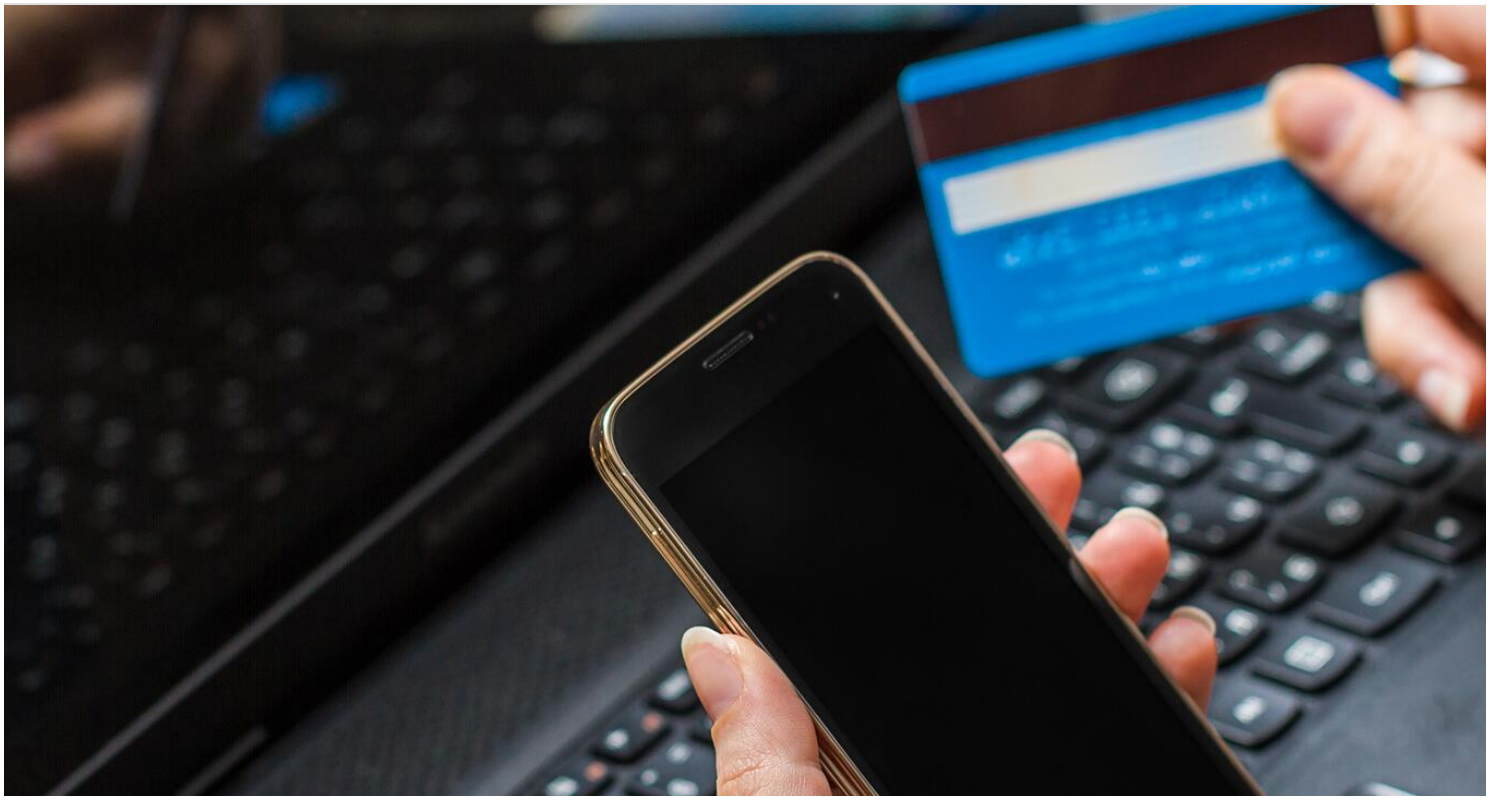
Ready

MENU



Cybersecurity

Protect Yourself | During an Attack | After an Attack | Additional Resources

Cybersecurity involves preventing, detecting and responding to cyberattacks that can have wide-ranging effects on individuals, organizations, the community and at the national level.

Cyberattacks are malicious attempts to access or damage a computer or network system. Cyberattacks can lead to loss of money, theft of personal, financial and medical information that can damage your reputation and safety.

Cyberattacks can occur in many ways, including:

Accessing your personal computers, mobile phones, gaming systems and other internet and Bluetooth connected devices.

Damaging your financial security, including identity theft.

Blocking your access or deleting your personal information and accounts.

Targeting children and adults.

Complicating your employment, business services, transportation and power grid.

Protect Yourself Against Cyberattacks

You can avoid cyber risks by setting up the proper controls. The following are things you can do to protect yourself, your family, and your property before a cyberattack occurs:

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

Keep software applications and operating systems up-to-date.

Using a password manager, use upper and lowercase letters, numbers and special characters, as well as, two-factor authentication (two methods of verification).

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, and when in doubt, do NOT click. Do not provide personal information.

Use encrypted (secure) Internet communications.

Protect your home and/or business on a strong, using a secure Internet connection and Wi-Fi network.

Use a stronger authentication such as a personal identification number (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 or facial recognition).

Check your account statements and credit reports regularly.

Only share personal information on secure sites (e.g. “https://”). Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a more 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.

Protect your home network by changing the administrative and Wi-Fi passwords regularly. When configuring your router, use either the instruction manual or speak to your internet-cable provider, to setup the Wi-Fi Protected Access 2 (WPA2) Advanced Encryption Standard (AES) setting, which is the strongest encryption option.

Regarding COVID-19:

Be cautious about sharing personal financial information, such as your bank account number, social security number, or credit card number.

Do not click on links in texts or emails from people you don’t know. Scammers can create fake links to websites. Visit government websites, like cdc.gov/coronavirus, directly in your internet browser.

Know that the government will not text or call you about “mandatory online COVID-19 tests,” outbreaks “in your area,” mandatory vaccinations, or to sell you COVID-19 cures.

Remember that the government will not call or text you about owing money or receiving economic impact payments.

Be aware that scammers may try to contact you via social media. The government will not contact you through social media about owing money or receiving payments.

If you have been exposed to COVID-19, a contact tracer from your local health department might call you to let you know and ask you to self-quarantine at home away from others. Discussions with health department staff are confidential. They will not ask for financial information.

Keep in mind that scammers may try to take advantages of financial fears by calling with

work-from-opportunities, debt consolidation offers, and student loan repayment plans.

During a Cyberattack

Check your credit statement for unrecognizable charges.

Check your credit reports to be aware of open accounts and/or loans you did not open.

Be alert for soliciting emails and social media users asking for private information.

If you notice strange activity, (e.g. inappropriate pop-up windows), limit the damage by immediately changing all of your internet account passwords.

Consider turning off the device. Take it to a professional to scan for potential viruses and fix. If you take your device to a store or local business, contact them in advance. Many companies have new guidelines to protect employees and individuals during the COVID-19 pandemic.

Let work, school or other system owners know.

Contact banks, credit card companies and other financial services companies where you hold 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.

Check to make sure the software on all of your systems is up-to-date.

Run a security scan on your computer/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

If you believe you have been a victim of a cyberattack, let the proper federal, state and local authorities know:

File a report with the Office of the Inspector General (OIG) if you think someone is illegally using your Social Security number.

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

File a report with the local police so there is an official record of the incident.

Report identity theft to the Federal Trade Commission.

Contact the Federal Trade Commission (FTC) at ftc.gov/complaint if you receive messages from anyone claiming to be a government agent.

Contact additional agencies depending on what information was stolen. Examples include contacting:

the Social Security Administration (800-269- 0271) if your social security number was compromised, or

the Department of Motor Vehicles if your driver's license or car registration has been stolen.

Report online crime or fraud to your local United States Secret Service (USSS) Electronic Crimes Task Force or the Internet Crime Complaint Center.

Engage virtually with your community through video and phone calls. Know that it’s normal to feel anxious or stressed. Take care of your body and talk to someone if you are feeling upset. Many people may already feel fear and anxiety about the coronavirus 2019 (COVID-19). The threat of a cyber attack can add additional stress. Follow CDC guidance for managing stress during a traumatic event and managing stress during COVID-19.

Additional Resources

- Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency
- Cyberattack Information Sheet(PDF)
- DHS Stop.Think.Connect.™ Campaign
- Federal Bureau of Investigation
- National Cyber Security Alliance
- Internet Crimes Against Children Taskforce
- NetSmartz

- iKeepSafe
- iSafe
- CFPB: How to Avoid COVID-19 Government Imposter Scams
- FCC COVID SCAMS
- FDIC Consumer News: COVID-19 and Your Financial Health

Last Updated: 03/16/2021

Disasters and Emergencies

All Hazards

Emergency Alerts

Attacks in Public Places

Avalanche

Bioterrorism

Chemical Emergencies

Cybersecurity

Drought

Earthquakes

Explosions

Extreme Heat

Floods

Hazardous Materials Incidents

Home Fires

Household Chemical Emergencies

Hurricanes

Landslides & Debris Flow

Nuclear Explosion

Nuclear Power Plants

Pandemic

Power Outages

Radiological Dispersion Device