Safety & Security

Bay-Vanguard is committed to helping you protect your personal and financial information. We want to keep our customers aware of how to best protect their accounts.

Protect your personal financial information

Email Phishing
Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. In some cases, the email may appear to come from a government agency or even your financial institution.

You may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity such as your mother's maiden name.

Bay-Vanguard will never request personal information via an email or over the phone unless you initiate the contact. If you receive a suspicious email delete it immediately. We will never email you and ask you to go to another site to "verify information."

Report Fraud Immediately
Call 410-768-5300 (Mon-Fri 9am – 4pm, Sat 9am -1pm)

How to protect yourself:

1. **Never provide your personal information in response to an unsolicited request**, whether it is over the phone or over the Internet. Emails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.
2. **If you believe the contact may be legitimate, contact the financial institution yourself**. You can find phone numbers and websites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. They key is that you should be the one to imitate the contact, using contact information that you have verified yourself.
3. **Never provide your password to anyone over the phone or in response to an unsolicited Internet request**.
4. **Review account statements regularly to ensure all charges are correct.**
5. **Keep updated virus protections on your computer**. Do not use unprotected internet connections.
6. If you are using Microsoft Windows XP operating system, please note that Microsoft is no longer releasing security patches for Windows XP. We advise customers to upgrade any Windows XP PC's to a supported operating system.

Passwords are the first line of defense against unauthorized access. You should make sure you have strong passwords for all accounts. All passwords should be changed regularly and not repeated.

A strong password contains:

- At least eight characters
- A combination of upper and lowercase letters, numbers and symbols
- Does not contain your user name or real name
- Does not contain a complete word

If You Think You're a Victim of Fraud

- Contact Your Bank and Your Credit Card Issuers Immediately
- Change PINs to All Your Bank Cards
- Stop using your computer and get it professionally wiped
- Ensure all security software is up to date
- Change User Names and Passwords to all your shopping, online banking and social networking accounts
- Get New Bank Cards and Account Numbers
- Place a 'Stop Payment' Order on missing or stolen checks
- Place a Fraud Alert on your credit reports
- Freeze your Credit
- Contact the Social Security Administration
- File a Police or Identity Theft Report
- Contact the DMV
- File a Complaint with the FTC

If you Suspect Your Identity has Been Stolen

1. Call your bank and credit card issuers immediately so they can start working on closing your accounts and clearing your name.
2. File a police report and call the fraud unit of the three credit-reporting companies.
   The fraud unit numbers are:

TransUnion	(800)680-7289
Experian	(888) 397-3742
Equifax	(800) 525-6285

3. Consider placing a victim statement in your credit report.
4. Make sure to maintain a log of all the contacts you make with authorities regarding the matter. Write down names, titles, and phone numbers in case you need to re-contact them or refer to them in future correspondence.
5. For more advice, contact the FTC's ID Theft Consumer Response Center at 1-877-ID THEFT (1-877-438-4338) or ftc.gov/idtheft.