M2.2.5 - quiz - Watering Hole Attacks and Typo squatting Quiz

Amanda Success (Period 9) (replace with your information)
Monday December 25, 2023
Seat 99 (Grade level 13)
Cyber Capstone

0. What is the key difference between misinformation and disinformation in the context of cybersecurity?
A. Misinformation is unintentional, while disinformation is intentional.
B. Misinformation involves spreading false information with the intent to deceive, while disinformation involves spreading false information without the intent to deceive.
C. Misinformation is spread through email, while disinformation is spread through social media.
D. Misinformation is often exaggerated, while disinformation is factual.
___ <- Type answer here

1. What is a key characteristic of watering hole attacks?
A. They rely on exploiting vulnerabilities in computer systems.
B. They involve directly targeting specific individuals or organizations.
C. They leverage common websites or resources frequented by the intended victims.
D. They require social engineering techniques to spread malware.
___ <- Type answer here

2. How do watering hole attacks take advantage of human behavior?
A. By exploiting vulnerabilities in browser software.
B. By relying on users' habitual visits to specific websites.
C. By tricking users into downloading malicious files.
D. By manipulating users into providing sensitive information.
___ <- Type answer here

3. What is typo squatting, also known as URL hijacking?
A. Hiding a button or link on top of another image.
B. Creating a fake company website with malicious scripts.
C. Slightly changing the URL of a website to resemble a well-known site.
D. Stealing cookies to authenticate users on a website.
___ <- Type answer here

4. How can users defend against watering hole attacks?
A. By installing anti-virus and anti-malware programs.
B. By avoiding common websites frequented by many users.

C. By relying on browser extensions to detect malicious URLs.
D. By being proactive and diligent in updating software and detecting unusual activities.
___ <- Type answer here

5. What is clickjacking in the context of client hijacking attacks?
A. Stealing cookies used to authenticate users.
B. Manipulating users into clicking on hidden buttons or links.
C. Using typosquatting to redirect users to malicious sites.
D. Exploiting vulnerabilities in browser software.
___ <- Type answer here

6. How does session hijacking occur in client hijacking attacks?
A. By stealing cookies to authenticate users on a website.
B. By slightly altering the URL of a legitimate website.
C. By exploiting vulnerabilities in browser software.
___ <- Type answer here

D. By hiding malicious scripts on common websites.