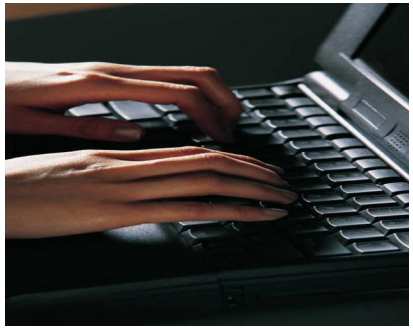
Friends Bank
A REAL HOMETOWN BANK

Online Banking Fraud Prevention Best Practices



Safe Computing is in your hands. We'll do our part, YOU do yours.

This brochure will provide you with information and best practices you can use to protect your personal information in an online environment.

USER ID AND PASSWORDS

- Create a "strong" password with at least 8 characters that include a combination of mixed case letters and numbers.
- Change your password frequently. Friends Bank Online Banking will automatically require you to change your password every 90 days.
- Never share username and password information with third-party providers.
- Avoid using an automatic login feature that saves user names and passwords.

PROTECTING ONLINE PAYMENTS & ACCOUNT DATA

When you have completed a transaction, ensure you log off to close the connection ("exit" button for Friends Bank online banking).

Reconcile by carefully monitoring account activity and reviewing all transactions initiated by you or your company on a daily basis.

Always verify the URL address before entering passwords or other personal information. A secured site/page will include "https".

Know who you are dealing with when purchasing online. Look for physical addresses and a working telephone number.

AVOIDING PHISHING, SPY-WARE AND MALWARE

Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.

Call the source of any e-mail you feel may be suspicious. Do not call any number listed on the e-mail. Call the number you are familiar with or look it up in a reputable directory.

Install anti-virus and spyware detection software on all your computers. Free software may not provide protection against the latest threats compared with an industry standard product.

Keep your computers updated regularly with the latest versions and patches of both anti-virus and anti-spyware software.

Ensure your computer operating system and key applications are patched and updated regularly.

Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.

Check your settings and select, at least, a medium level of security for your browsers.

Clear the browser cache before starting an online banking session in order to eliminate copies of Web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu.

GENERAL FRIENDS BANK ONLINE BANKING GUIDELINES

Do not use public or other unsecured computers for logging on to your online banking.

Check your last login date/time every time you log on.

Review account balances and detail transactions regularly (preferred daily) to confirm payment and other transaction data and immediately report any suspicious transactions to us.

View transfer history available through viewing account activity information.

Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping.

Take advantage of, and regularly view system alerts such as Balance Alerts, Transfer Alerts and Password Change Alerts.

Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.

Whenever possible, register your computer to avoid having to re-enter challenge questions and other authentication information with each login.

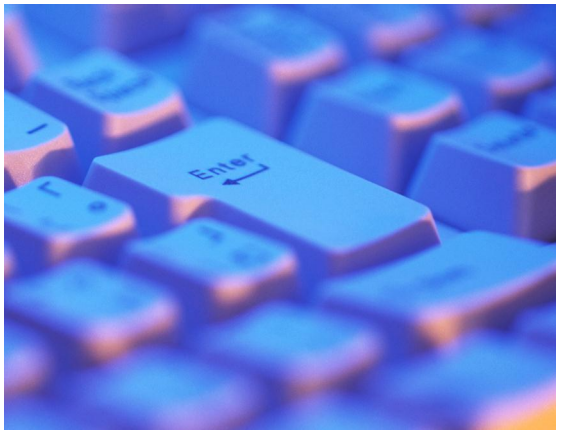
Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.

Never leave a computer unattended while using your online banking,

Never conduct banking transactions while multiple browsers are open on your computer.

For more information about internet fraud prevention, online banking, and protecting your personal information visit the Federal Trade Commission's website at www.ftc.gov

Think before you react. Most spam, viruses and fraudulent emails stress urgency and strongly suggest to take action now—don't become a victim, avoidance of clicking links, responding to unsolicited emails and providing personal information is your defense!



Let us help you to not become a victim of internet fraud. Of course, we know there is no guarantee of never becoming a victim, but together we can fight to protect against it. Please use this information and do not hesitate to call us if you have any questions or concerns.

Main Office: 2222 S.R. 44
New Smyrna Beach, FL 32168
Phone: 386-428-2299

Edgewater: 1504 S. Ridgewood
Edgewater, FL 32132
Phone: 386-424-9669

Ormond: 208 S. Nova Road
Ormond Beach, FL 32174
Phone: 386-671-9409

www.Friendsbank.com

Member
FDIC