

8. **Contact other agencies for other types of identity theft:**

- Your local office of the **Postal Inspection Service** if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity;
- The **Social Security Administration** if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud);
- The **Internal Revenue Service** If you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).

Call the fraud units of the three principal credit reporting companies to alert them that you may be the victim of identity theft.

You can also ask them to put a "fraud alert" on your credit file. This is something that the major credit bureaus attach to your credit report. When you, or someone else, try to open up a credit account by getting a new credit card, car loan, cell phone, etc., the lender should contact you by phone to verify that you really want to open a new account. If you aren't reachable by phone, the credit account shouldn't be opened. This should slow down anyone trying to open more credit in your name. You can request a "fraud alert" even if you aren't a victim of identity theft.

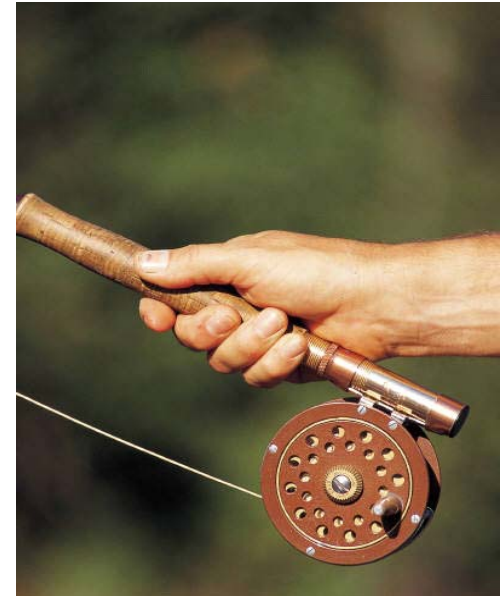
- **Equifax:** (800) 525-6285
- **Experian:** (888) 397-3742
- **Trans Union:** (800) 680-7289

You can learn other ways to avoid email scams and deal with deceptive spam at ftc.gov/spam.

Reference:

www.onguardonline.gov

PHISHING



DET SECURITY

Visit us at:

<http://itsecurity.wi.gov/>

DET SECURITY

Visit us at:

<http://itsecurity.wi.gov/>

What is Phishing?

“We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.”

“During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information.”

“You won a vacation for two! We are sending one lucky winner and a guest to Paris! Spend four nights in the City of Light enjoying classic sites like the Eiffel Tower, the Champs-Elysees and atmospheric cafes.

Have you received email with a similar message? It’s a scam called “phishing”—and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

Phishers send an email or pop-up message that claims to be from a business or organization that you may deal with—for example, an Internet service provider (ISP), bank, online payment service, or even a government agency.

The message may ask you to “update,” “validate,” or “confirm” your account information. Some phishing emails threaten a dire consequence if you don’t respond. The messages direct you to a website that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

Tips to Avoid Phishing Scams

- 1. If you get an email or pop-up message that asks for personal or financial information, do not reply. Don’t click on the link in the message, either.** Legitimate companies do not ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address yourself. In any case, don’t cut and paste the link from the message into your Internet browser—phishers can make links look like they go to one place, but that actually send you to a different site.
- 2. Use anti-virus software and a firewall, and keep them up to date.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can help protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current threats as well as older ones; that can effectively reverse the damage; and that updates automatically. A personal firewall can help stop uninvited users from accessing your computer. A firewall blocks unauthorized access to your computer and, if properly configured, can alert you if spyware already on your computer is sending information out. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software “patches” to close holes in the system that hackers or phishers could exploit.
- 3. Don’t email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information, contact the requestor using a phone number you know to be genuine.
- 4. Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- 5. Be cautious about opening any attachment or downloading any files from emails** you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer’s security.
- 6. Forward spam that is phishing for information** to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems. You also may report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.
- 7. If you believe you’ve been scammed, file your complaint at ftc.gov,** and then visit the FTC’s Identity Theft website at www.consumer.gov/idtheft. Victims of phishing can become victims of identity theft. While you can’t entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.