IDENTITY THEFT & CYBER SECURITY

Office of Information Technology

COLLEGE OF STATEN ISLAND/CUNY

College of Staten Island/CUNY
2800 Victory Blvd.
Staten Island, NY 10314

Office of Information Technology
Bldg. 22, Room 303
Computer Security at CSI

- At the College of Staten Island (CSI) the Office of Information Technology installs and maintains the most up to date technology to protect and secure the information distributed online throughout the campus offices and laboratories by means of firewalls, intrusion detection, authentication, and encryption software on the campus Local Area Network (LAN). Software that is designed to protect against viruses and hackers is installed on campus computers. The technology cannot protect against inappropriate or careless use, nor is it effective for use outside the campus LAN.
- If members of the College community suspect that they are victims of stolen identity or attack on their computers, they should notify OIT immediately – dial HELP.
- Steps to follow in the event of suspected identity theft are outlined below and given in complete detail in the FTC Facts for Consumers at the Website listed.

What is identity theft?

Identity theft is a crime in which an imposter obtains such key pieces of information as a Social Security number, driver’s license number, or credit card number to obtain merchandise and services, credit, and loans in the name of the victim.

How identity thieves obtain your personal information:
- They use personal information you share on the Internet.
- They scam you, often through email, by posing as legitimate companies or government agencies with which you do business.
- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks, and tax information.
- They complete a “change of address form” to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as “dumpster diving.”
- They fraudulently obtain your credit report by posing as a landlord, employer, or someone else who may have a legitimate need for, and legal right to, the information.
- They find personal information in your home.
- They get your information from the workplace in a practice known as “business record theft” by stealing files out of offices where you’re a customer, employee, patient, or student; bribing an employee who has access to your files; or “hacking” into electronic files.

How identity thieves use your personal information:
- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account.
- They open a new credit card account, using your name, date of birth, and SSN.
- They establish phone or wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they’ve incurred under your name.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.
- They give your name to the police during an arrest.

What can you do to minimize your risk?

- Maintain a secure computer and use email and the Internet with proper safeguards.
- Order a copy of your credit report from each of the three major credit bureaus. Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills, whether you’ve been sued or arrested, or if you’ve filed for bankruptcy. Make sure it’s accurate and includes only those activities you’ve authorized. By law, credit bureaus can charge you no more than $9 for a copy of your credit report. See “Credit Reports,” below, for details about removing fraudulent and inaccurate information from your credit report.
- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother’s maiden name, your birth date, the last four digits of your SSN, or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother’s maiden name. Use a password instead.
Ways to protect yourself and your information on the internet

Credit Bureaus
- Equifax — www.equifax.com
  To order your report, call: 1.800.685.1111
  To report fraud, call: 1.800.525.6285/
  TDD: 1.800.255.0056 or write:
  P.O. Box 740241, Atlanta, GA 30374-0241
- Experian — www.experian.com
  To order your report, call: 1.888.EXPERIAN (397.3742)
  To report fraud, call: 1.888.EXPERIAN (397.3742)/
  TDD: 1.800.972.0322 or write:
  P.O. Box 9532, Allen TX 75013
- TransUnion — www.transunion.com
  To order your report, call: 1.800.888.4213
  To report fraud, call: 1.800.680.7289/
  TDD: 1.877.553.7803; fax: 1.714.447.6034; or email:
  fraud@transunion.com or write: Fraud Victim Assistance
  Department, P.O. Box 6790, Fullerton, CA 92834-6790

Maintain vigilance
- Do not give personal information over the Internet, on the phone, or through the mail unless you initiated the contact or are sure you know the person with whom you are dealing.
  Identity thieves may pose as Internet service providers (ISPs), email contacts, representatives of banks, and government agencies to get you to reveal your SSN, mother’s maiden name, account numbers, and other identifying information.
  You can check the organization’s Website as many companies post scam alerts when their name is used improperly.
- Order a copy of your credit report once a year from each of the three major credit bureaus mentioned above.
- Guard your mail and trash from theft.
- Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox.
- Tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you’re discarding, and credit offers you get in the mail.
- Before revealing any personally identifying information (for example, on an application), find out how it will be used and secured, and whether it will be shared with others. Ask if you have a choice about the use of your information. Can you choose to have it kept confidential?
- Do not carry your Social Security card; leave it in a secure place. Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible.
- Carry only the identification information and the number of credit and debit cards that you’ll actually need.
- Pay attention to your billing cycles.
- Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work.

CYBER security

Password security
- Never share your password with anyone.
- Make sure your password is secure (avoid obvious names or birthdays and make sure it is at least six characters, including numbers, letters, and symbols). For example, 4Pa$$enure#1 or L3tsG0nyg! are examples of good passwords.
- Change your password periodically.
- Use different passwords for different purposes. For example, use different passwords for Websites, banking, and email.

Email security
- Never reveal personal information like passwords, Social Security number, or bank information in an email. Keep in mind that email is not an inherently secure form of communication.
- Do not download files from unknown senders and never click on hyperlinks from senders you do not know. Opening a file could expose your system to a computer virus (or Trojan) or a program that could hijack your modem. See Spyware and Spoofing below.

Website security

Spyware
- Spyware sneaks into your computer when you open infected e-mails, click on dubious Internet pop-up ads, or download many file-sharing services. Spyware or key loggers can manipulate your computer system, record your use of the Internet, and steal your passwords and credit card numbers. Current estimates are that over 78,000 Spyware programs are infecting computer systems. Spyware can steal your identity and is difficult to remove: do not open email and/or attachments from unknown sources, avoid pop-up ads, and be very careful with file-sharing.
Spoofing
• Websites that appear to be genuine, but are fraudulent (eBay look-alikes, for example), enter computers through emails known as “spoof” or “phishing.” Created by hackers or other unauthorized persons, these emails appear as information, promotions, or solicitations. If the email is suspicious, do not open it—delete it if opened, do not respond, and never click on the link. Genuine Websites will not request by email personal information, passwords, credit card numbers, etc. If you received a suspicious message, check the real Website and compare addresses and report the spoofs to the administrator of the Website.

Software updates
• Keep your software up to date via software patches. Many viruses, Trojans, and other security breaches can be stopped this way.

Viruses
• Use and update your virus protection software regularly and when a new virus alert is announced. Computer viruses or Trojan horses can have a variety of damaging effects, including the introduction of program code that causes your computer to send out files or other stored information.

Firewalls
• Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL, or T-1, which leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop unauthorized persons from accessing your computer. Without it, hackers can take over your computer and access your personal information.

Browsers
• Use a secure browser — software that encrypts or scrambles information you send over the Internet. Before providing sensitive or personal information online, be sure your information is encrypted by using only URL addresses that begin with “https://” (the s is for secure) and browsers that display a padlock in the bottom-right corner. Be especially careful if using an unfamiliar company or source online.

Laptops
• Store financial information in your laptop only if absolutely necessary. If you do have personal or financial information in your laptop, use a strong password — a combination of letters (upper and lower case), numbers, and symbols. Do not use an automatic log-in feature and always log off.

Disposing of a computer
• Before you dispose of a computer, delete personal information. Deleting files using the keyboard or mouse commands usually is not sufficient because the files may stay on the computer’s hard drive, where they may be easily retrieved. Use a “wipe” utility program to overwrite the entire hard drive. It makes the files unrecoverable.

Privacy policy
• Look for Website privacy policies. If no privacy policy is displayed, consider finding another site.

Think before you click
Remember, common sense can often be your best defense. If something doesn’t seem right, think before you click. In the past five years, over 27 million people have been victims of identity theft. An even larger number have been infected with viruses or Trojans, and many don’t even know it! While there is no one single guideline you can follow to protect yourself, the more information you have, the more secure your identity.
For detailed information, visit:
http://www.justice.gov/criminal/fraud/websites/idtheft.html
http://www.ftc.gov/