



Phishing Scams ... How to Avoid Them

It's a beautiful Sunday afternoon; the sun is glistening off the stream that I'm standing in awaiting the excitement of the big catch. As I get ready to cast off again, I find myself day dreaming about being back to work tomorrow morning, as I start to hear the phone ring, it happens, my line starts to pull very hard, it's the big trout I have been waiting for all day. Twenty minutes of fight and finally the 22-inch beauty is in my net.

That's going to look good in the fry pan!

Now that's a real whopper of a fish story! I do not even own a fishing pole! And trust me, if I was out fishing in such a beautiful place and work crossed my mind that would be a nightmare! Unfortunately this article isn't about that kind of fishing; in fact there isn't even a pole involved.

Phishing – pronounced “fishing” – is the latest form of identity theft. It's when thieves act as if they are representing an organization and try to “hook” the consumer into providing personal information. Once the consumer is “hooked,” the thieves can do lasting damage to a consumer's financial accounts. They can dupe consumers into providing their Social Security numbers, financial account numbers, PIN's, mother's maiden names and other personal information.



Here's how it works: Consumers receive an e-mail from an organization with which they do business. The e-mail typically includes bogus appeals such as problems with an account or billing errors, and asks the consumer to confirm his/her personal information. Different approaches include things such as “We're updating our records,” “We've identified fraudulent activity on your account,” or “Valuable account and personal information was lost due to a computer glitch.” To encourage people to act immediately, the e-mail usually threatens that the account could be closed or canceled.

Helpful hints to protect yourself:

- 1) Never provide your personal information in response to an unsolicited request.
- 2) If you believe the contact may be legitimate, contact the financial institution yourself.
- 3) Never provide your password over the phone or in response to an unsolicited Internet request
- 4) Review account statements regularly to ensure all charges are correct.

A research firm Gartner, Inc., reported that an estimated cost to consumers last year was 1.2 billion and that 5% of consumers were convinced to respond. 57 million Americans have received a “phishing” e-mail and the FBI has called phishing the “hottest, most troubling new scam on the Internet.”

In each of the next few months, enclosed with your monthly financial statement, we will be sharing “Phishing” brochures to further your knowledge on how and what to do to stop these “Internet Pirates” who are trying to steal your personal financial information.

**OUR GUARANTEED
LOYALTY YOUR LAW
ENFORCEMENT CREDIT
UNION
WILL ALWAYS PROVIDE
THE LOWEST LOAN
RATES!**

VEHICLE RATES

Includes street Legal motorcycles	
TERM	NEW (2005-04)
Up to 72 months	5.99%
	USED
Up to 72 months	6.99%

New & used boat, motor home & rv loan rates
Up to 180 months 6.99% apr

Computer loans:

36 months 9.75% apr \$5,000.00 max

SLECU VISA:

11.50% apr with checking/12.5% without

Signature loans:

48 months	15% apr	\$4,000.00
60 months	15% apr	\$5,000.00

Overdraft protection:

\$50.00 month-15.0%apr \$1,000.00 max

Share secured:

3.0% above current share rate

Term share certificate secured:

3.0% above CD rate

Home equity line of credit:

8.00% variable apr - 90% LTV up to 15year

First mortgage:

7.75%apr fixed-20yr / 2nd mortgage:
8.75%apr fixed-15year

Home improvement loan:

9.25% apr fixed - \$5,000.- \$20,000.00
- 15year

Member service is our specialty!

***APR=Annual Percentage Rate
On Approved Credit



S
L
E
C
U
L
O
a
n
R
a
t
e
s