Paul Parker

CS373

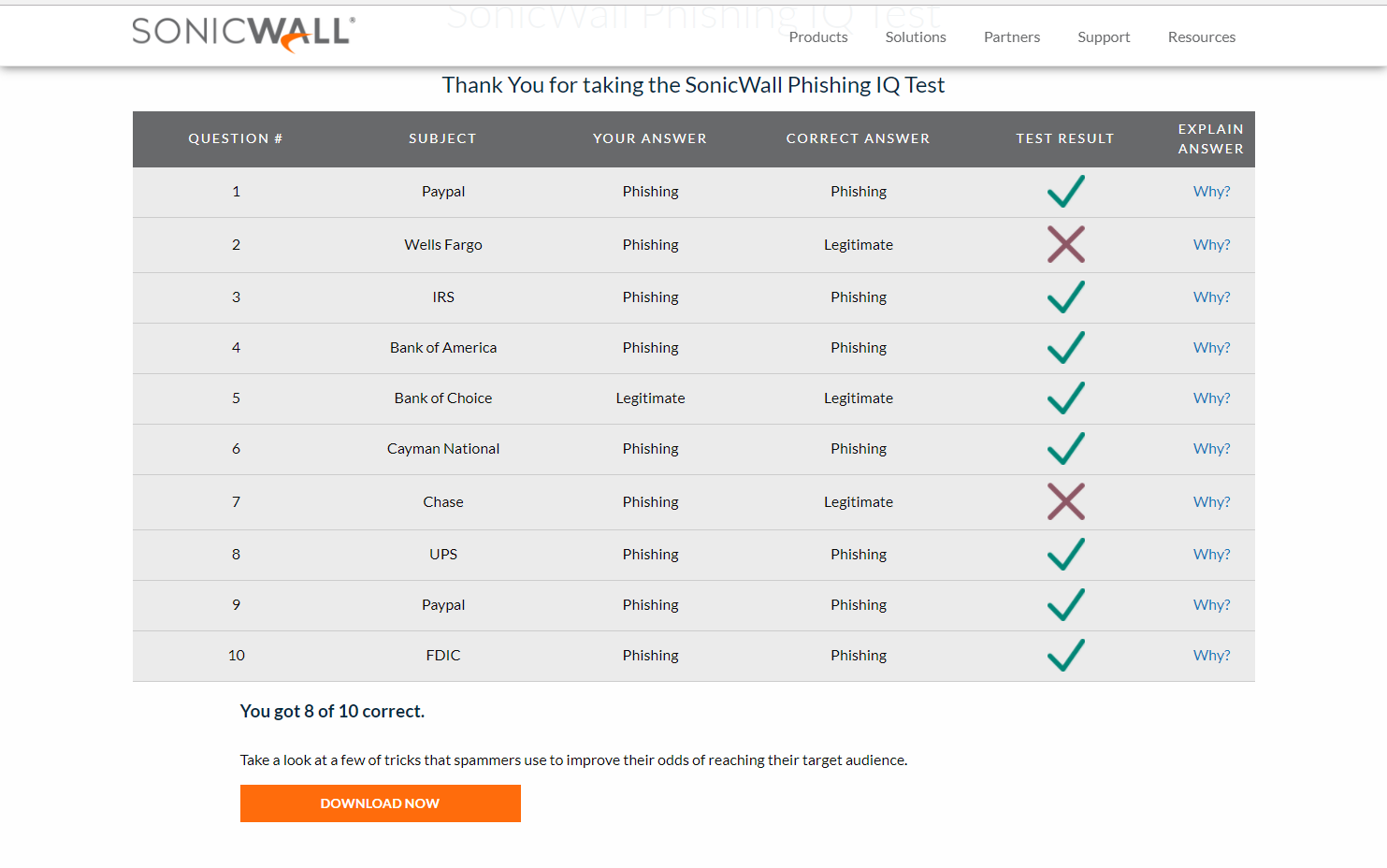
Unit 1 Homework

1. Case Project 1-4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Layering | Limiting | Diversity | Obscurity | Simplicity |
| Home Windows PC | Locked in my house, then my room, then password protected | Kept at my house behind locked doors, only myself, my parents, and my housekeeper could get access and only I have the password |  | Password is random numbers and letters |  |
| Work MacBook |  |  |  | Password is random numbers and letters |  |
| Android Smartphone |  | Kept on my person and only I use it |  |  | Only needs a fingerprint scan to access |

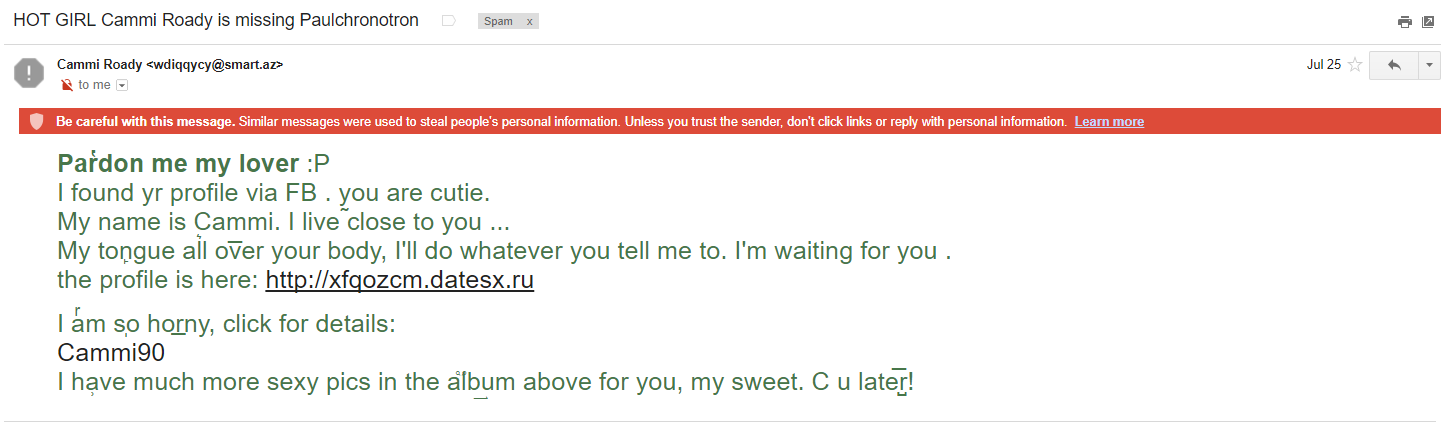
Based on this observation my computers aren’t that secure. I am missing a lot in the layering and diversity department. I could improve this by utilizing some more layering and diversity. For example, I can use the touch id feature of my MacBook so that it requires and fingerprint and a password. I can do something similar with my android at the sacrifice of simplicity by requiring a pin and a fingerprint to unlock. Biometrics is a pretty nice way to increase layers and diversity. I could try to locate a similar biometric product for windows. I do have good obscurity by trying to use passwords that are just random letters and numbers. It hurts my simplicity a bit because it makes them harder to remember, but also harder for an attacker to guess.

2. Phishing IQ Test



I think this test can be pretty useful if you know how to apply the results. I tended to err on the side of not trusting any e-mails with links in them, however, some legitimate e-mails included links. I’d rather navigate to the website by typing the url to what I know is the legitimate site rather than trust a hyperlink in an e-mail. It’s pretty good that have pretty detailed information about why or why not an e-mail is legitimate.

3. Recent spam e-mail



Gmail detected this as spam and also very helpfully included the warning that a similar message was used to steal people’s information. It is pretty obvious spam, but it looks like it’s trying to get around a filter by using weird characters, perhaps in an attempt to not match similarly worded messages that would end up in a basic text filter.

4. Gmail account:

Completely on me for waiting until the last minute. At the very least here is a screenshot of where it was sent to:

