

- **Monitor your account.**

Check your online balances and paper statements frequently to spot any fraudulent activity—and report it immediately to your bank.

- **Log off.**

Remember to sign off your bank's secured area when you have finished online banking. Also log off of your computer to prevent unauthorized access to your information and files.

- **Your protections.**

Individuals are protected against unauthorized electronic fund transfers, provided there is compliance with the institution's disclosed reporting requirements. Contact your local banker for information about protections and liabilities.

REMEMBER BE SAFE ONLINE.

Don't click on links in an unsolicited e-mail or share personal information online with anyone.

Ask Your Banker...

Safe Online Banking

Safe Online Banking

Convenient. Popular. Safe.

Online banking makes managing money convenient for millions of American households. With a few clicks of a mouse, customers can check deposits and pay bills, saving time and giving them more control over their finances.

To help ensure your safety while offering you this convenience, banks use sophisticated technology and monitoring techniques, intricate firewalls and other methods of securing customer data.

- **Multifactor authentication.**
Banks use more than one method for verifying a customer's identity before granting online account access. Forms of identification may include something you know (password or PIN) and something you have (ATM card, smart card). Banks also use authentication methods that you may not see, but that nonetheless assist them in knowing if you are who you say you are.
- **Encryption.**
Banks secure your transactions and personal information online using encryption software that converts the information into code that only your bank can read.
- **Privacy policies and training.**
All banks have stringent privacy policies. Employees are trained to treat your confidential information with the utmost care, meeting or exceeding federal and state mandates.
- **Fraud prevention.**
Banks typically use programs that monitor your account to help detect unusual activity.

Customers, too, play an important role in protecting financial information. Here's what you can do to enhance your online security:

- **Use a strong password.**
Experts advise using a combination of letters, numbers and characters, and caution you not to use easily guessed passwords, such as birthdays, children's names or home addresses. Change your password regularly and do not use the same password for multiple accounts.
- **Keep it to yourself.**
Don't share your password or any personal information online with anyone.
- **Avoid fraudulent Web sites.**
To help ensure the Web site you have visited is authentic and secure, when conducting financial transactions online look for a lock icon on the browser's status bar or a Web site URL that begins "https:" (the "s" stands for "secure").
- **Protect yourself online.**
Don't click on pop-ups claiming that your computer is infected or offering discounts, as you may be installing malicious software ("malware") on your machine.
- **Use antispyware.**
Install and regularly update virus protection software that detects and blocks "spyware"—programs that can give criminals access to your computer.
- **Be wary of e-mail.**
Do not share sensitive information via e-mail. If you receive an unscheduled or unsolicited e-mail claiming to be from your bank, proceed with caution. Close the email and log on to your bank's online banking yourself or check with your bank to make sure it's legitimate.