TOMPKINS
Mahopac Bank

How can I prevent becoming a victim of fraud?
- Be suspicious of any email, website, or person asking for financial information or passwords.
- Don't click on suspect links or open email attachments.
- Regularly change passwords.
- Review financial statements.
- Install updates offered by your operating system and software provider(s).
- Update antivirus regularly.

How can I safeguard my banking information?
- Do not write down login and password information.
- Never provide your login information to anyone. Mahopac Bank will never ask you for your password.
- Change your password at least once each quarter.
- Check your financial statements regularly, and report all suspicious activity.

How did my username and password get compromised?
Unfortunately, there are a number of ways accounts can be compromised. Logging into your online banking account while infected with a virus or entering your account information onto a malicious website masquerading as the legitimate login page are common sources of account compromise. A compromise of your personal email account can also be the source of a breach. Email accounts tied to financial websites should be treated with the same level of security as your online banking credentials.

Should I change my passwords often?
We recommend you change your password periodically but do not require password changes. It is a good practice to change your password quarterly, but please remember to not write it down where it can be easily found.

What do I do if my email or computer is compromised?
- Immediately notify Tompkins Mahopac Bank of any illegitimate transactions.
- Update virus definitions and run a full system scan.
- Run a malware removal tool. Many tools like Malwarebytes (www.malwarebytes.org) can be downloaded for free and can assist in virus removal.
- Change passwords on email and online banking accounts as well as any website that stores confidential information like credit card numbers.
- Compromised email accounts are commonly used to attack your acquaintances. Notify email contacts that your account was breached to prevent the attack from spreading further.

What can I do to protect my personal accounts?

Be aware and stay alert to potential attacks. If your information is compromised despite your best efforts, the faster you respond the easier it is to minimize or completely eliminate possible consequences.

- Check antivirus software for updates, install operating system patches, install updates for 3rd party applications like Java and Adobe Acrobat.
- Do not click suspicious links within email or open email attachments.
- If you find an email suspicious, use a different form of communication (a telephone call) to verify with the sender that the email is legitimate.
- Regularly change passwords, at least quarterly.
- Don't respond to "phishing" emails. Malicious emails should be deleted. Responding only confirms the email account is valid and active.
- Review financial statements and report any suspicious activity.

If your accounts are compromised ensure you act quickly to remove unauthorized access.

- Alert financial institutions of any fraudulent activity.
- Monitor any effected accounts diligently.
- Change email and online banking passwords.
- Contact credit reporting companies to place a fraud alert on your credit report
    - Equifax: 1-800-525-6285 http://www.equifax.com
    - Experian: 1-888-397-3742 http://www.experian.com
    - Trans Union: 1-800-680-7289 http://www.transunion.com
- Check your credit report. You are entitled to one free report every twelve months from each of the three credit reporting companies.
    - http://www.consumer.ftc.gov/articles/0155-free-credit-reports

What are the risks of using public WiFi?

While public WiFi can be convenient, it does carry some risk. Unencrypted data can be "sniffed" and viewed by malicious parties, potentially leading to account compromise.

- Only join public WiFi of a trusted source. When in doubt ask an employee if you're connecting to the correct network.
- Only enter usernames and passwords on secure sites. The website address should start with HTTP**S**://, the S stands for Secure.
- If prompted when you connect to the network, choose public network and not work or home.
- Avoid using public WiFi when possible for sensitive transactions.

How do I identify dangerous emails and what should I do if I receive one?

- Check the email sender and ensure there are no misspellings in the address.
- Hold your mouse over any URL before clicking. This will show where the link is actually taking you. Be aware of any misspellings or domain names that end with uncommon country codes like .ru or .ng Very few legitimate websites will use these domains.
- Be suspicious of any email asking for you to provide or confirm account information.
- Delete suspicious emails. Responding or clicking on any links can only have negative consequences.
- Report email masquerading as a legitimate organization to that company. Fraud related to Tompkins Mahopac Bank can be reported by email at MBinfo@tompkinsfinancial.com.

How do I determine if a website is safe to conduct business on?

- Check for certificate errors. There should be a picture of a closed lock near the website URL.

Ex: 

Or: 

- Be alert for any changes in the website design. Malicious copies often look unfinished or unpolished.
- Before you enter any information, make sure the website address is what you expect and you have not been redirected to another website.

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.

How we protect you:

- ***Trusteer***

  We have partnered with Trusteer, an IBM Company, and leading expert in financial security, to offer Trusteer Rapport online fraud protection software, customized to protect users of Tompkins Mahopac Bank Internet Banking – at no cost to you.

  - **For more information go to https://www.mahopacbank.com/personal/trusteer/**

- ***Cyveillance Protection***

  The Cyveillance Protected Seal is a trust mark displayed on the Web sites of organizations that utilize Cyveillance Anti-Phishing™ to provide early detection and immediate take down of malicious phishing sites. The seal indicates to consumers and site visitors that the organization is serious about proactively protecting its customers from online fraud and identity theft.

  - **For more information go to https://www.mahopacbank.com/privacy/cyveillance/**

- For more information about how to protect yourself go to **https://www.mahopacbank.com/home/privacyandsecurity/**

If you have any further questions, please contact your local branch.