

Ask Your Banker...

Safe Online Banking



American Bankers Association

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 ensure your safety while offering you this convenience, banks use sophisticated technology, 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 whether 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 for 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 a combination of letters and numbers and caution you not to use easily guessed passwords, such as birthdays or home addresses.
- Keep it to yourself.** Don't share your password or any personal information online with any person or company you do not know.
- 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 website URL that begins "https:" (the "s" stands for "secure").
- Use anti-spyware.** Install and periodically 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. Check with your bank to make sure it's legitimate.

- Monitor your account.** Check your balances online frequently to spot any fraudulent activity.
- Log off.** Remember to sign off your bank's secured area when you have finished online banking.

Remember:

Be safe online. Don't click on links in an unsolicited e-mail or share personal information online with a company or person you don't know.