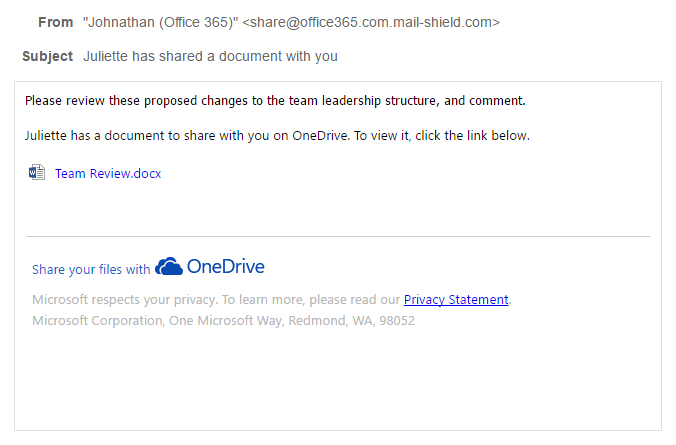
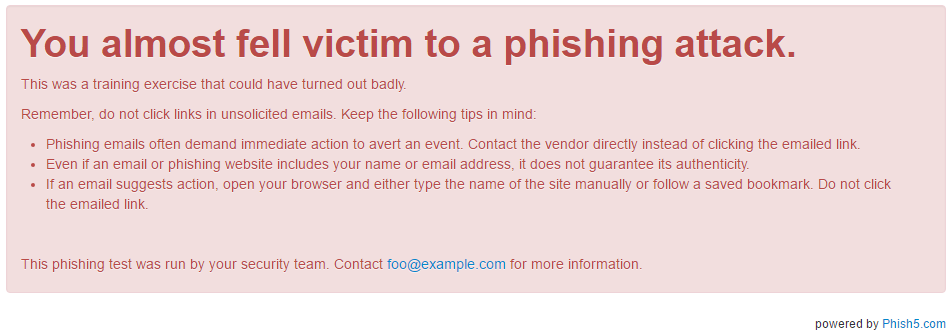
**Assignment 1 - Phishing**

*Jakob Roberts - v00484900 - SEng 360*

From my research on the internet and tools provided to me via recommendation, I have found three simple ways to get a message out in order to phish people. The first service I used was Phish5.com as they provided a service that went above and beyond most options as they would not only test for a successful phish but would also monitor possible vulnerabilities in a user’s system. The second service is a tool that is blatantly typically used for malicious purposes but can also be used by someone with proper intent: SET (Social-engineer toolkit) is a command line based tool for UNIX based systems that can do everything from creating fake webpages to sending out emails; everything that a phishing tool needs. The final service I used was simply installing Postfix on a Linux machine and was able to send out a mass email using a single bash command.

Beginning with Phish5’s service, I used a temporary email address from temp-mail.org to create an account on their website anonymously. I then went through their step-by-step tutorial to create a fake email as shown in Figure 1. Once that was create and I gave a list of recipients (targets), it then gave me the option to create a fake web-page that this would provide me with user login information for Office 365. The provided website from Phish5 can be seen in Figure 2. Because Phish5 is an organization that helps companies educate their employees, they also include a banner for after a victim has been caught in a phishing attack, this banner can be seen in Figure 3.



Phish5 is a professional grade tool that seems to imitate existing websites seamlessly and give the creator extensive information about the targets in the attack. In a large corporation where collecting valuable data on a phishing campaign may be difficult, Phish5 definitely simplified the process.



The next service I used was SET, it was slightly less intuitive than Phish5 but was nevertheless a very powerful tool for the tech-savvy. SET offers not just Social Engineering tools but also offers penetration testing services linked with a well known application called Metasploit. By combining these two services, a user can gain complete access to a computer after a phishing attempt has taken place as the file that was opened in the phishing attempt can open a backdoor in the victim's machine.

Once the social engineering attacks option was selected (option 1 in Figure 4), you are given a choice of 11 different options that spanned from everything like typical phishing attacks with websites and emails, to other esoteric options such as ones for arduino boards and QR codes. The options are then further narrowed to target specific known or possibly unknown vulnerabilities in a user’s system. This program is a lot more in depth than something that Phish5 offers and exceptionally more powerful. If I were to host my own phishing campaign at my office, I would use SET to cater precisely to the environments of the engineers and staff. As seen in Figure 5, the splash screen looks like something from the 80s, but beneath it is a powerhouse. This tool would likely be the most effective for a targeted audience, but is most definitely more complicated to set up and receive data than the service provided by Phish5.

The final option that I decided to talk about is being able to make a home-grown phishing campaign without relying on the pre-made tools from others. I decided to install Postfix (mail server client for Linux) and I set myself up as a host with Shaw. Using a fake email (I actually used “[example@shaw.ca](mailto:example@shaw.ca)” and it accepted it), I was able to send out an email using completely fake credentials with an attachment of either a plain text file or a html file. In most cases this would not be enough of an effective attack to actually steal information from a user as a website or other service would need to accompany it to be more valuable. However, the simplicity of running a simple bash command (Figure 6), a fake email can be sent out and a social engineering scam can be started.



From the three different phishing options discussed, I would not hesitate to use SET over all of them, it is by far the most efficient and powerful tool of the bunch for the tech-savvy user. By catering to the specific skillsets of all my employees (regardless of the business), I am able to keep people vigilant and aware when it comes to possible penetration attempts in the business’s security and infrastructure. Each tool has its pros and cons, but that revolves simply around the user interface and the depth of features, the content relies purely on the creativity of the creator; if the social engineer cannot craft a properly formed fake email, the phishing attempt will be null. I did not encounter any difficulties as I have performed a phishing campaign prior using the Postfix Bash command method and it worked wonderfully. After delving into using further tools, I would change my method to using SET as it is a much more refined tool than attempting to do it from scratch.