# ENPM665 Homework #5 – Penetration Testing

Version 2.1 – November 7th 2022

- Spin up a VM/instance in your cloud provider of choice
- Install Gophish - https://getgophish.com/
- ”Phish yourself” and take screenshots of the phish. Screenshots to submit:
    1. A screenshot of your Go Phish admin panel for the phishing campaign you launched showing a Cloud provider’s IP address/DNS name in the address bar
    2. A screenshot of your phish message. Cleverness is not needed here, but you do need to include your University ID number (ex: 103xxxxxx) the email message you send to yourself. Note: anti-spam tools used by many providers may block some of these messages so you may need to do some creative work in your phishing message and/or check your spam folder. If they end up in the spam folder that’s OK!
    3. A screenshot of the phishing site showing a cloud provider’s IP address/DNS name in the address bar.

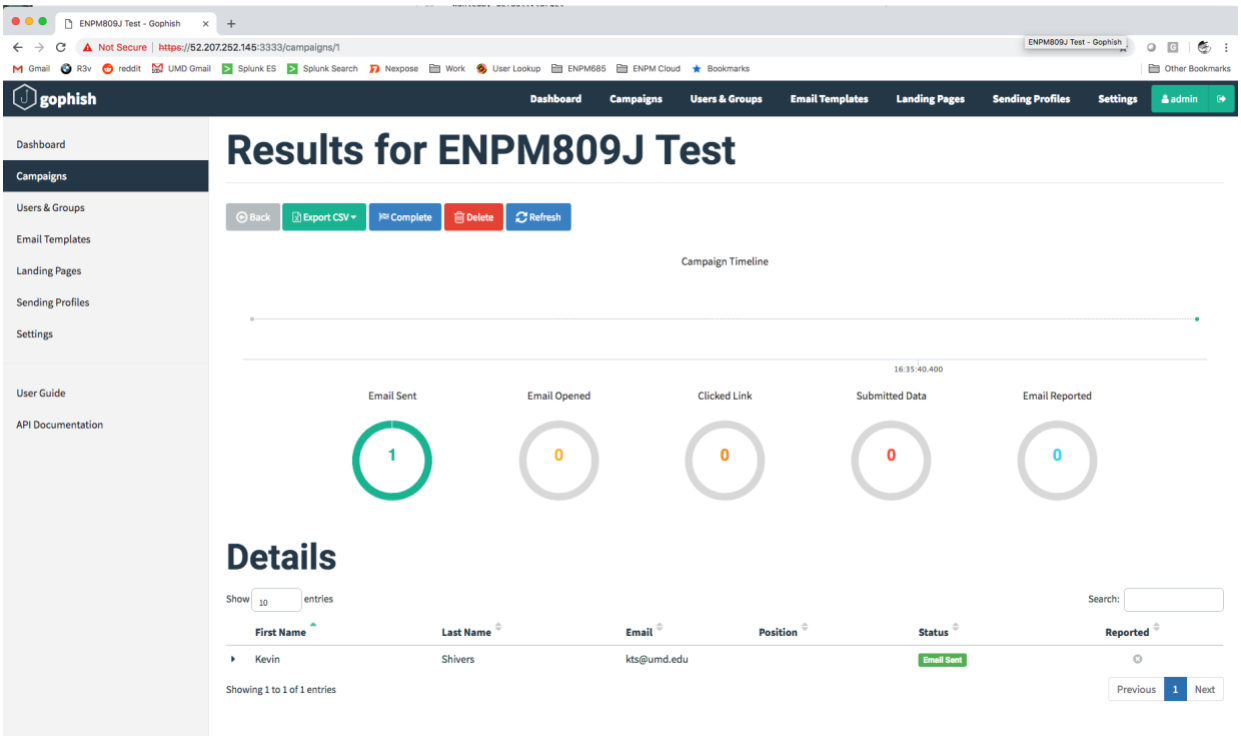
**Note:** AWS recently made some changes for sending email over port 25 from EC2 instances (they block it now, whereas they use to just rate limit it) that will make this exercise a little trickier than it was in prior courses. You will need to investigate tools like SES that can help send email for you in AWS. Other cloud providers may impose similar restrictions and have solutions for sending email that you may need to investigate. A free Sendgrid account (https://sendgrid.com/) may be another tool to investigate for the e-mail delivery.

Keep things simple and make this easy for yourself. This is just a test so it does not need to look legitimate, I want you to get some hands-on experience with a penetration testing tool and the system administrative work needed to get it set up (which is something penetration testers need to do in the real world quite often.) One example with keeping this easy for yourself in terms of SES – use the same email address for the To and From address.

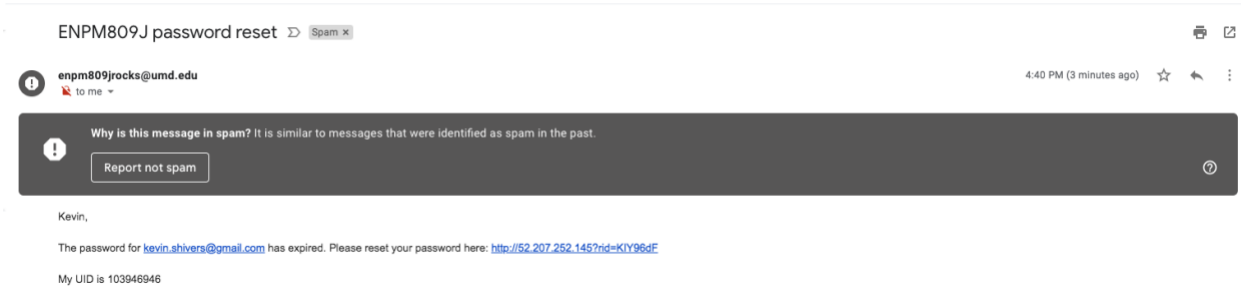
**Deliverable:**

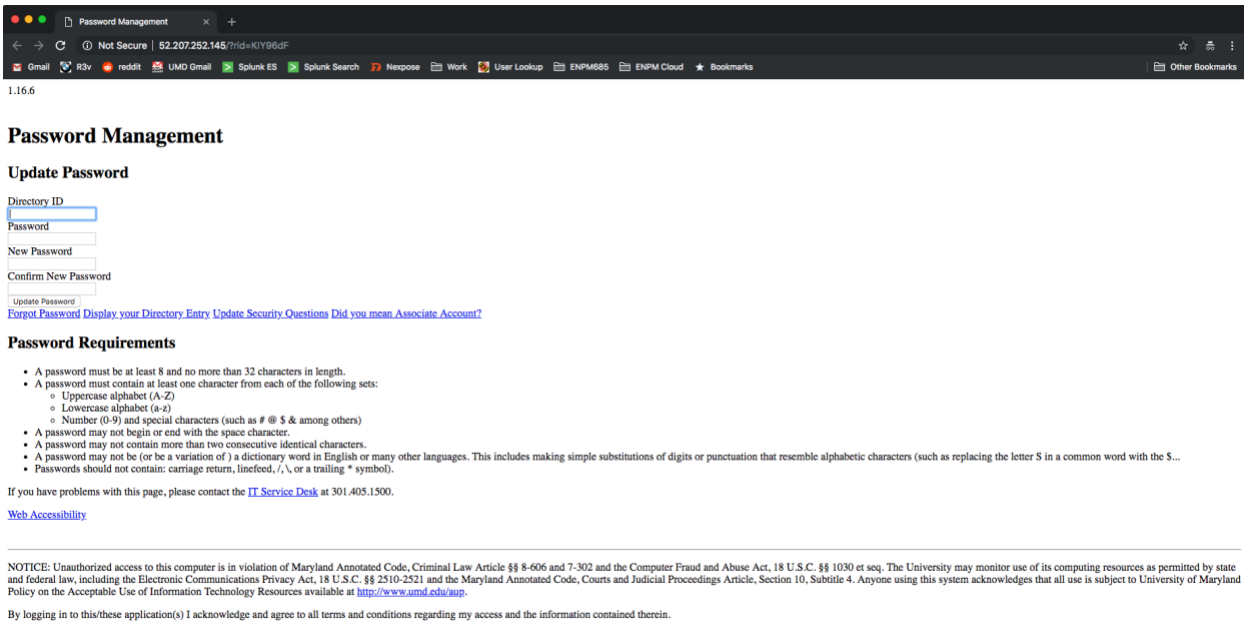
Your 3 screenshots. Examples on the next two pages:

1.


ENPM809J Test - Gophish
Not Secure | https://52.207.252.145:3333/campaigns/1
gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Settings
User Guide
API Documentation
Results for ENPM809J Test
Back
Export CSV
Complete
Delete
Refresh
Campaign Timeline
16:35:40.400
Email Sent
Email Opened
Clicked Link
Submitted Data
Email Reported
1
0
0
0
0
Details
Show 10 entries
Search:
First Name
Last Name
Email
Position
Status
Reported
Kevin
Shivers
kts@umd.edu
Email Sent
Showing 1 to 1 of 1 entries
Previous
1
Next

2.


ENPM809J password reset
Spam
enpm809jrocks@umd.edu
to me
4:40 PM (3 minutes ago)
Why is this message in spam? It is similar to messages that were identified as spam in the past.
Report not spam
Kevin,
The password for kevin.shivers@gmail.com has expired. Please reset your password here: http://52.207.252.145?rid=KIY96dF
My UID is 103946946




3.

**Note**: The cloud provider's IP address (in this case Amazon's) is clearly visible in all 3 emails.

**Also note**: In my example I cloned UMD's password rest page which links to CSS sheets hosted on a UMD site. That site has blocked external referrals requesting those CSS sheets which is why the page looks odd. That's OK for this exercise, a real-world example you would find a place to host those. You're also not limited to the UMD password reset page use anything you'd like!

## Don't forget to terminate your instance/VM when you're finished!