Courtesy of RiskSOURCE Clark-Theders

Unlike physical threats that prompt immediate action—like stopping, dropping and rolling if you catch on fire—cyber threats are often difficult to identify and understand. Cyber threats include dangers such as viruses erasing entire systems, intruders breaking into systems and altering files, intruders using your computer or device to attack others and 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 levels.

Before a Cyber Attack

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—such as banks, universities and businesses—will never 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 instincts. If you think an offer is too good to be true, it probably is.

RISKSOURCE® CLARK-THEDERS

- Password-protect all devices that connect to the internet and all 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 (every 90 days or so).
- 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.

During a Cyber Attack
Here are some of the steps you should take during a cyber attack:

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 (e.g., computers, gaming systems or tablets) 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 someone in it immediately. The sooner someone 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.

More About PII
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 licence number
- Vehicle registration plate number
- Credit card numbers
- Physical appearance
- Gender or race

Take these steps if you believe your PII has been compromised:
- Immediately change all passwords, and change your 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 businesses, 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.

Public Locations

- Immediately inform a manager or authority figure in charge. If someone has access to an IT department, contact the department immediately.

After a Cyber Attack

- File a report with the local police so there is an official record of the incident.
- Report online crime or fraud to the Internet Crime Compliant Center (IC3) or the federal government's internet fraud resource website. 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. You should also contact your state's DMV for transportation if your driver's license or car registration has been stolen.

In addition to insuring your home, RiskSOURCE Clark-Theders is committed to helping you and your loved ones stay safe when disaster strikes. If you would like more information on how to protect yourself from a cyber attack, please contact us at 513.779.2800 or www.risksource.com today.