Ransomware attacks on the increase;

over 400 percent during Covid-19 WFH guidance

3 ways to avoid a ransomware attack

People who have never experienced a data or security attack routinely say the same thing time and time again, "*We don't have any valuable data, why would a hacker want to attack us*?" The issue is that hackers are not specifically targeting you or your practice. They are targeting the whole health care profession. And, YES! This includes veterinary practices as well.

According to a CNBC article, "*Cyberattacks now cost companies $200,000 on average, putting many out of business.*" More than half of cyberattacks that happen daily occur to small businesses. Only 14 percent of these businesses are prepared to handle the attack. Here are two questions to ask yourself:

1) Does your business have fewer than 500 employees?
2) Does your practice do less than $10 million in revenue each year?

If your answer is yes to both these questions, then you are considered a small business and a target for a cyberattack. Here is another scenario.

1) Does your practice provide health care services? (Yes, this includes animals.)
2) Does your practice store your client and patient information?
3) Does your practice name contain the following words? Hospital, clinic, medical, care or practice?

If your answer is yes to these questions, you ARE in the highest statistical category to be attacked by cyber criminals. Here are two staggering statistics. From an article written by the AVMA "*Cybercrime a potential liability for clinics,*" the author states that cyberattacks are projected to cost businesses $6 trillion annually by 2021! There are reasons that hackers go after the entire healthcare industry, including veterinary practices.

1) Is your practice paper light or paperless?
2) Do you collect and store PII (Personally identifiable information)?

Hackers target the entire healthcare industry because most practices can answer yes to both questions above. Aging equipment and a lack of general concern about cyber security make for a perfect target.

"The veterinary industry is about 10 years behind when it comes to IT infrastructure."

Easy steps you can take to protect your data and records

1) **Use a VPN (virtual private network) service or your practice's VPN while working in public places.**

   If you travel to VMX, WVC or Fetch, make sure to connect to your practice's VPN or use a quality VPN service like NordVPN while on public wifi. This ensures you have a private tunnel that all your communication is sent through, so hackers will be unable to sniff your traffic.

   The same is true for staff working from home during COVID19 or anytime. Be sure to have them connect to your clinic's VPN before performing any work functions. Hackers know that home networks are ripe for the picking too. This is the reason for the over 400 percent increase in attacks since the start of the COVID19 pandemic.

2) **Regularly check your email account on https://haveibeenpwned.com/**

   This site keeps a record of all the databases that have been compromised. If your email account, like most, shows as compromised make sure that you no longer use the same email address and password combination that was used in the compromised site.

For Example:
Let's say my email address, Sarah@vetclinic.com was the email address I used to log into Adobe with the password of Password1! Adobe suffered a massive data breach in October 2013. I would want to make sure that I do not use sarah@vetclinic.com and Password1! anywhere else! It's also a good idea to make sure that your email password has been changed recently.

3) Staff training

This simple task has the biggest bang for the buck. We can invest millions into our cyber security infrastructure, but if we do not train our staff, it is as if the doors are wide open. You've heard the term "We're all human," which means "we all make mistakes." Learning to avoid those mistakes will go a long way to protect practices and private data.

"It is important to conduct some form of cyber security training at least once per year."