SCAM SPEAK

Knowledge is power. But if you don't know the rules of the game you can be taken. BIG TIME! To boost your knowledge of fraud prevention know-how, here's a guide to the latest terms in the lexicon of larceny – and the common cons behind them.

Brute force: A hacking method to find passwords or encryption keys by trying every combination of characteristics until the correct one is found.

Catfish: Someone who creates a fake online profile to intentionally deceive you.

Drive-by download: The down-loading of a virus or malware onto your computer or mobile device when you visit a compromised website - it happens without you clicking on anything at the site.

Ghosting: Theft of the identity of a deceased person to fraudulently open credit accounts, obtain loans or get utility or medical services in the person's name.

Hash busters: The random words or sentences contained in spam e-mails that allow these e-mails to bypass your spam filters.

Keylogger: A clandestine program that logs sequential strokes on your keyboard and sends them to hackers so they can figure out your log-in credentials.

Malvertising: Malicious online advertising that contains malware – software intended to damage or disable computers.

Man-in-the-middle attack: When a fraudster secretly intercepts and possible alters messages between two parties which believe they are securely communicating with each other.

Pharming: When hackers use malicious programs to route you to their websites (often convincing look-alikes of well-known sites), even if you've correctly typed in the address of the site you want to visit.

Phishing: The act of trying to trick you, often by email, into providing sensitive personal data or credit card accounts, by a scammer posing as a trusted business or other entity.

Ransomware: A malicious program that restricts or disables your computer, hijacks and encrypts files, and then demands a fee to restore your computer's functionality.

Scareware: A program that displays on-screen warnings of non-existent infections on your computer to trick you into installing malware or buying fake anti-virus protection.

Skimming: The capture of information from the magnetic stripe on your card on credit and debit cards by "skimmer" devices that are secretly installed on card-reading systems at gas pumps, ATM's and store checkout counters.

Smishing: Phishing attempts that go to your mobile devices via text message, telling you to call a toll-free number. Named for SMS (short message service) technology.

Spear-phishing: Phishing with personalized e-mail, often appearing to be from someone you know.

Spoofing: Any situation in which a scammer masquerades as a specific person, business or agency, but typically meaning the manipulation of your telephone's caller ID to display a false name or number.

Spyware: A type of malware installed on your computer or cell phone to track your actions and collect information without your knowledge.

Vishing: Short for "voice phishing," the use of recorded phone messages intended to trick you into revealing sensitive information for identity theft.

Whaling: Phishing attempt on a "big fish" target (typical corporative executives or payroll departments) by a scanner who poses as its CEO, a company attorney or a vendor to get payments or sensitive information.