4 ways to reduce the online risk in your practice
By Clint Latham, Lucca Veterinary Data Security
www.lucca.vet

There is no denying the web browser has become the new operating system. What does that mean in non-tech speak? For years the cyber security world focused on the computer operating system. The primary focus was on Microsoft Windows and Apple's MAC OS X. Web browsing with Chrome, Firefox and Safari are now so powerful that they present a greater security risk to veterinary practices.

With a rise in cloud-based practice management systems, practices now rely almost 100 percent on web browsers to access and manage their data. From a technology management perspective this is great. Cloud-based practice management systems reduce dependency on local hardware. At the same time, it increases web presence and exposure to increasing cyber security threats.

Let's look at some numbers from a report generated by a web protection tool used to protect practices.

Web Security Report < link > Note: best viewed using Google Chrome

In one day, practices average 617,059 web requests. By using a local PiMS (production information management system), such as Cornerstone, Avimark or Infinity, this can be reduced to 308,529 web requests per day. In this 24-hour period, Lucca stopped 4,560 cyber security threats for this practice. These are example of pre-Covid-19 threats. At the start of Covid-19, Lucca saw a 30 percent rise in cyber security threats across all participating clinics. The numbers continue to rise, indicating cyber security threats are increasing.

Here are four steps to implement immediately to help reduce your exposure.

1. **Use unique, strong passwords**

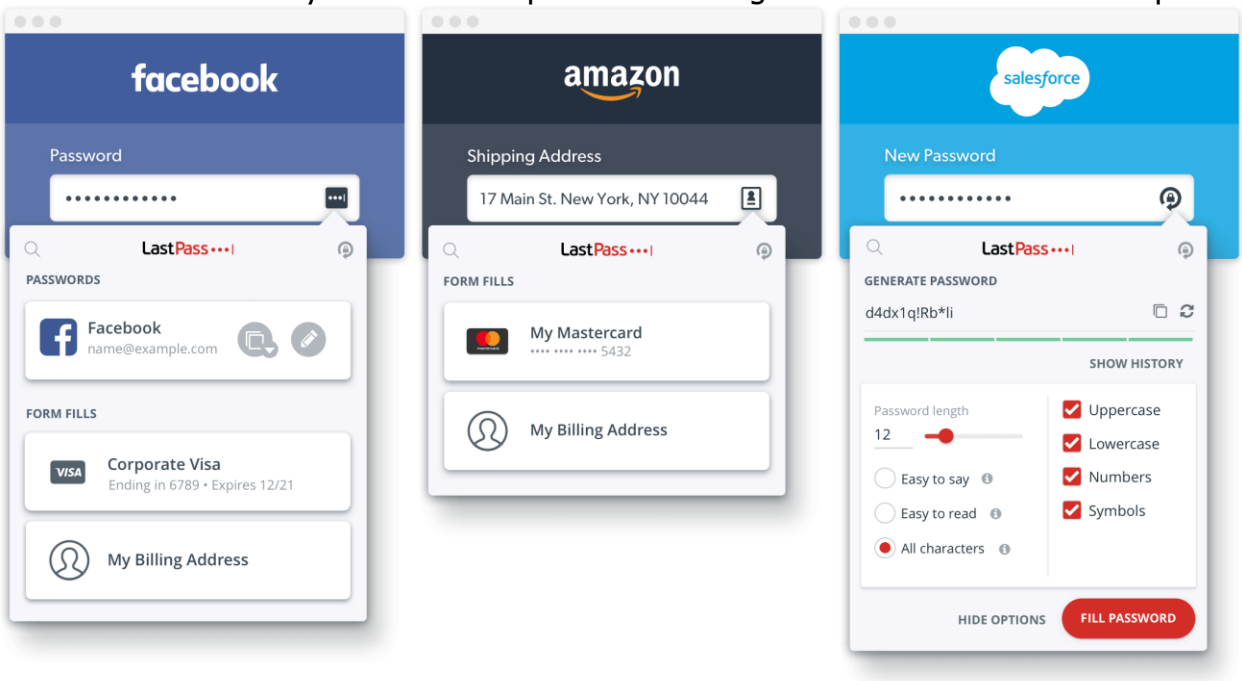
Most practices get hacked having guessable or previously compromised passwords. How many of you use Idex**** as your login to Cornerstone? Or when creating a password, you use the following formula?

Most commonly Hacked Password format: **Welcome1!**

When your password requires one upper case, one number and one symbol, you use the example above. You capitalize the first letter and then add the number one and an exclamation point to the end? This makes for a dream scenario for hackers. By using social engineering or a single crafty email they will be able to get your password. To make matters worse, your password then gets added to black market lists. This allows hackers to automate the hacking process with little to no effort.

2. Store passwords in a password manager

Use a password manager to create and manage your passwords. This is the first step to better internet security. Two favorite password managers are 1Password and Lastpass.



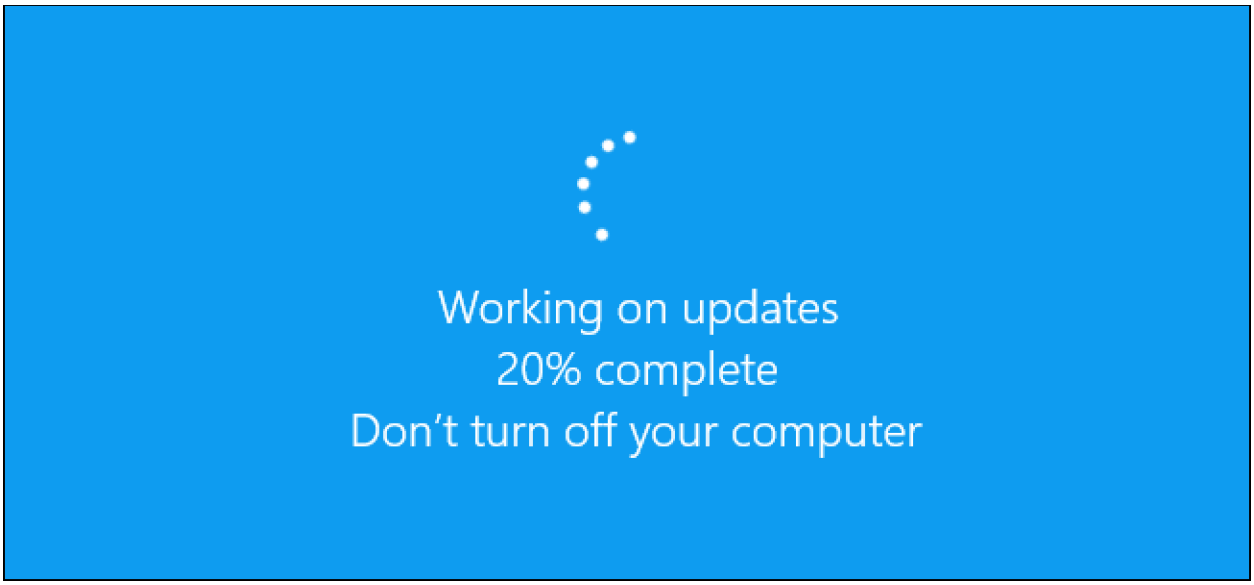
3. Keep your software updated

Software updates for the operating system, web browser and software are the easiest thing to do that have the greatest return. This includes all PCs, laptop, tablets and smart devices. These updates have important security updates to keep you safe.

Keep in mind hackers only need to find one way in. While we are faced with the challenge of finding all possible entry points, there are convenient methods to schedule updates to minimize the impact on your practice including:

- Schedule your Windows updates to run after hours
- Work with your cyber security vendor to schedule application security updates for all applications across your network
- Make sure to use the same applications and versions across all computers

There' is nothing worse than being in the middle of a client transaction when Windows decides it's going to shut down and install updates.



4. Enable two-factor authentication on all critical accounts

For accounts that are mission critical such as email, bank and Quickbooks, enable two-factor authentication, or 2FA. When you sign into one of these accounts, you must enter a one-time code. This code can be generated through an app such as Authy or a simple text message sent to your phone.

Here is an example of how this featured saved me. While traveling to a practice, I opened my laptop to check email. I had been working on some HIPAA compliancy issues for a colleague in human medicine. I received an email from the HIPAA auditor that looked legit. The email indicated he needed to share a confidential document. To access the document, I needed to log in to Microsoft Share point.

This was a legitimate process and something I do frequently. However, one caveat that gave it away as a scam. When I logged into this fake Microsoft Sharepoint account, I wasn't prompted to enter my 2FA code. I had set up the two-factor enabled step on my business email account. Then I was re-directed to a legitimate government form about HIPAA. I thought it was weird he would password protect this doc and was going to call to find out why. Then it happened. I started getting 2FA requests for my email account. Someone was trying to log into my account from Pakistan. Because I had 2FA enabled, they weren't able to do it. I used my password manager to update and create a new complicated password and moved on. Had I not had 2FA enabled on my account I would have been scammed. They would have had complete access to my account and could have created some serious damage.

2FA provided me a safety net for a scam.

If you make a habit of the four simple steps, you can quickly become one of the safest practices on the internet:

- Use unique, strong passwords
- Store passwords in a password manager
- Keep your software updated
- Enable two-factor authentication on all critical accounts

To learn more, request a FREE 30-minute phone consult Click Here