Data security to keep your veterinary practice safe

As the reliance on technology and electronic data continues to grow, veterinary offices are becoming more vulnerable to cyber security threats.

Many veterinarians believe that their business isn't at risk, when in fact, many hackers specifically target small veterinary offices because they believe that smaller businesses may not have the veterinary software in place for proper security. The other attractive factor is that there is potential access to a large amount of data that includes names, addresses, credit card information and even banking information.

Having a strong, reliable antivirus software is only the tip of the iceberg to protecting your most important asset– your client and patient data. Are you familiar with the different types of viruses and attacks that can happen to veterinary businesses — ransomware, spyware, and malware, just to name a few?

While these attacks can vary in severity, each one can compromise your veterinary practice and patient data, potentially causing downtime for your business. In fact, according to a study by Gartner Group, 43% of businesses were immediately put out of business by a major loss of computer records, and another 51% permanently closed their doors within two years. Knowing what to look for can help you prevent a data breach and ultimately protect your client records, so we've broken down a few of the most serious attacks that can impact your business so that you can take the necessary steps to avoid them.

P / 855-478-7920
E / Marketing.GSS.NA@covetrus.com
W / softwareservices.covetrus.com

covetrus

Spyware

Spyware is often associated with software that displays advertisements (adware), or software that tracks personal or sensitive information. Spyware can impact your computer by pushing additional advertisements, collecting personal information, and even changing the configuration of your computer. To protect your computer from spyware, avoid clicking on advertisements that seem too good to be true.

Malware

Malware is hidden within documents that are sent through spam email attachments or inside .ZIP files attached to emails. Once attachments are opened, the malware burrows into your computer, often creating an email which is then forwarded to your entire contact list. The best way to prevent a malware infection is to delete emails from people you don't know or to avoid opening attachments unless you know the sender.

Ransomware

Ransomware is a very serious attack that prevents you from running your computer. In most cases, the criminal encrypts your files completely (patient data, documents, spreadsheets, and images) and asks for a monetary fee to provide you with a key to unlock the encrypted files. Your best option may seem like paying the monetary fee, but actually, it's as simple as reverting to a backup of your data.

How do you protect yourself against these various forms of viruses? Take a look at your existing network security. Do you have an antivirus software? What about a data backup service? We never think about increasing our security until it's too late. Having a reputable antivirus software doesn't always translate to protection. Backing up your database is key to ensuring that if your files become corrupted, you don't lose data and can get your practice back up and running.

If you have a data backup solution in place, you can restore your data quickly and easily. We offer data backup services that work with your AVImark, ImproMed, RoboVet, and Rx Works software to store your data remotely and protect it against loss.

For more information or to sign up, call 855-478-7920 or email Marketing.GSS.NA@covetrus.com

P / 855-478-7920
E / Marketing.GSS.NA@covetrus.com
W / softwareservices.covetrus.com

covetrus