

Spoof emails can be a major problem for unsuspecting Internet users. Claiming to be sent by well-known companies, these emails ask consumers to reply with personal information, such as their credit card number, social security number or account password. These deceptive emails are called "Spoof Emails" because they fake the appearance of a popular Web site or company in an attempt to commit identity theft. Also known as "hoax" or "phishing" emails, this practice is occurring more and more frequently throughout the online world.

Warning Signs of a Spoof Email

A. Sender's Email Address

Spoof email may include a forged email address in the "From" line - Some may actually be real email addresses that have been forged. (From: billing@fnbmcgehee.com; From: questions@fnbmcgehee.com; From: support@fnbmcgehee.com).

B. Email Greeting

Many Spoof emails will begin with a general greeting such as "Welcome First National Bank of McGehee Customer."

C. Urgency

Claims that the Bank is updating its files or accounts - Don't worry, it is highly unlikely that First National Bank of McGehee will lose your account information.

D. Account Status Threat

Most Spoof emails try to deceive you with the threat that your account is in jeopardy and you will not be able to use your First National Bank Internet Banking account if you do not update it immediately.

E. Links in an Email

While many emails have links included, just remember that these links can be forged too.

F. Requests Personal Information

Requests that you enter sensitive personal information such as a User ID, password or bank account number by clicking on a link or completing a form within the email are a clear indicator of a Spoof email.

Legitimate First National Bank of McGehee Web Addresses

Examples of fake First National Bank of McGehee addresses:

<http://signin.fnbmcgehee.com@10.19.32.4/>

<http://signin-fnbmcgehee.com/>

Real First National Bank of McGehee Internet Banking Address:

<https://banking.fnbmcgehee.com/>

Here are some tips on how to protect your account and what to do if you think you may have responded to a Spoof email:

- **Scan for Viruses** Frequently scan your computer for viruses and make sure your virus software, operating system, and browser patches are up to date.
- **Vigilance Is the Best Line of Defense.** You should periodically check your account to see if there is any suspicious activity.

• **Change Your Password Frequently.** If you think your account security may have been breached, change your account password immediately and inform the bank.

• **Make Your Password Unique.** To prevent someone accessing multiple accounts, it is effective to have different passwords for each account. Also, a good password will include a combination of letters and numbers - this makes it more difficult for people to guess the password.

If you get an email that looks like it's from First National Bank of McGehee about a problem with your account or requests personal information, it's a fake email. First National Bank of McGehee only sends or requests information via our secure messaging network. These messages are only accessible after login to your FNB Internet Banking Account.

The good news about Spoof emails is that you are in control - you can protect your personal financial information by ignoring the spoof altogether. You should never provide contact, sign-in or other sensitive personal information in an email.

Reporting Spoof emails is easy.

If you have any doubt whether an email is really from us, here's how to report it:

1. Forward the message to info@fnbmcgehee.com.
2. Don't alter the subject line or forward the message as an attachment - doing so prevents us from investigating it further.
3. Once you have forwarded the email, you can then delete it from your email account.

Protecting Your Identity

Deter identity thieves by safeguarding your information.

1. Shred documents with personal information before discarding
2. Don't give out your Social Security number or other personal information unless you know who you're dealing with

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

1. Inspect your credit reports, financial statements and bills regularly for activity you did not authorize or expect

Defend against ID theft as soon as you suspect it.

1. Place a "Fraud Alert" on your credit reports
2. Close the affected accounts
3. File a police report
4. Report ID theft to the FTC

For more information, visit ftc.gov/idtheft