



Virginia State Police

Division 3

Appomattox, VA

The Virginia State Police HTCU

The High Technology Crime Unit is part of the Bureau of Criminal Investigation. The Appomattox Field Division is one of seven field divisions in the Commonwealth of Virginia. It covers 15 counties including the cities of Lynchburg, Charlottesville and Staunton. Two Special Agents are presently assigned to investigate computer-related crimes such as child pornography and exploitation, child sexual predator, identity theft and internet financial crimes.

The HTCU functions both as an investigative arm of BCI and as a partner with other local law enforcement agencies to assist in investigations by way of regional task forces.

Now that you know a little about us, we hope the information provided in this brochure will be useful to you as a citizen of the Commonwealth. Please visit the Virginia State Police main website at www.vsp.state.va.us.

Virginia State Police/BCI
Division 3 Headquarters
P.O. Box 577
Appomattox, VA 24522

Identity Theft

First and foremost is to prevent Identity Theft. Most ID Theft cases are difficult to solve due to the delay of reporting caused by the crime itself going undetected by the victim. Many victims are not aware of the crime until notified by a credit bureau check, a collection agency or another financial institution.

Simple Steps to prevent "Low-tech" Identity Theft

- Remove Social Security Number from Driver's License and Checks, use the DMV generated VADL number.
- Drop mail containing checks you have written at the Post Office or use the blue USPO drop boxes.
- Don't write the complete credit card numbers on checks when making a payment, just write the type of card and the last four digits (ex. "VISA 1234")
- Use "gel" pens when writing checks or other financial documents. The ink is harder to dissolve if a criminal came into possession of your document.
- Shred, tear-up or mark over any personal information before throwing it in the trash. Protect your name, address, telephone number and social security number, all of which can be used to establish fraudulent accounts.
- Opt-out from pre-approved credit card offers in the mail and tell your bank not to send "courtesy checks" with your billing statements. See helpful telephone and website lists.

Simple Steps to prevent "High Tech" Identity Theft

- Never give out your checking account number over the telephone or to any inquiry on the internet.
- Never give your personal information (name, date of birth, SSN, etc.) to anyone over the telephone or internet unless YOU initiated the transaction and it is with a business or person you know.
- Websites like PayPal, Ebay, Yahoo, AOL and your bank will NOT ask for passwords or other personal information using email. Official email will always be addressed to you using the name you opened the account in.
- Keep your anti-virus and anti-spyware software up-to-date on your computer and keep your firewall on, especially with cable and DSL accounts that are virtually connected 24/7.
- Change your default passwords if you are using a wireless router at home. Every thief knows that "linksys" is the default password for every WiFi router made by that brand.
- The safest form of payment on the internet is the credit card. The least safest is the "wired" funds like Western Union. Almost all scams want some form of electronic payment like EFTs, wired transactions or US money order.
- Review all credit cards statements as they are received. Call your bank if you have any suspicious telephone calls or account activity.