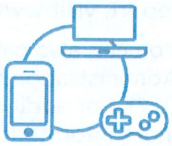
BE PREPARED FOR A CYBERATTACK

FEMA

FEMA P-2143/November 2020

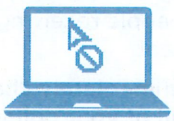
Cyberattacks can lead to loss of money, theft of personal information, and damage to your reputation and safety.

Cyberattacks are malicious attempts to access or damage a computer system.



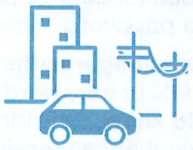
Can use computers, mobile phones, gaming systems, and other devices

Can include fraud or identity theft



Can block your access or delete your personal documents and pictures

May target children



May cause problems with business services, transportation, and power

PROTECT YOURSELF AGAINST A CYBERATTACK

Keep software and operating systems up-to-date.

Use encrypted (secure) internet communications.

Use strong passwords and two-factor authentication (two methods of verification).

Create backup files.

Watch for suspicious activity. When in doubt, don't click. Do not provide personal information.

Protect your home Wi-Fi network.

HOW TO STAY SAFE
WHEN A CYBERATTACK THREATENS

Keep your anti-virus software updated.

Use strong passwords that are 12 characters or longer. Use upper and lowercase letters, numbers, and special characters. Change passwords monthly. Use a password manager.

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** (e.g., fingerprint scanner).

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**.

Check your account statements and credit reports regularly.

Use secure internet communications. Use sites that use "HTTPS" if you will access or provide any personal information. Don't use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a secure connection.

Use antivirus solutions, malware, and firewalls to block threats.

Regularly back up your files in an encrypted file or encrypted file storage device.

Limit the personal information you share online. Change privacy settings and do not use location features.

Protect your home network by changing the administrative and Wi-Fi passwords regularly. When configuring your router, choose the Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES) setting, which is the strongest encryption option.

Limit the damage. Look for unexplained charges, strange accounts on your credit report, unexpected denial of your credit card, posts you did not make showing up on your social networks, and people receiving emails you never sent.

Immediately change passwords for all of your online accounts.

Scan and clean your device.

Consider turning off the device. Take it to a professional to scan and fix.

Let work, school, or other system owners know. Information Technology (IT) departments may need to warn others and upgrade systems.

Contact banks, credit card companies, and other financial accounts. You may need to place holds on accounts that have been attacked. Close any unauthorized credit or charge accounts. Report that someone may be using your identity.

File a report with the **Office of the Inspector General (OIG)** if you think someone is illegally using your Social Security number. **OIG reviews cases of waste, fraud, and abuse**. To file a report, visit www.idtheft.gov.

You can also call the Social Security Administration hotline at 1-800-269-0271. For additional resources and more information, visit http://oig.ssa.gov/report.

File a complaint with the FBI Internet Crime Complaint Center (IC3) at www.IC3.gov. They will review the complaint and refer it to the appropriate agency.

Learn tips, tools, and more at www.dhs.gov/stopthinkconnect.

FEMA

FEMA P-2143

Take an Active Role in Your Safety

Go to **Ready.gov** and search for **cyberattack**. Download the **FEMA app** to get more information about preparing for a **cyberattack**.