Cybersecurity 101:
What You Need to Know and Do to Protect Your Business

The number of data breaches in the news has grown frighteningly large. Worse, there's no sign that hackers are stopping their efforts to expose private information. As a result, it's a good time for businesses to understand the risks and start thinking about cybersecurity measures. Thankfully, this isn't a new threat – wise business owners have been protecting sensitive information for decades. Now is an excellent time to review and update your company's cyber security practices with the following tips from our friends at Small Business Trends.

Get To Know the Basics of Cybersecurity

If you're serious about protecting your company's data, it's important to understand the basics of cybersecurity. As the name suggests, this is the process of protecting your data from being accessed or stolen by others. Companies typically protect their data in two main ways: - The Network - The network is the system that connects all of your computers and devices such as printers and copiers to each other. The network is often the first line of defense against hackers who want to gain access to your company's data. - The Data - The data refers to the information contained on the computers. Companies protect their data in a number of ways, such as encrypting the data (scrambling the data so that only those with a key can unscramble it), limiting who can access it, and regularly checking for any signs of suspicious activity.

Don't Rely On Just One Form of Security

While it's important to use different kinds of security to keep your sensitive information safe, you don't want to rely on just one form of defense. If a hacker discovers a way to break through one barrier, you don't want them to be able to access everything. To stay as safe as possible, try to incorporate as many different types of security as possible. For example, you can use firewalls and antivirus software on your computers to prevent hackers from gaining access to your network. You can also use passwords to keep others from accessing your computers and sensitive information. You can also use encryption to make sure that even if someone does get access to your data, they won't be able to understand it without the key.

Make Data Storage and Transferring Safer

If you store sensitive information such as client data or financial records, you can make it harder for hackers to access it by storing it in a more secure location. One of the most common ways businesses store data is on a server, which is essentially a computer that contains a large amount of data. Servers are usually stored in a data center, which is a facility used to store servers. While data centers provide a secure location for storing data, they aren't impenetrable. If a hacker has gained access to the server, they can use tools to copy all the data on the server and store it elsewhere. One way to guard against this is to use two-factor authentication. This adds one more layer of security for anyone trying to log in to a server or other type of data storage mechanism.

Make Your Network More Secure

There are many ways to make your network more secure, such as keeping software updated, changing your passwords regularly, and making sure your firewalls are up to date. However, one of the most important ways to keep your network secure is to regularly check for any signs of unusual activity. This is called network monitoring and it involves checking to see if there are any signs of activity that seems abnormal. Typically, you'll use a piece of software to do this. When you're regularly monitoring your network, you can quickly spot any signs of unusual activity, such as someone trying to log in to your network from an unusual location.

Having Strong Passwords Doesn't Hurt Either

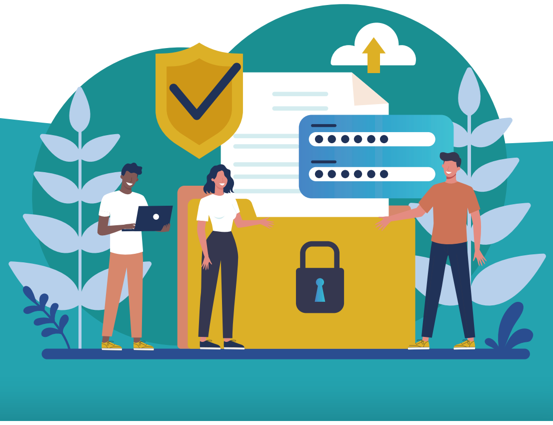
While many people focus on the other aspects of network security, it's also important to have strong passwords because without them, hackers can easily log in to your network. In fact, the most common way individuals log into a network is with their username and password. Almost every network regularly changes their passwords, but you don't have to wait for them to do it. You can change your passwords regularly by setting a reminder on your calendar. Experts recommend changing your passwords every few months. It can be easy to get in the habit of reusing the same passwords for all your accounts. However, that's a great way to give a hacker all they need to log in to your sensitive information. A good rule of thumb is to never reuse a password.

Be Careful Where You Store Client Information

While you want to make sure that you're protecting your clients' data, be careful about where you store information such as Social Security numbers or financial records. If someone hacks into your computer and copies the information, they'll be able to access it – even if you've taken the other steps to keep data safe. One way to protect sensitive information is to encrypt it. You can typically do this in a variety of software programs such as Word or Excel. There are also services, such as Box, that allow you to store your data but have a feature that encrypts it. This way, even if someone hacks into your computer and copies the information, they won't be able to access it.

Conclusion

While the threat of cybersecurity attacks has existed for decades, it has only recently become the subject of wide discussion, thanks to the growing number of high-profile breaches in both the private and public sectors. In light of these increased threats, it is vital that businesses introduce best practices into their operations to minimize the risk of falling victim to a breach. With these tips, you can better protect your company from cybersecurity threats.



ICE
TRUSTED IT PARTNER

CONTACT US TODAY

for a complimentary Security Posture Assessment

☎ 888-423-4801

✉ info@iceconsulting.com

🌐 www.iceconsulting.com