BINARY TATTOO
Define your digital identity

Glossary of Internet Fraud and Scam Terminology

Account Takeover – When a hacker or criminal has logged in to a victim's account and changed the email address or PIN, leaving the original user no way to access the account

Baiting – A type of scam that prompts the user to click on something like "You have just won! Click here to claim your prize"

Bot – A web robot, or computer program, that takes over a machine (real or virtual) when it gains access. Bots are a type of *malware*, or software used for malicious intent.

Botnet – A series of devices connected via the internet, each running one or more bots, like an army of malicious programs. Botnets can be very powerful bringing down large scale systems by attacking all at once. Often used in *DDoS* (Distributed Denial of Service) attacks on servers or systems connected on the Internet of Things.

Catfishing – The act of creating a fake account with someone else's pictures and details and then using that account to lure victims. Though sometimes 'innocently' used to meet people, Catfishers are often looking to extort something, be it data, images, or money.

Clickjacking – When a link is presented as one website but the final destination is a different web address. Ex It says "Unsubscribe" in the email but clicking the link sends your email address to another company for spamming.

DoS or DDoS – Denial of Service or Distributed Denial of Service. An attack where a system hits a website or service to the point that it can't handle all the requests and it shuts down. Distributed Denial of Service comes from multiple machines or a *botnet*.

Email Spoofing – When an email appears to be from a person you know but it is from a criminal instead. This is an easy scam on handheld devices because their email programs frequently display only the sender's name and not their email address. An email's display name is easily changed. If the emails seems suspect check the return address.

Grooming – When a criminal uses data that they have on unsuspecting victims to gain trust with them online. The data often comes from social media or public links that users are unaware of. Ex finding friends names, events attended, or personal information to open a conversation.

Hacker – A computer savvy person that knows how to break in to systems or defy rules of computer programs. The term is typically used to refer to criminals but are divided by 3 categories: Black Hats who are malicious, Grey Hats who are neither good or bad but hack because they can, and White Hats who look for breaches to help fix them.

Malware – Software installed on a computer that has malicious intent. Depending on design, malware can turn on cameras/microphones, steal data, corrupt data, or connect to other computers on a system.

Man-in-the-Middle Attack – An intercept in data from the user to the intended recipient. Frequently used in public WiFi, a Man-in-the-Middle attacker can intercept data from a user to the WiFi they are connecting to without the user even knowing.

Pharming – When a hacker is able to redirect a real web address to a fake one. This complicated scam is done by changing the files on the website host. The user types the address in properly but ends up on a duplicate site hosted by the criminal. This is extremely rare.

Phishing – A fake login screen that is a duplicate of a legitimate one. Criminals use the entered user name and password to gain access to the real site. The user commonly links to the phishing site through an email that prompts them to login in via a link.

Pretexting – A method of social engineering where the criminal lies about their role or intent to get additional information on someone. Ex "I'm calling to confirm a reservation but I seem to have lost the dates, can you please let me know what they are?"

Ransomware – A type of *malware* that locks a computer or device and then demands a paid ransom to unlock it.

Scareware – A series of warning messages that pop up on a computer that makes it appear as though the user has a virus or has downloaded *malware*. Ironically it is the act of clicking on Scareware or calling of 1-800 numbers is what gives the criminal access.

Social Engineering – Using human interaction and/or information to gain access to a system. Very effective when used in conjunction with any other scam such as *phishing*, or *grooming*. Examples are anywhere you fool someone into thinking you know more than you do, or you are someone your are not, to get them to give up extra information.

Spear Phishing – A targeted *phishing* attempt at a specific user or company. Spear phishing is the leading cause to cybersecurity breaches with human involvement.

Spyware – A type of *malware* that is designed to spy on the data or key strokes from a machine or device.

Typosquatting – When a criminal sets up a website that is similar to a legitimate site and has a slightly different web address in the hopes of catching people who make mistakes in spelling the website name. Ex. If you set up *Amazan.com* to trap people who misspell *Amazon*.

Troll – A person whose intent is to cause trouble or make people angry online. Not usually out to scam but can use some scamming techniques. All of the major networks provide easy ways to report trolls on their systems.

Whaling – A phishing attack targeted at a high profile employees like a CxO.

Questions? Comments? We'd love to hear from you: info@binarytattoo.com