



## Safeguarding Your Information

### Tips on a Secure Online or Mobile Banking Experience

At **Heritage Bank of Schaumburg**, the security of customer information is a priority. We are strongly committed to the safety and confidentiality of your records. Every day, dishonest individuals are busy developing new scams targeting the unsuspecting public. One of the best ways to avoid fraud is to become an educated consumer.

- Watch out for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as the real one. The intent is to lure you into clicking through to their Web site and giving out your personal information, such as a bank account number, credit card number or Online Banking login information.
- Always use your pre-established links to access Web sites and avoid clicking on links in unsolicited e-mails. If you ever receive a suspicious e-mail representing itself as **Heritage Bank of Schaumburg**, please contact a personal banker. Also, remember that e-mail is generally not encrypted so be wary of sending any sensitive information such as account numbers or other personal information in this way.
- Ensure that your own personal computer has updated anti-virus and firewall protections. Apply security patches for all of your programs and operating systems regularly.
- Passwords should be unique to you and changed regularly. Do not use birthdays or other numbers or words that may be easy for others to guess. Never write down your password or give it to another person, and do not save passwords on a publicly accessed computer.
- Monitor your account activity frequently using our free Online Banking services. Set up Balance Alerts to be notified via phone and/or e-mail when there are changes in your expected balance.
- Never leave your computer unattended once you have signed in to Online Banking. Always sign off and log out when you are finished with your session and close your browser.
- Enroll in electronic statements. Electronic statements help safeguard your information by eliminating a paper trail and prevent criminals from stealing your account information through the mail. You'll also be able to review your statement as soon as it's available, and not have to wait until it is delivered.

### Additional Tips for Secure Mobile Banking

- Use your mobile device's power/ON password/PIN feature to secure the device and prevent unauthorized access. Set it to auto-lock after a certain period of time.
- Do not permit your login ID or password to be "remembered" by the mobile browser, and don't store your passwords on your mobile device.
- Immediately disable mobile banking services on your device if it is lost or stolen. You can access the Mobile Banking Center by logging in to your personal online banking account and clicking on Customer Service. Or, you may call us at 847-524-4000 to disable the service.
- Do not use public WiFi connections to access mobile banking as they are not secure. Disable WiFi on your device and use a cellular or home network only.
- Download and install apps only from reputable sources. Also consider installing a security app from a reliable security provider.



HERITAGE BANK  
SCHAUMBURG

Please keep in mind that we will never ask for or email you requesting your online banking password. We may on occasion call to verify other information regarding your online activity should we see something of concern in your login patterns. If you plan to travel and use your Online Banking or debit card, it is very helpful to call us in advance to avoid your account being temporarily disabled for security purposes.

In case of errors or questions about your electronic transfers, call or write us at the telephone number or address listed, as soon as you can, if you think your statement or receipt is wrong or if you need more information about a transfer listed on the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error appeared.

For personal accounts, limitations on your liability for unauthorized electronic funds transfers and other electronic errors that are covered by Regulation E are explained in the EFT Disclosure Statement in our Consumer Terms and Conditions brochure.

If at any time you have questions regarding security or possible fraud, please contact our customer service representatives at the local branch.