**CS521 Project**

**Phishing site link:**

https://ec521-qr-project.web.app/

**Who we are attacking:**

People visiting the following website: <https://www.bu.edu/tech/support/mybuworks/gettingstarted/>

These people probably just were hired by BU, or are otherwise new to the mybuworks platform.

**• Project title**

Phishing with QR codes, Links, and the Duplication of Web Sites

**• A description of the problem that you studied**

Phishing, or the act of impersonating legitimate online sources in an effort to acquire sensitive information, continues to be one of the most common cyberattacks to date. Cyber criminals use various tactics in phishing schemes to deceive their victims, leading them to willingly provide credentials, personal information, and the like through seemingly trustworthy sources. These attacks can range in sophistication and methods, making them extremely difficult to prevent. However, the main workflow remains the same: send the victim a message over some medium (email, Short Message Service, QR code, or fraudulent ad) which contains a link to the legitimate-looking phishing website, then convince the victim to provide the desired information. In this project, we explored a range of phishing tactics, specifically focusing on methods for mimicking trustworthy websites and using fake QR codes.

**• A description of the approach that you followed to demonstrate/measure the problem**

To demonstrate the issue of phishing, we decided to focus on creating an attack that would directly impact the Boston University community. BU already has various security measures in place, including the utilization of cookies, https protocol, 2 factor authentication, and secure collection of data. While these steps have made it more difficult to create an authentic looking phishing scheme, our team was able to still implement a workflow that seems legitimate. Our phishing website impersonates the MyBUworks Getting Started page (https://www.bu.edu/tech/support/mybuworks/gettingstarted/), which was created by Boston University. In the original version, the QR code and the links send the user to the BU portal login page (with the base URL https://shib.bu.edu/), at which point they enter their username and password as the first portion of the two factor authentication system. It is expected at this point that the DUO second factor authentication will kick in, and the user is able to satisfy that as desired. This leads the user to the correct destination safely.

Our website, found at https://ec521-qr-project.web.app/, looks and functions similarly to the original BU website. It was created by copying html code from the Inspect page on the original website. Other web pages, such as the BU login page and a 404 error page on chrome were also copied. These pages were linked together to create the following user experience:

1. The user arrives at our MyBUworks getting started page (via email link or other message)
2. The user clicks a link to “Log in to MyBUworks”, which brings them to our fraudulent BU login page.
3. The user enters their login information as the first part of two factor authentication, and presses the “Continue” button.
4. Instead of being navigated to the DUO second factor authentication page, the user arrives at a fake 404 message page, meant to simulate a loss in WiFi connection or the like (this is not an uncommon occurrence on the BU campus). At this point, the login information collected on the false BU sign in page has already been stored in our Firebase database linked to our phishing site.
5. The user clicks on the “Reload” button after presumably checking their WiFi connection, which brings them to the real BU Login page, which should function as expected.

**• Describe potential mitigations against this problem, if any, and how you evaluated the proposed mitigation in case you have implemented it**

* don’t put a QR code on your website
* disable right click <https://code-boxx.com/hide-javascript-code-from-client/>
* try to encrypt your source code
* hide “View Source” option in the inspect element: https://www.howtocreate.co.uk/tutorials/javascript/security
* Really hard to fix this problem to be honest.
* Mostly need to educate people on how to tell if a website is secure
* Create QR codes that are branded <https://blog.beaconstac.com/2021/08/create-qr-code-templates/>

**• A summary of your results. These can be measurements, proof of concept code, ML results, …**