**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.