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