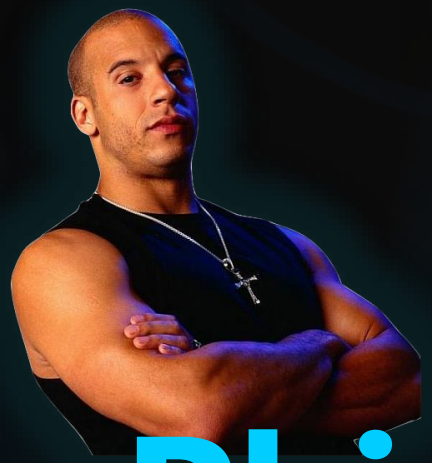


Phish & Furious

Unraveling Campaign Builder Vulnerabilities in a Blink-and-Breach World

Presented by: Raae Wolfram

>whoami

- Technology Professional, >15 years, non-traditional path
- Sr. Product Manager @ Microsoft
- New Yorker / Latina
- Mom
- Star Trek Fan
- Had brain surgery in 2016; radiation in 2022
- I don't drive ¯_(ツ)_/¯

>Phish & Furious Overview

Fast Track Defense: Getting up to Speed

>> Common flaws in tools like Mailchimp can be misused

>> Legitimate platforms like Mailchimp can undermine organizational reputation and security

>> Industry initiatives can drive adoption of mitigation strategies

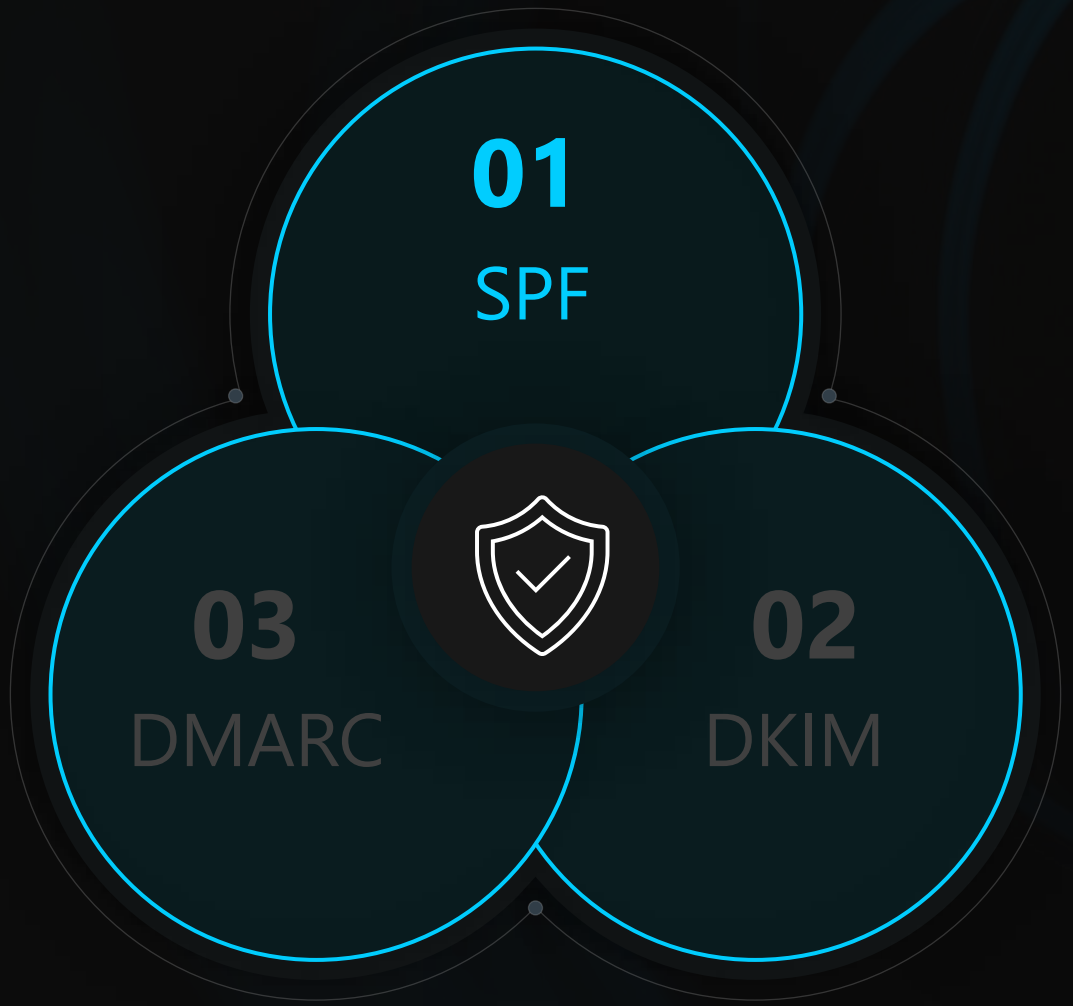
>A “Family” of Protocols

01
SPF

02
DKIM

03
DMARC

>Force Multipliers: SPF



01 SPF identifies authorized mail servers – prevents spoofed messages by ensuring that emails come from authorized sources.

02 DKIM verifies email integrity and sender identity – ensures that emails haven't been tampered with and come from authorized servers.

03 DMARC provides instructions on handling emails that fail SPF or DKIM checks – combines SPF and DKIM to enhance email security; prevents domain spoofing and phishing attacks..

SPF == Sender Policy Framework // DKIM == DomainKeys Identified Mail // DMARC == Domain-based Message Authentication, Reporting, and Conformance

>Lightwork Groundwork: SPF Fundamentals

```
"v=spf1 ip4:72.237.4.96 ip4:72.237.4.121
include:_spf.google.com include:_spf.salesforce.com
include:spf1.[REDACTED].edu include:spf2.[REDACTED].edu
include:spf3.[REDACTED].edu include:spf4.[REDACTED].edu ~all"
```

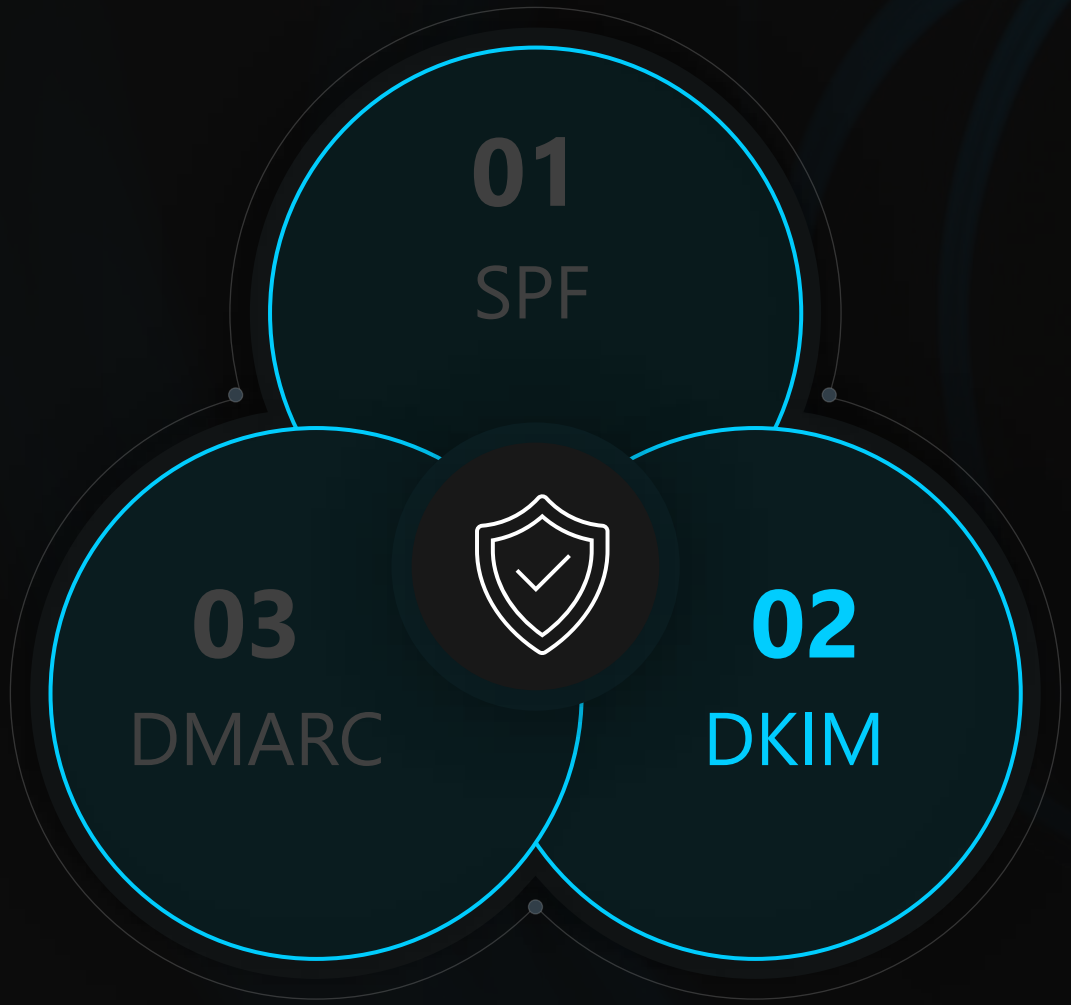
~all

VS

-all

```
"v=spf1 include:mailsenders.netsuite.com include:_spf.google.com include:mail.zendesk.com include:stspg-customer.com" "
mx:spe.intercom.io ip4:23.21.109.212 ip4:23.21.109.197 ip4:52.49.201.246 ip4:52.49.235.189 ip4:54.172.84.90 ip4:147.160.167.0/24
ip4:168.235.226.71" " ip4:168.235.226.72 ip4:168.235.226.73 ip4:168.235.226.74 ip4:168.235.233.211 ip4:168.235.233.212
ip4:168.235.233.213 ip4:192.254.121.248 ip4:167.89.63.53" " exists:%{i}._spf.mta.salesforce.com -all"
```

>Force Multipliers: DKIM



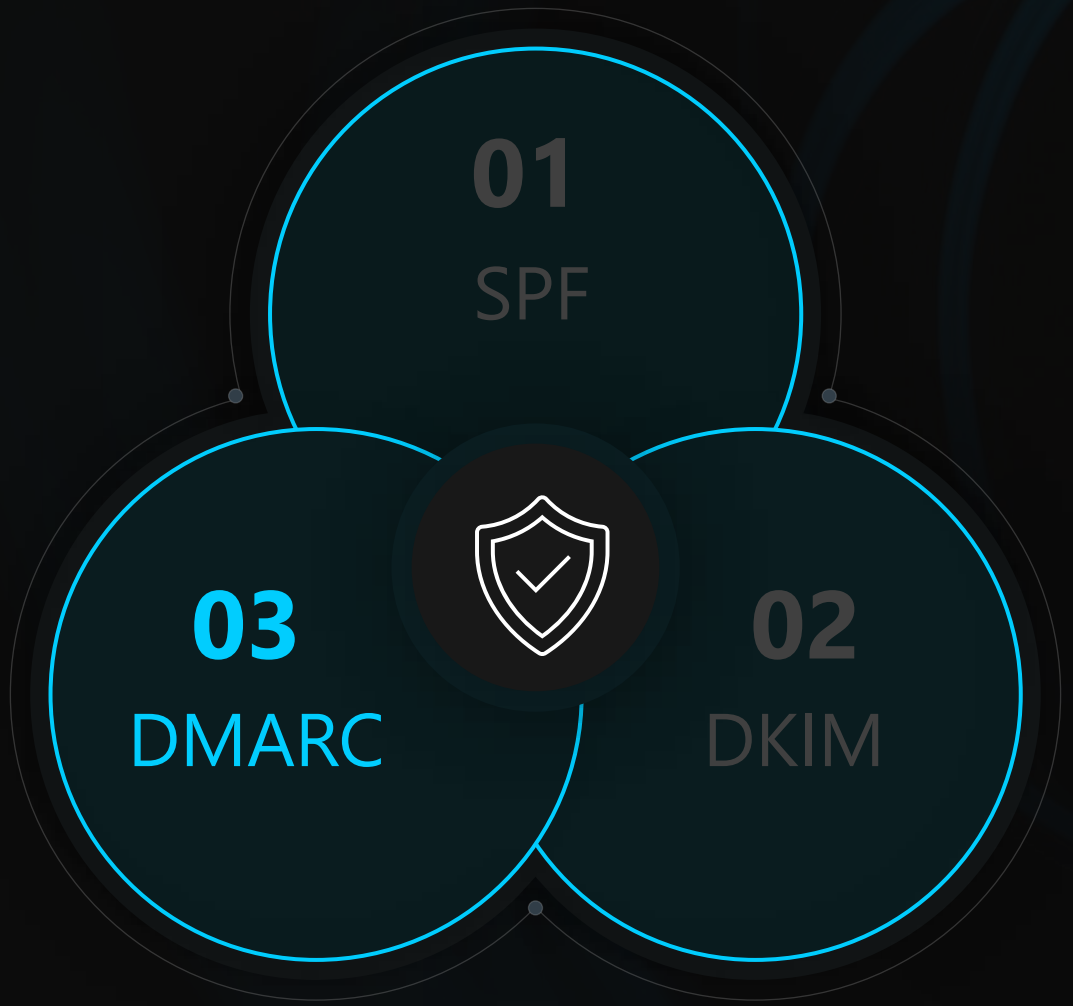
01 SPF identifies authorized mail servers – prevents spoofed messages by ensuring that emails come from authorized sources.

02 DKIM verifies email integrity and sender identity – ensures that emails haven't been tampered with and come from authorized servers.

03 DMARC provides instructions on handling emails that fail SPF or DKIM checks – combines SPF and DKIM to enhance email security; prevents domain spoofing and phishing attacks..

SPF == Sender Policy Framework // DKIM == DomainKeys Identified Mail // DMARC == Domain-based Message Authentication, Reporting, and Conformance

>Force Multipliers: DMARC



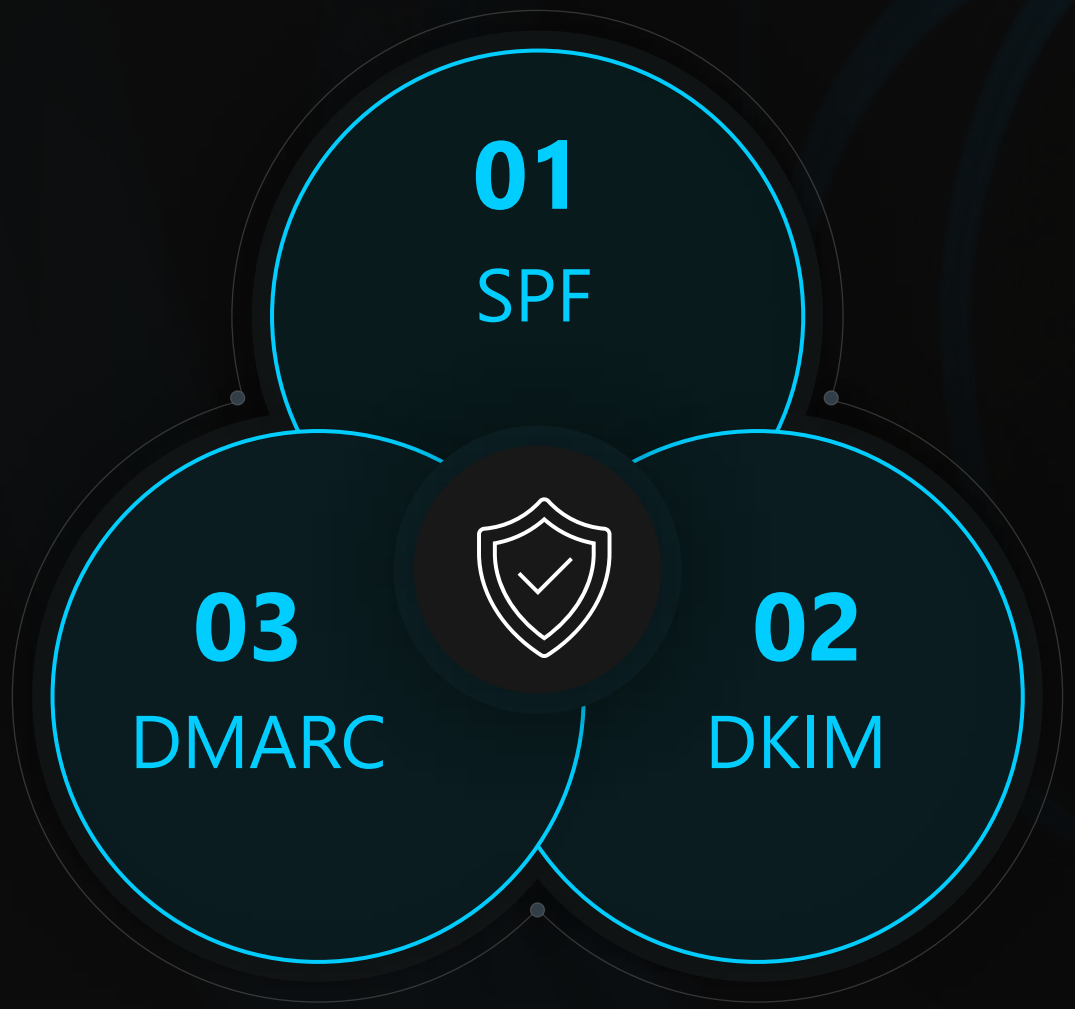
01 SPF identifies authorized mail servers – prevents spoofed messages by ensuring that emails come from authorized sources.

02 DKIM verifies email integrity and sender identity – ensures that emails haven't been tampered with and come from authorized servers.

03 DMARC provides instructions on handling emails that fail SPF or DKIM checks – combines SPF and DKIM to enhance email security; prevents domain spoofing and phishing attacks..

SPF == Sender Policy Framework // DKIM == DomainKeys Identified Mail // DMARC == Domain-based Message Authentication, Reporting, and Conformance

>Force Multipliers



01 SPF identifies authorized mail servers – prevents spoofed messages by ensuring that emails come from authorized sources.

02 DKIM verifies email integrity and sender identity – ensures that emails haven't been tampered with and come from authorized servers.

03 DMARC provides instructions on handling emails that fail SPF or DKIM checks – combines SPF and DKIM to enhance email security; prevents domain spoofing and phishing attacks..

SPF == Sender Policy Framework // DKIM == DomainKeys Identified Mail // DMARC == Domain-based Message Authentication, Reporting, and Conformance

>Domain Drift & Cyber Mayhem: A Saga in 4 Parts – Pt 1.

Get Domain Creds

>> Options: phishing emails, social engineering tactics, or exploiting vulnerabilities in the organization's network.

>> Insider threat could leak sensitive information or maliciously mishandle individual access

>Domain Drift & Cyber Mayhem: A Saga in 4 Parts – Pt 2.

Get Domain Creds

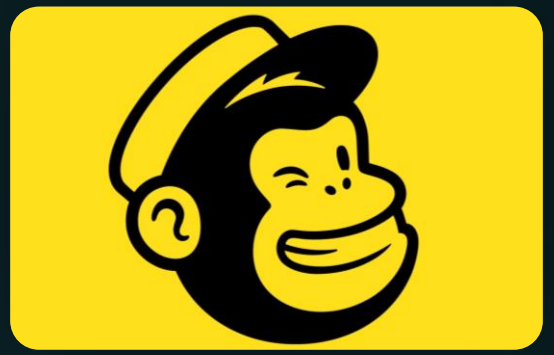
>> Options: phishing emails, social engineering tactics, or exploiting vulnerabilities in the organization's network.

>> Insider threat could leak sensitive information or maliciously mishandle individual access

Setup Campaign Builder

>> Choose a campaign platform – in this case, we used Mailchimp for Research purposes

>> Use domain account to verify email address with the service



>Domain Drift & Cyber Mayhem: A Saga in 4 Parts – Pt 3.

Get Domain Creds

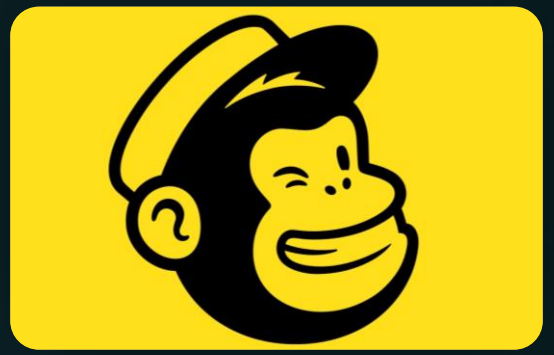
>> Options: phishing emails, social engineering tactics, or exploiting vulnerabilities in the organization's network.

>> Insider threat could leak sensitive information or maliciously mishandle individual access

Setup Campaign Builder

>> Choose a campaign platform – in this case, we used Mailchimp for Research purposes

>> Use domain account to verify email address with the service



Send Campaign Blast

>> Replace original domain email with spoof sender, (e.g., helpdesk@, support@, etc.)

>> Can send to internal user list or external targets

>Domain Drift & Cyber Mayhem: A Saga in 4 Parts – Pt 4.

Get Domain Creds

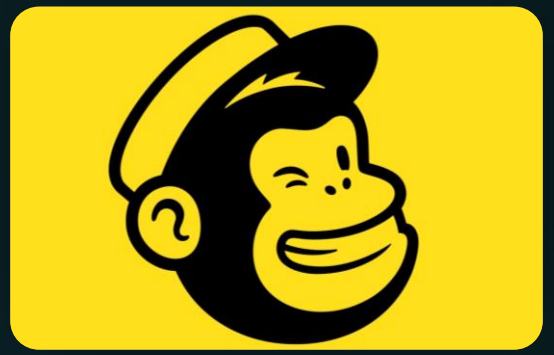
>> Options: phishing emails, social engineering tactics, or exploiting vulnerabilities in the organization's network.

>> Insider threat could leak sensitive information or maliciously mishandle individual access

Setup Campaign Builder

>> Choose a campaign platform – in this case, we used Mailchimp for Research purposes

>> Use domain account to verify email address with the service



Send Campaign Blast

>> Replace original domain email with spoof sender, (e.g., helpdesk@, support@, etc.)

>> Can send to internal user list or external targets

Wreak Havoc at Scale

>> While this requires a compromised domain email to start, the cascading fallout is non-trivial and could be catastrophic based on target and scenario

>Let's Drive this Forward...

Historical HTML Campaigns

>> As of late 2023, marketing platform supported campaign delivery to ***internal org*** recipients && ***external accounts***, with only the original account holder address verified with service

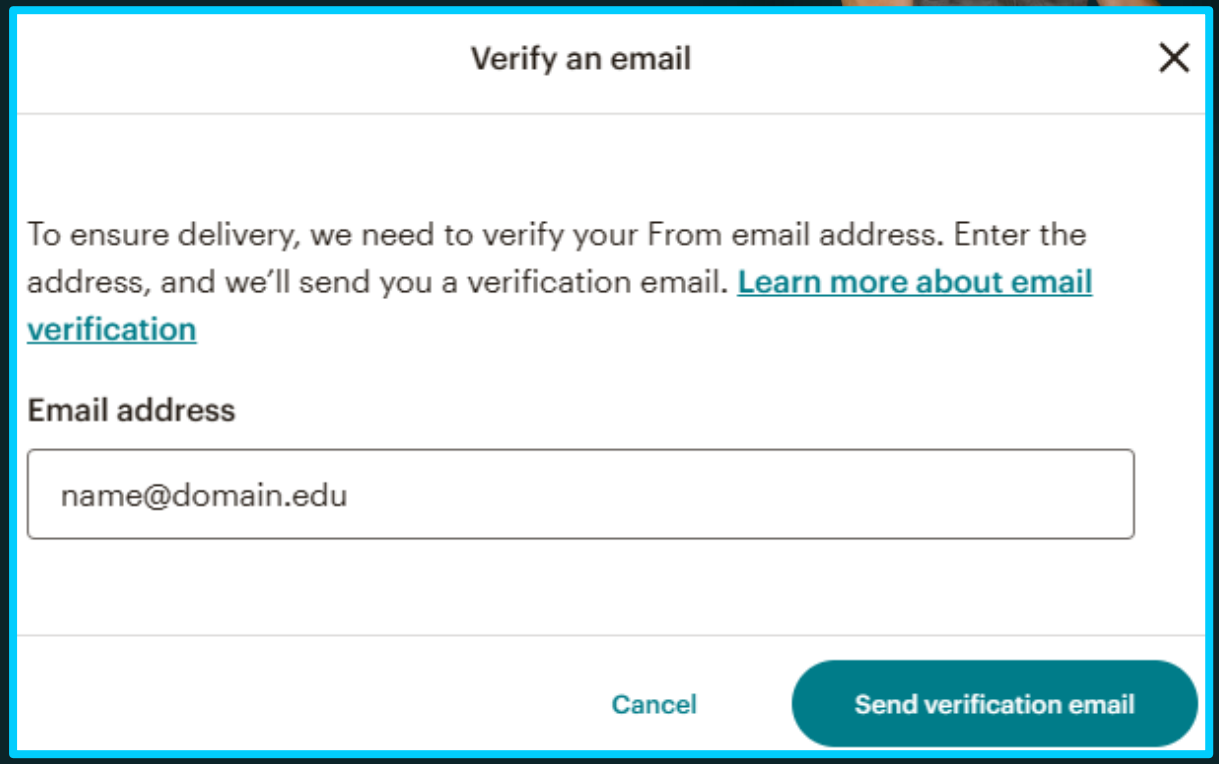
>> So, if <pawn>[@]university.edu signed up for service and verified account, then <pawn> can send emails appearing as ANY account (actual or fictitious) with the verified domain.

>On Your DMARCs, Ready, Set...

HTML Campaigns 2.0 for 2024

>> Google and Yahoo launched new DMARC requirements that went into effect February 2024 for any org that sends >5K emails – Marketing platform updated their UI to require email verification from individual senders

>> *"...SPF and DKIM provide protection against impersonation through better authentication, while DMARC creates a notification channel back to the domain-name owner to collect information on whether their email is being spoofed."*



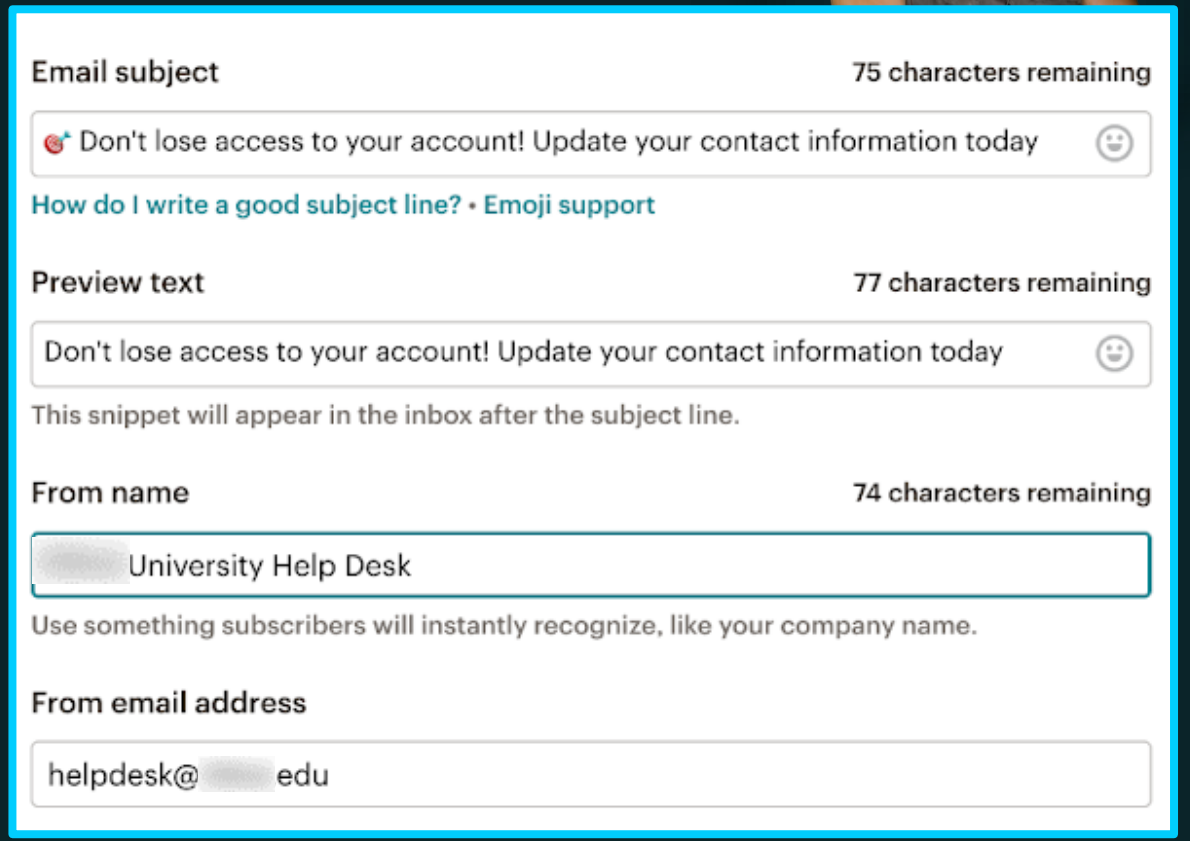
Read more: *https://www.darkreading.com/cybersecurity-operations/google-yahoo-push-dmarc-forcing-companies-to-catch-up*

>Let me take you for a ride...

Spoofpocalypse Begins...

>> We registered for service with pawn[@]<university>.edu address, but we're able to replace the original sender with the desired spoof sender: helpdesk[@]<university>.edu

>> We can customize From name to further drive appearance of legitimacy



>Going High Octane

Plaintext still packs a punch

>> Plaintext == no styling, just text – no images. Nothing fancy.

>> Lots of orgs use plaintext for legitimate comms – crisis management, service-related info, major time sensitive updates, calls to action, etc.

>> The email body included a URL that routed to a Rick Rolling video…

```
**** THIS IS A SIMULATION ****

In order to ensure that the University can locate and contact all students in cases of
emergency, the University is now requiring that all students verify their contact
information each semester. Please verify or update your contact information using the
link below. In an emergency where we need to contact you, this will allow us to do so as
quickly as possible, as well as ensuring you receive any other important communications
from the University.

This will only take a few moments of your time. Please complete and submit the form
today by clicking on the link below:

https://t.ly/sc-gK
================================================
*|LIST:DESCRIPTION|*

Unsubscribe *|EMAIL|* from this list:
*|UNSUB|*

Our mailing address is:
*|LIST:ADDRESS|*

Our telephone:
*|LIST:PHONE|*

Forward this email to a friend:
*|FORWARD|*

Update your profile:
*|UPDATE_PROFILE|*
```

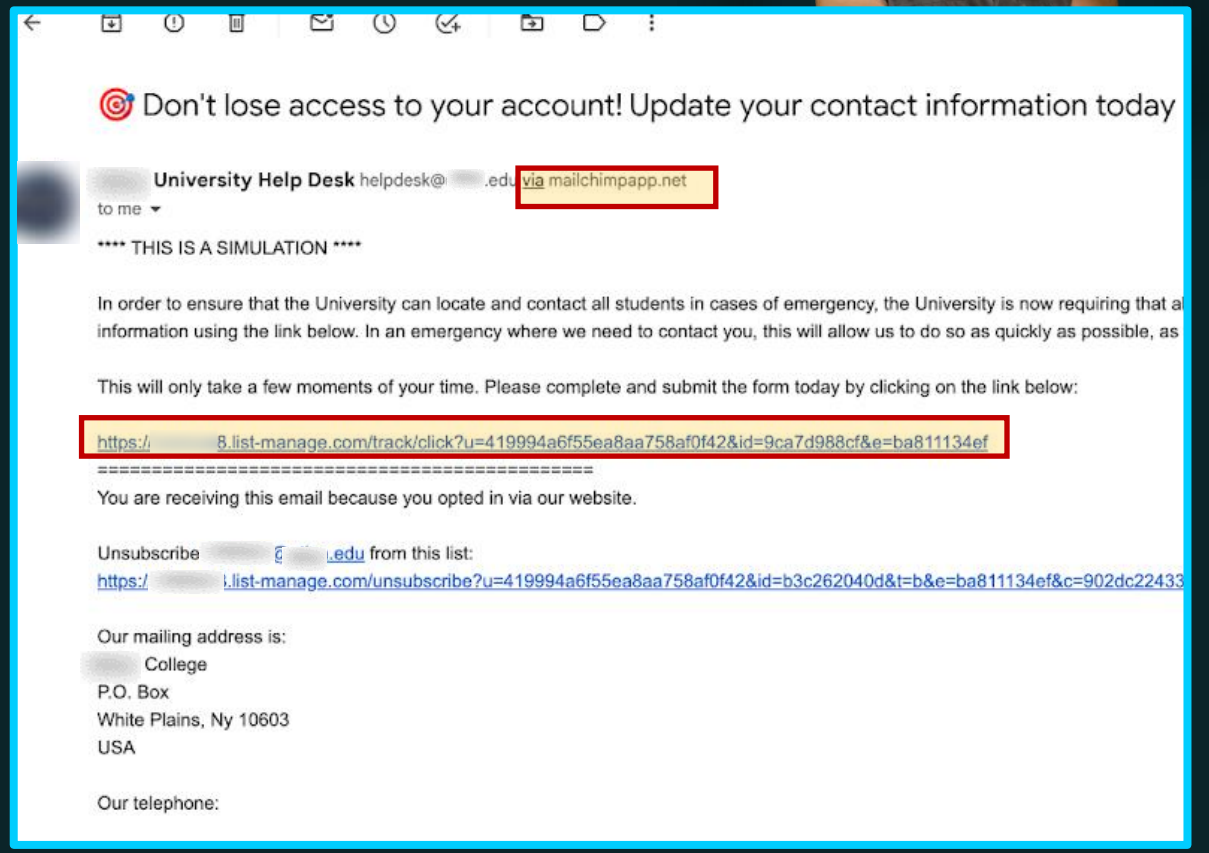
>[Desk]Top Gear POV

Red Flags as Technical Controls

>> Campaign sent to internal org addresses && external recipients – on desktop view, “via mailchimp” is appended to sender

>> Mail still arrived in Inbox without an alert, External banner, etc

>> Do targets got enough sense to not get got?

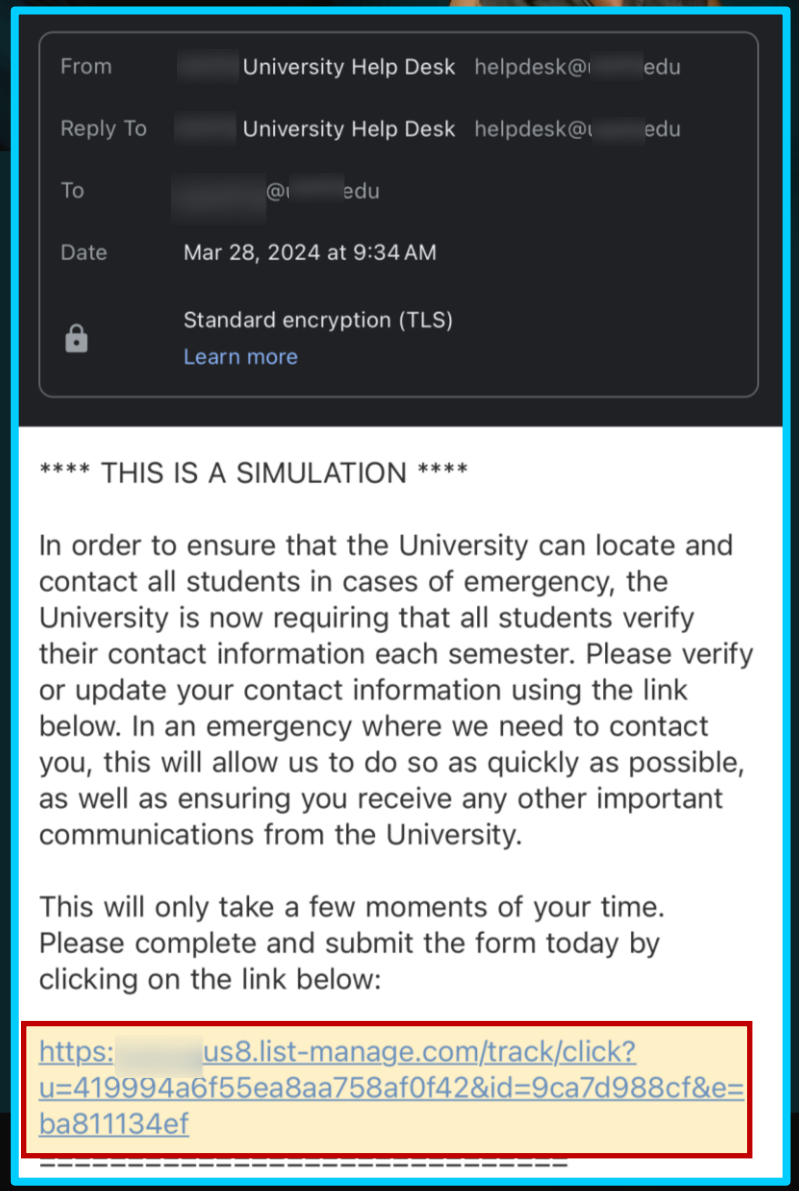


>Winning is winning…

All good rides come to an end(point)!

>> Mobile view comes in flawless, no “via service” appended to sender address

>> Campaign builder converted original URL to a string that includes the domain and appears legitimate



>Engine Check

Submitted a report via Responsible Disclosure program – returned as **Out of Scope** and **Closed**

Reached out to campaign builder service and shared concerns – received response that the **burden is on the org** to setup controls

Notified org of the situation and they are working to address

Asking the question: if marketing service can enhance controls for HTML Campaigns – which falls in their control – why is the talk track that **orgs can go CTRL F themselves** for Plaintext Campaigns?

Mar 29, 2024, 1:42 PM EDT

Authentication is our way to ensure safety of your domain and the email that is being sent to arrive in the inbox.

*Without authentication, there is not much on our end we can do to ensure these things…**this would actually be on your domains end rather than our end here**. Either way, authentication will solve this…*

- Name Redacted, Mailchimp

>Rollout && Follow-up

Vendor Controls

>> Update UI to restrict plaintext email campaigns to send with only verified accounts (at minimum)

Org Controls

>> Strengthen Email Authentication: SPF, DKIM, DMARC help verify the authenticity of incoming emails and prevent spoofing

Security Program Mitigations

>> SPF, DKIM, and DMARC

>> Set up an external banner or flag for emails delivered by Mailchimp servers

>> Use Advanced Email Filtering Solutions

>> End User Training and Awareness Efforts

Good Cyber Citizenship

>> Google & Yahoo's 2024 DMARC sets new standards in email security to thwart spoofing and phishing.

>> Their lead in the email sector paves the way for broader digital safety, urging all tech sectors to strengthen defenses.

>> A unified effort is key in our interconnected digital world.

Thank you