Project 4: AI in Social Engineering

By: Abel Woldemichael, Joel Castillo Gomez, Eli Parry-Giles, Jada Sweetney, Douglass Thompson

Overview

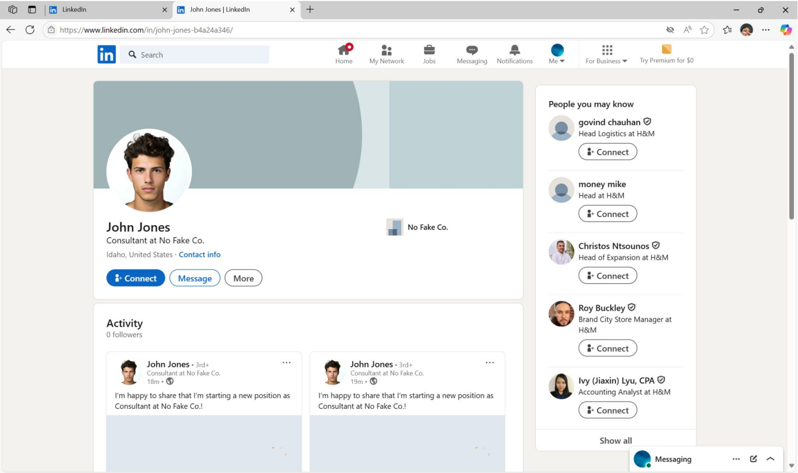
The following years has seen the rise of AI in various usages. Using AI to be able to to fake an person and use it to enact more convincing social engineering and phishing scams have rose in popularity. In this presentation we are going to demonstrate how one can go about using AI in that very scenario. From using AI deepfakes to lure a potential victim, to using AI to extract the victims personal data. We also cover various mitigations strategies and ways a individual or company can go about spotting these types of scams and how to defend against them.

Scenario

Victim: Victim A recently joined a new company called "NoFakeCo." Over the weekend, he received a call from an HR department employee. The call went unanswered, but a voicemail was left. The voicemail stated there was an error in one of his onboarding documents, which would delay his first paycheck. To resolve the issue, Victim A was instructed to respond to an email titled "Please update Onboarding Documents" and log into the company account to update the necessary information.

Reconnaissance

How was the victim’s information obtained? The attacker created a fake profile on LinkedIn to identify potential victims. New employees are often targeted as they are more susceptible to such attacks. The attacker collected the employee’s personal email from their LinkedIn page and performed "Profile Scraping" to identify current employees at the company to impersonate.



https://www.linkedin.com/in/john-jones-b4a24a346/

John Jones

Consultant at No Fake Co.

Idaho, United States · Contact info

No Fake Co.

Activity

0 followers

John Jones · 3rd+
Consultant at No Fake Co.
18m ·

I’m happy to share that I’m starting a new position as Consultant at No Fake Co.!

John Jones · 3rd+
Consultant at No Fake Co.
19m ·

I’m happy to share that I’m starting a new position as Consultant at No Fake Co.!

People you may know

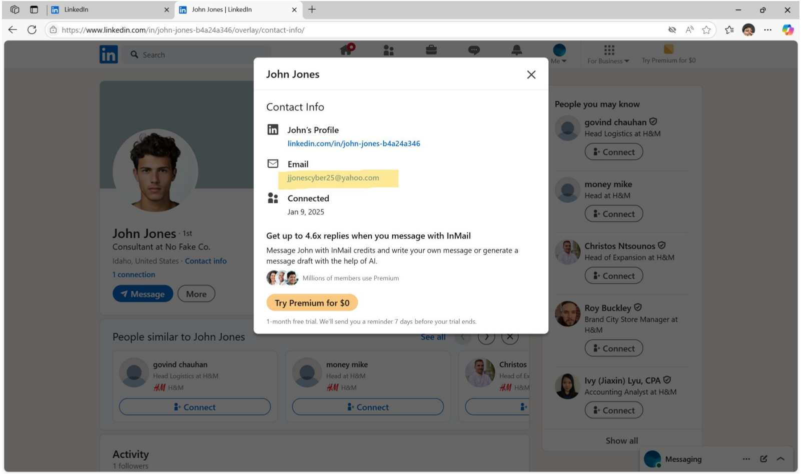
govind chauhan
Head Logistics at H&M

money mike
Head at H&M

Christos Ntsounos
Head of Expansion at H&M

Roy Buckley
Brand City Store Manager at H&M

Ivy (Jiaxin) Lyu, CPA
Accounting Analyst at H&M



https://www.linkedin.com/in/john-jones-b4a24a346/overlay/contact-info/

John Jones

Contact Info

John’s Profile
linkedin.com/in/john-jones-b4a24a346

Email
jjonescyber25@yahoo.com

Connected
Jan 9, 2025

Get up to 4.6x replies when you message with InMail

Message John with InMail credits and write your own message or generate a message draft with the help of AI.

Millions of members use Premium

Try Premium for $0

1-month free trial. We’ll send you a reminder 7 days before your trial ends.

John Jones · 1st
Consultant at No Fake Co.
Idaho, United States · Contact info
1 connection

People similar to John Jones

govind chauhan
Head Logistics at H&M
H&M

money mike
Head at H&M
H&M

Christos
Head of Ex
H&M

Activity
1 followers

People you may know

govind chauhan
Head Logistics at H&M

money mike
Head at H&M

Christos Ntsounos
Head of Expansion at H&M

Roy Buckley
Brand City Store Manager at H&M

Ivy (Jiaxin) Lyu, CPA
Accounting Analyst at H&M

Reconnaissance

Impersonation: The attacker found an HR employee’s (Angela Merc) information and email on their LinkedIn page. The same email was linked to an Instagram, where the attacker obtained photos and videos of the HR employee. This data was then used to create a deep fake voice recording requesting the victim to submit their information.

Reconnaissance - Leonardo.Ai

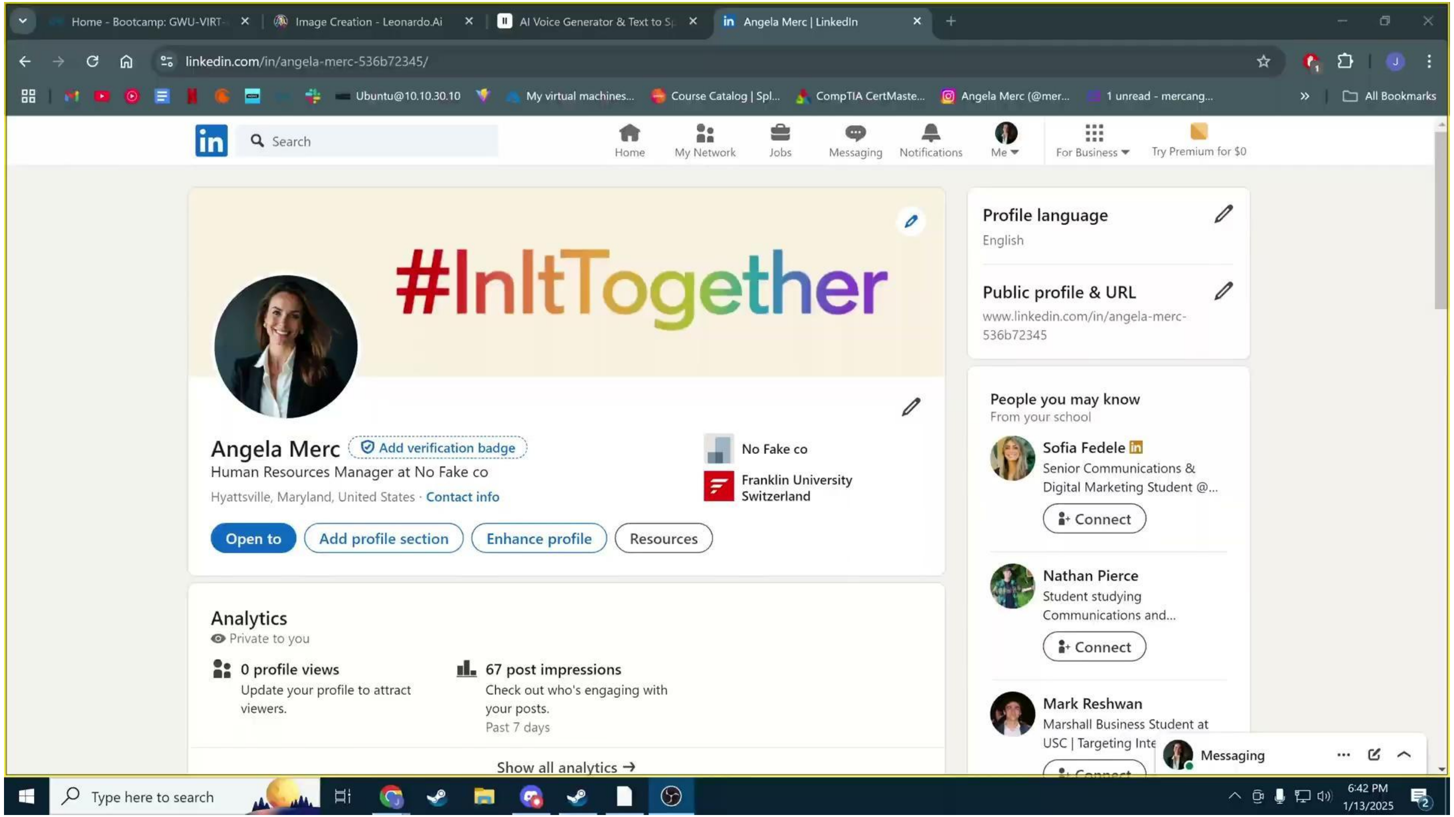
- Leonardo.ai is an ai image platform site that can produce AI generated images and videos. It can do this either from a text prompt, or a image reference.
- It's often used in areas such as graphic design but can also be used by bad actors impersonating someone.
- A free limited plan is available but pricing goes from $10/mo, up to $48/mo.

Reconnaissance - Elevenlabs.io

- Elevenlabs.io is another ai platform that specializes on replicating and generating high quality human-like speech. It uses advanced machine learning models to create realistic voiceovers and is typically used for audiobooks, content creation and accessibility.
- Elevenlabs.io also has a feature called voice cloning, which can take any recording of a voice and replicates it, mimicking the cloned voice.
- Elevenlabs.io includes a free plan without voice cloning, but plans range from $5/mo, up to $99/mo.

*No real person, voice or likeness was used in this presentation

Reconnaissance - Demo



Angela Merc

Human Resources Manager at No Fake co

Hyattsville, Maryland, United States · Contact info

No Fake co

Franklin University Switzerland

Analytics

Private to you

0 profile views

Update your profile to attract viewers.

67 post impressions

Check out who's engaging with your posts.

Past 7 days

Show all analytics →

Profile language

English

Public profile & URL

www.linkedin.com/in/angela-merc-536b72345

People you may know

From your school

Sofia Fedele

Senior Communications & Digital Marketing Student @...

Nathan Pierce

Student studying Communications and...

Mark Reshwan

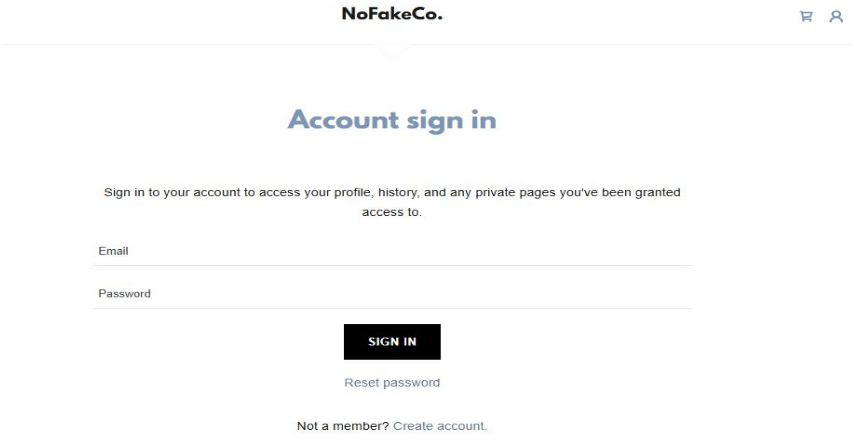
Marshall Business Student at USC | Targeting Inte

The Website

In order to “reel in” our potential victim we went ahead and created a fake, but convincing, looking website

https://nofakeco.godaddysites.com/

Earlier we prompted the victim to login to the website so as we could be able to steal their personal login credentials



Account sign in

Sign in to your account to access your profile, history, and any private pages you've been granted access to.

Email

Password

Not a member? Create account.

The attack

The Attack The attacker needed the victim to open the email and click on the link, which directed them to a fake company page. The victim would then enter their credentials and submit them. Once entered, the attacker would obtain the credentials and potentially access sensitive information about the victim or use other exploits to collect sensitive information about the company itself.

The attack

The Attack used an Open Source Tool called Gophish.

This phishing tool was used to copy the company’s main login page, where the victim can enter their credentials. When sent Gophish is able to retrieve said information and could be exported for potential exploitation.

Booting up Gophish

In a virtual machine running Kali Linux, our attackers downloaded the Open-source Phishing Framework from GoPhish. For this example, we used the `linux-64 bit.zip` file.

The GoPhish tool will be loaded onto your virtual machine as a zip file, which needs to be extracted. Using the terminal, we navigated to our Downloads directory (*cd Downloads/*), located the zip file, and used the extraction command(*tar gophish-v0.12.1-linux-64bit.zip*) . Once extracted, we opened the application and booted it up in the VM. (*./gophish*)

Upon booting, GoPhish provides the admin server URL (`https://127.0.0.1`) and default username/password. In the local browser, we entered the GoPhish server URL and used the default credentials. The site then guided us through the process of resetting the password and logging into the tool.

Gophish Attack Process

Sending Profile

In the GoPhish tool, our attacker initiated by creating the "Sending Profiles." This tool is going to show the victim what email address is being used. In real time attacks, attackers create a VPS server and SMTP service. In this case we used a gmail account.

The attacker collected the SMTP and the host of the gmail email and entered into the tool.

Gophish Attack Process

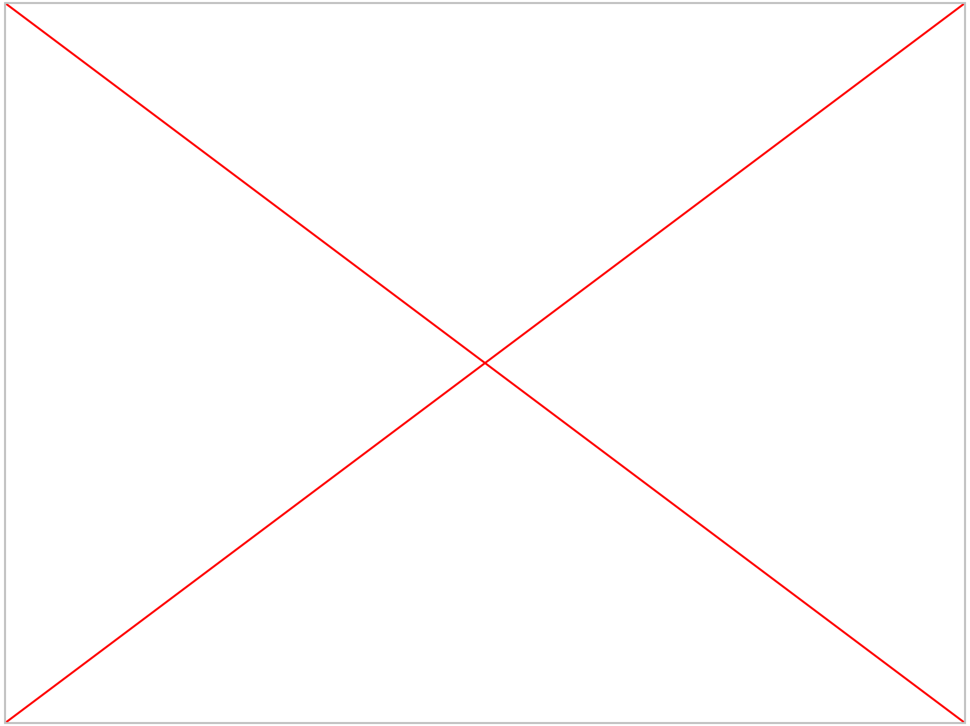
Landing Page

Next the attacker needs emulate the company’s login page where the victim can enter their credentials.

We opened the landing page tool and created and new page.The attacker copied the company’s website (https://nofakeco.godaddysites.com) entered it into the Edit Landing Page where the tool is then able to copy the HTML of the site and replicate it for an attack.

We’ll then save it the landing page as NoFakeCo

Landing Page Demo



Gophish Attack Process

Email Template:

Next the attacker needs to create an email template, this email will state it's the HR rep and will provide the victim the landing page where the credentials will be collected. This email will also need to have similar HTML to the emails sent from the company.

In order to do this we retrieved an email from NoFakeCo and copied the raw message. This will copy company logos, format, and any additional information needed to make the attack look real.

Gophish Attack Process

Email Template:

In the GoPhish tool we now entered went into the email template and imported the raw message.

We now had to rewrite the email message to stating it was Angela Merc and requesting the updated information.

Using AI (ChatGPT) we inputted the necessary information and it generated a new email template for us.

Gophish Attack Process

Email Template: Real Email from NoFakeCo

Hi John,
Thanks for creating an account with us. Please click the link below to activate your account and set a password.

Activate account

Once you create an account, you will be able to check out faster with your saved information, view your profile, bookings, and orders.

If you did not create an account with us, please disregard this email.

Thanks,
NoFakeCo.

Gophish Attack Process

Email Template: Recreated for attack

Dear John,

I hope this message finds you well.

As part of our payroll process, we require your updated bank account details for direct deposit. Could you please provide us with the necessary information at your earliest convenience? This will ensure that your payments are processed smoothly and without delay.

If you have any questions or need assistance, feel free to reach out to me directly.

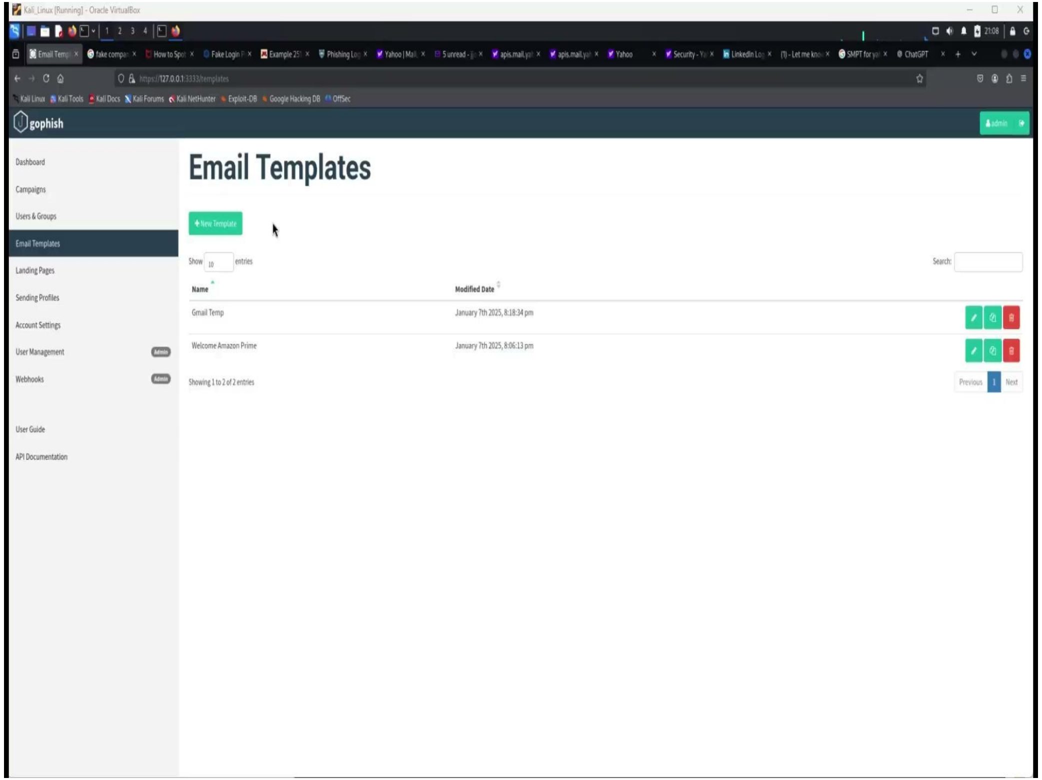
Thank you in advance for your prompt attention to this matter.

Use the hyperlink below to access your account.

Account

Best regards,
Angela Merc
Human Resources
NoFakeCo

Email Template Demo



Email Templates

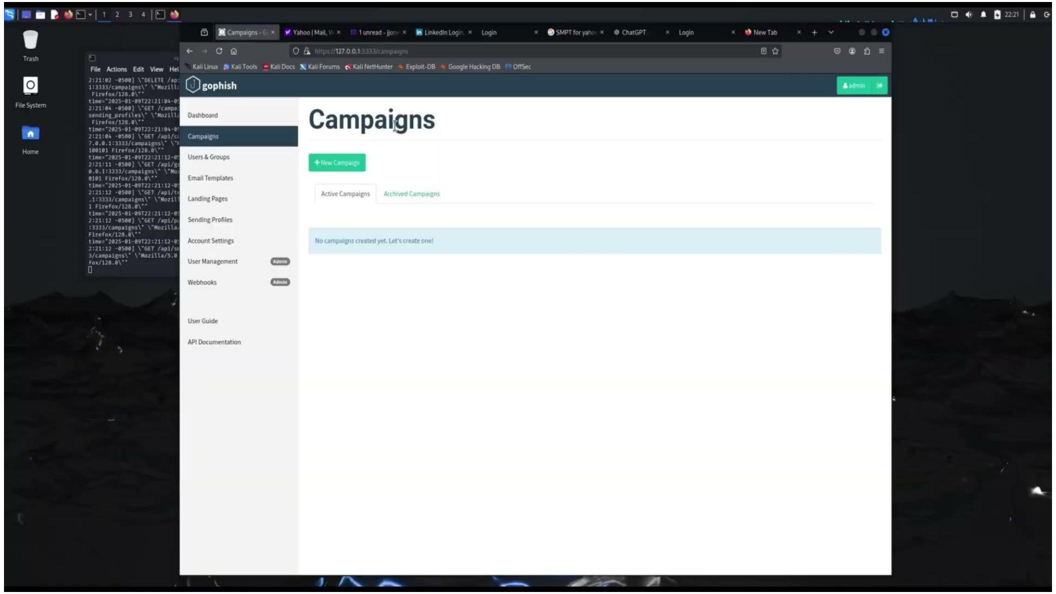
Show 10 entries

Name	Modified Date
Gmail Temp	January 7th 2025, 8:18:34 pm
Welcome Amazon Prime	January 7th 2025, 8:06:13 pm

Showing 1 to 2 of 2 entries

Gophish Attack Process

Lastly we needed enter the victim’s email into Users & Groups and created a new campaign where we can launch the attack.



```
2:21:02 -0500] \"DELETE /ap
1:3333/campaigns\" \"Mozill
 Firefox/128.0\""
time="2025-01-09T22:21:04-0
2:21:04 -0500] \"GET /campa
sending_profiles\" \"Mozill
 Firefox/128.0\""
time="2025-01-09T22:21:04-0
2:21:04 -0500] \"GET /api/c
7.0.0.1:3333/campaigns\" \"
100101 Firefox/128.0\""
time="2025-01-09T22:21:12-0
2:21:11 -0500] \"GET /api/g
0.0.1:3333/campaigns\" \"Mo
0101 Firefox/128.0\""
time="2025-01-09T22:21:12-0
2:21:12 -0500] \"GET /api/t
.1:3333/campaigns\" \"Mozill
1 Firefox/128.0\""
time="2025-01-09T22:21:12-0
2:21:12 -0500] \"GET /api/p
:3333/campaigns\" \"Mozilla
Firefox/128.0\""
time="2025-01-09T22:21:12-0
2:21:12 -0500] \"GET /api/s
3/campaigns\" \"Mozilla/5.0
fox/128.0\""
```

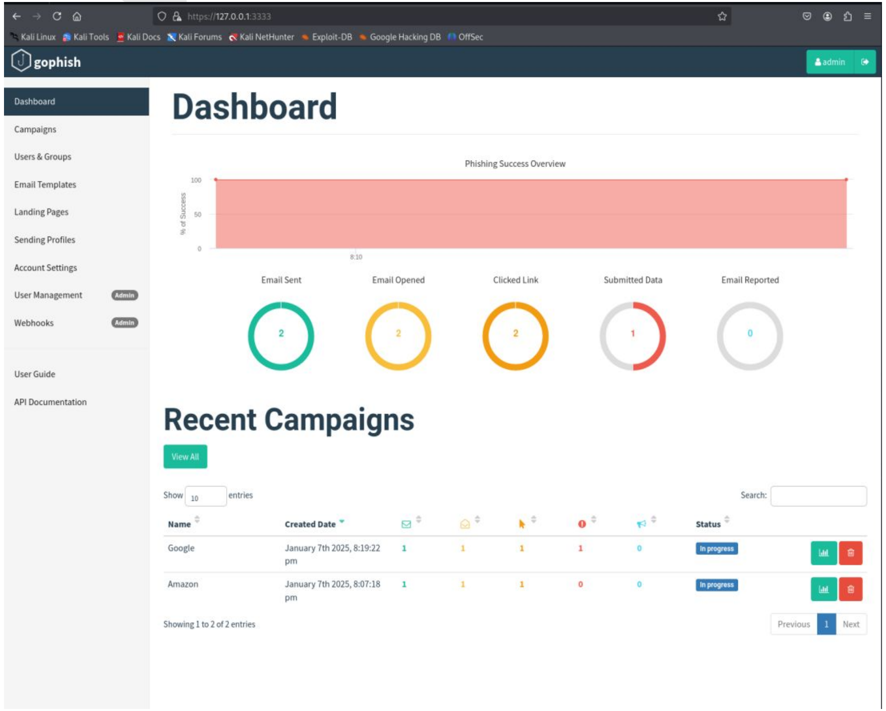
Campaigns

+ New Campaign

Active Campaigns | Archived Campaigns

No campaigns created yet. Let's create one!

Gophish



Dashboard

Recent Campaigns

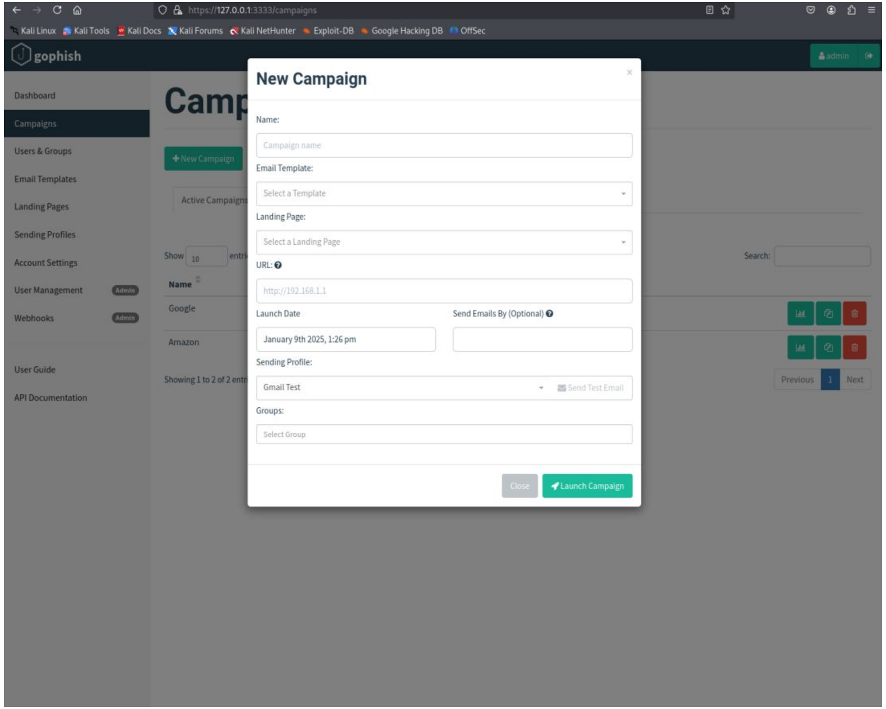
Show 10 entries

Search:

Name	Created Date	✉	✉	➤	❗	📢	Status
Google	January 7th 2025, 8:19:22 pm	1	1	1	1	0	In progress
Amazon	January 7th 2025, 8:07:18 pm	1	1	1	0	0	In progress

Showing 1 to 2 of 2 entries

Previous 1 Next



New Campaign

Name: Campaign name

Email Template: Select a Template

Landing Page: Select a Landing Page

URL: ? http://192.168.1.1

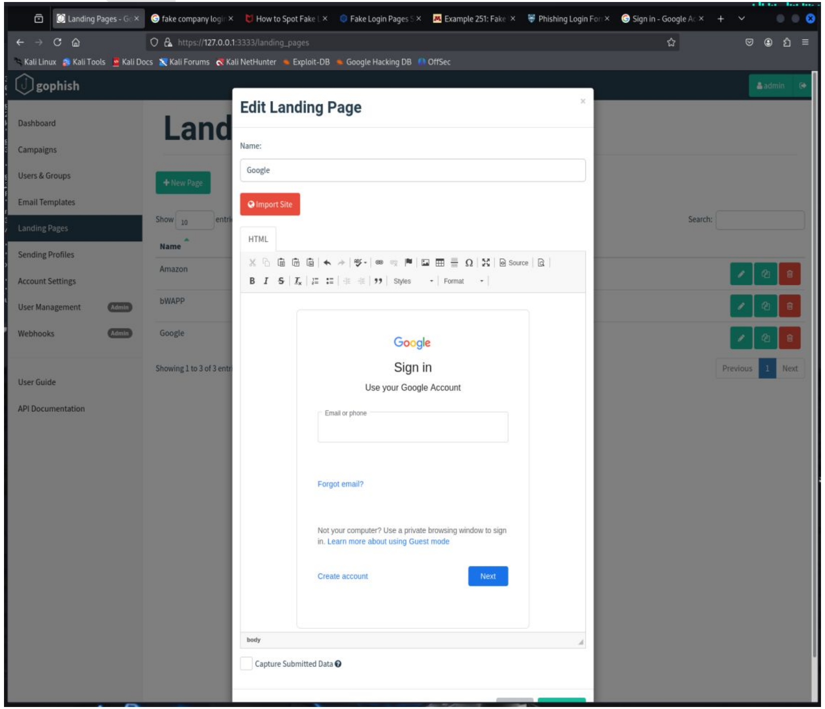
Launch Date: January 9th 2025, 1:26 pm

Send Emails By (Optional) ?

Sending Profile: Gmail Test — Send Test Email

Groups: Select Group

Gophish



https://127.0.0.1:3333/landing_pages

Edit Landing Page

Name: Google

HTML

Google

Sign in

Use your Google Account

Email or phone

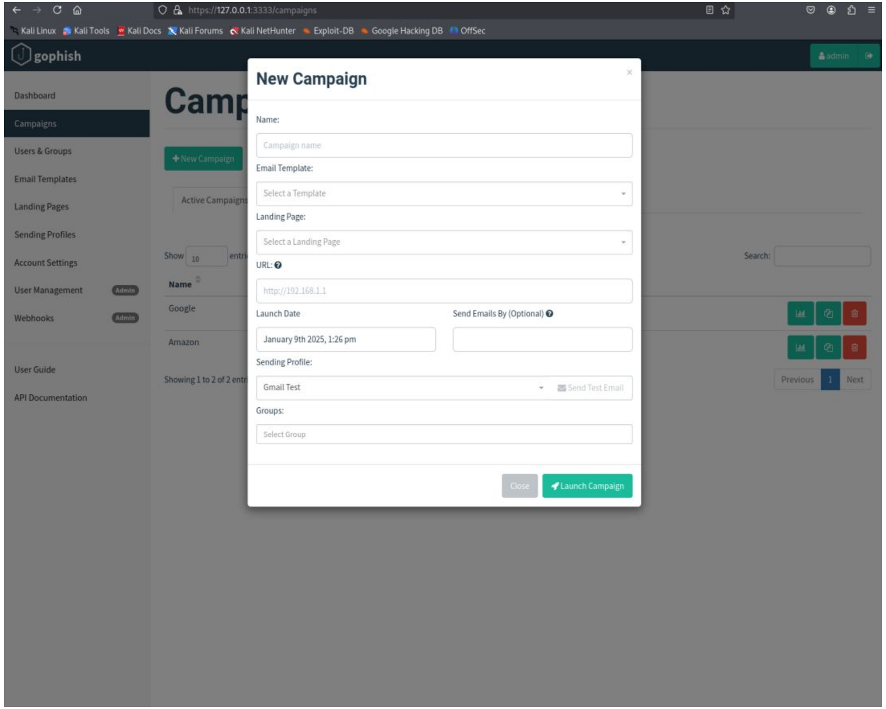
Forgot email?

Not your computer? Use a private browsing window to sign in. Learn more about using Guest mode

Create account

Next

☐ Capture Submitted Data



https://127.0.0.1:3333/campaigns

New Campaign

Name: Campaign name

Email Template: Select a Template

Landing Page: Select a Landing Page

URL: http://192.168.1.1

Launch Date: January 9th 2025, 1:26 pm

Send Emails By (Optional):

Sending Profile: Gmail Test

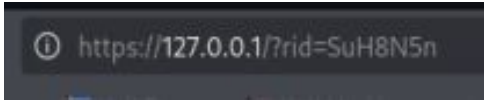
Groups: Select Group

Email Phishing Remediation

Look closely at the domain name.

Fake websites often deceive people by using domain names that closely resemble those of legitimate businesses or organizations. A closer look might reveal subtle differences, such as swapped letters or slight misspellings. If you notice a spelling error in the domain name, you're likely not on the official site, and it's best to close the tab.

In this case the domain name is obvious not the same as the company



https://127.0.0.1/?rid=SuH8N5n

Be careful with links in emails.

Phishing scams are incredibly prevalent. Scammers might send you emails that appear to be from reputable businesses, hoping you'll click on the links without hesitation. Always hover over links in unsolicited emails, and even those from brands, businesses, or people you recognize. If the link doesn't match the visible text or if it's a short link with an unclear destination, don't click it. Doing so could lead you to a lookalike website where your personal information might be compromised.

In this example we use a fake email to send over to our victim.

Email Phishing Remediation Examples

- In phishing attacks they are used to obtain login credentials, Malicious actors pose as trustworthy sources (e.g., colleagues, acquaintances, or organizations) to lure victims into providing their login credentials. Malicious actors can use the compromised credentials (e.g., usernames and passwords) to gain access to enterprise networks or protected resources, such as email accounts.
- Multi-factor authentication (MFA) can reduce the ability of malicious actors using compromised credentials for initial access. Despite this, if weak forms of MFA are enabled, malicious actors can still obtain access through phishing and other techniques.
- Malicious actors can send a multitude of approve or deny “push requests” until a user either accepts the request, often by accident or in frustration. Malicious actors may also deceive users by sending an email containing a link to a malicious website that mimics a company’s legitimate login portal. The user submits their username, password, and the 6-digit code MFA, which the actors then receive to authenticate as the user in the legitimate login portal.

Remediation

How to prevent getting contact information from open sources (Linkedin, Social Media, ETC)

- You should avoid sharing public information on social media and public sites discussing your job as it's also a gateway for attackers to target you. Even though you might have it on your indeed account or other job networking softwares its best that you keep the company you work for out of it and just your job position because these systems are available to the public for everyone to see.

- Use privacy settings on social media accounts to limit who has access to your information and to abide to the rules above so you don’t become a target as they know your position but not exactly who you work for so your work email doesn't become compromised

- Regularly monitor your account to view any suspicious activity that you can spot that you haven't done

Remediation

How the employee should verify if the message is real or not?

- Record and Report phishing emails that are being sent to you and report it to your IT department and CC management so they can be aware of current attacks and deal with attackers by listing the following email addresses as spams or block them as well as other emails with the same address format.

- If your not sure if an email is from a legit team member look back into the team member contact page. Where you can take that information and plug it into your email search engine and see if the email that was sent to you was from a legitimate team member. All team members that you have correlated with before or have been cc'd in an email before should generate in the search engine but this isn't going to work 100%. Even so it is a good method to try to confirm if the email is from legit source. You should also send the email to your IT department to have professionals evaluate the email and confirm that its safe, and legit.

- You should also be vigilant towards the email that was sent to you by checking for any incorrect spelling in the text of the email, and also the email address that it was sent from. You should also never download anything from these emails as it might contain malware that can interrupt or damage systems, escalating user privileges and maintain persistence on compromised systems. You should also never click on any links from these emails as it might direct you to a compromising site and it might be an infectious download.
- Try to also obtain team members professional and personal contact information for your own records so if you receive contact from an unknown number or email you can verify its legitimacy from your personal records.

Remediation

Steps to Take Following a Successful Phishing Attack

Employee awareness training programs should implement the knowledge of how to recognize phishing emails and how to properly proceed with dealing with phishing emails by following the incident response steps.

INCIDENT RESPONSE: If an organization identifies compromised credentials and/or successful malware from phishing activity, remediate the activity by:

1. Re-provisioning suspected or confirmed compromised user accounts to prevent malicious actors from maintaining continued access to the environment.

2. Auditing account access following a confirmed phishing incident to ensure malicious actors no longer have access to the initially impacted account.

3. Isolating the affected workstation after the detection of a phishing attack. This helps stop the executed malware from spreading further into the organization’s network.

4. Analyzing the malware. After isolating the affected workstation(s), have the malware analyzed by a team that specializes in malware analysis.

5. Eradicating the malware. Eradicate the malware from the network so other workstations within the organization’s networks can no longer be negatively impacted by the executed malware.

6. Restore systems to normal operations and confirm they are functioning properly. The main challenges at this phase are confirming that remediation has been successful, rebuilding systems, reconnecting networks, as well as correcting misconfigurations.

CISA (2023, October 1). Phishing Guidance: Stopping the Attack Cycle at Phase One. Cisa.Gove. Retrieved January 13, 2024, from https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf

Remediation

- Reporting policies for suspicious emails, phone calls, etc. Should all be reported to upper management and your IT support team.

- Email security protocols should have spam filters, and phone blocking capabilities