NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

Cyber Scam Puzzle

Can you match the type of scam to its definition?

___ Spyware

___ Whaling

___ Ransomware

___ Pharming

___ Scareware

___ Spear-phishing

___ Drive-by download

___ Spoofing

___ Brute-force attack

___ Man-in-the-middle attack

___ Smishing

___ Hashbusters

___ Vishing

___ Ghosting

___ Phishing

___ Catfish

___ Skimming

___ Keylogger

___ Malvertising

a	A hacking method to find passwords or encryption keys by trying every possible combination of characters until the correct one is found.
b	Someone who creates a fake online profile to intentionally deceive you.
c	The downloading 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.
d	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.
e	The random words or sentences contained in spam emails that allow these emails to bypass your spam filters.
f	A clandestine program that logs sequential strokes on your keyboard and sends them to hackers so they can figure out your log-in credentials.
g	Malicious online advertising that contains malware - software intended to damage or disable computers.
h	When a fraudster secretly intercepts and possibly alters messages between two parties who believe they are securely communicating with each other.
i	When hackers use malicious programs to route you to their own 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.
j	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.
k	A malicious program that restricts or disables your computer, hijacks and encrypts files, and then demands a fee to restore your computer's functionality.
l	A program that displays on-screen warnings of nonexistent infections on your computer to trick you into installing malware or buying fake antivirus protection.
m	The capture of information from the magnetic stripe on credit and debit cards by "skimmer" devices that are secretly installed on card-reading systems at gas pumps, ATMs and store checkout counters.
n	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.
o	Phishing with personalized email, often appearing to be from someone you know.
p	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.
q	A type of malware installed on your computer or cell phone to track your actions and collect information without your knowledge.
r	Short for "voice phishing," the use of recorded phone messages intended to trick you into revealing sensitive information for identity theft.
s	Phishing attempt on a "big fish" target (typically corporate executives or payroll departments) by a scammer who poses as its CEO, a company attorney or a vendor to get payments or sensitive information.

Adapted from *Scam-Proof Your Life* by Sid Kirchheimer