Protecting you p-card from Fraud

What to do if there's Fraud on your account:

US Bank diligently works to prevent fraud. If a p-card has unusual activity, small dollar charges (such as 1.00 or 2.00), red-flag vendors (such as foreign vendors or unsecured on-line companies), or vendors not normally used by the cardholder, the bank will temporarily close the account until the cardholder is reached. A decline may say, "Caution Account" or "Fraud". If the cardholder has not been notified already by US Bank, they must call the Fraud Investigations department at **1-800-523-9078** to verify charges.

On average P-cards yield over 80,000 transactions annually. The average P-card accounts compromised at Boston College is approximately 30 per year with no physical cards taken.

The most proactive thing you can do: CHECK YOUR STATEMENT every month. If possible, check your p-card purchases on a weekly basis on US Banks' Access-on-line even if you have no p-card activity.

Here's how they do it:

1. **Phishing**: An attempt to acquire information such as usernames, passwords, banking and credit card numbers usually by e-mail or instant messaging. The message asks you to click on to a site which is almost identical to your bank's to verify information.
   Here's what you can do: Don't clink on to anything that tells you to "verify your information here". Look at the link carefully, it will have added words, (dot com may appear twice): i.e.: www.bankofamerica.com.verifing.com.
   When in doubt, call your bank directly.

2. **Vishing**: Like Phishing except the criminal will call you directly on your phone, pretending to be from your bank or credit card issuer.
   Here's what you can do: Your bank or credit card issuer will NEVER call you asking for personal information. Never trust *anyone* who calls you and asks for your social security #, bank account # or credit card information.

3. **Spyware**: Computer software inadvertently installed on your computer when visiting or accidently visiting certain websites. Once installed, your every move can be tracked, including signing on to your bank website and entering your secret passwords as well taking stored information from the desktop and access to your email.
   Here's what you can do: Install anti-spyware on your home computer. BC already has this tool installed in work computers. However, there was an incident where an entire department's p-card numbers were stored and stolen off the desk-top from Internet criminals. Run your "Identify Finder"

program everyday to ensure sensitive information is not stored anywhere vulnerable. Store information in a secured server behind a firewall. Do not put credit card #'s in e-mail!

4. **Skimming:** Typically an "inside job" from a dishonest employee by a legitimate merchant who steals your credit card number directly from you. This usually happens in bars or restaurants where you are not in view of the transaction.
   Here's what you can do: Avoid outside shopping with your p-card. In general, you are more protected using a p-card on the internet. Please make sure the website you are using is a secure one. In the address bar, the website should begin with "https". The "s" at the end means it's a secure, encrypted site.

5. **Data Breach:** Trusted businesses that have your personal information stored may fall victim to being hacked. A data breach also takes place when a computer, media storage device or box of files is lost, stolen or misplaced.
   Here's what you can do: When a company is breached, the cardholders are usually notified or it is publically announced on the News. Please do not ignore that notification. If your p-card is involved in a breach, please contact pcard@bc.edu. Five P-cards in FY12 were compromised when a company called "Global Payments" was breached.

6. **Social Networking:** Thieves can now get personal information about you directly from your Facebook page. (Date of birth, maiden name, city zip code, etc.) They can use that information and pretend to be someone else to get more information from you or your network of friends. In addition, they can now answer any secret questions under a "forgot pass-word" field.
   Here's what you can do: Please keep your Facebook, Linked-In, Twitter, My-Space, etc settings private. Don't answer personal questions from someone you do not know (or *think* your know)