

# Phishing and Social Engineering

**Omar Alzubair**

04/16/2024

—

Independent Study

Student-Run Cybersecurity Center

—

Professor Forrester-Small

Professor Giraldo

---

## Abstract

This report reaches into the landscape of phishing and social engineering, focusing on the different strategies used to counter these threats. Highlighting the critical role of awareness and training, the report also explores the evolution of phishing tactics, including vishing and smishing. Through comprehensive analysis and case scenarios, this report provides valuable insights for organizations seeking to bolster their defenses against emerging phishing threats.



## Table of Contents

- 
- **Introduction**
  - **Phishing Scenarios**
  - **Use of AI and LLM**
  - **GoPhish Setup**
  - **GoPhish Campaign Test**
  - **Access Control Models**
  - **Employee Training**
  - **Security Mechanisms**
  - **Conclusion**
  - **Glossary**
  - **References**
-



## Introduction

As Charles Griffiths, a director of technology and innovation at AAG, aptly stated, "Phishing is the most common form of cybercrime, with an estimated 3.4 billion spam emails sent every day." This underscores the urgency and importance of our efforts in combating this pervasive threat.

Phishing, a common cyber-attack method, preys on human vulnerability using social engineering techniques, exploiting trust to gain sensitive information like usernames, passwords, or financial data. Phishers commonly use emails, messages, or fake websites that mimic legitimate ones to deceive targets. This threat extends to all online users, including students, faculty, and staff, highlighting the extent of its reach.

Vishing, a form of phishing, manipulates victims through voice communication, often posing as trusted entities over phone calls or voice notes. Attackers use social engineering techniques to manipulate individuals into disclosing sensitive information over the phone. Students may receive vishing calls pretending to be from their educational institution, asking for personal information or credentials.

Social media phishing involves using deceptive tactics on social platforms to trick users into disclosing personal information. Attackers create fake profiles, pages, or messages on social media to impersonate trusted entities, tricking users to click on malicious links or share sensitive information. Students often use social media extensively, making them susceptible to phishing attempts through platforms like Facebook, Instagram, or Twitter.

Apart from traditional phishing and vishing, various other types of phishing attacks exist. Piggybacking occurs when attackers gain unauthorized access by physically following someone with legitimate access. For example, a person traveling with a laptop connected to the hotel's Wi-Fi network could use piggybacking to share the Wi-Fi connection with personal networking gadgets like smartphones. While whaling targets high-profile individuals or executives within an organization, seeking sensitive information or credentials from them.

Recognizing the severity of these threats, within the Student-Run Cybersecurity Services Center (SCSC) I will be responsible for offering phishing including vishing, social media phishing and setting up phishing campaigns. This initiative aims to raise awareness and fortify defenses against evolving social engineering attacks.

Within this project, the report approach aligns with industry best practices and focuses on comprehensive training. By simulating real-world scenarios and deploying tailored phishing campaigns, the project seeks to educate and empower organizational members.

In summary, the SCSC's phishing project is a step towards bolstering cybersecurity defenses within the educational sector, promoting resilience against cyber threats while providing students with real-world experiences and challenges.

## Phishing Scenarios

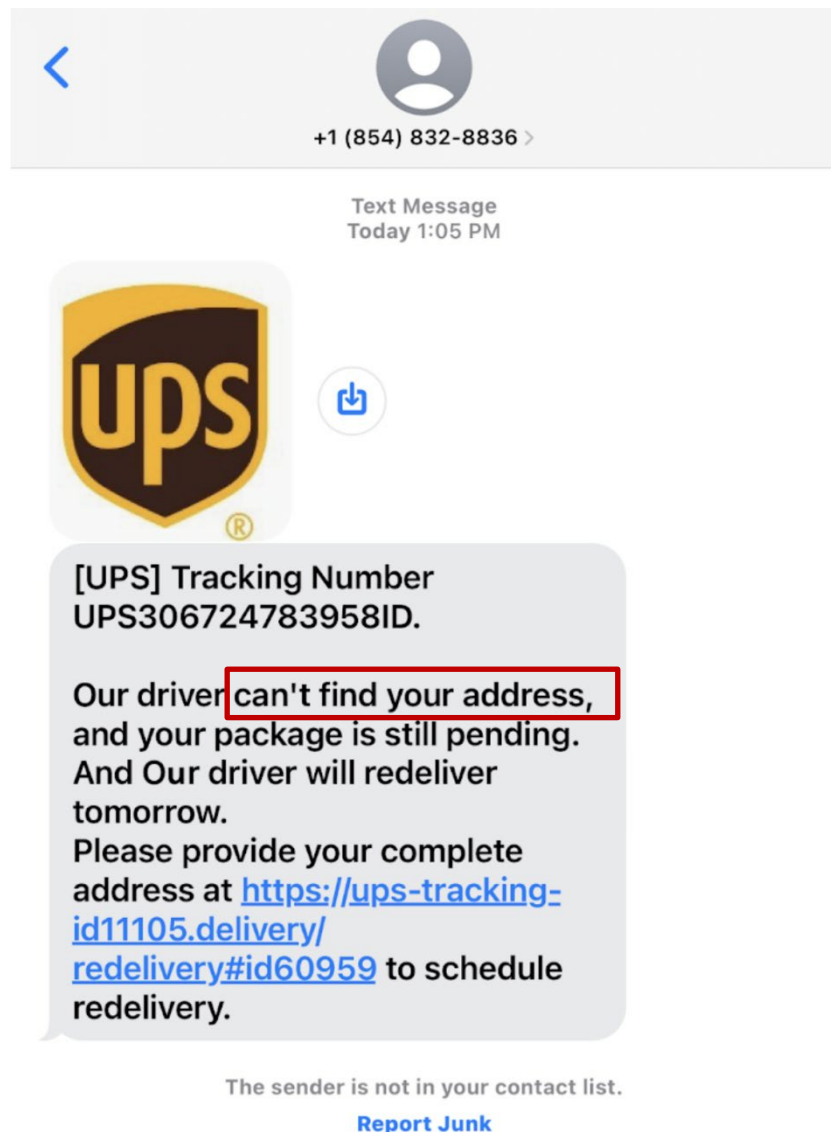
In **whaling** attacks, high-ranking individuals within an organization are targeted due to their access to vast networks and services. The attacker uses social engineering skills to urge the employee into action, often by impersonating someone of authority. For instance, in a high school setting, the financial administration of the institution oversees the management of the payroll system for its staff, encompassing sensitive data such as pay stubs, names, addresses, and social security numbers. Unfortunately, the integrity of this account was compromised because of an urgent email prompting the update of employee payroll information. The hyperlink embedded in the email directed the accountant to a seemingly authentic employee payroll service page, meticulously crafted by the attacker to deceive. Subsequent entry of credentials provided the attacker with unrestricted access to invaluable employee information, exposing them to potential exploitation.

The adoption of NIST SP800-171 security controls stands as a pivotal measure that could have prevented this security breach. Primarily, instilling user awareness among employees is imperative; comprehensive education empowers personnel to detect and block phishing attacks before they manifest. Additionally, the incorporation of Multi-Factor Authentication (MFA) serves as an effective deterrent against unauthorized access, significantly diminishing the probability of security breaches. MFA introduces an additional layer of security and verification, mandating users to confirm their identity through diverse means even in scenarios where credentials may have been compromised. These robust security measures collectively form the bedrock of the institution's defenses against phishing attacks. In the figure below, the attacker uses his social engineering skills to urge the employee and make him panic into thinking they must perform the action in a timely manner by an order coming from the CFO:



**Smishing** attacks, increasingly common, exploit individuals through fake mobile texts, urging them to click on harmful links. Social engineering tactics create a sense of panic, compelling individuals to act impulsively rather than logically. In this scenario in a travel agency, within the operational services of the agency is facilitating customer bookings for flights, hotels, and travel packages. A security breach happened when a new employee, who isn't familiar with industry standards, fell victim to a smishing attack. The attacker, pretending to be a resort representative on a social media platform, tricks the employee into sharing seemingly harmless details like a customer's name and phone number. With this information, the attacker then tricks customers in a second smishing attack, posing as the travel agency. They offer a free travel package, tempting customers to share more sensitive information and putting them at risk of exploitation.

The preventive fortification of the agency's security posture hinges on the meticulous implementation of security controls aligned with the specifications listed in NIST SP800-171. To address the employee's vulnerability in handling sensitive information, the initial defense strategy focuses on thorough training and awareness efforts. A consistent and detailed training program, designed especially for new hires, explains common phishing techniques in the industry. The training underscores the importance of verifying customer identities, empowering employees to recognize and proactively handle potential social engineering attacks. Adding an extra layer of defense happens when we put in place access controls. We do this by following the principle of least privilege, meaning employees only get access to customer data that's necessary for their job. While these measures might seem a bit tricky at first for both new and experienced employees, they really boost the agency's security. This helps keep the important information they handle safe and secure. The figure on the side shows an attacker posing as a package carrier inducing panic to prompt individuals to click on a link urgently:



In **spear phishing** attacks, social engineering is used to tailor emails, perpetuating another organization or person with whom the victim has exchanged communications before. In this case a recently established pizzeria encountered a sophisticated scam involving an urgent email, allegedly originating from their cheese supplier. This communication, which insisted on an immediate update of payment information through a provided link, cited an impending service of the payment system within a 24-hour timeframe. Lacking the necessary training, an unknowing employee fell prey to the deception, without being aware of navigating to a well-crafted billing page engineered by the attacker. Consequently, a payment was remitted under the misguided belief of authentic transactional engagement, with the employer remaining blissfully unaware of the fraudulent nature of the transaction. Without being suspicious to them, the attacker successfully diverted the funds, leaving the enterprise oblivious to the fraudulent transfer.

In fortifying the cybersecurity infrastructure of the pizzeria and mitigating such attacks, the importance of security lies in the implementation of a robust financial transaction anomaly detection system. This system would diligently analyze transactional dynamics between the pizza shop and its suppliers, swiftly identifying anomalies such as abrupt changes in payment amounts, recipient identities, and scheduled transaction times. By carefully monitoring and analyzing transactional activities, this system serves as a security layer against social engineering ploys targeting the enterprise's financial transactions.

Following the guidelines outlined by NIST, the integration of email filtering and authentication mechanisms assumes pivotal significance. These proactive steps help stop phishing emails before they reach the intended recipients. Strengthening email security acts like a protective barrier, keeping the pizzeria's communication channels safe from fake and deceptive messages. The figure below shows a fraudulent payment paycheck email from HR to a University of Delaware employee, where the attacker that uses urgency and manipulation by tricking the employee into thinking they got a raise :

From: UDEL HR <[hremployee payroll@udel.edu](mailto:hremployee payroll@udel.edu)>  
Date: August 13, 2015 at 12:48:29 PM EDT  
To: <[REDACTED]>  
Subject: Your August 2015 Paycheck



Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

Your salary raise documents are enclosed below:

[Access the documents here](#)

Faithfully

Human Resources

University of Delaware

## Use of AI and LLM

The increasing adoption of Artificial Intelligence (AI) and Large Language Models (LLMs) in cyber-attacks is raising concerns within the cybersecurity realm. These technologies enable attackers to automate and enhance various aspects of phishing attacks on a larger scale. Here are some ways in which AI and LLMs are utilized in such attacks:

### Natural Language Processing (NLP) Algorithms:

NLP algorithms, a subset of AI, excel in interpreting and analyzing human language and tones. Attackers leverage these algorithms to craft smishing and phishing emails that closely mimic human communication, increasing their believability to victims.

### Automated Phishing Campaigns:


AI facilitates the rapid execution of large-scale automated phishing campaigns, allowing attackers to target a broader audience at an accelerated pace. This scalability poses significant risks, necessitating more scalable mitigation techniques to counteract these attacks effectively.

### Voice Recognition and Manipulation:

AI-driven voice recognition and manipulation technology enable attackers to create realistic dialogues with familiar-sounding voices. By impersonating trusted individuals within organizations, attackers increase the likelihood of victim compliance with their fraudulent requests.

These advancements in AI and LLMs underscore the evolving sophistication of cyber threats, requiring organizations to implement robust defense strategies and stay vigilant against emerging attack vectors.

### AI-powered phishing protection with Sophos Email




**Advanced ML identifies imposters and BEC**

- Analyze tone and wording
- Identify impersonation targets
- Scan for imposters



**Real-time scans block social engineering**

- Spot key phishing indicators
- Identify anomalies in headers



**Pre and post delivery protection stops malware**

- Block malicious URLs and attachments
- Protect against URL re-writing
- Dynamically react to threats

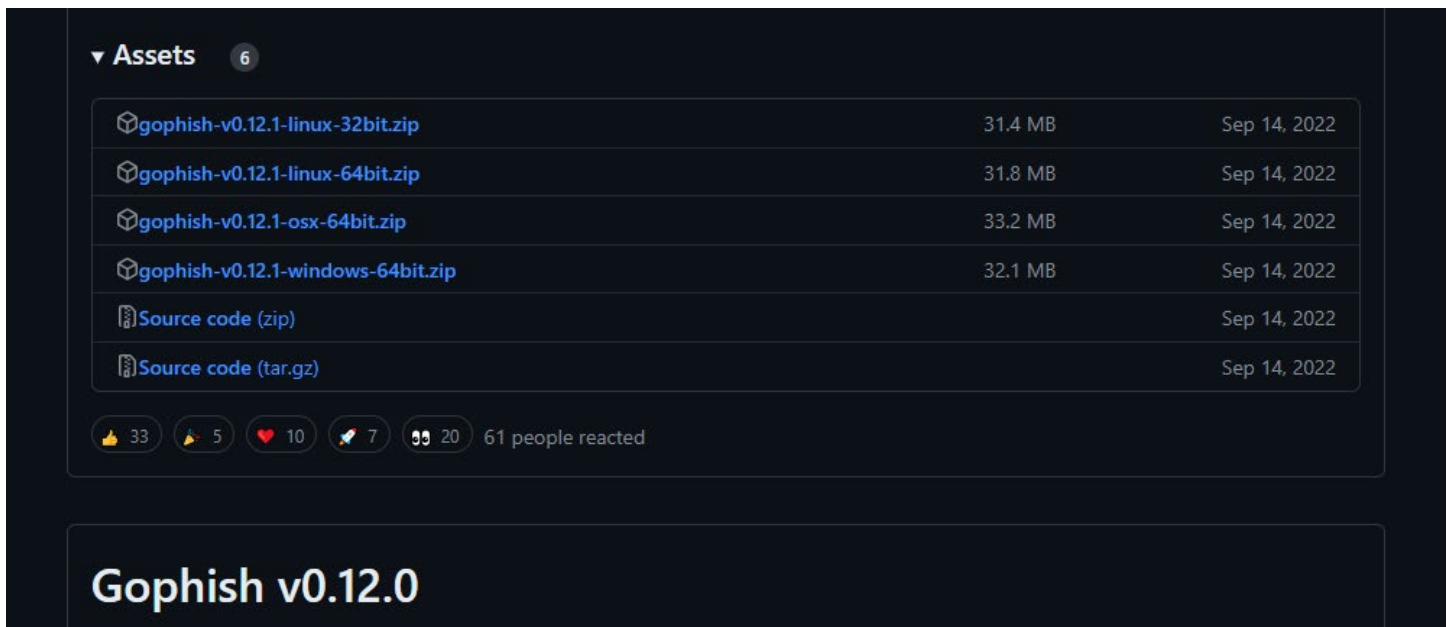
Sophos Email employs advanced machine learning and real-time scanning to protect orgs. against phishing and BEC attacks. It detects targeted impersonation, blocks phishing indicators, and provides pre- and post-delivery protection against malicious links and malware. Additionally, it offers a Search and Destroy feature to automatically remove threats from Office 365 mailboxes.



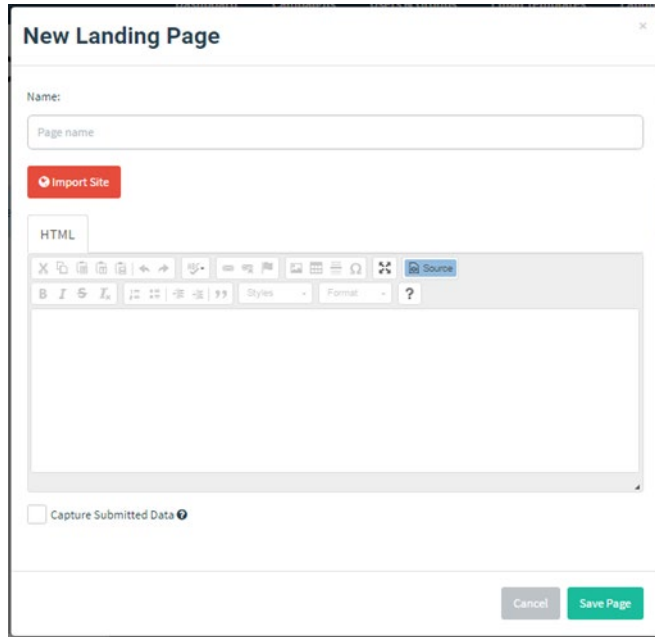
## GoPhish Set up

GoPhish is a user-friendly open-source platform designed for phishing testing within organizations. With an intuitive web-based interface, it offers professional-grade features like real-time reporting and results.

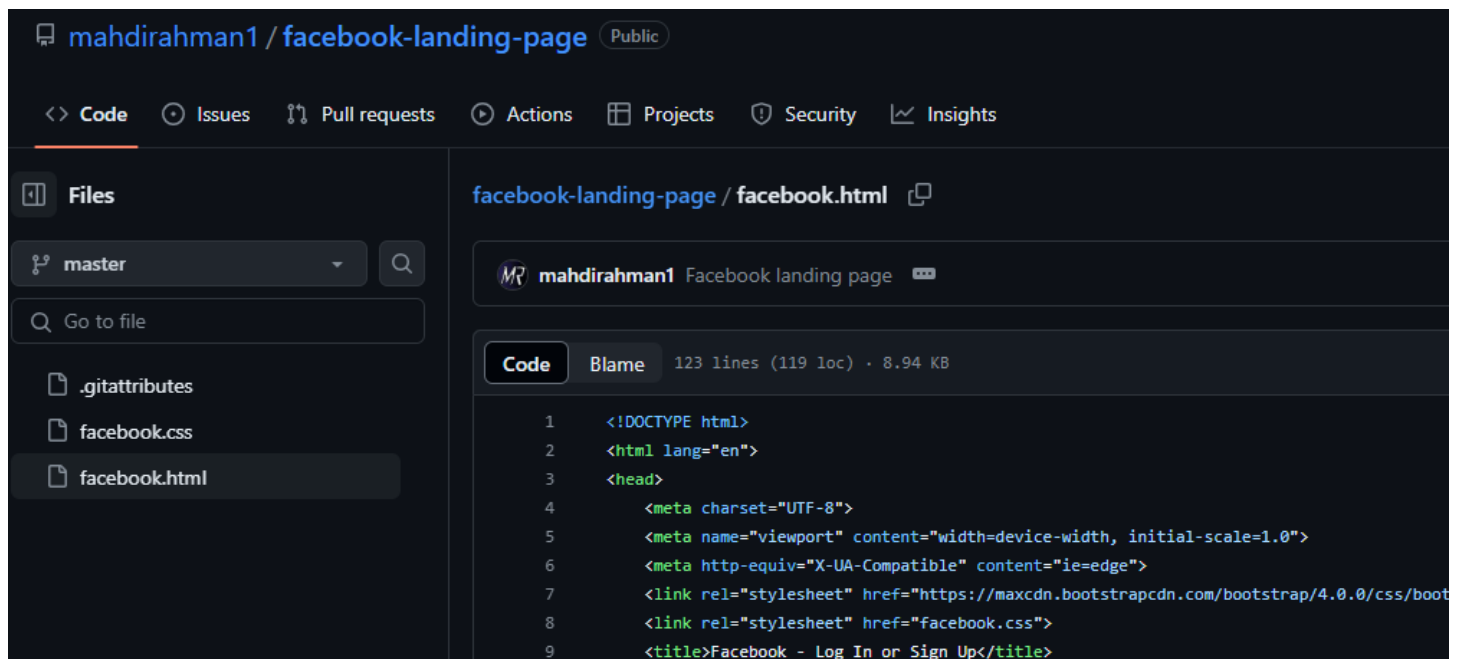
1. To set up GoPhish on your Windows host, start by visiting <https://github.com/gophish/gophish/releases> and downloading the latest Windows release. Once downloaded, extract the GoPhish package to a folder of your choice on the local drive. To initiate the GoPhish service, simply double click on "gophish.exe," which will open a command prompt indicating that a webserver has been launched on your local machine at <https://localhost:3333>. The command prompt will also provide admin credentials, prompting you to log in with the username "admin" and a randomly generated password. After the initial login, GoPhish will guide you through creating your personalized password for the admin user. Now that Gophish is set up let's dive into the sections within GoPhish.



2. Landing page: Creating landing pages in GoPhish is a straightforward process that allows you to customize HTML pages for users who click on phishing links. These pages support templating, credential capture, and user redirection after submitting credentials. To preview a landing page, use the HTML editor or launch a test campaign by browsing directly to the GoPhish listener. To get started, click on "Landing Pages" in the sidebar and select the "New Page" button. With this user-friendly interface, designing effective landing pages for phishing simulations becomes an accessible task. The HTML codes for commonly used websites such as Facebook, twitter (X), Spotify , etc. are found in GitHub. Here's a landing page example:



The capturing submitted data checkbox is utilized to help capture credentials from the landing page.



```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <meta http-equiv="X-UA-Compatible" content="ie=edge">
7   <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/boot
8   <link rel="stylesheet" href="facebook.css">
9   <title>Facebook - Log In or Sign Up</title>
```

Example of a Facebook landing page template that can be found on GitHub.

- # New Template

Name:
 

Example

Import Email

Subject:
 

Password Reset for {{FirstName}}

Text

HTML

**B** *I* S *I<sub>x</sub>*

Styles

Normal

Dear {{FirstName}} {{LastName}},

The password for ({{Email}}) has expired. Please reset your password [here](#).

Regards,

IT Department

---

The contents of this email are confidential and may be legally privileged. This email is solely for the intended recipient only. If you are not the intended recipient, please notify us at the earliest

body p

☒ Add Tracking Image

+ Add Files

Show
 

10

 entries
 Search:

Name

No data available in table

Showing 0 to 0 of 0 entries
 

Previous

Next

- # New Sending Profile
- Name:
- contact@
- Interface Type:
- SMTP
- From:
- contact@
- Host:
- smtp.gmail.com:587
- Username:
- contact@
- Password:
- \*\*\*\*\*
- ☒ Ignore Certificate Errors ?

5. **Users & Groups:** This is where you are going to create the list of your targeted users and groups by going to “Users & Groups” and selecting “New Group”. Here you can specify the first and last name of your targeted users along with their email address and position withing the organization. It also gives you the option to import users from a CSV file in the case of targeting a larger audience.

6. Finally, setting up a campaign which will utilize all these sections into one. Here you choose which groups emails should be sent out to, as well as which email templates, landing pages, and sending profiles are used. The sections within the campaign are going to look like the ones provided in the figures shown:

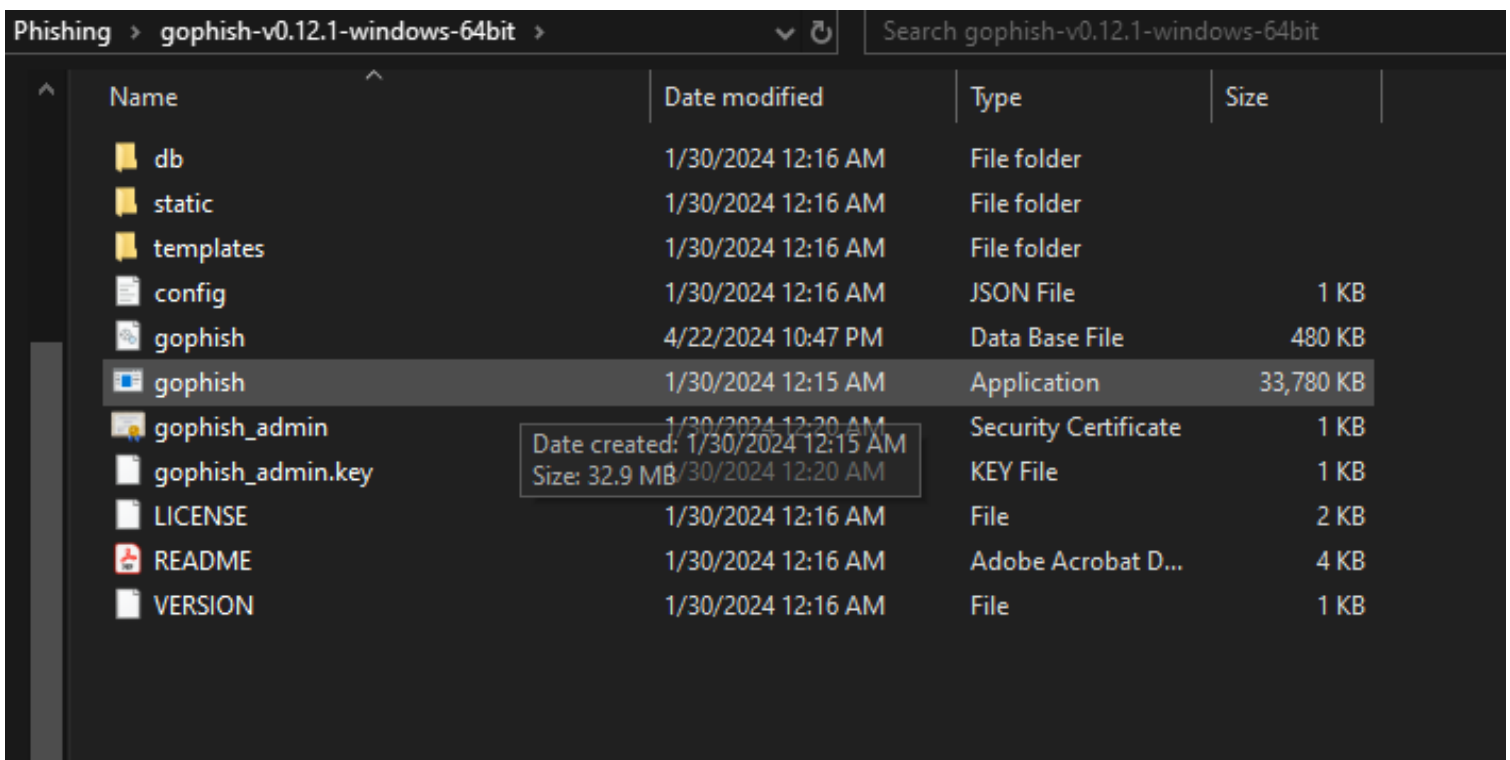
- **Name** - The name of the campaign
- **Email Template** - The email that is sent to campaign recipients. This is created in the [Email Templates](#) section of the documentation.
- **Landing Page** - The HTML that is returned when a recipient clicks the link in the email template. This is created in the [Landing Pages](#) section of the documentation.
- **URL** - This is the URL that populates the {{URL}} template value, commonly used in email templates. This should be a URL or IP address that points to the GoPhish phishing server and is reachable by the recipient.
- **Launch Date** - This is the date that the campaign will begin. See [Scheduling Campaigns](#) for more information.
- **Send Emails By** - This is the date all emails will be sent by. See [Scheduling Campaigns](#) for more information.
- **Sending Profile** - This is the SMTP configuration to use when sending emails. This is created in the [Sending Profiles](#) section of the documentation.
- **Groups** - This defines which groups of recipients should be included in the campaign.



## GoPhish Campaign Test

### 1. Download and Installation:

- I downloaded the latest Windows release of GoPhish. After downloading, I extracted the GoPhish package to my class folder on my Windows host. To launch the GoPhish service, I simply double-clicked on "gophish.exe," which launched a webserver at <https://localhost:3333>. Admin credentials were provided for initial login (username: "admin" with a randomly generated password which related on was changed to my own choice).



Phishing > gophish-v0.12.1-windows-64bit > Search gophish-v0.12.1-windows-64bit				
Name	Date modified	Type	Size	
db	1/30/2024 12:16 AM	File folder		
static	1/30/2024 12:16 AM	File folder		
templates	1/30/2024 12:16 AM	File folder		
config	1/30/2024 12:16 AM	JSON File	1 KB	
gophish	4/22/2024 10:47 PM	Data Base File	480 KB	
gophish	1/30/2024 12:15 AM	Application	33,780 KB	
gophish_admin	1/30/2024 12:20 AM	Security Certificate	1 KB	
gophish_admin.key	1/30/2024 12:20 AM	KEY File	1 KB	
LICENSE	1/30/2024 12:16 AM	File	2 KB	
README	1/30/2024 12:16 AM	Adobe Acrobat D...	4 KB	
VERSION	1/30/2024 12:16 AM	File	1 KB	

## 2. Landing Page Creation:

- I designed a customized HTML landing page within GoPhish to simulate FedEx delivery tracking. I utilized templating and redirection features, directing users to a phishing awareness page upon submission that teaches users how to spot a phishing email.

### Edit Landing Page

Name:

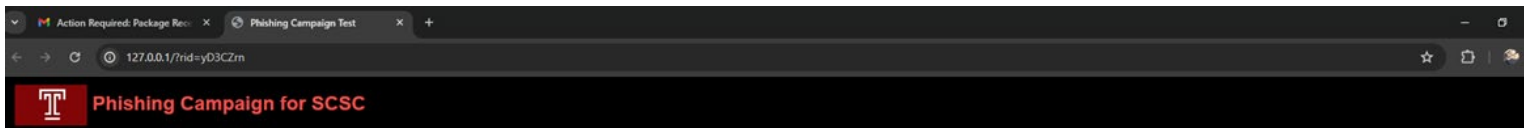
Your Package Pickup

Import Site

HTML

```
<html lang="en"><head>
  <title>COMAPNY Phishing</title>
  <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css"/>
  <style>
    .header{
      background-color: #000;
    }
  </style>
</head>
<body>
  <div class="header">
    <div class="container">
      <div class="row">
        <div class="col-md-12">
          <h1>Phishing Campaign for SCSC</h1>
        </div>
      </div>
    </div>
  </div>
  <div class="content">
    <div class="container">
      <div class="row">
        <div class="col-md-12">
          <div class="text-center">
            <p>You clicked on a simulated phishing test.</p>
            <p>Here are some tips to help you stay safer in the future</p>
          </div>
          <div class="row">
            <div class="col-md-33">
              <div class="text-center">
                <p>Tip: #1</p>
                <p>Stop, Look, Think</p>
                <p>Did anything look out of the ordinary? Did you recognize the spelling mistakes? Did you recognize the senders email address?</p>
                <div class="border p-5">
                  Your Package Pickup <admin@yourpackagepic
                </div>
              </div>
            </div>
            <div class="col-md-33">
              <div class="text-center">
                <p>Tip: #2</p>
                <p>Do you spot a red flag?</p>
                <p>When receiving any email from an external sender, there's always a caution message at the very top. Do you see this banner?</p>
                <img alt="Screenshot of Outlook showing a caution banner for a native external sender." data-bbox="430 808 610 850"/>
              </div>
            </div>
            <div class="col-md-33">
              <div class="text-center">
                <p>Tip: #3</p>
                <p>When in doubt throw it out</p>
                <p>If you ever think that an email is suspicious it is better to err on the side of caution. Forward it to abuse@temple.edu</p>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>
</body>
</html>
```

☐ Capture Submitted Data ?



You clicked on a simulated phishing test.  
Here are some tips to help you stay safer in the future

#### Tip: #1

##### Stop, Look, Think

Did anything look out of the ordinary? Did you recognize the spelling mistakes? Did you recognize the senders email address?

Your Package Pickup <admin@yourpackagepic

#### Tip: #2

##### Do you spot a red flag?

When receiving any email from an external sender, there's always a caution message at the very top. Do you see this banner?



#### Tip: #3

##### When in doubt throw it out

If you ever think that an email is suspicious it is better to err on the side of caution. Forward it to abuse@temple.edu


### 3. Email Template Setup:


- In the “Email Templates” section, I created a FedEx delivery phishing email template in HTML format that mimics legitimate FedEx notifications, urging immediate action to click the link.

# Edit Template

Name:

Package Pickup

 Import Email


Envelope Sender: 

admin@yourpackagepickup.com

Subject:

Action Required: Package Received

Text HTML




```
<body>
<div align="center"></div>

<p><font face="Verdana">Dear {{.Email}},</font></p>

<p><font face="Verdana"><font face="Verdana">You've received a package! Your
company has enrolled you in "Your Package Pickup" to simplify the mailroom process
and get your package to you fast.</font></font></p>
```

☐ Add Tracking Image

 Add Files



Dear Omar,

You've received a package! Your company has enrolled you in "Your Package Pickup" to simplify the mailroom process and get your package to you fast!

The details of your package are as follows:

**Type:** Parcel  
**Carrier:** Fed Ex  
**Tracking Number:** 231300687629630  
**Method:** 2-Day Express Saver  
**Origin:** Philadelphia, PA

TO get started, you'll need to log into your account. It only takes a minute to get going - you can use your corporate e-mail credentials to log in.

Set up your account now!

Your Username: Omar

<https://www.yourpackagepickup.com/pickup>

Once you've set up your account online, you'll select how you'd like to receive your package. It's really that easy!

Let us know if you have any issues with your shipment at <https://www.yourpackagepickup.com/track>

Best,  
Your Package Pickup Care Team  
[admin@yourpackagepickup.com](mailto:admin@yourpackagepickup.com)

Here's the email content:

“Dear Omar,

You've received a package! Your company has enrolled you in "Your Package Pickup" to simplify the mailroom process and get your package to you fast!

The details of your package are as follows:

**Type:** Parcel  
**Carrier:** Fed Ex  
**Tracking Number:** 231300687629630  
**Method:** 2-Day Express Saver  
**Origin:** Philadelphia, PA

TO get started, you'll need to log into your account. It only takes a minute to get going - you can use your corporate e-mail credentials to log in.

Set up your account now!

Your Username: Omar

<https://www.yourpackagepickup.com/pickup>”



#### 4. Sending Profile Configuration:

- I configured a sending profile using my Gmail account for sending FedEx phishing emails. Ensuring the "from" section contained a valid email address, I utilized Gmail's SMTP host (smtp.gmail.com:465).

### Edit Sending Profile

Name:

Interface Type:

SMTP

SMTP From: ?

Host:

Username:

Password:

☒ Ignore Certificate Errors ?

Email Headers:

YourPackagePickup

admin@yourpackagepicku

+ Add Custom Header

Show  entries

Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

Previous

Next

Send Test Email

5. **Users & Groups Management:**

- As the sole user for testing purposes, I created a single user profile in the “Users & Groups” section. I specified details such as name, email address (mine), and position (target recipient) within the organization.

### Edit Group

Name:

Phished

+ Bulk Import Users

Download CSV Template

First Nam

Last Nam

Email

Position

+ Add

Show 

10

 entries

Search:

First Name	Last Name	Email	Position
Omar	Alzubair	omz101199@g...	IT

Showing 1 to 1 of 1 entries

Previous

1

Next

Close

Save changes

6. **Campaign Setup:**

- I combined all sections into a comprehensive FedEx delivery phishing campaign. Customizing target groups, email templates, landing pages, and sending profiles accordingly, I configured campaign parameters to simulate a realistic phishing scenario. The timeline shows the activity of the emails sent from the moment the campaign is created to when the user clicks on the link and in some cases provide his user credentials.

### Details

Show 

10

 entries

First Name	Last Name	Email	Position
Omar	Alzubair	omz101199@gmail.com	IT

#### Timeline for Omar Alzubair

Email: omz101199@gmail.com  
Result ID: hzzUjRl

Campaign Created

April 22nd 2024 10:15:06 pm

Email Sent

April 22nd 2024 10:15:09 pm

# New Campaign

Name:

Your Package|Pickup Campaign

Email Template:

Package Pickup

Landing Page:

Your Package Pickup

URL: ?

http://127.0.0.1:80

Launch Date

April 22nd 2024, 10:13 pm

Send Emails By (Optional) ?

Sending Profile:

Your Package Pickup

Send Test Email

Groups:

× Phished

Close

Launch Campaign

### Note on Testing Limitations:

Testing outside the local machine is not feasible due to connection restrictions, limiting access to the local host. As the sole user, testing is restricted to my host machine. Collaborative testing with colleagues is only possible through a LAN network connection.

## Access Control Models

**Access Control Models:** A framework encompassing the management and restriction of access to an organization's infrastructure once user identity has been authenticated. Implementing these models is critical as they mitigate the risk of unauthorized access to valuable organizational assets. Here are four types of access control systems:

### **Mandatory Access Control (MAC):**

In MAC, access controls are determined and enforced by the system or data owner, with end-users having no control over system configurations. This model includes two security frameworks:

**Biba:** Focused on maintaining Integrity within the CIA triad, this model allows users with lower clearance levels to read information with higher clearance, while users with higher clearance can only write to lower clearance levels.

**Bell - LaPadula:** Emphasizing confidentiality, this model restricts users at higher clearance levels to write only at their level but allows them to read at their level and below. It is commonly used to enforce the principle of least privilege.

### **Role Based Access Control (RBAC):**

RBAC assigns permissions based on users' roles within the organization, streamlining access management by predefining permissions for each role rather than individually assigning permissions to users.

### **Discretionary Access Control (DAC):**

In DAC, access decisions are delegated to the system or data owner, who grants authority to determine resource access and actions. This model empowers individuals to maintain control over their own objects and associated files/programs.

### **Lattice-based Access Control (LBAC):**

LBAC manages access rights within a system using a lattice structure, assigning each user a unique combination of permissions akin to a unique key. This structure ensures data integrity and availability by preventing unauthorized access to data.

After assessing these access control models and their respective designs, Role Based Access Control emerges as the most suitable option for countering phishing threats. Its scalability, simplicity, and adherence to the principle of least privilege make it highly effective in reducing the impact of phishing incidents. By assigning permissions based on predefined roles, RBAC limits the scope of an attack if a user's account is compromised, thereby mitigating potential damages caused by phishing attacks. RBAC provides a structured and organized approach to access management, enhancing resilience against the risks posed by phishing attacks.



## Employee Training


Before delving into the specifics of conducting training campaigns, it's crucial to underscore the importance of employee training in combating phishing attacks. Employee training serves as a frontline defense against cyber threats, particularly phishing, which often relies on human error or lack of awareness to succeed. Effective training programs equip employees with the knowledge and skills needed to recognize phishing attempts, thereby reducing the likelihood of falling victim to such attacks. By educating employees on common phishing tactics, red flags to watch out for, and best practices for responding to suspicious emails or messages, organizations can significantly mitigate the risk of data breaches, financial losses, and reputational damage. Here's a general procedure on how to go about these training campaigns:


- 1. Phishing Campaign:** Implement a well-structured phishing campaign along with smishing and vishing scenarios to test employee's ability to identify and report phishing attacks.
- 2. Data analysis:** After results are generated, review the results of these tests to identify patterns and areas of weaknesses withing the employees, categorize the attacks that were most successful. Generate a report that details the findings with metrics showing the success percentage of different types of attacks and what department had the most successful mitigation.
- 3. Training:** Once results are gathered, develop a tailored training program that addresses the types of attacks that were most successful and targets the weaknesses that each user experienced. Also make it a habit to hold cyber security awareness seminars throughout the area that includes regular training and updates on the latest phishing strategies.
- 4. Policies:** Review and improve any security policies that might have had a flaw and were discovered during the phishing campaign, ensure that it aligns with the latest and best industry standards that satisfies the organization's needs.
- 5. Technology implementation:** Just like the policies, make sure to implement robust technical solutions to the systems that were exposed during the campaign such as email filtering to better prevent these attacks.
- 6. Summary Report:** Generate a summary report and present these findings and updates to your stakeholders and senior management, emphasizing the importance of finance in staying consistent with these employee trainings and ongoing cybersecurity development.

Statistics on phishing attacks for the year 2023 by PhishProtection and the effectiveness of security trainings on employees picking out phishing emails:

**PhishProtection.**


**KEY PHISHING STATISTICS FOR 2023**


 **22%** of phishing emails contained hacks


**80%** of organizations experienced at least one severe cloud security incident 


**“ ”** **\$4.9 million** costliest attack costs to recover from a phishing attack.

- 1** **1 out of 4,200** emails sent is a phishing scam email.
- 2** **277 days** to detect a data breach in their organizations
- 3** **83%** of phishing sites used Domain Validated (DV) SSL Certificates

 **11%** **11%** of phishing emails contained malware

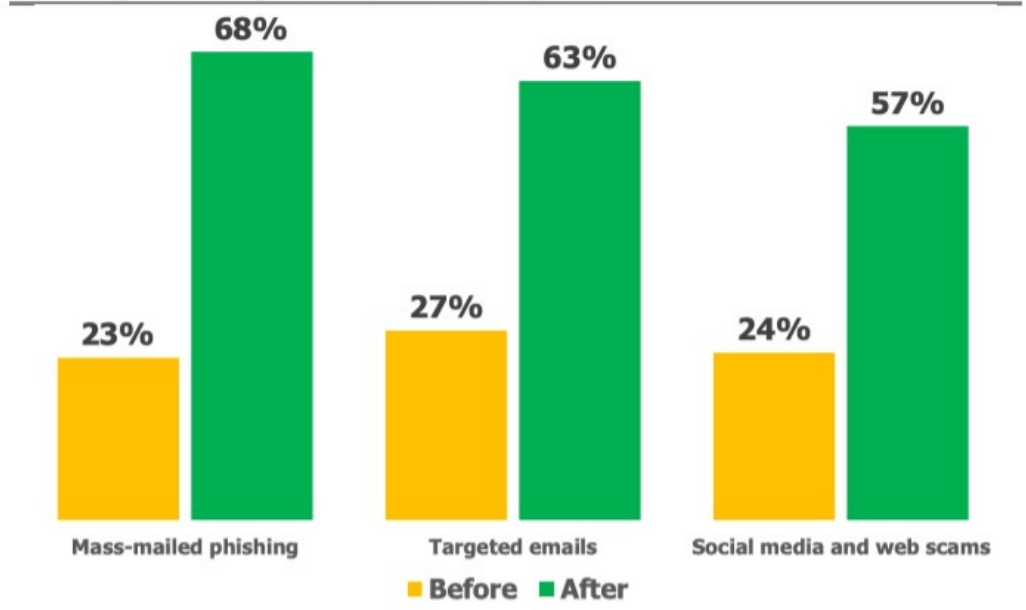
 **36%** **36%** of all data breaches in 2022 involved phishing.

 **48%** **48%** of emails sent in 2022 were spam.

 **83%** **83%** of UK businesses suffered a phishing attack.

**PhishProtection**  
5965 Village Way Suite 105-234, San Diego, CA 92130.  
Phone: +1-855-647-4474 (USA), +44-808-168-7042 (GB).  
[www.phishprotection.com](http://www.phishprotection.com)

**Perceived Ability of Employees at Recognizing Various Threats Before and After Security Awareness Training**  
Percentage Indicating "Capable" or "Very Capable"



Source: Osterman Research, Inc.

## Employee training tools and guides:

- **Phishing box (test)** : <https://www.phishingbox.com/phishing-test>
- **Microsoft phishing awareness video** : <https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>
- **Spiceworks training test**: <https://community.spiceworks.com/t/free-phishing-stress-test-and-employee-training/801374>

## Security Mechanisms

### Security Mechanisms

According to NIST glossary collection, security mechanism is defined as “a device or function designed to provide one or more security services usually rated in terms of strength of service and assurance of the design.” In phishing, this can refer to the various techniques and services used to prevent or mitigate the risks of phishing attacks or social engineering. E.g. 2FA (2 factor authentication), encryption protocols and anti-phishing software.”

### Authentication

To ensure that user's access is not compromised and is accessed by the authorized individual. Verifying the authenticity of the user is crucial in protecting the confidentiality of user's personal information and sensitive information on their social media accounts. These verifications protect individuals against data breaches and identity theft and create trust and integrity among users.

Implementing the MFA helps enhance security by adding an extra security layer of protection above the password level. This forces the user to provide different forms of verification, such as a combination of passwords and a timed passcode that regenerates every new session. This combination ensures that even if the password gets compromised, the adversary will still need access to the passcode to bypass the second form of verification, making it more complicated. There're other forms of MFA such as phone/ SMS verification but they relatively offer the same form of extra security which reduces the likelihood of unauthorized access.

### Email Security

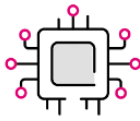


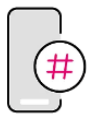

Email security offers a range of tools and techniques to minimize phishing emails and filter out unwanted potential harmful emails. These technologies are designed to detect and filter out any suspicious emails and malware induced messages. For example, Outlook security controls offer encryption for emails, MFA and a built-in malware and spam detection filter. With the advancements of LLM, machine learning is used to generate algorithms that can be used to learn from previous phishing email's patterns and used to detect future attempts. Additionally, frameworks such as SPF, DKIM AND DMARC are frameworks and tools that work hand in hand checks to verify the authenticity of an email, where SPF checks all the emails to ensure that they are all coming from the chosen trusted domain before getting to the recipient. DKIM uses cryptography as a form of authentication to check that an email is coming from someone who has a verified private key and is verified by the mail server. DMARC is the final step where the organization tailors it to their needs, for example they can implement a policy where emails that fail the DKIM verification are rejected.

### Social Media Platforms Security

Ensuring that social media privacy settings are configured and tailored to the user's needs is critical to protect users' information and their online presence. Social media platforms offer us a unique set of settings that we can modify to control the visibility of our profiles, posts, and other personal information. Limiting access to one's profile and restricting the content the general audience can see provides an initial step in reducing smishing attacks and identity thefts. Social media social engineered attacks usually rely on psychological factors, that's why education users about these techniques are important to help them become more aware in detecting impersonations and scams. Combining these two factors strengthen the users' online profiles and maintain security while enjoying their social media content.

## Utilization of Applications like Scam Shield by T-Mobile

Vishing is one of the most common attacks nowadays that is being exploitable for their lack of security. With the emergency of AI and LLM, attackers can use tools to impersonate users' voice which can be used for identity theft. T-Mobile implemented a secure mobile application 'Scam Shield', which offers users a range of robust features. One of the most interesting features is real-time caller ID. This feature allows users to see detailed information about the incoming call and rationalize about whether to answer or decline it based on their experience with previous calls. Additionally, users can report scam calls which are then stored in a database which consequently be used in the future to detect scam calls and alert the users about it before they answer it as a notification. This smooth integration which integrated with the network supplier, uses advanced technologies within the network to protect their consumers from vishing attacks which creates trust between the users and the suppliers. This mechanism should be implemented by every mobile carrier with their databases linked to a secure network to provide larger coverage. Here's the features offered by T-Mobile on their website:

 <p><b>Advanced network technology.</b></p> <p>Our supercharged network analyzes every call using A.I., machine learning, and patented technologies. And our defenses update every six minutes to stay ahead of scammers.</p>	 <p><b>Built-in Scam Block protection.</b></p> <p>With built-in protection technologies, you can keep scammers away with Scam ID, Scam Block, and Scam Counter that identify and help stop them—before you ever get the call.</p> <p><small>Qual's service &amp; capable device req'd. Turning on Scam Block might block calls you want; disable any time.</small></p>	
 <p><b>Know who's calling with free Caller ID.</b></p> <p>With full Caller ID access, you can reduce unidentified calls by displaying a caller's information, even if they're not in your contact list. You can also see if a call is in a spam category such as telemarketing. All you need to do is enable it in the app.</p> <p><small>Qual's service &amp; capable device req'd.</small></p>	 <p><b>Keep your personal number personal.</b></p> <p>Scam Shield gives you an extra PROXY number that you can use when you don't want to share your private phone number. Need to change your number? You can for free—for any reason—up to one time per year.</p> <p><small>Qual's service &amp; capable device req'd. 1 per account; may be cancelled for non-use. In some circumstances, access to 911 may be limited. See DIGITS Terms of Use for additional 911 information.</small></p>	 <p><b>Report scam calls.</b></p> <p>Help protect everyone from scam calls, spam calls, and robocalls with Scam Reporting. Identify suspicious callers or fraudsters and help prevent their calls from being received by you—or others—in the future.</p>



## Conclusion

The widespread phishing attacks in today's digital landscape, as highlighted by Charles Griffiths, emphasizes the critical need for proactive measures to combat this threat. Phishing, encompassing various techniques such as vishing, smishing, and spear phishing, exploits human psychology through social engineering tactics, posing significant risks to individuals and organizations.

The initiative within the Student-Run Cybersecurity Services Center (SCSC) to address phishing attacks, including vishing and social media phishing, is a commendable step towards strengthening cybersecurity defenses within the educational sector. By raising awareness and implementing comprehensive training programs, the project aims to empower organizational members to recognize and mitigate social engineering attacks effectively.

The utilization of AI and LLMs in cyber-attack strategies highlights the evolving techniques of phishing attacks. However, by implementing robust security mechanisms such as Multi-Factor Authentication (MFA), email filtering, and social media privacy settings, organizations and individuals can significantly mitigate the risks posed by phishing threats.

Furthermore, the deployment of open-source tools like GoPhish for phishing testing within organizations, coupled with employee training and awareness campaigns, serves as a frontline defense against phishing attacks. By fostering a culture of cybersecurity awareness and vigilance, organizations can effectively mitigate the impact of phishing incidents and safeguard sensitive information. Since it's an open-source platform, which means it's freely available for anyone to use and modify. This aligns perfectly with our mission at the cybersecurity center to provide accessible cybersecurity solutions. Additionally, GoPhish is flexible and allows us to tailor our campaigns to specific scenarios and adapt to evolving cyber threats.

Considering the dynamic nature of cyber threats, continuous evaluation, and enhancement of security measures, along with ongoing employee training and policy improvements, are essential for maintaining robustness against phishing attacks. Through collaborative efforts and proactive measures, we can collectively strengthen our defenses and mitigate the risks posed by phishing in today's digital landscape.

## Glossary

- NIST SP800-171: A set of security controls and guidelines outlined by the National Institute of Standards and Technology (NIST) to enhance the cybersecurity posture of organizations, focusing on protecting sensitive information.
- Security Breach: Unauthorized access or compromise of sensitive information, leading to potential exploitation, fraud, or other malicious activities.
- Phishing: A cyberattack method where attackers use deceptive emails, messages, or websites to trick individuals into divulging sensitive information, such as usernames and passwords.
- MFA (Multi-Factor Authentication): An additional layer of security requiring users to verify their identity through multiple means, reducing the risk of unauthorized access even if credentials are compromised.
- Smishing: A form of phishing attack conducted through SMS or social media, where attackers attempt to trick individuals into revealing sensitive information.
- Social Engineering: Manipulative techniques used by attackers to deceive individuals into disclosing confidential information or performing actions that may compromise security.
- Access controls: Security measures that limit and regulate access to systems or data, often following the principle of least privilege, where employees only have access to the information necessary for their job.
- Transaction Anomaly Detection System: A security system designed to identify irregularities or suspicious patterns in financial transactions, helping to detect and prevent fraudulent activities.
- Email Filtering: The process of automatically sorting and blocking emails based on predefined criteria to prevent phishing emails and malicious content from reaching recipients.
- Authentication Mechanisms: Methods and technologies used to verify the identity of users or systems, enhancing the security of communication channels, and preventing unauthorized access.
- Cybersecurity Infrastructure: The combination of hardware, software, and processes designed to protect an organization's digital assets and information from cyber threats.
- Email security: Measures and protocols implemented to safeguard email communication channels, preventing the delivery of phishing emails and enhancing overall security.
- Hyperlink embedded: A link within electronic content, such as an email or webpage, that directs the user to another location when clicked.

- Artificial Intelligence: the development of computer systems capable of performing tasks that typically require human intelligence, encompassing problem-solving, learning, and adaptation.
- Large language model (LLM): an artificial intelligence model characterized by its extensive pre-training on vast textual data, possessing millions or billions of parameters, enabling it to understand and generate human-like language for diverse natural language processing tasks.
- Framework: A structure that provides a base and the foundation for a system or concept.
- Access control: The process of regulating the access to information by determining who or what can access this data and what actions can be taken.
- End-user: The user and the consumer of a product or service.
- Mitigation: The action taken to reduce the damage and impact of a threat, in our case to prevent damage done by cyber-attacks.

## References

- Paycheck Spear Phishing Emails Target UDel Employees | Secure UD Threat Alerts. 13 Aug. 2015, [sites.udel.edu/threat/2015/08/13/paycheck-spear-phishing-emails-target-udel-employees](https://sites.udel.edu/threat/2015/08/13/paycheck-spear-phishing-emails-target-udel-employees).
- Brad. "Why Is Phishing Awareness Training Important for Employees? - PhishProtection.com." PhishProtection.com, 9 Oct. 2023, [www.phishprotection.com/phishing-awareness/why-is-phishing-awareness-training-important-for-employees](https://www.phishprotection.com/phishing-awareness/why-is-phishing-awareness-training-important-for-employees).
- CrowdStrike. "How to Implement Phishing Attack Awareness Training." crowdstrike.com, 22 Jan. 2024, [www.crowdstrike.com/cybersecurity-101/phishing/phishing-attack-awareness-training](https://www.crowdstrike.com/cybersecurity-101/phishing/phishing-attack-awareness-training).
- Usecure. "How effective is security awareness training?"blog.usecure.io, <https://blog.usecure.io/does-security-awareness-training-work>
- Imber, Daniel. "The Latest Phishing Statistics (Updated April 2024) | AAG IT Support." AAG IT Services, 8 Apr. 2024, [aag-it.com/the-latest-phishing-statistics](https://aag-it.com/the-latest-phishing-statistics).
- Adam, Sally. "Get AI-powered Phishing Protection With Sophos Email." Sophos News, 2 Sept. 2021, [news.sophos.com/en-us/2021/08/26/get-ai-powered-phishing-protection-with-sophos-email](https://news.sophos.com/en-us/2021/08/26/get-ai-powered-phishing-protection-with-sophos-email).
- T-Mobile® Scam Shield App – Block Scam and Unwanted Calls (Free & Premium). [www.t-mobile.com/benefits/scam-shield](https://www.t-mobile.com/benefits/scam-shield).
- Campaigns | Gophish User Guide. docs.getgophish.com/user-guide/documentation/campaigns.
- Gophish. "GitHub - Gophish/Gophish: Open-Source Phishing Toolkit." GitHub, [github.com/gophish/gophish](https://github.com/gophish/gophish).
- Sutarwala, Umme. 10 Best Practices for Social Media Security. 22 Aug. 2023, [www.sprinklr.com/blog/social-media-security-best-practices](https://www.sprinklr.com/blog/social-media-security-best-practices).
- What Is Email Filtering? Definition and Examples | Darktrace. darktrace.com/cyber-ai-glossary/email-filtering.
- GfG. "Types of Security Mechanism." GeeksforGeeks, 10 Sept. 2020, [www.geeksforgeeks.org/types-of-security-mechanism](https://www.geeksforgeeks.org/types-of-security-mechanism).
- Brad. "Invest in Phishing Awareness Training for Your Employees - PhishProtection.com." PhishProtection.com, 1 Aug. 2023, [www.phishprotection.com/products/phishing-awareness-training](https://www.phishprotection.com/products/phishing-awareness-training).
- FreeZeroDays. GoPhish-Templates/Landing\_Pages at Master · FreeZeroDays/GoPhish-Templates · GitHub. [github.com/FreeZeroDays/GoPhish-Templates/tree/master/Landing\\_Pages](https://github.com/FreeZeroDays/GoPhish-Templates/tree/master/Landing_Pages).