

Protect Yourself on the World Wide Web

- Never open an email spam or other emails from unknown sources. They may perhaps contain viruses or other programs that make your computer vulnerable to attack.
- Never click on a link in an email claiming to need financial or personal information from anyone and never provide personal or account information to unknown parties or unsecured websites.
- Don't put any personal information such as credit cards or your social security on any website that you are not familiar with and are not sure is valid and secured.
- Be aware of techniques for redirecting website users to "cloned" replica sites without their knowledge, also known as "pharming." Watch for odd error messages, unexpected page layout, content or other strange site behavior.
- To keep hackers from stealing information on your computer:
 - install a firewall and make sure it's turned on
 - install virus protection software and keep it updated
 - keep administrative names and passwords up to date
 - set wireless networks to "no broadcast"
 - and be sure to power down your computer when it's not being used.
- Be cautious when downloading anything in an email until you can verify the validity of the source. This includes the new social media platforms such as Facebook and You Tube.
- Before getting rid of your computer, eliminate all storage drives. Don't rely on the "delete" or trash function to remove files containing sensitive information.