

RISK Alert

exclusively for Bond Policyowner

Date:
11/21/2011

Risk type:
Other

States:
All states

Holiday Shopping Alert

As the holiday season approaches, it is important to be aware of potential scams. Con artists are working hard to get their hands on your member's money as well as personal and financial information. To help reduce the risk and protect credit union members, we offer a list of potential scams along with tips for a safer and smarter holiday shopping season.

Alert Details

Many consumers will be using their mobile devices and computers to conduct their holiday shopping and so will the cyber scammers! Mobile device scams are a top threat this year based on the increase in mobile malware and malicious apps. Consumers should be aware of all potential threats in order to safeguard their funds and personal information this holiday season. Let's work together to keep the scammers away from credit unions and your members. Potential scams and tips to be aware of and share with your members are listed below.

Holiday Scams and Tips

- Watch for mobile malware – especially deals for black Friday and cyber Monday.
- Be cautious when looking for free mobile apps - may be an attempt to steal information.
- Watch for malicious screensavers, ring tones and e-cards.
- Watch for purchase offers of fake anti-virus software – this scam may trick you into purchasing the software.
- Secure your computer – at a minimum, have anti-virus, anti-spyware and a firewall.
- Remember to turn off your computer when you're done shopping.
- Watch for social media scams – phony Facebook and Twitter sites or other online promotions and contests.
- Beware of scammers advertising popular holiday items.
- Check out the seller of items – research before you buy.
- Don't fall for the mystery shopping scam asking you to shop for \$XX dollars (ex: \$100).
- Online coupon scams may ask for your personal or financial information using email.
- Holiday phishing scams – Don't fall for emails, text messages or phone calls asking for personal or financial information.
- Monitor credit, debit and account numbers used for your holiday shopping to help identify any unauthorized usage.
- Vacation scams – don't post holiday pictures until you are back home.
- Lighted parking lots – survey the parking lot surroundings. Make sure you have your car keys in your hands before entering the parking lot.
- If an offer or item sounds too good to be true, it's probably a scam.
- Report scams to the Federal Trade Commission at www.ftc.gov or call toll-free 1.877.ftc.help (1.877.382.4357)

Related Resources

- [Protection Resource Center](#) for additional RISK Alerts and/or white papers (id/password required)