



Knight Foundation
School of Computing
and Information Sciences

KFSCIS/FIU

Spring 2024 Capstone 2



Knight Foundation
School of Computing
and Information Sciences

Don't Get Hooked: Understanding Phishing Attacks

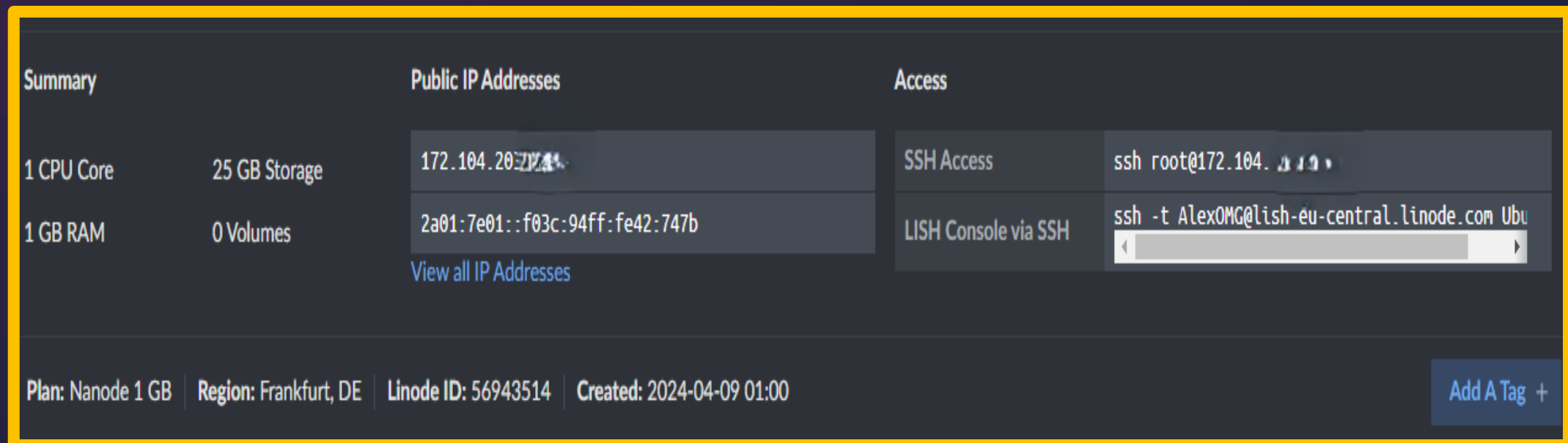
Student: Alejandro Arrocha

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

Email phishing is a prevalent form of cyberattack that relies on deceptive emails to trick recipients into taking specific actions, such as clicking on malicious links, downloading attachments containing malware, or divulging sensitive information. Email phishing is one of the most common forms of phishing attacks. Attackers send fraudulent emails that appear to come from legitimate sources, such as banks, social media platforms, or government agencies. These emails often contain links or attachments that lead to malicious websites or download malware onto the victim's device. For this Campaign, we put ourselves in the position of any email attacker to learn and understand how easy it can be done. These are the basic elements, tactics and tools involved in our Phishing Campaign.

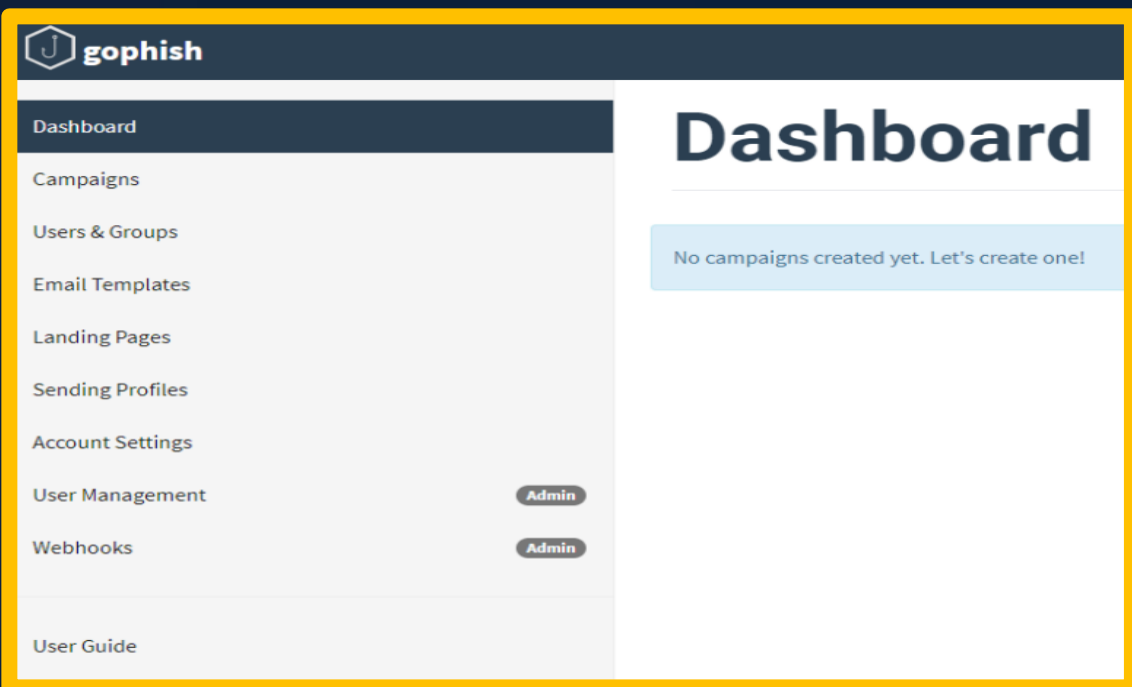
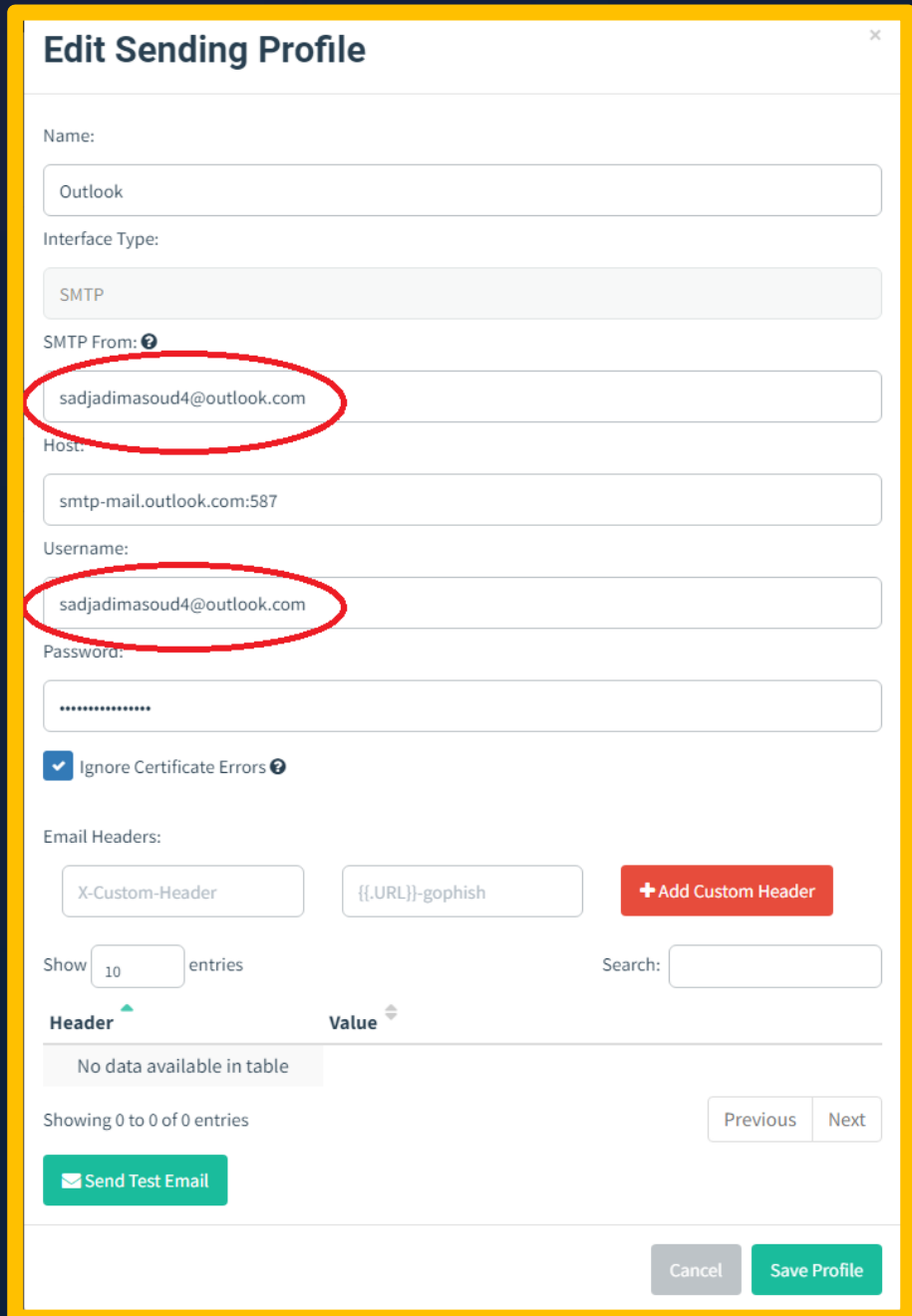
Step 1: Getting a VPS and Gophish Tool

- VPS stands for Virtual Private Server
- Created by partitioning a physical server into multiple isolated virtual servers
- Each VPS operates independently with dedicated CPU, RAM, storage, and network bandwidth
- Utilized Akamai Linodes to rent a Debian 64bit Ubuntu OS
- Provided a Public IP address
- Connected via SSH access



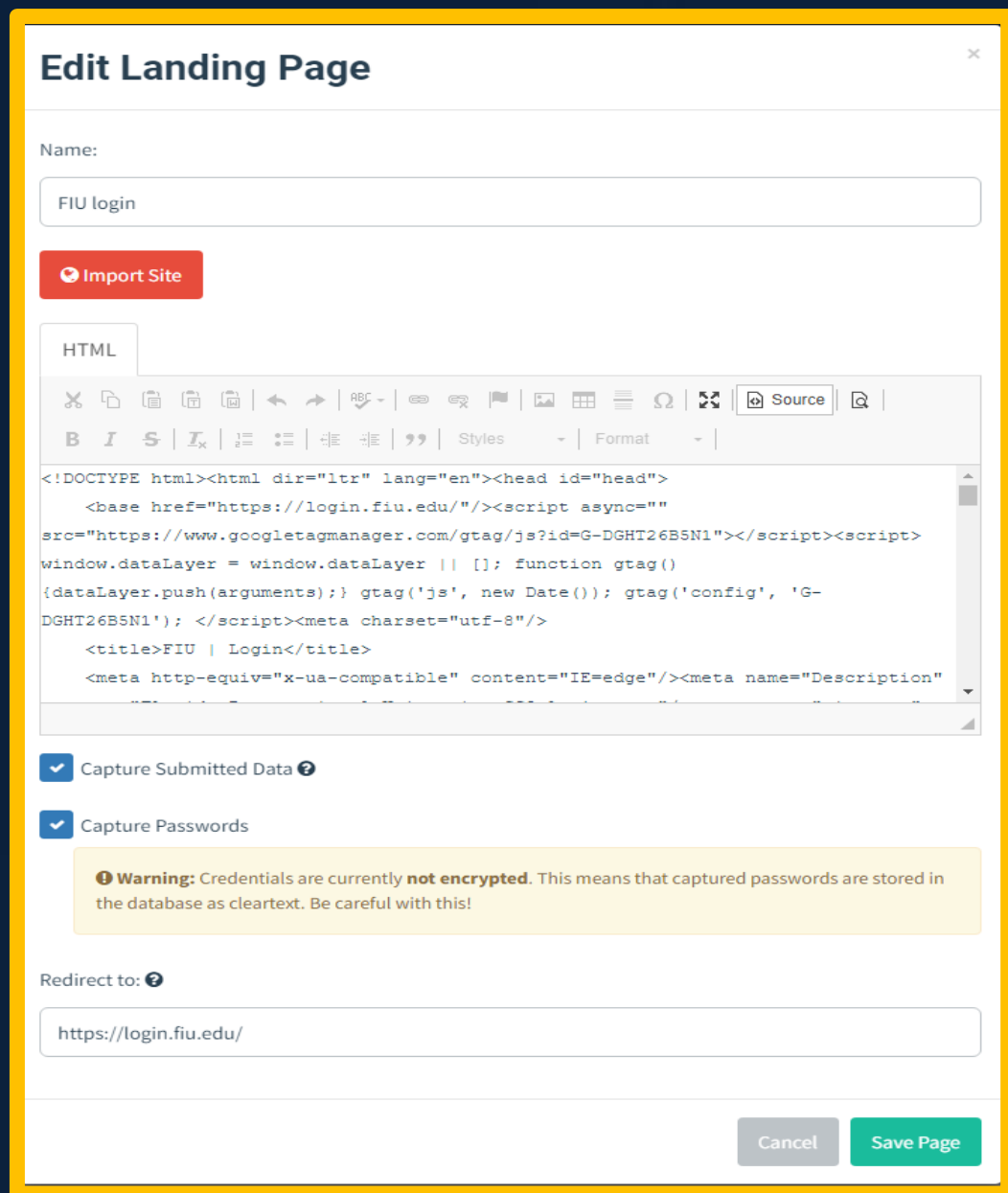
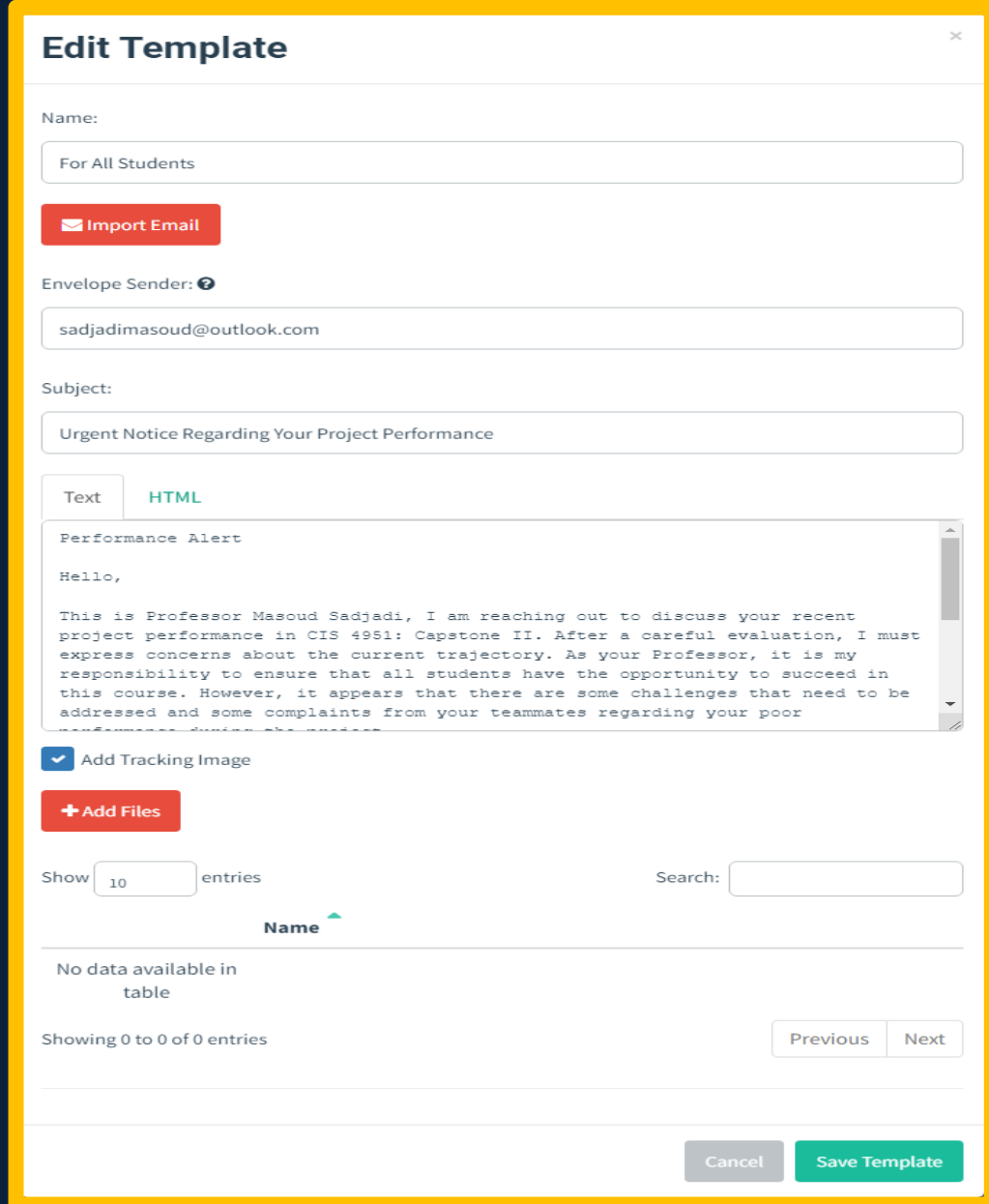
Step 2: Playing with Gophish

- Gophish website:
- Well-made and user-friendly
- Intuitive design
- Clear navigation
- Seamless functionality
- Easy for newcomers to try out and play with



- Sending Profile:
 - Allows selection of email provider and SMTP server
 - Determines sender appearance to recipients
 - Helps in avoiding detection as a phishing scam by using familiar email sources

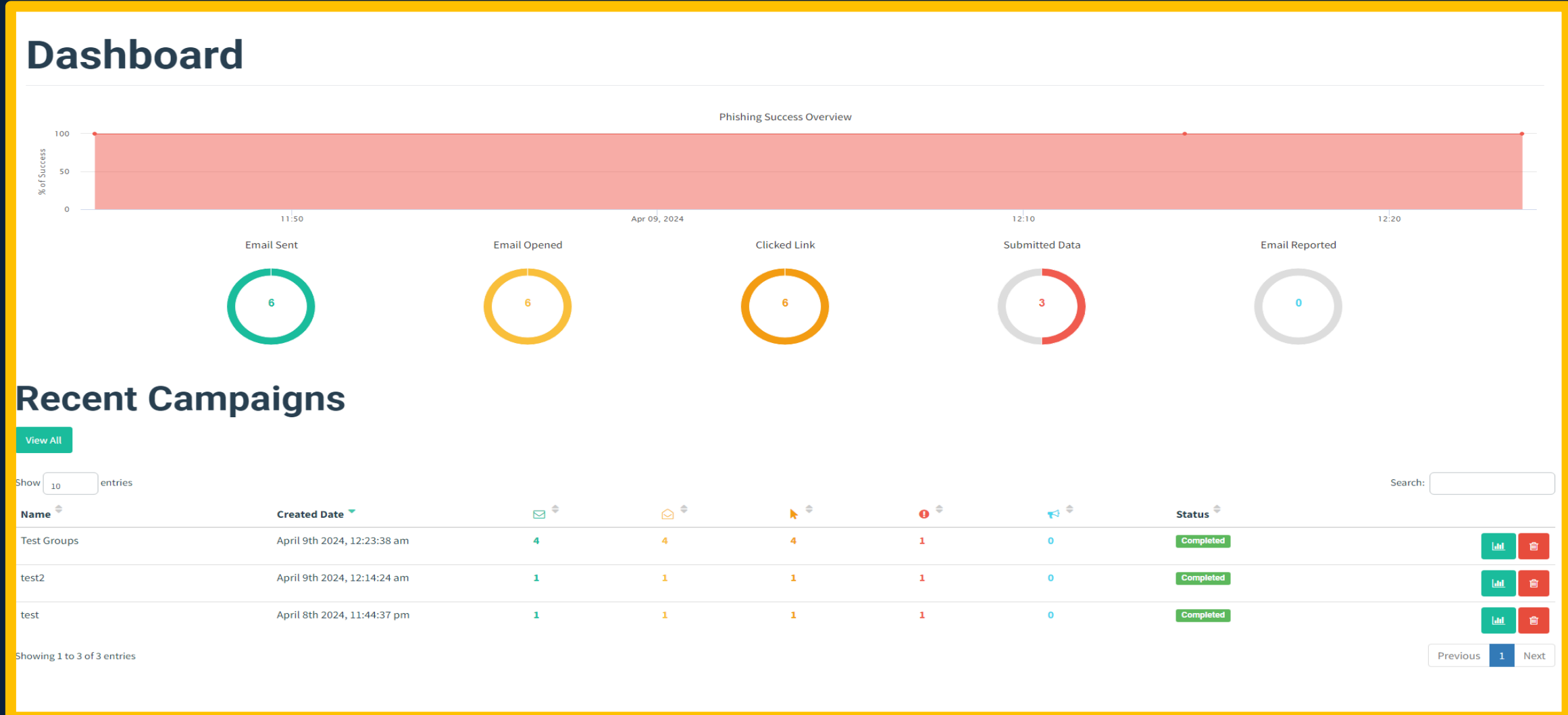
- Email template creation:
 - Designed to resemble an important email from a professor
 - Mentions a student's poor performance in the course
 - Urges immediate contact with the professor via a link in the template
 - Created using HTML to customize appearance and layout



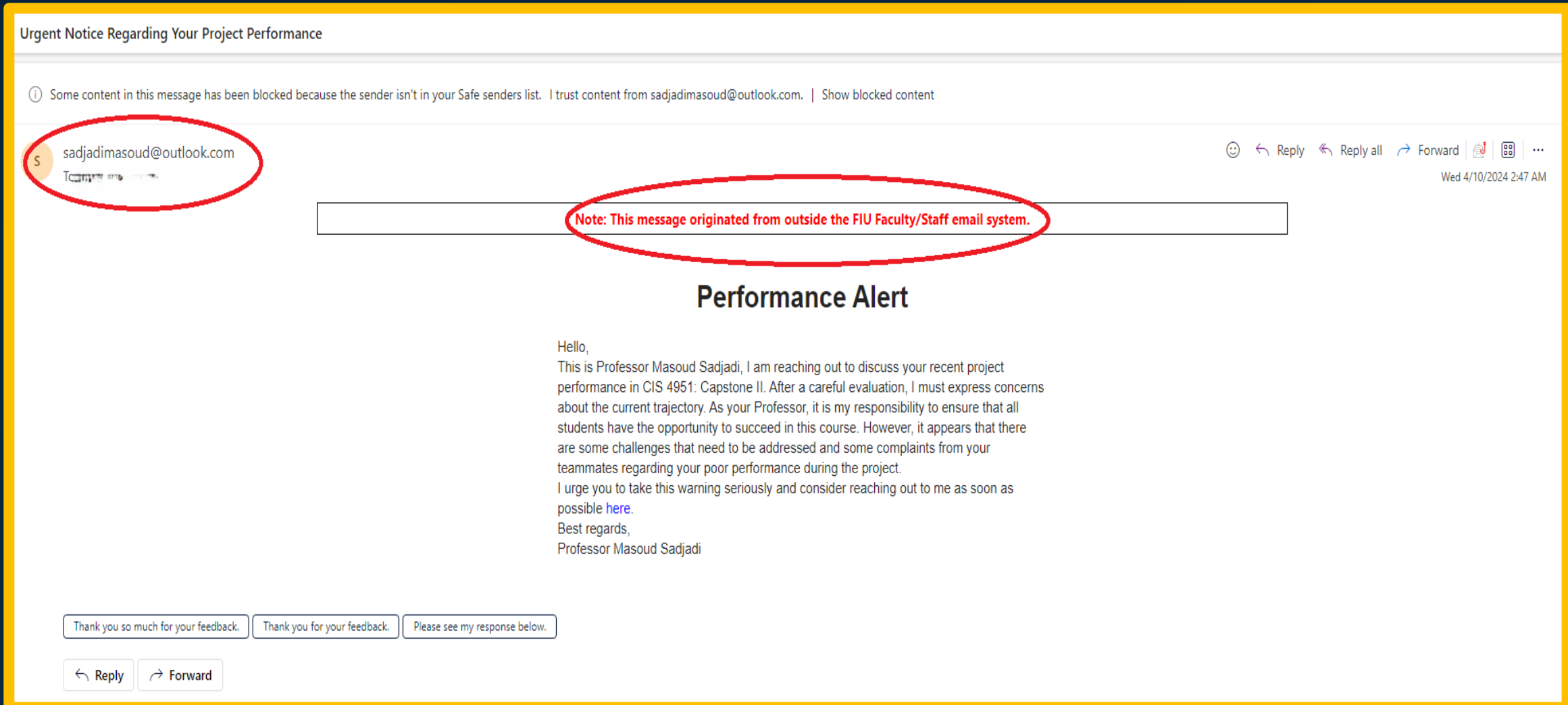
- Add subjects' emails to Users Group section
- Create landing page:
 - Resembles FIU login page
 - Provides convincing appearance for authenticity
- Phishing campaign is ready to start

Step 3: See the Results

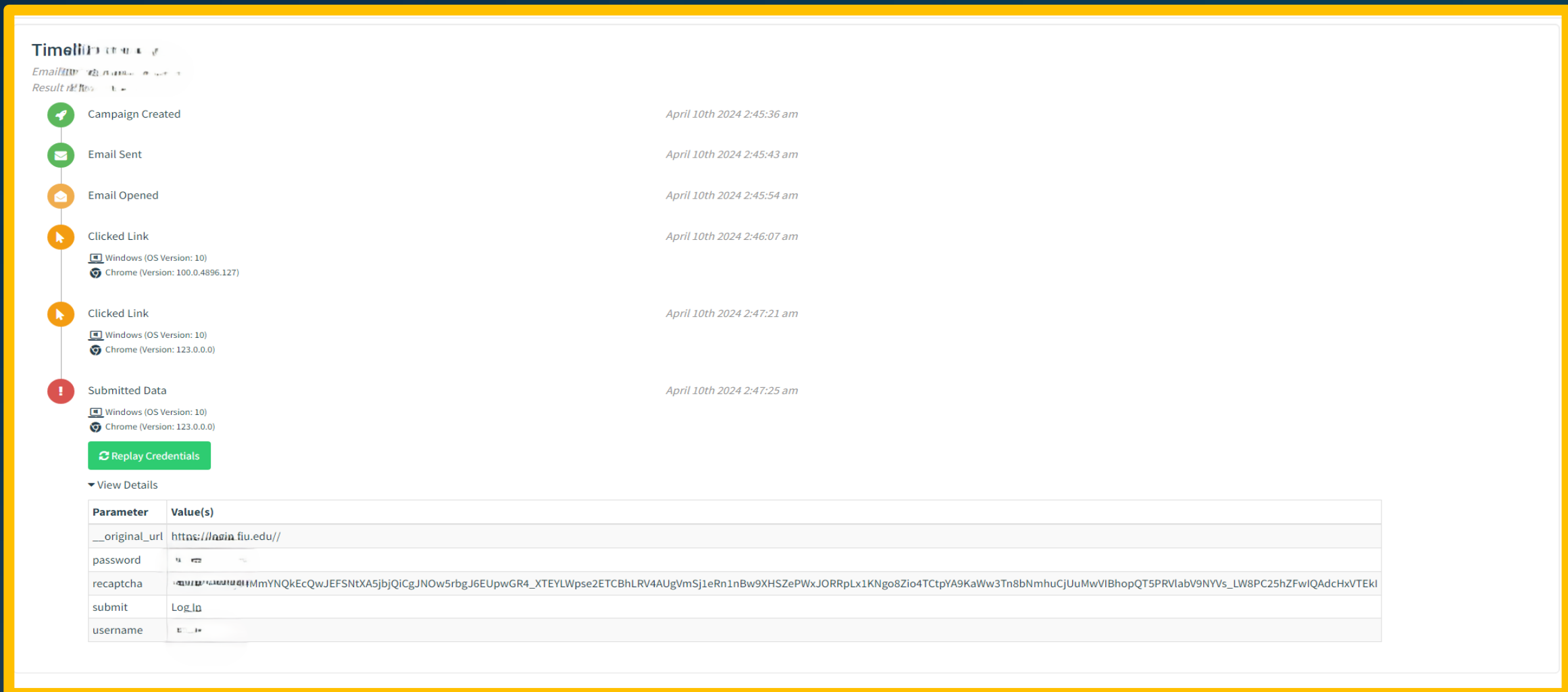
- Gophish Dashboard features:
 - Track and monitor campaign activities
 - View email reception times and dates
 - Monitor email openings
 - Track clicked links
 - Monitor submitted data



- User's perspective:
 - Receives email resembling an important message from a professor
 - Outlook's features highlight potential phishing scams
 - Users can easily recognize suspicious emails



- Attacker's perspective:
 - Instantly collects users' credentials
 - Gains insight into users' device type, OS version, and browser information upon link click



REFERENCES: Phishing For Dummies, Cisco Special Edition, Published by John Wiley & Sons, Inc.; GitHub; Youtube Screeck, Youtube I.T Security Labs.



Knight Foundation
School of Computing
and Information Sciences

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.



Knight Foundation
School of Computing
and Information Sciences