Cyber Security

As the number of mobile users, digital applications, and data networks increase and as technology keeps changing at an astounding rate, so do the opportunities for cyber threats and exploitation. Cybercriminals are finding new and creative ways to manipulate users and technology all the time, creating network outages, compromised data, computer viruses, and other incidents that affect our lives in ways that range from inconvenient to life-threatening.

What is Cyber Security?

Cyber security focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, alteration, or destruction.

Why is Cyber Security Important?

Many individuals and businesses collect, process, and store a great deal of confidential information on a variety of devices (i.e. computers, tablets, mobile phones) and transmit that data across various networks to other devices. With the growing number and complexity of cyber-attacks, ongoing attention and care are required to protect sensitive personal and business information.

Protect Yourself and Your Devices – Here's How:

- Never click on links in suspicious emails. They could contain viruses and malware that could contaminate your device. If you do think the email is legitimate, go to the site and log on directly or hover over the link in the email, which will display the actual destination. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.
- Never open the attachments in suspicious emails. They could contain viruses and malware that could infect your device. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.
- Be suspicious of unknown links or requests sent through text messages. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.
- Do not give out personal information over the phone or on your cell phone for something you did not initiate. If contacted over the phone by someone claiming to be a retailer, collection agency, or someone you know (i.e. relative, employee from doctor office or bank), do not

give out your personal information. Ask them to provide you their name and a call-back number or locate the company's valid contact information. Just because they may have some of your information does not mean they are legitimate!

- **Do not give out personal information through emails.** If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- **Set secure passwords and don't share them with anyone.** Avoid using common words, phrases, or personal information and update regularly.
- **Keep your operating system, browser, anti-virus and other critical software up to date.** Security updates and patches are available for free from major companies.
- **Pay close attention to website URLs.** Malicious websites sometimes use a variation in common spelling (i.e. "Goooogle.com" instead of "Google.com," "Equifacks.com" instead of "Equifax.com") or a different domain (i.e. ".com" instead of ".net") to deceive unsuspecting computer users. This is known as typosquatting, or URL hijacking, which is a form of cybersquatting that is used by fraudsters to redirect users in order to gain information to commit crimes.

Helpful Tips:

Phishing attacks may appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as:

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

Some email messages are more suspicious than others, but be especially cautious if the message has any of the characteristics listed below. These characteristics are just guidelines—not every suspicious email has these attributes, and some legitimate messages may have some of these characteristics:

- it suggests tragic consequences for not performing some action
- it promises money or gift certificates for performing some action
- it offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- it claims it's not a hoax
- there are multiple spelling or grammatical errors, or the logic is contradictory
- there is a statement urging you to forward the message

- it has already been forwarded multiple times (evident from the trail of email headers in the body of the message)

The Internet offers convenient shopping, but it is also convenient for attackers, giving them multiple ways to access the personal and financial information of unsuspecting shoppers. You can protect yourself!

- Do business with reputable vendors. Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor. If an organization wants to have a secure web site that uses encryption, it needs to obtain a site, or host, certificate. There are two elements that indicate that a site uses encryption:
  - a closed padlock, which, depending on your browser, may be located in the status bar at the bottom of your browser window or at the top of the browser window between the address and search fields
  - a URL that begins with "https:" rather than "http:"
- Use a credit card. There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Additionally, because a debit card draws money directly from your bank account, unauthorized charges could leave you with insufficient funds to pay other bills. You can minimize potential damage by using a single, low-limit credit card to making all of your online purchases. Also use a credit card when using a payment gateway such as PayPal, Google Wallet, or Apple Pay.
- Check privacy policies. Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.