We help you cut through the complexity of cybersecurity. Here’s your guide to the common lingo of cutting-edge fraud terms and tactics:

**Adware**
Software that displays advertising content on your computer and might include malicious code or a redirect to a malicious website.

**Bot or Web Bot and web crawler**
An attack on a computer or network in which bandwidth is taken away from legitimate users and denied to the point where the computer’s or network’s services are unavailable to clients.

**Credentialed Harvesting**
By setting up look-alike web sites (e.g., by taking over "creditcard.com") with a page that exactly mimics the actual portal, thieves can trick users into entering their passwords which are captured and used by the attacker.

**Denial-of-Service (DoS)**
An attack on a computer or network where the attacker attempts to flood or resources are overloaded to the point where the computer system or network’s services are unavailable to clients.

**Keylogger**
Software that monitors and captures everything a user types on a computer keyboard, used for technical support and surveillance purposes.

**Malware**
Also known as "malicious software," malware is designed to harm, attack or take uncontrolled control over a computer system. Malware includes viruses, worms, Trojan horses, some keyloggers, spyware, adware and bots.

**Phishing**
A scam that involves the use of replicas of existing web pages to trick legitimate users into entering personal, financial or password data.

**Pop-Ups**
A type of malicious software designed to block access to your computer system until a sum of money is paid. Although ransomware is usually aimed at individuals, it's only a matter of time before businesses are targeted as well.

**RetroVirus**
A type of malicious software which targets a computer system to steal data such as credit card numbers, bank account information, Social Security numbers, and other sensitive information.

**Vishing**
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 unsuspecting caller is then directed through an automated telephone system to relinquish their sensitive information.

**Worm**
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.