

Don't Get Hooked: Understanding Phishing Attacks

Student: Michaela Dunston

Mentor: Dr. Masoud Sadjadi

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

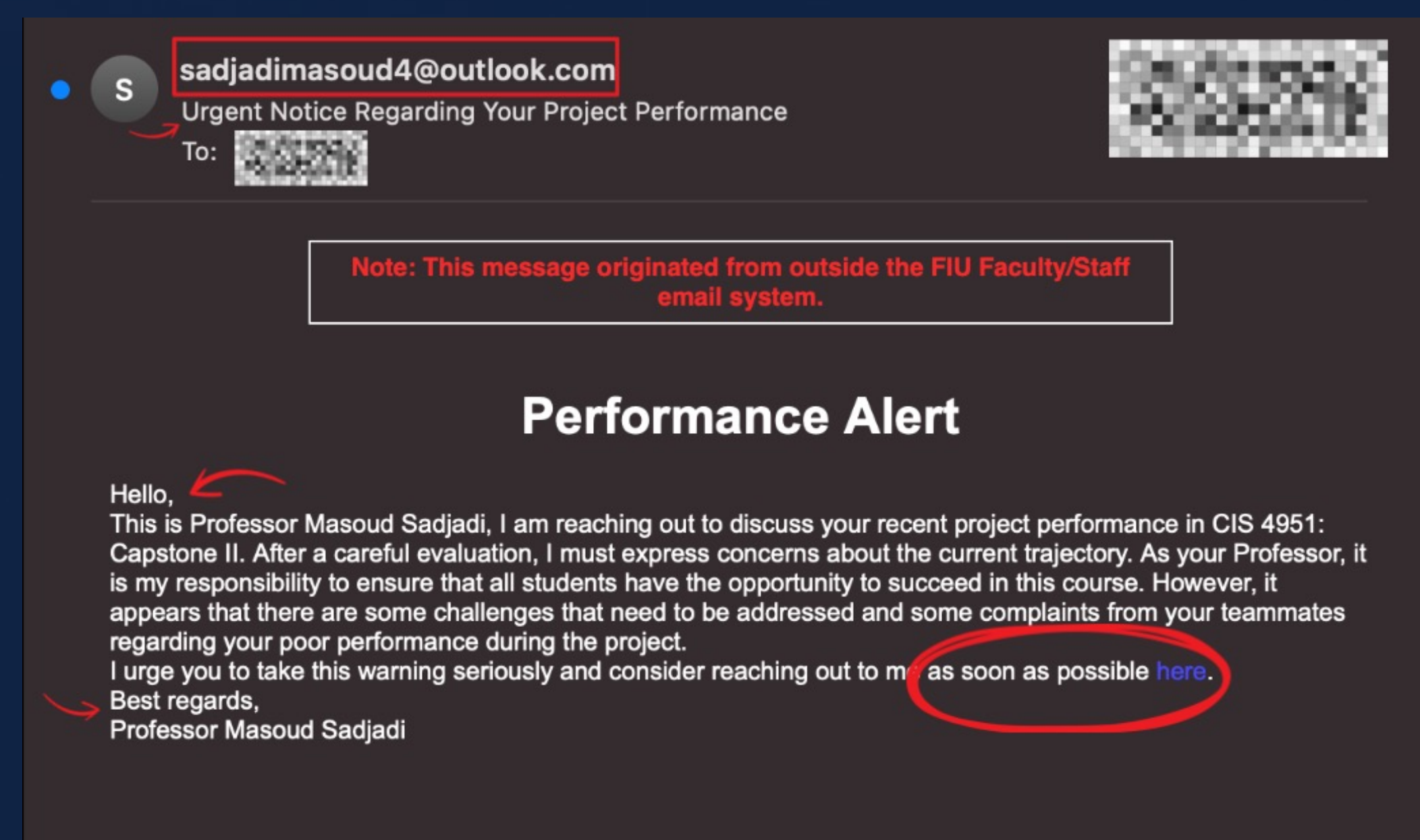
Red Flags

Red flags in phishing attempts are warning signs or indicators that help individuals identify potential scams.



Implementation

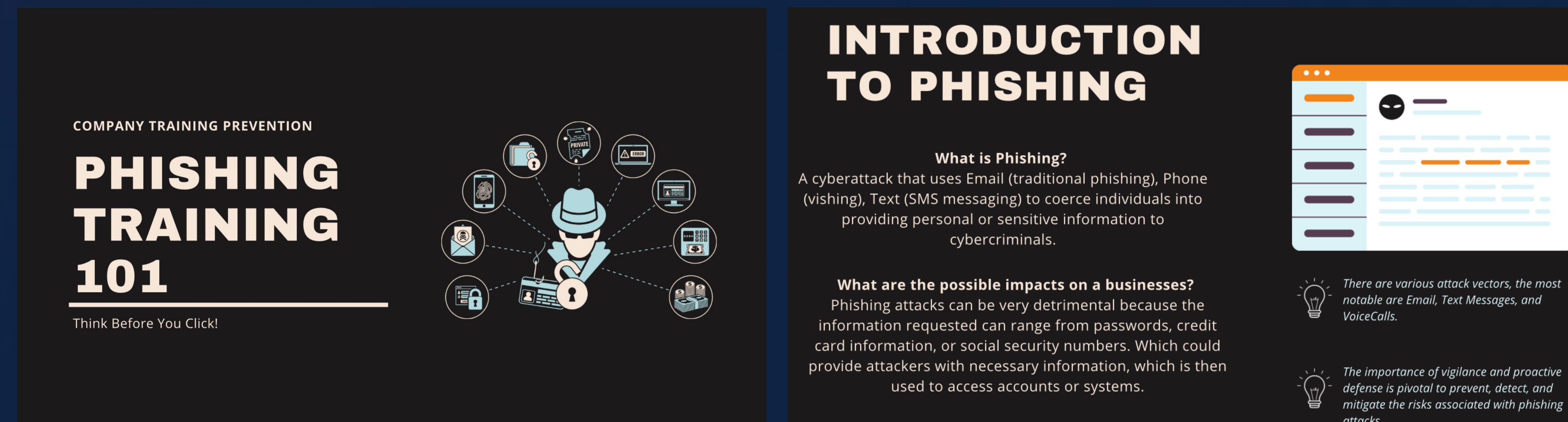
The phishing characteristics we covered in our training encompass urgent language, emails purportedly from the institution but with sender email mismatches, irregular punctuation, absence of a signature or official logo, and inclusion of suspicious links



Current System

Throughout this term, we delved into the complexities of Email Phishing, leveraging the Gophish platform for comprehensive exploration and testing. I took on the responsibility of overseeing the deployment process, conducting development testing, and was subsequently tasked alongside my teammate Mario Vega with designing a tailored Phishing Training program aimed at educating users susceptible to Phishing Attacks.

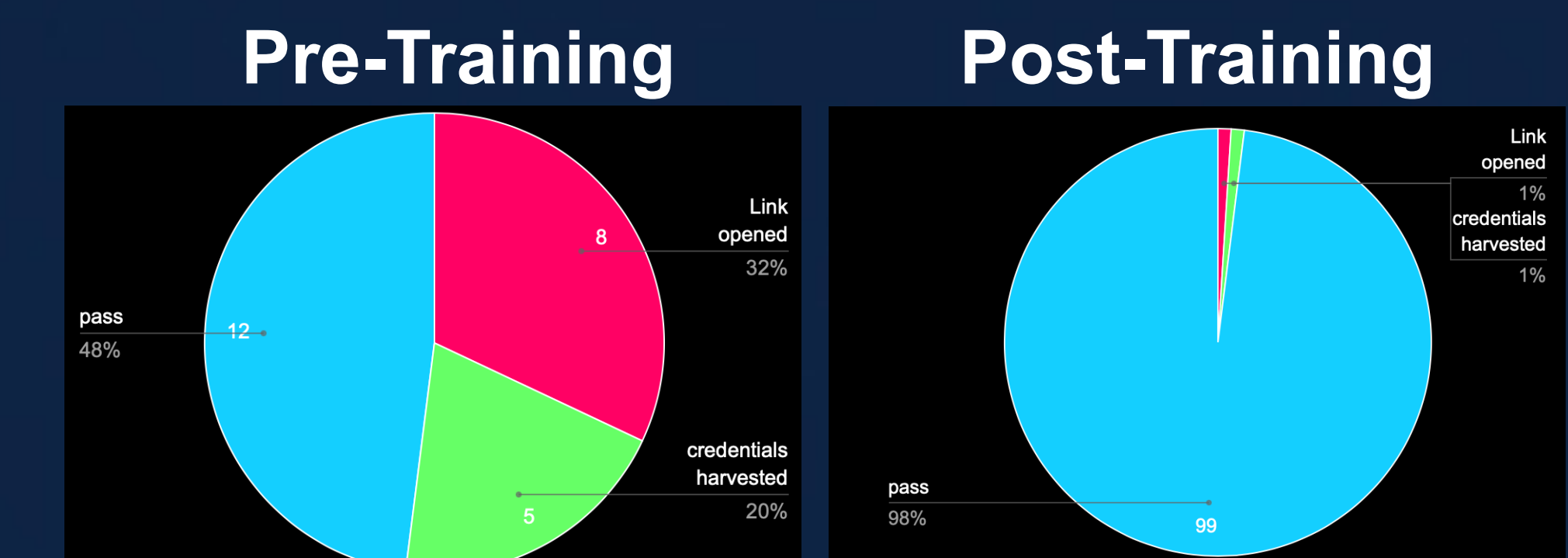
Implementation



Summary

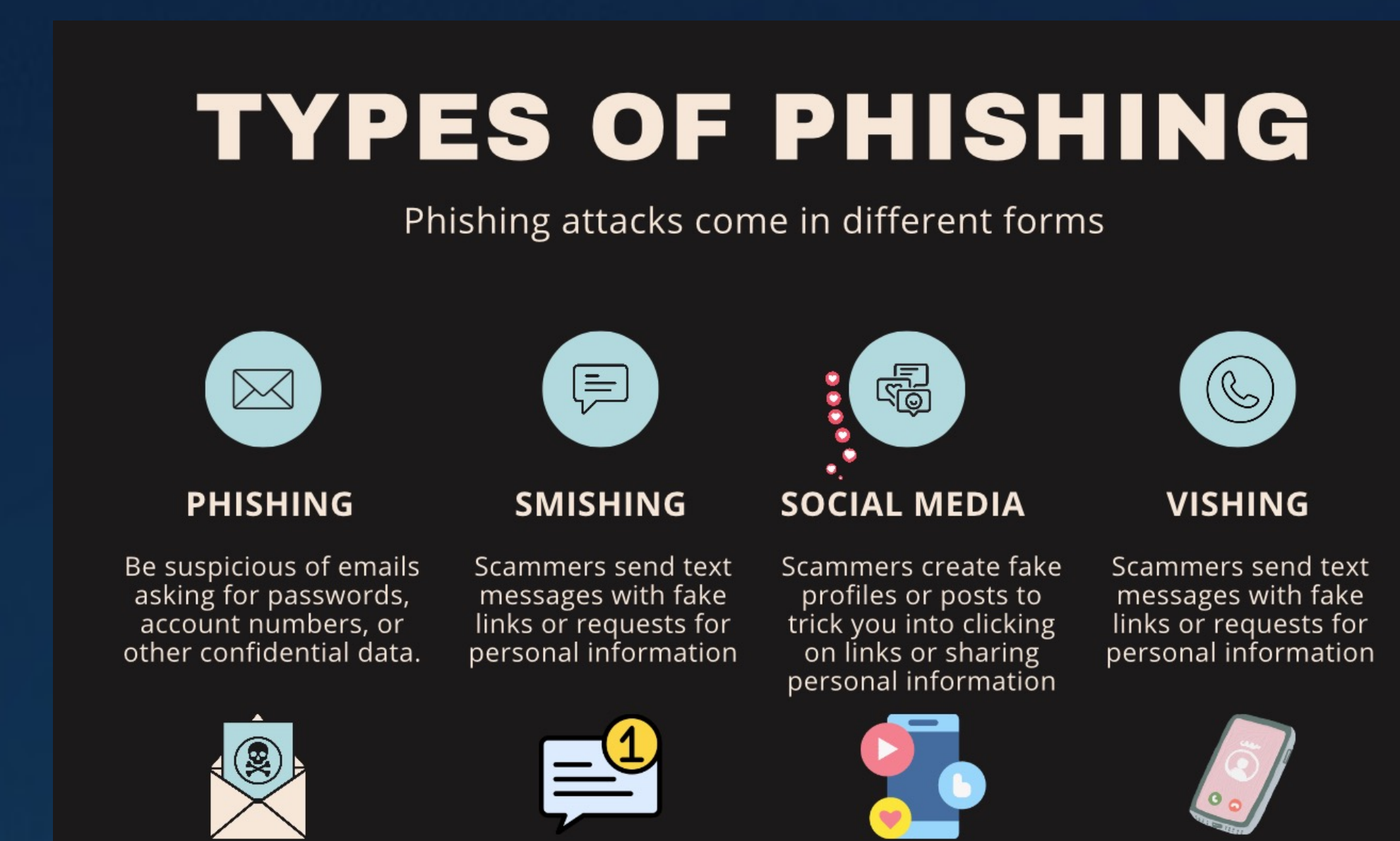
Phishing stands out as a straightforward method for digital attackers to claim numerous victims and potentially gain substantial rewards simultaneously. The surge in remote and hybrid work arrangements has propelled phishing attacks to unprecedented levels, exploiting the extended screen time of employees and providing cybercriminals with ample opportunities to strike. When users invest time in understanding the motivations behind phishing, the mechanics of phishing attacks, and the increasing prevalence of social engineering tactics, they empower themselves against digital threats. They can delve into various email-based phishing schemes, gaining insights into recognizing and reporting such attacks.

Statistics of users who were impacted by our Phishing Training



Types of Phishing

Phishing attacks come in different forms, Email Phishing (suspicious emails), Smishing (text messages), Social Media (fake accounts), & Vishing (Phone calls and messages with fake links)



Email Phishing

The most common form. A deceptive message designed to deceive recipients into disclosing confidential information such as passwords or credit card details. These emails frequently mimic reputable entities such as banks or well-known websites to enhance their credibility. Their objective is to exploit an individual's trust in these organizations, convincing them to divulge personal details, click on harmful links, or download attachments that may contain malware.

REFERENCES: <https://www.linkedin.com/learning/cybersecurity-awareness-phishing-attacks/>, <https://getgophish.com>

ACKNOWLEDGEMENT

The material presented in this poster is based upon the work supported by the Knight Foundation School of Computing and Information Sciences We/I thank Dr. Sadjadi for his/her/their assistance and mentorship that I/we received throughout the senior design project.