Cybersecurity Awareness Month

October 2022

Cybersecurity Awareness Month
#SeeYourselfInCyber
www.mass.gov

Background

Since 2004, October has been recognized as National Cybersecurity Awareness Month. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) have led the effort to bring awareness to cyber threats and the best ways to mitigate those threats. In addition, many other federal, state, and local government agencies have used this time to increase awareness. Cybersecurity Awareness Month has been a time for combined effort between government entities and industry participants to help protect individuals on the internet and has become even more important as cybersecurity threats and their level of complexity has increased. Everyone has a role in strengthening their cybersecurity protections. Here are some easy things you can do to protect yourself online. #SeeYourselfInCyber

- Multi-factor authentication (MFA)
- Use strong passwords
- Recognize and report Phishing
- Update your software

Cybersecurity Awareness Month
#SeeYourselfInCyber
www.mass.gov

Weekly Schedule

Week 1 …….. Multifactor Authentication

Week 2 …….. Use Strong Passwords

Week 3 .....Recognize and Report Phishing

Week 4 ..... Update Your Software

Cybersecurity Awareness Month
#SeeYourselfInCyber
www.mass.gov

Week 1: Multifactor Authentication (MFA)

Many of the best cyber practices are easy to implement, but they go a long way in protecting against cyber-attacks. It is important to take all steps that can deter cyber criminals or make it harder for them to access your information. Certain practices like enabling MFA will increase your security online. What is multifactor authentication? Multifactor authentication is a system used to add multiple levels of authentication for an account. To be considered MFA there should be at least two of something you know, something you have, or something you are. One example of multifactor is debit card and pin number. To withdraw money at an ATM you must insert a debit card (something you have) and enter a PIN (something you know).

Enabling Multifactor Authentication

- Enable MFA on any account that has the capability especially high-risk accounts like banking applications and medical portals.
- Look into applications that provide authentication services.
- Enable Biometric authentication on mobile devices for additional security.

Cybersecurity Awareness Month
#SeeYourselfInCyber
www.mass.gov

Week 2: Use Strong Passwords

Passwords are the most common type of authentication[1]. We all have a plethora of usernames and passwords for our numerous online accounts. Creating strong passwords for accounts reduces the risk of account compromise and identity theft. Malicious actors have software that can brute force accounts or guess passwords. These tools and techniques work best if someone's password is easily guessable.

Password Best Practices

- **Length –** Try to use the longest password the account allows.
- **Complexity –** Adding complexity to a password such as numbers, capital and lowercase letters, and symbols, makes it harder to guess a password.
- **Use Unique Passwords –** Do not use the same password for multiple accounts. Reusing passwords can lead to multiple compromised accounts.
- **Password Manager –** Use a password manager to save your complex passwords. It is impossible to remember all of your passwords for all of your accounts. Setting up a password manager application is a great way to securely store long and complex passwords. Use your preferred application store to find the Password manager that works best for you.
- **Do not use dictionary words –** Words that can be found in the dictionary can be easily guessed or cracked.

[1] https://www.cisa.gov/uscert/ncas/tips/ST04-002

Cybersecurity Awareness Month
#SeeYourselfInCyber
www.mass.gov

Week 3: Recognize and Report Phishing

Phishing is when a criminal will try to get you to click on a link or attachment, most often through email, and then will steal your information or install malware on your device. Phishing schemes are the most popular way criminals will try to steal your passwords, credit cards, SSN or other personal information. Phishing schemes have become more prevalent along with the rise in remote work. While phishing schemes can be complex, they often have a few telltale signs, and you are able to protect yourself from them if you can spot the signs listed below. If you suspect an email to be a phishing scheme, make sure to not click any links or attachments and block the email through your email software.

How to Spot a Phishing Scam

- **Suspicious Email Address** – Ensure the email address matches the emails of the reputable company. If the email does not match, then the email may be a phishing scam.
- **Suspicious wording or language –** Typos can be an indication of a phishing scheme.
- **Spoofed hyperlinks –** Hover over the hyperlink to reveal the actual link. If the actual link does not match the text link, then the email may be a phishing scheme.
- **Generic Greetings** – Many phishing emails use generic greetings to maximize the number of potential victims.

Cybersecurity Awareness Month
#SeeYourselfInCyber
www.mass.gov

Week 4: Update Your Software

Updating your software is one of the most effective ways to protect yourself from cyber-attacks, and thankfully it is also one of the simplest. When manufacturers release updates to their operating systems, they are not just adding new features to your devices. They are also likely adding to their cybersecurity measures to protect you and your devices from cyber-attacks. It is also important to realize that updating your operating systems as soon as updates are released will ensure your device is vulnerable for less time. While operating systems on your phones and computers are the most obvious systems to update, they are only part of the picture. With the rise of the Internet of Things (IOT), many smart home devices are now connected to the internet. These devices on your network are a potential spot of vulnerability, and it is good practice to keep their software update to date as you would with your phone or computer. Another commonly forgot about device is your Wi-Fi router. Your Wi-Fi is the portal to your network, and cyber criminals will often try to gain access to the information on your devices by going through your Wi-Fi router. Like with many other best security practices, keeping your software up to date is a simple task to complete but does a great job at protecting you and your information.

Always remember to update your:

- Wi-Fi router
- Applications
- Operating Systems
- Internet of Things (IOT) devices like smart appliances when updates become available