

Passwords

- Don't share your password with anyone. No one from Tompkins Mahopac Bank will ever ask you for it.
- If it's easy to remember, it might be easy to guess.
- Choose complex passwords with special characters and capital letters.
- Avoid incrementing the number at the end of a password. For example don't change P@s\$word1 to P@s\$word2.
- If you don't remember when the last time you changed your password, it's time.
- Never write your passwords down where they can be easily found.
- Don't use the same password across multiple secure websites.

Computer Security

- You lock your house; lock your PC (To do so, hold the Windows key and press L).
- Your antivirus is only helpful if it's up to date. Make sure antivirus definitions are being updated.
- Think before you click. Most viruses are installed through malicious links on websites or within email.
- Update applications like Java, Adobe Acrobat, and Adobe Flash frequently. Never skip updates for these commonly exploited applications.
- Never send personal information via email.
- Know what your financial websites look like, and be aware of any changes that could indicate a virus or redirect to a malicious site masquerading as the legitimate website. Examples include: misspelled web addresses like <http://www.mahapacbank.com>, spelling errors on the web page, and invalid email addresses.
- Check your bank & credit card statements and all financial records regularly. Look carefully for any irregularities.
- Treat your email with the same caution that you would an online banking site. Email can be used to reset passwords and gain unauthorized access to other websites.
- Hold your mouse over links in email before clicking to see where it actually leads.
- Be aware of what your children use your computer for.

If your information or accounts are compromised

- Immediately report any unauthorized charges to your bank or the card issuing organization.
- Run a complete anti-virus/anti-malware scan. Malwarebytes is a convenient and free anti-malware application www.malwarebytes.org.
- Change passwords for email and all financial organizations.
- Contact credit reporting companies to place a fraud alert on your credit report.
 - o Equifax: 1-800-525-6285 <http://www.equifax.com>
 - o Experian: 1-888-397-3742 <http://www.experian.com>
 - o Trans Union: 1-800-680-7289 <http://www.transunion.com>

How do I protect my smartphone?

- Don't follow links you receive in unsolicited email or text messages.
- Use official mobile phone applications. Go to <https://www.mahopacbank.com/mobile/> to download apps for your IOS, Android, or Blackberry device.
- Never "jailbreak" or "root" your phone. Doing so can give applications unintended access to the operating system and compromise the integrity of your transactions.
- Password protect your mobile device. Smartphones often have as much sensitive information as a computer and are much easier to misplace.
- Never respond to urgent emails or text messages claiming to be from a bank or other financial institution. Forward these messages to abuse@tompkinsfinancial.com.
- Install software to find and remotely wipe your smartphone. Not only can you prevent a stolen phone from turning into a stolen identity, but as an added bonus, it can help recover a misplaced device.

