fastweb!
A MONSTER COMPANY

Student Bulletin

Avoiding & Preventing Identity Theft

How can you protect yourself from being an ID theft victim?

- Shred and crosscut documents such as old bank, brokerage and credit card statements, old credit cards and pre-approved credit card offers.
- Make sure you receive replacement credit or bank cards in a timely manner. If not, contact the issuer immediately.
- Do not provide personal or financial information after clicking on a link in an email message from your bank or financial institution. The email message may be a forgery designed to collect your personal and financial information.
- Do not post personal information on blogging, instant messaging and community websites. This includes your photo, home address, the school you attend or home and cell phone numbers, your Social Security number (SSN) and/or date of birth.
- Password protect all your accounts with made-up words and change them frequently. Do not use your mother's maiden name as a password or confirmation. For passwords, use a combination of letters and numbers, not anybody's name as a password, nor abcdef, 123456 or qwerty, as it is standard for a cracker to try all dictionary words (including combinations of two words) and names. Use a different password for each account.
- Memorize your SSN and passwords so they do not need to be written down.
- Never give out SSN, credit card or bank numbers to an unsolicited e-mailer or caller, even from parties that seem legitimate (e.g., your bank or credit card company).
- Order your free credit report three times per year. Visit www.annualcreditreport.com or call 1-877-322-8228 for more information. You are entitled to one free credit report per year from each of the three main credit bureaus (Equifax, Experian and TransUnion). Place a fraud alert on your file right away if you find fraudulent items on your report. Warning: Avoid "look-a-like" web sites with a similar name to annualcreditreport.com; these sites aren't really free.
- Do not use your SSN as an ID number. Also, do not include SSN on your driver's license or school ID.
- Notify your credit card company if you are missing a statement in the mail. It may have been stolen.
- Keep a list of all credit cards, bank account and customer service numbers and a photocopy of the front and back of each card in a locked, safe place. Do not store this information on your computer, PDA or cell phone.
- Do not apply for any scholarship that asks for your SSN on the application form. They do not need to know your SSN unless you win the scholarship.

What to do if you're an ID theft victim

- Contact your bank and credit card issuers.
- File a report with your local law enforcement.
- File a report with the Federal Trade Commission at: www.consumer.gov/idtheft.
- Contact the main credit bureaus (Equifax, Experian, TransUnion) to place a fraud alert on your file.
- Notify your post office if mail was stolen.
- Notify your phone company and / or your internet service provider if your ID was stolen over the phone.
- Notify the Social Security Administration (www.ssa.gov) if your SSN was compromised.

Beware of Phishing & Pharming!

"Phishing" refers to unsolicited emails that bear the logo of your bank or credit card. They appear legitimate, but are traps to lure you into giving out your information. Never give out your SSN, credit card, PINs, passwords, bank account numbers or date of birth to an unsolicited emailer or caller. Banks and other financial institutions will never ask you to give them your password.

"Pharming" refers to a virus or program planted on your computer that takes over your browser. When you type in legitimate websites, you are then taken to a false copy of that site that captures your usernames and passwords. Install virus protection software and run it often!

Identifying Scholarship Scams

- You have to pay a fee or "taxes"
- Money-back offers or guarantees
- Credit card or bank account required
- Provides "exclusive" information