

Get busy Phishing or get busy paying

*“Great results, can be achieved with small forces.”
— Sun Tzu, The Art of War*



Disclaimer

The views, thoughts, and opinions expressed in the presentation belong solely to the author, and not necessarily to the author's employer, organization, committee or other group or individual.



Roei Sherman

♠ Red Team & PT Manager @  AB InBev



♠ Co-organizer @  BOSIDES TLV

♠ OSCP, GPEN, GXPN, CCSK – SANS Advisory Board



<https://bettheadversary.com>

bta@bettheadversary.com



<https://github.com/xFreed0m>



[x_Freed0m](https://twitter.com/x_Freed0m)



Security products bingo

The image is a comprehensive grid of security product logos, organized into 15 distinct categories. Each category is represented by a dark header bar with white text. The logos themselves are small, colorful icons of various security companies, densely packed within each category's grid. The categories include:

- Network Security:** Network Firewall (e.g., Infoblox, Cisco, Palo Alto) and Network Monitoring/Forensics (e.g., Blue Coat, SecPulse, Ixia).
- Endpoint Security:** Endpoint Prevention (e.g., McAfee, Cylance, Symantec) and Endpoint Detection & Response (e.g., Opswat, Ziften, SentinelOne).
- Application Security:** WAF & Application Security (e.g., Akamai, Cloudflare, Imperva) and Vulnerability Assessment (e.g., Bugcrowd, Rapid7, Checkmarx).
- Managed Security Service Provider:** A collection of MSSP logos such as Atlat, Verizon, and Trustwave.
- Web Security:** Log management and security solutions like LogRhythm, Splunk, and Logentries.
- Messaging Security:** Email and messaging security products from vendors like Proofpoint and Microsoft.
- Risk & Compliance:** Risk assessment and compliance tools from companies like PwC and GRX.
- Security Operations & Incident Response:** SIEM (Security Information and Event Management) and Incident Response solutions like IBM, LogRhythm, and Splunk.
- Data Security:** Data loss prevention and security tools from vendors like Symantec and Veeva.
- Mobile Security:** Mobile device management and security solutions like Lookout and AirWatch.
- Industrial / IoT Security:** Security solutions for industrial and IoT environments from companies like MOCANA and Bastille.
- Threat Intelligence:** Threat intelligence and analysis tools like ThreatMatrix and RiskIQ.
- Identity & Access Management:** IAM solutions from vendors like Okta and Ping Identity.
- Cloud Security:** Cloud security and compliance solutions like AWS IAM and Palo Alto.
- Fraud Prevention / Transaction Security:** Fraud prevention and transaction security tools like FICO and RiskIQ.
- Specialized Threat Analysis & Protection:** Specialized threat analysis and protection solutions like InetSec and FortiGate.

People are the weakest link?

- We like free things
- We don't pay attention
- We get scared easily
- We are built to comply
- We are vulnerable. All of us.



Can we make them stronger?

People can be a strong security layer.

- They are free (or already paid for...)
- They are smarter than code
- They can do both detect and prevent
- No patch for human stupidity. But there are Hotfixes.



Arming the masses!



The scenario

- Start Easy\Hard & adjust to the current level
- Realistic -
<https://www.phishtank.com/> | past incidents
- Sensitive - COVID19, aiming for win-win
- Whitelisting - we are here for the people, not the products
- Plan the entire program, not just the current campaign



Act on the results

- Train - not just drills
- Equip - give them the tools - technical and logical
- Organize - build a plan, not a campaign
- They are not to blame, we are



Let's do it (for free)

- We do it on Debian 9 - gophish is cross platform
- Ports needed - 22, 80, 443, 3333
- You need to buy a domain
- Script is initial setup, only required once (per machine)
- Hardening is on YOU

- It's gonna be fun :)



HTTPS cert (people like green locks)

- We want to make reliable
- Using EFF certbot
- Require a domain and port 80 open to WW
- Script option #4

```
3) Ubuntu Prep          7) Get DNS Entries
4) Install SSL          8) Install GoPhish
Server Setup Script - Pick an option: 4
certbot 1.10.1 from Certbot Project (certbot-eff/) installed
Enter your server's domain or done to exit: xfreed0m.art
Enter your server's domain or done to exit: done
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Account registered.
Requesting a certificate for xfreed0m.art
Performing the following challenges:
http-01 challenge for xfreed0m.art
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/xfreed0m.art/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/xfreed0m.art/privkey.pem
  Your cert will expire on 2021-04-02. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:
```



NOT BY SCHEP

SMTP server

- We are using Postfix
- We also install Dovecot, OpenDKIM & OpenDMARC - if looking for more reliability
- We install everything on the same server, can be separated
- script option #5

```
Restarting Services
```

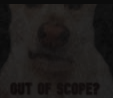
```
Checking Service Status
```

```
● postfix.service - Postfix Mail Transport Agent
  Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
  Active: active (exited) since Sat 2021-01-02 21:51:26 UTC; 1min 17s ago
  Process: 9061 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
  Main PID: 9061 (code=exited, status=0/SUCCESS)
  Tasks: 0 (limit: 4915)
  CGroup: /system.slice/postfix.service
```

GoPhish

- Open-Source phishing platform
- cross-platform support - Linux\Windows\Mac
- Actively developed and supported
- Has two built in “Gophish” headers
- Run the binary from screen to avoid crash on SSH exit
- Script option #8

```
01-02T21:53:30Z" level=info msg="Please login with the username admin and the password [REDACTED]"
01-02T21:53:30Z" level=info msg="Starting admin server at https://0.0.0.0:3333"
01-02T21:53:30Z" level=info msg="background worker started successfully - waiting for campaigns"
01-02T21:53:30Z" level=info msg="Starting IMAP monitor manager"
01-02T21:53:30Z" level=info msg="Starting new IMAP monitor for user admin"
01-02T21:53:30Z" level=info msg="Starting phishing server at http://0.0.0.0:443"
```



Sending profile

- The server sending the emails
- Here we choose who the message will be “from”
- Here we are using the same server



New Sending Profile

Name:

Postfix

Interface Type:

SMTP

From:

Master Splinter <splinter@xfreed0m.art>

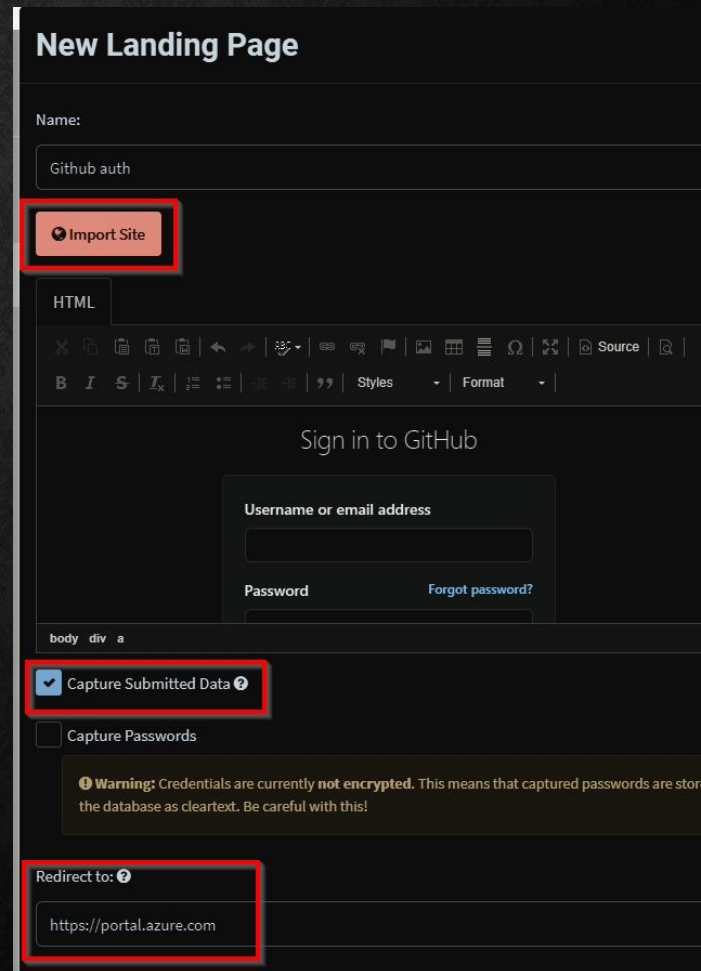
Host:

localhost

Username:

Create \ clone the landing page

- Where the users will get once clicking the link
- Build yourself or “borrow” from someone ;)
- decide what to capture (username only or passwords also?)



New Landing Page

Name: Github auth

Import Site

HTML

Sign in to GitHub

Username or email address

Password [Forgot password?](#)

body div a

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: ?

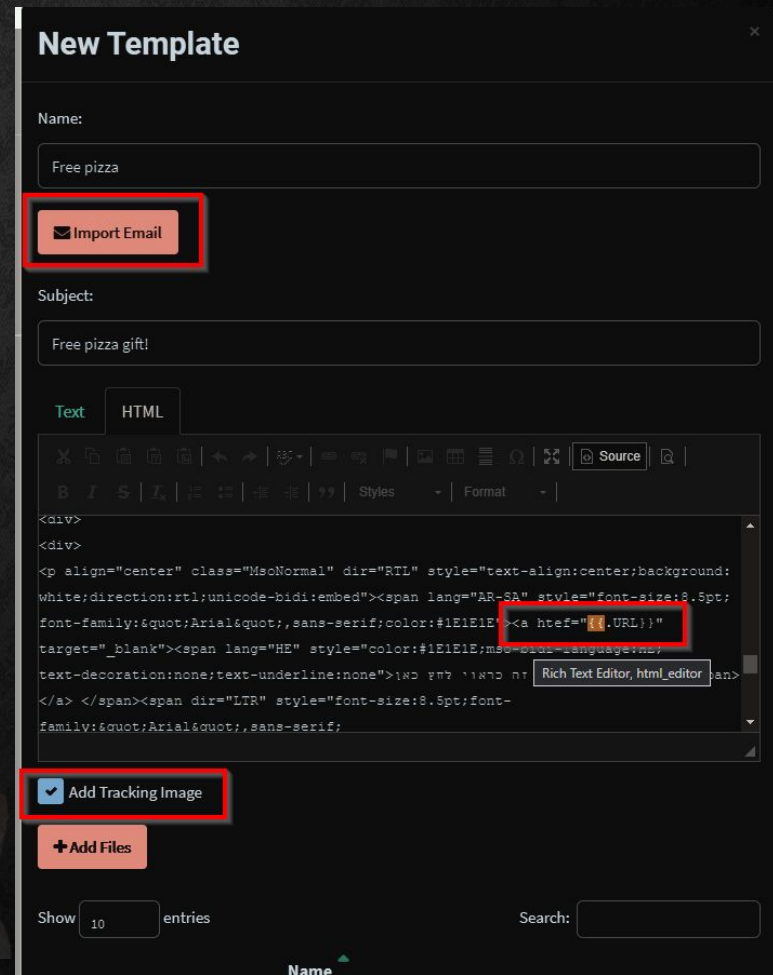
https://portal.azure.com



NOT IN SCOPE?

Create \ clone the email

- The actual email we will send
- Build yourself or “borrow” from someone ;)
- Make to test it multiple times



New Template

Name: Free pizza

Import Email

Subject: Free pizza gift!

Text HTML

Add Tracking Image

+ Add Files

Show 10 entries Search:

```
<div>
<div>
<p align="center" class="MsoNormal" dir="RTL" style="text-align:center;background:
white;direction:rtl;unicode-bidi:embed"><span lang="AR-SA" style="font-size:8.5pt;
font-family:"Arial";,sans-serif;color:#1E1E1E" ><a href="{URL}"
target=" _blank"><span lang="HE" style="color:#1E1E1E;mso-bidi-language:HE;
text-decoration:none;text-underline:none"> זה קראו למש כאן </span> </a> </span><span dir="LTR" style="font-size:8.5pt;font-
family:"Arial";,sans-serif;
```


Import the users

- Bulk import using the CSV template
- divide based on your preference

New Group

Name:

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

[+ Add](#)

Show entries Search:

First Name	Last Name	Email	Position
Leonardo		leo@cyberint.co	
Michelangelo		mike@cyberint.co	
Roei		roei.s@cyberint...	

Showing 1 to 3 of 3 entries [Previous](#) [1](#) [Next](#)



NOT IN SCOPE?

GET BUSY PHISHING!

- Who
- What
- When
- Divided?

New Campaign ✕

Name:

Email Template:

Landing Page:

URL: ?

Launch Date Send Emails By (Optional) ?

Sending Profile:
 ✕ ✉ Send Test Email

Groups:

Free pizza gift!

MS

Master Splinter <splinter@xfreed0m.art>
To Roei Sherman



Reply

Reply All

Forward



Sun 1/3/2021 12:21 AM



אם אינך רואה מייל זה כראוי לחץ כאן

<https://xfreed0m.art?rid=b0wxkf1>
Click or tap to follow link.



איזדה כיף לכם!

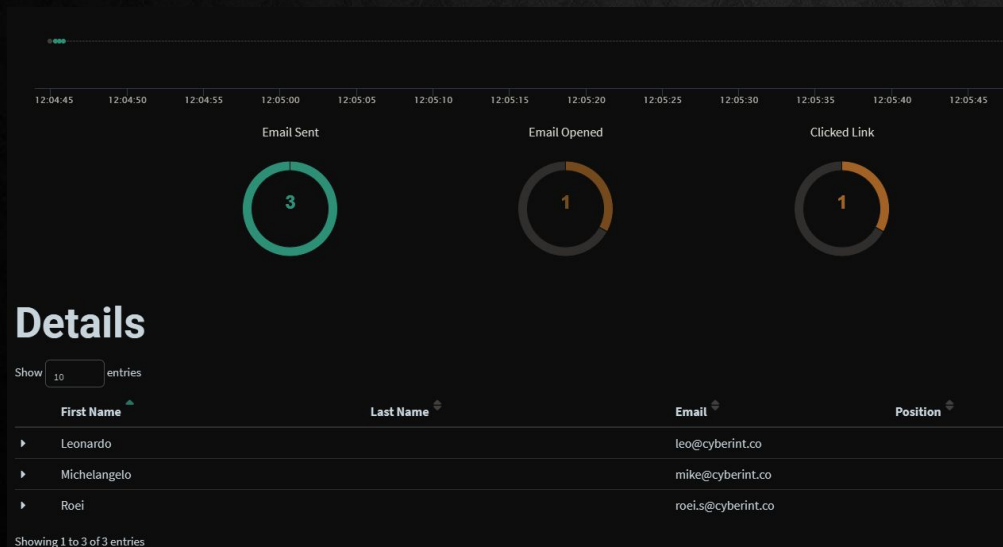
הזמנתם, גירדתם, הרווחתם!



**אצבעות
מוצרלה**

Sit and Stare AKA statistics

- Opened, Clicked, entered credentials
- When, Where, How much
- Export to CSV - no fancy graphs
- Save the information for improvement tracking



Timeline for Leonardo

Email: leo@cyberint.co

Result ID: 8VGtagt

- Campaign Created
- Email Sent
- Clicked Link
 - Windows (OS Version: 10)
 - Chrome (Version: 87.0.4280.88)
- Clicked Link
 - Windows (OS Version: 8.1)
 - Chrome (Version: 84.0.4147.135)
- Submitted Data
 - Windows (OS Version: 10)
 - Chrome (Version: 87.0.4280.88)

Replay Credentials

View Details

Parameter	Value(s)
__original_url	https://github.com/login/session
allow_signup	
authenticity_token	ehxzIY0glypSyGR+60EQmjoU28xadViadNhFmJ/4ZdErT
client_id	
commit	Sign in
integration	
login	Leonardo
required_field_2407	
return_to	

If it won't be simple, it simply won't happen

- As part of arming the masses, we should give them the tools, not just the knowledge
- Easy, simple and fast
- I'm not lazy, I'm efficient - 1-Click phishing reporting



1-Click phishing report button

- Elli da King



- Verify subscription supports mails out on 25 or use other infrastructure

<https://getgophish.com/>

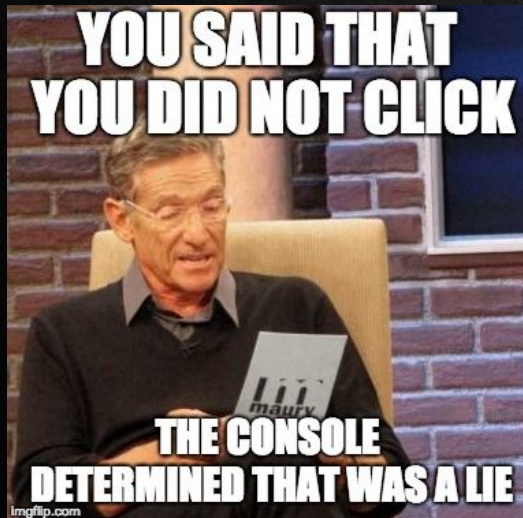
- <https://docs.getgophish.com/user-guide/template-reference>

<https://github.com/xFreed0m/Postfix-Server-Setup>

- Certificate
- DNS records
- Postfix + DKIM + SPF + DMARC
- optional features - hardening, email client



Get busy Phishing or get busy paying



<https://bettheadversary.com>

bta@bettheadversary.com



<https://github.com/xFreed0m>



[x_Freed0m](#)

