New York State University Police

Officers of the New York State University Police serve as the principle law enforcement and emergency response agency at 28 SUNY campuses. Approximately 600 University Police officers are employed throughout the state with 21 stationed at SUNY Cortland.

All New York State University Police are duly appointed police officers trained to the highest standards in law enforcement, crisis intervention, first aid and other areas of emergency response.

The University Police Department can be found in Whitaker Hall.

Police and Emergency Contact Information

For emergencies on campus, please call 911 or 607-753-2111 for a direct line to UPD dispatch. Emergency lines also can be found around campus marked by blue lights.

To ask questions, report concerns or discuss non-emergencies, please contact the University Police Department at 607-753-2112 or upd@cortland.edu.

New York State University Police
Whitaker Hall, Room 110
Emergency: 911 or 607-753-2111
Non-Emergency: 607-753-2112
upd@cortland.edu

SUNY Cortland
UNIVERSITY POLICE DEPARTMENT

Fraud and Identity Theft

Identity Theft

One of the worst kinds of theft a person can experience is identity theft, which often involves having social security or financial account numbers scammed or stolen.

Easy prevention methods to deter ID thieves:

- Keep your social security card safe. Don't carry it with you in a wallet or pocket. Make sure it is locked away if you have roommates or maintenance personnel entering your house.
- Do not share your social security number even with people you know.
- Place a hold on your mail when you know you will be away from home for several days.
- Do not provide personal information on social media or to people you have met online.
- Shred financial and government documents before throwing them out.
- Create complex passwords that are difficult to guess and do not share passwords with anyone.
- Use firewalls and security programs to protect your information. Make sure these are kept up to date along with your device's operating system.
- Do not respond to emails or phone calls that ask for personal information.
- Do not click on internet search results that you feel may be suspicious.
- Be cautious when downloading apps and software from third-party sources.
- Use two-factor authentication for your accounts.

Scams and Fraud

Your personal information can be the most valuable thing you have, so it's important to protect it and predict how people will try to steal it. Thieves often will pretend to be other people or that they represent government agencies. Knowing how to identify real people and representatives can save you thousands of dollars and a lot of grief.

Common things to look out for when identifying fraudulent calls or emails:

- Do not respond to calls for immediate action. Scammers try to get your money and information before you realize it's a scam.
- If a caller begins the conversation with "Can you hear me?" do not respond. This is a common way to record you saying "yes" which they will use to make it appear as if you have given consent.
- Don't respond to threats over the phone such as deportation or violence. Government agencies will never threaten you nor will they ever ask for payment in the form of gift cards or digital currency services (i.e. Apple Pay, Venmo, PayPal, Bitcoin, etc.).
- Don't respond to calls or emails from government agencies. First contact with these sources will almost always be through the mail. If you are concerned about the authenticity of a government email or phone call, contact that agency via the information found on their official website.
- Don't click on links or files from unknown email addresses, only from people you trust.

Common Ways Identity Theft and Fraud Happen

- **Rummaging:** Going through your trash to find pieces of personal information.
- **Skimming:** Using hidden devices to steal credit card information when you swipe your card at various locations and ATMs.
- **Phishing:** Sending fraudulent emails pretending to be financial or government agencies to try to get you to input personal information.
- **Catfishing:** Deceptive activity where a criminal creates a fake persona online to target a victim for blackmail, fraud, identity theft or violence. Commonly used to lure a victim into an online relationship where the victim feels comfortable providing personal information to the "catfish" or meeting them. In-person meetings may lead to interpersonal violence against the victim.
- **Old-fashioned theft:** Stealing wallets, purses, mail, checks or tax information. Also includes looking over your shoulder while you input personal information and passwords via a phone, tablet or computer.

Recovering From Identity Theft or Fraud

- Close or freeze accounts that were opened/used fraudulently in your name.
- Contact the specific company where your username or password has been compromised.
- Filing a police report is always a good idea.
- Report the theft to the Federal Trade Commission at identitytheft.gov. After giving some information on the nature of the theft, the website will provide a personalized step-by-step list for you to follow.