gophish

User Guide

Table of Contents

What is Gophish?

Gophish is a phishing framework that makes the simulation of real-world phishing attacks dead-simple. The idea behind gophish is simple – make industry-grade phishing training available to *everyone*.

"Available" in this case means two things –

- **Affordable** – Gophish is currently open-source software that is completely free for anyone to use.
- **Accessible** – Gophish is written in the Go programming language. This has the benefit that gophish releases are compiled binaries with no dependencies. In a nutshell, this makes installation as simple as "download and run"!

Version

This User Guide is for gophish "community edition" version 0.1.2.

License

Community Edition

```
The MIT License (MIT)

Copyright (c) 2013-2016 Jordan Wright

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
```

Key Terms

The following key terms will be used in this document:

- Campaign – A single set of emails (built with templates) sent to one or more groups of users
- User – A single target of phishing campaigns
- Group – A group of Users
- Template – An email template (subject, body, attachments, etc.) to be used in Campaigns
- Landing Page – HTML that is presented when a user clicks the phishing link

Setup

Installation

Installing Gophish Using Pre-Built Binaries

Gophish is provided as a pre-built binary for most operating systems. With this being the case, installation is as simple as downloading the ZIP file containing the binary that is built for your OS and extracting the contents.

Installing Gophish from Source

One of the major benefits of having written gophish in the Go programming language is that it is extremely simple to build from source. All you will need is the Go language and a C compiler (such as gcc).

To install gophish, simply run "`go get github.com/gophish/gophish`". This downloads gophish into your $GOPATH.

Next, navigate to $GOPATH/src/github.com/gophish/gophish and run the command "`go build`". This builds a gophish binary in the current directory.

Understanding the config.json

There are some settings that are configurable via a file called config.json, located in the gophish root directory. Here are some of the options that you can set to your preferences:

Key	Value (Default)	Description
admin_server.listen_url	127.0.0.1:3333	IP/Port of gophish admin server
admin_server.use_tls	false	Use TLS for admin server?
admin_server.cert_path	example.crt	Path to SSL Cert
admin_server.key_path	example.key	Path to SSL Private Key

Creating SSL Certificate and Private Keys

It's a good idea to have the admin server available over HTTPS. While automatic SSL cert/key generation will be included in a later release, for now let's take a look at how we can leverage openssl to generate our cert and key for use with gophish (this assumes you already have openssl installed!)

We can start the certificate and key generation process with the following command:

```
openssl req -newkey rsa:2048 -nodes -keyout gophish.key -x509 -days 365 -out
gophish.crt
```

Then, all we have to do is answer the CSR process that asks for details such as country, state, etc. Since this is a local self-signed cert, these won't matter too much to us.

This creates two files, gophish.key and gophish.crt. After moving these files into the gophish root directory (in the same folder as config.json), we can have the following in our config.json file:

```
"admin_server" : {
      "listen_url" : "127.0.0.1:3333",
      "use_tls" : true,
      "cert_path" : "gophish.crt",
      "key_path" : "gophish.key"
```

```
    }
```
Now when we launch gophish, you'll connect to the admin server over HTTPS and accept the self-signed certificate warning.

Running Gophish

Now that you have gophish installed, you're ready to run the software. To launch gophish, simply open a command shell and navigate to the directory the gophish binary is located.

Then, execute the gophish binary. You will see some informational output showing both the admin and phishing web servers starting up, as well as the database being created. This output will tell you the port numbers you can use to connect to the web interfaces.

```
gophish@gophish.dev:~/src/github.com/gophish/gophish$ ./gophish
 2016/01/10 23:13:42 worker.go:34: Background Worker Started Successfully - Waiting
for Campaigns
 2016/01/10 23:13:42 models.go:64: Database not found... creating db at gophish.db
 2016/01/10 23:13:42 gophish.go:49: Admin server started at http://127.0.0.1:3333
 2016/01/10 23:13:42 gophish.go:51: Phishing server started at http://0.0.0.0:80
```

Managing Users

Gophish allows you to create and manage multiple user accounts, each with their own templates, campaigns, groups, etc. Here are some common actions on how to manage these accounts:

DANGER:

*When you first launch gophish, you should immediately change the admin password,
as the default is clearly published!*

Changing Your Password

To change your password, first login to gophish. Then, navigate to "Settings":

Figure 1 - Settings Page

From here, you can change your password by filling out the field "Old Password" with your current password and by filling out the field "New Password" with the password you want to set.

When you click "Save", you should see a confirmation message that your password has been changed.

Changing Your API Key

If you ever need to change your API key, you can do so from the "Settings" page. After clicking the "Reset" button, you will see a confirmation message that the reset was successful:

Figure 2 - Resetting API Key

Registering a New Account

By default, only the admin account is registered. Only existing accounts can register new gophish users. To register a new account, navigate to http://[gophish]/register or click the "Add User" button on the Settings page:
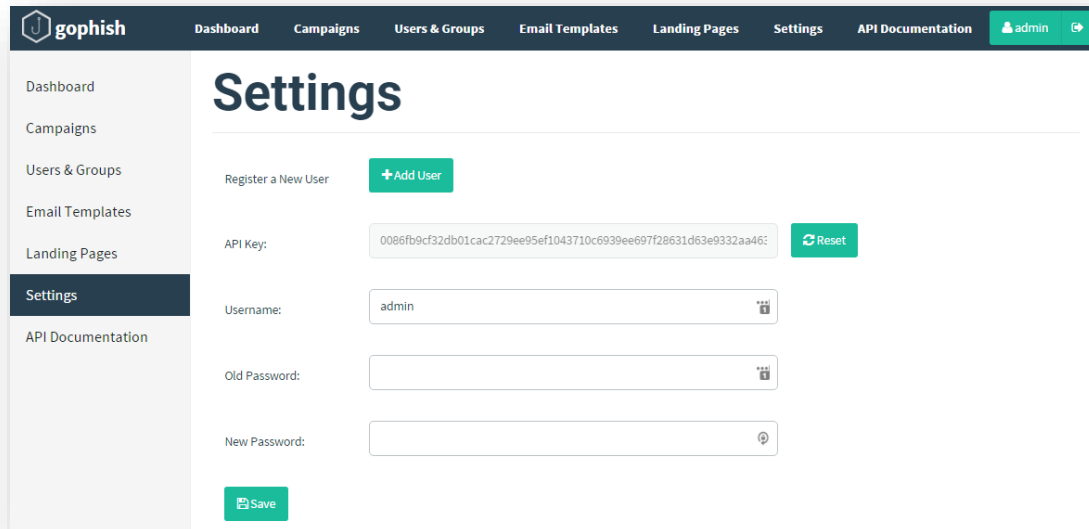

Figure 3 - Add User Button

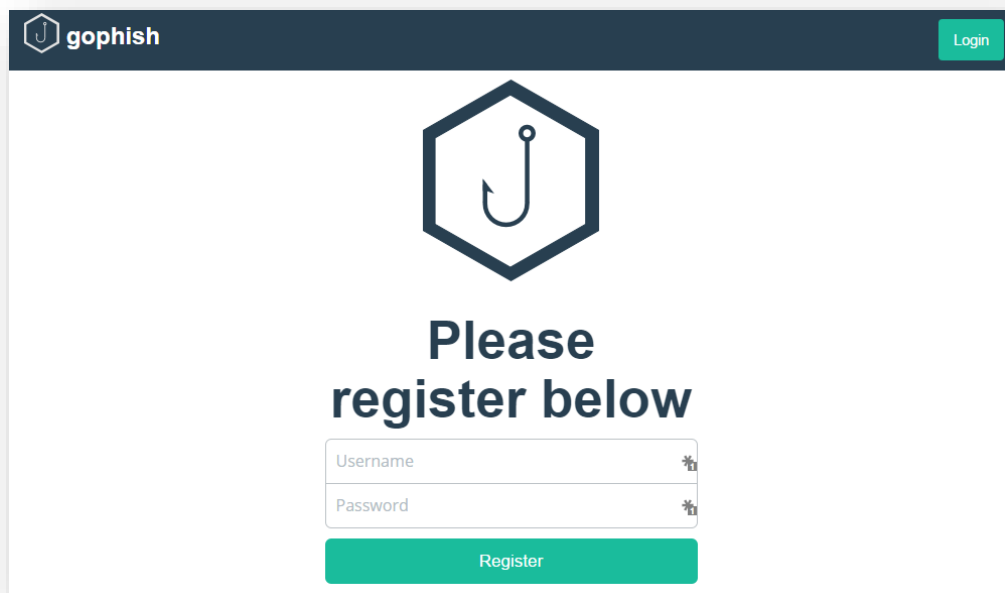On this page, you can create a new username/password.

Figure 4 - Registering a New Account

After creating this account, you will be taken to the login page, where you can login using the new account's credentials.

Now let's setup a campaign!

Introducing Morning Catch Corporation

For this documentation, we will step through the process of setting up users, templates, and a full campaign from scratch for a fake company called Morning Catch. In this case, we are assuming the role of a security administrator of Morning Catch and have been given the authorization to perform this training.

As a note, this fake company is based on a great VM used specifically for testing phishing frameworks that you can download here if you're interested.

The fake company will consist of 3 users: Richard Bourne, Boyd Jenius, and Haiti Moreo.

How to Setup a Campaign from Scratch

Now that we have adjusted the settings to our liking, let's run a campaign! There are a minimum of three steps you need to launch a phishing campaign from gophish:

1. Create the list of users to be targeted
2. Create the email template (the "phish")
3. Create and execute the actual campaign

Let's show each step in detail to see how we can run a campaign against the employees of Morning Catch.

Creating Users & Groups

The first thing we need to do before we can launch a campaign is to figure out who to target. There are a *ton* of ways to gather/generate email addresses for potential targets. You can either harvest email addresses from public information using OSINT if you are aiming to simulate a realistic scenario.

Now that we have our list of users, let's import them into gophish.

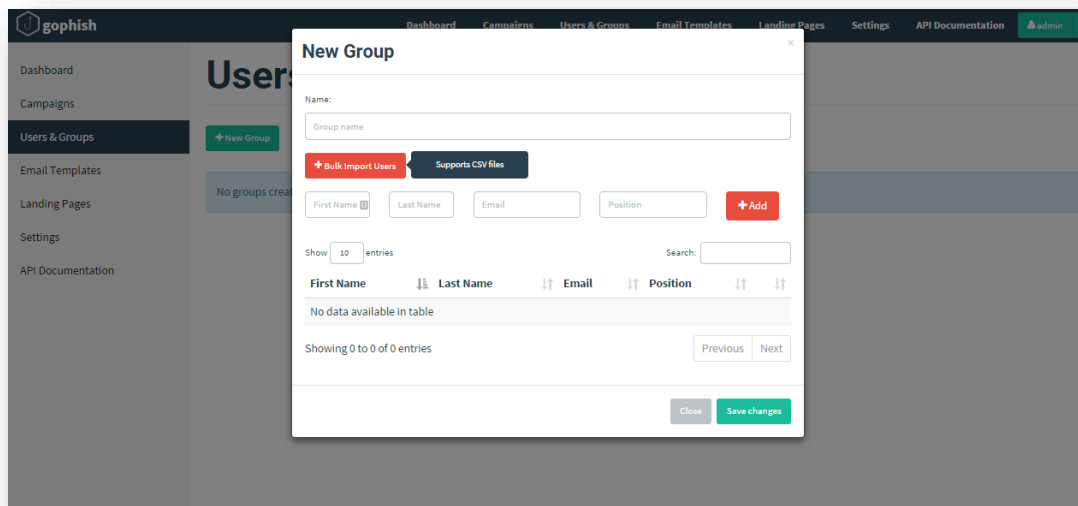To add a group, navigate to the "Users & Groups" page and click "New Group":

Figure 5 - Creating a Group

Since we are performing phishing simulation for Morning Catch, we can call our group "Morning Catch Employees".

Now we have to add the members. There are two ways to do this:

- Add each member's details one at a time using the form inputs
- Bulk import the group from a CSV file

To save time (and typing!) let's go with the CSV option.

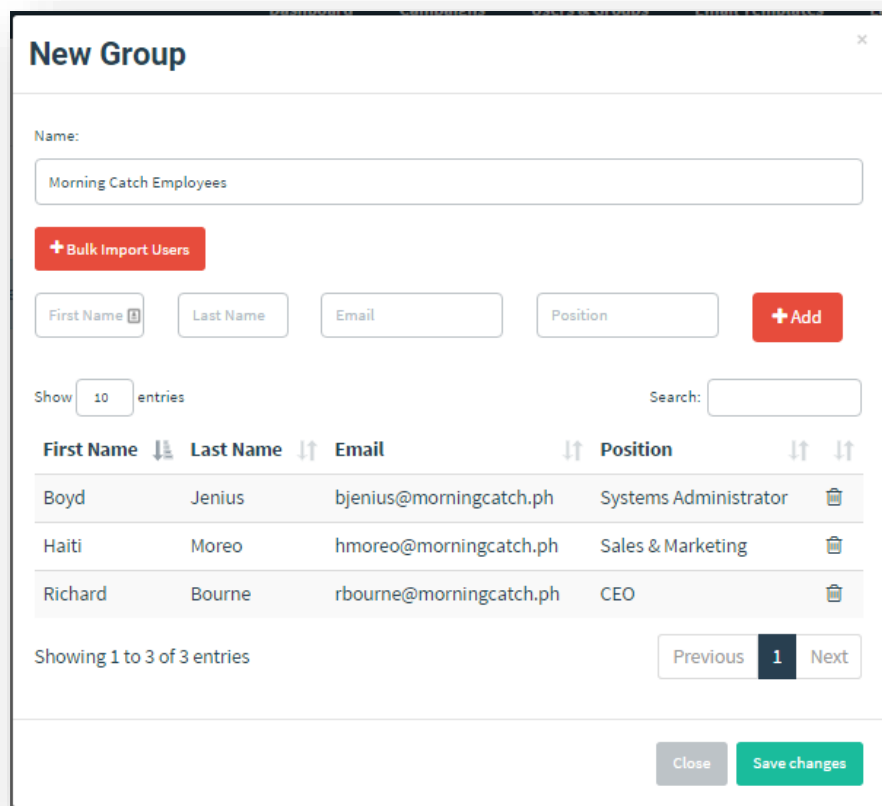The CSV format gophish expects has the following header values:

- First Name
- Last Name
- Email
- Position

So, the CSV for Morning Catch would look like the following:

```
First Name, Last Name, Position, Email, Company
Richard,Bourne,CEO,rbourne@morningcatch.ph,Morning Catch
Boyd,Jenius,Systems Administrator,bjenius@morningcatch.ph,Morning Catch
Haiti,Moreo,Sales & Marketing,hmoreo@morningcatch.ph,Morning Catch
```

Figure 6 - Morning Catch Employees CSV

After uploading this CSV using the "Bulk Import Users" button, we see that our members were added automatically:

Figure 7 - Importing Users from CSV

After clicking "Save changes", we see a confirmation message that our group was created.

Tip:

If you don't see the group show up right away, refresh the page and it should appear in the table.

Creating Templates

A "Template" is the content of the emails that are sent to targets. They can be imported from an existing email, or created from scratch. Additionally, templates can contain tracking images so that gophish knows when the user opens the email.

To create a template, first navigate to the "Email Templates" page and click the "New Template" button.

Figure 8 - Template Creation Page

For our example, let's create a template from scratch to send to the employees of Morning Catch.

We notice that Morning Catch comes with a webmail portal. Let's craft a simple template that suggests the user needs to go reset their password. Obviously, this is a simple scenario, and by using the "Import Email" feature, you can import existing emails directly into gophish for a greater effect.

By clicking the "HTML" tab, we will see the editor we can use to create our HTML content:
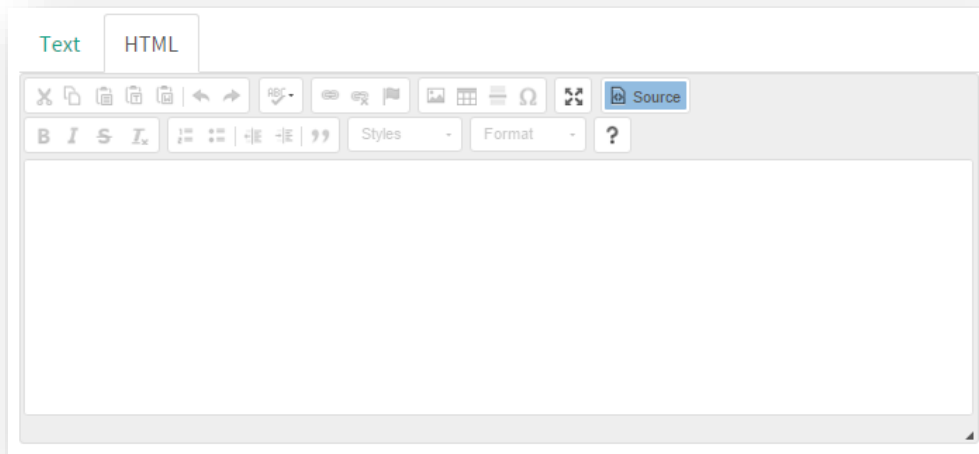
Figure 9 - HTML Editor

Since our content is pretty simple, we can just click the "Source" button and be taken to the more visual editor, which will be enough for our purposes:
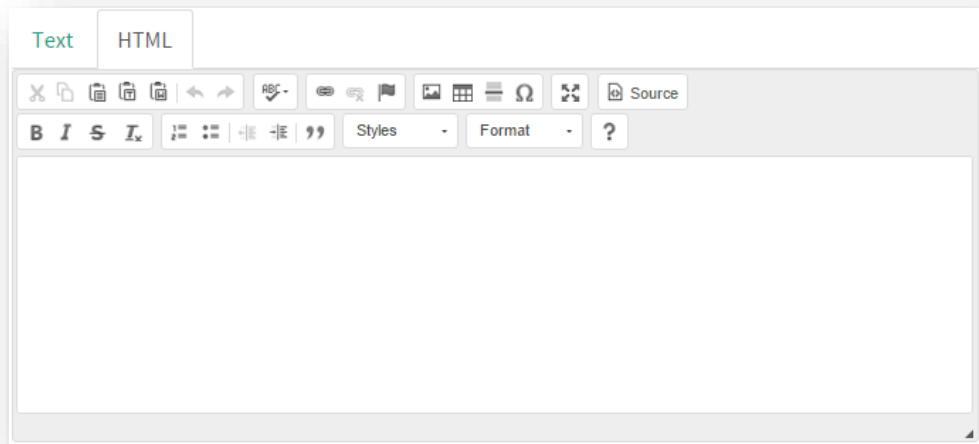
Figure 10 - Visual HTML Editor

For now, we will include the following text in the HTML portion of the email:

"Dear {{.FirstName}}

Records have indicated that your webmail password may have been compromised in a recent data loss incident. As soon as possible, please reset your webmail password using this link.

Regards,

{{.From}}"

Wait – what are those "{{.FirstName}}" things? These are **template variables**. This is part of a very powerful feature of gophish that allows us to tailor the emails and landing pages users see to their specific details. For example, a user named "John Doe" might see "Dear John" when he receives the email. You can find a full listing of the supported template variables in the Appendix.
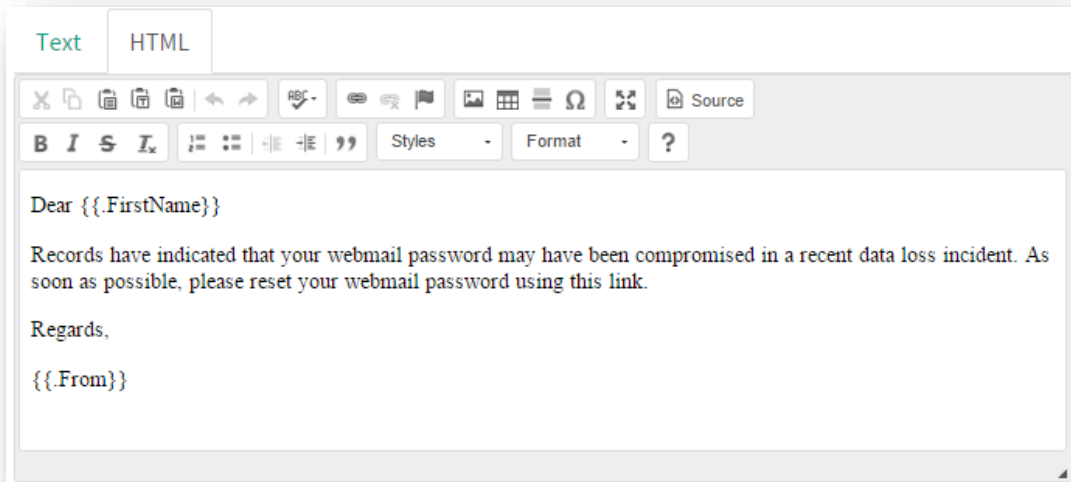

Figure 11 - HTML Editor with Content

You'll notice that we selected the checkbox that says "Add Tracking Image". This adds a 1x1 image that is used to track if the user opens the email. Without this, you will not be able to know if the user opened the email unless they click the link to your {{.URL}}. All this checkbox does is to append the "{{Tracker}}" variable to your HTML automatically for you.

The last thing we'll want to do with the template text is to add a link to our landing page. By highlighting "link" and clicking the hyperlink button (middle button in the top row), we see the following dialog appear:
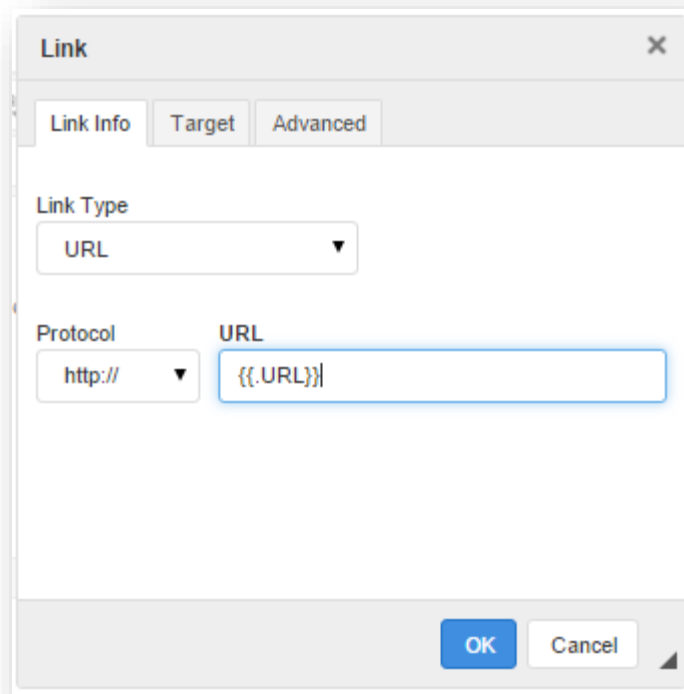
Figure 12 - Hyperlink Editor

Then, we click OK to exit the dialog.

After we setup the email content, we can attach files if desired. This is helpful if you want to create an attachment that simulates a malware infection. In fact, it should be possible to create attachments that will update the gophish campaign if the attachment is open, giving insight into which users are susceptible to opening malicious files.

Finally, we need to save our template by clicking the "Save Changes" button.

If you don't see the template show up right away after clicking "Save Changes", refresh the page and it should appear in the table.

Creating a Landing Page

Landing pages are the actual HTML pages that are returned to the users when they click the phishing links they receive.

To create a landing page, navigate to the "Landing Pages" page and click the "New Page" button.
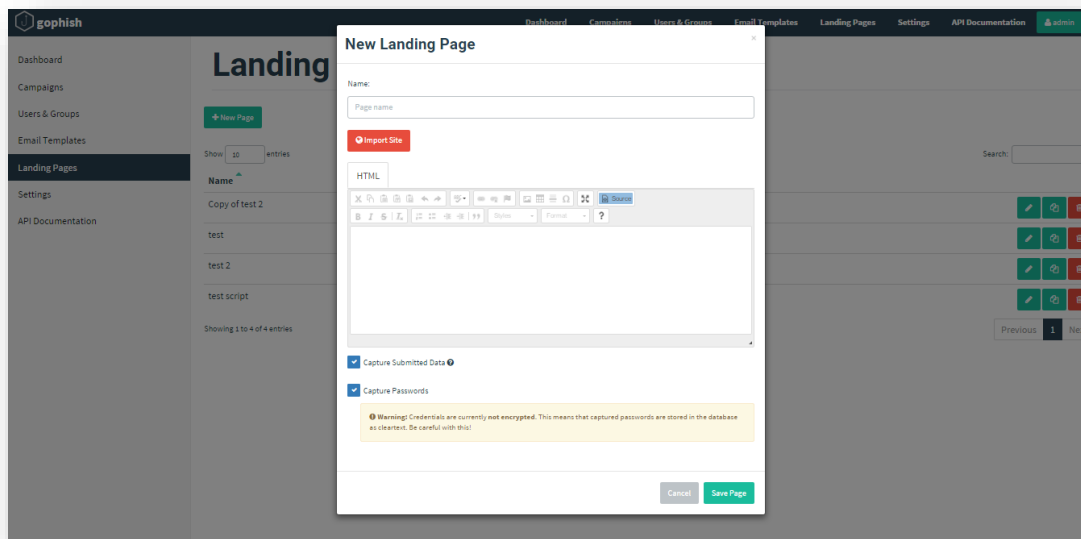
Figure 13 - Create a Landing Page

On this page, we have the ability to set the name of our landing page, as well as creating the content. The content is HTML code that can either be created from scratch, or imported from a URL to clone an existing website.

As a security administrator, you might normally want to set this to a page to training documentation indicating that the user was a victim of simulated phishing, as well as steps the user can take to identify and report phishing attempts in the future.

For our scenario, we will do something a bit different.

We know that our company, Morning Catch, has a webmail login page at http://morningcatch.dev/mail. It looks similar to this:
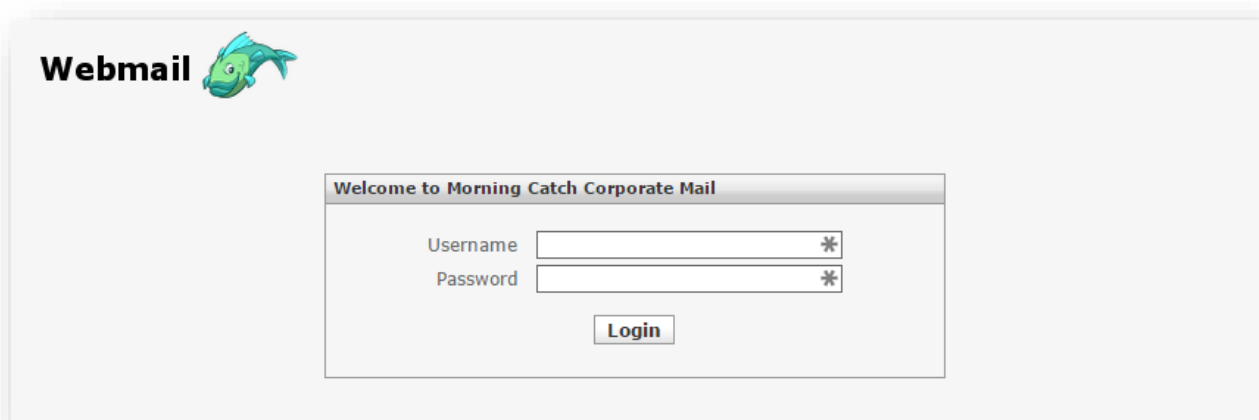
Figure 14 - Morning Catch Webmail Login

Let's use gophish to import this landing page directly. By clicking the "Import Site" button, we are presented with the following screen:
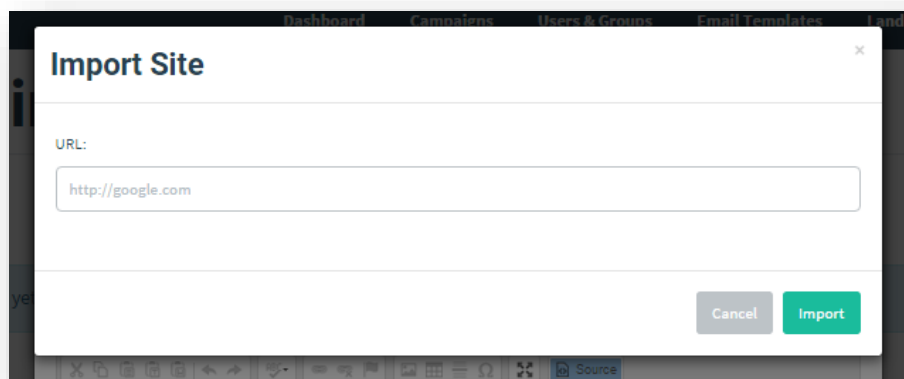
Figure 15 - Importing a Site

If we put the webmail URL into the "URL" field and click the "Import" button, we will see gophish go out to the site and pull down the HTML. Then, we are navigated back to our previous screen, where we can see and edit the imported site.
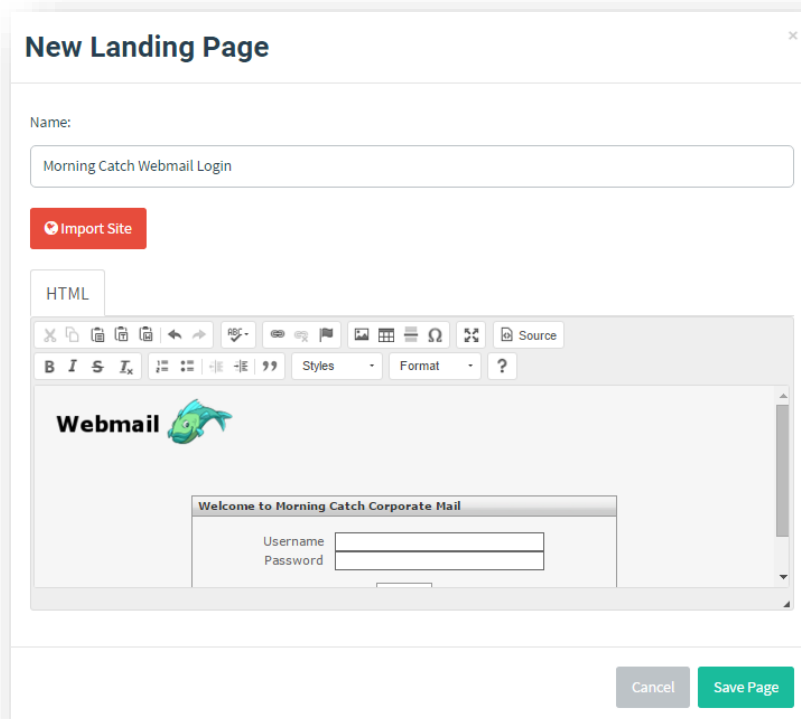

Figure 16 - Importing the Morning Catch Webmail Login

Now that we have the HTML imported, we can focus on capturing credentials. Gophish will always change the forms on the page to be submitted to the server so you will know if the user submitted data. However, gophish also offers the following options:

- Capture Credentials – This option tells gophish to capture all input (**excluding** passwords)
- Capture Passwords – This option tells gophish to also capture passwords

DANGER:

Captured credentials (including passwords!) are currently stored in plaintext. Be careful with this!

Now that we have completed configuring our landing page, we can click "Save Page" to save the landing page.

If you don't see the landing page show up right away after clicking "Save Changes", refresh the page and it should appear in the table.

Creating a Campaign

The last thing we need to setup is the campaign itself. To setup a campaign, first navigate to the "Campaigns" page and click the "New Campaign" button:
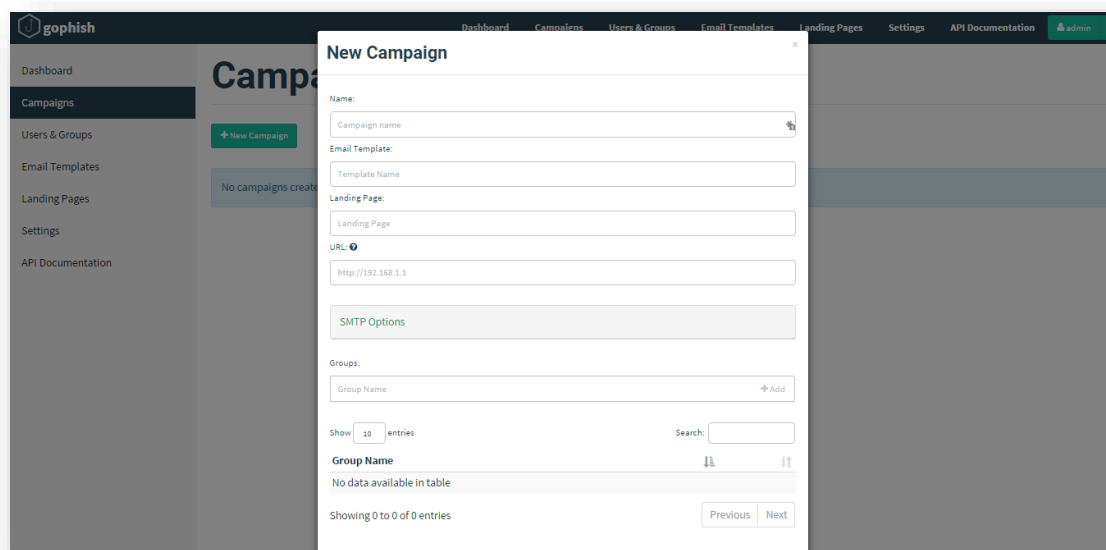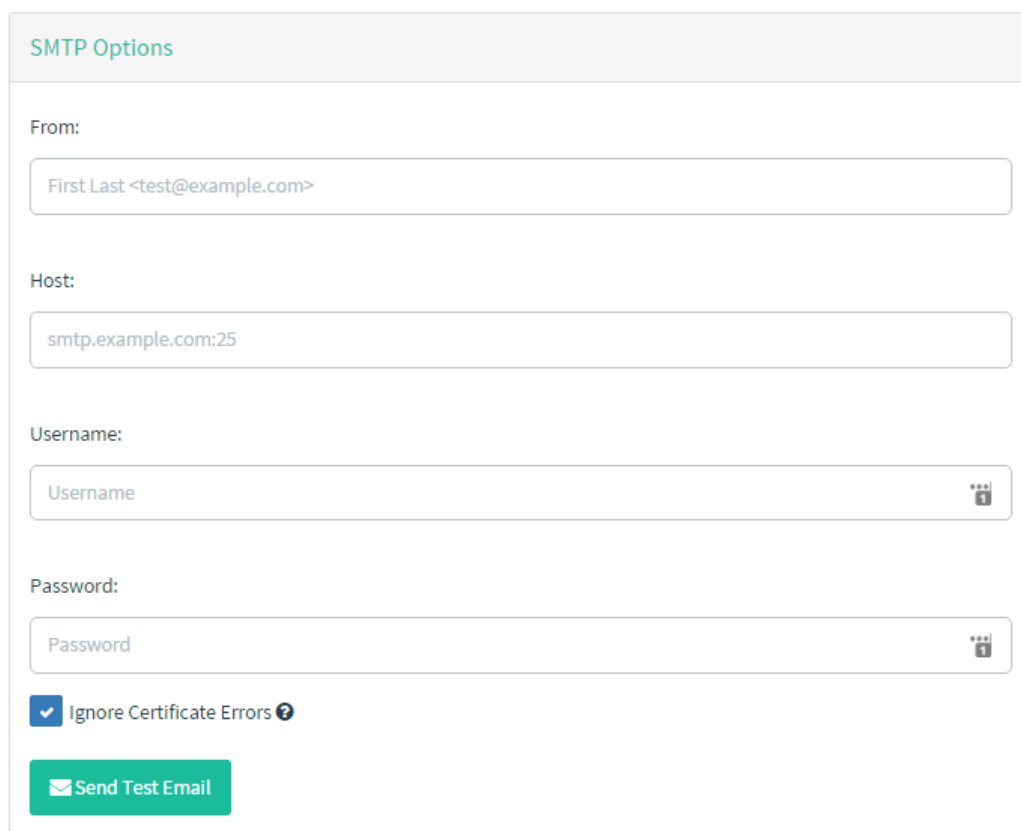

Figure 17 - Creating a New Campaign

We start by setting the campaign name, email template, and landing page we want to use. Gophish makes this easy by providing autocomplete functionality when we are setting the template and landing pages.

Next, we need to set the URL that the users will be directed to. This need to be the IP address of the gophish host (and port!) **that is reachable by the users**. This means that if you are only targeting internal users, you would probably be fine using the host's internal IP address. However, if your targets are coming in externally, you will need to setup gophish to be reachable externally and set this field to be the external (public) IP address.

It is important to note that you can also use a domain name if the domain resolves to the correct IP address for the gophish listener!

Next, we expand the SMTP options and are presented with the following:

Figure 18 - SMTP Options

The first field we fill out is the "From" field. This field describes who the email will appear to have been sent from. In our example, let's spoof the user "System Administrator <sysadmin@morningcatch.ph>".

The rest of the SMTP options should be set according to the settings in use by your organization, or to an open relay. For our cases, we know that Morning Catch's SMTP server is at smtp.morningcatch.dev and TCP port 25, and we know that we do not need to authenticate, so we can leave the username/password blank.

Finally, we just need to choose what groups we want to include in this campaign. Gophish's autocomplete functionality will help make this easy. It's important to note that, after selecting the group you want to add, you must click enter to actually add it to the list of groups. It should look like this:

Figure 19 - Adding a Group to a Campaign

That's it! Once we click "Save Changes", our campaign will be launched automatically and emails will be sent to the targets.

If you don't see the campaign show up right away after clicking "Save Changes", refresh the page and it should appear in the table.

By refreshing the page, we should see our campaign listed as "In Progress":

Figure 20 - In Progress Campaign

Viewing Campaign Results

Now let's take a look at how we can track results from a campaign.

We can access our campaign from a couple of places – the "Dashboard", or the "Campaigns" page. By clicking the "View" button for our campaign (green button), we see the following overview stats:
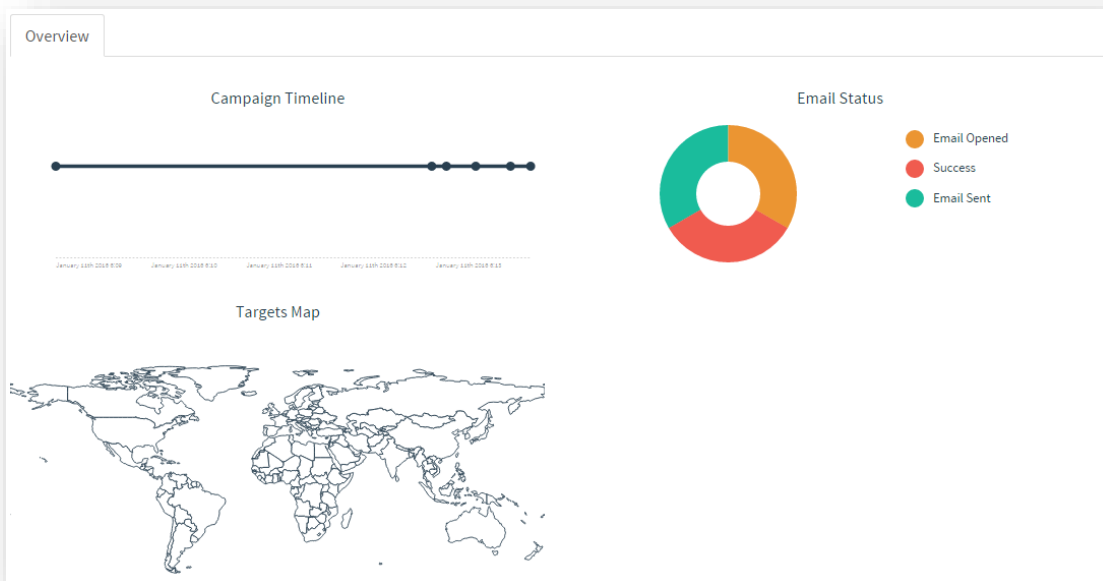
Figure 21 - Overview Results

It looks like in our scenario, we had 2 out of the 3 users open the email, and one user clicked the link.

We can see the detailed statistics at the bottom of the page:

Figure 22 - Campaign Details

Looks like we had a successful campaign, and have found areas where training can be provided!

We can expand the details on each row to see the "Timeline" for each user. For example, if we expand the row for "Boyd Jenius", we see the following:
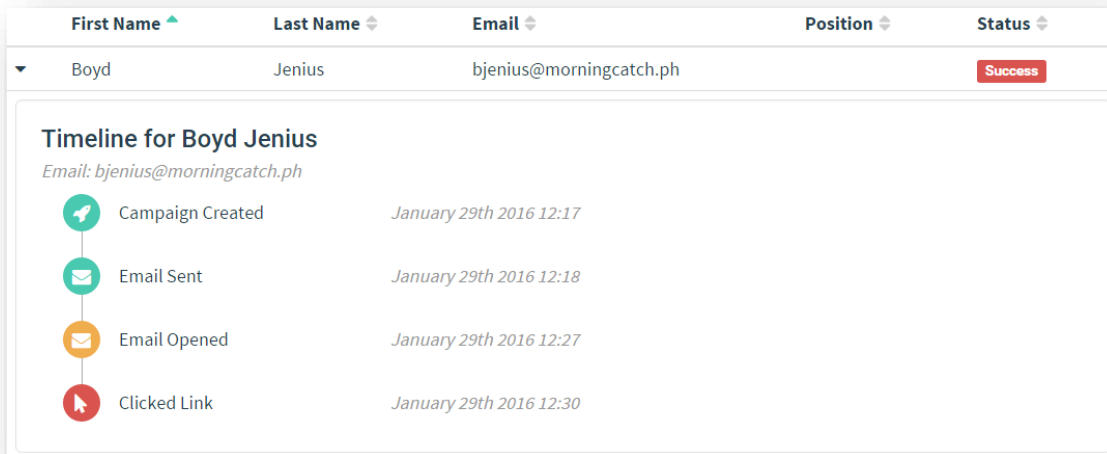
Figure 23 - Viewing the Timeline for Boyd Jenius

This timeline gives us insight into every event that occured for Boyd Jenius during this campaign.

Exporting Campaign Results

We can also export the campaign results as CSV for reporting or importing into another process. This is simple do to using the "Export" button at the top of the results screen:
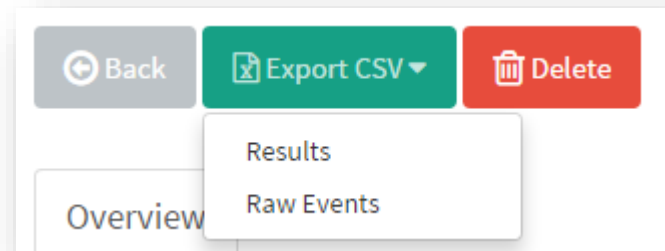

Figure 24 - Exporting Options

The two options are:

- **Results –** this exports the final results for each user. For example, this would export the target details for Boyd Jenius and the result "Success".
- **Raw Events** – this exports all the raw events that occurred during the campaign. This means that you'll see an entry for any time an email was sent, a link was clicked, as well as any errors.

Appendix

Template Variable Reference

The following variables are available to be used in templates and landing pages:

Tip:
*Remember – Templates are **case sensitive**!*

Variable	Description
{{.FirstName}}	The target's first name
{{.LastName}}	The target's last name
{{.Position}}	The target's position
{{.From}}	The spoofed sender
{{.TrackingURL}}	The URL to the tracking handler
{{.Tracker}}	An alias for
{{.URL}}	The phishing URL