AVMA LIFE®
Veterinarian Inspired Coverage

AVMA PLIT®
Protecting you through it all

Cyber Crime in the Age of COVID-19:

7 Items Veterinary Practice Owners Should Consider

Viruses aren't the only bad agents threatening businesses in the wake of COVID-19. Cyber criminals are preying on vulnerable business computer networks, now taxed by a smaller workforce and curbside service.

Cyber criminals are studying email correspondences, looking for holes in the way organizations are currently operating. They're finding new opportunities to target vulnerable employers who are now implementing new protocols and procedures.

They're even baiting curious and anxious employees with phony websites impersonating healthcare organizations and then inserting malware into their business network. It is estimated that there are 2,000 coronavirus-related sites created every day, most of them malicious. These sites are targeting states with high infection rates to try to steal information and credentials. Fraudulent emails and text messages from banks or other reputable institutions have become more and more frequent.

As always, a computer network's greatest cyber vulnerability is its own employees. **Veterinary practice owners must be more vigilant now than ever. Follow these seven guiding principles to protect you and your business.**

1 review current IT policies

Organizations should review their current policies regarding remote access, even if your clinic remains open with staff present. Inform employees of the approved technology by your company and the proper ways to use the technology. Implement controls for all transfers of funds, regardless of the size and especially when there has been a change in a process or procedure. Similarly, remind your employees not to share personal or business-related confidential information.

2 use strong passwords

While most clinics are deemed essential and are operating, many veterinary employees access business email or file systems at home using personal phones, iPads and other devices. Ask employees to use more robust passwords now - not “123456.”

3 only visit reliable sites

Teach employees to recognize which websites offer reliable data on the current crisis and ask them to avoid visiting sites on their work devices that aren’t reputable. For COVID-19 crisis updates, instruct employees to visit reputable sites including the AVMA, state VMA, AVMA PLIT, AVMA LIFE, CDC or WHO sites.

4 create a response plan

It’s important to put together a one-page list of internal and external contacts necessary post-breach. Include contacts for law enforcement, all stakeholders – clinic owners, doctors and staff – your cyber crime insurance broker, a privacy attorney and a forensic investigator. Timing and communication post-breach will make or break it for an organization. This one-page list will be key to coming out on top.

5 report immediately

Cyber crimes aren’t reported to law enforcement at the same rate other crimes are, but they should be. The FBI’s Cyber Division works exclusively on these crimes and can provide increased protection when they are reported.

6 perform updates

Security patches should be maintained and updated regularly on both individual laptops and the clinic's network. While simple, this will act as a critical baseline firewall for the network.

7 review your coverages

Do your policies cover "bring your own" device exposures? third-party computer systems that may have interruptions in service? other potential exposures like social engineering?

Looking for more guidance?
Contact a AVMA Trust Cyber Consultant.

AVMA PLIT®

800-228-7548

Get Started

Visit the AVMA Trust COVID-19 Resource Centers

LIFE Resources

PLIT Resources

DISCLAIMER: This document contains only a general description of coverages and does not include all the benefits and limitations found in the policies. Coverages may vary. All reference to coverages are subject to the policy's conditions and exclusions. The insurance policy will form the contract between the insured and the insurance company.

AVMA LIFE® AVMA PLIT®