NYC Cyber Command

Cybersecurity for City Employees Working from Home

Working remotely—from your home or other locations—brings a unique set of cybersecurity challenges. There are easy steps that NYC employees should take to reduce the risk to themselves and the City. Malicious actors capitalize on issues of significant public interest and are using current COVID-19 fears to their advantage.

Identify

As an employee, make sure you keep track of your devices, along with what data you access from remote locations. Make sure you follow all of your Agency's guidance regarding accessing City systems and data.

Protect

Whether you use Windows, Mac or Linux, enable your systems to download and install updates automatically.

For more information: Software Updates - Update your defenses

Any password that isn't the default and that is not your agency name or personal information (such as your name or a close family members' name, which are easy to guess) is better than keeping the default. We recommend you take it a step further. To better remember your passwords, try using phrases or short sentences, or use password management software.

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

For more information: Password Management - Beyond simple passwords

New York City has also created tools that can help secure 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 insecure Wi-Fi network and offers recommendations on how to address the threats. The app was designed with your privacy at the forefront. No personal information leaves the device.

Employees can also utilize Quad9, a free, easy to use, security solution that uses the internet's Domain Name System (DNS) to protect employees home networks against the most common cyber threats. It also preserves and protects privacy. It's easy for users to set up at home.

Stay vigilant when opening emails and avoid phishing. Phishing is a fake email disguised to appear legitimate. The sender hopes you will click on a dangerous link or attachment. Most large email providers have some built in filters to help you avoid most phishing scams. For the ones that get through make sure you know how to spot them. Take three minutes of training at https://phishingquiz.withgoogle.com/

For more information: Threat Prevention - Prevent Phishing and Viruses

NYC Cyber Command

Ransomware is the fastest growing threat to everyone who owns a computer. Protect the City's data by using online agency backup systems such as OneDrive or others. Always follow your agency's backup policy.

Finally, if possible, you should always use antivirus software. If you have an agency issued device, it will have antivirus software installed. If you are using a personal device, employees can purchase anti-virus software such as McAfee or Norton, along with several free services such as Avast, AVG, Sophos, or Windows Defender. Make sure that you keep the software updated as well as its associated antivirus signature file.

Detect

How do you know if it has happened to you?

These are just a few of the possible indicators:

1. 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.

2. Your data usage skyrockets. Most malicious actors are trying to upload information to your computer or download information, and this increases your data usage. You can put in place data usage trackers or ask your ISP to set alerts on your account to warn you when your data usage exceeds a certain level.

3. Your computer constantly displays pop-up windows, especially the ones that encourage you to visit sites or download software.

4. You notice changes to your home pages, desktop, or files. Limiting user privileges vice giving everyone the ability to modify everything will help you detect malicious modifications.

5. 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

6. Your computer frequently crashes or restarts without warning.

7. You notice unknown programs that startup when you turn on your computer.

8. You receive notifications that your password doesn't work or notifications that your password has changed.

NYC Cyber Command

Respond

If you think you have detected a breach or an active compromise--What do you do?

Isolate the compromised asset.

- Disconnect any ethernet cords and turn off other connections to the device, such as WiFi and Bluetooth. However, you may want to leave the device powered on for investigation purposes.
- Check other devices and connections to see if they have signs of being compromised, as well.
- Do not connect any new devices to the compromised device, or the network.
- Do not continue to process or enter additional data on the device or network.

Get Help

City employees will notify their agency's IT and Cybersecurity departments; remind them to notify the NYC Cyber Command Security Operations Center. Follow your agency's direction on what to do next.

If a personal device is involved, contact your ISP and your anti-virus vendor and inform them of the situation.

For any personal cybersecurity compromises, ransomware incidents or cybercrime, individuals should report it immediately to the NYPD and the FBI's Internet Crime Complaint Center and local FBI Field Office.

Recover

Activate your agency's approved backup plan and carry out your work from known clean devices and a clean network.

Further Resources

https://workfromhome.globalcyberalliance.org/