Holiday Scams Alert

Alert Details

Consumers around the country are gearing up for the holiday shopping season. Fraudsters are also preparing for the holiday season to prey upon unsuspecting consumers. Ongoing awareness of these scams is critical to help members protect their personal and financial information this holiday season.

Risk Prevention Tips

- Secure home computers and mobile devices: Members should ensure their home computers are secure with a firewall and antivirus software before performing any online transactions. Operating system patches should be downloaded when made available by software vendors. Members should also protect mobile devices (mobile phones, tablets, etc.) used to conduct online transactions by installing antivirus software.
- Phishing scams: Members should not respond to emails, text messages, and phone calls that advertise the sale of gift cards, holiday gifts, promotions, contests and jobs.
- Be wary of holiday offers for free items: Members should avoid tempting holiday offers, such as free downloadable applications for smartphones, antivirus software, screen savers, ring-tones and electronic greeting cards, which may be infected with viruses and/or malware.
- Bonus charity scams: Members should confirm the legitimacy of the charity through the Better Business Bureau.
- Monitor accounts: Members should periodically monitor their deposit and credit card accounts to identify any unauthorized transactions. Members should be instructed to immediately report unauthorized transactions to the credit union.
- 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

McAfee's Avoid the 12 Scams of the Holidays

United States Computer Emergency Readiness Team (US-CERT) online security tips

Federal Trade Commission Charity Checklist