CYBER SECURITY FOR THE OPHTHALMIC PRACTICE

Cybercriminals are highly incentivized to target medical practices

BY CRAWFORD IFLAND

Cybersecurity seems to be in the news on a weekly basis, from breaches to identity theft to massive settlements from companies who have misused or mishandled customer data. Cybersecurity is a hot topic today for good reason: In 2017, 54% of companies experienced one or more successful attacks that compromised their data and/or IT infrastructure.[1]

Anyone who handles sensitive data is living in an increasingly dangerous world. This is all the more true for medical practitioners, for whom extensive compliance requirements, regulation, and penalties for mishandling sensitive patient information have never been greater. According to *Reuters*, patient records can be 10 to 20 times more valuable than credit card information, so there is an obvious incentive for cybercriminals to target medical practices.[2] After all, credit card numbers can be changed overnight, but addresses, employers, insurance documents, and diseases cannot.

What practical steps can ophthalmologists take to secure their practices in the age of daily attacks and extensive regulatory compliance? This article explores how to increase cybersecurity and mitigate risks associated with running a modern ophthalmic practice.

IN YOUR OFFICE

The no-brainer: antivirus software. Whenever multiple computers are connected to the internet and to each other in a business environment, antivirus software is a must. Many ophthalmic practices use Windows PCs, which means they are particularly vulnerable. There are hundreds of thousands of known viruses for Windows, with more surfacing every day. For practices using Macintosh computers, good antivirus software is still important. Software that can recognize threats, malicious files, and the like is incredibly important and an obvious first step in securing your practice.

Separate Wi-Fi networks. Another recommended measure is creating separate Wi-Fi networks for staff and for patients. This is a must when dealing with sensitive health information. Separating your Wi-Fi networks (or not offering in-office Wi-Fi to patients at all) is especially important if any of your diagnostic tools connect to the internet. Recent estimates suggest that one out of four medical devices is

KEY

- **VPN** = virtual private network
- **SSL** = secure sockets layer
- **CDN** = content distribution network
- **2FA** = two-factor authentication
- **DDoS** = distributed denial-of-service attack, an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources

Figure 1. A virtual private network, or VPN, prevents other users from being able to *sniff* your network traffic.

connected to a network, so this is a huge potential liability.

Remember the 2013 Target breach, in which more than 40 million customer credit cards were compromised? The hackers didn't actually target Target itself; instead, they were able to breach the security of the HVAC contractor that Target had hired to work on its systems. The vendor had access to the same Wi-Fi system that Target's point-of-sale machines were on, so when they got hacked, Target's entire system was compromised as well. The hackers were able to obtain millions of customer records in just a few days.

VPN. Beyond having separate public and private Wi-Fi networks, it is also recommended that each computer in your physical office obtain and use a virtual private network (VPN) to further secure network communications (Figure 1). Have you ever used the public Wi-Fi in your local Starbucks to send an email or to access your online banking? Unless you were using a VPN to encrypt your data, anyone else on that Wi-Fi network could theoretically see the information your device was sending and receiving. Say goodbye to that online banking password.

A VPN stops other users from being able to *sniff* your network traffic. Think of it as a tunnel—data are passing through, but they are obscured to anyone trying to look in from the outside. Even if someone were to crack the Wi-Fi password for your main network, he or she wouldn't be able to see any information coming through that network. VPNs encrypt all data, making the data useless and unreadable to anyone sniffing traffic on your network.

Password managers. You've separated your public Wi-Fi and the private network that your office staff uses for billing, electronic health records, and diagnostic devices. What if your office is broken into or physically compromised? One of the most practical security measures the average person can take is to strengthen passwords. Password management software (eg, 1password) is an incredibly easy way to store all of the passwords you use and to reset your current passwords to random, virtually uncrackable alphanumeric strings (Figure 2).

A shared team account is an easy way for office staff to share passwords for your practice's most frequently used online services, including your website, social media accounts, and billing applications. You can delegate access to everyone in your organization or create separate vaults for different teams, giving access only to those who truly need it.

For reference, I tested the password I used to log into my email this morning. It would take a supercomputer about 640 quintillion years to crack. In contrast, it would take only 19 minutes to crack the average American's password. Perhaps it is time to shred the sticky notes littering your office and trade them in for a more secure solution.

ON THE WEB

SSL. If you are serious about securing your practice from data breaches, you also need to consider the security of your website. Although implementation of website security measures can easily escalate to complex solutions, the easiest way to cover your bases is to install a secure sockets layer (SSL) certificate on your website.

SSL certificates encrypt all data sent to and from your website. Even if

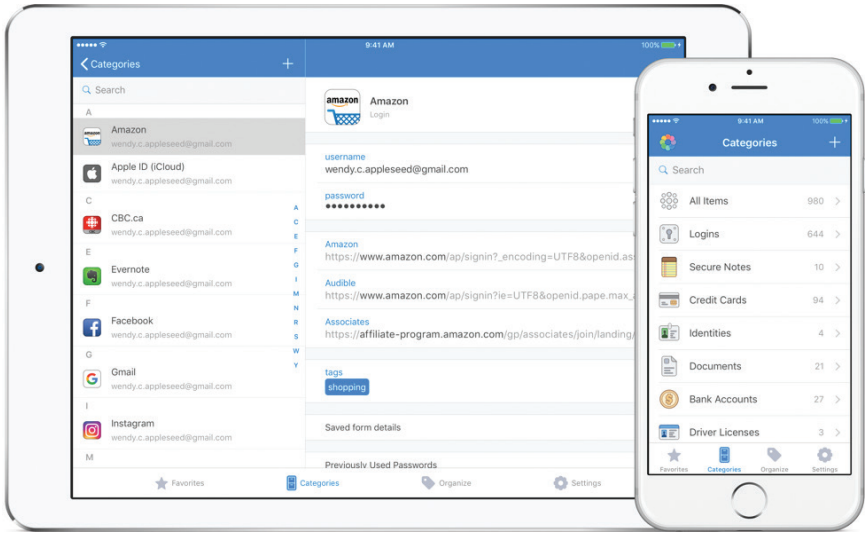

Figure 2. Password management software is an easy way to store passwords and to reset them to random, virtually uncrackable alphanumeric strings.

someone were able to intercept any data sent to or from your website (eg, appointment requests with sensitive patient information), the data would be unreadable. Most SSL certificates cost less than $100 per year, so, if you collect any sort of personal or health-related information on your website, this step is a no-brainer.

CDN. When handling sensitive patient information, security is the primary goal, but what about business goals? What if your website is attacked or goes down unexpectedly? What could the downtime cost your practice in terms of efficiency, lost time, and lost revenue?

Using a content distribution network (CDN) such as Cloudflare can help mitigate this risk. Cloudflare has servers and data centers around the world that can increase uptime for your website and help handle the load, should your website receive lots of traffic or fall prey to a distributed denial-of-service attack. Cloudflare's servers can also help serve your content to users faster and make your website safer and more secure, minimizing the potential for loss due to downtime or attacks.

Two-factor authentication. Two-factor authentication (2FA) is a verification process by which online services require not only a password but also something that you have physical access to, such as your cell phone. Have you ever tried to log into Facebook and been prompted for a six-digit passcode that was texted to your cell phone? That's 2FA at work, and it's much more secure than a traditional password alone.

Combined with a good password manager, 2FA is a powerful way to secure your online accounts and prevent unwanted intrusions. For example, my Facebook password is *D7YCs$jmiahFqpnkGtLiGxvzR*. Go ahead and try to log in. Because I have 2FA turned on, you won't be able to log into my account unless you have physical access to my cell phone (which, last I checked, was in my pocket). The website https://twofactorauth.org is a great resource for finding online services that support 2FA. I strongly recommend combing through the list and turning on 2FA for each account you use, both personally and for your practice.

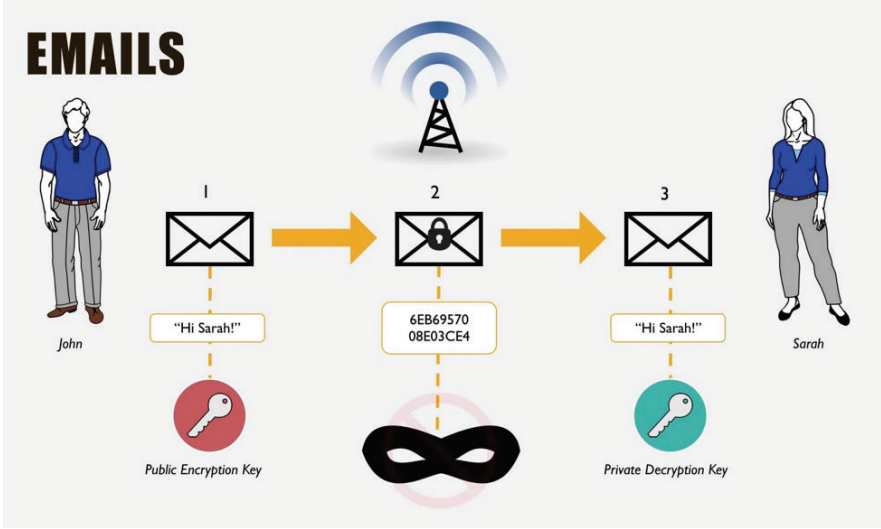

Figure 3. Secure encrypted email server Pretty Good Privacy relies on public-key cryptography to encrypt and secure emails.

IN YOUR COMMUNICATIONS

Encrypted email. What about email communications? How can you ensure that those are secure? There are plenty of HIPAA rules about what a medical practice can and cannot communicate via email, but, if you're concerned that emails may get intercepted, I recommend using secure, encrypted email services such as Pretty Good Privacy (PGP).

PGP is the technology Edward Snowden used to communicate with *The Guardian* reporters who helped him leak secret information in 2013. It is an encryption system that is impossible to crack, and, while it may be overkill for communicating with patients, it is a useful way to encrypt sensitive communications among staff.

PGP relies on a technology called *public-key cryptography* to encrypt and secure emails. Think of it as a mailbox with two keys (Figure 3). One key is used to deposit mail in the mailbox. This is known as your *public key*, and you can give it out to anyone. Tweet it to the whole world if you want or post it on a billboard—it doesn't matter. Anyone in possession of your public key will be able to send you encrypted email that only you can read. The other key is known as your *private key*. You—and only you—should have access to this private key, or else anyone will be able to read your emails.

Secure file upload sites. If patients or business associates need to send you sensitive documents but don't want to rely on PGP, consider using secure file upload sites, such as ShareFile. These file-sharing applications use bank-level encryption and security, so they are incredibly secure ways to share sensitive documents you wouldn't want to fall into the wrong hands.

SECURITY CULTURE

It is worth mentioning that the most sophisticated tools in the world won't help if you don't use them. According to the Ponemon Institute, the chances that your business will experience a data breach are as high as one in four. What's worse, the average cost of a data breach exceeds $3.5 million.[3]

In the WannaCry attack of 2017, global organizations such as FedEx, Nissan, and the UK National Health Service were crippled by attacks that could have been prevented by simple security measures. It's not that these organizations didn't have the resources to combat such attacks; it was the lack of a security-minded culture that led to the cataclysmic results.

The first step in implementing a security practice is to create and foster a security-minded culture. It comes down to your people, your vendors, and the way you conduct business. Although I strongly recommend implementing some or all of the security tactics mentioned in this article, you must walk through the proper use of these tools with your staff. Helping employees and vendors understand why these tools are in use is the best way to ensure compliance and foster a security-minded culture.

Although the suggestions outlined in this article are certainly not an exhaustive list, their careful and successful implementation will place you well on your way to having a more secure ophthalmic practice and extra peace of mind. ■

Disclaimer: Messenger does not claim to be an expert on HIPAA compliance and cannot be held responsible for misuse of this information. Always consult a cybersecurity expert when installing or implementing cybersecurity measures.

1. Crowe J. 10 must-know cybersecurity statistics for 2018. February 2018. Barkly. https://blog.barkly.com/2018-cybersecurity-statistics. Accessed June 30, 2018.
2. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. *Reuters*. September 24, 2014. https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924. Accessed July 1, 2018.
3. Ponemon L. Know the odds: the cost of a data breach in 2017. June 20, 2017. IBM Security Intelligence. https://securityintelligence.com/know-the-odds-the-cost-of-adata-breach-in-2017/. Accessed June 30, 2018.

CRAWFORD IFLAND
- Founder and Creative Director, Messenger: Marketing for the Modern Ophthalmologist
- crawford@messenger.md; Twitter @messengerMD
- Financial disclosure: None