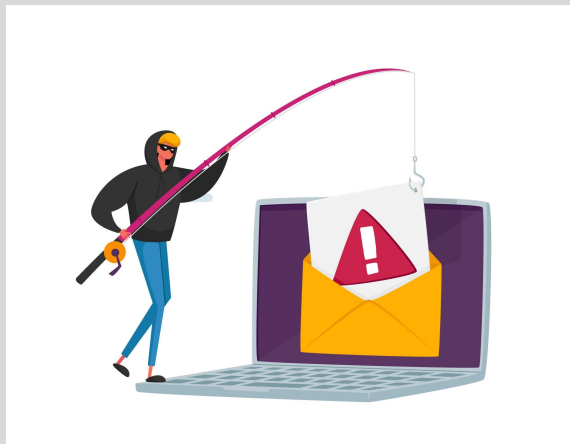


Gophish BootCon: Hook, Line, and Security

“Don’t get caught slippin’—stay phish-free!”



Created by: Andrew B. | Bre M. | Mia Q. | Wiley J.

What is Phishing?

Phishing: a scam where attackers pretend to be a trustworthy source to steal your sensitive information



Phishing Family Tree: It's a Big, Scammy Family



Gophish: The Ethical Hacker's Secret Weapon

- **Free Open-source phishing simulation toolkit**
- Used by **security teams** to test employee awareness
- Simulates real phishing campaigns without harm
- Helps train people to recognize suspicious emails

Gophish lets us play the bad guys—without actually being bad guys. It's designed to help organizations test their defenses before real attackers do. Think of it as cyber paintball... but with email.



The Dark Side of Gophish

- **Anyone** can access!
- Everything that can be used ethically can also be used for **bad**
- In the wrong hands, they can capture everything
- It only needs one ***click*** and/or ***password***...



Why did the hacker bring a fishing pole to the office?



To catch some phish, of course.....



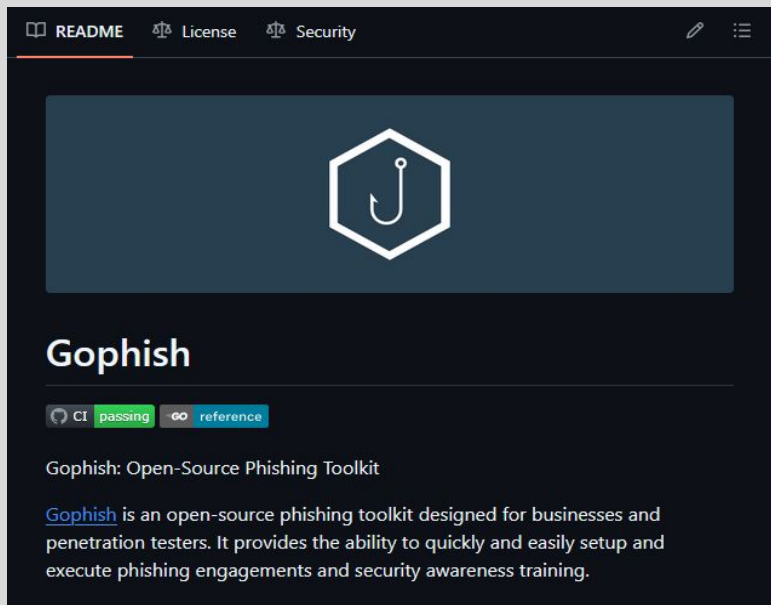
Installing and Opening Gophish

Gophish Installation – Windows

- Download the latest release from github.com
- Extract the ZIP to `C:\gophish`
- Open `\gophish` file
- Run Gophish: `.\gophish.exe`
- Go to `https://localhost:3333` in your browser
- Log in with the credentials shown in the console

Easy as 1, 2 & 3

Github, the bible for nerds



Unzip and you're ready to launch.

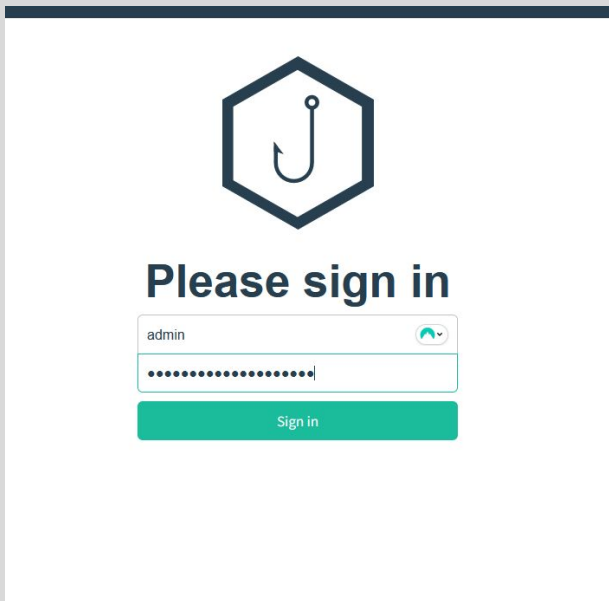
Name	Date modified	Type
Yesterday		
gophish.db	5/28/2025 8:10 PM	Data Base File
gophish_admin.crt	5/28/2025 8:07 PM	Security Certificate
gophish_admin.key	5/28/2025 8:07 PM	Keynote Presentation
config.json	5/28/2025 8:06 PM	JSON File
LICENSE	5/28/2025 8:06 PM	File
README.md	5/28/2025 8:06 PM	Markdown Source File
VERSION	5/28/2025 8:06 PM	File
gophish.exe	5/28/2025 8:06 PM	Application
db	5/28/2025 8:06 PM	File folder
templates	5/28/2025 8:06 PM	File folder
static	5/28/2025 8:06 PM	File folder

Cmd Prmt and Login

Admin, password, url

```
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
time="2021-09-14T11:54:44+02:00" level=info msg="Please login with the username admin and the password e1414bb8c8464ade"
time="2021-09-14T11:54:44+02:00" level=info msg="Starting IMAP monitor manager"
time="2021-09-14T11:54:44+02:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2021-09-14T11:54:44+02:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2021-09-14T11:54:44+02:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2021-09-14T11:54:44+02:00" level=info msg="Starting new IMAP monitor for user admin"
time="2021-09-14T11:54:44+02:00" level=info msg="TLS Certificate Generation complete"
time="2021-09-14T11:54:44+02:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
2021/09/14 11:55:03 http: TLS handshake error from 127.0.0.1:62735: remote error: tls: unknown certificate
2021/09/14 11:55:06 http: TLS handshake error from 127.0.0.1:61997: remote error: tls: unknown certificate
time="2021-09-14T11:55:06+02:00" level=info msg="127.0.0.1 - - [14/Sep/2021:11:55:06 +0200] \"GET / HTTP/2.0\" 307 51 \"\n\" \"/Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36\""
time="2021-09-14T11:55:06+02:00" level=info msg="127.0.0.1 - - [14/Sep/2021:11:55:06 +0200] \"GET /login?next=%2F HTTP/2.0\" 200 1033 \"\n\" \"/Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36\""
time="2021-09-14T11:55:06+02:00" level=info msg="127.0.0.1 - - [14/Sep/2021:11:55:06 +0200] \"GET /images/logo_inv_small.png HTTP/2.0\" 200 1118 \"https://127.0.0.1:3333/login?next=%2F\" \"/Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36\""
time="2021-09-14T11:55:06+02:00" level=info msg="127.0.0.1 - - [14/Sep/2021:11:55:06 +0200] \"GET /images/logo_purple.png HTTP/2.0\" 200 4735 \"https://127.0.0.1:3333/login?next=%2F\" \"/Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36\""
time="2021-09-14T11:55:06+02:00" level=info msg="127.0.0.1 - - [14/Sep/2021:11:55:06 +0200] \"GET /css/dist/epoch.css\"
```

Ready to log in






Wait—Was This Even Legal?

- ✓ *No sensitive data was collected*
- ✓ *Only personal LinkedIn was used to simulate sender*
- ✓ *Participants were informed post-simulation*
- ✓ *No impersonation of others occurred*
- ✓ *Goal was to demonstrate how easily phishing can happen*



Crafting the Bait: How We Built the Phish

What We Built:

-  **Landing Page:** Cloned LinkedIn login page
-  **Email Template:** Dummy email with spoofed sender
-  **Target:** One placeholder user



How We Did It (Tools + Process)

Step	Tool Used	Description
1	GoPhish	Created and launched campaign
2	Cloudflare	Created a secure tunnel for external access
3	Rebrandly	Shortened phishing URL
4	Link	LinkedIn Wiley T Johnson (mocked)

Crafting the Bait: How We Built the Phish

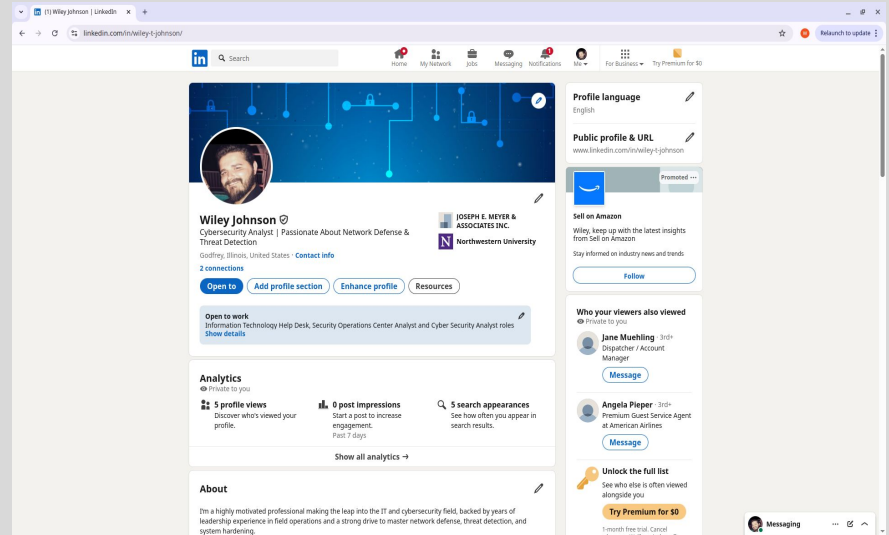
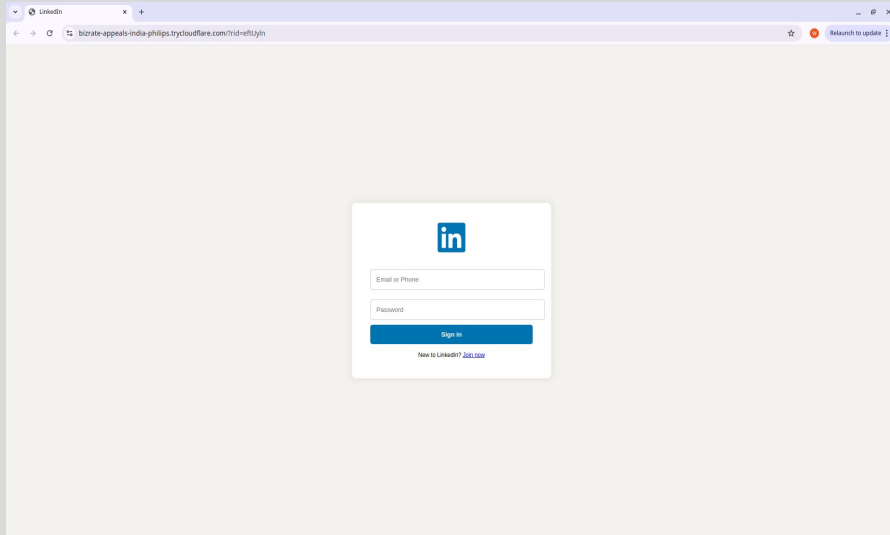
Why It Worked (Psychology of the Click)

- “It looked legit.”
- “The link seemed harmless.”
- “They didn’t expect to be tested.”

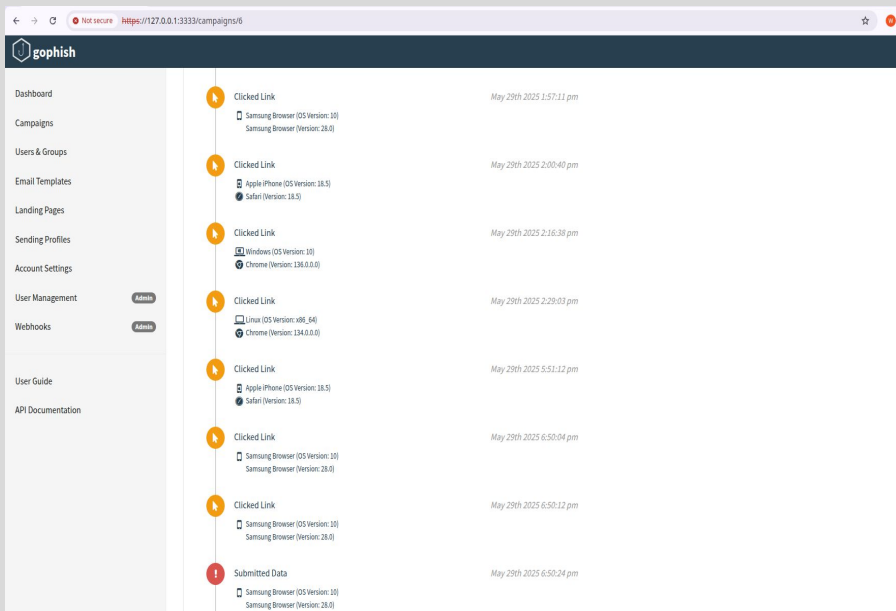


“Phishing succeeds not because tech fails, but because we trust what feels familiar.”

Landing Page



Monitoring the Campaign



Results for LinkedIn Home



Monitoring

- Tracked link clicks in real time via GoPhish dashboard
- No actual emails sent, no credentials captured — **just emails & click tracking**
- **6** Users clicked in **7** hour campaign

Demo

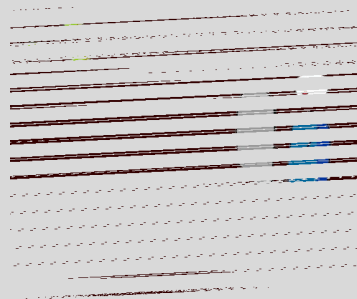
Mitigations: How to Not Get Hooked

Train the Humans : 🧠 *your brain is the first firewall*

- Security Awareness Training, helps users recognize threats like phishing, vishing, and smishing.
- Simulated phishing campaigns give people safe practice

It's like cyber self-defense class—but no punching involved.

- Teach users to “Hover, Think, Verify”



Email Defense Tools

Enable Email Filtering & Scanning

Use **DMARC**, **DKIM**, and **SPF** to prevent spoofing

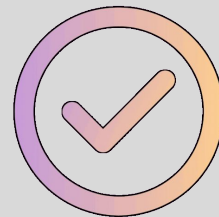


- **SPF** = "Name on the guest list" (Sender Policy Framework)
- **DKIM** = "Signature matches" (DomainKeys Identified Mail)
- **DMARC** = "Checks the bouncer's checklist" (Domain-based Message Authentication, Reporting & Conformance)

These tools validate if an email is really from who it says it is. Think of them as **email bouncers**—only letting the real VIPs in.



Personal Habits

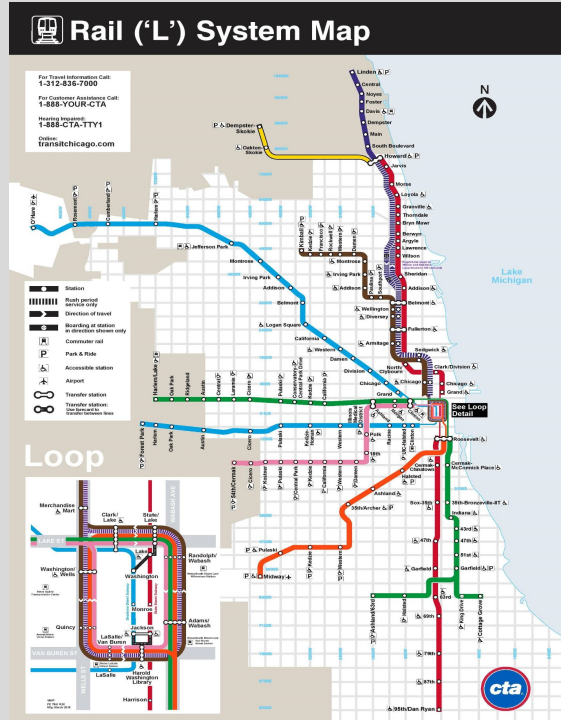


- When in doubt, Don't click!
- **Go to the site yourself** (don't trust Rebrand.ly in the wild).
- Enable MFA whenever possible

Hover before you click, trust your gut!

The “L”

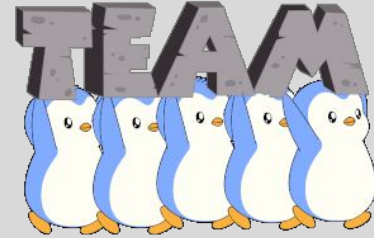
remember clicking suspicious links is like licking a pole on the RedLine. Just...don't do it!



Mitigation Recap

Build the (Fire)Wall, Not the Excuses

- 🧠 + 💪 Human Training
- ✉️ + 🛡️ Email Tools
- 👤 + 🚫 Safe Habits



Cybersecurity isn't just a tech problem—it's a people problem. Train the people, and you strengthen the system.

Stay alert—don't become the phish story in your next company newsletter

QUESTIONS

