PANEL OF EXPERTS

Cybersecurity

FROM OUR SPONSOR

Cybersecurity: Where to start?

What's the minimum I can do to stay safe online? Does a private individual need to take the same precautions at home as they would as an employee at work? These are two questions that I am frequently asked and the answer to both of these questions are timed perfectly with Cybersecurity Awareness Month October 2022, an awareness campaign promoted by the Cybersecurity Infrastructure Security Agency (CISA).

While there are literally hundreds of controls that can and need to be put in place to satisfy various regulatory and contractual mandates (such as HIPAA, PCI-DSS, SHIELD, CMMC, etc.) CISA has identified four things that EVERYONE (at home or at work, in your personal life or in the office) should be doing to be safe online. Everyone should: 1. Use multi-factor authentication (MFA) whenever it's available 2. Use STRONG passwords 3. Learn to identify and report Phishing emails and 4. Update your software and systems.

This year's Cybersecurity Awareness theme "See yourself in cyber" is intended to explain that everyone has a role to play, and can feel confident operating in a cyber world. The basic steps called out in the campaign are both minimum steps that everyone should be doing, and represent pretty strong controls which will go a long way towards keeping you safe while using the Internet and its related technologies.

The first two basic controls have to do with identifying who you are on-line. The Internet is largely anonymous, making it difficult to determine whose data should be accessed by whom. The way we all prove ourselves in a computer world is by authentication. There are three ways to prove who you are: with something you know (like a password), with something you have (like a key, or an electronic fob), or with something you are (like a fingerprint, or facial recognition). Multi-factor authentication means to use two or more of these methods to prove who you are, like a physical key and a combination or PIN. Using two or more is stronger than using just one. If you access information remotely, like on-line banking or connecting to your work by VPN, you should use MFA to make doubly sure that it's you accessing and not someone impersonating you. Unfortunately, not every website or program has multi-factor authentication, yet. The most common authentication is still the password, and a major cause of cyber incidents is that people still use weak passwords (like PASSWORD1, or their birthday) that are pretty easy for others to guess. A strong password is one that you can easily remember (so you don't need to write it down) but that anyone else will find it hard to guess. Longer passwords are better, because they are harder to guess by "brute force." A line from a song or poem are good strong passwords: "The rockets' red glare" is 22 characters long, has upper- and lower-case letters and a special character.

Regarding the third control, a phish is an email (or could be a text or voicemail) that pretends to be from someone it's not, and tries to trick you into going to a website, or opening an attachment, or entering your password. These activities are then used to launch ransomware or steal your money or data. Regular training and practice help users to identify and report phishing attempts to IT. Reporting suspected phishing attempts allows IT to block further attempts and protect others.

At home and at work, we all use dozens of computer programs and tools every day. Step four reminds us that these items need to be kept up-do-date to ensure that they can't be compromised by a hacker who knows there's a bug or other vulnerability. Many cyber incident causes are due to mistakes in programs or outdated systems that are easily hacked. Take the time every month to check to see if there are updates for your computer or phone, and apply the patches.

These four controls are basic and essential, but may not be simple to execute, especially in a corporate environment. The logistics of patching hundreds of computers monthly, or getting all users to adopt strong passwords may take some thought and effort, but it's well worth the effort. As the saying goes, a journey of a thousand miles begins with a single step. These four steps are a very good place to start.

William M. Prohn
Managing Director, Dopkins System Consultants; Director of Information Technology

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

For a Strategy to get Started with a Cybersecurity program contact:
William M. Prohn
wprohn@dopkins.com

Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS
200 International Drive | Buffalo, NY 14221 | 716.634.8800