Cybersecurity Consulting

Share this to:

5 Tips on How to Prevent Cybercrime for SMBs

October 13, 2022 5 Minutes

The number of business leaders considering how to prevent cybercrime for their organizations has increased rapidly. This is because small businesses are the target of more than 40% of data breaches, putting the onus on leadership to protect assets.

A complete cybercrime defense program requires different solutions that safeguard each of the layers of your network. However, there are some practices that you and your employees can follow to reduce the risk of a data breach.

Read on to learn some tips on how to prevent cybercrime for SMBs. You can also share them with your employees so they too can help safeguard your assets.

A robust cybersecurity program takes advantage of a number of technologies. Learn about them in this easy-to-digest infographic: Infographic: The Layered Cybersecurity Defense

1. Use Strong Passwords and MFA (Multi-Factor-Authentication)

You might have heard it often, but strong passwords or passphrases are one of the most important steps to prevent unauthorized access. A strong password should be at least 16 characters long and include numbers and symbols.

A passphrase is simply a longer password based on words that are easier to remember. For example, the phrase "fishing for bass in Ontario" can be turned into the passphrase "Fi$hing4BassinOntario." Not only is this more memorable than a random string of characters, it also satisfies the length requirement of a strong password.

After you have set up a strong passphrase, consider taking advantage of MFA, a second layer of security for your accounts. This is especially helpful when a business has shared credentials. Asking employees to verify their identity with an **MFA method such as an authenticator app or text codes sent to a mobile device** will minimize the risk of unauthorized access into company accounts are secure even if credentials get stolen or accidentally shared.

Related Blog: 5 Common Cybersecurity Mistakes

2. Train Your Staff to Recognize Phishing Attempts

A recent phishing email campaign created to trick employees to send funds had the sender pretend to be the recipients' boss. The employees received an email thread that seemed to come from the company's partners or clients, which added to its fraudulent legitimacy.

Phishing attempts—communication-based attacks in which bad actors pose as trusted senders—are one of the top five activities that cause data breaches for businesses. Malicious actors have progressively improved their phishing tactics such as using email addresses and links that look trustworthy, and even using information employees share on social media to craft more personalized emails.

However, phishing emails do have certain giveaways your staff can look for in order to avoid clicking malicious links and sending sensitive company data or funds. **Alert employees in your organization to look for the following phishing warning signs:**

- A sense of urgency, e.g., "The human resources department needs your W2 form"
- An illegitimate email address, e.g., jsmith@walmmart.com (notice the double Ms)
- Grammar or spelling errors
- Suspicious links (hover the cursor over them to see where they lead)
- Seemingly random attachments

An employee email address can become the door into valuable company data or the company's network, therefore it's important to be wary of suspicious emails that could compromise your cybersecurity posture.

3. Update Your Devices and Software Regularly

Cybercriminals have online networks where they share information such as known system vulnerabilities. Since it can take manufacturers 97 days on average to deploy patches, this knowledge can become widespread among online hacking networks. Therefore, installing updates as soon as they are released is crucial to your cybercrime defense.

Software updates should include operating systems, applications, tools, and firmware on all network devices. **Consider also using a risk-based assessment strategy to discover which systems and devices in your network should be prioritized** and how to implement the best cyber strategy for your organization.

Related Blog: The Latest Cybersecurity Best Practices from the FBI, NSA, and CISA

4. Stay Up to Date with Cyber Trends

The news of ride-share company Uber falling victim to cybercriminals has shaken the cybersecurity world. What stands out from this event is that a contractor's credentials were used to breach the company's systems and cause a large amount of damage, both financial and reputational.

Knowing the malicious actor used social engineering techniques to receive credentials from the contractor helps organization **leaders understand the importance of cybersecurity training for employees.**

How can you protect your business from cybercrime with this information? Keeping up with these trends will help you better understand the kind of tactics bad actors use to breach business networks, what techniques cybersecurity professionals recommend to prevent incidents, and how to best prepare you and your team to avoid such compromises.

To begin learning more about current cyber threats, consider searching for cybersecurity news in your preferred browser, or visiting sites such as Cybercrime Magazine, Wired's cybersecurity section , and the FBI's page on cyber news.

5. Identify Your Data and Assets

Today's final tip on how to prevent cyber crime for your business is knowing what information devices, and systems you *need to protect*.

Since not all data or devices are critical to the security of your business,—for instance, image files of a company outing might not necessarily compromise a network—**focusing knowledge and resources on protecting sensitive or proprietary data** as well as devices and systems needed to conduct business will only strengthen your security strategy.

The NIST (National Institute of Standards and Technology) developed a framework to protect organizations against cyberattacks. It is not surprising that "Identify" is the first step of their five-step cybersecurity framework.

The NIST defines its identity area as follows: "The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy."

"The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes"

Once you have identified which data, devices, systems, and personnel—your IT or outsourced cybersecurity team, for instance—you will be better equipped to protect them and create a back-up plan in case they are compromised.

Bottom Line

Protecting your business against malicious actors takes time, knowledge, and the right team. We hope these tips on how to prevent cybercrime jump-start discussions in your organization on the best way to create a cybersecurity program that is tailored to your network.

Consider also partnering with a cybersecurity provider that can assess your environment, find any vulnerabilities, and plan a cybersecurity strategy that takes into account your organizations' resources and needs.

Check out the different types of solutions that can be used to create a thorough cybersecurity strategy in this helpful infographic: Infographic: The Layered Cybersecurity Defense.

Share this to:

Cybersecurity Consulting Blog

13753 W Boulton Blvd
Mettawa, IL 60045

info@DOTSecurity.com
833.920.1467

Follow us