AT-A-GLANCE: CYBERSECURITY

10 Tips to Know: Before an Cyberattack

1. **Use strong passwords that are 12 characters or longer.**
2. **Use a stronger authentication such as a PIN or password that only you would know.** Consider using a separate device that can receive a code or uses a biometric scan.
3. **Watch for suspicious activity** that asks you to do something right away, offers something that sounds too good to be true or needs your personal information. Think before you click.
4. **Check your account statements and credit reports regularly.**
5. **Use secure Internet communications.**
6. **Use sites that use HTTPS if you will access or provide any personal information.** Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a secure connection.
7. **Use antivirus and malware solutions, and firewalls to block threats.**
8. **Regularly back up your files** in an encrypted file or encrypted file storage device.
9. **Limit the personal information you share online.** Change privacy settings and do not use location features.
10. **Protect your home network by changing the administrative and WiFi passwords regularly.**

During A Cyberattack

- ✓ Check your credit card and bank statements for unrecognizable charges.
- ✓ Check your credit reports for any new accounts or loans you didn't open.
- ✓ Be alert for emails and social media users that ask for private information.
- ✓ If you notice strange activity, limit the damage by changing all of your internet account passwords immediately.
- ✓ Consider turning off the device that has been affected. Take it to a professional to scan for potential viruses and remove any that they find. Remember: **A company will not call you and ask for control of your computer to fix it. This is a common scam.**
- ✓ Let work, school or other system owners know what happened.
- ✓ Run a security scan on your device to make sure your system is not infected or acting more slowly or inefficiently.
- ✓ If you find a problem, disconnect your device from the Internet and perform a full system restore.

After A Cyberattack

- ✓ Contact banks, credit card companies and other financial service companies where you hold accounts.
- ✓ File a report with the Office of the Inspector General (OIG) if you think someone is using your Social Security number illegally.
- ✓ File a complaint with the FBI Internet Crime Complaint Center (IC3).
- ✓ File a report with the local police so there is an official record of the incident.
- ✓ Report identity theft to the Federal Trade Commission.
- ✓ If your Social Security number was compromised contact the Social Security Administration.
- ✓ If your driver's license or car registration has been stolen contact the Department of Motor Vehicles

Cuyahoga County Office of Emergency Management
P: 216-443-5700 | ema@cuyahogacounty.gov
@CuyahogaOEM
Facebook.com/CuyahogaOEM