Protecting Your Personal Information

- **Data Capture** – Cyber criminals can use special tools to capture information sent over the Internet and over wireless network connections.

  How to Protect Yourself
  - ✓ Do not send sensitive information such as Social Security numbers, credit card numbers, userIDs and passwords, etc. in unencrypted email. Some emails are sent in plain text over the Internet and can be read by anyone with the proper tools and know how.
  - ✓ Do not use unsecure public wireless access points to access your online banking account, social networking sites or to shop online. Cyber criminals can use special tools to intercept the wireless communications and collect your userIDs, passwords, and credit card numbers.
  - ✓ Make sure your home wireless network uses WPA2 as its encryption protocol. If you use WEP or WPA encryption on your wireless network, it is not secure and you should upgrade to WPA2 as soon as possible.
  - ✓ Use a strong passphrase instead of a short password to protect your account.

- **Infected Web sites** – Cyber criminals use legitimate web sites to infect your computer with malware. They usually accomplish this by injecting malicious code in the site's hypertext links or advertising banners that either download malware to your computer or redirect you to malicious web sites. These "drive-by" type attacks are common place and can be very dangerous.

  How to Protect Yourself
  - ✓ Try to visit only reputable sites. Sometimes, these web sites also get infected too, so be careful everywhere.
  - ✓ Watch out for typo scamming. This tactic is also known as "cybersquatting" and "typo-squatting" and is often used by cyber criminals with the hope that you will be directed to their site because you mistyped a well-known site's address such as cnn.com. For example, it is possible that a cyber criminal could create a malicious site using the domain name DNN.com, hoping to get hits from people looking for CNN.com. When people mistakenly visit the DNN.com site, malware would be installed on their computers.
  - ✓ Avoiding clicking on advertising banners and popup windows.
  - ✓ Preview hyptertext links before clicking on them. You can do this by hovering your mouse curser over the link. Your Internet browser should display the link's address in the message bar at the bottom of the page. Don't click on links that appear to redirect you to non-legitimate sites.
  - ✓ Install anti-virus software and keep it updated.

- **Phishing Email** – This is a favorite of thieves that involves them masquerading as a legitimate source such as a familiar company or someone you know. Phishing usually involves a variety of phony scenarios to convince you to either send money or provide your personal information such as Social Security numbers, credit card numbers, or online banking credentials. Phishing is a big business right now that makes big money for cyber criminals.

  How to Protect Yourself
  - ✓ Never provide your personal information in response to unsolicited email requests. Generally, businesses do not request personal information such as online banking credentials or Social Security numbers via email. If in doubt, call the company using a number that you have located from a legitimate telephone listing. Never call the number listed in the email.
  - ✓ Do not open suspicious or unsolicited email, delete it instead.
  - ✓ Do not open email attachments or click on links in unsolicited email.
  - ✓ Install anti-virus and anti-spyware software and keep it updated.
  - ✓ Keep all of your computer's software updated with the latest security updates including the operating system, application software, and add-ons and plug-ins such as browser plug-ins.
  - ✓ Only share your primary email address with those you know.
  - ✓ Do not post your primary email address on social networking or job-posting sites.
  - ✓ Check a website's privacy policy before providing your email address to ensure that it will not be provided to third parties. Many sites allow you to opt out of sharing your personal information.

- **Malicious Email** – This category is generally unsolicited email that contains malware, which is activated by clicking on a link within the email or opening an attached document.

  How to Protect Yourself
  - ✓ Do not open suspicious or unsolicited email, delete it instead.
  - ✓ Do not open email attachments or click on links in unsolicited email.
  - ✓ Install anti-virus and anti-spyware software and keep it updated.
  - ✓ Install a firewall and keep it turned on.
  - ✓ Keep all of your computer's software updated with the latest security updates including the operating system, application software, and add-ons and plug-ins such as browser plug-ins.

- **Downloads** – Malicious code can be hidden in shareware, pirated software, music or videos. By installing or downloading the files to your computer, you could install malicious code or a back door to your computer that cyber criminals can use to gather your personal information.

  How to Protect Yourself

  ✓ Do not download pirated software, music or videos.
  ✓ Avoid downloading files from peer-to-peer (P2P) networks.
  ✓ Download shareware or free software only from reputable sites.