First Midwest Bank

Secure Internet Behavior
Information Security for Commercial Banking Clients

Using the Internet safely - What precautions can you take?
Having information at your fingertips is a valuable tool. Understanding the risks of using that tool and how to use it safely are just as valuable to know. With information stored on local servers, the advent of “clouds”, sharing information through social networks, ultimate mobility provided by wifi hotspots, and countless other accessibility options, using the internet safely is something that should be taken seriously.

- Many establishments offer wireless hotspots for customers to access the Internet. Since the network is untrusted and security is often weak, these hotspots are susceptible to attacks. When used, limit your activities to web browsing. Avoid accessing online banking or other services that require you to login or enter personal information.
- Do not forward email or documents from home computers to work computers via email or removable media. Generally, work computers are configured more securely. Have work content sent to your work email address. Use work provided remote access to get to work email and documents from home. If work does not provide remote access or a laptop, a password-protected, encrypted USB storage drive can be used to carry and work on documents at home.
- Information which has traditionally been stored on a local computer is steadily moving to the Internet cloud. Information in the cloud is difficult to remove and governed by the privacy policies and security of the hosting sites. Businesses or individuals who post information to these web-based services should ask themselves “Who will have access to the information I am posting?” and “What controls do I have over how this information is stored and displayed?” before proceeding.
- Social network sites are very convenient and efficient means for sharing personal information with family and friends. This convenience also brings some level of risk; therefore, social network users should be aware and understand what personal data is shared and who has access to this data. Think twice about posting information such as address, phone number, place of employment, date of birth, and family relationships. If available, limit access to posted personal data to “friends only.” Be wary of receiving content from people you do not directly know or in conjunction with third party games.
- Email accounts are common attack targets. To reduce risk, consider using different usernames for home and work email addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts. Do not set out-of-office message on personal email accounts or send replies to Internet email addresses for business email accounts. Only send out-of-office messages to other employees.
- Unsolicited emails containing attachments of web links should be considered suspicious. If the identity of the sender can’t be verified or the message does not make sense, delete the message. Be very wary of an email requesting personal information or offering a get-rich quick scheme. It is very easy to send messages with a fake From: address. Do not assume a message is legitimate solely based on the From: address.

More precautions continued on the next page >>

Want to learn more about information security for your business banking transactions? Visit firstmidwest.com/safe for the most current resources on a wide array of information security topics.

First Midwest Bank

Secure Internet Behavior
Information Security for Commercial Banking Clients

Using the Internet safely - What precautions can you take? (continued)

- Ensure that passwords (and PINs or pass-phrases) are properly protected since they provide access to large amounts of personal and financial information, and even access to conduct financial transactions. Passwords should be strong, unique for each account, and difficult to guess. A strong password should be at least 10 characters long and contain multiple characters types (lowercase, uppercase, numbers, and special characters). Disable the feature that allows programs to remember passwords and automatically enter them when required. Additionally, many online sites make use of self-service password recovery or challenge questions. The answers to these questions should be something that no one else would know or find from Internet searches. Consider creating your own question, if possible, or providing a false answer to a fact-based question, assuming the response is unique and memorable.
- Never share your passwords with anyone. You are responsible for the actions of your account. Each user must have their own account. Do not use automatic login features that save passwords.
- Do not use public or other unsecured computers for online banking.
- Always logoff your online banking application when you are done, especially if you are using someone else's computer.

Important Note

- First Midwest Bank will never request sensitive information through unsolicited email. If you receive unsolicited email requesting your account number(s), Social Security Number, PINs or passwords, do not divulge any information or click on any links contained within.

Want to learn more about information security for your business banking transactions? Visit firstmidwest.com/safe for the most current resources on a wide array of information security topics.