

DIGITAL EMPOWERMENT NETWORK

INTERSHIP REPORT

WEEK#05



PRESENTED BY ALIZA JAVED
CID DEN10161

CONTENTS

1. About The Company
2. Identifying Phishing Emails
3. Introduction to Phishing Emails
4. Creating Phishing Emails
5. How To Prevent Phishing Emails
6. Conclusion

ABOUT THE COMPANY

At Digital Empowerment Network, we are dedicated to empowering Pakistan's university students through a wide range of initiatives that foster leadership, academic growth, and technical expertise. By bridging the digital divide with workshops, coding camps, and hackathons, we equip students with essential skills to thrive in the modern workforce. Our commitment to education extends beyond the classroom, as we reinvest proceeds from our revenue-generating partnerships into impactful programs and charitable initiatives, providing resources and support to underserved communities. We believe in the power of education to create well-rounded individuals who can drive innovation and make a positive impact on society.

IDENTIFYING PHISHING EMAILS

1.Objective:

Identify phishing emails.

2.Description:

How will you identify it and how can you create such phishing emails which are hard to identify as phishing.

3.Key Steps:

- Identify phishing emails.
- Create phishing emails.
- Spread awareness about phishing emails.

INTRODUCTION TO PHISHING EMAILS

Phishing emails are one of the most common and dangerous methods used by cybercriminals to deceive individuals and organizations into divulging sensitive information. These emails typically masquerade as legitimate messages from trusted entities, such as banks, online services, or even colleagues, aiming to trick the recipient into performing actions that compromise security. The purpose of phishing attacks is often to steal login credentials, personal information, or financial data, which can then be used to commit fraud, identity theft, or further attacks on organizations.

Phishing emails have evolved significantly over time. Early phishing attempts were often easy to spot due to poorly written messages, obvious fake URLs, or unprofessional formats. However, today's phishing emails are far more sophisticated, with attackers often investing time and resources to create highly convincing messages. These emails may include official logos, well-written content, and links that appear legitimate at first glance. The intent is to manipulate human psychology, typically by creating a sense of urgency or fear, such as threatening to close an account or warning of an unauthorized transaction. This pressure causes recipients to act hastily, often clicking on malicious links or providing personal information without careful consideration.

One of the most concerning aspects of phishing is its versatility and wide reach. Phishing emails can be sent to thousands of potential victims in a matter of seconds. Attackers may target specific individuals through spear phishing, a more personalized form of attack that incorporates details about the recipient to make the email seem more trustworthy.

Given the growing sophistication of phishing attacks, it is crucial for individuals and organizations to be aware of how to identify and protect themselves against these threats. Spotting phishing attempts often involves looking for telltale signs such as suspicious email addresses, requests for personal information, unsolicited attachments, or links that do not match the company's official website. Additionally, organizations must prioritize employee education and implement email security measures to detect and block phishing attempts before they reach inboxes.









CREATING PHISHING EMAILS

Demonstration using gophish:

- Install gophish for windows.

 [gophish-v0.12.1-windows-64bit.zip](#)


- Extract the files and open gophish application.

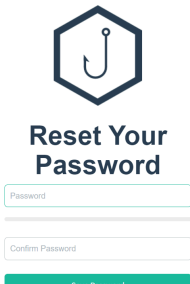
 config	10/9/2024 1:56 PM	JSON Source File	1 KB
 LICENSE	10/9/2024 1:56 PM	File	2 KB
 README	10/9/2024 1:56 PM	Markdown Source ...	4 KB
 VERSION	10/9/2024 1:56 PM	File	1 KB
 gophish	10/9/2024 1:56 PM	Application	33,780 KB
 templates	10/9/2024 1:56 PM	File folder	
 db	10/9/2024 1:56 PM	File folder	
 static	10/9/2024 1:56 PM	File folder	

- Sign in to gophish using the username and password provided default in the gophish application.

```
C:\Users\Aliza J\Downloads>g
OK 20180223101813.0.5.1_user_reporting.sql
OK 20180524203752.0.7.0_result_last_modified.sql
OK 20180527213648.0.7.0_store_email_request.sql
OK 20180830215615.0.7.0_send_by_date.sql
OK 20190105192341.0.8.0_rbac.sql
OK 20191104103306.0.9.0_create_webhooks.sql
OK 20200116000000.0.9.0_imap.sql
OK 20200619000000.0.11.0_password_policy.sql
OK 20200730000000.0.11.0_imap_ignore_cert_errors.sql
OK 20200914000000.0.11.0_last_login.sql
OK 20201201000000.0.11.0_account_locked.sql
OK 20220321133237.0.4.1_envelope_sender.sql
time="2024-10-09T13:56:52+05:00" level=info msg="Please login with the username admin and
the password 6c4accbe00913e6c"
time="2024-10-09T13:56:52+05:00" level=info msg="Background Worker Started Successfully -
Waiting for Campaigns"
time="2024-10-09T13:56:52+05:00" level=info msg="Starting phishing server at http://0.0.0
.0:80"
time="2024-10-09T13:56:52+05:00" level=info msg="Starting IMAP monitor manager"
time="2024-10-09T13:56:52+05:00" level=info msg="Creating new self-signed certificates fo
r administration interface"
time="2024-10-09T13:56:52+05:00" level=info msg="Starting new IMAP monitor for user admin
"
time="2024-10-09T13:56:52+05:00" level=info msg="TLS Certificate Generation complete"
time="2024-10-09T13:56:52+05:00" level=info msg="Starting admin server at https://127.0.0
```

- Reset the default password.

 gophish admin



- Create a new sending profile and enter the details.

New Sending Profile ✕

Name:

Interface Type:

SMTP

SMTP From: ?

Host:

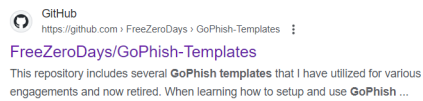
Username:

Password:

☒ Ignore Certificate Errors ?

Email Headers:

- For email template, go to github and type giphish templates and open it.



- Open the repository and open the landing pages and copy the html code for the email.

GoPhish-Templates / Landing_Pages / Instagram_Landing_Page.html

FreeZeroDays Rename Instagram Landing Page.html to Instagram_Landing_Page.html 86895ff · 2 years ago History

Code Blame 123 lines (123 loc) · 9.43 KB Code 55% faster with GitHub Copilot

```

1 <div dir="ltr" style="margin: 0; padding: 0;">
2   <table id="m_-7319109037895721555email_table" style="border-collapse: collapse;" border="0" width="100%" cellpadding="0">
3     <tbody>
4       <tr>
5         <td id="m_-7319109037895721555email_content" style="font-family: Helvetica Neue,Helvetica,Lucida Grande,tahoma,verdana,arial,sans-serif; background: #f
6           <table style="border-collapse: collapse;" width="100%" cellpadding="0">
7             <tbody>
8               <tr>
9                 <td style="line-height: 20px;" colspan="3" height="20">&nbsp;</td>
10              </tr>
11             <tr>
12               <td style="line-height: 1px;" colspan="3" height="1">&nbsp;</td>
13             </tr>
14           </tbody>
15         </td>
16       </tr>
17     </tbody>
18   </table>
19 </div>

```


- Paste into the html section of the email template and do the changes accordingly and save them.

New Template

Name:

Instagram Login

[Import Email](#)

Envelope Sender: 

Subject:

Urgent Action Required

Text HTML

823013

If this wasn't you, please [reset your password](#) to secure your account.


© Instagram Menlo Park CA 94022

- For landing pages, copy the code for the landing page of instagram and paste the html code and allow the checkbox for capturing data and passwords. Also enter the original url of the instagram to redirect and save the changes.

B I S Ix [Icons] Styles Format


Instagram

Phone number, username, or email

☒ Capture Submitted Data 

☒ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: 

<https://instagram.com>

Cancel Save Page

- Create a new group and save the changes after adding the details.

New Group ×

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

Show entries Search:

First Name	Last Name	Email	Position
No data available in table			

Showing 0 to 0 of 0 entries

[Previous](#) [Next](#)

[Close](#) [Save changes](#)

- Create a new campaign, schedule the phishing attack and launch the attack.

Name:

Email Template:

Landing Page:

URL:

Launch Date:

Sending Profile:

Groups:

[Close](#) [Launch Campaign](#)

Are you sure?

This will schedule the campaign to be launched.

[Cancel](#) [Launch](#)

- The dashboard will now look like this.

Admin

[Dashboard](#)
[Campaigns](#)
[Users & Groups](#)
[Email Templates](#)
[Landing Pages](#)
[Sending Profiles](#)
[Account Settings](#)
[User Management](#)
[Webhooks](#)
[User Guide](#)
[API Documentation](#)

Email Sent

0

Email Opened

0

Clicked Link

0

Submitted Data

0

Email Reported

0

Details

Show entries Search:

First Name	Last Name	Email	Position	Status	Reported
Aliza	Javed	javed@company.com		Scheduled	

Showing 1 to 1 of 1 entries

[Previous](#) [1](#) [Next](#)

- The target will now get an phishing email that appears to be the legitimate instagram login page.

Urgent Action Required: Suspicious activity on your Instagram Account - Hi Aliza, Someone tried to log in to your Instagram...

00:05



Hi Aliza,

Someone tried to log in to your Instagram account.

If this was you, please use the following code to log in:

823013

If this wasn't you, please [reset your password](#) to secure your account.

© Instagram, Menlo Park, CA 94022

This message was sent to [Aliza](#) and intended for [alicia.____in@gmail.com](#). Not your account? [Remove your email](#) from this account.

- If the target clicks on the reset password option it is redirected to the phishing website that gets the credentials of the user and redirects to the original instagram page.

HOW TO PREVENT PHISHING EMAILS

Phishing emails are one of the most common cyber threats, designed to trick recipients into revealing sensitive information like passwords, credit card numbers, or even installing malware. The key to preventing phishing attacks lies in a combination of awareness, technical controls, and good email hygiene. Here are a few effective strategies to help safeguard yourself and your organization from phishing threats.

1. Recognize the Signs of Phishing

The first line of defense against phishing is to recognize suspicious emails. Phishing emails often look legitimate, mimicking well-known organizations or individuals. Key red flags include spelling or grammatical mistakes, generic greetings (like "Dear Customer"), a sense of urgency ("Your account will be suspended"), or links that don't match the sender's official domain. Always hover over links to inspect the URL before clicking, and be cautious of any unexpected attachments or requests for personal information.

2. Use Multi-Factor Authentication (MFA)

Even if an attacker manages to steal your credentials through a phishing attack, multi-factor authentication (MFA) can stop them from gaining access to your accounts. MFA requires a second form of verification, such as a text message code or fingerprint scan, adding an extra layer of security. Implementing MFA across personal and organizational accounts drastically reduces the effectiveness of phishing attacks.

3. Keep Software Updated

Outdated software can be a gateway for phishing attacks. Cybercriminals often exploit vulnerabilities in old software versions to install malware or access sensitive data. Regularly update your operating system, browsers, and email clients, as well as install patches for security vulnerabilities to protect yourself against such attacks. Most updates contain security fixes that close the gaps exploited by cybercriminals.

4. Implement Email Security Solutions

Technical controls are also crucial for phishing prevention. Deploy advanced email filters to automatically detect and block phishing emails before they reach users. Many modern email security solutions use machine learning to identify patterns common in phishing attempts, such as malicious links or attachments. Additionally, enabling anti-phishing and anti-spam tools in email clients provides an extra layer of protection.

5. Educate Employees

For organizations, conducting regular phishing awareness training is essential. Employees should be educated on how phishing attacks work, what to look out for, and how to report suspicious emails. Simulated phishing exercises can help employees practice identifying these threats without the risk of real-world consequences. This reduces the likelihood of falling victim to an actual phishing attack.

6. Avoid Clicking on Links in Unsolicited Emails

If an email looks suspicious or asks for sensitive information, do not click any links it contains. Instead, visit the official website directly by typing the URL into the browser or using a trusted bookmark. Phishing emails often direct users to counterfeit websites where login credentials are harvested. By avoiding these links, you can avoid entering personal details on malicious websites.

7. Verify Email Senders

When in doubt, verify the authenticity of the email by contacting the sender through a different medium, such as calling their official phone number or using another trusted communication method. Cybercriminals often impersonate legitimate entities or coworkers, but a quick verification can help you avoid falling victim to phishing.

CONCLUSION

In conclusion, in my fifth week at the Digital Empowerment Network, I gained invaluable insights into phishing attacks, from identifying and simulating phishing emails to implementing prevention strategies. This experience not only deepened my technical understanding of how phishing attempts are constructed but also sharpened my ability to anticipate and mitigate these cyber threats. By mastering phishing detection techniques and learning about critical defenses such as multi-factor authentication, software updates, and employee training, I am now better equipped to protect both individuals and organizations from these attacks.

The practical skills I've acquired, including the ability to create realistic phishing simulations, have provided me with a hands-on understanding of the tactics used by cybercriminals. This has further enhanced my awareness of the importance of vigilance, education, and advanced security measures in maintaining strong cybersecurity defenses. Moving forward, I plan to continue building on these foundational skills, applying them to real-world scenarios, and contributing to creating safer digital environments in my future cybersecurity career.