Web Security III

Question 1 ***Web Security Wrap-Up: UI-Based Attacks and Privacy*** ()

(a) **Phishing**

A phishing attacker tries to gain sensitive user information by tricking users into going to a fake version of a website they trust. The attacker might convince the user to go to what *appears* to be their bank and to enter their username and password.

i. What are some ways that attackers try to fool users about the site they are going to? How do they convince people to click on links to sites?

ii. What are some defenses you should employ against phishing?

(b) **Web Tracking**

What kind of information do sites gain about you when you visit them? How could a business learn about many of the sites you visit and construct a detailed profile of you based on your web habits?

Question 2 ***Clickjacking*** ()

In this question we'll investigate some of the click-jacking methods that have been used to target smartphone users.

(a) In many smartphone browsers, the address bar containing the page's URL can be hidden when the user scrolls. What types of problems can this cause?

(b) Smartphone users are used to notifications popping up over their browsers as texts and calls arrive. How can attackers use this to their advantage?

(c) QR codes haven't taken off and become ubiquitous like some thought they would. Can you think of any security reasons why this might be the case?