Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

October is Cybersecurity Awareness Month: Here's 4 Things YOU can do

Patrick Rost prost@dopkins.com October 2022

For the past 19 years, October has been recognized as Cybersecurity Awareness Month in the United States. This year the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) have collaborated to create a campaign designed to provide information and resources to help educate the public. Their campaign theme, *"See Yourself in Cyber,"* reinforces the human element of Cybersecurity. With this campaign they have established **four things you can do** to increase your Cybersecurity posture. To support this campaign Dopkins & Company has released a weekly blog discussing each of these topics:

- Enable Multi-Factor Authentication
- Use Strong Passwords
- Recognize and Report Phishing
- Update Your Software

While reading these blogs keep the theme (See Yourself in Cyber) in mind. Each of these key action steps is something YOU can do to increase Cybersecurity at home, work, and school. While each blog will discuss the actions individuals should take, they will also touch on how businesses can help their employees succeed with each action.

You can view the campaign directly on CISA's website at https://www.cisa.gov/cybersecurity-awareness-month.

What is Multi-Factor Authentication (MFA)?

You have most likely heard of Multi-Factor Authentication and may know what it is already. MFA has become a requirement to being approved for Cyber Insurance and on most third-party questionnaires. Some companies, especially financial institutions, require MFA setup when accounts are created and have enforced requirements on existing accounts. Many other companies offer it as an optional feature in account security settings.

Understanding MFA relies on understanding both authentication and factors. **Authentication** is the process of verifying an identity, or who you say you are (i.e., username/email). Because anybody can go to a website and type in your email address you need to prove it is actually you. This is most commonly done using a password, a single factor. There are several types of **factors** with the three most common being something you know, something you have, and something you are:

- **Something you know** is the most frequently used and includes passwords and PINs.
- **Something you have** is a unique item that is in your possession like a smartcard, USB drive, hardware authenticator or software authenticator.
- **Something you are** includes biometrics like fingerprint, facial recognition, voice recognition, etc.

MFA uses at least two *different* factors to provide authentication. Let's take a look at examples of what is and is not MFA.

Is MFA:

- A low-tech example is an ATM card (something you *have*) with your PIN (something you *know*). Walking up to the ATM with just the card is not enough to withdraw money. The same is true if you walk up to the ATM without your card and just enter your PIN.
- Substitute the ATM for your banking website. Here you enter a password (something you *know*) and the code that was sent to your phone (something you *have*) by text.
- A slightly better version of the previous example is entering your password (something you *know*) and a code generated on your phone (something you *have*) by an authenticator app. This prevents the code from being sent over the internet to you and only exists on your phone.

Is NOT MFA:

- Logging into a website with a password (something you *know*) and a PIN (something you *know*) is not MFA because it uses the **same factor twice**.
- Unlocking a phone with just facial recognition (or fingerprint) is only using something you *are* and no second factor. If this is paired with a password/PIN then it can become MFA.
- Entering a building using your key fob (something you *have*) uses only one factor.

Importance

Why is this something insurance, banking, and other industries are starting to require? Why is this the first of four items being highlighted by CISA? Simply put: Humans create weak passwords which act as a single line of defense. And even strong passwords can be guessed, stolen, and cracked. For more on strong passwords read our next blog on key action step #2: using strong passwords. While enabling MFA does not eliminate the need for a strong password, it is an extra layer of protection should it become compromised.

Barriers to Implementing

With all of the attention on MFA there still may be reasons your organization has not enabled MFA everywhere it should be.

- **Unaware of software/websites that should have MFA enabled** – It is important to maintain an inventory of the software in use throughout your organization. This is especially true for web and cloud-based software. If you don't have a record of the software you use it is easy to overlook security settings. Start by creating a list of all software that is in use and indicate which of them are accessible from the internet.
- **MFA is not offered** – There is still software that does not support the use of MFA. You should reach out to tech support to see if it can be setup or if it is in development. It may be time to evaluate the risk involved with continuing to use the software without MFA. If it is older software that is no longer being updated or supported it may be time to research new options.
- **Long list of places to enable** – After creating your software inventory you may be left with a long list that will take time to get through. Choose the software that represents the greatest risk if compromised and start there, continuing through the list until complete.
- **Unsure which second factor to use** – Using any second factor is better than none. While an authenticator is more secure than a texted code, if you can enable MFA via text today and implement an authenticator over time don't wait on enabling MFA via text. Software authenticators are apps that can be downloaded right to smartphones. If employees don't have capable smartphones, or company policy doesn't allow for personal phones to be used, hardware authenticators can be purchased or other alternatives researched.

Defining a strong password

In order to use strong passwords, it is vital to know what a strong password is. At a high level a strong password is **easy for you to remember** but **difficult for someone else to guess**. We will take a look at how to achieve each of these along with additional best practices.

While reading this blog keep the first blog in this series on Multi-Factor Authentication (MFA) in mind, it is still extremely important to enable MFA. Creating a strong password and enabling MFA complement each other, *neither is a replacement for the other*.

Difficult for someone else to guess

Password best practices of the past have resulted in people creating passwords that are easy to remember at the cost of also being easy for someone else to guess. An example of this bad practice would be using a child's name and date of birth. Anybody who knows you, has access to public record, or has access to view your social media accounts (do you share publicly or accept strangers' requests to connect?) can piece this information together and make educated guesses at your password. Sometimes the easily guessable password includes other combinations like a company name, "123456", or even "password" itself. These common or easily guessable passwords must be avoided in order to create a password that is difficult for someone else to guess.

Passwords must also never be reused or shared. If you share a password, it gives another person full access to your account. Control of that account and the password is now out of your hands. **Reusing passwords across multiple accounts can result in one compromised password granting access to several accounts.** Every account should have a password that is not similar to any other. Adding a number, or changing just a couple characters, to the same password is not good enough to be truly unique.

Easy for you to remember

So, let's look at how to create an easy to remember password that is better than *P@ssword2*. This can be accomplished using a passphrase, which is a short sentence of full words typed out.

The first method of creating a passphrase is using a popular song lyric, movie quote, or literary passage. One example is: *LifeislikeaBoxofChocolates*. This passphrase is 26 characters with a few random capital letters, and can easily have spaces or numbers added at a random spot to make it longer. If you are a Forrest Gump fan you will never forget it, and its length and variation of characters makes it difficult to guess.

Another method is to select random words to avoid using anything that has meaning. You may be able to achieve this by looking around your work environment for ideas. You could also use an online random word generator. This will create something like: *NativeGarageDeleteMerit*. While not as easy to remember as using the previous method, it is easier to remember four words than the complex passwords of the past that were not as long as they should have been. This passphrase is 22 characters and like the previous example can easily have spaces or numbers added at a random spot to make it longer. This passphrase's length and randomness makes it difficult to guess.

Recent studies have found the average person has 100 or more (even up to 150+) online accounts with passwords.

One Exception.. Password Managers A password manager will securely store your account usernames and passwords. This can save you from creating and remembering 100+ unique passphrases. Password managers are an exception to the "easy for you to remember" rule because you can use the password manager to generate a very long (30+ character) random password for your accounts. Because it is stored in your password manager you do not need to remember it and it is much more difficult for someone else to guess. Password managers are made secure by signing in using a passphrase created following best practices outlined in this blog along with enabling Multi-Factor Authentication (MFA). Stored credentials are encrypted so only your strong password and MFA can access them. Password managers have the added benefits of allowing passwords to be copied/pasted into websites or even auto-filled using their secure browser extension. Password managers are also available across multiple devices and locations for ease of access to accounts.

It is important to point out the difference between using a password manager and other methods of storing passwords. These methods should **not** be used and should be replaced with a password manager:

- Saving passwords in a file on a PC – This is a high risk because if unauthorized access is granted to the PC containing the password file all of the stored accounts are now compromised. Unauthorized access could be a compromise from someone outside the organization or someone internally who has permissions they should not.
- Writing/printing passwords – Passwords stored on paper can only be accessed from one location and can be destroyed during a disaster. Transporting them with you increases the risk of being misplaced or stolen. It is also difficult to update the documented passwords when they change.

- Saving to your browser – Credentials saved in a browser can be stolen if the PC, or even just the browser, become compromised.

Barriers to Implementing

These steps to using strong passwords may seem fairly straightforward for an individual; but, how does an organization require all employees to follow password best practices? The first step is to create (or update) a password policy. If the requirements are not defined in a policy there is nothing dictating what employees should do and no authority to back it up. A policy alone is likely not enough. Providing a business class password manager and encouraging (or requiring) use will go a long way. Password requirements of all systems, internal and external, should be reviewed to make sure only secure passwords that match your policy can be created. Employees will need to be trained regularly on the most recent policy and best practice.

Defining phishing

In 2021 Phishing was the second most frequent and second most costly initial attack vector. In addition, 91% of successful data breaches started with a spear phishing attack.

Phishing is a social engineering attack, one that doesn't attempt to hack a computer system but attempts to hack a person. Phishing is a type of attack that attempts to get a person to unknowingly take a malicious action. Phishing is an unsolicited communication via email, text (SMS), or voice (over the phone), examples of each:

- **Email** – Over time everybody has seen the different types of emails that appear like they are coming from someone within their organization, or someone they know, but are really from a fake account.
- **SMS/Text (Known as Smishing)** – Over the past few years there has been an increase in the number of text messages that purport to be from a bank, shipping company, or other trusted entity that include malicious links.
- **Voice (Known as Vishing)** – Includes those calls purporting to be about your extended car warranty, activity on your credit card, or from "tech support" just looking to help with a problem on your computer you didn't know you had.

The goal varies but may include getting you to install malicious software (Malware) onto your computer, enter your credentials on a site where they can be stolen, or to transfer funds to criminals.

Common terms related to phishing:

- **Spear phishing** – A phishing attack that is customized to target an individual(s), usually because of their role (i.e., finance, HR, IT admins). Attacker will use publicly available information in their customization.
- **Whaling** – Advanced type of spear phishing that targets individual(s) because of their high rank, typically members of the C-suite. Attacker may spend weeks or months gathering information about their target to provide a convincing attack.

Recognizing Phishing

The first step in recognizing phishing is being aware that these types of attacks exist and that they target everybody. Once you are aware that you are constantly a target you can start looking for the phishing attacks that are coming your way. Phishing usually contains red flags that should raise suspicion and cause you to proceed with additional caution. The largest red flag is that the **communication was unsolicited**. The attacker wants you to perform an action so they initiate the conversation. They will introduce a problem you did not know you had and a solution to this problem (how convenient!).

These unsolicited communications will be from someone you do not know, even though most times they are spoofed to appear to be from someone you do know. Be sure to check the "From:" field in the email carefully to make sure the email address of the sender is correct. If it says the email is from Patrick Rost with a random Gmail address it is not actually from me. Also, look out for fake domains with extra, missing, or swapped out characters. An email from dopklns.com may look legitimate but a closer look will reveal the lower case "L" rather than an "i" in the name. This can be done with any company and is done frequently with larger corporations like Google, Microsft, Amaz0n and more. (Did you catch the misspelling in each of those?)

This offered solution leads you to the **action they want you to take** (click a link, type your password into a website, send money, etc.). With this action is a **false sense of urgency** that a negative consequence will occur if the action is not taken soon. *If you do not reset your password in the next 4 hours you will be locked out, click the link to set a new password* or *Your service will be discontinued if you do not renew by the end of the day, renew at this link*. Other red flags may include: links that don't go where they state, requests for sensitive information, offers too good to be true (lottery winner, inheritance), and poor formatting/grammar.

Reporting Phishing

Just recognizing phishing is a large task, but is only the first half of this action step. Once phishing is recognized it cannot be ignored. Each organization must have a policy and method to report phishing attacks. Reporting the attacks potentially allows IT staff to block the sender so the same attack does not get to other employees. They can also follow-up with any employees that did already receive the phishing attempt. Reporting methods will vary by organization but may include emailing an IT contact/helpdesk, emailing a specific phishing address, calling IT/helpdesk, manually opening an IT support ticket, or adding a button to Outlook that handles reporting the email. You should make sure you are aware of your organization's policy for reporting phishing attempts. If you are responsible for the policy, you should make sure it exists, is updated, and is communicated to your employees.

Barriers to Implementing

If you did not previously know what phishing is and how to recognize attempts, it is very likely the same for your employees. And even if you did, how confident are you that *every employee* understands and can recognize phishing? Providing training to employees is vital. This training should be offered to all employees when they are hired (or when the program is first implemented) and on an on-going basis. Recurring training allows updates to be provided as the landscape changes and also acts as a way to keep the reality of phishing at the top of employee's minds. Many training platforms include simulated phishing tests which give employees an opportunity to see examples of phishing. If you are already providing training to employees (or once you implement it) then you can move on to establishing a method for reporting. Most platforms that offer simulated phishing tests also offer a solution for reporting phishing attempts. It is then up to you to decide where these reports go and how they are handled. Technology exists that will automatically react by blocking sources of phishing and can even remove emails from inboxes. Without this technology there should at least be a policy to manually react to reported phishing.

Update your Software

This month's final action item is to update your software. Before you can update your software, you will need to know what software you are using. This requires an accurate and up-to-date list of all software in your environment and should include the version you are using and the most current version available.

One of the first considerations is the **age of your software** and whether it is in support and still receiving updates from the vendor. A good example is Windows 7, Microsoft ended support for the an operating system on January 14, 2020 meaning they have not released routine updates in nearly three years. The same situation will happen for Windows 10 on October 14, 2025 giving everybody three years from now to update to Windows 11 or a future version of Windows. It is possible that you still have legacy software running in your environment that has been around for 5, 10, or even 20+ years. If this software has not been kept current by the vendor there will be significant vulnerabilities that can be compromised. If your vendor is no longer providing updates you will need to evaluate the risk of keeping the legacy software vs changing to a newer product.

Types of updates

After you confirm your software is receiving updates you will have to know what is included in the updates you receive. Most vendors will release occasional **version (feature) updates**. These updates are meant to increase the usefulness or functionality of a product. They may include changing how the software looks, where menu items are, or completely new things to do. It is not urgent to install version updates unless they also include changes to fix bugs and vulnerabilities. But, these types of changes are usually released in the more frequent **security updates (known as patches)**. Some vendors release security updates on a schedule while others release them as needed. Patches do not change the overall software but just small pieces of the code. Patches are meant to fix known vulnerabilities that can be used against you. These patches should be *installed as soon as they can be*. Often times the vulnerabilities are actively being exploited on other systems. If the vulnerabilities were previously unknown, the release of the patch allows them to be discovered and makes the unpatched system more of a target than before the release of the patch.

Microsoft releases security updates for supported Windows Operating Systems in the afternoon of the second Tuesday of each month, in what is known as Patch Tuesday. This past month was on the 11th, in November it will be on the 8th. Because of this, the following day is known as Exploit Wednesday, where attackers will begin to exploit the newly disclosed vulnerabilities.

A final update to consider is **definition updates**. Within some software, primarily anti-virus, there are definitions. These update independently from the software itself and should always be kept current. Some definitions update constantly and usually software can be set to check automatically on an interval (i.e., every hour).

Cloud Software

There has been a significant move to cloud software the past several years. Cloud software is any software hosted by someone other than your own organization. This includes websites you sign into including payroll, HR, asset management, etc. You may also sign into an entirely different system in order to access software. Regardless of how it is accessed you still need to verify your software is properly updated. Many times, when you contract with a third-party, they will manage the updates for you and keep everything up-to-date, but this needs to be confirmed.

Barriers to Implementing

This blog led with the recommendation of creating a software inventory to assist tracking updates. While this is important to ensure no software is overlooked, it should not take priority over the updates themselves. Both tasks can be done simultaneously with the inventory serving as the initial documentation of the status of updates. A more thorough inventory can be developed after it is ensured software is current.

One of the largest concerns with running updates or patches is the downtime caused while they are installed and the system reboots. This will cause each employee to lose time while their workstation updates. Additionally, servers will need to be rebooted which can cause additional down time for everybody. Scheduling servers (and possibly even workstations) to update off-hours during a maintenance window will minimize the impact. This should always be done with operations in mind, but should not be avoided altogether. Having an effective patch management platform will be greatly beneficial in tracking and coordinating the logistics of updating all systems. This will help automate the process as well as scheduling during the appropriate times.

Another large concern is that the update will cause the system, or a component of the system, to stop working properly. This stresses the importance of having backups that can be reverted to if needed. It also makes a case for having a test environment that closely replicates the operating environment.

While addressing the software in your organization don't overlook any non-business devices used by employees. If employees are allowed to use their own PC to access your system, do they keep it up to date? Same question for personal phones that link to organization email. Your organization's policies and acceptable use agreements need to address whether employees can use their own devices and the expectations/requirements around such use.

For more information, contact Patrick Rost, CISSP [prost@dopkins.com].

About the Author

Patrick M. Rost, CISSP, CMMC-AB RP

Patrick assists clients with improving their cyber security from a technical perspective. With nearly 10 years of information technology experience in a variety of industries, he is well-suited to assist clients in implementing, maintaining and protecting their computer networking environments.