F&M Bank

Tips for Secure Online Banking

Follow the Correct URL
Always access our internet banking by typing the correct URL (http://www.fmbankva.com) into your browser. Never click on a link in an email to take you your online banking account or enter personal details.

Password Security
You should always be wary if you receive unsolicited emails or calls asking you to disclose any personal details or card numbers. This information should be kept secret at all times. Be cautious about disclosing personal information to individuals you do not know. We will never contact you directly to ask you to disclose your password information.

If It Sounds Too Good to be True...
It probably is. Don't be conned by convincing emails offering you the chance to make some easy money. As with most things, if it looks too good to be true, it probably is. Be cautious of unsolicited emails from overseas - it is much harder to prove legitimacy of the organizations behind the emails.

PC Security
It is important to use up-to-date anti-virus software and a personal firewall. If your computer uses Microsoft Windows, it is important to keep it updated via the Windows Update feature. Equally if you use another operating system you should check regularly for updates. Ensure you also regularly patch Java and Adobe products. These items are frequently updated because of vulnerabilities and hacker use of those vulnerabilities to install malware on your computer. Consider using a single computer for your online banking and restrict other uses on it.

Avoid Public Wireless Internet Access
You should be vigilant if you use internet cafes or a computer that is not your own and over which you have no control. Hackers and identity thieves often monitor these networks or install malware to capture your login credentials.

Keep your Identity Private
Your identity can be as easily stolen offline as it can online. It is important that you comply with instructions about destroying expired bank cards.

- Do not write down your Username and Password and leave it next to your computer.
- Do not Cache your online banking passwords.
- Do not use the same password for online banking that you use for any other website. If compromised, thieves now have your internet banking password.
- You should also consider using a crosscut shredder to destroy bank and other statements that may contain sensitive personal information.
- It is advisable to store retained documents in a suitable locked and fireproof container.
- Use a complex password that is not easily guessed. It should not contain full names or words. It should include special characters and be at least 8 characters long.

Check Your Statements
It is important to check your statements regularly; a quick check will help identify any erroneous or criminal transactions that might have been performed on your account without your knowledge.

Check Your Banking Session Is Secure
When undertaking any banking on the internet, check that the session is secure. There are two simple indicators that will tell you if your session is secure. The first is the use of https:// in the URL. Some browsers such as Mozilla Firefox change the color of the url window when you are in a secure session. The other indicator is the presence of a digital certificate represented by a padlock or key in the bottom right-hand corner. If you double click on this icon it should provide you with information about the organization with which you have entered in to a secure session.

Check for Spywares/Malware
In addition to being protected by using up-to-date antivirus software, you should also regularly use software to remove spyware from your computer as these programs record information about your internet use and transmit it without your permission. In some circumstances this can compromise your PC security. Remember current anti-virus software does not catch 100% of every virus. Consider utilizing multiple programs to regularly scan your computer.

Ensure You Log Off Properly
It is important to completely log off from your internet banking session; simply closing the window you performed the transaction in may not close the banking session. If your computer is infected with a Trojan, your session may become hijacked by a criminal and financial transactions may be performed without your knowledge. It is also advisable to disconnect from the internet if you are not planning to use it.

What We Do to Make Your Online Banking Session Secure
We use a combination of Secure Socket Layer (SSL) protocol and passwords to protect your information. In addition, stronger authentication is used as appropriate to particular markets. We also monitor online login and financial transactions for suspicious activities.

Sound Advice
If you ever get an email, phone call, or letter that appears to be from F&M Bank asking you to provide or verify your personal identification or bank account information, or asking you for up-front money to claim a windfall, it is a scam or an attempt at identity theft.

When in doubt, don't respond to the email address or phone number contained in the request. Instead, call us at **540-896-8941**. After hours, you can also call the Hot Card Center at **888-297-3416** to report a lost or stolen card.