**Chapter 3: “That Is Not an Option Unless It’s in a Body Bag”**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

Presented to Dr. Renita Murimi

1. What technologies have we been slow to adopt or not adopted in the US, but are popular around the world?

One of the technologies that we have been slow to adopt is new payment technologies. U.S. consumers are hesitant to break away from their traditional card and cash ways due to safety reasons. Additionally, the U.S. does not see enough benefits in new payment technologies. Updating payment systems is expensive and with few customers taking advantage of “tap and go” and other recently developed technologies. However, in countries such as Australia and China, established infrastructure and a fully developed system allows the market for contactless payments. More than 82% of Australians use tap and go payment every week. In contrast, in China, mobile payments totaled up to more than $5.5 trillion (“Why is the US Slow to Adopt New Payment Technologies?”, n.d.).

1. Outline a strategy for effective social media usage.

A strategy for effective social media usage includes choosing the right social media medium, identifying your audience, selecting and sharing an intended content effectively, and engaging the audience in discussions, tracking results, analyzing the collected data, and making tweaks to optimize the social media usage for the intended purpose.

1. What is the primary motivation for social media?

The primary motivations for social media include information seeking and exchange. Other motives can also be for entertainment, personal utility, and convenience. These motivations are related to the user’s behavior, sense of belongingness to a group, and the level of satisfaction that one gets from it.

1. How can you engage someone specific in social media conversations?

To engage someone specific in social media conversations, one must choose a subject that they know the other person is interested in and ask them questions to let them talk about themselves. It is also essential to carefully investigate what they’re saying and support their opinions, which will engage them to talk more. Additionally, using the RPM interrogation techniques, supporting them one day, and criticizing them the other day is critical to keep them engaged.

1. Is our social media behavior an extension of our personalities? What challenges does it pose to cybersecurity?

Our social media behavior may be an extension of our personalities. That is, people with pre-existing social structure and socially adaptive characters will use social media for more communication than those who are less socially adept. On the other hand, individuals who struggle to make social connections physically might use social media to develop a social relationship.

Unfortunately, online social media personality can also diverge from offline personality as it gives individuals a means to physically hide while being courageous to communicate things that they wouldn’t normally do in person.

1. Explain the use of CRIME and RPM in cybersecurity.

CRIME can be used in cybersecurity to detect and identify malicious individuals with evil intent, such as disgruntled employees who are compromised and seeking revenge using their ideology and money-oriented goals to satisfy their ego.

On the other hand, RPM can be used in cybersecurity to investigate what happened during a cyber-attack, identify individuals responsible for the crime, and use rationalization, projection, and minimization of their actions to keep them engaged and gather more information for investigation or even make a decision.

1. How can you censor social media usage? Internet usage?

Social media and internet usage can be censored using techniques such as IP address blocking, URL blocking via a proxy, and DNS tampering. These mechanisms allow one to block access to specific sites, domains, or IP addresses, preventing users from accessing the information on the internet or social media sites.

1. What is the difference between white hat hackers and black hat hackers?

The difference between white hat hackers and black hat hackers is their intension towards computer systems. That is, black hat hackers are criminals that use their computer skills to harm or damage computer systems. On the other hand, white hat hackers are ethical hackers that have approval from the system’s owner to use their computer skills to identify weaknesses in systems. They provide their findings, suggest ways to resolve security issues and address mitigation strategies.

References

Why is the U.S. Slow to Adopt New Payment Technologies? Retrieved February 10, 2020, from https://independentretailer.com/2018/03/20/why-is-the-us-slow-to-adopt-new-payment-technologies/