

LIGHTHOUSE.NET

2972 West 8th Street, Suite A

Sault Ste. Marie, MI 49783

(906) 632-1820

(888) 883-3393

www.lighthouse.net

www.sault.com

A Subsidiary of Cloverland Electric

Fax (906) 632-3049



February 1st, 2009

Beware of Phishing (Fishing) Schemes!

Dear Subscribers:

"Phishers" are criminals who trick people into providing personal information (like passwords, bank account numbers, credit card numbers, etc.) on fake Web sites. You may get an e-mail, instant message, pop-up message or even a phone call by someone pretending to be from a bank, business or credit card company. The phisher will try to tell you it's urgent that you update your personal information. They may even tell you that your identity has been stolen. This is a trick! Don't fall for it! Reputable companies would never ask for personal information that they already have.

It Can Be Hard to Spot a Fake Web Site!

If you're lucky, you can spot a phishing site by looking at the Web address. If the company's name is spelled incorrectly, like "www.paypa1.com" instead of "www.paypal.com," it's a fake. But since phishers are using increasingly sophisticated tactics, this is your best defense:

1. Don't share your personal information, such as passwords, for "verification" purposes, be it online or by phone.
2. Keep your anti-virus software up-to-date and install a firewall.
3. Don't click on pop-ups or links within emails. That's inviting trouble.
4. Use secure passwords with numbers or characters; make them as long as possible.

Never use a name or place as a password or short passwords like "sammy" that can be easily guessed or hacked. Secure passwords like "s7B090ktwq" are difficult for hackers to decipher. If the site security allows characters (for example; !, @, #, \$, %, ^, &, *) adding them in your password will increase its security. You can learn more and test the "strength" of your password at Microsoft (<http://www.microsoft.com/protect/yourself/password/create.mspx>) to see how it rates for security.

If you receive an email with a link about your bank, credit card or other account, don't use any of the links within the email. Go directly to the company page as you would normally and log in to view your account. You can also call the company on their normal telephone number from your card, phonebook or your statement, never use the number supplied with the email!

If you receive an offer or notice that is too good to be true, it is! Don't fall for emails or calls that offer you money or tell you that you have won something you never entered! These scams exploit the idea that you can get something for nothing. Never accept a check or other money without consulting with our local financial institutions. Many people have lost money by taking fake checks and currency in exchange for real money or goods. There are a lot of unscrupulous people out there.

If You Become a Victim of Identity Theft:

If you suspect that you may have already been duped, place a "fraud alert" with the three credit reporting agencies—[TransUnion](#), [Experian](#) and [Equifax](#) and monitor the accounts that you think may have been affected. If they have been compromised, close them right away!

The next step is to file a police report and report the identity theft to the [Federal Trade Commission](#). The Federal Trade Commission has a great Web site, [OnGuard Online \(www.onguardonline.gov\)](http://www.onguardonline.gov), that offers even more information about phishing and other Internet scams.

Please protect yourself and always use secure passwords.

Sincerely,

Steve Mason
General Manager

**Full Service Internet Access with Highspeed & Broadband
Computer Sales, Service & Support**

Leading the way to the Internet

Lighthouse.net is not regulated by the Michigan Public Service Commission