Keeping Your Virtual Information Safe Starts with Email and Password Management

Checking your email is something most of us do so frequently that we rarely give it a second thought. Unfortunately, however, hackers and other cybercriminals often use email as their pathway into a company's sensitive data and important information.

Even more alarming is that some companies, like small businesses, are often even more vulnerable than others. And the risk continues to grow, with 2021 being the worst year on record for cybersecurity threats.

A cybersecurity plan for your business and employees, along with processes and security protection measures, is your best defense for your business against potential cyber threats. The email inbox is a vulnerable entryway into your business, but the right steps can protect your team from harm.

Securing Your Email Inbox from Cyber Threats

The first step in keeping your private information and sensitive data safe is protecting the most vulnerable entry points, like your email inbox. Securing internal and external communications is a simple but essential step in keeping hackers out while keeping your team and proprietary information safe.

Start With Password Management

Just like you wouldn't leave the keys to your sports car lying on the dashboard, you shouldn't leave your inbox open to a cybercriminal looking for an easy opportunity. Remember, your password is the one thing keeping the bad guys out of your inbox and other data on your network systems.

Password management tools can help keep your password information securely organized, and two-factor authentication adds another layer of security. Still, the easiest step that you and anyone in your organization can take to improve security is to create a strong and complex password or passphrase.

The only way to ensure that your passwords will protect your data is to follow password management best practices. When passwords and accounts become compromised, it can lead to serious and costly data breaches and other cyber threats.

Encryption Best Practices

Most of us just assume that the only people who read our emails will be those we sent the communications to. However, the best way to ensure that information is only viewed by the intended recipients is to encrypt all emails, especially those containing sensitive information.

We recommend that all devices, computers, and email accounts be protected with this essential security component.

Implement Cybersecurity Policies and Processes

Unless you're only concerned with your own email accounts and network access, creating and implementing cybersecurity policies and processes for everyone in your organization is essential.

Password management, two-factor authentication, and encryption won't help keep your information safe unless all users understand how and why to use the various features and commit to maintaining data and keeping systems secure.

Everyone who has access to your systems or uses an email account associated with your business must understand and follow best practices and procedures related to email security. It only takes one weak password for a hacker to gain access to all your most sensitive data.

Cybersecurity Resources for Professionals

In addition to the critical security steps we just discussed, there are several other tools and resources you can use to create the most secure environment for your emails and additional private information. Remember, a successful cybersecurity plan starts with clear policies and processes that you put in place to ensure all users are keeping data safe.

Workplace Policies for Electronic Communications

With the expansion of digital communication, it's critical to have a policy in place outlining the expectations and responsibilities of using electronic communication tools like email. Security threats like the misuse of internal communication or general poor business practices can result from improper use of electronic communications.

If you create an electronic communications policy, be sure to cover things like keeping private information and data confidential, maintaining account security, how internal and external communications may be used or shared, and so on.

This is also a good place to share your expectations and guidelines for members of your organization using social media, blogs, the company's website, or any other communication tools.

Email Usage and Password Requirement Policies

Another important consideration is how employees and others within your organization are expected to use email services and other network features. A policy can outline acceptable (and unacceptable) uses for email, messaging apps, and social media sites.

These policies can help prevent potential security breaches and lower the risk of having multiple users on your email account and other web services.

Password management is essential for protecting your most sensitive data. A password management policy instructs users on the kinds of passwords they must use, how to generate passwords, and what's acceptable for storage, use, and change requirements.

An email retention policy is also a good idea for any business. Microsoft recommends that you have employees purge any unnecessary emails, especially those that aren't directly related to the business. Many companies have a retention policy of 60 to 90 days. After that, emails should be discarded.

The Bottom Line

Just like you lock the doors to your home when you leave, you should also take steps to secure access points to your private data and information. This is even more important when you have a lot of people using a shared network or company email accounts.

With the rise in cybercrime and the millions of phishing emails that are distributed each week, it's more important than ever to take preventative measures against becoming a victim.

Protecting yourself, your business, and your IT team from potential threats starts with securing your email inbox and ensuring that all members of your organization understand how to do the same. Both internal and external communications can become a vulnerability if used improperly.

Cyber security is an essential investment in your business and your reputation. Putting measures in place on the front end will save you from losses in the event of a security breach. Don't wait to become a victim to implement policies and processes to secure your inbox and other accounts to keep your data and private information safe and secure.