Cybersecurity: How Managers Can Prepare for What Lies Ahead

5 necessary actions to prepare for the future, as recommended by the Department of Homeland Security (see: https://www.dhs.gov/national-cyber-security-awareness-month):

1. **Keep a clean machine**. Keep the security software, operating system, and web browser on your devices updated. Keeping the software on your devices up to date will prevent attackers from being able to take advantage of known vulnerabilities.
2. **Enable stronger authentication.** Always enable stronger authentication for an extra layer of security beyond the password that is available on most major email, social media and financial accounts. Stronger authentication (e.g., multi-factor authentication that can use a one-time code texted to a mobile device) helps verify that a user has authorized access to an online account.
3. **When in doubt, throw it out**. Links in email and online posts are often the way cyber criminals compromise your mobile devices. If it looks suspicious—even if you know the source—it's best to delete or, if appropriate, mark it as "junk email."
4. **Make your passwords long & strong**. Use complex passwords with a combination of numbers, symbols, and letters. Use unique passwords for different accounts.
5. **Secure your Wi-Fi network**. Your office and home wireless router is the gateway entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network, and your digital devices, by changing the factory-set default password and passwords.

Best Practices for Personal Use from Symantec's 2016 Internet Security Threat Report: https://www.symantec.com/about/newsroom/press-kits/istr-21:

- Research the capabilities and security features of an Internet of Everything (IoE) device before purchase.
- Perform an audit of IoE devices used on your network. Some refer to this as "Asset management". It is amazing how much equipment cannot be accounted for!
- Change the default credentials on devices.
- Use a strong encryption method when setting up Wi-Fi network access.
- Many devices come with a variety of services enabled by default. Disable features and services that are not required.
- Modify the default privacy and security settings of devices according to your requirements.
- Disable or protect remote access to IoE devices when not needed.
- Use wired connections instead of wireless where possible.
- Regularly check the manufacturer's website for firmware updates.
- Ensure that a hardware outage does not result in an unsecure state of the device.

International City/County Management Association (www.icma.org)

ICMA, the International City/County Management Association, advances professional local government through leadership, management, innovation, and ethics. Our vision is to be the leading professional association dedicated to creating and supporting thriving communities throughout the world.

Public Technology Institute (www.pti.org)

Created by and for cities and counties, the not-for-profit Public Technology Institute promotes innovation and collaboration for thought-leaders in government, and advances the use of technology to improve the management and delivery of services to the citizen.