Always log out of internet sites that you visit.

Don't just "X" out of the web browser screen when leaving an internet site. You should use the application "close" or "exit" feature.

Never download unauthorized shareware programs or files without authorization.

Never download programs without first verifying the validity of the information.

How does Reg E protect my business accounts?

Regulation E, under the Electronic Funds Transfer Act, is specifically geared towards consumer accounts as defined by Regulation E. There currently are no similar loss protections for commercial customers.

Here are some "risk-assessment" questions to consider about your company's security?

1. How complex are the passwords required to access your company workstations?
2. Do you currently have anti-virus programs installed on your company workstations / network?
3. Do you take advantage of the patches and upgrades available from software providers?
4. Do you have segregation of daily duties? (e.g.: Are specific people granted access to the banking information? Are there specific duties assigned to specific employees?)
5. What processes do you currently have in place to ensure the security of your business and related information? (e.g.: Do employees have access to the office after-hours? If so, how many and what is the deciding criteria to grant access?)
6. Who has access to download or install information on company workstations? (Are you only allowed to download or install programs if you are the administrator?)
7. Do you monitor your accounts daily? Verifying balances and checking transactions?

Severn Savings Bank will **NEVER** request a customer's personal information (bank card number, account number, Social Security number, Personal Identification Number or password) through email. If you should ever receive an email or phone call requesting personal, confidential information that appears to be from Severn Savings Bank, **DO NOT** respond and contact the Bank immediately at 410-260-2000.

Who can you call to report an issue or ask a question?

- Relationship Manager
- Local Branch Manager

Severn SAVINGS BANK FSB

200 Westgate Circle, Suite 200
Annapolis, Maryland 21401

Annapolis: (410) 260-2000
Baltimore: (410) 841-2000
Toll Free: 1-800-752-5854 | FAX: (410) 841-6296

SevernBank.com

safe banking tips

Severn SAVINGS BANK FSB

EQUAL HOUSING LENDER FDIC

It's safe here.

One of the fastest growing white-collar crimes is identity theft, which occurs when an identity thief gains access to and uses an individual's personal identifying information without his or her knowledge in order to commit fraud or theft. You can protect your privacy and minimize the risk of becoming a victim of identity theft by taking the following steps:

Personal Identifying Information

- Always protect personal identifying information, such as your date of birth, Social Security number, credit card numbers, bank account numbers, Personal Identification Numbers (PINs) and passwords.
- Do not give any of your personal identifying information to any person who is not permitted to have access to your accounts.
- Do not give any of your personal identifying information over the telephone, through the mail or online unless you have initiated the contact or know and trust the person or company to whom it is given.

Credit, Debit and ATM Cards

- Limit the number of credit, debit and ATM cards that you carry.
- Cancel all cards that you do not use.
- Retain all receipts from card transactions.
- Sign new cards as soon as you receive them.
- Report lost or stolen cards immediately.

Credit Reports

- Order a copy of your credit report annually and review it for accuracy.
- Check your credit report for unauthorized bank accounts, credit cards and purchases.
- Look for anything suspicious in the section of your credit report that lists who has received a copy of your credit history.

Telephone and Internet Solicitations

- Be suspicious of any offer made by telephone, on a Web site or in an email that seems too good to be true.
- Before responding to a telephone or Internet offer, determine if the person or business making the offer is legitimate.
- Do not respond to an unsolicited email that promises some benefit but requests personal identifying information.
- Severn Savings Bank will never request a customer's bank card number, account number, Social Security number, Personal Identification Number (PIN) or password through email. If you should receive an email requesting such information that appears to be from Severn Savings Bank, do not respond to the email and contact Severn Savings Bank immediately.

Home Security

- Store extra checks, credit cards, documents that list your Social Security number, and similar items in a safe place.
- Shred all credit card receipts and solicitations, ATM receipts, account and credit card statements, canceled checks, and other financial documents before you throw them away.

PINs and Passwords

- Memorize your PINs and passwords and keep them confidential.
- Change your passwords periodically or as needed.
- Avoid selecting PINs and passwords that will be easy for an identity thief to figure out.
- Institute the practice of changing passwords every 30–90 days.
- Require minimum length and complexity of passwords.

Wallets and Purses

- Do not carry more checks, credit cards, debit cards, ATM cards and other bank items in your wallet or purse than you really expect to need.
- Do not carry your Social Security number in your wallet or purse.

Miscellaneous

- Use common sense and be suspicious when things do not seem right.
- Be suspicious of any proposed transaction that requires you to send an advance payment or deposit by wire transfer.
- Monitor and balance your account daily.
- Do not e-mail proprietary information without encrypting software.

Additional Security Items for Business Customers

Dedicated Workstation

Designate a specific workstation as the "Banking Workstation" and limit its use to only banking business. This workstation should not be used for web browsing.

Dual Control

Assign one user with the authority to create a transaction and choose a different user to actually submit / approve the transaction.

Always Update Workstations w/ Latest Anti-Virus Software

Advances in technology happen at lightning speed as do the number of ways someone can wreak havoc on your accounts and computers. Make sure your anti-virus software and patches are up to date.

Always lock workstations if leaving them unattended.

Locking workstations will prohibit unauthorized users from gaining access to programs on your workstation when you are not around.