

EFFECTIVE PHISHING

with

GOPHISH

ABOUT

Senior Network Penetration Tester for BSI AppSec
GXPN, OSCP, OSWP, CISSP, etc.

Co-Instructor: Full Scope Social Engineering @ BlackHat
Practical Remote Social Engineering @ WWHF

On Twitter at @highmeh

PHISHING OVERVIEW



Why is this important?

“



thaddeus e. grugq

@thegrugq



Give a man an Oday and he'll have access for a day, teach a man to phish and he'll have access for life.

2:35 AM · Feb 7, 2015 · [Tweetbot for iOS](#)

5.2K Retweets **7.6K** Likes

ABOUT THIS TALK

For **beginners**

(although 1337 SE's may learn something, too)

Quickly set up a phishing server and build campaigns

Track user behavior **–or–** pwn users more effectively

The best way to teach good habits? Constant
reinforcement

And finally...

...ITS FUN TO DO BAD THINGS.



PHISHING BY THE NUMBERS

For the C-Levels

33%

of breaches in 2018
involved social
engineering

32%

of breaches in 2018
involved phishing

29%

of breaches in 2018
used stolen
credentials

<https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

78%

...of all espionage incidents involved phishing

<https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

OVERVIEW

Blue Team

- Set up a GoPhish Server
- Build believable campaigns
- Scale up sophistication
- Track user interaction, reporting, and trends

Red Team

- Set up a GoPhish Server
- Build malicious portals to capture credentials
- Deliver payloads and reuse credentials

GOPHISH FRAMEWORK

<https://getgophish.com/>

- Mature and Robust
- Actively Maintained
- GUI and API
- FREE



Gophish

GOPHISH SETUP IN 5 MINUTES

- Spin up an EC2 Instance
- Log in via SSH
- Install Golang
- Download and unzip GoPhish
- Run GoPhish

GOPHISH SETUP IN 5 MINUTES

- Download and Configure (Details)

On your host:

```
$ ssh user@ip_or_hostname
```

On your server:

```
$ sudo apt-get update && sudo apt-get -y install golang unzip
```

```
$ wget https://github.com/gophish/gophish/releases/download/v0.8.0/gophish-v0.8.0-linux-64bit.zip
```

```
$ sudo unzip gophish-v0.8.0-linux-64bit.zip -d /opt/gophish
```

```
$ cd /opt/gophish
```

```
$ tmux new -s gophish *
```

```
$ sudo ./gophish
```

* Optional, kinda

GOPHISH SETUP IN 5 MINUTES

- Log In

On your host:

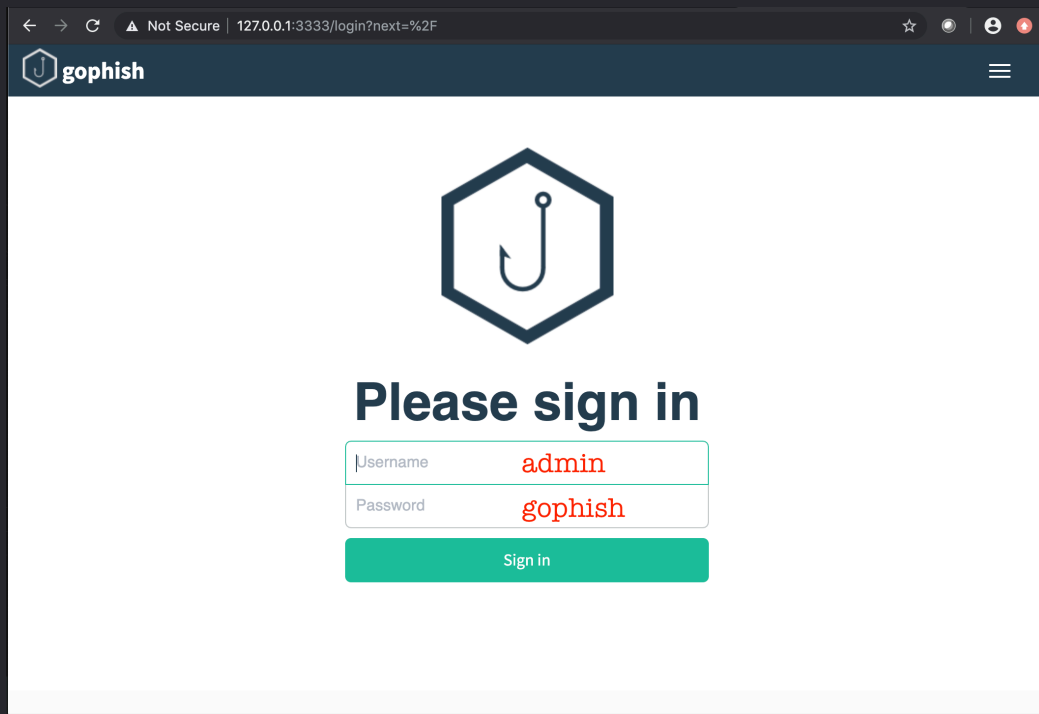
```
$ ssh -Nf -L3333:localhost:3333  
user@ip_or_hostname
```

In your browser:

<https://127.0.0.1:3333>

Username: admin

Password: gophish



....but it doesn't do anything yet.

GoPhish is a framework used to create and manage phishing campaigns, but it doesn't create anything by default

Fortunately, it's painless to set up a campaign from scratch.

BUILDING A CAMPAIGN: THE PIECES

Users & Groups

A list of users you want to phish, including emails, names, and titles

Email Templates

The actual e-mail you want to send, in HTML, text, or both

Landing pages

The page that users are sent to and interact with, if they click the link

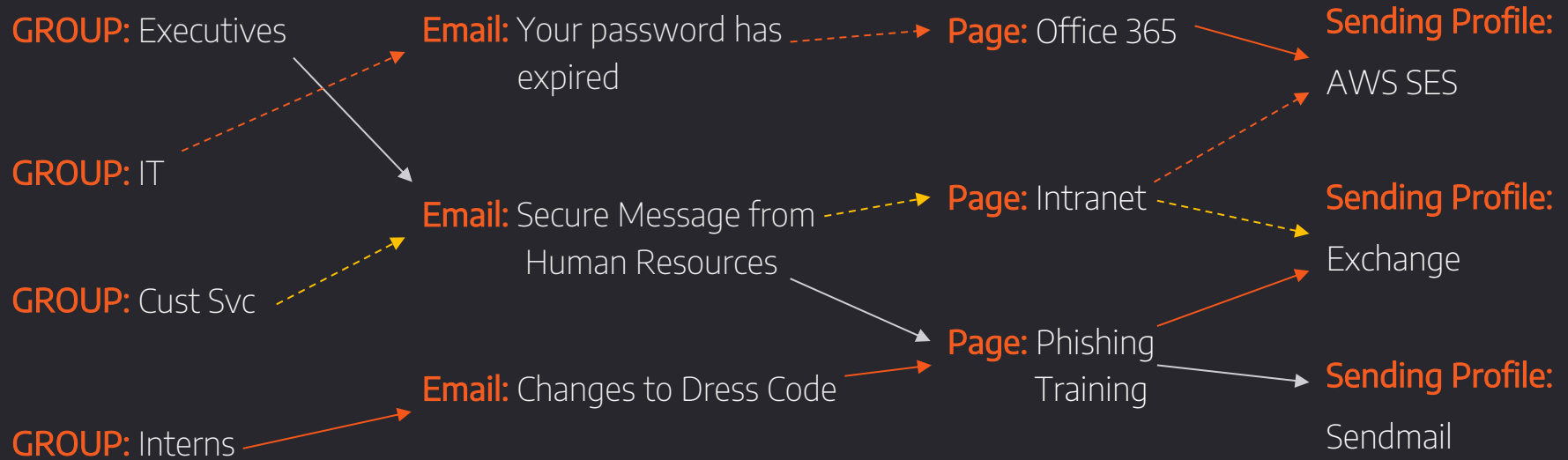
Sending Profile

The email server itself, and the settings that allow your phish to be sent

A **Campaign** consists of all of the above items together

Email Template sent via *Sending Profile* to *User Group* directing to a *Landing Page*

BUILDING A CAMPAIGN: MIX AND MATCH!



LETS BUILD A CAMPAIGN!

In the next few slides, we'll build out a phishing campaign in GoPhish, step by step.

LETS BUILD A CAMPAIGN! Sending Profile

The sending profile tells GoPhish how to send the email itself.

The only *required* fields are Name, From, and Host – but your server may require a username and password, too.

New Sending Profile

Name: Profile name

Interface Type: SMTP

From: First Last <test@example.com>

Host: smtp.example.com:25

Username: Username

Password: Password

☒ Ignore Certificate Errors ⓘ

Email Headers:

Header	Value
X-Custom-Header	{{URL}}-gophish

Show 10 entries Search:

No data available in table

Showing 0 to 0 of 0 entries Previous Next

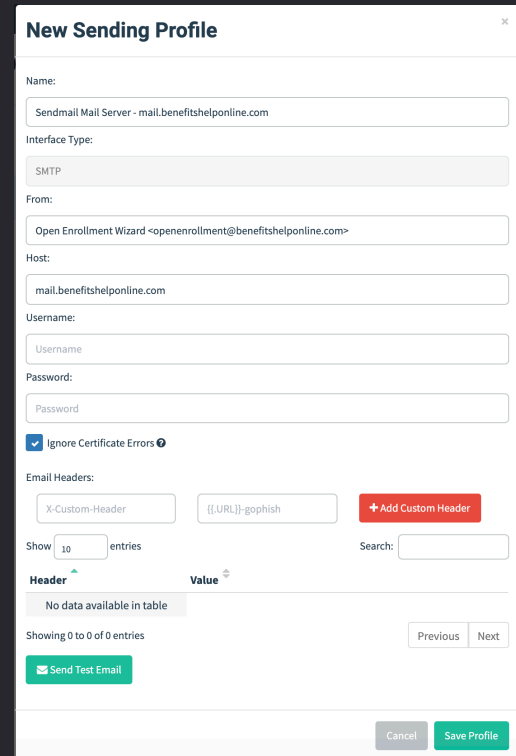
[Send Test Email](#)

[Cancel](#) [Save Profile](#)

LETS BUILD A CAMPAIGN! Sending Profile

The sending profile tells GoPhish how to send the email itself.

The only *required* fields are Name, From, and Host – but your server may require a username and password, too.



The screenshot shows the 'New Sending Profile' form in GoPhish. The form includes the following fields and options:

- Name:** Sendmail Mail Server - mail.benefitshelponline.com
- Interface Type:** SMTP
- From:** Open Enrollment Wizard <openenrollment@benefitshelponline.com>
- Host:** mail.benefitshelponline.com
- Username:** Username
- Password:** Password
- ☒ **Ignore Certificate Errors**
- Email Headers:**
 - X-Custom-Header
 - [[URL]]-gophish
 - + Add Custom Header
- Show:** 10 entries
- Search:** Search
- Header** and **Value** columns (No data available in table)
- Showing 0 to 0 of 0 entries**
- Buttons:** Send Test Email, Cancel, Save Profile

LETS BUILD A CAMPAIGN! Users and Groups

Users and groups allows you to enter logical groups of targets to phish.

The only *required* field is **Email**, but entering all fields allows you to pull from those fields into emails for a tailored phish

Tip: You can batch-upload via CSV file

The screenshot shows a 'New Group' modal window. At the top, there's a title 'New Group' with a close button (X). Below the title is a 'Name:' label followed by a text input field containing 'Group name'. This field is highlighted with a red border. Below the name field are two buttons: '+ Bulk Import Users' (red) and 'Download CSV Template' (with a download icon). Underneath these are four input fields: 'First Nam', 'Last Nam', 'Email', and 'Position'. The 'Email' field is highlighted with a red border. To the right of the 'Position' field is a red '+ Add' button. Below the input fields, there's a 'Show' dropdown set to '10' and the word 'entries'. To the right is a 'Search:' label and an empty search input field. Below this is a table header with columns: 'First Name', 'Last Name', 'Email', and 'Position'. The table body shows a message 'No data available in table'. At the bottom left of the table area, it says 'Showing 0 to 0 of 0 entries'. At the bottom right of the table area are 'Previous' and 'Next' buttons. At the very bottom of the modal are two buttons: 'Close' (grey) and 'Save changes' (green).

LETS BUILD A CAMPAIGN! Users and Groups

Users and groups allows you to enter logical groups of targets to phish.

The only *required* field is **Email**, but entering all fields allows you to pull from those fields into emails for a tailored phish

Tip: You can batch-upload via CSV file

New Group

Name:

+ Bulk Import Users

Download CSV Template

Jayme

Hancok

jayme@blackjackn

Janitor

+ Add

Show 10 entries

Search:

First Name	Last Name	Email	Position	
Ben	Franklin	bfranklin@targe...	CEO	

Showing 1 to 1 of 1 entries

Previous 1 Next

Close

Save changes

LETS BUILD A CAMPAIGN! Landing Page

The landing page dialog gives you a WYSIWYG editor to build the page the user will see when they click the phishing link

If “Capture Submitted Data” is checked, any posted forms will capture all user input (except passwords)

New Landing Page

Name:

Page name

Import Site

HTML

Undo Redo Bold Italic Text Color Background Color Link Unlink List Indent Outdent Styles Format

Source

☐ Capture Submitted Data ?

Cancel Save Page

LETS BUILD A CAMPAIGN! Landing Page

The landing page dialog gives you a WYSIWYG editor to build the page the user will see when they click the phishing link

If “Capture Submitted Data” is checked, any posted forms will capture all user input (except passwords)

New Landing Page

Name:

Open Enrollment Landing Page - Credential Capture

Import Site

HTML

X Undo Redo Bold Italic Text Color Background Color Link Unlink Table Insert Table Remove Table Full Screen Source

<!DOCTYPE html>
<html lang="en">
<head>
 <base href="https://www.healthcare.gov/login" /><meta charset="utf-8"/><meta content="IE=edge; chrome=1" http-equiv="X-UA-Compatible"/>
 <title>Health Insurance Marketplace for Individuals | HealthCare.gov</title>
 <meta name="description" content="" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8"/><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
</head>
<body>
</body>
</html>

☐ Capture Submitted Data ?

Cancel Save Page

LETS BUILD A CAMPAIGN! Landing Page

You can also import a valid site by using the “Import Site” function.

This hotlinks images and keeps links intact, so be careful!

Note: Some scripts may not work – test before going live with a phishing campaign

The image shows two overlapping windows from a web application. The background window is titled 'New Landing Page' and contains a 'Name:' label with a text input field labeled 'Page name'. Below this is a red-bordered button labeled 'Import Site'. Underneath the button is an 'HTML' editor with a toolbar containing icons for undo, redo, bold, italic, text color, background color, link, unlink, list, and table. The foreground window is titled 'Import Site' and features a 'URL:' label with a text input field containing the text 'http://google.com'. At the bottom right of this window are two buttons: 'Cancel' and 'Import'.

LETS BUILD A CAMPAIGN! Landing Page

For **red team** or offensive campaigns, the landing page dialog box has an option to capture passwords, and to redirect users to another page after the form is posted.

Red Tip: Send the users to a malicious payload (like an .hta) instead of a webpage

Blue Tip: Capture data but not passwords, redirect to a phishing education page

The image shows a web browser window with an HTML editor and a landing page configuration dialog box. The HTML editor displays the following code:

```
<!DOCTYPE html>
<html lang="en">
<head>
  <base href="https://www.healthcare.gov/login" /><meta charset="utf-8"/><meta
content="IE=edge; chrome=1" http-equiv="X-UA-Compatible"/>
  <title>Health Insurance Marketplace for Individuals | HealthCare.gov</title>
  <meta name="description" content="" /><meta http-equiv="Content-Type"
content="text/html; charset=utf-8"/><meta name="viewport" content="width=device-
width, initial-scale=1, maximum-scale=1">
</head>
<body>
</body>
</html>
```

The landing page configuration dialog box has the following options:

- ☒ Capture Submitted Data
- ☒ Capture Passwords

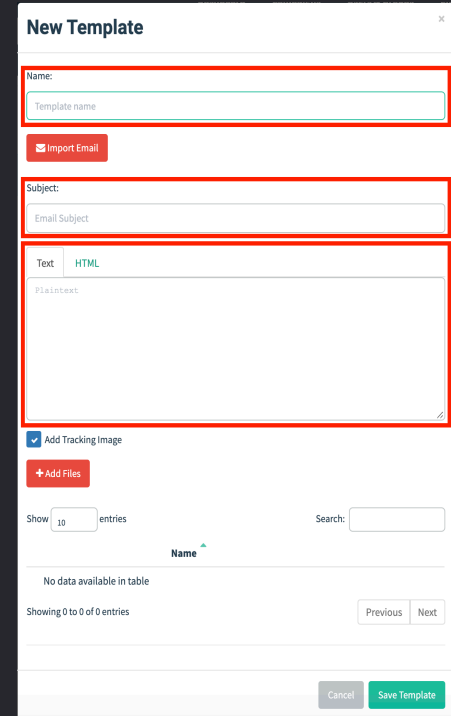
A warning message is displayed: **Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

Buttons: Cancel, Save Page

LETS BUILD A CAMPAIGN! Email Template

The Email Template dialog contains the text and HTML emails that will be sent to your targets.
Note you can import an email if you have one you want to clone.



The screenshot shows the 'New Template' dialog box. It has a title bar with 'New Template' and a close button. The main content area is divided into sections. The first section is 'Name:' with a text input field containing 'Template name'. The second section is 'Subject:' with a text input field containing 'Email Subject'. The third section is 'Text' and 'HTML' tabs, with the 'HTML' tab selected, showing a large text area with 'Placeholder text'. Below these sections are a checkbox for 'Add Tracking Image' (checked), an 'Add Files' button, and a table with columns 'Show' and 'Name'. The table is empty, showing 'No data available in table'. At the bottom are 'Cancel' and 'Save Template' buttons.

New Template

Name:

☒ Import Email

Subject:

Text HTML

Placeholder text

☒ Add Tracking Image

Show entries Search:

Name

No data available in table

Showing 0 to 0 of 0 entries

LETS BUILD A CAMPAIGN! Email Template

The Email Template dialog contains the text and HTML emails that will be sent to your targets.

Note you can import an email if you have one you want to clone.

New Template

Name:

Open Enrollment Email - Credential Capture

Import Email

Subject:

{{FirstName}}, Open Enrollment starts today!

TextHTML

XUndoRedoBoldItalicTextLinkListTableLinkListSource

B I T A Styles Normal

Dear {{FirstName}},

YourBenefitsOnline is pleased to partner with your employer for benefits selection during 2019 Open Enrollment! Using your custom portal page, you can:

- Review and select your healthcare plan (5 plans offered)
- Add additional coverages, such as Life and AD&D
- Manage dependents and add them to your plan

body p font

Add Tracking Image

Add Files

Show10entries

Search:

Name

No data available in table

Showing 0 to 0 of 0 entries

PreviousNext

CancelSave Template

LETS BUILD A CAMPAIGN! Variables

You may have noticed code such as `{{.FirstName}}` in previous slides. These are variables that draw from other parts of GoPhish to customize a campaign.

Variables	Source
<code>{{.FirstName}}</code> , <code>{{.LastName}}</code> , <code>{{.Email}}</code> , <code>{{.Position}}</code>	Users & Groups
<code>{{.RId}}</code> , <code>{{.TrackingURL}}</code> , <code>{{.Tracker}}</code> , <code>{{.URL}}</code> , <code>{{.BaseURL}}</code>	Campaigns
<code>{{.From}}</code>	Sending Profile

LETS BUILD A CAMPAIGN! Variables

You may have noticed code such as `{{.FirstName}}` in previous slides. These are variables that draw from other parts of GoPhish to customize a campaign.

`{{.LastName}}`

`{{.FirstName}}`

`{{.Email}}`

`{{.Position}}`

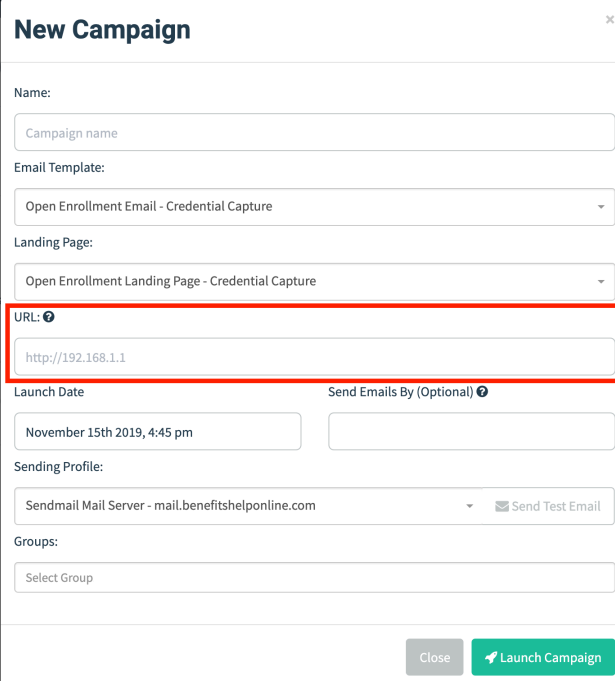
The screenshot shows the 'New Group' form in GoPhish. The form has a 'Name' field with the value 'Corporate Users - Sales Staff (US Only)'. Below the name field are two buttons: '+ Import Users' and 'Download CSV Template'. Below these buttons is a list of users with columns for First Name, Last Name, Email, and Position. The first user is 'Jayme Hancock' with email 'jayme@blackjackn'. The second user is 'Janitor' with a red '+ Add' button next to it. Below the list is a search bar and a table with columns for First Name, Last Name, Email, and Position. The table has one entry: 'Ben Franklin' with email 'bfranklin@targe...' and position 'CEO'. At the bottom of the form are 'Close' and 'Save changes' buttons.

First Name	Last Name	Email	Position
Ben	Franklin	bfranklin@targe...	CEO

LETS BUILD A CAMPAIGN! Creating The Campaign

The Campaign dialog box ties everything together. This allows you to mix and match by selecting one of each:

- Sending Profile
- User Group
- Email Template
- Landing Page



New Campaign [X]

Name:

Email Template:

Landing Page:

URL: ⓘ

Launch Date: Send Emails By (Optional) ⓘ

Sending Profile:

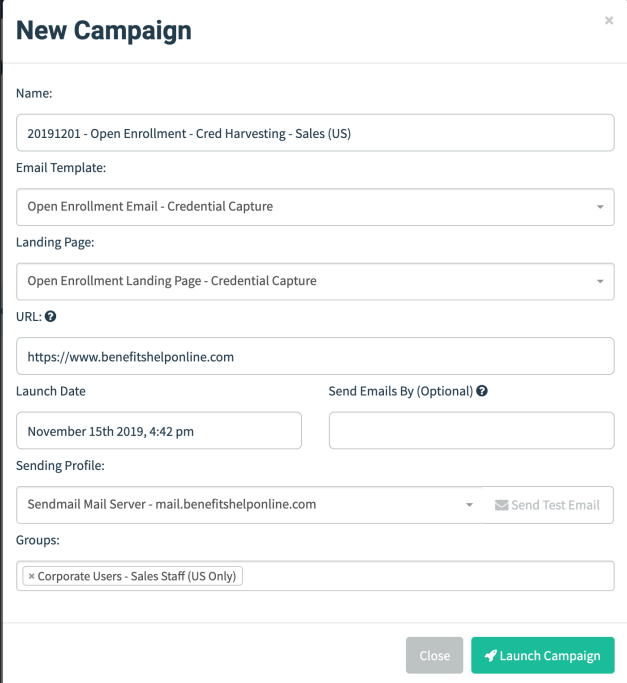
Groups:

LETS BUILD A CAMPAIGN! Creating The Campaign

The Campaign dialog box ties everything together. This allows you to mix and match by selecting one of each:

- Sending Profile
- User Group
- Email Template
- Landing Page

Note: As of this version, GoPhish doesn't have a dropdown for the URL. Be sure this is typed correctly and uses the correct protocol!



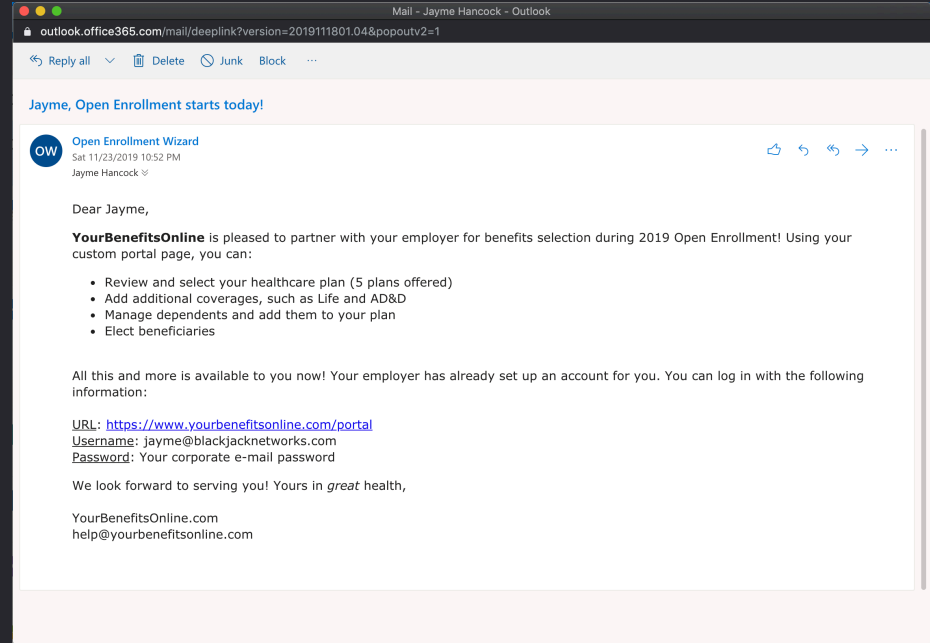
The screenshot shows the 'New Campaign' dialog box with the following fields and options:

- Name:** 20191201 - Open Enrollment - Cred Harvesting - Sales (US)
- Email Template:** Open Enrollment Email - Credential Capture
- Landing Page:** Open Enrollment Landing Page - Credential Capture
- URL:** https://www.benefitshelponline.com
- Launch Date:** November 15th 2019, 4:42 pm
- Send Emails By (Optional):** (Empty field)
- Sending Profile:** Sendmail Mail Server - mail.benefitshelponline.com
- Groups:** Corporate Users - Sales Staff (US Only)
- Buttons:** Close, Launch Campaign

LETS BUILD A CAMPAIGN! Sending The Campaign

Once the campaign is sent and confirmed, the user receives an email. Note that the variables (*{{.FirstName}}*, etc.) are replaced with actual values.

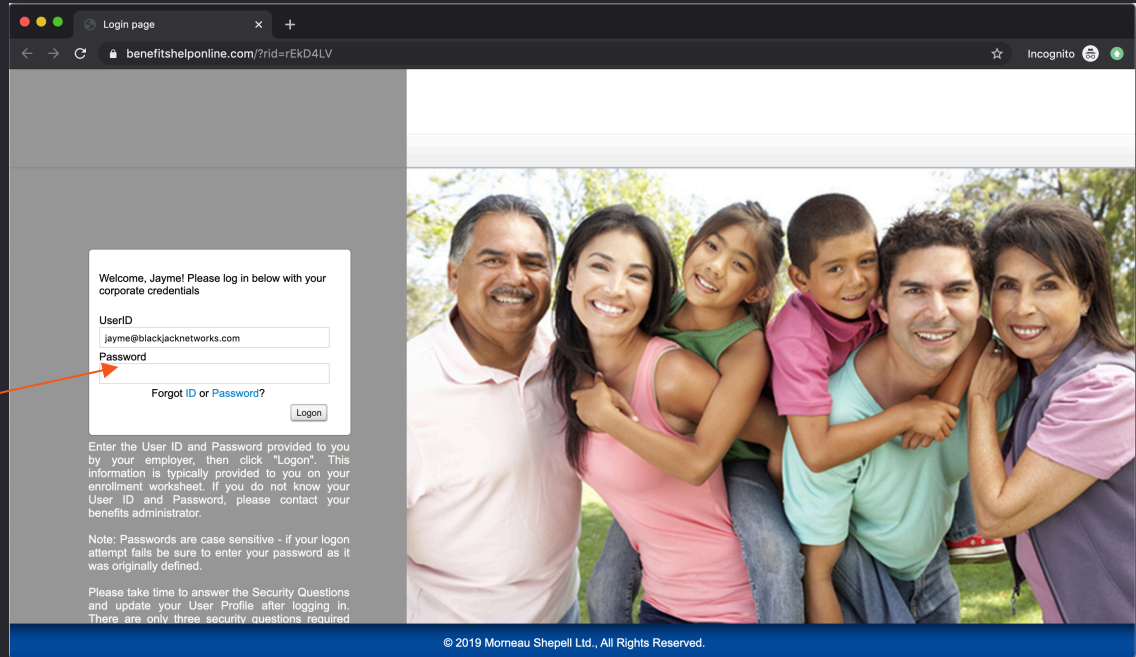
If the phish is convincing, the user clicks your link...



LETS BUILD A CAMPAIGN! Sending The Campaign

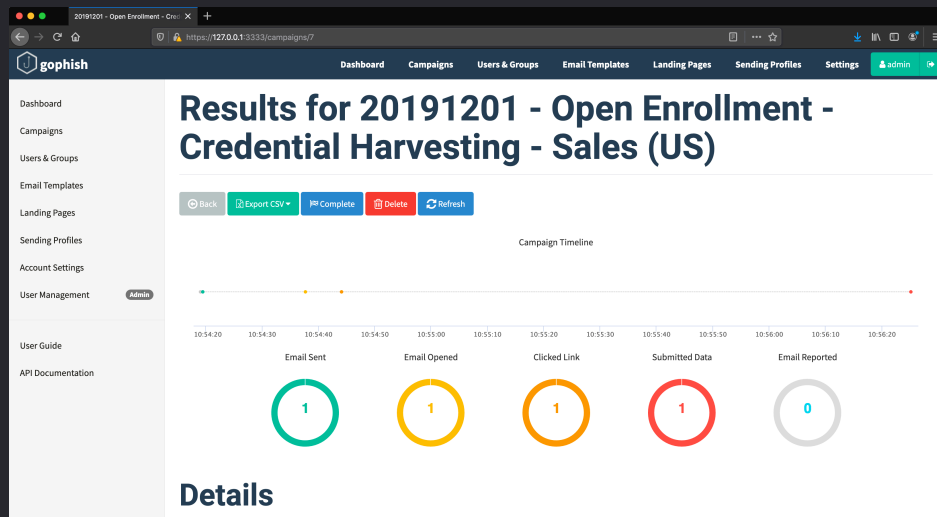
...and hits the landing page.

If the landing page is convincing, the user enters their creds...



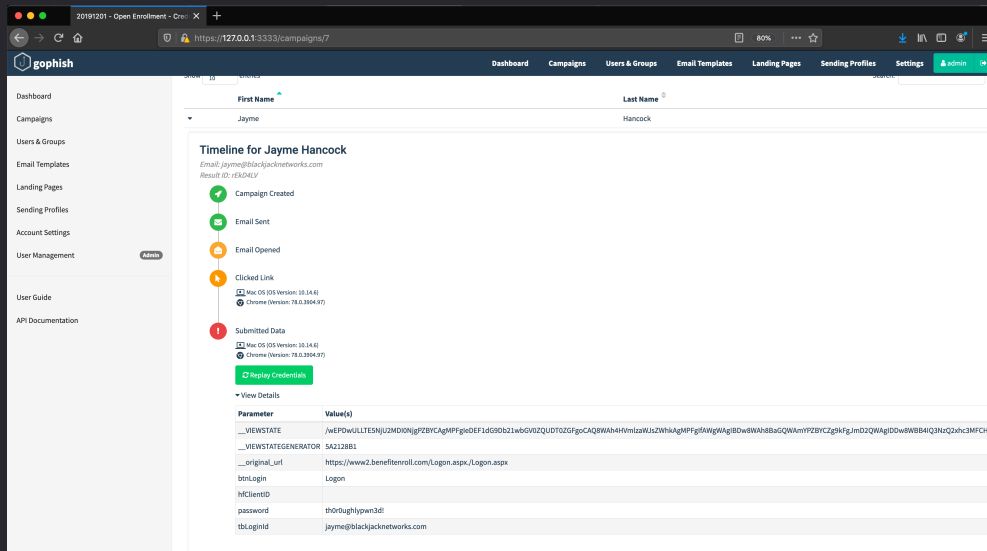
LETS BUILD A CAMPAIGN! Sending The Campaign

In the GoPhish Admin Console, under Campaigns, we can see a timeline of user interactions. Note that the one user in scope has opened the email, clicked the link, and entered data.



LETS BUILD A CAMPAIGN! Sending The Campaign

Selecting a user and scrolling down gives a detailed timeline, and all submitted data. We've now got credentials to continue our attack.



Now that we can phish, lets talk Phishing Strategy

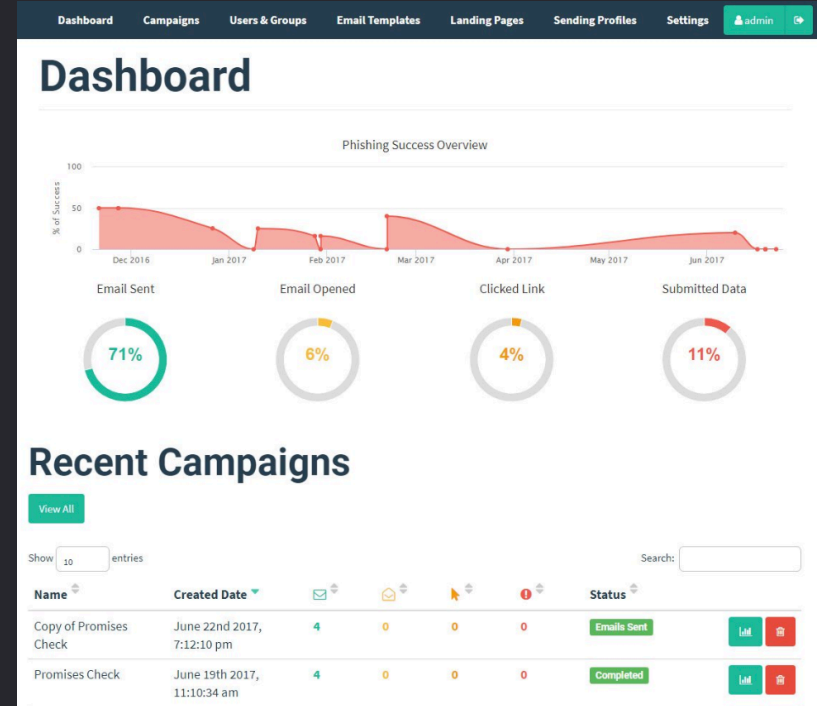
BLUE TEAM

GOALS: Blue Team

- Metrics, Metrics, Metrics
- Measuring security posture
- User Awareness Training
- Justification of services / controls

GOALS: Blue Team

- Metrics, Metrics, Metrics
 - Built in dashboard gives (limited) info at a glance



https://twitter.com/jw_sec

GOALS: Blue Team

- Metrics, Metrics, Metrics
 - Campaign Export:
 - **Results**
 - Raw Events

id	status	ip	latitude	longit	send_date	reported	modified_da	email	first_name	last_name
rEkD4LV	Submitted Data	100.15.	38	-97	2019-11-24T	FALSE	2019-11-24T	jayme@	Jayme	Hancock
f2LgMg2	Submitted Data	99.241.	38	-97	2019-11-24T	FALSE	2019-11-24T	testuser@	Tom	Jones
a93MgnT	Clicked Link	13.4.11	38	-97	2019-11-24T	FALSE	2019-11-24T	internet@	Bob	Barker
t8f821v	Email Opened	91.91.3	38	-97	2019-11-24T	FALSE	2019-11-24T	fakeuser	Fake	User

“Export CSV > Results”

GOALS: Blue Team

- Metrics, Metrics, Metrics
 - Campaign Export:
 - Results
 - **Raw Events**

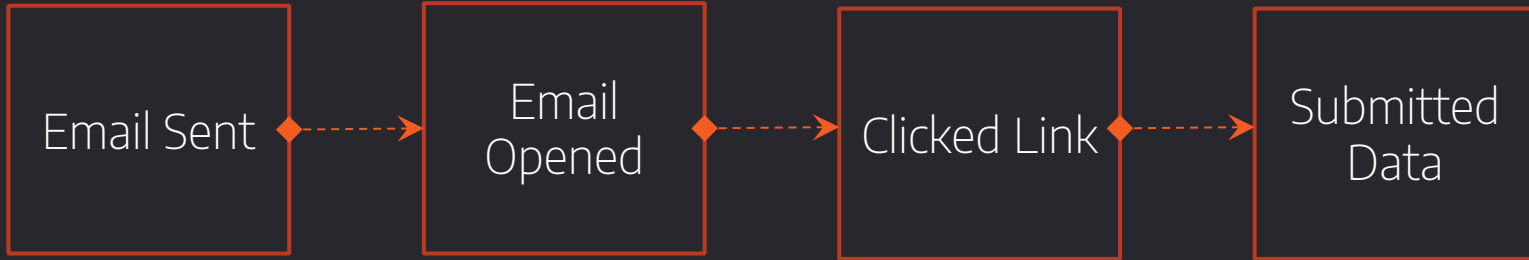
email	time	message	details				
	2019-11-24T03:54:19.096	Campaign Created					
jayme@	2019-11-24T03:54:19.544	Email Sent					
jayme@	2019-11-24T03:54:37.708	Email Opened	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T03:54:44.140	Clicked Link	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T03:56:25.197	Submitted Data	{ "payload": { " __VIEWSTATE": ["/wEPDwULLTE5NjU2MDI0Njg0f				
jayme@	2019-11-24T16:44:38.721	Email Opened	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T16:45:45.869	Clicked Link	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T16:45:47.150	Clicked Link	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T16:46:04.585	Clicked Link	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T16:46:04.756	Clicked Link	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T16:47:17.600	Clicked Link	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				
jayme@	2019-11-24T16:47:17.807	Clicked Link	{ "payload": { "rid": ["rEkD4LV"] }, "browser": { "address": "100.15.2				

“Export CSV > Raw Data”

GOALS: Blue Team

Phishing Lifecycle:

Only the latest step is reported in the “Results” output



GOALS: Blue Team

- Metrics, Metrics, Metrics
 - Reporting: GoReport
 - Clean reporting style
 - Customizable .docx
 - Perfect for internal deliverables

Executive Summary

Campaign Results For: Demo Campaign
Status: In progress
Created: 17:08:13 on 2019-03-29
Started: 17:08:13 on 2019-03-29
Completed: Still Active

Campaign Details

From: Example Sender <foo@example.com>
Subject:
Phish URL: http://localhost
Redirect URL: Not Used
Attachment(s): None Used
Captured Credentials: False
Stored Passwords: False

High Level Results

Total Targets: 298

The following totals indicate how many events of each type occurred:

Total Open Events: 159
Total Click Events: 37
Total Report Events: 12
Total Submitted Data Events: 1

The following totals indicate how many targets participated in the campaign:

Individuals Who Opened: 159
Individuals Who Clicked: 37
Individuals Who Reported: 12
Individuals Who Submitted: 1

Summary of Events

The following table summarizes who opened and clicked on emails sent in this campaign.

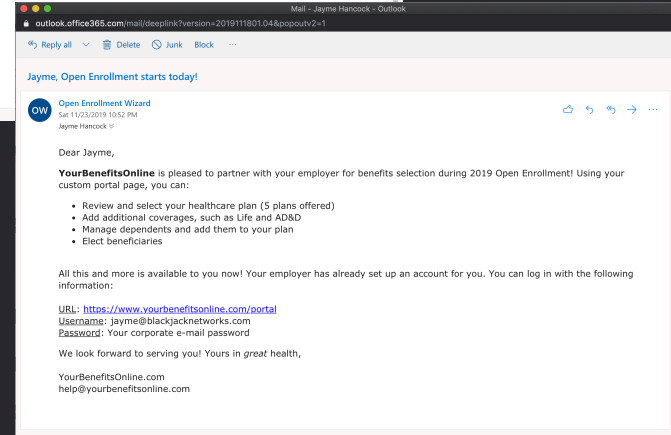
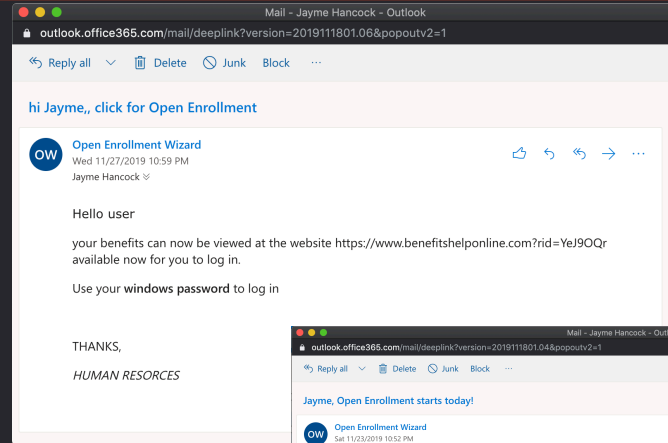
Email Address	Open	Click	Data	Report	OS	Browser
Aaron.Koch@example.com	✓	✗	✗	✗	N/A	N/A
Aaron.Lopez@example.com	✗	✗	✗	✗	N/A	N/A
Adrian.Cross@example.com	✗	✗	✗	✗	N/A	N/A
Aimee.Graham@example.com	✓	✗	✗	✗	N/A	N/A
Alejandro.Stevens@example.com	✗	✗	✗	✗	N/A	N/A
Alexandria.Marshall@example.com	✗	✗	✗	✗	N/A	N/A
Alison.Casey@example.com	✓	✗	✗	✗	N/A	N/A
Alyssa.Morgan@example.com	✓	✗	✗	✗	N/A	N/A
Amanda.Atkins@example.com	✓	✓	✗	✗	Windows XP	Firefox 5.0
Amanda.Sanchez@example.com	✓	✗	✗	✗	N/A	N/A
Amanda.Stone@example.com	✓	✗	✗	✗	N/A	N/A
Amy.Ross@example.com	✓	✗	✗	✗	N/A	N/A
Andrea.Powers@example.com	✗	✗	✗	✗	N/A	N/A
Andrew.Bryan@example.com	✗	✗	✗	✗	N/A	N/A
Andrew.Citessa@example.com	✗	✗	✗	✗	N/A	N/A

<https://github.com/chrismaddalena/GoReport>

GOALS: Blue Team

- Measuring Security Posture
 - Email Sophistication

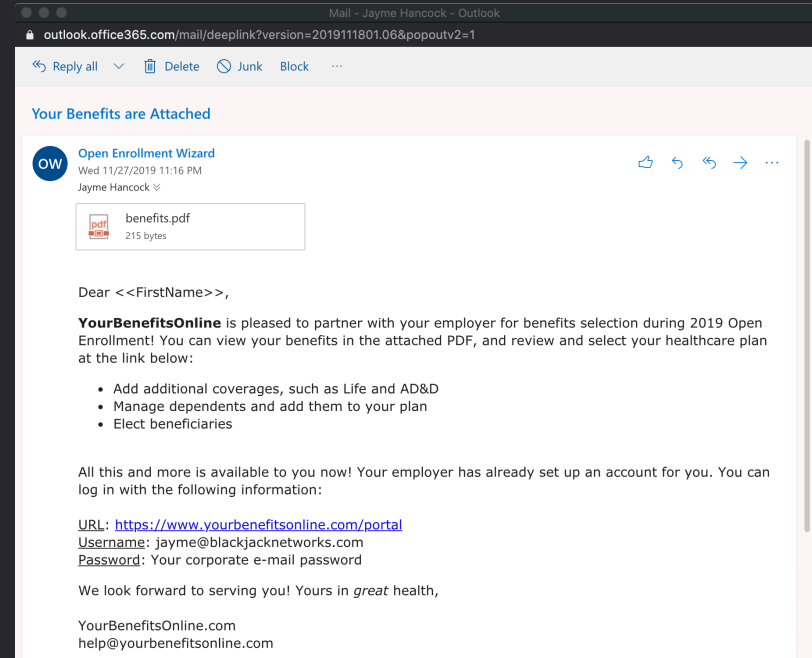
What level of sophistication gets spotted/reported? Which slips through?



GOALS: Blue Team

- Measuring Security Posture
 - Email Sophistication

Do users open emails with attachments more often?

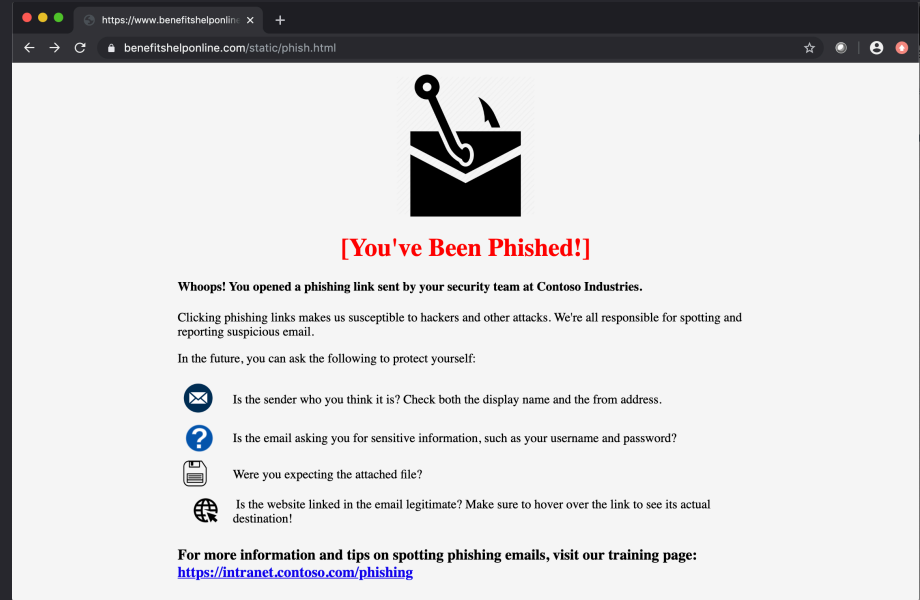


GOALS: Blue Team

- User Awareness Training
 - Redirect URL

Save static assets in:
gophish/static/endpoint

They'll upload to:
<https://phishingurl.com/static/file.html>



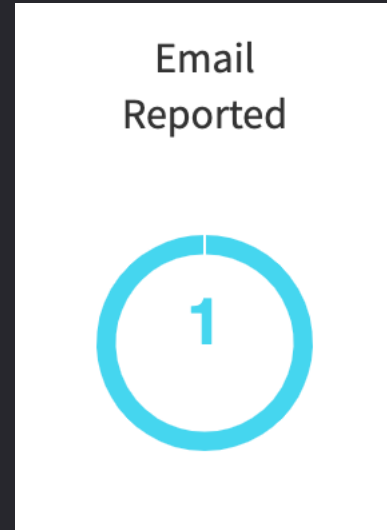
GOALS: Blue Team

- User Awareness Training
 - Built-In Reporting

GoPhish has a “Report” functionality built-in.
Navigating to:

<https://phishingurl.com/report?rid={{.Rid}}>

Sets the report flag to “Yes”



GOALS: Blue Team

- User Awareness Training
 - Built-In Reporting

Downside: Server-side code exists to handle reporting. Client-side does not.

- You can build an Outlook/Gmail plug-in
- You can give your admins a tool like PhishReporter.py:

<https://github.com/highmeh/phishing/blob/master/phishreporter.py>

```
$ ./phishreporter.py
[+] Connecting...
[?] Enter RID to report: rEkD4LV
[+] Locating the campaign for rEkD4LV...
[+] Found RID in Campaign #7...
[+] jayme@blackjacknetworks.com reported rEkD4LV as a phishing email!
```

GOALS: Blue Team

- Justification of services / controls

Pretty self explanatory: If your users continue to click phishing emails despite testing and training, you may be able to justify implementing additional technical controls. Data talks.

RED TEAM

GOALS: Red Team

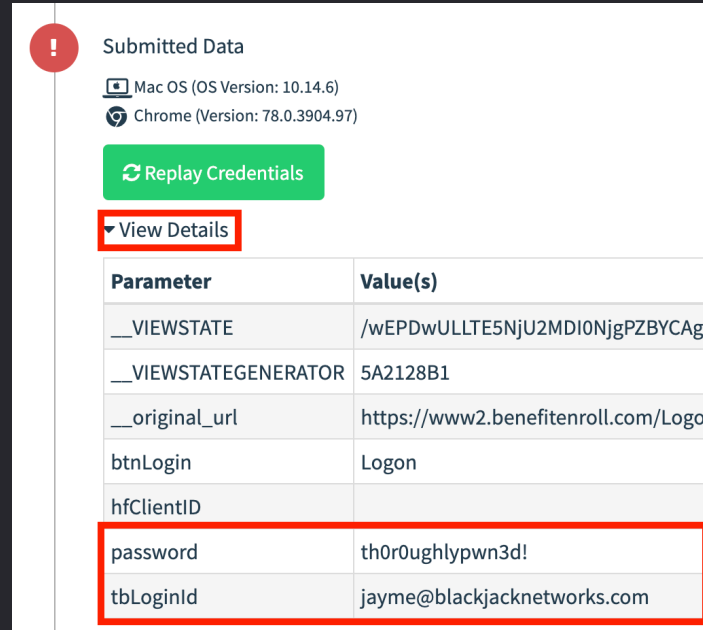
- Capture Credentials
- Deliver Payloads

GOALS: Red Team

- Capture Credentials
 - Raw Capture
 - Log in to service

GOALS: Red Team

- Capture Credentials
 - **Raw Capture**
 - Log in to service



The screenshot displays a web application interface with a red exclamation mark icon in the top left corner. The main content area is titled "Submitted Data" and includes the following information:

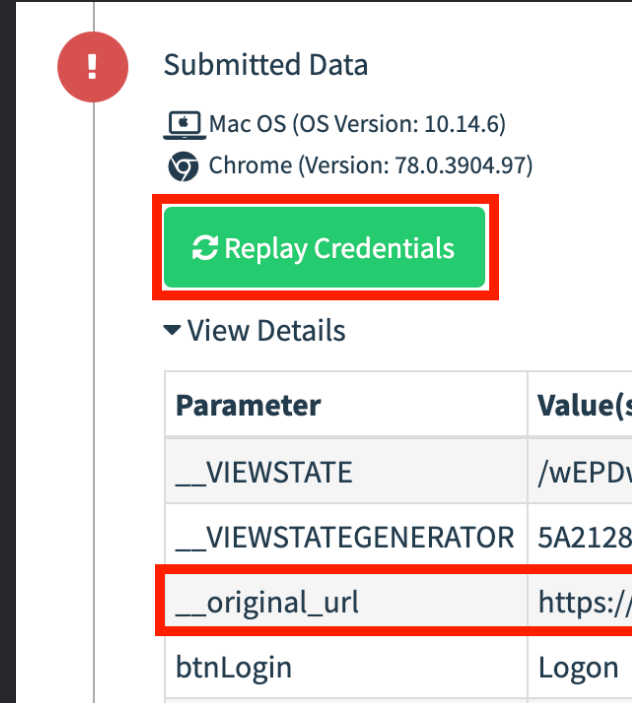
- Mac OS (OS Version: 10.14.6)
- Chrome (Version: 78.0.3904.97)
- A green button labeled "Replay Credentials"
- A red-bordered button labeled "View Details"

Below the "View Details" button is a table with two columns: "Parameter" and "Value(s)". The table contains the following data:

Parameter	Value(s)
__VIEWSTATE	/wEPDwULLTE5NjU2MDI0NjgPZBYCAgM
__VIEWSTATEGENERATOR	5A2128B1
__original_url	https://www2.benefitenroll.com/Logon
btnLogin	Logon
hfClientID	
password	th0r0ughlypwn3d!
tbLoginId	jayme@blackjacknetworks.com

GOALS: Red Team

- Capture Credentials
 - Raw Capture
 - **Log in to service**



The screenshot displays a web application interface with a red warning icon and the text "Submitted Data". Below this, it shows the operating system and browser information: "Mac OS (OS Version: 10.14.6)" and "Chrome (Version: 78.0.3904.97)". A green button labeled "Replay Credentials" is highlighted with a red border. Below the button is a dropdown menu labeled "View Details". A table with two columns, "Parameter" and "Value(s)", is shown. The table contains four rows: "__VIEWSTATE" with value "/wEPDv", "__VIEWSTATEGENERATOR" with value "5A2128", "__original_url" with value "https://", and "btnLogin" with value "Logon". The row containing "__original_url" is highlighted with a red border.

Submitted Data

Mac OS (OS Version: 10.14.6)

Chrome (Version: 78.0.3904.97)

Replay Credentials

▼ View Details

Parameter	Value(s)
__VIEWSTATE	/wEPDv
__VIEWSTATEGENERATOR	5A2128
__original_url	https://
btnLogin	Logon

GOALS: Red Team

- Capture Credentials
 - Raw Capture
 - **Log in to service**

Sends a post request with the captured data in a separate browser window

**Where do you want the
credentials submitted to?**

<https://www.totallylegit.com/submit.aspx>

OK

Cancel

GOALS: Red Team

- **Deliver Payloads**
 - Email Attachment
 - Host and redirect

GOALS: Red Team

- Deliver Payloads
 - **Email Attachment**
 - Host and redirect

New Template

Name:
Open Enrollment Email - Credential Capture (Attachment)

Import Email

Subject:
Your Benefits are Attached

Text **HTML**

X Undo Bold Italic Link Unlink Source

`<html>
<head>
 <title></title>
</head>
<body>
<p>Dear <<FirstName>>,&br/></p>`

Add Tracking Image

+ Add Files

Show 10 entries Search:

Name
benefits.pdf

Showing 1 to 1 of 1 entries Previous 1 Next

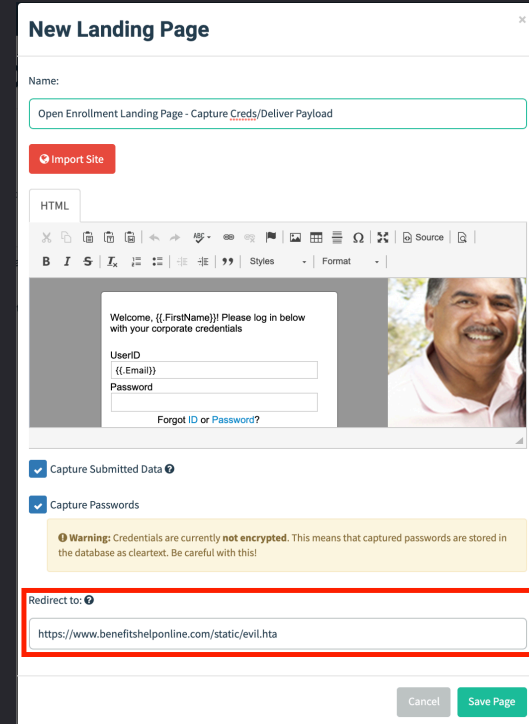
Cancel Save Template

GOALS: Red Team

- Deliver Payloads
 - Email Attachment
 - **Host and redirect**

Save payloads (ex: evil.hta) in:
gophish/static/endpoint

They'll upload to: <https://phishingurl.com/static/evil.hta>



The screenshot shows the 'New Landing Page' configuration window in Gophish. The 'Name' field is set to 'Open Enrollment Landing Page - Capture Creds/Deliver Payload'. Below this is an 'Import Site' button. The main content area shows a preview of the landing page, which includes a welcome message with a placeholder for the first name, a login form with fields for 'UserID' (placeholder: {{.Email}}) and 'Password', and a 'Forgot ID or Password?' link. To the right of the form is a placeholder image of a man. Below the preview, there are two checked options: 'Capture Submitted Data' and 'Capture Passwords'. A warning message states: 'Warning: Credentials are currently not encrypted. This means that captured passwords are stored in the database as cleartext. Be careful with this!'. At the bottom, the 'Redirect to:' field is highlighted with a red box and contains the URL 'https://www.benefitshelponline.com/static/evil.hta'. 'Cancel' and 'Save Page' buttons are at the bottom right.

TARGET COLLECTION

The important part

TARGET COLLECTION

Targeting the right users is crucial to both red and blue team engagements

For Red: Staying in scope, finding likely targets

For Blue: Targeting training and continuous phishing

TARGET COLLECTION

Blue:

Determine users in scope, generate a list. Modify the list as data is gathered

Use Open-Source Intelligence Gathering to determine footprint available to an attacker

TARGET COLLECTION

Red:

Ask for a list of approved contacts, or a list of users to exclude

Use Open-Source Intelligence Gathering to find your targets

TARGET COLLECTION

Automation

Multiple open-source tools exist to help collect target data from public internet sources.

TARGET COLLECTION

Automation: Lure

Lure scrapes webpages, pilfers email search pages, and checks databases to find targets. It's **designed** to work with GoPhish.

<https://github.com/highmeh/lure>

```
L U R E | Phishing Target Collection Automation
          jayme.hancock@bsigroup.com
```

```
-----
[X] Hunter.io           [+] GoPhish Server Online
[X] LinkedIn           [!] HIBP Checking Disabled
[X] GitHub
[ ] TheHarvester
[X] MailsHunt
[ ] Scrape Webpage
-----
```

```
[+] Checking hunter.io (980/1000 queries remaining)
[+] Checking LinkedIn (via Bing Search)
[+] Searching GitHub
[+] Checking MailsHunt
[+] Final list contains 149 targets.
[+] Target list '20191201201241_Jayme_contoso.com' (ID: 2) added!
```

BEST PRACTICES

Increasing Effectiveness

GENERAL TIPS: HTTPS

Configure HTTPS!

By default, GoPhish uses a self-signed certificate. This isn't good if you want a successful campaign.

- Use LetsEncrypt!
- After issuing a certificate, add the path to config.json and enable TLS:

```
"use_tls": true,  
"cert_path": "/etc/letsencrypt/live/domain/fullchain.pem",  
"key_path": "/etc/letsencrypt/live/domain/privkey.pem"
```

GENERAL TIPS: HTTPS

HTTPS: Multiple Phishing Domains

If you host multiple phishing domains, consider configuring a TLS certificate with Subject Alternative Names:

```
$certbot certonly -d phishingdomain.com -d anotherphishingdomain.com -d  
athirdphishingdomain.com -d evenmorephishingdomains.net
```


GENERAL TIPS: TRANSPARENCY

GoPhish adds two headers to each email by default:

“X-Mailer: GoPhish”

“X-Gophish-Contact: admin@domain.com”

These add transparency to your campaigns:

- Identifies you as non-malicious to incident responders
- Provides an abuse contact

More info: <https://github.com/gophish/gophish/issues/1057>

GENERAL TIPS: TRANSPARENCY

Red teaming and afraid this will burn you?

Compile it yourself; comment out references to “X-Mailer” and “config.ServerName”:

```
gophish/models/maillog_test.go
gophish/models/maillog.go
gophish/models/smtp_test.go
gophish/models/email_request.go
gophish/models/email_request_test.go
```

GENERAL TIPS: MAIL SERVERS

High Reputation Mail Servers

Sure, you can install up Sendmail and get your DNS records configured...

- Is the server configured properly?
- Are SPF, DKIM, and DMARC configured correctly?
- Has your mail server's IP been blacklisted in the past?

Consider using a high reputation mail server; many are available for free under a certain threshold (usually around ~10,000 emails per month.) Ex: Amazon SES, Sendgrid

TAKEAWAYS

In summary...

KEY TAKEAWAYS

Phishing doesn't have to be difficult.

Creating convincing campaigns shouldn't be subject to your budget.

Attackers aren't just hitting your external hosts and giving up – educate and prepare your users.

Numbers talk – baselining your users' social engineering readiness will get initiatives pushed through faster.

THANKS!

ANY QUESTIONS?

@highmeh