PEAPACK-GLADSTONE BANK

Private Banking since 1921

Cybersecurity In The Workplace

4 Tips to Keep Your Business Safe and Secure

Keeping information safe and secure is challenging developments for businesses of all sizes over the last few years. Expeditious shifts from in-person to online to hybrid workplaces forced companies to change, or at least reexamine, their cybersecurity practices and protocols, and far too often they weren't prepared. In fact, according to CyberEdge's Cyberthreat Defense Report, 85% of organizations suffered from a successful cyberattack in 2021.

Now, businesses who have suffered cyberattacks along with companies who've been fortunate enough to avoid being a victim of breaches and hack are looking at ways they can bolster their defenses and safeguard their data. But which plans, practices, and services should these organizations invest in?

Below are 4 steps businesses of all shapes and sizes can take to better protect themselves against cyber-attacks:

Identify "Crown Jewels" of Your Business

Understanding what information cybercriminals are after most is essential to combating cyber-attacks. Therefore, creating an inventory list of the valuable data and assets within your organization, including manufacturer, model, hardware, and software information, is of the utmost importance. In addition, take note of who has access to important data and information while also accounting for all storage locations. This practice will ensure that business leaders have a track record of accessibility so that they know where to look in case of a vulnerability or breach.

Protect Assets by Updating and Authenticating

At the end of the day, protecting your data and devices from malicious actors is what cybersecurity is all about. To accomplish this, make sure your security software is current. Investing in the most up to date software, web browsers, and operating systems is one of the best defenses against a host of viruses, malware, and other online threats. Furthermore, make sure these devices have automatic updates turned on, so employees aren't tasked with manually updating devices. Additionally, make sure all data is being backed up either in the cloud or via separate hard drive storage.

Cybersecurity In The Workplace

Another important way to keep your assets safe is by ensuring staff are using strong authentication to protect access to accounts and ensure only those with permission can access them. This includes strong, secure, and differentiated passwords. According to a 2021 PC Mag study, 70% of people admit they use the same password for more than one account. Using weak and similar passwords makes a hacker's life a lot easier and can give them access to more materials than they could dream of. Finally, make sure employees are using multi-factor authentication. While this may result in a few extra sign-ins, MFA is essential to safeguarding data and can be the difference between a successful and unsuccessful breach.

Monitor and Detect Suspicious Activity

Companies must always be on the lookout for possible breaches, vulnerabilities, and attacks, especially in a world where many often go undetected. This can be done by investing in cybersecurity products or services that help monitor your networks such as antivirus and antimalware software. Moreover, make sure your employees and personnel are following all established cybersecurity protocols before, during, and after a breach. Individuals who ignore or disregard important cybersecurity practices can compromise not only themselves, but the entire organization. Paying close attention to whether your company is fully embracing all your cybersecurity procedures and technology is incumbent upon business leaders.

Have a Response Plan Ready

No matter how many safeguards you have in place, the unfortunate reality is that cyber incidents still occur. However, responding in a comprehensive manner will reduce risks to your business and send a positive signal to your customers and employees. Therefore, businesses should have a cyber incident response plan ready to go prior to a breach. In it, companies should embrace savvy practices such as disconnecting any affected computers from the network, notifying your IT staff or the proper third-party vendors, and utilizing any spares and backup devices while continuing to capture operational data.