, Trojans or bloatware to infect your computer. Training yourself and your staff to identify unsafe emails and avoid unsafe downloads is good practice.

#Tip 8 – Careful what you plugin to your computer

If you connect a phone, flash (thumb) drive or portable hard drive to your computer ask yourself whether you trust the device and if you know anything about where it's been? For example, if it's your friend's phone and you know they are frequently online visiting bizarre websites, perhaps it's inadvisable to connect the phone to work PC. Viruses can be easily transferred once devices are plugged in.

#Tip 9 – Realise you are a target

In the modern world you don't need to be a bank, military installation or NASA to be the target of a hacking attempts. Hackers routinely hack Gmail, iTunes and other personal accounts to try and scrape email addresses and personal information such as credit card numbers from your account. The 'it won't happen to me' attitude can land you in strife.

#Tip 10 – Protect your devices

Whether it's a phone, tablet or PC you should ensure there is a pin, password or other security mechanism to prevent intruders from using your device if it is lost or if someone other than yourself tries to access it. When walking away from your work PC, it is advisable to lock it to prevent other people from accessing information, eg patient records.

Other quick tips

- Ensure the firewall on your PC is activated (this is a default feature of Windows and Mac operating systems)
- Consider refreshing your passwords intermittently, between 30 and 180 days depending on the sensitivity of the service or information it protects
- Read your emails with suspicion before clicking or replying

If you have any questions regarding your membership, please contact MIPS' 24/7 Clinico-Legal Support and Advice line on 1800 061 113.

Related articles

CAREER LEADERSHIP PROGRAM >