8 Simple Steps for Securing your Community Pharmacy

The HSE ransomware attack is no longer dominating the news but the HSE is still feeling its aftereffects. Despite being given a decrypt key for its data, it will cost the HSE at least €100m and months of work to restore its systems. Of course, the HSE has support from the exchequer and access to expert help. Small businesses including community pharmacies do not have these luxuries, so prevention is especially important.

Simon Woodworth BSc MSc PhD
Director, MSc in Cyber Risk for Business, Cork University Business School

Step 1: Operating System fully licenced and up to date

All your PCs should be running Windows 10. Windows 7 is out of support. This means that if a bug is discovered in Windows 7 and Windows 10, then only Windows 10 will be patched. As the bug and patch have been made public, this makes your Windows 7 system even more vulnerable because an exploit is much easier to develop. Note that is it possible sometimes to upgrade to Windows 10 using your existing Windows 7 license key.

Step 2: Software fully licenced and up to date

All your pharmacy, accounting and office software should also be fully up to date and fully licensed. This ensures that you receive all the necessary patches and bug fixes when available. Pharmacy PCs should NOT be used for any purpose other than business and staff should not have admin privileges to install new software or change settings.

Step 3: Antivirus installed

At minimum you should have Windows Defender switched on and up to date. This provides adequate protection, but you may prefer your own antivirus product. There are many to choose from and some are free, so do some online research and pick one that suits your business. Don't have two antivirus products installed and running at the same time.

Step 4: Mind your accounts and passwords

Every user should have their own account and passwords for login to any application should be secure. In general, passwords should be at minimum 12 characters long and contain small letters, capitals, numbers, and symbols. These can be very hard to remember, though. Try coming up with longer passwords made up of 4 words strung together, which make a scene that you can recall easily. Never pick a password that contains personal or work-related information.

As mentioned in Step 1, most users do not need and should not have admin privileges. This limits the damage an inexperienced staff member can do to your systems, and it can also limit the damage a virus or malware can do if accidentally downloaded.

Step 5: Secure your router and network

No customer should have access to your network. Make sure you change the default username and password on your broadband router. If you offer customer WiFi, it must be kept separate from your business WiFi and LAN. Your router may support such a setup. If not, adding a second cheap router and connecting it to your network via its WAN port will provide a simple way of keeping customers away from your business data.

Step 6: Make backups

Your pharmacy most likely uses online applications that back up your data elsewhere. Check that this is the case. For your local files and applications, consider backup up to a USB drive that can be removed from the premises. Alternatively, subscribe to a cloud backup service like Microsoft OneDrive or Google Drive. Remember that all backups should be tested regularly, otherwise they may let you down.

Step 7: Don't click that link!

This step and the next are all about staff awareness. First, never click on a link on an unsolicited email or an unfamiliar website. This is how ransomware attackers gain access to your systems. It's much easier to fool a member of staff into doing something silly than hack into your computers. For similar reasons, avoid plugging in USB drives unless you are absolutely certain it is from a known trusted source.

Step 8: Beware of scams and frauds

Small business can be particularly vulnerable to invoice fraud. This is where a fraudster submits a fake invoice for a known supplier, with different bank details. Always check the bank details are those originally provided by the supplier from a legitimate email or postal address. Beware of other phone or email attempts to extract banking or personal details. Never provide passwords or PIN numbers over the phone.

In conclusion, there are a number of technical steps you can take to make your pharmacy secure and to greatly reduce the risk of damage from a cyberattack. However, technical security solutions are worthless unless staff are properly trained on the safe use of the computers in your business. They need to be very aware of potential scams and frauds. Securing your pharmacy properly will build trust with your customers and suppliers.