



## **Personal Online Banking Best Practices**

Cyber criminals, like most criminals, are opportunistic. They seek out vulnerabilities on computers to send spam and phishing emails or try to trick people into providing information that allow criminals to pillage bank accounts or steal identities. Home computers are favorite targets of criminals. You need to be vigilant in protecting your personal and financial information by employing trusted security technology and by employing the same intuition you use in the “off-line” world. We are providing these best practices to assist you in mitigating your risk of loss while online.

### **Fake Emails/Phishing**

- Do not reveal personal or financial information in an email. Do not respond to email solicitation for this information. This includes links sent in an email.
- Do not send sensitive information over the Internet before checking a website’s security.
- Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain. (e.g. .com vs .net)
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use the contact information provided on a website connected to the request or included in the email. Instead, check your own previous statements for the contact information.
- Install and maintain anti-virus software, firewalls, and junk email filters.
- Do not open attachments from strangers or those with strange filename extensions. If a file has a double extension, like “heythere.doc.pif”, it is highly likely that this is a dangerous file and should not be opened. In addition, do not open email attachments that have file endings of .exe, .pif, or .vbs. These could be executable files that can cause damage to your computer if opened.
- Many fraudulent emails contain urgent messages claiming your account will be closed if sensitive information is not provided immediately or that important security information needs to be updated online.

### **Choose Safe Passwords**

- Passwords should have at least eight characters and include uppercase and lowercase letters, numerals and symbols.
- Never use passwords that repeat numbers or letters.
- Avoid common words. Some hackers use a program that tries every word in the dictionary.
- Do not use personal information such as name, children’s name, birthdates, etc. that someone might already know or easily obtain.
- Change passwords regularly (at least every 90-180 days). If you believe that your system has been compromised, change passwords immediately.
- Use different passwords for each online account you access (or at least a variety of passwords.)
- Do not share sign-ons and passwords with others.
- Do not write down your sign-ons and passwords. If you have to store them, store them in a location where they would not be easily found.

- Remember to log off when you are done using websites that require a user ID and password.
- Disconnect and shut down when you are not using your computer.

**Download Trusteer Rapport** We recommend that you download **Trusteer Rapport**. Trusteer Rapport helps prevent criminals from withdrawing money from bank accounts. The service has been specifically designed to combat online banking threats and represents an essential part of your bank's security systems. The service consists of lightweight security software that locks down the browser and stops Man-in-the-Browser (malware), Man-in-the-Middle, and Phishing attacks against your bank accounts and other protected websites. Trusteer is also capable of removing financial malware it discovers on protected machines.

### **WiFi Hotspots**

The most convenient wireless services—free hotspots offered by coffee shops, schools, libraries, etc.—carry the greatest risks. Many hotspots are completely open, or protected by a common password that you get for the price of a cup of coffee. Clever scammers using the network can intercept messages as you send and receive information. If you're connecting to email or e-commerce sites, you may be transmitting passwords that can be intercepted by near by crooks.

If you are going to use a public WiFi hotspot, make sure your security tools (anti-virus, anti-spyware, and firewall) are all up-to-date and active. Some firewalls can be used to secure your wireless connections, but **the best way to avoid interception is to avoid conducting sensitive transactions over public wireless networks.**

### **General Financial Management Best Practices**

- Review your deposit account transactions as frequently as possible - daily is ideal. You can do this via telephone banking and other online banking solutions.
- Set up online banking alerts that send you an email or a text message when certain transactions occur, when a transaction exceeds a specified maximum, or when your balance level goes below a specific balance.
- Never write your PIN on your Debit or ATM card.

### **Merchants Bank Data & Network Security Protections**

Merchants Bank has a long standing commitment to protect customers vital data and in that regard has built a comprehensive system of policies and procedures, including both physical and software controls, to mitigate risk. The Bank has also designed our systems to provide multiple layers of security and protections to provide an even more secure environment. See the Security Section of our website for more details at [www.mbyt.com](http://www.mbyt.com).

**We have provided the above Retail Online Banking Best Practices to assist you in protecting your confidential and financial information. Please be sure to implement these practices to mitigate your risk of loss. Merchants Bank is not responsible for losses related to security weaknesses within your personal online banking access devices such as your home computer, cell phone, mobile device, etc.**