Cyber Attack

Often times, we may not realize that our actions online might put us, our families, and even our country at risk. Learning about the dangers online and taking action to protect ourselves is the first step in making the Internet a safer place for everyone. Cybersecurity is a shared responsibility and we each have a role to play.

Cybersecurity involves protecting that infrastructure by preventing, detecting, and responding to cyber incidents. Unlike physical threats that prompt immediate action–like stop, drop, and roll in the event of a fire–cyber threats are often difficult to identify and comprehend. Among these dangers are viruses erasing entire systems, intruders breaking into systems and altering files, intruders using your computer or device to attack others, or intruders stealing confidential information. The spectrum of cyber risks is limitless; threats, some more serious and sophisticated than others, can have wide-ranging effects on the individual, community, organizational, and national level. These risks include:

- Organized cybercrime, state-sponsored hackers, and cyber espionage can pose national security risks to our country.
- Transportation, power, and other services may be disrupted by large scale cyber incidents. The extent of the disruption is highly uncertain as it will be determined by many unknown factors such as the target and size of the incident.
- Vulnerability to data breach and loss increases if an organization's network is compromised. Information about a company, its employees, and its customers can be at risk.
- Individually-owned devices such as computers, tablets, mobile phones, and gaming systems that connect to the Internet are vulnerable to intrusion. Personal information may be at risk without proper security.

Before:

You can increase your chances of avoiding 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 cyber incident occurs.

- Only connect to the Internet over secure, password- protected networks.
- Do not click on links or pop-ups, open attachments, or respond to emails from strangers.
- Always enter a URL by hand instead of following links if you are unsure of the sender.
- Do not respond to online requests for Personally Identifiable Information (PII); most organizations – banks, universities, companies, etc. – do not ask for your personal information over the Internet.
- Limit who you are sharing information with by reviewing the privacy settings on your social media accounts.
- Trust your gut; if you think an offer is too good to be true, then it probably is.
- Password protect all devices that connect to the Internet and user accounts.

- Do not use the same password twice; choose a password that means something to you and you only; change your passwords on a regular basis.
- If you see something suspicious, report it to the proper authorities.

The extent, nature, and timing of cyber incidents are impossible to predict. There may or may not be any warning. Some cyber incidents take a long time (weeks, months or years) to be discovered and identified. Familiarize yourself with the types of threats and protective measures you can take by:

- Signing up for the United States Computer Emergency Readiness Team (US-CERT) mailing list to receive the latest cybersecurity information directly to your inbox. Written for home and business users, alerts provide timely information about current security issues and vulnerabilities. Sign up here.
- Becoming a *Friend* of the Department of Homeland Security's Stop.Think.Connect. Campaign and receive a monthly newsletter with cybersecurity current events and tips. Sign up here.

During:

Immediate Actions

- Check to make sure the software on all of your systems is up-to-date.
- Run a scan to make sure your system is not infected or acting suspiciously.
- If you find a problem, disconnect your device from the Internet and perform a full system restore.

At Home

- Disconnect your device (computer, gaming system, tablet, etc.) from the Internet. By removing the Internet connection, you prevent an attacker or virus from being able to access your computer and perform tasks such as locating personal data, manipulating or deleting files, or using your device to attack others.
- If you have anti-virus software installed on your computer, update the virus definitions (if possible), and perform a manual scan of your entire system. Install all of the appropriate patches to fix known vulnerabilities.

At Work

- If you have access to an IT department, contact them immediately. The sooner they can investigate and clean your computer, the less damage to your computer and other computers on the network.
- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can

be alert for any suspicious or unusual activity.

At a Public Place (library, school, etc.)

- Immediately inform a librarian, teacher, or manager in charge. If they have access to an IT department, contact them immediately.

Immediate Actions if your Personally Identifiable Information (PII) is compromised:

PII is information that can be used to uniquely identify, contact, or locate a single person. PII includes but is not limited to:

- Full Name
- Social security number
- Address
- Date of birth
- Place of birth
- Driver's License Number
- Vehicle registration plate number
- Credit card numbers
- Physical appearance
- Gender or race

If you believe your PII is compromised:

- Immediately change all passwords; financial passwords first. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- If you believe the compromise was caused by malicious code, disconnect your computer from the Internet.
- Restart your computer in safe mode and perform a full system restore.
- Contact companies, including banks, where you have accounts as well as credit reporting companies.
- Close any accounts that may have been compromised. Watch for any unexplainable or unauthorized charges to your accounts.

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

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

- If your PII was compromised, consider other information that may be at risk. Depending what information was stolen, you may need to contact other agencies; for example, if someone has gained access to your Social Security number, contact the Social Security Administration. You should also contact the Department of Motor Vehicles if your driver's license or car registration has been stolen.
- For further information on preventing and identifying threats, visit US-CERT's Alerts and Tips page.

This information is taken from: http://www.ready.gov/cyber-attack

This and other training modules from this website will be helpful to your family and you as an ARES member. It might be advisable to print these modules out and keep them in a binder for your family to be able to refer to in your absence. Being prepared is no accident.