Protecting Your Business from the Inside

An Employee Cybersecurity Checklist

Your employees are your best defense—and biggest weakness—in the fight against cybercrime. In 2017, an international I.T. risks survey demonstrated that **careless employees were the single biggest cause of data loss or leakage for businesses of ever size**. This survey showed that **employees were involved in 1 out of 5 serious data breaches**. It also showed that the **average financial impact of a data breach for small- to medium-sized companies is $86,000**.

You can save yourself a lot of trouble (and money) by reviewing this cybersecurity checklist. Share it with your employees, and set aside some time to work through each step to make sure that your business is protected from outside threats through the cooperation and dedication of everyone who works inside your walls. These tips may seem basic—and in truth, they are; however, many companies neglect some of these simple security practices to the detriment of their data and security.

Top Tips for Better Employee Security

1 Dedication to security should be a part of corporate culture.

A culture of cybersecurity awareness should be encouraged from the very top. Executives can lead the way by ensuring the proper security practices are a priority. Make sure leaders show up to training sessions, and demonstrate through practice their dedication to strong security.

2 Better security starts with your employees.

The more your employees know about how security best practices, the safer your business will be. Ensure that all employees understand and observe company security policies. Post security policies where they will be seen and review them regularly. Make sure employees understand their role in keeping your business safe.

3 Make time to train your employees on cybersecurity.

Many cybersecurity and data loss incidents begin with a simple mistake. The key to keeping this from happening is education your employees. Teach them to recognize social engineering methods. Train them to resist phishing, ransomware, and spear phishing attacks. Use a variety of methods, including in-person training, webinars, infographics, and video lessons. And do not forget to review on an ongoing basis.

4 Review policies, procedures, and practices on a regular basis.

Take the time to reassess your policies at regular intervals to make sure that your security practices are taking into account changes in technology, company makeup, and advances in I.T., as well as any security holes you may have addressed in practice but not in writing.

5 Control user access rights and privileges.

Maintaining strict control over who has access to specific programs and devices, and sensitive data and information is vital to strong security. Maintaining this control should be a key function of your I.T. department or provider.

6 Keep a fully up-to-date record of rights and privileges.

Knowing who has access to what can save you a lot of time when there is an incident. Recording all user access rights and privileges may seem elementary, but many companies fail to follow through on this very simple step.

7 Keep all systems up to date and perform regular scans.

Your systems are constantly changing. There are new devices and programs that need to be checked on an ongoing basis as new hires join your team, and new initiatives are put into practice. Make sure that new tools are vetted by your I.T. team, and scan your entire system for vulnerabilities on a regular basis.

8 Perform patches and updates when they become available.

Patches for vulnerable components and applications are made available by vendors on a regular basis. Be sure to take the time to update these systems as necessary. Do not put off performing an update for any reason. You may want to schedule a weekly time to install updates.

9 Give employees a simple way to notify I.T. about possible security issues.

Once employees recognize the signs of a breach, make sure they know who to call. Post contact names and numbers clearly. Consider installing a dedicated line employees may use to report cybersecurity trouble. Encourage employees to err on the side of caution when it comes to reporting possible breaches or attempts.

10 Use multi-layered security.

Don't trust your business to a single security solution or approach. A multi-layered solution watches for threats from multiple angles, ensuring that your systems can be safe from human error as well as other threats which may come your way.