The Wall Street Journal **December 8, 2021**

"Journal Report: CYBERSECURITY"

****

"Do You Speak Cybersecurity?"

The industry has its own language. Time for a quiz! **by Cheryl Winokur Munk**

We all know cybersecurity is a people issue, but time and time again, cyber experts trying to raise awareness among employees and senior executives use terms like "zero-day exploit" that no one outside of cybersecurity really understands. The industry has its own language, and it can be difficult for laypeople to understand.

Here's a quiz to test yourself on some commonly used cybersecurity terms.

1. Attack Surface

A. A "WarGames" style monitor at a cybercriminal command center where hackers can watch attacks in real time.

B. The moment when a large-scale hack or virus becomes apparent.

C. The sum of the different points bad actors can use to enter your systems.

D. A decoy hackers use to make targets think they have stopped a continuing attack.

2. Backdoor

A. The USB port on your computer that is vulnerable to malicious software.

B. A secret entry point established to circumvent normal security measures for access to software or a computer system.

C. A food-delivery service favored by hackers.

D. A place on the back of prototype computers that can be used for biometric breath exhalation logins, or BELs.

3. Bug Bounty

A. A type of software that can soak up a lot of bugs, quickly.

B. A system that is overrun by malicious software.

C. Reward proffered by some organizations and developers to individuals who report a vulnerability or bug.

D. The amount of money hackers can make from placing a bug in a computer.

4. Catfishing

A. When hackers bottom-feed, targeting the smallest, most-vulnerable companies.

B. When cybercriminals remotely reverse the polarity on a target company's server.

C. When companies turn the tables on hackers, catching them in the act.

D. When a bad actor creates an online fictional persona for deceptive purposes.

5. Clickjacking

A. An attack that fools victims into clicking on a link that seems to take them to one place but instead routes them to an attacker's site.

B. The selling of corrupted AC power cords designed to steal your laptop information.

C. When people repeatedly click on a link, inadvertently creating an opening for hackers.

D. A type of login that requires a special hand-held clicker.

6. Key Logger

A. A unique alphanumeric code that verifies authorized software access.

B. Software that records users' keystrokes to collect passwords and other high-value information.

C. Slang for beer that coders drink at all-night coding sessions.

D. The grunt at software companies who has to do the most boring coding.

7. Multifactor Authentication (MFA) or Two-Factor Authentication (2FA)

A. A method of password storage where users are required to keep sensitive information in two or more hard-to-remember places.

B. A password-management system that more than two people have to agree on in order for it to be valid.

C. A security approach that asks users to give at least two credentials, such as a password and biometric, to access an organization's data or systems.

D. All of the above

8. Penetration Testing

A. Also known as pen-testing, it's an attempt to evaluate how hack-proof a system is by trying to exploit it.

B. What hackers who want legitimate jobs have to go through before being hired by software companies.

C. A hacker game to see how many random businesses they can infiltrate in a set amount of time, usually 12 hours.

D. A videogame version of Dante's "Inferno" where players have to hack their way through the concentric circles of hell.

9. Phishing

A. An email from your company that provides login information.

B. The music hackers play when launching an attack on a big target.

C. A slang term for annoying marketing calls, based on a mashup of "phone" plus "fishing."

D. When attackers send emails that purport to be from reputable parties to induce recipients to reveal personal information.

10. Ransomware

A. A pejorative term for overpriced software.

B. The digital currency hackers use to buy and sell malicious software.

C. A type of malicious software attack that blocks access to a computer system until the victim pays a sum of money to unlock it.

D. Clothes that hackers use so they can identify each other at parties.

11. Social Engineering

A. The practice of personalizing your home-screen image.

B. A cyberattack aimed at stealing user data where the attacker pretends to be a trusted individual or organization to trick the victim. Common techniques include phishing and smishing.

C. The art of teaching employees how to avoid becoming victims of cyberattacks.

D. The term used by psychologists to help introverted techies get more engaged in real-life relationships.

12. Sockpuppet

A. A fictitious online identity used for deceptive purposes.

B. An insulated cover for small smartphones.

C. A low-level employee in a ransomware gang.

D. How cybercriminals refer to company employees who fall for the simplest scams.

13. Smishing

A. Fraudulent software that combines the photos from one person's phone with another's.

B. When cybercriminals attempt to gather personal information by sending fraudulent messages via text messages, or SMS.

C. Term for fending off an attempted cyberattack, derived from the Old Norse term for "destroy."

D. Slang for what two hackers do when they're in love.

14. Zero-Day Exploit

A. The deadline of Jan. 1, 2030, for updating smartphones, or otherwise their data could be wiped out.

B. The name of a videogame whose goal is to break into the secret accounts of an offshore bank.

C. When hackers infiltrate a software company, and place a bug into the software so it's vulnerable as soon as it goes online.

D. A software vulnerability that's either previously unknown or has no developed patch, leaving hackers free to do damage.

15. Zero Trust

A. The name of a cryptocurrency bank that was the first to also provide passbook savings accounts.

B. A password-protection system that requires four-factor authentication every time you log in.

C. Concept that says devices shouldn't be automatically trusted, even if they have been verified previously.

D. A play on the movie "Zero Thrust," about a failed rocket project, it refers to a cybersecurity system that gets hacked before it's even put on the market.

Ms. Winokur Munk is a reporter in West Orange, N.J. She can be reached at reports@wsj.com.

ILLUSTRATION BY GIACOMO BAGNARA

Answers: 1. C; **2.** B; **3.** C; **4.** D; **5.** A; **6.** B; **7.** C; **8.** A; **9.** D; **10.** C; **11.** B; **12.** A; **13.** B; **14.** D; **15.** C