# IT666 – Social Engineering Lab

Ryan J. Skelly 3/9/2021

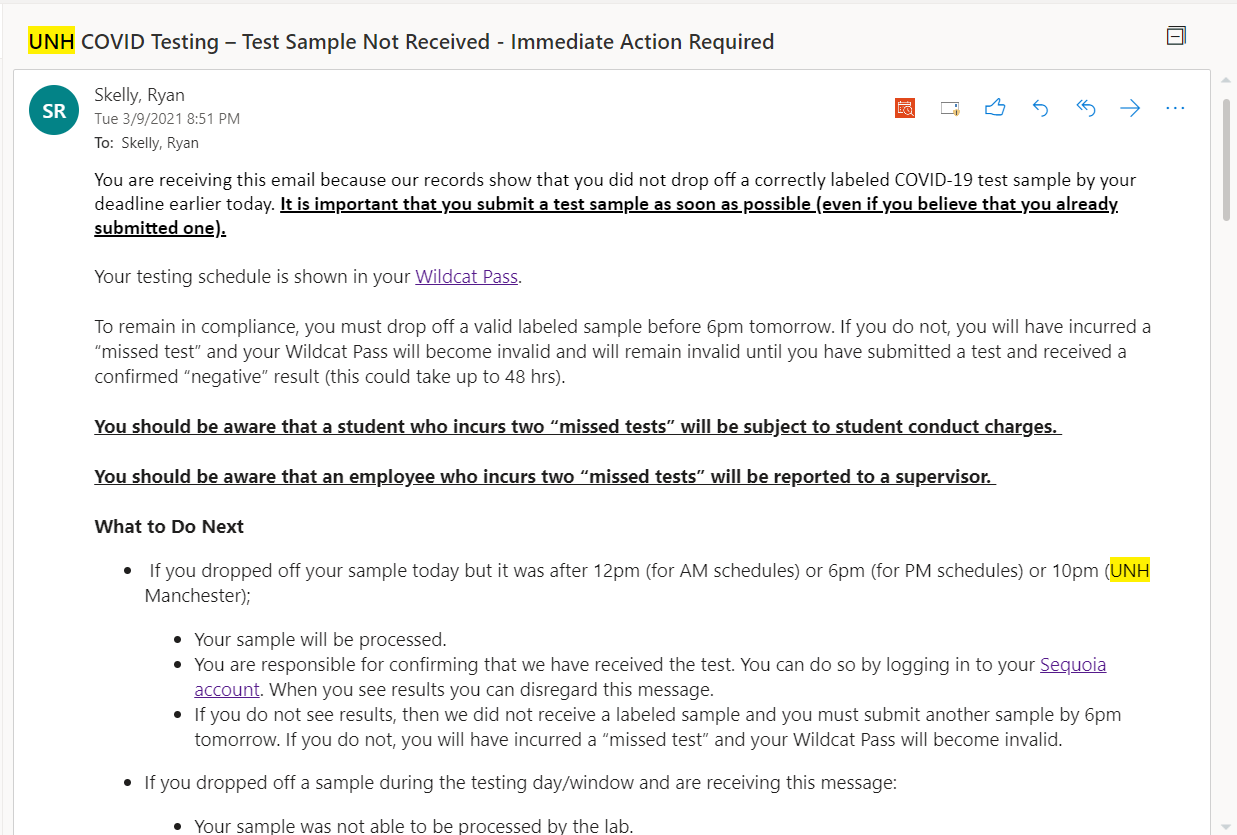
Rjs1070@wildcats.unh.edu

**Lab report:**

Task 1: (5 points for each scenario above) 1) Determine the type of social approach that was used. 2) Describe one action the target might have taken to determine it was a social engineering attack.

1. Pretexting, the target could have asked the hacker more identifiable information, or the target could badger their HR dept. IT to set up a more secure password reset system, like sending password info to the email of the user, and them from there being able to initiate a password reset.
2. Blasting, the target could set up a spam email catch or a filter that would restrict emails only coming from known addresses.
3. Baiting, the targets could have brought the usb device to the lost and found instead of plugging it in, if they were scattered around the parking lot enough, the organization may be able to smell that somethings phishy and let the rest of the employees know that there are trojan infected usbs being distributed and to beware
4. Quid Pro Quo, the target could have installed anti-virus/malware software, or done more investigation into the fraudsters IT assistance services(and how legitimate they really are)

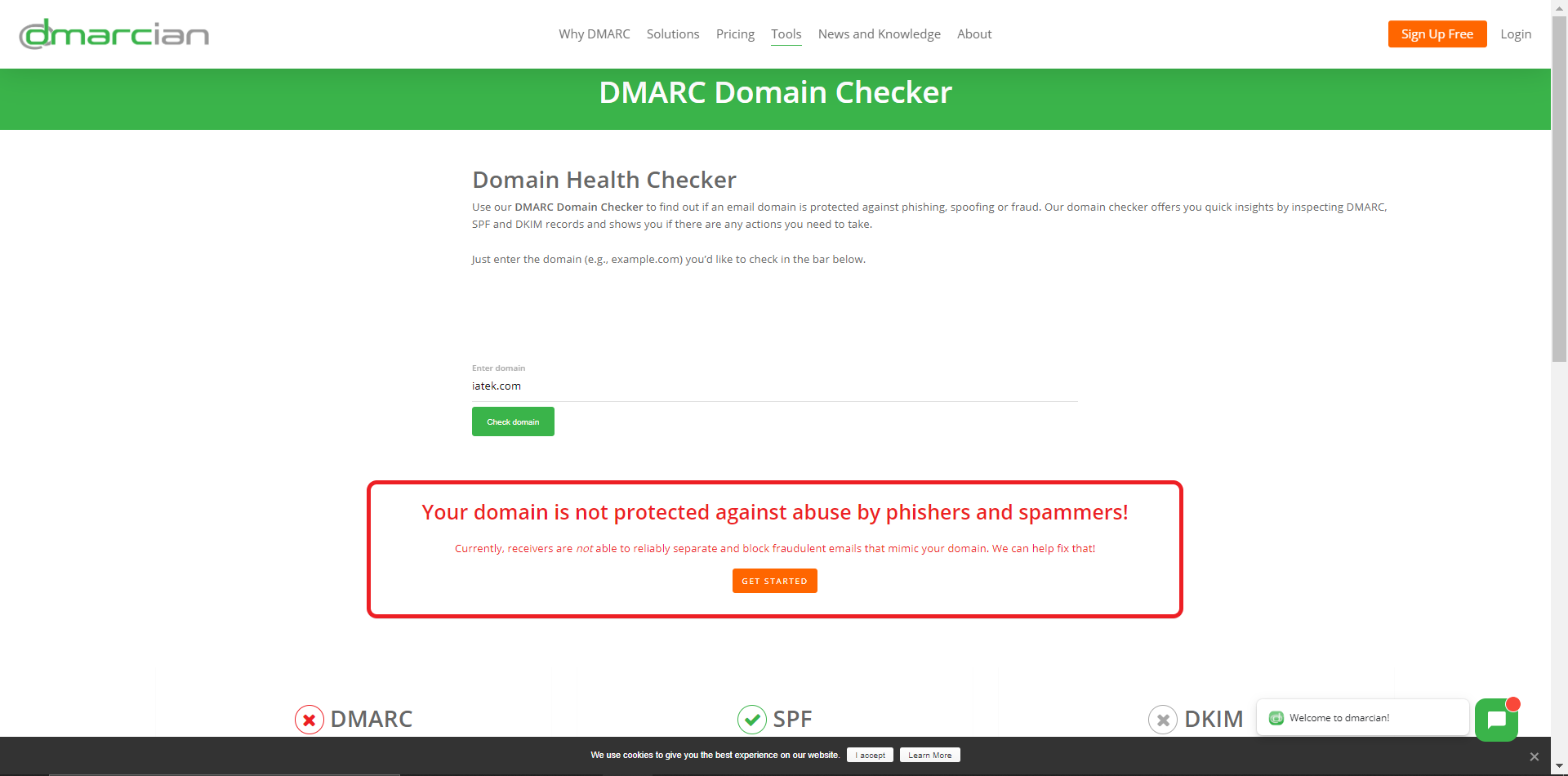
Task 2.1: (10 points) Take a screenshot of the phished email in your email reader.



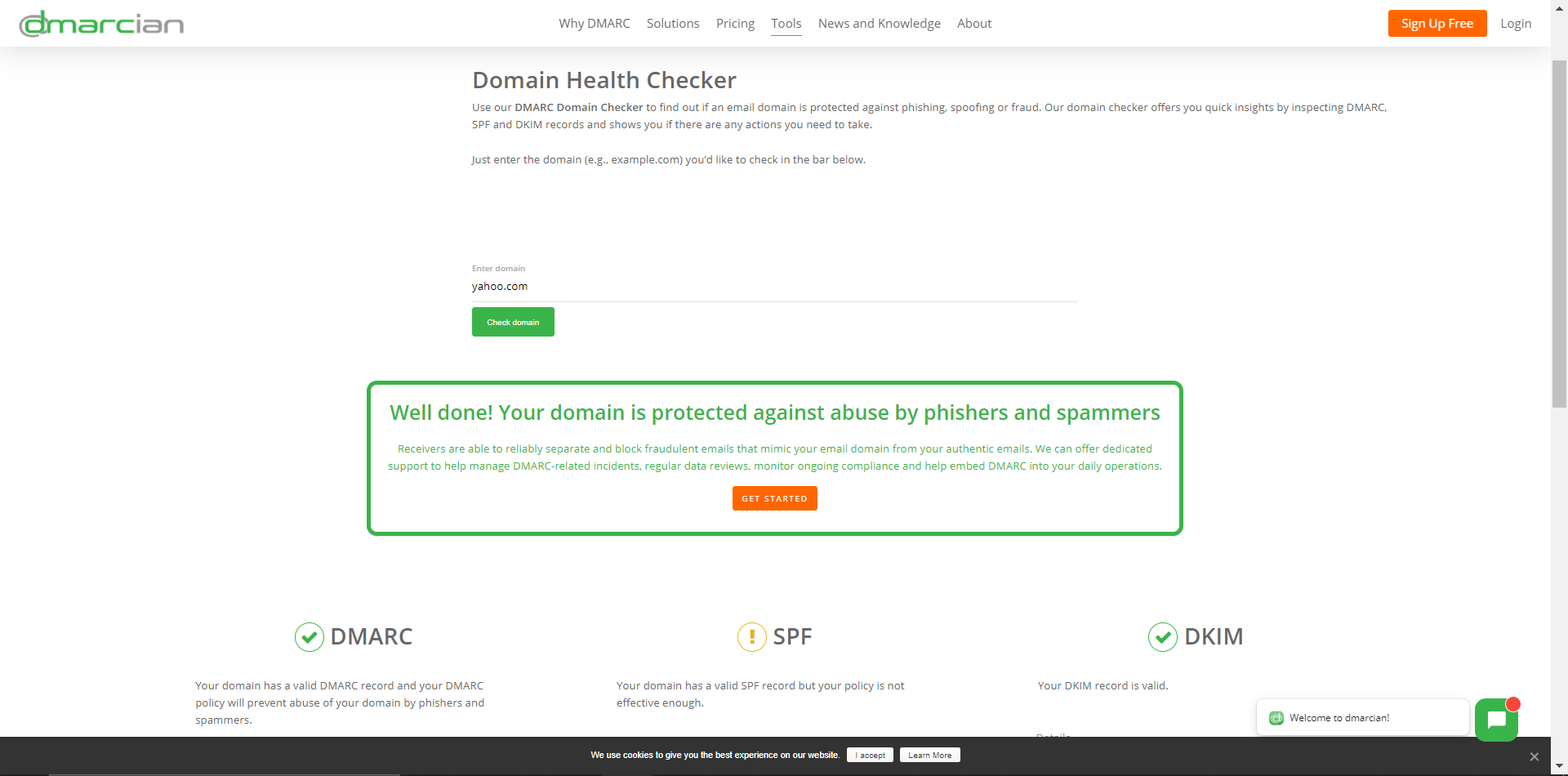
Task 2.2: (10 points) Describe what happens when the user is “hooked” in your phishing email

I spoofed a test sample not received phishing email designed to bait the users into clicking any of the links on the message. I rerouted all of the hyperlinks(including “mailto:” addresses) to take the target to rick astley’s never gonna give you up, however the where the link leads doesn’t matter because it could be something more malicious.

Task 3.1: (10 points) Find a domain that IS NOT protected against abuse. Provide a screenshot of the results.



Task 3.2: (10 points) Find a domain that IS protected against abuse. Provide a screenshot of the results.



Task 4: (20 points) List 4 new facts about your target

1. Twitter : @graf\_comp\_sec, could send Direct message bots to spam links, hoping you click on one
2. CTO of <http://securityxing.com/>, could create a fake email saying that I was able to achieve XSS attack on the website, and that I can setup the infrastructure to make sure it doesn’t happen again, and make a malicious link that would lead to the proof(image) of the actual vulnerability, but actually leads to a bogus link for clickbaiting
3. DOB: 9/3/1957, could send a birthday email with a “click to apply discount code” link
4. Suspected dwelling: 3 Sonia Dr, Dover, could mail an Attack usb to the address, or to use the last fact too, a birthday card with a free “unformatted” 1TB flash drive as a gift.

Task 5: (20 points) Bcc yourself and provide a screen capture of the email.

