

AmeriFirst Bank

Customer Information Security Awareness

At AmeriFirst Bank, we take the safeguarding of your information seriously. In fact, we believe keeping your information safe and secure is every employee's responsibility. We also encourage you to take steps in protecting your personal information.

No employee of AmeriFirst Bank will ever email or call you requesting your personal information, including account numbers, passwords, driver's license, Social Security Numbers, etc. by phone, email or a link to a website.

If you choose to contact AmeriFirst Bank using e-mail, please do not send privileged or personal information via regular e-mail to us as information transmitted through this medium is not encrypted and therefore not secure. If you need to send privileged or personal information to AmeriFirst Bank by email please contact an AmeriFirst employee for a link to our secure email portal.

Protecting Yourself when Online

The online banking industry continues to see an increase in fraudulent activity year after year. With malware, virus attacks and scams becoming more prevalent.

Phishing

Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email from an organization with which you may or may not do business. In many cases, the email has been made to look exactly like a legitimate organization's email would appear, complete with company logos and other convincing information. The email usually states that the company needs you to update your personal information or that your account is about to become inactive, all in an effort to get you to click the link to a site that only looks like the real thing. This is still one of the most popular ways for the criminal to get all the necessary information to access your accounts online.

No reputable business will ever email you requesting that you update your personal information, including account numbers, system passwords or Social Security Numbers via a link to their site.

Follow these guidelines to protect yourself from phishing scams:

- Never click on a link from a business requesting your personal information.
- Pay close attention to the URL (Internet address) behind the link. Often in phishing attempts, if you hover the cursor over the link the fraudsters want you to click on, it has nothing to do with the actual company they claim to be.
- If your Financial Institution uses watermarks or personal images, do not log in unless you see the correct image on the screen.
- Report any phishing attempts to your Financial Institution and to the Federal Trade Commission on their website.

If you are ever in doubt the validity of the caller or email, call the company at their public phone number or go to their website and sign in to your account. Never use the number given to you by the caller or click on any link in a suspicious email, open a new Internet session and manually key in the business' web address. If the business genuinely needs information from you, they will have you log in to your online account to see the request.

Ransomware

Ransomware is a form of malicious software (Malware) that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data "hostage" until the victim pays a ransom, frequently demanding payment in Bitcoin. One popular technique - someone will call you saying there is a problem with your computer and they need access to it to fix it. They usually say they are with a reputable company like Microsoft, Norton, etc. No legitimate company will do this. Another popular

Ransomware (Cont'd)

Technique is the use of email **Phishing** campaigns which typically requires you to take some kind of action such as clicking on a link or downloading a malicious attachment.

Here are some tips to help protect against malware.

- Always make sure you have the latest Windows updates.
- Make sure your computer has the latest anti-virus updates.
- Backups are crucial. Keep your files backed up regularly and periodically on a separate device.
- Do not open emails from unknown addresses.
- Do not click on unverified links in your emails.
- Be suspicious of visiting unsafe, unsecure or unreliable websites.
- Take extra caution when on social media and do not click on skeptical ads.
- If you receive a message from your family or friends with a link, before you click on it, verify that they did send it because infected machines can sometimes send random messages with links.

What are some ways to protect myself from fraud?

Besides following the tips mentioned in the previous examples, here are some best practices to help safeguard your personal and financial information.

- Change your passwords often. Even if your financial institution doesn't require it, it is a good practice to change your passwords at least every six months. An easy way to remember: change them when you change your clocks to adjust for Daylight Savings Time.
- Don't use the same ID and PIN/Password for every online account you have.
- Create passwords that mix letters, numbers, and special characters
- Never disclose your login credentials to other people or companies.
- Do not store your ID and Password information where others could gain access to it. It is best not to write the information down at all.
- Do not use public computers and open wireless networks for sensitive online transactions. Wi-Fi spots in airports, hotels, coffee shops, and other public places can be convenient but they are rarely safe. If you're accessing the Internet through an unsecured (unsafe) network, you should be aware that malicious individuals might be able to eavesdrop on your connection. This could allow them to steal your login credentials, financial information, or other sensitive information. Any public Wi-Fi should be considered "unsecure."
- Businesses that use online banking services should consider doing periodic risk assessments and evaluate their controls in place to protect them.
- Do not send confidential information of any kind by email unless it is encrypted.
- Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.
- Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn't come on time, contact the business.

As Cyber Criminals tactics continue to evolve an excellent source of information on how to prevent identity theft and what to do if you are a victim of identity theft is the Federal Trade Commission website at www.ftc.gov. Homeland Security's website www.onguardonline.gov and the Federal Trade Commission website www.ftc.gov have valuable information about staying safe online.

If you notice any suspicious or unusual activity related to any of your accounts, contact us immediately at 1-800-298-1763 or at any Branch Office; Union Springs 334-738-2060, Vaughn Road 334-409-2980, Prattville 334-358-0351 or Lee County 334-821-1329.