

FDIC

Safe Internet Banking - Protect Your Privacy

Protect Your Privacy

Some consumers may want to know how their personal information is used by their bank and whether it is shared with affiliates of the bank or other parties.

Starting July 2001, banks are required to give you a copy of their privacy policy once you become their customer, regardless of whether you are conducting business online or offline. You may also see a copy of it posted at the bank's Web site. By reviewing this policy you can learn what information the bank keeps about you, and what information, if any, it shares with other companies.

Banks may want to share information about you to help market products specific to your needs and interests. If you do not wish to participate in information sharing, however, you have the right to prevent your bank from sharing your private personal information with parties not affiliated with the bank, except in certain limited circumstances. As of July 2001, your bank should provide a clear method for you to "opt out" of this type of information sharing.

You may have heard that some companies track your Web browsing habits while at their site, to understand your interests and then to market particular services or promotions. You may want to ask whether your bank tracks your browsing habits if these practices concern you. Also, your Web browser may enable you to block the ability of outside companies to track your browsing habits. Your bank and your internet service provider may have more information about how to protect your privacy online.

Help Keep Your Transaction Secure

The Internet is a public network. Therefore, it is important to learn how to safeguard your banking information, credit card numbers, Social Security Number and other personal data.

Look at your bank's Web site for information about its security practices, or contact the bank directly.

Also learn about and take advantage of security features. Some examples are:

- **Encryption** is the process of scrambling private information to prevent unauthorized access. To show that your transmission is encrypted, some browsers display a small icon on your screen that looks like a "lock" or a "key" whenever you conduct secure transactions online. Avoid sending sensitive information, such as account numbers, through unsecured e-mail.
- **Passwords or personal identification numbers (PINs)** should be used when accessing an account online. Your password should be unique to you and you should change it regularly. Do not use birthdates or other numbers or words that may be easy for others to guess. Always carefully control to whom you give your password. For example, if you use a financial company that requires your passwords in order to gather your financial data from various sources, make sure you learn about the company's privacy and security practices.
- **General security** over your personal computer such as virus protection and physical access controls should be used and updated regularly. Contact your hardware and software suppliers or Internet service provider to ensure you have the latest in security updates.

If you have a security concern about your online accounts, contact your bank to discuss possible problems and remedies.

Remember that nonfinancial websites that are linked to your bank's website is not FDIC-insured.

As an added convenience to their customers, some banks offer online links to merchants, retail stores, travel agents and other nonfinancial sites. An outside company's products and services are not insured by the FDIC, and your bank may not guarantee the products and services.

As in everyday business, before you order a product or service online, make sure you are comfortable with the reputation of the company making the offer. Only then should you give out your credit card or debit card number. And never give the number unless you initiated the transaction.