10 Tips for Avoiding Online Scams

International scam artists use clever schemes to defraud millions of people around the world each year, threatening financial security and generating substantial profits for criminal organizations and common crooks. Being on guard online can help you minimize your chance of becoming a victim of an online scam. The Federal Trade Commission offers the following 10 tips to help you stay safe online.

1. **Don't send money to someone you don't know,** such as an online merchant you've never heard of. It's best to do business with companies you know and trust. If you buy items through an online auction, consider a payment option that provides protection, like a credit card. Don't send cash or use a wire transfer service, and don't pay upfront fees for the promise of a big pay-off—whether it's a loan, a job or prize money.

2. **Don't respond to e-mails, phone calls, text messages or ads that ask for your personal or financial information.** Don't click on links or call phone numbers included in the message, either. The crooks behind these messages are trying to trick you into sending money and revealing your bank account information.

3. **Don't play a foreign lottery.** Not only is it illegal to play foreign lotteries, but it's also a sure way to lose a lot of money. Don't be tempted by messages that boast enticing odds in a foreign lottery or messages that claim you've already won. Inevitably, you'll be asked to pay "taxes," "fees," or "customs duties" to collect your prize. If you send money, you won't get it back, regardless of the promises.

4. **Remember that wiring money is like sending cash: Once it's gone, you can't get it back.** Criminals often insist that people wire money, especially overseas, because it's nearly impossible to reverse the transaction or trace the money. Don't wire money to strangers, to sellers who insist on wire transfers for payment or to someone who claims to be a relative in an emergency (and wants to keep the request a secret).

5. **Don't agree to deposit a check from someone you don't know and then wire money back, no matter how convincing the story.** By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. You are responsible for the checks you deposit: When a check turns out to be a fake, you'll be responsible for paying back the bank.

6. **Read your bills and monthly statements regularly.** Scammers steal account information and then run up charges or commit crimes in your name. Dishonest merchants sometimes bill you for monthly "membership fees" and other goods or services you didn't authorize. If you see charges you don't recognize or didn't agree to, contact your bank, card issuer or other creditor immediately.

7. **In the wake of a natural disaster or another crisis, give to established charities rather than one that seems to have sprung up overnight.** Pop-up charities probably don't have the infrastructure to get help to the affected areas or people, and they could be

collecting the money to finance illegal activity. Check out www.ftc.gov/charityfraud to learn more.

8. **Talk to your doctor before buying health products or signing up for medical treatments.** Ask about research that supports a product's claims—and possible risks or side effects. Buy prescription drugs only from licensed U.S. pharmacies. Otherwise, you could end up with products that are fake, expired or mislabeled—in short, products that could be dangerous. Visit www.ftc.gov/health for more information.

9. **Keep in mind that if something sounds too good to be true, it probably is.** If someone contacts you promoting low-risk, high-return investment opportunities, stay away. When you hear pitches that insist you act now, guarantees of big profits, promises of little or no financial risk or demands that you send cash immediately, report them at www.ftc.gov.

10. **Know where an offer comes from and who you're dealing with.** Try to find a seller's physical address (not just a P.O. Box) and phone number. With Voice over Internet Protocol (VoIP) services and other web-based technologies, it's tough to tell where someone is calling from. Do an Internet search for the company name and website and look for negative reviews. Check them out with the Better Business Bureau at www.bbb.org.

For more information and practical tips on guarding against Internet fraud, securing your computer and protecting your personal information, visit www.onguardonline.gov.

These tips are provided by Charter Bank