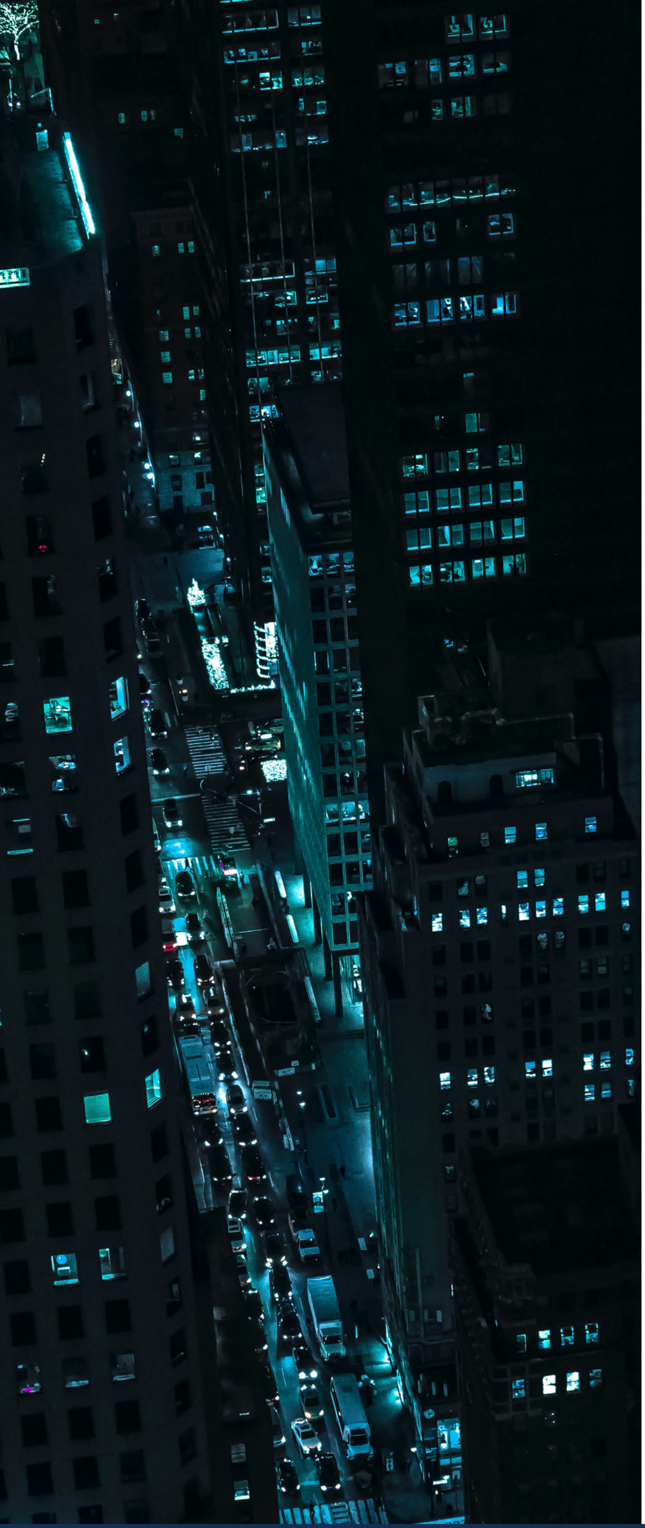
next I.T.

8 Cyber Security Best Practices For Your Small To Medium-Size Business

How does your SMB avoid being a victim of a cyber-attack?
This guide will provide you with 8 best practices for SMB cyber security.



It's easy to think because you have a small to medium-size business, cybercriminals will pass over attacking your company. The "not much to steal" mindset is common with small business owners in regards to cyber security, but it is also completely incorrect.

In reality, the U.S. Congressional Small Business Committee found that 71 percent of cyber-attacks happened at businesses with less than 100 employees. Even more concerning, the 2016 State of SMB CyberSecurity Report by Ponemon and @Keeperfound that 50 percent of SMBs have had a security breach in the past year.

But why are small businesses attacked more often than larger businesses? Almost all cyber-attacks are to obtain personal data to use in credit card or identify theft. While larger enterprises typically have more data to steal, small businesses have less secure networks, making it easier to breach the network. CSO.com by IDG's article "Why criminals pick on small businesses" says that by using automated attacks, cybercriminals can breach thousands or more small businesses, making the size less of an issue than the network security.

The CSO.com article says that lack of time, budget and expertise for proper security is a top reason for the high rate of SMB attacks. Other reasons include not having an I.T. security specialist, not being aware of the risk, lack of employee training, not updating security programs, outsourcing security and failure to secure endpoints.

next I.T.

How does your SMB avoid being a victim of a cyber-attack?

Here are 8 best practices for SMB cyber security

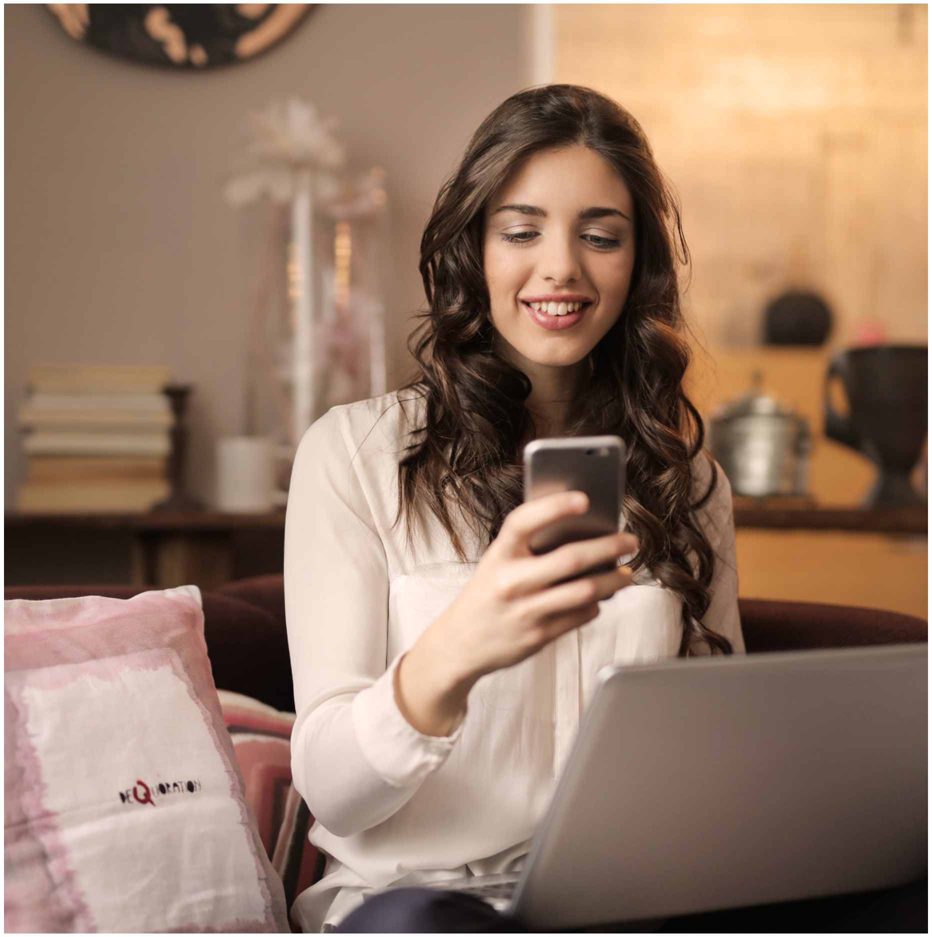
01 | Use a firewall

One of the first lines of defense in a cyber-attack is a firewall. The Federal Communications Commission (FCC) recommends that all SMBs set up a firewall to provide a barrier between your data and cybercriminals. In addition to the standard external firewall, many companies are starting to install internal firewalls to provide additional protection. It's also important that employees working from home install a firewall on their home network as well. Consider providing firewall software and support for home networks to ensure compliance.

02 | Document your cybersecurity policies

While small businesses often operate by word of mouth and intuitional knowledge, cyber security is one area where it is essential to document your protocols. The Small Business Administration (SBA)'s Cybersecurity portal provides online training, checklists and information specifically to protect online businesses. The FCC's Cyberplanner 2.0 provides a starting point for your security document. Consider also participating in the C3 Voluntary Program for Small Businesses, which contains a detailed toolkit for determining and documenting cyber security policies.

03 | Plan for mobile devices



With 59 percent of businesses currently allowing BYOD, according to the Tech Pro Research 2016 BYOD, Wearables and IOT: Strategies Security and Satisfaction, it is essential that companies have a documented BYOD policy that focuses on security precautions. With increasing popularity of wearables, such as smart watches and fitness trackers with wireless capability, it is essential to include these devices in a policy. Norton by Symantec also recommends that small businesses require employees to set up automatic security updates and require that the company's password policy apply to all mobile devices accessing the network.

04 | Educate all employees

Employees often wear many hats at SMBs, making it essential that all employees accessing the network be trained on your company's network security policies.

Since the policies are evolving as cybercriminals become savvier, it's essential to have regular updates on new protocols. To hold employees accountable, have each employee sign a document stating that they have been informed of the policies and understand that actions may be taken if they do not follow security policies.

05 | Enforce safe password practices

Yes, employees find changing passwords to be a pain. However, the Verizon 2016 Data Breach Investigations Report found that 63 percent of data breaches happened due to lost, stolen or weak passwords. According to the Keeper Security and Ponemon Institute Report, 65 percent of SMBs with password policies do not enforce it. In today's BYOD world, it's essential that all employee devices accessing the company network be password protected.

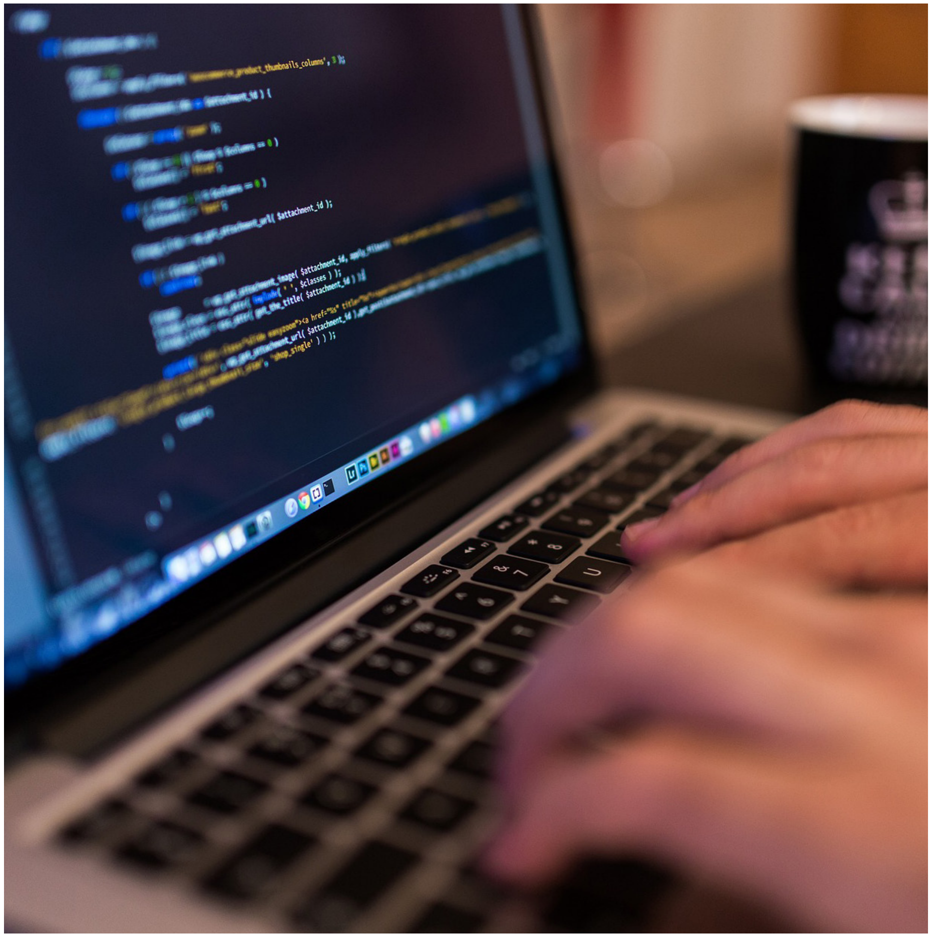
In the Business Daily article "Cybersecurity: A Small Business Guide," Bill Carey, vice president of marketing and business development at Siber Systems, recommended that employees be required to use passwords with upper- and lowercase letters, numbers and symbols. He says that SMBs should require all passwords to be changed every 60 to 90 days.

06 | Regularly back-up all data

While it's important to prevent as many attacks as possible, it is still possible to be breached regardless of your precautions. The SBA recommends backing up word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Be sure to also back up all data stored on the cloud. Make sure that backups are stored in a separate location in case of fire or flood. To ensure that you will have the latest backup if you ever need it, check your backup regularly to ensure that it is functioning correctly.

07 | Install anti-malware software

It's easy to assume that your employees know to never open phishing emails. However, the Verizon 2016 Data Breach Investigations Report found that 30 percent of employees opened phishing emails, a 7 percent increase from 2015. Since phishing attacks involve installing malware on the employee's computer when the link is clicked, it's essential to have anti-malware software installed on all devices and the network. Since phishing attacks often target specific SMB employee roles, use the position-specific tactics outlined in the Entreprenuer.com article "5 Types of Employees Often Targeted by Phishing Attacks" as part of your training.



08 | Use multifactor identification

Regardless of your preparation, an employee will likely make a security mistake that can compromise your data. In the PC Week article "10 Cyber Security Steps Your Small Business Should Take Right Now," Matt Littleton, East Regional Director of Cybersecurity and Azure Infrastructure Services at Microsoft, says using the multi-factor identification settings on most major network and email products is simple to do and provides an extra layer of protection. He recommends using employees' cell numbers as a second form, since it is unlikely a thief will have both the PIN and the password.

Security is a moving target. The cyber criminals get more advanced every day. In order to protect your data as much as possible, it's essential that each and every employee make cyber security a top priority. And most importantly, that you stay on top of the latest trends for attacks and newest prevention technology. Your business depends on it.

next I.T.

If you are still wondering how you can keep your business ahead of the game, find out how we can help with more than 20 years of I.T. experience.

Call or email us at
1 866.388.6398 or sales@next-it.net