UTM

UNIVERSITI TEKNOLOGI MALAYSIA

SECP1513-TECHNOLOGY AND INFORMATION SYSTEM

Section 03

Proposal Topic: Cybersecurity
Lecturer: Dr. Muhammad Iqbal Tariq Idris

Name	Matric Number
AVIDIAN DIPESH SIVA	A23CS0052
TEE SOON KIET	A23CS5009
MOHAMMAD DANIAL BIN NASHARUDIN	A23CS0125
MERVYN BEE ZHENG CHENG	A23CS0245
MOHAMED OMAR MAKHLOUF	A23CS4014
TISHEN A/L SANTHIRAGASAN	A23CS0192

1. Client background.

Our client is an educational institution managing extensive student data. With their presence on social media platforms, especially on Telegram, where they are currently relying on anti-scammer bots as part of their cybersecurity measures. Data breaches through phishing attacks, are still causing leaks of personal information, loss of personal and financial assets or even blackmailing.

2. Existing technology used by the client summary.

Social media platforms rely on a combination of traditional security measures, such as firewalls and antivirus software, to protect their accounts' information. However, these measures often fall short in detecting and preventing sophisticated phishing attacks that exploit human vulnerabilities. Additionally, social media platforms themselves offer limited built-in security features, leaving businesses susceptible to targeted phishing campaigns.

3. Problem with existing technology used by the client.

The existing technology and tools for anti-phishing are not effective against advanced phishing techniques. Human error is also a significant factor in data breaches.

3.1. Dynamic URL Changes

Phishing links shared on social media can dynamically change, making it challenging for traditional link-scanning tools to keep up. The rapid spread of malicious content can occur before the links are flagged.

3.2. Limited awareness

Phishing attacks often involve social engineering tactics that manipulate individuals into divulging sensitive information. Limited awareness results in a failure to recognize and resist these manipulative techniques.

3.3. Insufficient Real-time Detection

The existing systems lacks real-time detection capabilities, allowing certain phishing attacks to go undetected until after potential damage has already happened.

4. Proposed idea to overcome the problems.

Implement anti-scammer bots to proactively identify and address phishing attempts on social media. These bots can use machine learning to analyze messages and identify suspicious patterns in real-time, helping reduce the risk of phishing attacks. Anti-scammer bots can also monitor user interactions and flag instances where someone is attempting to impersonate a trusted source. Additionally, these bots can send educational messages to users to help them avoid phishing attacks.

5. Advantages to the proposed idea.

Anti-scammer bots can help to reduce the risk of data breaches by providing proactive protection. The real-time detection ensures anti-scammer bots can identify and respond to phishing threats immediately, minimizing the risk of unauthorized access to student data. Machine learning integration enables the bots to adapt swiftly to new phishing tactics, ensuring a proactive and real-time defense against evolving threats on platforms like Telegram. They can also help to educate users about phishing tactics and how to protect themselves. Additionally, anti-scammer bots can complement existing security measures to provide a more comprehensive approach to phishing protection.