Best Practices for Cybersecurity

Below is a list of some simple best practices for cybersecurity that can be applied to your environment to help ensure a more secure workplace. These practices along with the many other cybersecurity frameworks and tools will help increase your security posture as you navigate your way through implementing a strong cybersecurity program.

1. Implement user training for cybersecurity and assign a cybersecurity manager.
Compromised email and social engineering are some of the biggest threats that face networks today. A malicious link or compromised email makes up a large portion of incidents seen in cybersecurity. It is essential to confirm emails, especially those with attachments, and do not give out sensitive data such as a password. To help with this, train your employees on the appropriate actions to take and what to do if they feel that they are a victim of an attack. User training is vital to establishing good habits that will help prevent compromise. Assigning a cybersecurity manager will allow your organization to develop training regimens and develop SME's to protect your network better.

2. Use a strong password.
Most every point of entry into our technology involves a username and password. A common mistake is using easily remembered passwords and using them throughout multiple systems. The password that gets you into your Facebook should never be the password that gets you into a secure environment, such as a work computer. Establish a password policy and threshold for your organization. Password complexity, expiration, and thresholds are a very important step to help prevent unauthorized access to your system.

3. Multifactor Authentication (MFA).
Multifactor authentication is a growing technology that involves authenticating more than one time to a network or location. For example, if you log into a system with MFA, a secret code can be sent to your cell phone that must be entered to access the system. This allows confirmation that the user is who they say they are and not a bad actor who has stolen someone's password. Microsoft stated in 2019 that users who enable multi-factor authentication (MFA) for their accounts would end up blocking 99.9% of automated attacks.

4. Track third party and remote access.
With many organizations moving to third party vendors for security and operation to help save cost and increase productivity, it is essential as ever to establish and understand third party access and security. As an organization who is purchasing services, it is your right to have them follow your security standards and processes. Laws and compliance are beginning to develop that make the hiring organization responsible for data breaches as a third party. Ensure during procurement or go back and speak to your vendors to talk about security and make clear the expectations.

5. Back up important information and verify that you can restore it.
Due to hardware failure, virus infection, or other causes, you may find yourself in a situation where data that is stored on the device you use is not accessible. A common fear for most organizations is the well-known ransomware. To prevent a costly recovery and possible loss of all your data, make sure to regularly back up any data which is essential to your organization. Also, be sure to test, you can recover that data periodically. It is easy to say I have a backup. However, are you sure that the back-ups work? Also, be sure that the back-ups and working data connections are secure and do not connect in a way that would allow both to be corrupted should an attack commence.

6. Keep personal information safe.
Be wary of suspicious e-mails and phone calls. Never respond to emails asking you to disclose any personal information. Policies should be in place that establishes that no one should ask for personal information or access information. A common threat is an email or phone call from a bad actor pretending to be local IT or a superior asking for personal information or a password. This should never happen in a secure environment. This will also allow you to train your employees against this type of threat, both at work and outside of work.
Be careful about what networks you connect to. Connecting to the airport Wi-Fi or local Starbucks leaves you open for a multitude of attacks and data theft. Sensitive information should only be accessed on secure networks and authorized connections. Using your cell phone to conduct business is not as safe as one may think. Acceptable use policies should be established to prevent such unsecured connections.

7. Limit social network information.
Facebook, Twitter, LinkedIn, and other social networks have become an integral part of our online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post and where you access these sites. Be wary of allowing social network access on systems and networks that also transmit secure data.

8. What's connected?
Critical infrastructure has matured over the years. At a time, there were air gaps between operational equipment and a piece of network equipment. But that line is starting to disappear, and it is important to know where the operations side is connected to the network. These connections must be secured and limited to only essential personnel and equipment. Everything from thermostats to watches is now connected to networks, so everyone must be vigilant of who and what is connecting to their network.

9. Create a Baseline for your network.
Use the aforementioned frameworks to create a security baseline that does not change without an approval process and documentation. This will allow you to track and maintain your network policies in the proper manner. Deviation from the newly created security baseline can be tracked and therefore risk can be minimized and better controlled.

10. Inventory your assets.
One of the most beneficial things an organization can do is inventory their assets. A top-down inventory will allow you and others to assess the size and tools appropriate for your size network. This will also allow an organization to identify critical assets which will allow a more specific approach to security implementation. This can greatly improve cost-benefit analysis and security efficiency by allowing you to focus more on critical assets than the non-critical ones.

Those are just a few helpful hints to keep you and your devices and information secure. Please visit the following sites for more tips on how to protect yourself:

- StaySafeOnline- https://staysafeonline.org/
- OnGuardOnline- https://www.consumer.ftc.gov/features/feature-0038-onguardonline

Remember, if you are unsure about something, ask for help!
Learning about information security and safe computing needn't be a daunting task. If you have questions and you're unable to find the information on our site, please let us know. Our contacts section is a great place to start.