Fraud Tactics

Tactics

Different fraud tactics all share the same goal: to obtain your personal, confidential and financial information for fraudulent use.

From obtaining your information 'the old fashioned way' via discarded mail, to newer electronic methods including emails that ask you to verify personal information under the guise of a trusted source like your financial institution fraudulent activity comes in many different forms.

Malware

Also known as 'malicious software', malware is designed to harm, attack or take unauthorized control over a computer system. Malware includes viruses, worms and Trojans. It's important to know that Malware can include a combination of all three of the types noted.

Phishing

A scam that involves the use of replicas of existing Web pages to try to deceive you into entering personal, financial or password data. Often suspects use urgency or scare tactics, such as threats to close accounts.

Vishing

Vishing is a type of phishing attack where the attacker uses a local phone number in the fake email as a means of obtaining your sensitive information. The goal is to fool you into believing the email is legitimate by instructing you that responding to the request by phone is safer than responding by email and shows authenticity. The unsuspecting caller is then tricked through an automated phone system to relinquish their sensitive information.

Pharming

Pharming takes place when you type in a valid Web address and you are illegally redirected to a Web site that is not legitimate. These 'fake' Web sites ask for personal information such as credit card numbers, bank account information, Social Security numbers and other sensitive information.

Dumpster Diving

Thieves rummage through trash looking for bills or other paper that includes your personal information.

Trojan

A Trojan is malicious code that is disguised or hidden within another program that appears to be safe (as in the myth of the Trojan horse). When the program is executed, the Trojan allows attackers to gain unauthorized access to the computer in order to steal information and cause harm. Trojans commonly spread through email attachments and Internet downloads. A common Trojan component is a "keystroke logger" which captures a user's keystrokes in an attempt to capture the user's credentials. It will then send those credentials to the attacker.

Spoofing

Spoofing is when an attacker masquerades as someone else by providing false data. Phishing has become the most common form of Web page spoofing. Another form of spoofing is URL spoofing. This happens when an attacker exploits bugs in your Web browser to display incorrect URLs in your browser location bar. Another form of spoofing is called "man-in-the-middle". This occurs when an attacker compromises the communication between you and another party on the Internet. Many firewalls can be updated or configured to significantly prevent this type of attack.

Fraud Tactics

Tactics

Spyware

Loaded on to your computer unbeknownst to you, spyware is a type of program that watches what users do and forwards information to someone else. It is most often installed when you download free software on the Internet. Unfortunately hackers discovered this to be an effective means of sending sensitive information over the Internet. Moreover, they discovered that many free applications that use spyware for marketing purposes could be found on your machine, and attackers often use this existing spyware for their malicious means.

Pop-Ups

A form of Web advertising that appears as a "pop-up" on a computer screen, pop-ups are intended to increase Web traffic or capture email addresses. However, sometimes pop-up ads are designed with malicious intent like when they appear as a request for personal information from a financial institution.

ATM Card Skimming

ATM Card Skimming is a method used by criminals to capture card data from the magnetic stripe on the back of your ATM/Check Card or Credit Card. Instances of skimming have been reported where the perpetrator has put a device over the card reader slot of an ATM or gas station pump, which reads the magnetic strip as the user unknowingly passes their card through it. More common scenarios for skimming are at restaurants or bars where the skimmer has possession of the victim's card out of their immediate view to obtain the magnetic stripe information.

PIN Capturing

PIN Capturing happens when criminals attach small cameras and other imaging devices to ATMs to fraudulently capture your PIN number as you use the keypad. Once the perpetrator has both the magnetic stripe information and the PIN, a fraudulent card is made and used to withdraw money from accounts.

RetroVirus

This virus specifically targets your computer defenses. It will look for vulnerabilities within your computer operating system or any third party security software. Most security vendors have some form of tamper-proof measure in place, so it is important to keep your patches up-to-date. Retro Viruses are usually combined with another form of attack.

Worm

A worm is similar to a virus but with an added, dangerous element. Like a virus, a worm can make copies of itself; however, a worm does not need to attach itself to other programs and it does not require a person to send it along to other computers.

Worms are powerful malware programs because they cannot only copy themselves, they can also execute and spread themselves rapidly across a network without any help.

Virus

A computer virus is a malicious program that attaches itself to and infects other software applications and files without the user's knowledge, disrupting computer operations. Viruses can carry what is known as a "payload," executable scripts designed to damage, delete or steal information from a computer.

A virus is a self-replicating program, meaning it copies itself. Typically, a virus only infects a computer and begins replicating when the user executes the program or opens an "infected" file.

Viruses spread from computer to computer only when users unknowingly share "infected" files. For example, viruses are commonly spread when users send emails with infected documents attached.