You worked hard for your money - don't let a stranger steal it from you.

PHISHING SCAMS

New variations of the old "phishing" scams have surfaced in North Dakota, and Attorney General Wayne Stenehjem warns North Dakotans to be cautious. Aware that most of us are suspicious of unsolicited emails, scam artists are trying their luck with the telephone. "The best way to avoid becoming a victim is to hang up on scam artists," said Stenehjem.

COMPUTER ERROR WARNING SCAM

The goal of this scam is to gain access to information on the victim's computer. The scam artist pretends that a computer in the home has been sending error messages to the company and in order to fix the error, it is necessary for the "service technician" to gain access to the consumer's computer. The scammers often mention "Microsoft" or "teamviewer.com," although they have used other deceptive names.

After "confirming" the consumer's name, address and other personal information, the scam artist provides step-by-step instructions to gain access to the computer and then reports that the error has been fixed. In fact, the consumer has just unlocked the computer and given the scam artist access to the financial information, including online banking and credit card accounts and passwords, stored on the computer.

- **If you receive a call claiming that your computer has been sending error messages, just HANG UP. Don't try to "play along" with the scam artists.**

SERVICE DISRUPTION SCAM

In another variation of the scam, a phony customer service technician calls and claims that work on cellular telephone towers in the area may disrupt cell phone service for the consumer so the service provider is offering a month's credit on the bill to make up for any inconvenience.

All the consumer has to do is "confirm" the billing address and the account holder's personal information, and the scam artist will give the consumer a supposed confirmation number to be used to claim the credit.

- **If you are asked to "confirm" billing or account information, that's a sure sign the call is a SCAM. Legitimate callers will not need you to confirm that information, because the business already has it from when you opened the account or started receiving the services.**

CREDIT MONITORING SCAM

Scam artists are taking advantage of the recent highly publicized security breaches at some of the nation's largest retailers by sending emails claiming to be from these companies, offering free credit monitoring for the affected customer. The scam email includes a link to a supposed credit monitoring service and requires the victim to enter their social security number.

In fact, the credit monitoring service in the email is a fake, and any personal and financial information entered on the phony website goes straight to the scam artists.

- **Companies send data breach notifications via regular mail to the mailing address they have on file for you, NOT by email or telephone. If you receive a telephone message about a data breach, IGNORE it - even if it includes an offer of free credit monitoring or credit protection services for "victims."**

Prepared by the Consumer Protection Division of the North Dakota Office of Attorney General
1050 E. Interstate Avenue, Suite 200, Bismarck ND 58503
(701) 328-3404; Toll-free (800) 472-2600; TTY: (866) 290-4236
www.ag.nd.gov