

- ✓ **Call:** Telephone the organization identified, using a number that you know to be legitimate.
- 3. Remember:
  - There is no legitimate reason for someone who is giving you money to ask you to wire back money -that's a clear sign that it's a scam. If a stranger wants to send you a check, insist on a cashier check for the *exact amount*, preferably from a local bank or a branch in your area.

- You are responsible for any check you deposit. If the check turns out to be fake, you owe your bank the money you withdrew.
- If you think someone is trying to pull a fake check scam, don't deposit it - report it! Contact the **National Consumer's League's National Fraud Information Center.** [www.fraud.org](http://www.fraud.org) or (800) 876-7060

- If you believe that you have provided sensitive financial information about yourself through a phishing scam, you should:
  - ✓ Immediately contact your financial institution.
  - ✓ Contact the three major credit bureaus and request that a fraud alert be placed on your credit report. The credit bureaus and phone numbers are:
    - Equifax, 1-800-525-6285;
    - Experian, 1-888-397-3742; and
    - TransUnion, 1-800-680-7289
  - ✓ File a complaint with the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov) or 1-877-382-4357.



511 Main Street  
PO Box 450  
New London, MN  
56273  
320-354-2011

PO Box 62  
Sunburg, MN  
56289  
320-366-3885

1690 1st St. South  
PO Box 1740  
Willmar, MN  
56201  
320-235-5900

[www.lakeregion.com](http://www.lakeregion.com)



# Protecting Yourself Against E-mail Fraud and Fake Check Scams



Internet "phishing" scams and fake check scams are rapidly growing fraud crimes today.

Phishing is an internet scam that typically involves a bogus e-mail message. The scammer uses legitimate materials such as a company's web site graphics and logos, in an attempt to bait consumers into disclosing sensitive personal information such as credit card, bank account, and Social Security numbers. The scammers tell the e-mail recipients they need to "update" or "validate" their billing information to keep their accounts active.

Fake check scams usually begin with someone offering to:

- Buy something you advertised for sale;
- Pay you to work at home;
- Give you an "advance" on a sweepstakes you have won, or
- Give you the first installment on the millions you will receive for agreeing to transfer money in a foreign country to your bank account for safekeeping.

Fake check scams may be initiated by telephone or by sending e-mails or faxes to people randomly chosen from newspaper and online advertisements.

## Precautions to Prevent Yourself from Becoming a Victim of Fraud Crimes

1. Never respond to an unsolicited telephone call, fax, letter, e-mail, or Internet advertisement that asks for detailed financial information. Know whom you are dealing with.
2. If you receive a suspicious e-mail:
  - ✓ **Stop:** Resist the urge to immediately respond and to provide the information requested.
  - ✓ **Look:** Read the text of the email several times and ask yourself why the information requested would really be needed.