People: The Frontline of Cybersecurity

Three good habits for small practices

Did you know an estimated 90 percent of cyber-attacks could be prevented by implementing cybersecurity best practices for some of the most common and pervasive cyber risks today?[1] Cybersecurity consists of all technologies and practices that keep computer systems and electronic data safe.[2] Everyone in a small practice needs to understand how to avoid being the victim of a cyber-attack, which can compromise patient privacy and disrupt operations.[3, 4] Learn about basic cybersecurity best practices, including practical habits that anyone can adopt.

1. Recognize and Avoid Phishing Scams

Phishing is when cybercriminals use fraudulent emails or text messages to trick victims into disclosing sensitive information (passwords, account numbers, etc.) or clicking a link to install a virus that can damage, disrupt, or steal information on any programmable machine (computer, tablet, mobile phone, etc.), service, or network.[5] To carry out these tasks, cybercriminals count on people being tired, rushed, distracted, or forgetful, and usually pretend to be a trusted source.[6]

Tips: [7, 8]

- Be cautious of emails that are out of the ordinary or unexpected (unrelated to your job responsibilities, sent at an unusual time, from an unknown sender, etc.)
  - Other warning signs include "urgent" messages and unusual grammar or wording
- Confirm the email is legitimate first
  - Hover over the "From" display name to see the full email address; it's common for cybercriminals to use a trusted name (a known company, coworker, client, etc.), so make sure the email address matches the person they are claiming to be

[1] United States Government Accountability Office, *DOD Needs to Take Decisive Actions to Improve Cyber Hygiene*, April 2020. Available at: www.gao.gov/assets/gao-20-241.pdf.
[2] University of Southern New Hampshire. *What is Cybersecurity and Why Is It Important?* February 2021. Available at: www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security.
[3] Health Sector Council, *Cybersecurity Practices for Small Health Care Organizations*. Available at: www.healthsectorcouncil.org/wp-content/uploads/2018/12/tech-vol1-508.pdf.
[4] Medical Economics, *The Growing Cyber Threat to Physician Practices*, May 2019. Available at: www.medicaleconomics.com/view/growing-cyber-threat-physician-practices.
[5] Cybersecurity and Infrastructure Security Agency, *Report Phishing Sites.* Available at: www.us-cert.cisa.gov/report-phishing#:~:text=Phishing%20is%20an%20attempt%20by,legitimate%20organization%20or%20known%20individual.
[6] See n. 2, *Supra*.
[7] See n. 2, *Supra*.
[8] HIPAA Journal, *Most Common Healthcare Phishing Emails Identified,* October 2018. Available at: www.hipaajournal.com/most-common-healthcare-phishing-emails-identified/.

- Carefully examine the email address for subtle inaccuracies, like changes to a single letter or character (e.g., **john.smith@nycompany.com** instead of **john.smith@mycompany.com**)

- Check embedded links by hovering (not clicking) over the link to make sure it matches the text of the URL (i.e., web address)
- Don't open attachments that seem odd or end in .exe, .vbs, .wsf, .cpl, .cmd, .scr and .js
- Report suspicious emails and then delete immediately

2. Create Strong Passwords

Passwords help protect personal and business accounts we rely on every day.[9] Cybercriminals use sophisticated techniques and tools to guess password combinations across millions of accounts, so it's important to understand what makes a password weak or strong.[10, 11]

Weak passwords…

- Include personal information that is publicly available or easy to guess, like the names of family members, birthdays, phone numbers, or addresses
- Use repetitive or sequential characters (e.g., aaaaaa, 1234,!@#$)
- Have already been compromised in a breach or recycled across multiple accounts

Strong passwords…

- Consist of a minimum of 8 characters in length
- Use a passphrase, which includes multiple words that are easy to remember but hard to guess (e.g., graceful elephants dance)
- Are different for each unique account

Source: National Institute for Standards and Technology, *Easy Ways to Build a Better P@$5w0rd,* October 2017. Available at: www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd.

[9] The SL Store, *Password Security: What Your Organization Needs to Know.* Available at: www.thesslstore.com/blog/password-security-what-your-organization-needs-to-know/#:~:text=Password%20security%20is%20the%20combination,type%20of%20memorized%20secret%20authenticator.
[10] American Medical Association, *How to improve your cybersecurity practices,* 2017. Available at: www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/cybersecurity-improvements.pdf.
[11] Cybersecurity and Infrastructure Security Agency, *APT Groups Target Healthcare and Essential Services,* May 2020. Available at: www.us-cert.cisa.gov/ncas/alerts/AA20126A.

Tips:

- Do not post passwords in plain sight or share login credentials with coworkers[12]
- Avoid using the same password for different accounts. Online tools, such as password managers, store passwords securely and make it easier to use a unique password for every account[13]
- Use multi-factor authentication (MFA) whenever possible. MFA verifies a user's identity with two or more pieces of information (e.g., token-base authentication, Captcha boxes, or instant messaging) before permitting access to a system[14]

3. Install and Maintain Anti-Virus Software

Antivirus software helps protect devices and data from cybercriminals. Without it, a small office is more susceptible to viruses and malware infecting a computer, tablet, phone, and other devices. Anti-virus software (Norton, Bitdefender, Malwarebytes, etc.) is widely available and reliable at low cost.[15]

Tips:[16]

- Practice management should ensure anti-virus software is installed and maintained on all machines, including tablets and mobile phones
- Enable automatic updates and scan all machines periodically to defend against viruses
- Make sure everyone in the practice understands that scheduled updates should never be canceled

Common Signs of a Computer Virus

- System will not start normally or repeatedly crashes
- Homepage randomly switches to another website
- Frequent pop-up ads
- Unable to control the mouse/pointer

Source: National Cybersecurity Alliance, *How to Tell If Your Computer Has a Virus and What to Do About It*, June 2019. Available at: www.staysafeonline.org/blog/how-to-tell-if-your-computer-has-a-virus-what-to-do-about-it/

[12] See n. 2, *Supra*.
[13] EDUCAUSE, Password Managers, July 2019. Available at: www.library.educause.edu/-/media/files/library/2015/7/passwordmanagers-pdf.pdf.
[14] See n. 2, *Supra*.
[15] Office of the National Coordinator for Health Information Technology, *10 Best Practices for the Small Health Care Environment*, November 2010. Available at: www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf
[16] *Ibid*.

Assessing Current Cybersecurity Protections

The following resources can help a practice assess cybersecurity and identify opportunities to educate staff:

The Security Risk Assessment Tool at Healthit.gov
Diagrams HIPAA Security Rule safeguards and provides tools to help organizations document their processes for mitigating risks
www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

MHCC Cybersecurity Self-Assessment Readiness Tool
Includes select elements from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to help practices identify gaps in cybersecurity readiness related to people, processes, policies, and technology
www.mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Cybersecurity_Self-Assessment_Tool.pdf

Information Security Awareness Assessment Quiz for Employees
A beginner-level quiz consisting of 10 questions that gauge awareness of cybersecurity
www.ciatec.com/2019/05/information-security-awareness-assessment-quiz-for-employees/

Additional Resources

Instructions and materials to create a cybersecurity awareness email campaign
www.cisa.gov/publication/cybersecurity-awareness-month-publications

Cybersecurity training toolkits, including posters, videos, and reference materials
www.cdse.edu/toolkits/cybersecurity/training.html

Platform for free and short employee training videos and exercises
www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html

Cybersecurity checklists for small health care practices
www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf

List of password manager products
www.cnet.com/tech/services-and-software/best-password-manager

List of anti-virus software products
www.cnet.com/tech/services-and-software/best-antivirus/

Questions?
Contact: Kelly Scott, Program Manager
kelly.scott@maryland.gov