American First National Bank

Expertise. Efficiency. Excellence.

Helping You Protect Your Online Presence

How We Protect You…

American First National Bank is committed to helping secure your personal information. Here are a few tips that we hope will help you protect yourself.

How we identify you:

Unique Username and Password

When you sign up for online banking, we ask you to create a username and password to access your accounts. This information is encrypted during sign on.

To create a strong username and password consider using a unique phrase with a mix of letters and numbers that you only use for AFNB accounts. Avoid using any part of your email address or information shared on social media, like the name of your pet, favorite movie, or anything else that someone could easily guess. We recommend your username and password only be used for your AFNB account. For a stronger password, pick a phrase with a mix of letters and numbers. The longer your password, the harder it is to crack.

How We Protect You…

How we protect your data:

24/7 Fraud Monitoring

We are helping to keep your money safe by monitoring your account and alerting you to certain account activity we find suspicious. If your banking behavior differs from your usual activity, we may restrict account access or prevent certain types of transactions. Further proof of identity may be required before we restore online access.

Encryption & Browser Requirements

All online and mobile banking sessions are encrypted to help protect your accounts. In addition, American First National Bank only supports browsers that adhere to our encryption standards. We may block outdated browsers that could lead to a security risk, so be sure to keep your browsers up to date.

Automatic Sign Off

AFNB will automatically sign you off from your online or mobile banking session after a period of inactivity. This reduces the risk of others accessing your information from your unattended computer or mobile device. For your security, always sign off after completing your banking activities.

Mobile Banking

American First National Bank has made it safe and secure to manage your bank account from almost anywhere, anytime on your mobile devices with the AFNB Mobile App for iPhone®, iPad® and Android™ devices. However, online security and protection of your identity and personal information is a team effort. Take these additional steps to understand what we do and what you can do to protect your mobile device.

What we do to protect mobile banking:

We encrypt your personal information such as your user name, password and account information when you send it over the internet. American First National Bank's Mobile Banking application and mobile browser will then decode any encrypted information.

We apply a number of security devices, checkpoints and procedures such as firewall systems and intrusion detection software, encryption of sensitive information while it is sent over the internet and when stored in our systems, internationally recognized security standards and industry best practices, and the use of application profile and password with context-based multifactor security.

Mobile Banking

What you can do to protect from mobile banking fraud:

If your device allows access via your fingerprint or facial recognition, pay special attention to prevent misuse, as it may also give access to your American First National Bank Mobile Banking app when Biometric ID authentication is enabled.

As a reminder, we will never ask our customers for account numbers, passwords or other sensitive personal information by email, telephone, or text message. Likewise, you should never send sensitive information such as account numbers, Social Security numbers or passwords via email or text message because these are often transmitted over the internet without any protection.

How to protect your device:

1. Enable automatic locking.
2. Enable Biometrics.
3. Keep all applications and operating systems up to date.
4. Avoid doing banking activities when on public Wi-Fi Networks.
5. Never leave your phone unattended

Cybersecurity

More and more people are conducting their banking business online and on their mobile devices, making cybercrime an increasingly larger threat. For American First National Bank, cybersecurity is a top priority.

Even though cybercrime is a growing issue, there is a lot that you can do to protect yourself.

YOU ARE THE GREATEST DEFENSE AGAINST

CYBER THREATS

———————————————————————————-

Phishing:

Phishing (pronounced “fishing”) is a type of cybercrime that uses email to target an unsuspecting individual. Usually to attempt to gain personal information to be later used in an account compromise.

Indicators of a Phishing email:

1. Email may contain a misspelling in a name or email address so as to appear to come from someone you know.
2. Email may be sent from an unknown address .
3. Email may contain false account information.
4. Email may contain unknown hyperlinks.

A good practice is to not click on any links in a suspicious email. And never enter any personal information when prompted.

Cybersecurity

SMishing:

This is a type of attack similar to phishing, however it is done via SMS Texting to your cell phone.

The best way to stop SMishing is to simply not respond to messages from an unknown sender and delete the message.

Remember, American First National Bank will not contact you to obtain personal information via text.

MALWARE:

Malware generally takes the form of a computer virus or other malicious software that attacks your computer. Often this unwanted software runs in the background collecting information that you type in online. Ultimately transmitting the information back to an attacker. Malware can run undetected for long periods of time on your computer.

The best way to prevent Malware is to be wary of websites that may appear suspicious. And keep your Anti-Virus software up to date as well as install your operating system patches and updates.

Think Before You Click