Skimmers

Identity thieves can obtain your credit card information by a hi-tech method called skimming, using a tiny data-collection device (known as a “skimmer”). A skimmer device can be mounted to the front of an ATM machine or easily concealable in a small portable device.

When customers make a purchase, their cards are swiped through the business's credit-card machine, where the card data is read from the magnetic strip and phoned in for approval. The credit card can then be swiped using a "skimmer" device to capture the card's data on the magnetic strip. This data is then later used to create fake credit cards and make fradulent charges unknown to the victim. Credit card skimming can occur anytime your card leaves your direct possession. Another common skimmer-scam involves locating a portable skimmer card-swipe device near the business's own card-scanner, or even a portable device carried in the pocket of a server.

Victim of Identity Theft or Fraud

Immediately report the crime to your local law enforcement agency and to the three credit bureaus listed below.

EXPERIAN (formally TRW)
Phone: 888-EXPERIAN (888-397-3742)
Website: www.experian.com

EQUIFAX
Phone: 888-685-1111
Website: www.equifax.com

TRANS UNION CORPORATION
Phone: 800-680-7289
Website: www.tuc.com

IDENTITY THEFT

ETSU POLICE
EMERGENCY
(24 Hours)
911
POLICE DISPATCH
(24Hours)
(423) 439-4480
email: bucprevention@etsu.edu
www.etsu.edu/dps

ETSU
East Tennessee State University

IDENTITY THEFT (ID Theft)

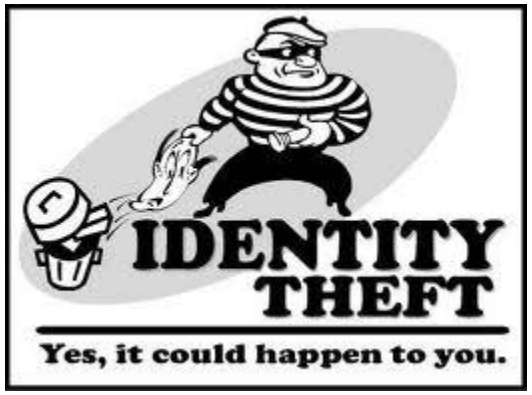
Identity theft is when someone else uses your personal information without your permission to commit fraud and other crimes such as: Obtain credit and credit cards from banks and retailers, steal money from existing accounts, apply for loans, establish accounts, rent an apartment, file bankruptcy, or obtain a job. Identity theft may be used to facilitate or fund other crimes including illegal immigration, terrorism, phishing and espionage. Victims of identity theft may not even know about the fraud for months or even several years.

Types of Identity Theft

- Criminal ID Theft- (posing as another person when apprehended for a crime)
- Financial ID theft- (using another's identity to obtain credit, goods and services)
- ID cloning-(using another's information to assume his or her identity in daily life)
- Medical ID theft-(using another's identity to obtain medical care or drugs)

Targets for Identity Thieves

- Financial Statements
- Online Transactions
- Credit Card Receipts
- IT equipment or Storage Media
- Public Records
- Resumes through False Job Offers
- Social Networking Websites



Means of Identity Theft

Dumpster Diving – Is when criminals go through your trash to obtain thrown out mail that contains personal information.

Phishing – Is sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to obtain private information.

Vishing – Is contacting the public via telephone claiming to be an established legitimate enterprise in an attempt to obtain private information.

Email Scams – Soliciting personal information or money via email correspondence.

Employees – Employees accessing confidential information.

Smishing – Is sending a text to a victim from a false enterprise to attain personal account information.

Skimmers – An Electronic Device used to capture ATM and credit card information from a magnetic strip.

Shoulder Surfing – Someone looking over your shoulder attempting to attain your pin or access code.

Prevention Tips:

- Shred personal financial documents before discarding them.
- Do not provide personal or financial information over the phone to an unknown caller.
- Pay attention to billing cycles.
- Review monthly credit card and other financial statements for unauthorized use.
- Be wary of someone looking over your shoulder trying to steal important financial information when using ATMs and phone cards.
- Do not use your mother's maiden name, your birth date, last four digits, or similar series of numbers as a password for anything.
- Do not carry your social security card, birth certificate, or passport, unless necessary.
- Do not print personal identifiers such as your social security number, date of birth, or driver's license number on your checks.
- Use your social security number only when necessary.
- Do not respond to emails to requesting personal identifier information.