RECOMMENDATIONS FOR ACCOUNT HOLDERS

- Be vigilant in reviewing your financial statements and monitoring your transactions. Monitor your financial accounts (e.g. bank, credit card, retirement etc.) at least weekly through online, mobile, voice banking or the ATM.
- Never leave your computer, tablet or mobile phone unattended when using any Internet banking, mobile banking or other financial services.
- After you have completed your Internet or mobile banking session, log off to ensure that the session is completed.
- Lock your computer or mobile device whenever you plan to leave it unattended.
- Never use publicly available information to create your password.
- Change your passwords frequently.
- Avoid using password managers.
- When you log into mobile banking, be aware of the people around you. Even if you are speaking on your phone, be careful not to give account numbers or other personal information within earshot of others.
- Never click on links or applications that you receive in e-mail from an unknown source, as those are common ways viruses, malware and malicious software are installed.
- If you get an e-mail with links purporting to be from Home Federal and you are unsure or are not expecting it, please visit our main website through your browser or call us at 318-222-1145 to verify legitimacy.
- If you receive eStatements on your account at Home Federal, you should receive an email notification when the statement is available, including a link to view the statement online. This link will take you to a secure site which will require that you sign in with your pre-determined user ID and Password. Remember, Home Federal Bank will never send an e-mail asking for your personal information.
- Do not send confidential information such as taxpayer identification numbers or account numbers via unsecured (unencrypted) e-mail.

Wireless carrier data usage rates may apply.

MORE RECOMMENDATIONS

- Keep your passwords/pin confidential. Under no circumstance will you be asked to provide it to Home Federal.
- Never store your sign on, password, and answers to your challenge questions on your phone. Frequently delete text messages received from us on your mobile device, even though they don't contain sensitive information.
- While using the Internet, verify use of secure session ("https://" and not "http://") in your browser's address bar. This is your indication that the data being transmitted between your browser and Home Federal systems is securely encrypted.
- Install anti-virus and anti-malware software.
- If you have a mobile device such as a Smart phone or tablet, ensure that you install software capable of remotely wiping the device should it get stolen or lost.
- If your device is lost or stolen, please review your account activity and contact us immediately regarding any suspicious transactions. Additionally, notify your mobile carrier and suspend your service.
- Install mobile software only from the Android Market or the Apple App Store and never a 3rd party site.
- Do not "jailbreak" your iPhone or "root" your Android to avoid unintentionally opening "backdoors" for malicious software.
- Do not modify your device. This could leave it susceptible to infection from a virus.
- Turn off wireless device services such as Wi-Fi, Bluetooth and GPS when they are not being used.
- Avoid using unsecured public wireless connections. If you must, then use VPN software to provide a secure "tunnel" within which to work.
- Use privacy settings on social networking sites to control who is able to access your personal information.
- Sign up for e-mail or text message alerts through HFB Online Banking. Select the Accounts tab and the drop down titled Account Alerts to select your customized alerts.
- Checks and your financial statements all have your private financial information on them. Request electronic statements and use online bill pay whenever possible to reduce the paper trail and the risk of your account information being compromised.
- Update your app, from time to time, with the most recent Home Federal Bank mobile banking app. As we update security features and add new features, you'll want to be sure you have the most current version.

www.hfbla.com/privacy-security • 318-629-BANK (2265)

HFB
HOME FEDERAL BANK
A Better Way

Member FDIC

PERSONAL ACCOUNTS Guidance

BETTER PRACTICES
for Mobile & Online Banking

HFB
HOME FEDERAL BANK
A Better Way

YOUR SECURITY IS OUR TOP PRIORITY.

New supervisory guidance and standards from the Federal Financial Institutions Examination Council (FFIEC) are assisting Home Federal Bank and account holders to make online banking safer and more secure from account hijacking and unauthorized funds transfers.

UNDERSTANDING THE FACTORS

Online security begins with the authentication process, which confirms that it is you logging into your account, and not someone who has stolen your identity. Authentication generally involves one or more basic factors:

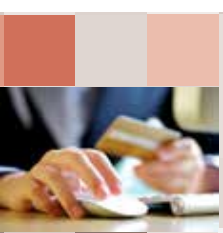
- Something the user knows (password, PIN)
- Something the user has (ATM card, smart card)
- Something the user is (fingerprint)

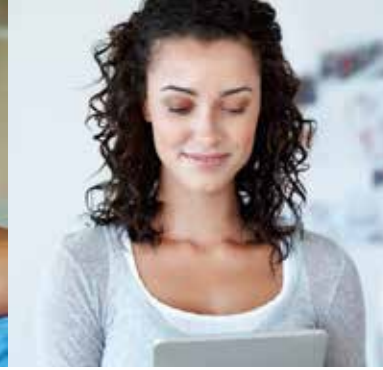
Single factor authentication utilizes one of these methods; multi-factor authentication utilizes more than one, and therefore is considered a stronger fraud deterrent. When you use an ATM, you are utilizing multi-factor authentication: Factor number one is something you have, your ATM card; factor number two is something you know, your PIN.

To ensure your continued security online, Home Federal uses both single and multi-factor authentication, as well as additional "layered security" measures when appropriate.

LAYERED SECURITY FOR INCREASED SAFETY

Layered security is characterized by the use of different controls at different points in a transaction process so that a flaw in one control is generally compensated for by the strength of a different control. An example of layered security might be that you follow one process to log in (user/password), and then give additional information to authorize funds transfers.





Layered security can significantly strengthen the security of online transactions by protecting sensitive customer information and preventing identity theft. It also reduces account takeovers and the resulting financial losses.

The goal of these layers is to allow Home Federal to authenticate customers and detect and respond to suspicious activity related to initial login. Then later, we can reconfirm the authentication when additional transactions involve the transfer of funds to other parties.

INTERNAL ASSESSMENTS

The new supervisory guidance offers ways Home Federal Bank can detect anomalies that could indicate fraud. The goal is to ensure that the level of authentication called for in a particular transaction is appropriate to the transaction's level of risk. Accordingly, Home Federal has concluded a comprehensive risk-assessment of its current methods as recommended in the FFIEC guidelines. These risk assessments consider, for example:

- Changes in the internal and external threat environment
- Changes in the customer base adopting electronic media
- Change in the customer functionality offered through electronic banking
- Actual incidents of security breaches, identity theft, or fraud experienced by Home Federal or the banking industry

Whenever increased risk to your transaction security might warrant it, Home Federal will be able to conduct additional verification procedures, or layers of control, such as:

- Utilizing call-back (voice) verification, e-mail approval, or cell phone-based identification
- Employing customer verification procedures, especially when opening accounts online
- Analyzing banking transactions to identify suspicious patterns
- Establishing dollar limits that require manual intervention to exceed a preset limit.

CONSUMER PROTECTION UNDER "REG E"

Home Federal Bank follows specific rules for electronic transactions issued by the Federal Reserve Board known as Regulation E. Under the consumer protections provided under Reg E, you can recover internet banking losses according to how soon you detect and report them.

If you report the losses within two days of receiving your statement, you can be liable for the first $50. After two days, the amount increases to $500. After 60 days, you could be legally liable for the full amount.

NOTICE SUSPICIOUS ACTIVITY?

If you notice suspicious activity within your account or experience security-related events, you can contact us at 318-222-1145. We react quickly to remedy such reports, and we are available to assist you with any questions you may have.

Whenever increased risk to your transaction security might warrant it, Home Federal Bank has additional verification procedures, or layers of control, such as:

- Fraud detection and monitoring systems that include consideration of customer history and behavior
- Dual customer authorization through different access devices
- Out-of-band verification transactions
- Transaction value thresholds, number of transactions allowed per day, and allowable payment windows (e.g., days and times)
- Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities
- Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud
- Account maintenance controls over activities performed by customers either online or through customer service channels