

# Cybersecurity Tips for Businesses

Businesses have several opportunities to strengthen their defense against a cyberattack. Here are some things you can do today with little or no additional expense:



## Regular Software and Patch Updates

Update computers (manually or automatically) especially from Windows or Windows-based programs. Also update the firmware /security patches for all the devices in the workplace — Wi-Fi router's, printers, scanners, etc.



## Train Employees

Train employees on cybersecurity measures and establish basic security practices/policies for employees.

- Require strong passwords
- Establish Internet use
- Develop procedures on how to handle & protect customer information/other vital data.



## Passwords and Authentication

Require strong passwords that consists of numbers, letter and symbols – the more characters, the better. Enable multi-factor authentication (MFA) into employees' devices and apps.

*\*Tip: There are password keepers, apps for storing and managing passwords, that not only keep track of passwords but also set reminders when they are due for an update.*



## Timely Risk Assessments

Regardless of the size of your organization, consider incorporating risk assessments into your cybersecurity process. Brainstorm "what if" scenarios for cybersecurity, especially as they relate to data storage.



## Use Virtual Private Networks (VPNs) – Remote Access

VPNs mitigate the effects of a cyberattack because VPNs also encrypt data. As such, they can serve as an extra measure of security when employees are using their home wireless network, a network at another worksite or a café or restaurant, or a public internet access point.



## Regular File Backups

Backing up files might seem like a rather 1990s way to protect data, but even in the modern world of cloud storage and backup, it is relevant. Storing copies of data offline is a good idea and can be critical in recovering from situations like ransomware.



## Deploy Antivirus

Antivirus software should be installed on corporate-owned devices and on devices owned by employees that are used for work-related purposes. The antivirus software needs to be updated regularly.



## Secure Your Wi-Fi Networks

If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router, so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router. Two easy things you can do to help with security is change the router's default name and password.



## Protect Payment Cards

Isolate payment systems from other, less secure programs. Manually entering your card information when you make a purchase reduces the chance of it being compromised.



## Limit Physical Access to Computers

Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs and should not be able to install any software without permission.

## Helpful Resources

The descriptions and links below are provided for informational purposes only. Newtown Savings Bank (NSB) does not endorse any non-NSB product or service and is not responsible for the content of non-NSB websites, including their accuracy, completeness, or timeliness. Please also refer to the NSB website (nsbonline.com) for additional information:

### [Microsoft Cybersecurity Tips and Technology for Small Businesses](https://www.microsoft.com/en-us/store/b/microsoft-small-business)

(<https://www.microsoft.com/en-us/store/b/microsoft-small-business>)

### [FBI Cyber Crime](https://www.fbi.gov/investigate/cyber)

(<https://www.fbi.gov/investigate/cyber>)

### [Cybersecurity and Infrastructure Security Agency \(CISA\)](https://www.cisa.gov/)

(<https://www.cisa.gov/>)

### [Federal Trade Commission \(FTC\) Cybersecurity Basics](https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics)

(<https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics>)

### [U.S. Chamber of Commerce - Cybersecurity](https://www.uschamber.com/security/cybersecurity)


(<https://www.uschamber.com/security/cybersecurity>)

### [Global Cyber Alliance's \(GCA\) cybersecurity toolkit for small businesses](https://gcatoolkit.org/smallbusiness/)

(<https://gcatoolkit.org/smallbusiness/>)

### [Free training materials, security configuration guides from Internet Security Alliance](http://isalliance.org/)

(<http://isalliance.org/>)

 Small business owners should ensure that key vendors are also following good cybersecurity practices.

What's a key vendor? One that could cause major business disruption if they stop providing their service.