# Understanding How to Protect your Accounts at Marquette Savings Bank

Criminals use a variety of methods to gain access to your accounts. Protecting your accounts from criminal activity starts with understanding their methods. Take the time to read about the typical tactics used to steal from you.

**Phishing**

Phishing is a way of a tricking an end-user into revealing sensitive information such as usernames, passwords, or account and card details by masquerading as a trustworthy entity in the electronic world.

Phishing can occur through any channel so you must be alert to the validity of any information request you receive. Often it can happen through fraudulent websites that may look legitimate. Marquette asks you to pick a picture and a matching phrase as part of our sign-on protocol, so that you are sure when you see that picture and phrase that you are on our website. If you don't see your chosen picture and phrase, close your browser immediately and notify the bank. The following tips may make you better aware of this problem so you are not the next catch.

**Email.** If you receive an unencrypted email (especially if you have not been in contact with the company/person) you should not answer any question that may reveal personal information such as PIN numbers, passwords, user names, social security numbers, and account or card details. If you receive an email asking for any information like this, you should delete it and contact the sender directly to ensure the validity of the request.

**Telephone.** If you receive a phone call asking for any personal information and you are unsure of the validity of the request or the company/person is unknown to you, end the call immediately. If you are still unsure, a simple return call to the company/person may confirm the validity of the call.

**In person.** If someone comes to your door that you do not recognize, refuse entry and refrain from answering questions. Never leave personal information in open site of visitors.

**Social Engineering**

Social engineering, similar to phishing, is the act of manipulating people into actions or divulging confidential information, usually for the purpose of information gathering, fraud or computer system access.

To prevent becoming a victim of social engineering, refrain from answering questions asked by unknown entities.

**Viruses and Spyware**

**Viruses.** A computer virus is a program that can copy itself and infect multiple computers. It can damage programs, delete files, reformat your hard drive and other destructive outcomes. It can be transferred from websites, email, links in email, internet sites and other removable storage such as USB drives.

**Spyware** is a type of malware that is usually put on the computer without the user's knowledge. It can be very difficult to detect, can slow your computer down and most dangerously, record things such as your personal information, website habits, software used and other keystrokes.
The best way to protect your computer from viruses and spyware is to install a recommended anti-virus program. There are many excellent programs available which can be easily researched using online search engines. Once anti-virus/anti-malware software is installed, it is important to keep the software updated with automatic, daily updates.

Use caution when clicking on links from unknown sources or attachments and links in emails. Often infection of a computer happens with a simple click.

**Secure Connections**

A secure connection is vital when logging on to sites that exchange sensitive, personal data such as online banking or other sites where account or card information may be used. Secured Sockets Layer is commonly trusted technology which allows safe transfer of information. You will know you are in a SSL environment if your URL indicates a https: address, instead of the normal http:. Also, many browsers display a closed padlock somewhere on the screen when you enter a SSL environment. If you do not see the https: and/or the padlock, do not enter personal information on the website.

**Email**. Unless email messages are sent from "Secure Messaging" in our online banking service after you have logged in, emails sent to Marquette carry some risk of intrusion. Do not send personal, confidential information such as account numbers or social security numbers in the text of your email.

- Understanding how to Protect your Marquette Accounts is continued on the next page -

# Understanding How to Protect your Accounts at Marquette Savings Bank

**Creating a Strong Password**

A strong password is vital in protecting your account. Hackers use computer programs that can crack passwords within seconds if it is too simple. Creating strong passwords makes it more difficult to crack.

The two main rules to remember when creating a strong password are length and complexity. Your password should be at least 8 – 10 characters in length; the more characters, the stronger the password. Your password should contain at least one capital letter, one lower-case letter, one number and one special character (symbol).

Do not use easily discovered items for passwords such as names, phone numbers, addresses, sports teams, or user-names. Never write down your passwords and change your passwords frequently. Never share your password with anyone. Do not use the same password for more than one site.

An easy tip to creating strong passwords is to use your password as an acronym or a paraphrased statement. For example: "I love Marquette Savings Bank, the Hometown Bank" could be made into the following complex password, "!1uvM$Bth3Hb".