Gone Phishing, be back soon!

PRESENTED BY: GrnBeltWarrior

WHY THIS TALK?

DISCLAIMER:

This topic and the information contained within this talk is for educational purposes.

I can't talk about situations/scenarios regarding my employer.

My way is not THE way.

ABOUT ME:

V2Ugd2IuIHRvZ2V0aGVyLCB3ZSBsb3NlIHRvZ2V0aGVy

FROM THE 2020 VERIZON DBIR:

Credential theft, social attacks (i.e., phishing and business email compromise), and errors cause the majority of breaches (67% or more).

https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf

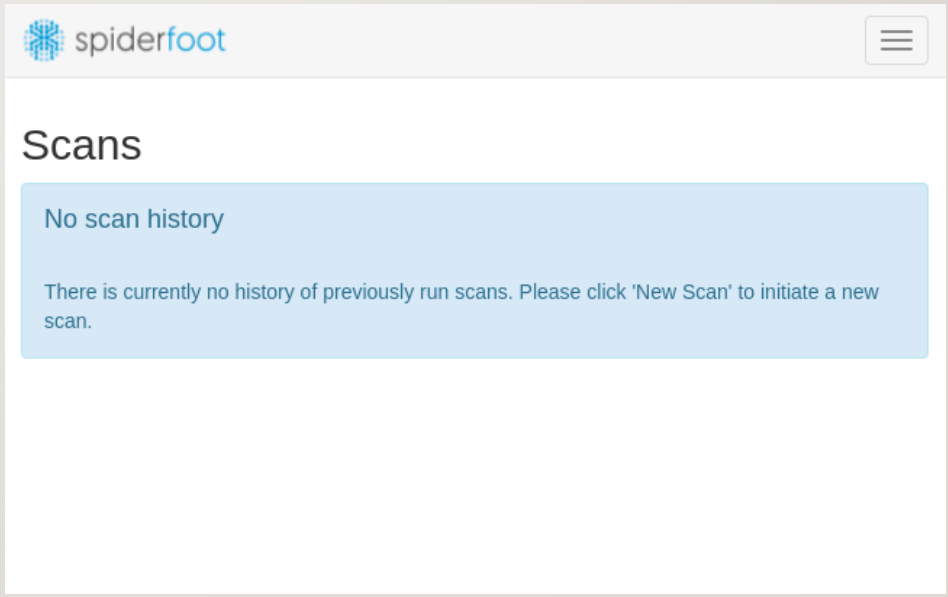
What is phishing?

- https://attack.mitre.org/techniques/T1566/
- You are aiming to get the victim to click. (Primary Goal)
- Payloads will vary but here are some examples of how you can line up your phishing emails:
  - Winning a gift card.
  - Purchasing issues (unexpected charge).
  - Access cancelation (Seriously, announce something is going to be taken away that they don't use and some people will panic.)

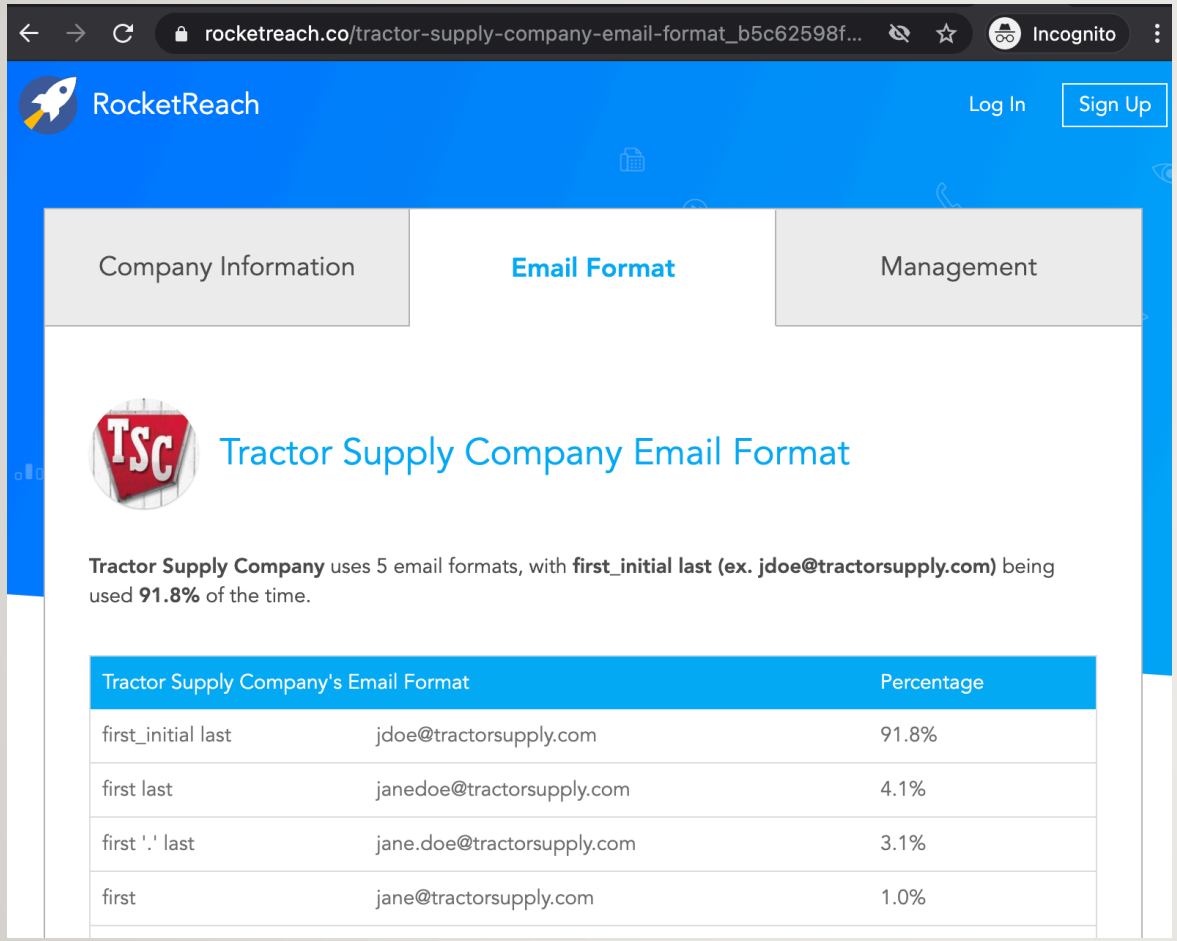
AUTOMATING OSINT:

- Recon-NG

- Spiderfoot

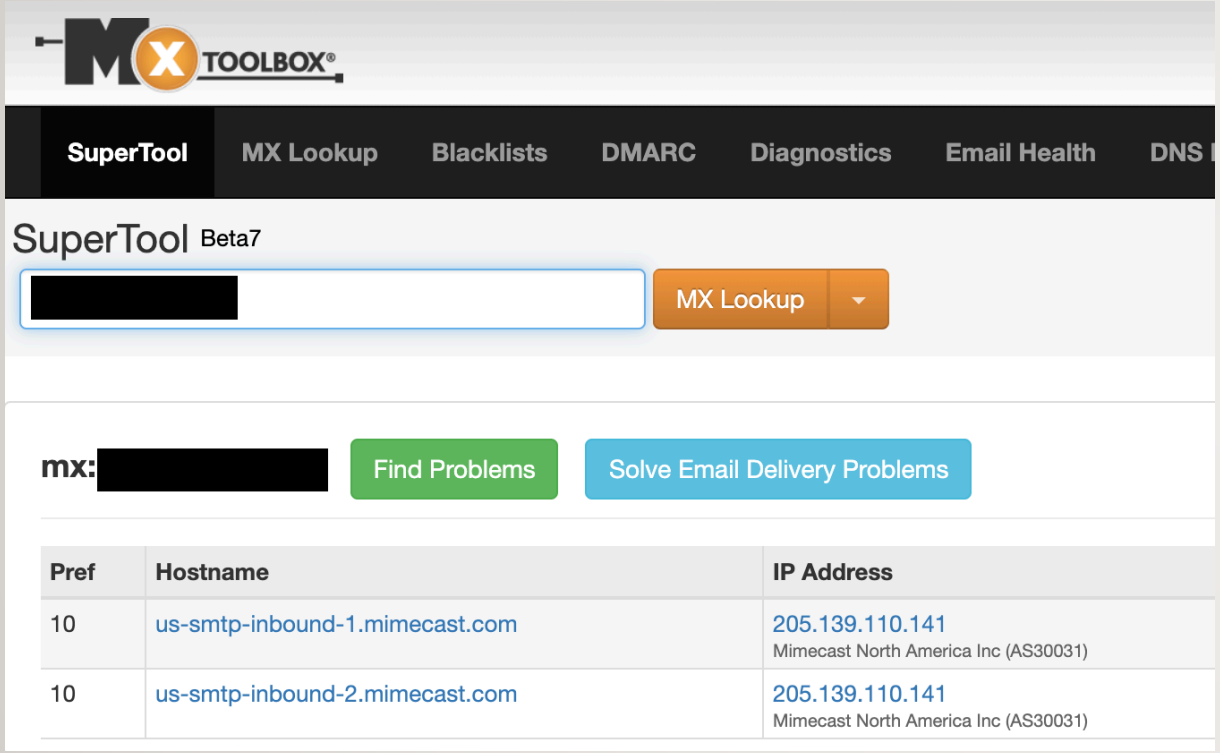


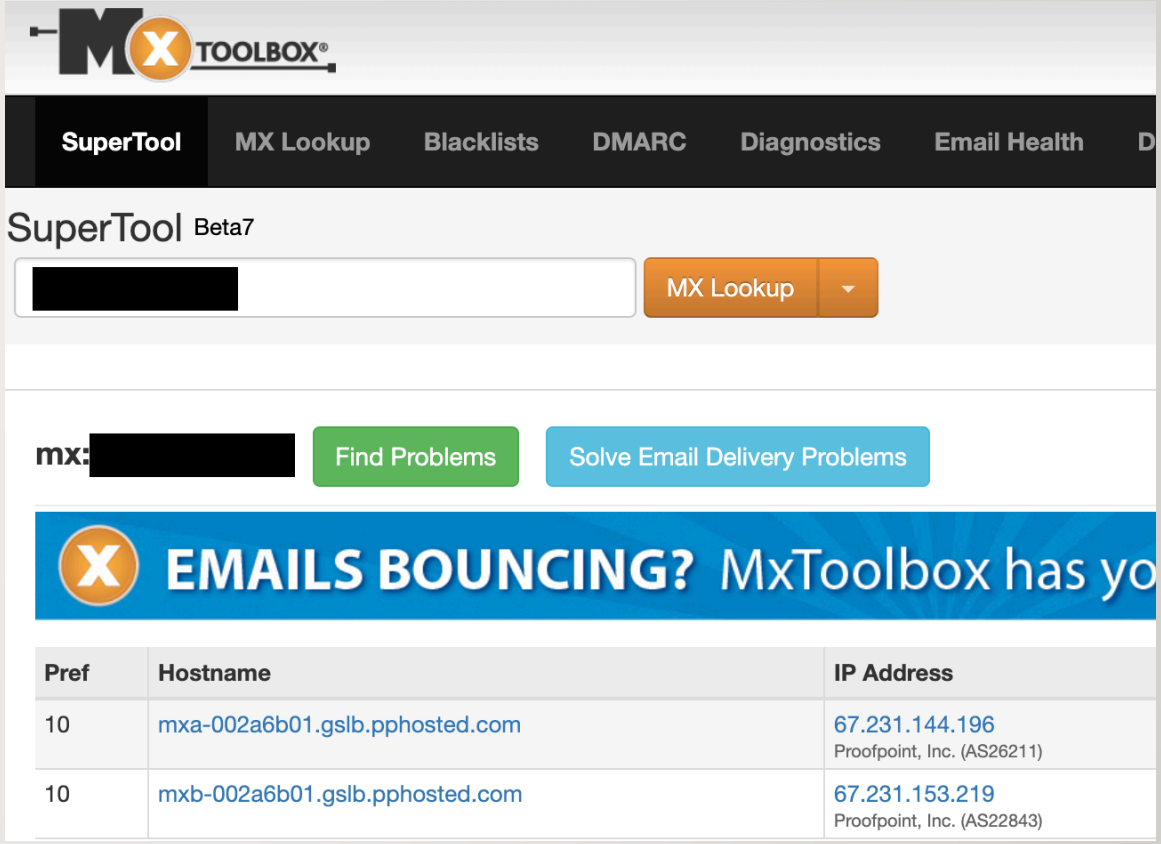
OSINT: EMAIL ADDRESS FORMAT



- Creating a fake LinkedIn Account, you can see employees of an organization, based upon your connections.
- From the reported format, you may be able to craft email addresses from those listed as employees.
- hunter.io: email lists are available, for coin.
- Issues in crafting your own from the likes of LinkedIn: Gabe vs Gabriel might result in email bounces, raising suspicion.

OSINT: MAIL SYSTEMS USING MXTOOLBOX





GEARING UP:

- Free hosted options: Yahoo.
- Self hosted:
  - GoPhish
    - https://github.com/gophish/gophishiRedMail
  - iRedMail
    - https://github.com/iredmail/iRedMail
    - https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki#easy-web-based-phishing
- Phishing at scale:
  - Mailgun
    - https://www.mailgun.com/
  - Sendgrid
    - https://sendgrid.com/

OPSEC

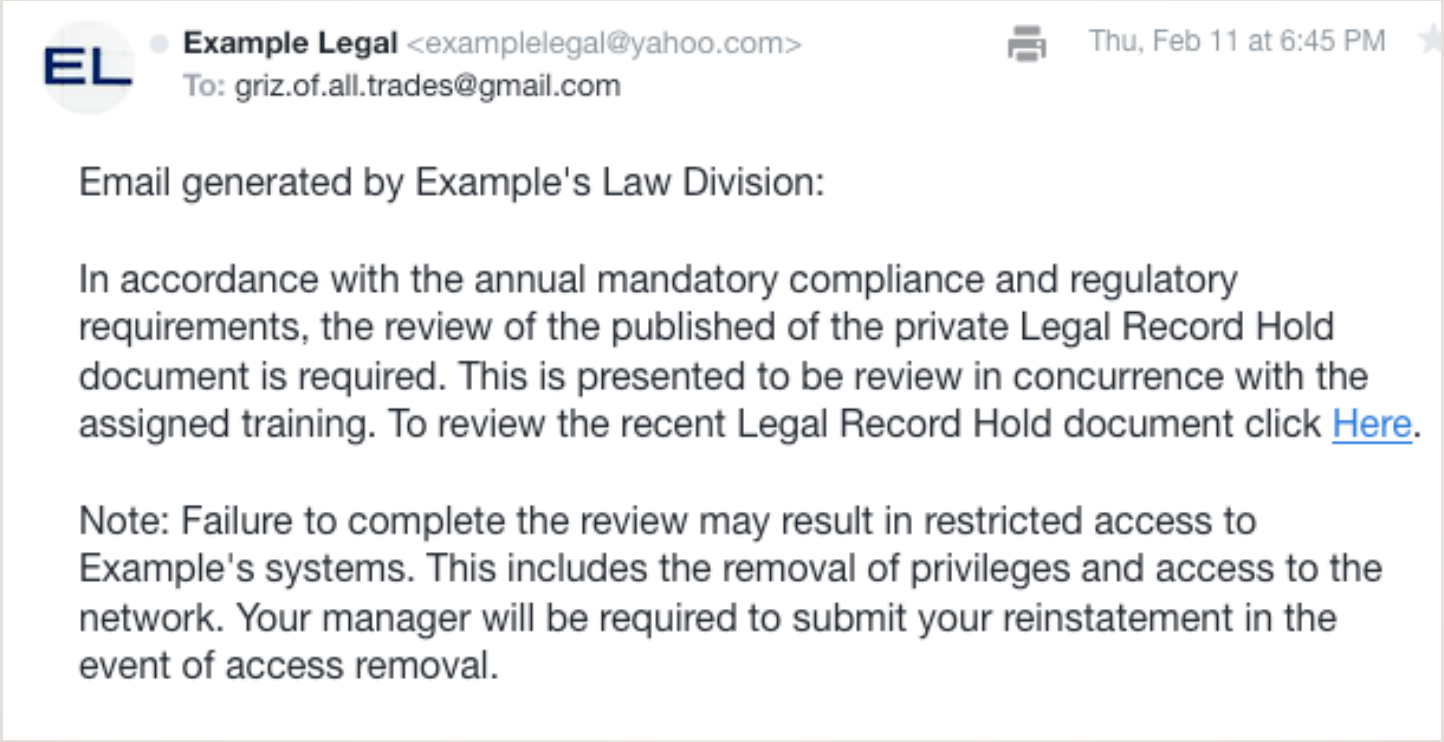
- Domains
- Categorizations
- Links
- Redirectors

Received: from breakawaydistributing.com ()
by creativedude248726@gmail.com;
Tue, 11 Apr 2017 14:12:51 +0000 (UTC)
Message-ID: <D5342094.84830072@breakawaydistributing.com>
Date: Tue, 11 Apr 2017 07:12:24 -0700
Reply-To: "USPS International" <lrnvaoy1467488@breakawaydistributing.com>
From: "USPS Ground" <lrnvaoy1467488@breakawaydistributing.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.14) Gecko/20080421
Thunderbird/2.0.0.14
X-Accept-Language: en-us
MIME-Version: 1.0
To: creativedude248726@gmail.com
Subject: Our USPS courier can not contact you parcel # 754277860
Content-Type: text/plain;
charset="us-ascii"
Content-Transfer-Encoding: 7bit

WHY SEEDING?
WHAT IS SEEDING?

We don’t want the first emails from our newly purchased and categorized domain to be malicious.

EXAMPLE:
USING YAHOO



Example Legal <examplelegal@yahoo.com>
To: griz.of.all.trades@gmail.com

Thu, Feb 11 at 6:45 PM

Email generated by Example's Law Division:

In accordance with the annual mandatory compliance and regulatory requirements, the review of the published of the private Legal Record Hold document is required. This is presented to be review in concurrence with the assigned training. To review the recent Legal Record Hold document click Here.

Note: Failure to complete the review may result in restricted access to Example's systems. This includes the removal of privileges and access to the network. Your manager will be required to submit your reinstatement in the event of access removal.

YAHOO AND BITLY

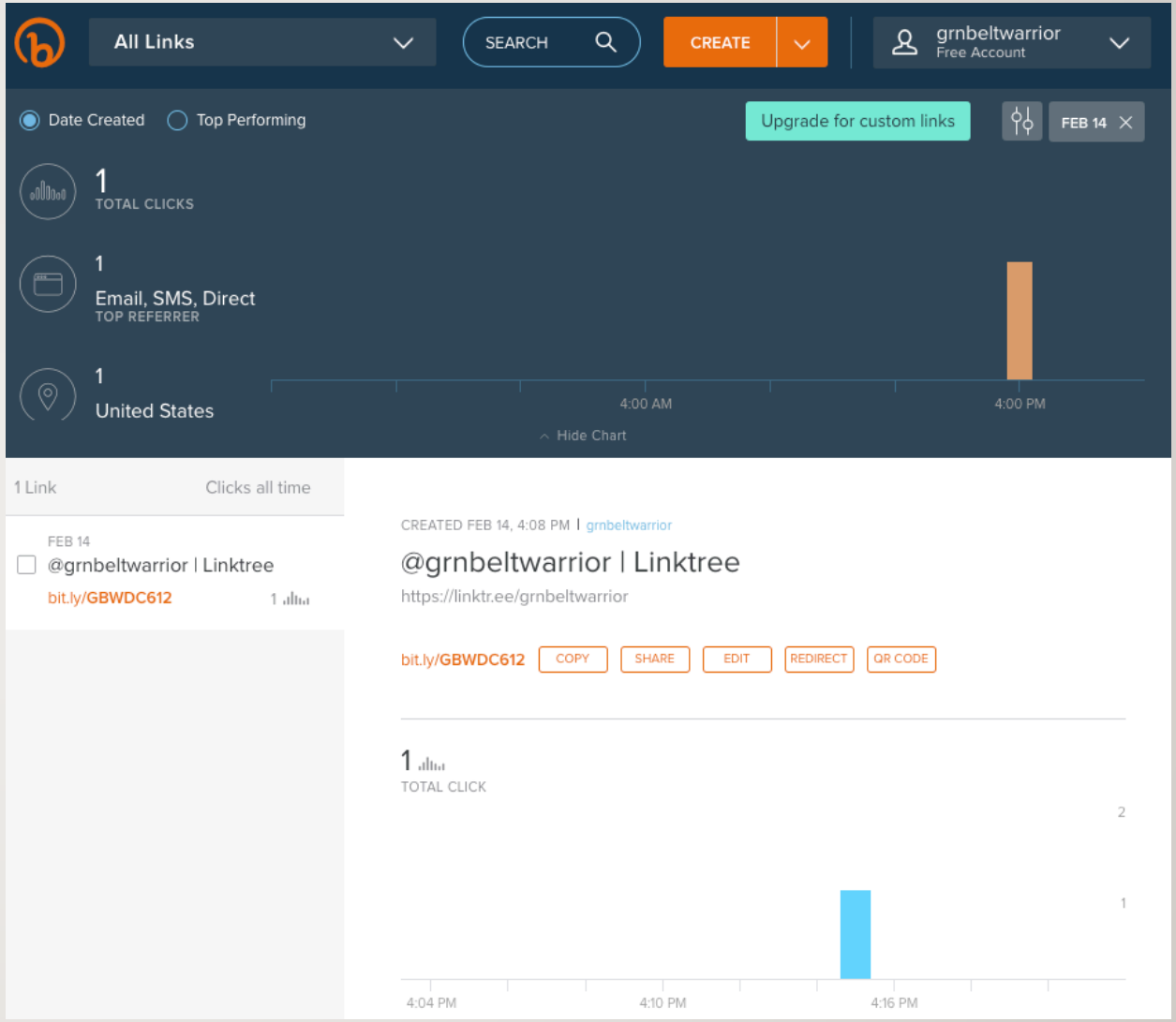
EL **Example Legal** 10:19 AM
To: griz.of.all.trades@gmail.com >

Notification - Legal Hold

Email generated by Example's Law Division:

In accordance with the annual mandatory compliance and regulatory requirements, the review of the published of the private Legal Record Hold document is required. This is presented to be review in concurrence with the assigned training. To review the recent Legal Record Hold document click: bit.ly/GBWDC612.

Note: Failure to complete the review may result in restricted access to Example's systems. This includes the removal of privileges and access to the network. Your manager will be required to submit your reinstatement in the event of access removal.



DETAILS HELP AND FRUSTRATE

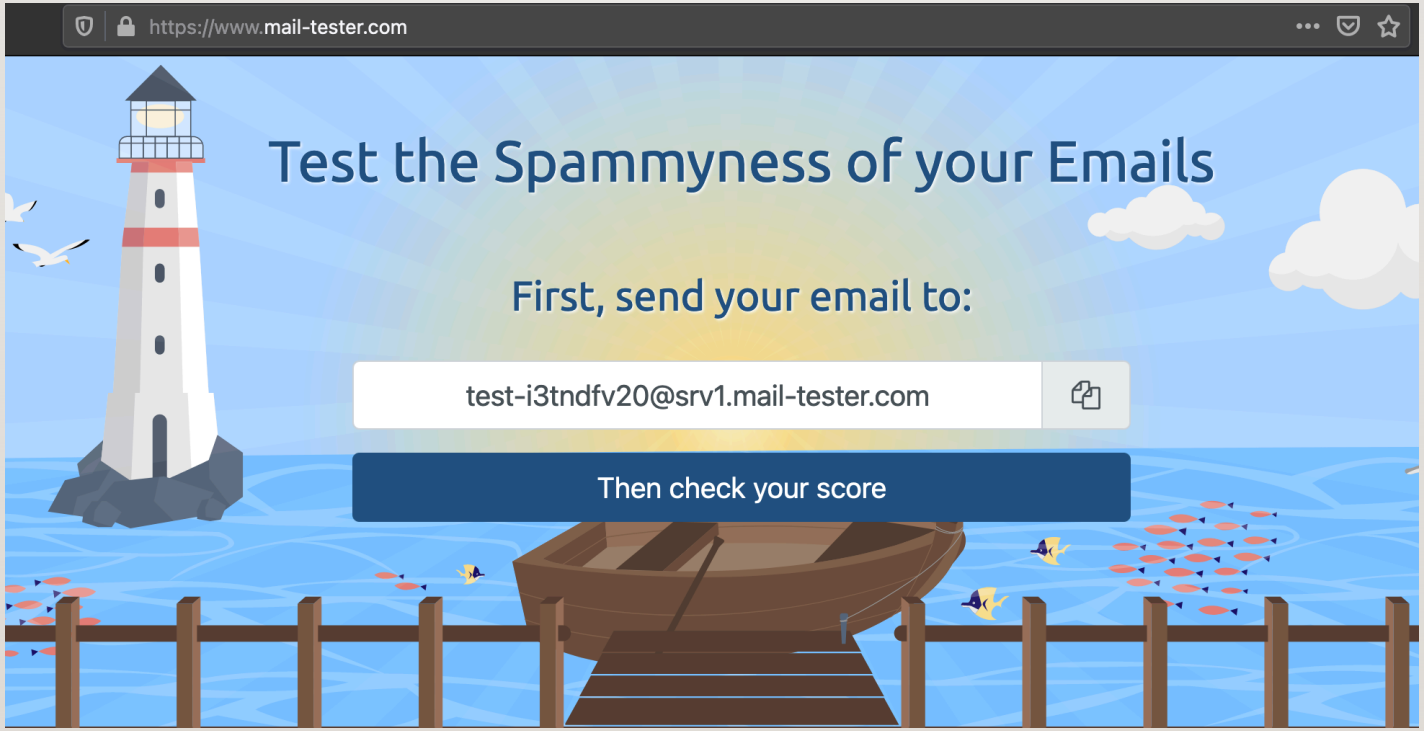
When testing, it's a good idea to review the email headers.

Look for items that can stand out.

- FROM email addresses
- Originating IP Addresses
- Attachment Names
- Embedded URLs
- Subject Line
- Display Name

  The most frequently spoofed "header from" field is the Display Name, for which there is currently no authentication mechanism available.

TESTING MAIL SETTINGS:

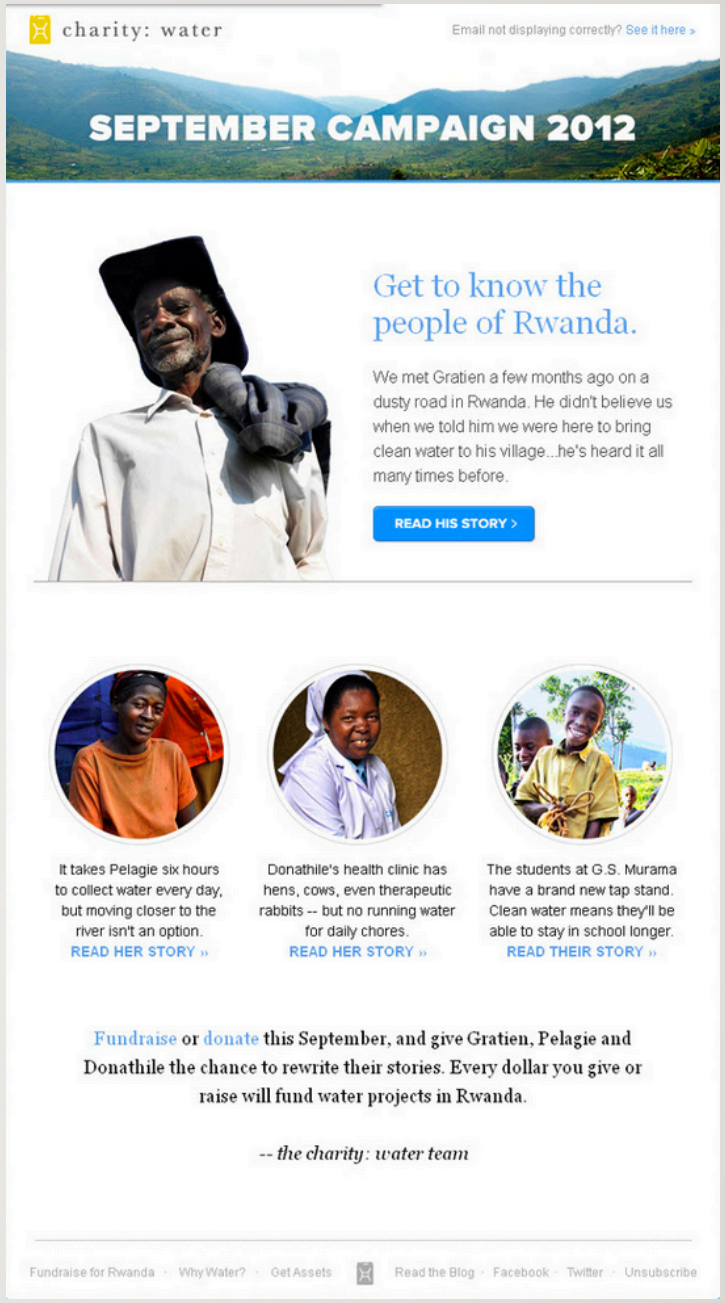


Checking items like: DKIM + SPF + DMARC

REPUTATION AND SEEDING, OH MY.

Signing up for junk email lists. Does this impact overall reputation?

Seeding: sending non-malicious emails. Take an email, modify some of the image links back to your webserver. Then you can look through the apache logs to see if/when and the IP space the images were loaded from.



PUTTING THINGS TOGETHER

Google Play Music

We'll soon delete all of your Google Play Music library and data

On 24 February 2021, we will delete all of your Google Play Music data. This includes your music library, with any uploads, purchases and anything you've added from Google Play Music. After this date, there will be no way to recover it.

You can download your Google Play Music library and data with Google Takeout, or transfer it to YouTube Music. As a reminder, with one click, you can still transfer your music library, including uploads, playlists and recommendations, to YouTube Music before 24 February 2021.

TRANSFER TO YOUTUBE MUSIC

If you have any questions, we're here for you. Take a look at our support resources.

The Google Play Music and YouTube Music teams


```
<!doctype html public "- / /w3c / /dtd xhtml 1.0 transitional / /en" "https=
: / /www.w3.org /tr /xhtml1 /dtd /xhtml1-transitional.dtd">

<html xmlns=3Dhttps://www.w3.org/1999/xhtml lang=3Den>
<head>
<title>Google Play Music data</title>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dutf-8">
<!--[if !mso]><!-->
<meta http-equiv=3DX-UA-Compatible content=3DIE=3Dedge>
<!--<![endif]-->
<meta name=3Dviewport content=3D"width=3Ddevice-width, initial-scale=3D1.0"=
>
<meta name=3Drobots content=3D"no index">
<link href=3Dhttps://fonts.googleapis.com/css?family=3DRoboto:400,300,500,7=
00 rel=3Dstylesheet type=3Dtext/css>
<!--[if mso | ie]>
      <style>
         .oufnt{font-size:37px !important;}
         .oupad{padding-left:32px !important;}
         .sup {
         vertical-align: 1px !important;=20
         font-size: 100% !important;
         }
         .bull27{font-size:24px !important}
         .bull271{line-height:36px !important}
         .font41{font-size:41px !important; line-height:50px !important;}
         .padt6_outlook{padding-top:2px !important;}
         .font_outlook{
            font-size: 46px !important;
            line-height: 58px !important;
         }
      </style>
      <![endif]-->=20
<!--[if ie]>
      <style>
         .sup {
         vertical-align: 6px !important;=20
         font-size: 80% !important;
         }
      </style>
      <![endif]-->
<style type=3Dtext/css>
@font-face {
    font-family: 'YouTube Sans';
    font-weight: 400;
    font-style: normal;
```

IMPROVISE
ADAPT
OVERCOME
AKA WHAT'S THE HACK?

Test, test and test s'more.

Setup iRedMail, configured SendGrid with our iRedMail instance.

This allowed us to send with SendGrid's API and python.

Out of office emails then routed back to our iRedMail instance.

TIME TO GO PHISHING…

- Setup SendGrid Sender Authentication, tying back to the iRedMail setup.
- Test, test, test.
- Check sending information when interacting with sendgrid, is the message accepted for delivery.
- Monitor apache, if that's what you are using, for access to your images.
- If you are hosting a payload, use a redirector to punt requests to the payload location if it doesn't match your intended target.
- Check your iRedMail mailboxes.
- If you get an out of office email (you tested this right?) depending on the time frame, you might use this again when sending your other emails (payloads).
- Out of office proves you can send to the recipient and a response comes all the way back to you.
- The same care and feeding of your phishing domains, should be taken with your payload hosting domains and your C2 domains.

WHAT WE COVERED:

Recommended reading:

https://breakdev.org/evilginx-2-4-gone-phishing/

- What is phishing.
- The lures we can use to get the end user to click.
- Options to send in our tacklebox.
- Yahoo as an example.
- OSINT to your advantage.
- OPSEC considerations.
- Looking for issues/email headers that can be flagged.
- Domain seeding and why it can be useful.
- Combining technologies to get more useful information.

QUESTIONS?

@grnbeltwarrior

linktr.ee/grnbeltwarrior