5 ways to protect your veterinary practice from cybersecurity scams

When you're running an independent veterinary practice, cybersecurity probably isn't the number one item on your to-do list. It's important to stay on guard. The National Cyber Security Alliance (NCSA) found that 28 percent of the small business owners they surveyed had been through an official data breach within the past year.

Scammers are always coming up with new ways to dupe people. But you can watch for specific signs to avoid becoming a victim of internet fraud. Here are 5 ways to protect your veterinary practice from cybersecurity scams.

1 Be aware of suspicious emails

These communications appear as if they're from a reputable source, such as a bank, credit card company, or online store. They'll typically include messages such as:

- There has been abnormal activity or multiple log-in attempts on your account
- There is an issue with your payment information
- You need to confirm your personal information

Be cautious if:

- There are misspellings in the sender's email domain
- The link shows a different URL than the text says when you hover over it
- The greeting is generic, such as "Dear Sir/Madam" or "Dear Valued Customer"

2 Don't click on links in emails

It's best not to click on links from emails. Instead, go directly to your internet browser to type in the site's address. This ensures that you don't get caught in a phishing attack.

If you're not sure if a communication you've received is legit, contact the company directly before you give out any information or click any potentially harmful links.

3 Change your passwords frequently

Make sure your passwords are complex and different for every site. Try using a password manager to store all your passwords and to generate new ones. That way, you only need to keep track of one password.

4 Enable multifactor authentication

Multifactor authentication means that when a user signs into email, they have to provide more information to access the account. This info could include answering a security question, providing a pass code or responding to a push alert on your mobile device. Contact your email provider to find out how to enable multifactor authentication

5 Contact the authorities

If you do receive a suspicious communication, report it. When you file a complaint with the FBI's Internet Crime Complaint Center (IC3), it helps fight cybercrime. Your complaint may be sent to relevant law enforcement agencies for further investigation.