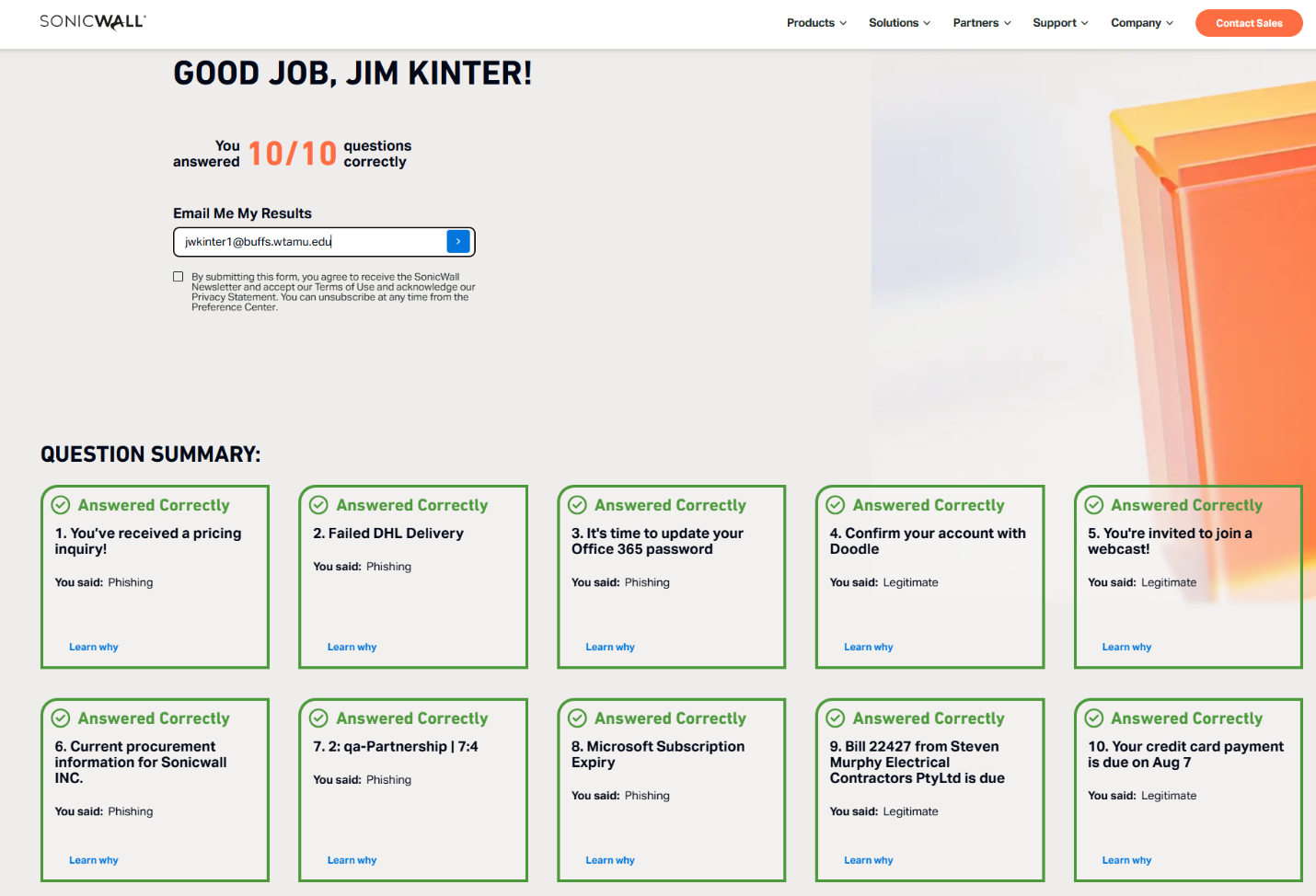
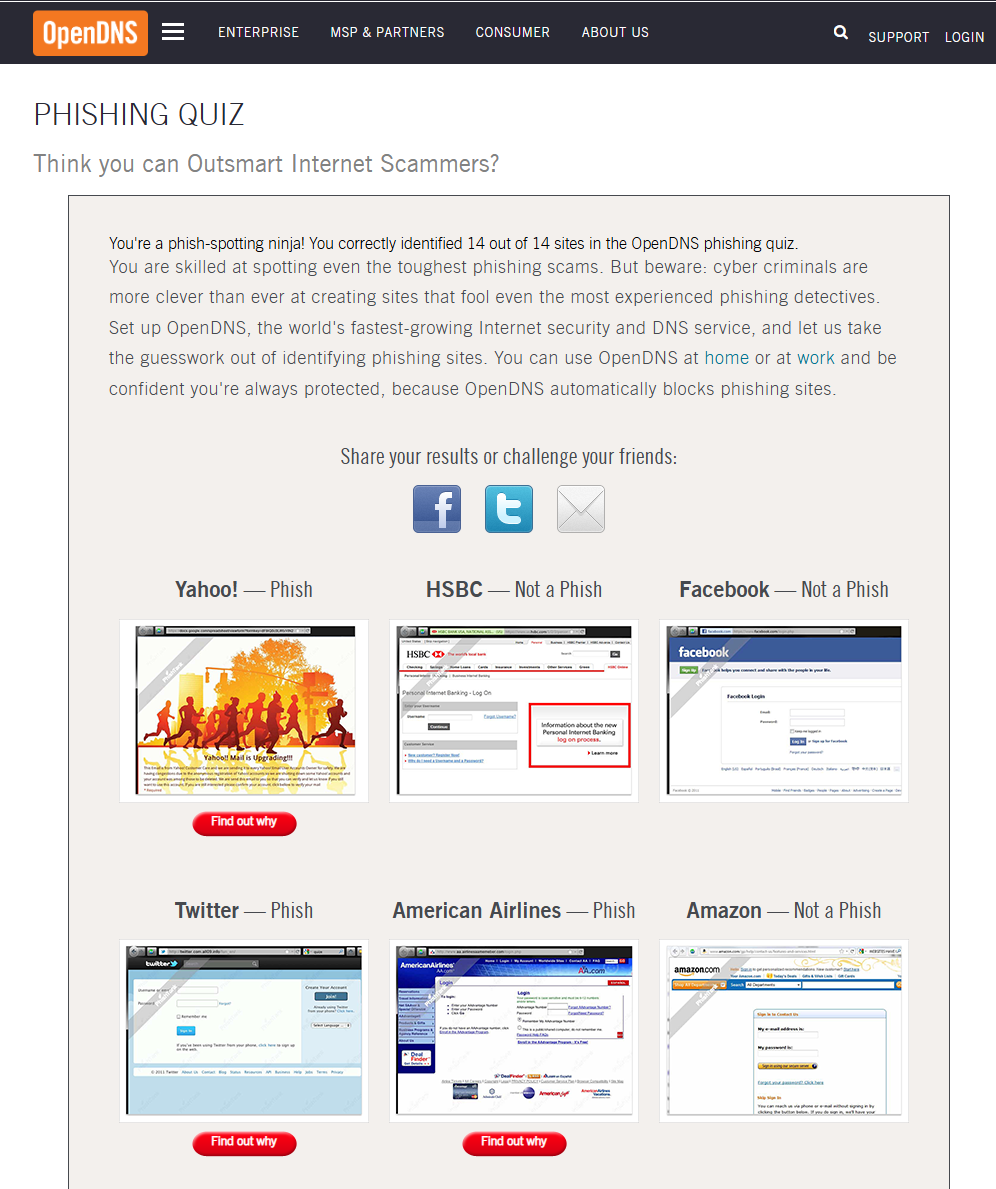
Wireless Survey/Phishing Assignment Assignment

Jim Kinter

CIDM6340

1. What did you do – I started the assignment by opening my laptop and then jumping into my truck. I then drove around my neighborhood. I live in a small neighborhood comprised of 30 homes, each sitting on lot sizes between 5 and 10 acres, most on the higher end of that range. My home sits on a 5.25-acre lot. As part of this exercise, I tested to see whether my home WiFi was being broadcast by any of the three Wireless Access Points or the Point-to-Point network link between my garage and my house. As the second part of this assignment, I opened a browser and followed the link to the Sonicwall Phishing Test and captured the results. I then used the second link in the assignment to take the OpenDNS Phishing Quiz.
2. What are the results – As I drove around the neighborhood, I was able to pick up moderate to weak signals from almost every house (22/30) in the neighborhood. Of the 23 properties where I was able to identify a Wi-Fi network, four of them offered unauthenticated access and 8 of them used an SSID that allowed me to know which house they were associated with. The WiFi radio on my laptop uses the IEEE 802.11 technologies to search for wireless networks within the 2.4GHz or 5GHz frequency bands. The IEEE 802.11 protocol defines standards for wireless local area networks to allow for passive or active scanning. Active scanning identifies available networks by collecting their SSID (network name/identifier) and security settings (like WPA2 or WEP). The scan I ran identified 4 networks in my neighborhood that were configured as Open, or not requiring authentication. To preserve the relationships with my neighbors I didn’t probe any further. Another bad practice that I observed was that the homeowners identified their network by assigning an SSID that allowed me to associate the network with a particular property (either because I know the homeowner’s name or they used their property address). I similarly chose not to investigate these networks any further. I returned to my home where, after I “forgot” my home network, I was unable to identify any available networks on my property. I expect that this is because, during a previous class that I took from you, I undertook a holistic security review of my home, and all attached devices and during that process, I configured all Wireless Access Points to not broadcast the SSID, and I configured the router to only allow connections from known devices (I loaded the MAC addresses of each device into the router and restricted access to devices on that list). The SSID for my network is a random 7-digit number that has no correlation to me, or my property. After this exercise, I took both Phishing Quizzes where I got perfect scores on each. As I work for ExxonMobil, a core requirement for employment at the company is ongoing awareness of and sensitivity to potential cyber threats. I’ve become very familiar with how to read a URI or an email address for validity. The only one that gave me pause was the Failed DHL delivery notice on the SonicWall quiz as the only threat indicator was the errant backslash in the hyperlink in the email. This one was very tricky.





1. What did you learn – My biggest learning from this exercise is that the time and effort spent last year to minimize the attack surface of the network and implement practices to ensure that all devices on the network are running patched OS and the most up to date firmware has been time well spent. Taking a defense in depth approach, regularly assessing network devices, monitoring changes in network behaviors or hosts, using tools like NMAP, ShieldsUp, Wireshark, and reviewing event logs are great steps to protect my family; however, I also can’t use this finding to get complacent or convince myself that the things that you’ve taught me are enough. Risk mitigation is a never-ending process of inspection, adaptation, and investment. I also discovered, by gently probing my neighbor’s networks, that almost everyone has Wireless Internet in their home, they’re mis-configuring those networks by using too much power, poor naming conventions, and, at least in a few cases, complete disregard for internet safety. I learned from the phishing quizzes that ongoing trainings at work, and many years of experience have taught me to recognize most obvious phishing attempts and that the most dangerous attacks are those where someone has paired social engineering (a phone call collecting key information, then using that information to craft a hyper-realistic email or website and then using that attack surface. One of the most helpful tactics I use at work is to leverage email headers coupled with outlook rules such that inbound email that has been scanned by out anti-virus and spam filtering infrastructure allows me to interrogate the header for origination from a sender outside of our network, then using an Outlook rule to move emails from external senders into a specific folder. This allows me to see emails from an internal sender in one inbox and emails from an external sender in another inbox. Any emails in the external inbox are generally a higher candidate for being a cyber threat and so I can treat those with a different set of eyes. Over time I’ve learned that this process works well because phishing attacks that are attempting to impersonate internal senders are much more easily identified.