Phishing Awareness Simulation
For
Deerfield Beach Police Department
By

DEERGUARD

DEFENDERS

Cyber Security Intern

Aadith Preetham (C0902681)

Submission: 7 Feb 2025

Table of Contents

Introduction

Purpose

This report contains details of a phishing attack simulation as part of cybersecurity training exercises for the Deerfield Beach Police Department to raise awareness about the dangers of cyber threats. The simulation was inspired by a real-world phishing incident reported by the Supreme Court of India, where attackers attempted to steal sensitive information via fraudulent emails. By replicating a similar scenario within a controlled environment, this exercise aimed to educate staff on recognizing and mitigating phishing threats.The goal was to analyze and demonstrate common phishing techniques, assess user understanding and educate staff on recognizing and preventing cyber threats.

Scope

This simulation involved creating phishing emails from a fake email ID that was created by Deerfield Beach Police Department's IT Department and a cloned website that looked and worked exactly like LinkedIn to mimic a real-world cyber incident.

Definitions

1. Phishing: A cybercrime where attackers use fraudulent messages to deceive individuals into providing sensitive information, such as login credentials.
2. Social Engineering: The use of manipulation to exploit human error for unauthorized access or data theft.
3. Credential Harvesting: The process of stealing usernames and passwords through deceptive means, often via fake websites.
4. Malicious Link: A URL that leads to a fraudulent website designed to deceive users and steal their data.
5. Clone Website: A duplicate of a legitimate website, often used by attackers to trick users into providing sensitive information.
6. Email Spoofing: The creation of email messages with a forged sender address to mislead the recipient into trusting the message.
7. Two-Factor Authentication (2FA): An additional layer of security that requires not only a password and username but also something that only the user has on them, such as a physical token or mobile app verification.
8. IP Logging: The process of recording the Internet Protocol (IP) addresses of users to track their locations and actions.
9. Awareness Training: A program designed to educate employees about recognizing and responding to cybersecurity threats.

Real-World Case Study Reference

Recently, the Supreme Court of India flagged a phishing attack where emails impersonated official communications, aiming to steal sensitive data. The incident highlighted the sophistication of modern phishing methods and underscored the importance of awareness and prevention.

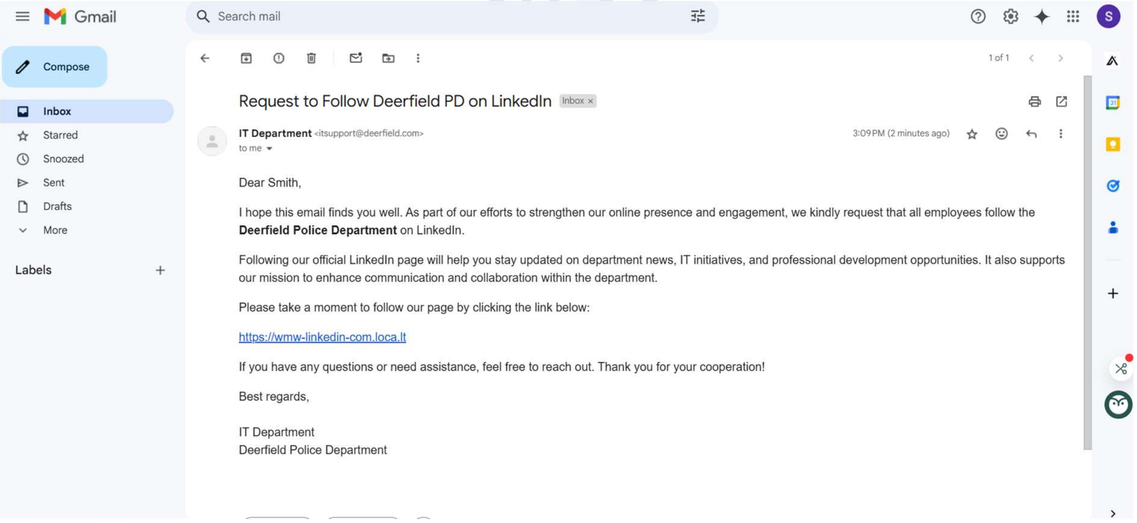
This simulation incorporated:

- Realistic email designs to mimic trusted sources.
- A cloned website that mirrored LinkedIn’s login interface.
- Tactics inspired by the Supreme Court incident to enhance relevance and impact.

How it was planned

Phishing Emails

Emails were crafted to appear as official IT Department communications, encouraging recipients to connect with the department’s LinkedIn profile.



Request to Follow Deerfield PD on LinkedIn Inbox ×

IT Department <itsupport@deerfield.com>
to me
3:09 PM (2 minutes ago)

Dear Smith,

I hope this email finds you well. As part of our efforts to strengthen our online presence and engagement, we kindly request that all employees follow the **Deerfield Police Department** on LinkedIn.

Following our official LinkedIn page will help you stay updated on department news, IT initiatives, and professional development opportunities. It also supports our mission to enhance communication and collaboration within the department.

Please take a moment to follow our page by clicking the link below:

https://wmw-linkedin-com.loca.lt

If you have any questions or need assistance, feel free to reach out. Thank you for your cooperation!

Best regards,

IT Department
Deerfield Police Department

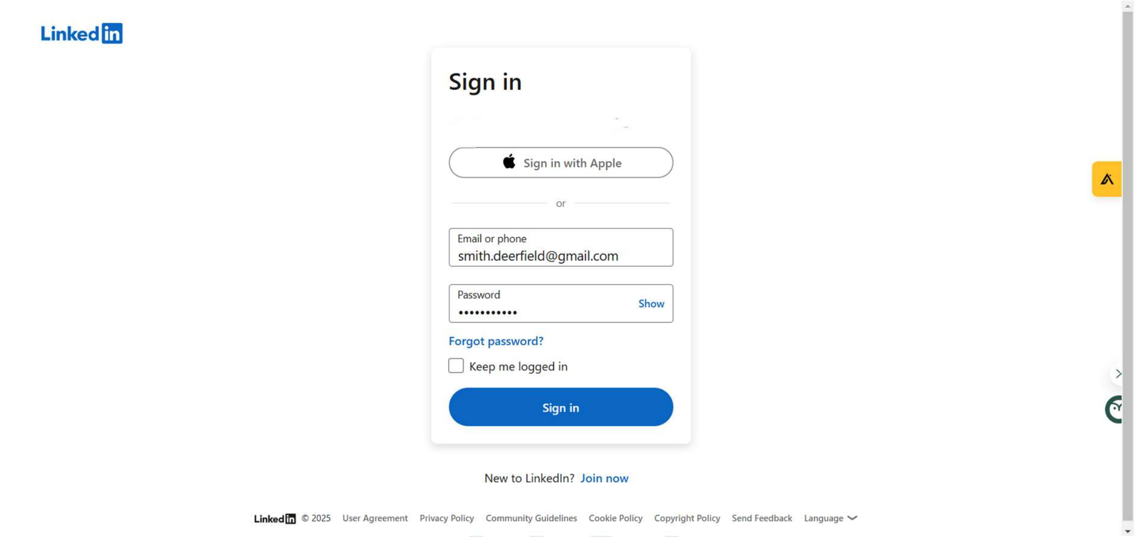
Fig 1: Email sent to DBPD staff members

Key Characteristics:

- Subject Line: "Request to Follow Deerfield PD on LinkedIn."
- Sender Address: itsupport@deerfield.com.
- Email Content: A formal tone urging employees to click a link and connect.
- Malicious Link: https://wmw-linkedin-com.loca.lt.

Cloned LinkedIn Website

A cloned LinkedIn login page was developed to collect user credentials. The page mimicked the original platform's branding and functionality.



Sign in

Email or phone
smith.deerfield@gmail.com

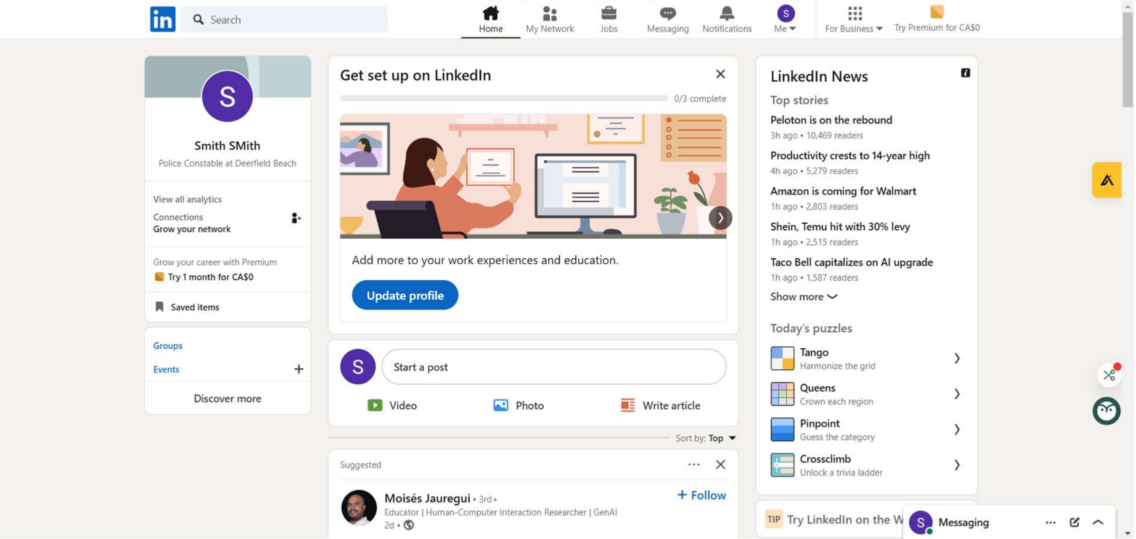
Password
•••••••••••

☐ Keep me logged in

New to LinkedIn? Join now

Linked in
Sign in with Apple
or
Show
Forgot password?
Sign in
Linked in © 2025 User Agreement Privacy Policy Community Guidelines Cookie Policy Copyright Policy Send Feedback Language

Fig 2: Login page for the cloned website



Smith SMith
Police Constable at Deerfield Beach

Get set up on LinkedIn
0/3 complete
Add more to your work experiences and education.

LinkedIn News
Top stories
Peloton is on the rebound
3h ago • 10,469 readers
Productivity crests to 14-year high
4h ago • 5,279 readers
Amazon is coming for Walmart
1h ago • 2,803 readers
Shein, Temu hit with 30% levy
1h ago • 2,515 readers
Taco Bell capitalizes on AI upgrade
1h ago • 1,587 readers

Today's puzzles
Tango – Harmonize the grid
Queens – Crown each region
Pinpoint – Guess the category
Crossclimb – Unlock a trivia ladder

Suggested
Moisés Jauregui • 3rd+
Educator | Human-Computer Interaction Researcher | GenAI
2d •

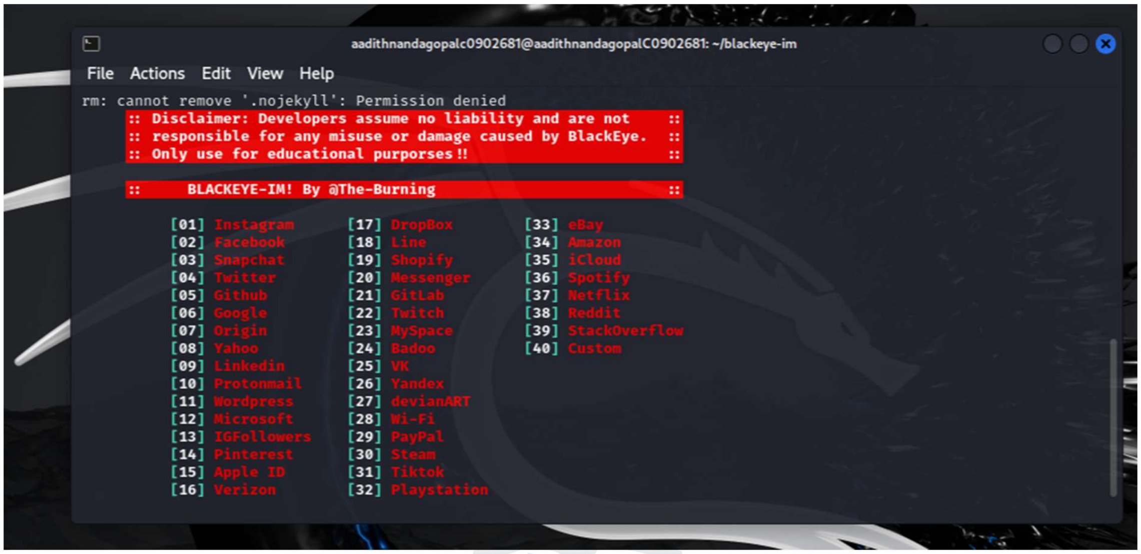
Fig 2: Cloned website on the victim's side

Features:

- Login fields for usernames and passwords.
- Data capture mechanism for storing submitted credentials.
- Slight URL modifications to evade detection.

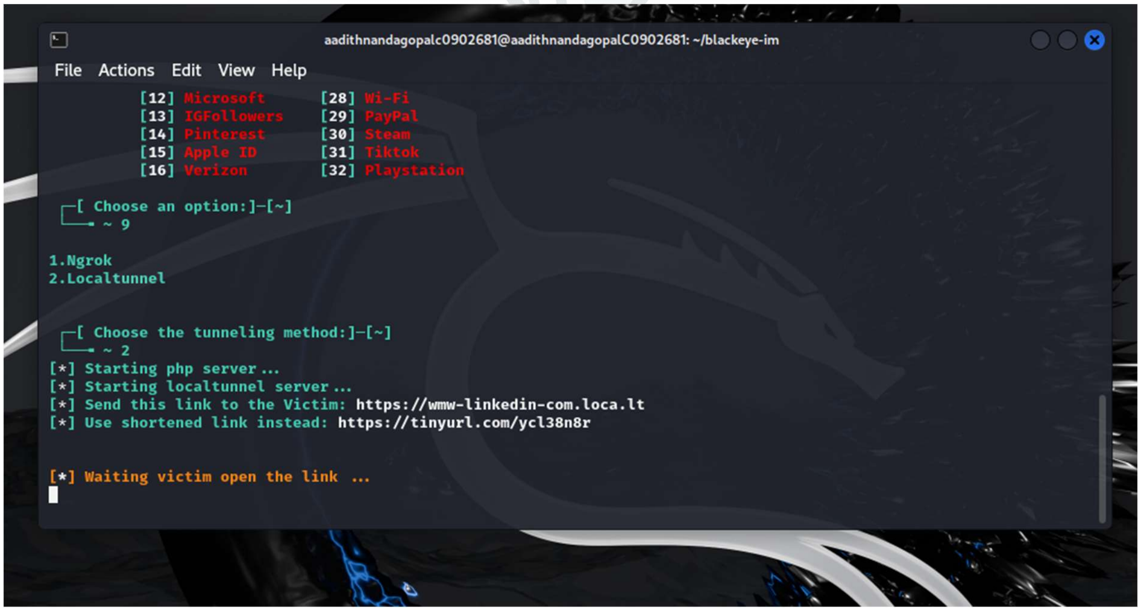
Tools Used

- Blackeye: A phishing toolkit to create a fake website.


aadithnandagopalc0902681@aadithnandagopalC0902681: ~/blackeye-im
File Actions Edit View Help

```
rm: cannot remove '.nojekyll': Permission denied
     :: Disclaimer: Developers assume no liability and are not    ::
     :: responsible for any misuse or damage caused by BlackEye.  ::
     :: Only use for educational purporses !!                     ::

     ::      BLACKEYE-IM! By @The-Burning                         ::

          [01] Instagram        [17] DropBox         [33] eBay
          [02] Facebook         [18] Line            [34] Amazon
          [03] Snapchat         [19] Shopify         [35] iCloud
          [04] Twitter          [20] Messenger       [36] Spotify
          [05] Github           [21] GitLab          [37] Netflix
          [06] Google           [22] Twitch          [38] Reddit
          [07] Origin           [23] MySpace         [39] StackOverflow
          [08] Yahoo            [24] Badoo           [40] Custom
          [09] Linkedin         [25] VK
          [10] Protonmail       [26] Yandex
          [11] Wordpress        [27] devianART
          [12] Microsoft        [28] Wi-Fi
          [13] IGFollowers      [29] PayPal
          [14] Pinterest        [30] Steam
          [15] Apple ID         [31] Tiktok
          [16] Verizon          [32] Playstation
```

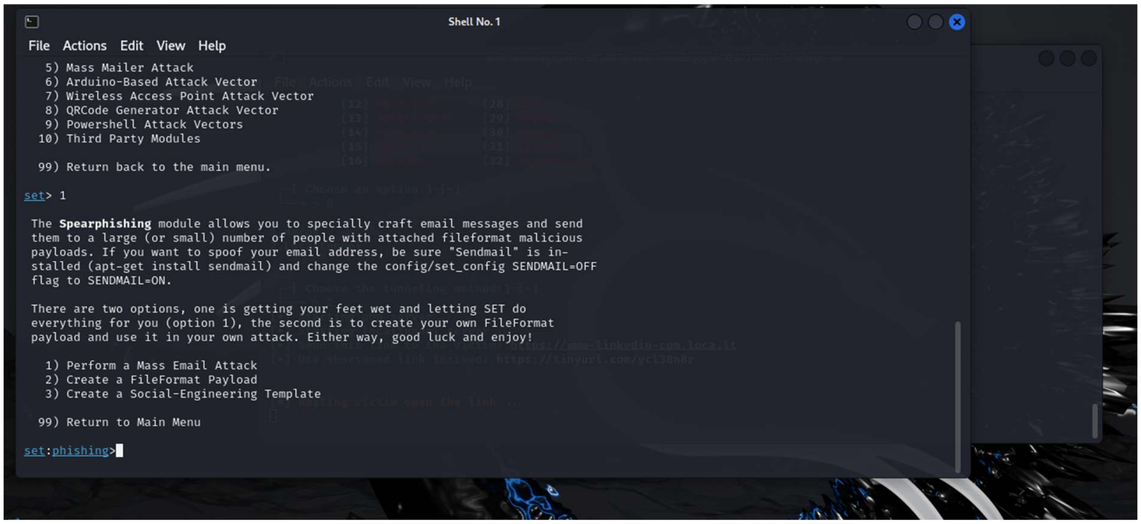
Fig 3: BlackEye toolkit


aadithnandagopalc0902681@aadithnandagopalC0902681: ~/blackeye-im
File Actions Edit View Help

```
          [12] Microsoft        [28] Wi-Fi
          [13] IGFollowers      [29] PayPal
          [14] Pinterest        [30] Steam
          [15] Apple ID         [31] Tiktok
          [16] Verizon          [32] Playstation

  ┌─[ Choose an option:]─[~]
  └──• ~ 9

1.Ngrok
2.Localtunnel


  ┌─[ Choose the tunneling method:]─[~]
  └──• ~ 2
[*] Starting php server ...
[*] Starting localtunnel server ...
[*] Send this link to the Victim: https://wmw-linkedin-com.loca.lt
[*] Use shortened link instead: https://tinyurl.com/ycl38n8r


[*] Waiting victim open the link ...
█
```

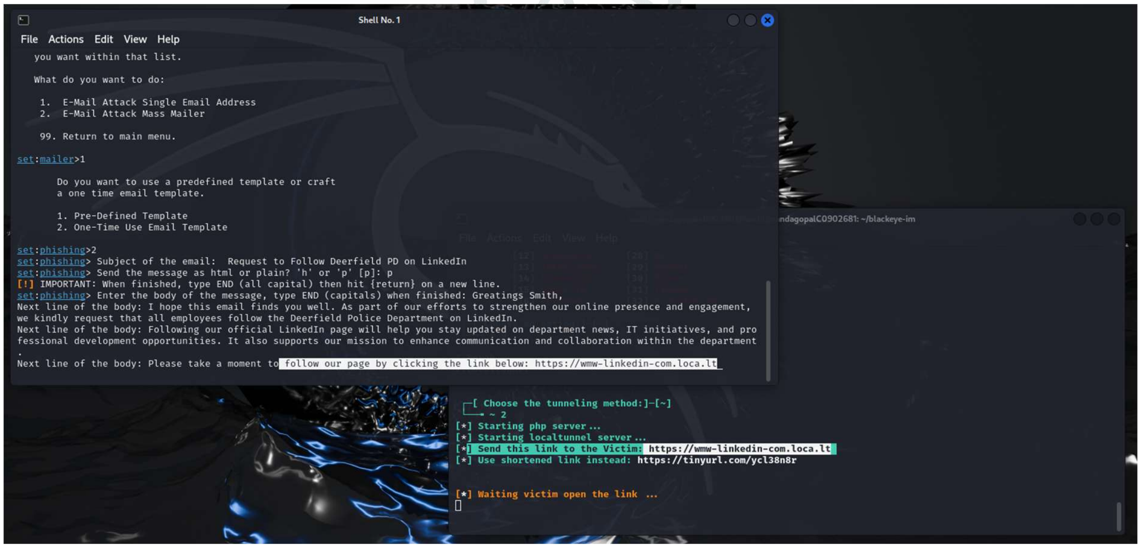
Fig 4: Login page for the cloned website

- LocalTunnel: A service for exposing the site to the internet.



```
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>
```

Fig 5: LocalTunnel



```
   you want within that list.

   What do you want to do:

    1.  E-Mail Attack Single Email Address
    2.  E-Mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>1

       Do you want to use a predefined template or craft
       a one time email template.

       1. Pre-Defined Template
       2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email:  Request to Follow Deerfield PD on LinkedIn
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Greatings Smith,
Next line of the body: I hope this email finds you well. As part of our efforts to strengthen our online presence and engagement,
we kindly request that all employees follow the Deerfield Police Department on LinkedIn.
Next line of the body: Following our official LinkedIn page will help you stay updated on department news, IT initiatives, and pro
fessional development opportunities. It also supports our mission to enhance communication and collaboration within the department
.
Next line of the body: Please take a moment to follow our page by clicking the link below: https://wmw-linkedin-com.loca.lt
```

```
┌─[ Choose the tunneling method:]─[~]
└──• ~ 2
[*] Starting php server ...
[*] Starting localtunnel server ...
[*] Send this link to the Victim: https://wmw-linkedin-com.loca.lt
[*] Use shortened link instead: https://tinyurl.com/ycl38n8r


[*] Waiting victim open the link ...
```

Fig 6: Rearranging details for the victim

Simulation

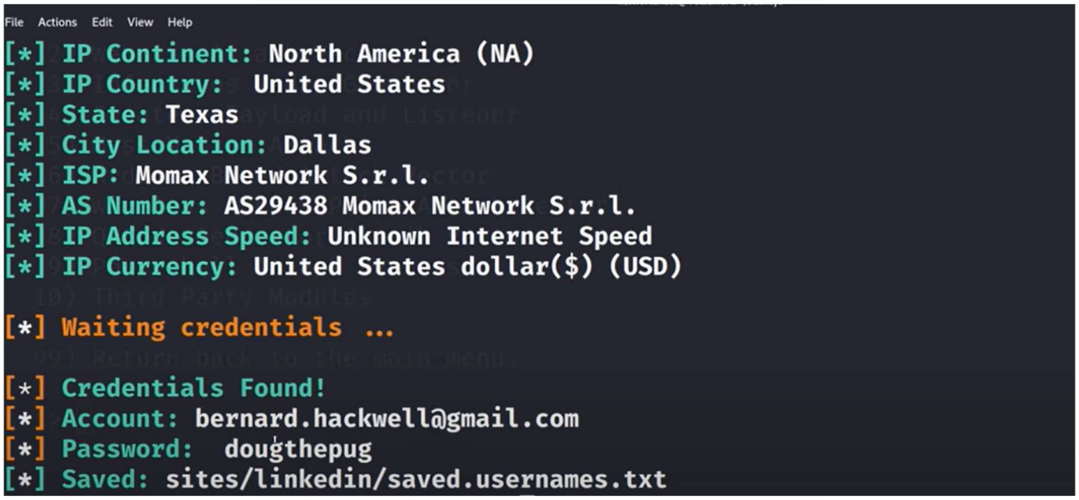
Deployment

The phishing emails were distributed to a controlled group of department staff. The malicious website was hosted via LocalTunnel to facilitate external access.

Monitoring Victim Interaction

Victim engagement was tracked, including:

- Link clicks.
- Credential submissions on the cloned site.
- Logging of IP addresses and geographical data.



```
[*] IP Continent: North America (NA)
[*] IP Country:  United States
[*] State: Texas
[*] City Location: Dallas
[*] ISP: Momax Network S.r.l.
[*] AS Number: AS29438 Momax Network S.r.l.
[*] IP Address Speed: Unknown Internet Speed
[*] IP Currency: United States dollar($) (USD)

[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: bernard.hackwell@gmail.com
[*] Password:  dougthepug
[*] Saved: sites/linkedin/saved.usernames.txt
```

Fig 8: Geographic location and ISP information of the victim

Results

- Emails Sent: 10
- Links Clicked: 7
- Credentials Entered: 4
- Locations Logged: Dallas, Texas, among others.

Findings and Analysis

Vulnerabilities Identified

- Insufficient scrutiny of email sender details.
- Lack of awareness about altered URLs.
- High trust in emails appearing to originate from known entities.

Key Insights

The exercise demonstrated the ease with which phishing attacks can compromise user security. It highlighted a need for enhanced vigilance and training.

Recommendations

Preventive Measures

- Verify email sender addresses and URLs before interacting.
- Hover over links to inspect their destination.
- Enable multi-factor authentication (MFA) for sensitive accounts.
- Regularly update software and maintain strong passwords.

Training Programs

- Conduct regular phishing simulations to evaluate awareness levels.
- Provide step-by-step guides for recognizing phishing attempts.
- Develop a protocol for reporting suspicious emails.

Safety Video

As part of the phishing awareness program, a safety video was created to educate staff on identifying and preventing phishing attacks. The video includes:

- An introduction to phishing and its potential consequences.
- A breakdown of the phishing email and cloned LinkedIn website used in the simulation.
- Steps to verify email authenticity and recognize malicious links.
- Practical cybersecurity tips, such as enabling two-factor authentication and reporting suspicious emails.
- A call to action encouraging employees to stay vigilant and proactive.

The safety video has been uploaded to YouTube for easy access by staff. Please refer to the following link to view the video:

Contact Information

Here’s a contact list for the Deerfield Beach Police Department (DBPD) staff to report phishing emails or potential personal information compromises:

Department Contacts

Role	Name	Title	Phone	Email
Incident Handler (Lead)	Jay Chhanang	Cybersecurity Officer	555-0101	j.chhanang@dbpd.gov
Incident Handler (Backup)	Mishika C.	IT Manager	555-0102	m.chhanang@dbpd.gov
Network	Linda B	Network Engineer	555-0105	l.bray@dbpd.gov
Server	Xytus Joseph	Server Specialist	555-0106	x.joseph@dbpd.gov
Executive	Jishant Acahrya	Chief of Police	555-0108	j.acharya@dbpd.gov

External Contacts

Role	Organization	Name	Title	Phone	Email
Network Security Vendor	TechSecure Solutions	Peter Clark	Support Lead	555-0201	p.clark@techsecure.com
Cyber Insurance Provider	SafeNet Insurance	Amanda White	Account Manager	555-0202	a.white@safenet.com
Legal Counsel	LegalEase Law Firm	Laura Green	Lawyer	555-0203	l.green@legalease.com
Ransomware Response Team	Encryptor Recovery Inc.	Rachel Adams	Recovery Manager	555-0204	r.adams@encryptor.com

Conclusion

This simulation underscored the importance of phishing awareness in mitigating cybersecurity risks. By replicating a real-world incident, the exercise provided practical insights into vulnerabilities and informed strategies to address them. Immediate adoption of the recommended measures will enhance the department’s resilience against future attacks.

References

- Blackeye Phishing Tool in Kali Linux. (2021, November 25). Retrieved from GeeksforGeeks website: https://www.geeksforgeeks.org/blackeye-phishing-tool-in-kali-linux/
- Canadian Centre for Cyber Security. (2020, April 6). Don’t take the bait: Recognize and avoid phishing attacks - ITSAP.00.101. Retrieved from Canadian Centre for Cyber Security website: https://www.cyber.gc.ca/en/guidance/dont-take-bait-recognize-and-avoid-phishing-attacks
- Farrier, E. (2024, March 23). Clone phishing: What it is and how to prevent it - Norton. Retrieved from us.norton.com website: https://us.norton.com/blog/online-scams/clone-phishing
- Mastercard. (2021, March 26). Security Education & Awareness: Phishing Prevention. Retrieved February 6, 2025, from YouTube website: https://www.youtube.com/watch?v=CVJiZIjdOOE
- Microsoft. (2021). Protect yourself from phishing. Retrieved from support.microsoft.com website: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44
- Phishing Awareness Training Campaign - University of Victoria. (2024). Retrieved February 6, 2025, from Uvic.ca website: https://www.uvic.ca/systems/support/informationsecurity/phishing/
- Prakash, S. (2025, January 9). Supreme Court faces phishing attack; flags it to law-enforcement agencies - The Tribune. Retrieved February 6, 2025, from The Tribune website: https://www.tribuneindia.com/news/india/supreme-court-faces-phishing-attack-flags-it-to-law-enforcement-agencies/
- Team, C. (2022, March 8). How To Clone A Website. Retrieved from Codecademy Blog website: https://www.codecademy.com/resources/blog/how-to-clone-a-website/