Keeping your Pharmacy IT Safe from Attack

The catastrophic attack on the IT systems of the HSE and the Department of Health may have happened as a result of one of the hundreds of thousands of members of staff innocently clicking on a link in an email.... just think about that.

How many times have you received an email and opened it without checking the sender's address? Or clicked on a link, or opened a file or a photograph without stopping to think?

The repercussions from the cyber attack on 14th May are still being felt throughout the Irish healthcare system and the frightening thing is that IT experts say that it was a case of 'when', not 'if'.

Pharmacists are particularly vulnerable to cyber attack, and the devastating consequences that it could have on your business and your patients. Your IT systems are at the very heart of the way that you work, holding everything from confidential patient details, dispensing histories, and the mechanism whereby you submit your monthly claims to the PCRS. Many also contain staff details, wages details and information about your business bank account.

Enhanced Anti Virus

Should you be the unfortunate recipient of a cyber attack like the one experienced last May and you do not have enhanced Anti Virus measures in place there is often very little you can do to retrieve your vital patient data. We currently provide Antivirus software to the majority of our customers but the attack on the HSE systems has shown that this will not prevent systems from being compromised from a virus that has never been seen before. We have sourced an enhanced type of Antivirus, which notices changes in behaviour patterns and not just previously identified viruses, this is known as EDR (Endpoint Detection and Response).

EDR uses machine learning and artificial intelligence to track potential threats and acts to remediate and even roll devices back to their pre-attack state—delivering results with both speed and accuracy. This solution can allow for the infected device to be disconnected from the network, minimising the risk of all other systems becoming compromised.

As we believe that this EDR antivirus is greatly superior to other AVs on the market place, we have pushed this out to every single one of our customers who sources their AV from us. This is being offered free of charge for the first six weeks of deployment, until 30th June 2021. In the event that McLernons customers decide NOT to continue with this enhanced level of protection from a cyber security attack, they are asked to email 'ITSecurity@mclernons.com' before 1st July 2021.

There are no 100% guarantees when it comes to protecting against a cyber attack, but each additional measure that you take will increase your overall protection.

Increasing IT security

Although we are your Pharmacy IT systems partner, you are responsible to ensure that all the IT systems operating in your business are done so in as safe a way as possible. We can help, advise and recommend steps that you should take to minimise the risk but ultimately the responsibility vests in you.

As a bare minimum, we recommend that all pharmacies have a robust firewall, a proven back-up system and have upgraded their hardware from obsolete and out-of-date systems, such as Windows 7 machines, which have passed their end of life and may be supported – at an additional cost by you – in a very limited way.

We recently contacted all our customers who were still relying on Windows 7 systems to run their business and look after their patient data, and are happy to give further information to those wishing to upgrade to Windows 10.

We will be sending out further information and advice on improving the cyber security of your pharmacy, and advising of the steps that we are taking as your IT business partner to help strengthen your pharmacy systems but if you have any queries please do not hesitate to contact us on 'ITSecurity@mclernons.com'.

Do you do any of the following on your pharmacy systems?

	Y	N
• use a 'free' email account?	☐	☐
• access other websites on your MPS system?	☐	☐
• use default passwords for all systems and staff?	☐	☐
• fail to regularly change these passwords?	☐	☐
• Use unsupported Windows 7 systems?	☐	☐
• Have no or inadequate antivirus?	☐	☐
• Lack a firewall?	☐	☐
• Have an open Wifi?	☐	☐
• Fail to train your staff on how to recognise cyberattacks?	☐	☐

IF YOU HAVE ANSWERED YES TO ANY OF THESE, THEN YOUR IT SYSTEMS ARE AT RISK FROM CYBER ATTACK, AND CONTACT US IMMEDIATELY ON 'ITSecurity@mclernons.com'