Tips on Protecting Yourself from Fraud

Email Fraud- Know What to Watch for

A few common giveaways for fraudulent emails are:

- Requests for personal information, such as bank account numbers, passwords, credit/debit card number, mother's maiden name, or Social Security number.
- Do not address you by name or not acknowledging the company with which you do business
- Include a sense of urgency, such as alert you that your account will be shut down unless you confirm your information
- Warn you that you've already been a victim of fraud
- Contain spelling or grammatical errors

Avoiding Credit Card Fraud

- Don't give out your credit card number unless the site is secure and reputable. Look for security symbols/icons on the page
- Do your homework on the company or individual to ensure they are legitimate
- Look for a physical address rather than just a Post Office box. Check for a phone number and call to make sure it is correct and working
- Be cautious when dealing with individuals/companies from outside your own country

Telephone Fraud Protection

- Unless you have initiated the call, it's best to avoid giving out account or personal information over the phone
- When in doubt, ask for more information about the organization calling or the offer being presented
- Never feel obligated to provide your personal information or account numbers over the phone
- Stay informed so you're aware of the latest trends in telephone fraud
- If you don't feel comfortable with the phone call, hang up and dial your financial institution or the company they were claiming to be

Save the Social Media Vacation Posts until You Get Back Home

It may be tempting to post details of where and when you'll be traveling, but **don't**. By revealing such specifics, you are providing information that could be used by criminals to target your home while you're gone. Another common scam involves compromising email accounts to contact your friends or family with requests for help, claiming that you were robbed while on vacation and need money. Sending private posts and photos during your vacation to family and friends is OK, but if you post them publicly, you increase the risk of someone using that information for malicious activities. Also, make sure your children understand what, and when, they should post regarding your vacation plans.

Do Not Use Public Computers and Public Wireless Access for Sensitive Transactions

Wi-Fi spots in airports, hotels, train stations, coffee shops and other public places can be convenient, but they're often not secure and can leave you at risk. If you're online through an unsecured network, you should be aware that individuals with malicious intent may have established a Wi-Fi network with the intent to eavesdrop on your connection. This could allow them to steal your credentials, financial information or other sensitive and personal information. It's also possible that they could infect your system with malware. Any free Wi-Fi should be considered "unsecure." Therefore, be cautious about the sites you visit and the information you release. Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi. Also, consider using a cellular 3G/4G connection, which is generally safer than a Wi-Fi connection.