Beware – Online Scams

Any of us are susceptible to online scams…below are just a few examples. If you have any questions, or feel you have been solicited by a scammer please contact our Customer Service department at 903-759-0751 and they will help research your account for any possible fraudulent activity!

1. **Social Media scams** – Scammers can use sites like Facebook and Twitter to scam consumers during the holidays. Be careful when liking Fan Pages, clicking on fake alerts from friends' accounts that have been hacked, or installing suspicious "deals" or apps that give your private data away. Also beware of Twitter ads and special discounts for popular gifts using blind, shortened links. It's always best NOT to click on the link embedded in…go straight to the website from your web browser. If the deal is real it will be on the website.

2. **Malicious Mobile Apps** – Be careful not to download a malicious application designed to steal information or send out premium-rate text messages. Make sure that you only download applications from official app stores and check other users' reviews and the app's permission policies.

3. **Travel Scams** – It's vacation season! Before booking travel arrangements, beware of scams with too-good-to-be-true deals, phony travel webpages with beautiful pictures and rock-bottom prices. The Federal Bureau of Investigation (FBI) also warns travelers of a hotel Wi-Fi scam where a malicious pop-up ad prompts computer users to install a popular software product before connecting to their hotel Wi-Fi. Do a security software update before traveling to guard against the latest scam. DO NOT go to your confidential bank account online or other confidential type websites on a hotel, restaurant, or other UNSECURE Wi-Fi setup.

4. **Shopping Spam/Phishing** – Cheap Rolex watches and pharmaceuticals may be advertised as the "perfect gift" while "gift themed" emails may try to trick you into revealing financial or personal details by posing as an offer from a legitimate business.

5. **The iPad, iPhone, and other hot gift scams** - Cybercrooks are likely to mention must-have gifts in dangerous links, phony contests and phishing emails.

6. **Skype Message Scare** – A Skype message scam attempts to infect victims' machines, and hold their files for ransom. The threat appears as a Skype instant message with the scam line "Lol is this your new profile pic?" Clicking on the link downloads a Trojan onto the computer.

7. **Bogus gift cards** – Be wary of buying gift cards from third parties and buy instead from the official retailer.

8. **SMISHing of phishing via text message** – We all text! How many times a day! The scammer tries to lure you into revealing information by pretending to be a legitimate organization.

9. **Phony E-tailers** – Phony e-commerce sites that appear real will try to lure you into typing your credit card number and other personal details.

10. **Fake Charities** – Cybercriminals may try to fool you into thinking that they are a real charity, such as the Red Cross, with a "stolen logo and copycat text." It is safer to visit the charity's legitimate website directly.

11. **Dangerous e-cards** – Some are malicious and may contain spyware or viruses, or download a Trojan.

12. **Phony classifieds** – Phony offers may ask for too much personal information or ask you to wire funds via Western Union.

13. **Craigslist Scams** – Buying and selling on Craigslist can be safe. Just be cautious at all times. If you sold an item and are expecting to receive a specific amount in the mail, but you receive a check for much more (typically $2,000 or $3,000) then it is a fraud. DO NOT send the item you sold to the person, DO NOT follow the instructions in the letter that will be included with the check to "deposit the check and send them the difference".

14. **Phantom Debt-Fake Collections Scam** - This scam is similar to the jury subpoena/fake arrest scam. The victim receives a telephone call or email/written notification form what appears to be a Law Enforcement agency stating they have an outstanding Insufficient Check from several years ago that had not been made good. Demand is for instant payment via Money Order or similar transaction or else an arrest warrant will be issued.

15. **$9.84 credit charge scam** – If you see a charge for $9.84 on your statement give it a hard look. Scanners are charging stolen card numbers for a small amount of money, and many recent victims were billed $9.84. The scammers believe few cardholders will review such a small amount – and the card companies won't aggressively investigate them. Cybercriminal gangs from Cyprus, the United Kingdom, and India are known for purchasing stolen credit card numbers on the black market and making fraudulent $9.84 charges.