ONLINE BANKING SECURITY TIPS

Magnolia Bank is committed to maintaining the privacy and security of all account information, whether accessed online, in person or via any other method. Below is important information and useful tips for accessing your account(s) online:

Encryption

When signing in to your online banking account, you connect via encrypted Secure Sockets Layer (SSL) technology. We also provide you with the option of utilizing security alerts that you can customize based on your personal notification preferences.

Password Security

Magnolia Bank expires passwords periodically to help increase your overall security profile. We recommend using different passwords for any e-banking sites, which should not be the same passwords used for any social media sites such as Facebook or Twitter. It may seem inconvenient to maintain multiple passwords, however, it wouldn't take long for a hacker to access all of your account information once your password was stolen or compromised if you use the same one across various sites. We also strongly recommend PIN, password or fingerprint protecting any mobile device that you use. In the event it is lost or stolen, the password will provide an extra layer of security.

We also recommend using "strong" passwords. Strong passwords consist of a combination of letters, numbers and special characters. A short phrase is ideal (i.e. Wayt0g0!). Whatever you chose, make your password unique and never write it down in a location that could be easily found. If you have multiple sites requiring passwords, you can utilize a password protected spreadsheet listing the user IDs and passwords. Just make sure this spreadsheet is password protected with your most complex password of all! And, do not share your password with anyone.

Network Security

It is never a good idea to log into a banking site via a wireless hot spot or any unsecured network. Only access financial data from a network that you know is secure.

We recommend always logging off when you are finished with your online banking session, whether you are at home, work or on your mobile device.

Social Engineering

Social engineering is the skill of manipulating people to give up confidential information. Common attacks include: e-mail hi-jacking, baiting scenarios (great deals on classified or auction sites), foreign offers such as sweepstakes or lottery. Do not respond to any requests for financial information or passwords, use search engines instead of relying on links contained in messages, be cautious of unsolicited messages, set spam filters to high and secure computing devices. If you receive an e-mail from what looks like Magnolia Bank requesting personal information, do not respond and contact us.

Magnolia	Parkway Plaza	Lincoln Hills	Elizabethtown
270.324.3226	270.358.3183	270.358.3111	270.765.4072

You can also reach us by email at: customerservice@magnoliabank.com

Correspondence with Magnolia Bank

Magnolia Bank will contact you from time to time. However, we will never email or text you requesting login information or ask for personal account information via email or text. Never respond to an email or text message that asks for this type of information. Emails from fraudulent sources are referred to as "phishing" and fraudulent text messages are referred to as "Smishing". If you have been taken advantage of online, report it immediately to the Federal Trade Commission (FTC).

Hackers are at work every day trying to steal personal or account information. Be diligent with what you share and remember that Magnolia Bank will never ask for your PIN or password.

Additional Security Features

Magnolia Bank is always working to increase security within your online banking experience. Another security feature enabled is the Security Verification Questions that provide an additional layer of security. Users are required to answer a question that was setup by the user at enrollment each time they login.

Magnolia Bank also masks account numbers within the online banking system. Masked accounts only display a specific portion of the account. Our online banking also places persistent cookies on the user's computer as one way of authentication. How long the cookie remains depends on how long the website has programmed the cookie to last.

Best Practices for Protecting Mobile Devices

Keep apps and mobile devices up to date by using the most current operating system. Disable Wi-Fi auto connect. Allow downloads from only trustworthy sources and require notification before an app is downloaded. We recommend using the same security precautions to navigate the internet on a smart device as you do on a personal computer.

Best Practices for Protecting Computers

Keep the most current operating systems and update your browser anytime there are new security updates available. Install antivirus software and keep the software updated. Do NOT install software you are unfamiliar with. Additionally, you can install a firewall on your computer to prevent access.