**Computer Fraud and Abuse Challenge Key – Game 2**



**Left column**

**W.C. Crimes**

* Top Question - Inflating advertising revenues by hiring individuals to repeatedly open the advertisements of the Web site’s online advertisers.

**Correct Answer : AGREE** *–* ***Click fraud***

* Middle Question – Intentionally posting false information on a Web site about a political candidate, would be an example of this type of abuse?

***Answer Given : Slandering Correct Answer: DISAGREE – Internet Misinformation***

*While slandering is the spreading of false information about someone. The computer abuse term used is internet misinformation.*

* Bottom Question - Wearing a digital audio player, this employee appeared to be listening to music, while in reality the device was being used to download unauthorized company data. Which cyber crime was this employing perpetrating?

***Answer Given: Walking Correct Answer: DISAGREE –Podslurping***

*Walking term is fictitious.*

**Samuel Sharkie**

* Top Question – Fraudsters bought a significant number of shares of penny stock and used the Internet to spread overly optimistic, false information about the company to create a buying frenzy to drive up the stock price. The fraudsters then sold their stock at a profit.

***Answer: AGREE – Internet Pump and Dump***

Middle Question – Sam, what is the name given to a computer fraud where products are offered for sale by someone pretending to run a legitimate E-business, and customer information is collected with no intent to deliver the product?

***Answer: AGREE - Posing***

* Bottom Question – A spammer doing this sends out millions of e-mails to randomly generated addresses using combinations of letters added to known domain names in the hopes of reaching a percentage of actual email accounts.

***Given Response: War Dialing Correct Answer: DISAGREE – Dictionary Attack***

*War dialing is dialing phone lines to find idle modems to access a system, capture the attached computer, and gain access to the network.*

**Bootleg Buccaneer**

* Top Question – Fraudsters tampered with Aldi’s debit card readers by planting a small device that recorded transaction data in order to steal confidential information. Bootleg, what type of fraud was perpetrated?

***Answer: AGREE – Chipping***

* Middle Question - A computer engineer watched the keystrokes entered by a system administrator log onto the company ERP. The programmer later logged into the company’s HR system to see the salaries of his colleagues. What is the engineer guilty of doing?

***Answer: AGREE – Shoulder surfing***

* Bottom Question - Bootleg, what is another term for Web-page spoofing?

***Given Response: Trawling . Correct Answer: DISAGREE – Phishing***

Trawling is a fictitious term in terms of computer fraud.

**Center Column**

**Cookie Booker**

* Top Question – Napster, a peer-to-peer file sharing service was found guilty of this cyber fraud.

***Answer: AGREE – Software Piracy***

* Middle Question - In 2007, three individuals hacked into the cash registers of a New York restaurant chain. They installed this type of software that located readable “Track 2” data from credit and debit cards as it was sent over the company’s network to headquarters for processing.

***Given Response: Rootkit Correct Answer: DISAGREE – Packet Sniffer, Man-In-the-Middle, probably okay too.***

*Notes****:*** *A rootkit conceals process, files, network connections, and system data from the operating system and other programs. A packet sniffer inspects information packets as they travel through networks. Track 2 data is the name for the magnetic strip on a debit or credit card that contains, PIN numbers, security codes as well as the card number. The solution to this threat is to have data encrypted at the point of swipe. In this fraud 5,000 cards were stolen and financial institutions lost $600,000.*

* Bottom Question – In 2010, U.S. citizens received fraudulent electronic messages from an organization that purported to be the IRS. The message indicated the recipients’ EFT tax payment was not received and asked then to send confidential information.

***Answer: AGREE – Email Spoofing***

August, 10, 2010, IRS, *Current Scams and Phishing sites posing at the IRS.* Retrieved from: http://www.irs.gov/privacy/article/0,,id=226755,00.html

******

**Debit Deville**

* Left Question – In order to secretly communicate with each other, terrorists hid secret code in seemingly legitimate online job advertisements.

***Given Response: Crypto-ads Correct Answer: DISAGREE – Steganography***

*Crypto-Ads is a fictitious term.*

* Middle Question – Citi Bank was a victim of this computer fraud. Using Javascript, customers’ Citi Bank browser tabs were changed. When customers clicked on the tab to log back into their Citi Bank account, they were providing confidential information to the perpetrators.

***Given Response: Superzapping. Correct Answer: DISAGREE – Tabnapping***

*Superzapping is bypassing system controls to perform illegal acts.*

* Right Question - A nonprofit executive changed the salary figures listed on the entity’s Form 990 just prior to transmitting it electronically to the IRS. The executive wanted to avoid incurring excessive compensation penalties.

***Answer: AGREE – Data Diddling***

**Identity Theftly**

Top Question – This computer fraud involves making purchases for immaterial amounts on stolen credit cards in order to determine which stolen cards can still be used to make purchases. Accounts still good are sold to others.

***Given Response: Pharming. Correct Answer: DISAGREE – Carding***

*Pharming involves redirecting Web site traffic to a spoofed Web site.*

* Middle Question – A waiter double swiped customers’ credit cards using the restaurant’s card reader and another reader personally owned. The victims’ stolen credit cards were used to then purchase merchandise.

***Answer: AGREE - Skimming***

* Bottom Question - When someone uses a neighbor’s unsecure WiFi network without permission, in order to gain free access to the Internet, what is occurring?

***Answer: AGREE - Piggybacking***

**Right Column**

**Phonie Business**

* Top Question - Phonie, Oprah Winfrey and George Bush are two of these?

***Given Response: Enigmas. Correct Answer: DISAGREE: Viruses***

*The Oprah Winfrey virus caused the size of a hard drive to shrink to 80 MG and then expand again. The George Bush virus fills all available free space with bogus files.*

* Middle Question - What are techniques used to trick people into disclosing confidential information called?

***Answer: AGREE – Social Engineering***

* Bottom Question – On March 29, 2010, ABC News reported that several Massachusetts teenagers were criminally charged for sending text messages and using Facebook to persistently taunt a 15 year old classmate who committed suicide. What is this activity called?

***Answer: AGREE – Cyber-bullying***

**Sneaks Ratter**

* Top Question - According to a SEC complaint filed in San Francisco, Igors Nagaicevs broke into online brokerage accounts at large U.S. broker-dealers. He manipulated stock prices by making unauthorized trades in the customers’ accounts. What is gaining control of the customer accounts called? (Incident reported January of 2012).

***Answer: AGREE - Hijacking***

Middle Question - A modified payroll program increased the federal withholding amounts by a few cents per pay period for hundreds of employees. The excess payments were credited to the perpetrator's withholding account, which, at income-tax time the following year, yielded large refunds from the IRS. (*Network World Security Newsletter*, July 24, 2002.)

***Answer: AGREE – Salami Technique***

* Bottom Question - William T. Frelix and 11others were indicted for using hotel customers’ identities and credit cards to purchase $100,000 in goods and services. The perpetrators obtained the confidential information by fishing through hotel trash bins. (June 15, 2010, *The City Paper*, Nashville, TN. Online article by James Nix, “Dumpster diving suspects in airport hotel fraud ring headed to court” <http://nashvillecitypaper.com/content/city-news/dumpster-diving-suspects-airport-hotel-fraud-ring-headed-court>

***Given Response: Foraging Correct Answer: DISAGREE – Dumpster Diving or Scavenging***

**The Masked Hacker**

* Top Question - What are fraud perpetrators doing when, through repeated attempts to logon, they guess the access codes of a legitimate users?

***Answer: AGREE – Password Cracking***

Middle Question - BackOrifice, Netbus, and SubSeven are examples of what type of malware?

***Given Response: Worms. Correct Answer: DISAGREE – Trap or Back Door***

*Worms are self-replicating programs that harm networks and require no human intervention to activate. A trap door is a way into a system that bypasses normal authentication controls. Sometimes they are intentionally created by programmers in case of a system failure.*

* Bottom Question – In 2008, the Facebook Jobs web page was subjected to this type of attack when code inserted to the web page created a phony login screen tricking users into handing over their credentials.

***Given Response: HTML spoofing Correct Answer: DISAGREE – Cross-Site Scripting***

*HTML spoofing is a fictitious phrase*

**Changing the position of the Questions**

***I***nstructors can change the location of the questions per celebrity by changing the order of the question marks in each cell on Game Board (Slide 8). The question marks are underneath the X and O shapes. Move them off of a cell, reposition the question marks, then reposition the X and O shapes on top of the celebrity’s image. The feedback slides will remain attached to the questions so that the integrity of the game remains intact.