What is Phishing?

Phishing is one of the biggest rackets hitting consumers over the Internet. Consumer Reports Magazine reports that the average victim loses $850 and total marketplace damage exceeds $630 million annually.

So what exactly is **phishing**? It is an e-mail that appears to be from a familiar financial institution, web site (ex: PayPal), vendor (ex: Visa or MasterCard) or Internet retailer (ex: Best Buy). The message claims a problem exists or their "security department" is updating your account. Sometimes it says that there as been suspicious or unauthorized activity and they are freezing your account until you reconfirm the information.

It is called **"phishing"** because the senders - frequently in Canada, Russia or China - send the messages by the million all over North America. They have no idea who will respond or if they are reaching actual customers. They are **"phishing"** for responses.

Don't be fooled into giving your personal account information to con artists in a foreign country. The e-mail links look exactly like the real e-mail addresses of the institutions (known as "spoofing") but they are clever counterfeits too.

Fifth Third Bank was a victim of a recent **phishing** scam and the e-mail looked like this:

Dear Fifth Third Bank Client:

The Fifth Third Bank Technical Department is performing a scheduled software upgrade to improve the quality of banking services. By clicking on the link below you will begin the procedure of the user details confirmation. (Bogus link appeared here)

These instructions are to be sent to and followed by all Fifth Third Bank clients. We apologize for any inconvenience and thank you for your cooperation.

Fifth Third Bank Technical Service

Pretty convincing! Remember, your financial institution already has your account and personal information and would *never* send you an e-mail requesting an update to those items. Please call us if you receive any requests through e-mail that involve your account information with our credit union. Never click on a link within an e-mail if you are unsure of the source. Trust your gut. If it looks suspicious or you have doubts then follow-up by phone and investigate the source.

In most cases, our credit union will contact you by phone or mail if we need to discuss anything regarding your account or personal information. To safeguard your privacy, we will not contact you by e-mail in regards to this type of information.

Go to www.consumer.gov/idtheft for more information on phishing and how to protect yourself.