

Identity Theft – Glossary of Terms

Identity Theft – Also known as identity or credit fraud, happens when someone steals personal information such as your account number or Social Security Number, and then uses this information illegally, such as applying for loans, establishing accounts in your name, or making unauthorized withdrawals from your existing accounts.

Email Fraud – A fraudulent (a.k.a. spooking, imposter, phishing) email is one that has been forged so it looks like a legitimate email from a particular organization (such as NECU). Its goal is to trick you into providing sensitive personal information that can be used for identity theft.

Mail Fraud – Mail fraud is a method identity thieves use to obtain your personal information. They steal your mail, which may include pre-approved credit card applications or any other information that will help them get credit in your name.

Phishing – “Phishing” refers to a person or a group of cyber-criminals who create an imitation or copy of an existing legitimate web page to trick users into providing sensitive personal information. Responding to “phishing” emails put your accounts at risk.

Vishing – “Vishing” or “Voice Phishing” leverages Voice over Internet Protocol (VoIP) to obtain your personal information such as account or PIN numbers. You may receive a telephone call from an automated random dialer stating they are a legitimate business (such as NECU). They may then say your credit card or account has been deactivated or used illegally and instructs you to dial a fake toll-free number. Once you dial this number, you are then told to enter your credit card number and PIN. If you give this information, you face the risk of your accounts being compromised.

Dumpster Diving – Dumpster diving is another method identity thieves use to obtain your personal information. They go through garbage bins looking for people’s personal information (account numbers, PIN number, passwords). That’s why it’s very important to always shred your important documents before throwing them out.

Shoulder Surfing – Shoulder surfing is a term used to describe what identity thieves can do to try and get your personal information. They may do this by hanging around close to the ATM, or wherever you may enter your PIN, or they can even watch you from a distance using binoculars. Be aware of who is around you whenever you are entering your PIN.

Skimming – Skimming is another method identity thieves use to get your personal information. It’s usually done by an employee of a restaurant, gas station, or any other place where you swipe your card. They have little swiping tools of their own, which they use to quickly swipe your card. To prevent this, you can request to swipe your own card at the establishments’ payment terminal.