# RIPHAH INTERNATIONAL UNIVERSITY


## Faculty of Computing
## FINAL YEAR PROJECT INITIAL PROPOSAL

# Phish Net
## (Phishing Simulation & Cyber Awareness)

### Project Team

| Full Name of Student | SAP Id | Program | Contact Number | Email Address |
|---|---|---|---|---|
| Ali Kayani | 37539 | BSCYB | 0334-8141448 | 37539@students.riphah.edu.pk |
| Umar Waqar | 27668 | BSCYB | 0312-0204073 | 27668@students.riphah.edu.pk |
| | | | | |
| | | | | |

**Dr. Jawaid Iqbal**
Assistant Professor

# Project Proposal

**Project Title:** Phish Net, Phishing Simulation & Cyber Awareness

## Description:

Phish Net is the need of the hour for the Pakistan's Technology Industry. Having not much input in the Cyber Security domain and especially the Phishing dilemma. This project would be the revelation the **industry starves**. With numerous phishing attempts being made from High-level VIP victims, private companies, public institutions, military organizations and education & healthcare institutions.

In today's digital age, cyber threats are evolving at an alarming rate, yet Pakistan's technology sector has **limited resources dedicated** to tackling one of the most pressing issues—phishing attacks. These attacks don't just target individuals; they compromise VIPs, private companies, government institutions, military organizations, and even hospitals and universities. Despite this growing threat, there's a **significant gap** in cybersecurity education and preparedness across the country.

Right now, most businesses rely on foreign cybersecurity solutions, leaving them dependent on international providers and vulnerable to external policies. Without a homegrown solution, Pakistan remains exposed to **financial losses**, data breaches, and operational disruptions caused by cybercriminals.

Introducing Phish Net: A Game-Changer in Cybersecurity

Phish Net is designed to **fill the gap** by providing a **localized** phishing prevention and cybersecurity awareness system tailored specifically for Pakistan's digital landscape. This platform will offer:

- Phishing simulations to train employees and test an organization's vulnerability.
- Advanced email filtering to prevent malicious emails from reaching inboxes.
- Structured cybersecurity training to build awareness and resilience across industries.
- Real-time threat intelligence to detect & neutralize cyberattacks before causing damage.
- Behavioral analytics to identify insider threats and suspicious activities.

With Pakistan's National Cyber Security Policy 2021, emphasizing the urgent need for stronger cybersecurity measures, Phish Net aims to **support businesses, institutions, and government agencies** in proactively addressing cyber risks. It will not only help

organizations **stay ahead of the curve** (evolving threats) but also ensure **compliance** with international cybersecurity regulations, reducing the risk of penalties and reputational damage.

## Why Phish Net Matters?

One of the biggest challenges Pakistan faces is the lack of a centralized cybersecurity awareness and **response system**. Organizations are often unaware of new cyber threats and global regulations, making them vulnerable to attacks and compliance issues. Phish Net aims to **bridge this gap** by providing a **comprehensive**, domestic solution that helps businesses protect their data, secure their operations, and train their workforce effectively.

## Key Objectives:

- Train and educate employees through interactive phishing simulations and awareness programs.
- Help organizations comply with international cybersecurity standards to avoid penalties and security risks.
- Establish a real-time phishing threat intelligence database for better risk detection and prevention.
- Improve incident response strategies and minimize financial losses caused by cyberattacks.
- Strengthen Pakistan's overall cybersecurity framework, reducing dependence on foreign solutions.

## Building a Safer Digital Environment

Phish Net is more than just a cybersecurity tool—it's a strategic initiative to strengthen Pakistan's digital resilience. By empowering businesses and institutions with the knowledge and tools to prevent phishing attacks, we can create a safer, more secure online environment for everyone.

In the long run, this initiative will not only **enhance national security** but also protect businesses from financial and reputational harm, paving the way for a more secure and self-reliant digital future.