OFFICE OF EMERGENCY MANAGEMENT

Cyber Preparedness

Background

The widespread availability of computers and connections to the Internet provides everyone with 24/7 access to information. Unfortunately, some individuals exploit the Internet through criminal behavior and other harmful acts. Criminals can try to gain unauthorized access to your computer and then use that access to steal your identity, commit fraud, or even launch cyber attacks against others. By following cyber security practices, you can limit harm not only to your computer, but to everyone's computer.

TERMINOLOGY	
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.
Cyber Security	The ability to protect or defend the use of cyberspace from cyber attacks.
Cyberspace	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Precautionary Measures

- 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); Remember, 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. Never share your password.
- If you see something suspicious, report it to the proper authorities.
- Check to make sure the software on all of your systems is up-to-date.

During a Cyber Attack – Immediate Actions

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 should be alerted for any suspicious or unusual activity.

If you think your Personally Identifiable Information (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 and watch for any unexplainable or unauthorized charges to your accounts.

After

- Report online crime or fraud and file a report with the local police, the Electronic Crimes Task Force and the Internet Crime Complaint Center, so there is an official record of the incident.
- Report identity theft to the Federal Trade Commission.
- If your PII was compromised, consider other information that may be at risk.
- Depending on what information was stolen, you may need to contact other agencies; for example, if someone has gained access to your Social Security number and/or your drivers license and car registration, you will need to contact the Social Security Administration and the Department of Motor Vehicles.