Cybersecurity

Cybersecurity involves preventing, detecting, and responding to cyber incidents that can have wide ranging effects on the individual, organizations, the community and at the national level.

Before a Cyber Incident

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.
- Familiarize yourself with the types of threats and protective measures you can take by:
    - **Sign up** for the United States Computer Emergency Readiness Team mailing list.
    - **Sign up** for the Department of Homeland Security's Stop.Think.Connect. Campaign and receive a monthly newsletter with cybersecurity current events and tips.

During a Cyber Incident

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.
- If in a public setting immediately inform a librarian, teacher, or manager in charge to contact their IT department.
- Report the incident to your local police so there is a record of the incident. You may also contact federal agencies able to provide assistance and investigate the incident:
    - FBI **field offices** and **Internet Crime Complaint Center**
    - **National Cyber Investigative Joint Task Force**
      or call 855-292-3937
    - U.S. Immigration and Customs **field offices** or **cyber crimes**
      or call 866-347-2423
    - **National Cybersecurity and Communications Integration Center** or call 888-282-0870
    - **U.S. Computer Readiness Team**

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.

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.
- 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.

After a Cyber Incident

- 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 additional agencies depending on what information was stolen. Examples include contacting the Social Security Administration if your social security number was compromised, or 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.