NYC Cyber Command

RETURN TO BUSINESS SECURELY

from New York City Cyber Command

As you restart your business, following just a few simple steps will make your business, your employees, and your customers more secure.

Whether a business has just one employee or a hundred, its approach to cybersecurity can follow the same format as the U.S. Government or a Fortune 500 company.

Identify, Protect, Detect, Respond and Recover

Step 1: Identify

A good business keeps accurate books! Take stock of the different devices, connections and data stores that are critical to your business. Use this worksheet to help you.

For more information and tools to help you identify your assets visit Inventory – Know What You Have from the Global Cyber Alliance, a non-profit organization focused on protecting small businesses and individuals from malicious cyber actors.

As part of your business continuity planning be sure to identify ways you can continue to operate without your IT assets or with a serious degradation to your IT environment. As part of that identification process be sure to identify if any software or hardware that you own/operate comes with any support options that are free or offered at discounts to small businesses i.e. Microsoft for Defender.

Step 2: Protect

Now and always, it's important for employees to be careful to avoid emails or other communications that may be scams. There are also protections that owners and managers can put in place to help block harmful activities or alert employees to danger.

Help your employees avoid phishing! Phishing is a fake email disguised to appear legitimate in order to convince recipients to click dangerous links or attachments that expose sensitive information. Most large email providers have built-in filters to help you and your employees avoid most phishing scams. For the ones that get through, make sure you and your staff know how to spot them. Ask your employees to take three minutes of free training at: Google Phishing

Ensure your computers' operating systems (i.e., Windows, macOS, etc.) are set to download and install updates automatically.

For more information: Software Updates – Update your defenses

Passwords are a basic protection. All passwords should be changed from their factory default as a minimum. Don't use something others could easily guess, like the word "password," obvious numbers such as "12345," and names of family members or your business. Also, don't use the same password for multiple log-ins. We recommend you take it a step further by using passphrases or short sentences The most efficient and effective way to use passwords securely is to utilize password management software like LastPass, Dashlane or BitWarden.

For more information: Password Management – Beyond simple passwords

New York City has created an app to help secure your employees' mobile devices: NYC Secure. The NYC Secure app is a free mobile app that alerts you if your mobile device or tablet encounters threats such as a potentially unsecured Wi-Fi network and will offer recommendations on how to address the threats. The app was designed with your privacy at the forefront. No information about you leaves the device.

For more information: NYC Secure

Your employees can also utilize Quad9, a free and simple to use security solution that protects your business' systems—and your employees home networks—against some of the most common threats. Like NYC Secure, it also preserves and protects privacy. It's easy for users to set up at home or at the office by following a simple set of instructions.

For more information: Quad 9 - DNS Security

Ransomware is the fastest growing threat to everyone who owns a computer. Protect your data by using online backup systems, a managed backup service provider, or backup your data to a business owned data storage device that you unplug and disconnect from your computer after completing a data backup.

For more information: Destructive Attacks – Defend against ransomware

Always enable password update notifications on your accounts to include your email account. Even better, implement multi-factor authentication to remove the possibility that cracking your password exposes your business to criminals.

For more information: Email Protection – Protect your email and reputation

Finally, you and your employees should use antivirus software. You can purchase antivirus software for individuals, get a set of licenses for your employees from vendors such as McAfee or Norton, or you can use one of several free services such as Avast, AVG, Sophos,

or Windows Defender. Many of these services include a firewall that can help protect you against unauthorized access to your systems. Regardless of the service you use, make sure that you keep the software updated as well as its associated antivirus signature file.

Step 3: Detect

Even Fortune 500 companies get hacked. How do you know if it has happened to your business?

Here are just a few indicators your system may be compromised:

- Your computer or Internet connection slows down in a big way—this could mean that malicious programs are running in the background or your computer is communicating with a bad actor instead of doing what you want.
- Your computers are constantly displaying pop-up windows, especially the ones that encourage you to visit sites or download software.
- You notice changes to your home page, desktop, or files. We recommend you limit user privileges instead of giving everyone the ability to modify everything on their company devices. This will help prevent mistakes and halt malicious software.
- Your email account shows emails being sent from your email account without your knowledge. This indicates that your email account has been compromised and your computer is most likely being controlled by a bad actor.
- Your computer frequently crashes or restarts.
- You notice unknown programs that start when you turn on your computer.
- You notice suspicious programs automatically connecting to the Internet.
- You receive notifications that your password doesn't work or notifications that your password has changed.

If you have an IT/Cybersecurity person or you are a bit of a computer expert yourself, you should consider services such as Splunk or Sentinel that can identify all your assets and monitor them for compromise.

Respond

If you think your device, data or network may be compromised, you should immediately activate your response plan.

A good response plan includes steps like:

- Immediately disconnecting all devices from the Internet, as well as disconnecting all your devices from each other. Do this by unplugging any ethernet cords, turning off WiFi and Bluetooth on every device. (Don't turn them off)
- Pausing to create a list of each asset or data store that you think has been compromised.
- Implementing your non-IT business plan which should be part of your response plan. This could be steps like giving wait staff order pads and pencils, having an appointment manager start taking appointments in an appointment book, or starting to track inventory in a ledger.
- Calling for help by reaching out to your internet service provider, any cyber-security vendors that you use.
- Notifying law enforcement of the incident. You can call your local NYC Police Department or you can report it to the FBI's Internet Crime Complaint Center.

Recover

Your business will get back on its feet quicker if you keep backups that are stored separately from your everyday devices and business network. If you are restoring data from a backup after a potential event, be sure to create an additional backup before restoring your backup data to any devices—and do not restore to any device or network that may still be compromised. Finally, be sure to identify and protect all new assets and networks to prevent future incidents.

For more information: Back It Up - Stay Safe Online

Look forward to a more detailed program that will show you how to spend 15 minutes a day to make your business more secure. Until then feel free to explore CISA's Cyber Essentials.