Shopping Online Securely

The holiday season is near. Many of us will be looking to buy the perfect gift and shop online. Unfortunately, cyber criminals will be active as well, creating fake shopping websites and other online shopping scams to steal your information or money.

Holiday Scams

- **Fake Online Store**
  - Criminals create fake websites that look like well-known stores and brands.
  - You can end up with counterfeit or stolen items.
- **Counterfeit or Stolen Items**
  - Criminals mimic the look of real sites or use the names and logos of well-known stores or brands.
- **Phishing**
  - Criminals create fake online stores that attempt to trick you into giving away sensitive information.
- **Text Messages**
  - Scammers on Legitimate Websites
  - Large-scale, automated email or text messages can make it look like they are coming from reputable companies.
- **Email Attachments**
  - Scammers may embed malicious links or files in emails to trick you into taking action.
- **Vishing**
  - Scammers may call you impersonating a financial institution.
- **Social Media**
  - Scammers may post ads for free trials or discounted merchandise.

Fraud Prevention Tips

- **Secure Site**
  - Use secure sites. Verify the security of the website by looking for the small padlock symbol in the browser bar.
  - Double-click on the URL in your browser to see if the website address begins with HTTPS (not HTTP).
- **Secure Your Account**
  - Protect your account by using a strong password for each of your accounts.
  - Enable two-factor authentication (2FA) for added security.
  - Regularly update your browser, and other software to increase your resistance to common malware, phishing, and other common attacks.
- **Monitor Your Transactions**
  - Track your transactions and report any suspicious activity immediately.
- **Third Party Service Providers**
  - Be cautious of any link or attachment provided in an email.
  - Be suspicious of ads or promotions on search engines or social media that are significantly lower than those you see at legitimate websites.
  - If you receive a suspicious or fraudulent correspondence claiming to be from Amazon or another service provider, do not click on any links or attachments.
- **If You Become a Victim - Notify**
  - If you believe you have been scammed on an online purchase, report it immediately.
  - If you think you've entered your password on a fraudulent website, go to the authentic site and change your password immediately.
  - If you believe your credit card has been compromised, contact your bank immediately.
  - If you entered your payment information on a website or mobile app, contact your financial institution immediately.
  - If you receive a suspicious or fraudulent correspondence claiming to be from a legitimate organization, do not click on any links or attachments.
  - If you are notified that your credit card has been cancelled, and your voicemail informs you that your credit card has been cancelled, and you must call a number back to reactivate it, do not do so.
  - If you receive a voicemail saying your credit card has been cancelled, and the credit card has been cancelled, and you must call a number back to reactivate it, do not do so.