

Phish & Furious

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

Presented by: Raee Wolfram

About Calculated Chaos

>> Raee Wolfram has over 15 years of professional experience in IT, a decade of which focused on healthcare IT. She currently serves as a Senior Product Manager at Microsoft, building out their first party managed security services.

>> Raee was raised in a close-knit Puerto Rican family in the Bronx and brings a unique cultural perspective to her work. She resides in Westchester, New York, with her child, miscellaneous Star Trek memorabilia and assorted tchotchkes, and a beloved cat.



Raee Wolfram



A cyber practitioner during the day, a chaos whisperer by choice. Skillfully treading the line of chaotic good, with a dynamic touch for turning digital chaos into organized solutions.

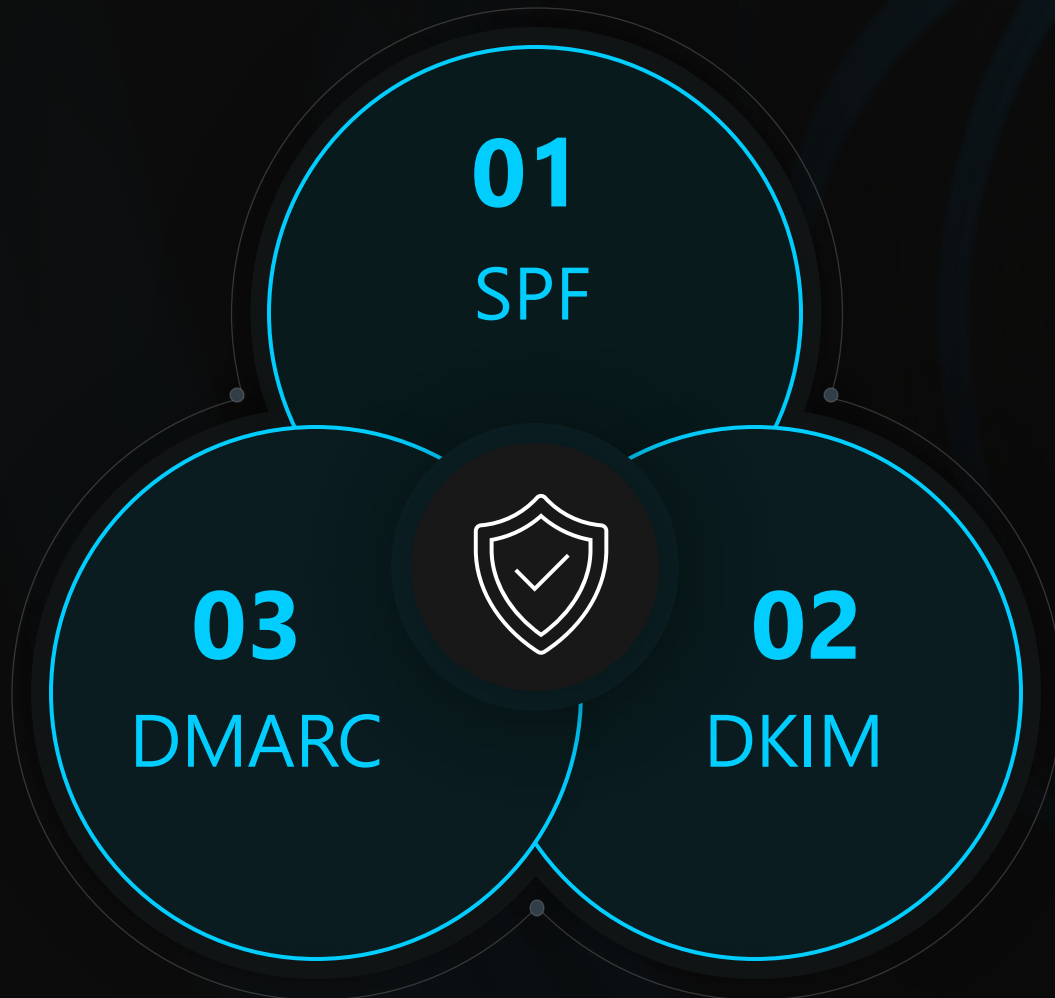
> Phish & Furious Overview



Fast Track Defense: Getting up to Speed

- >> This presentation will cover vulnerabilities in campaign builders such as Mailchimp and how they can be exploited for phishing attacks.
- >> We will delve into technical aspects like trust manipulation and the scalability of these attacks, along with key considerations for mitigating these risks.
- >> The overall aim is to provide practical strategies to understand and combat evolving phishing threats.

> 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..

> Domain Drift & Cyber Mayhem



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.

From: **Administrator** <admin@university.edu>
Date: Thu, Nov 9, 2023 at 8:57 PM
Subject: This is a test for conference proposal
To: <pawn@university.edu>

[View this email in your browser](#)



This is a test

Very impressive conference proposal idea here — just

>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."*

Verify an email

To ensure delivery, we need to verify your From email address. Enter the address, and we'll send you a verification email. [Learn more about email verification](#)

Email address

name@domain.edu

Cancel

Send verification email

> 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

Email subject 75 characters remaining

🔗 Don't lose access to your account! Update your contact information today 😊

[How do I write a good subject line?](#) • [Emoji support](#)

Preview text 77 characters remaining

Don't lose access to your account! Update your contact information today 😊

This snippet will appear in the inbox after the subject line.

From name 74 characters remaining

University Help Desk

Use something subscribers will instantly recognize, like your company name.

From email address

helpdesk@[redacted].edu

>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

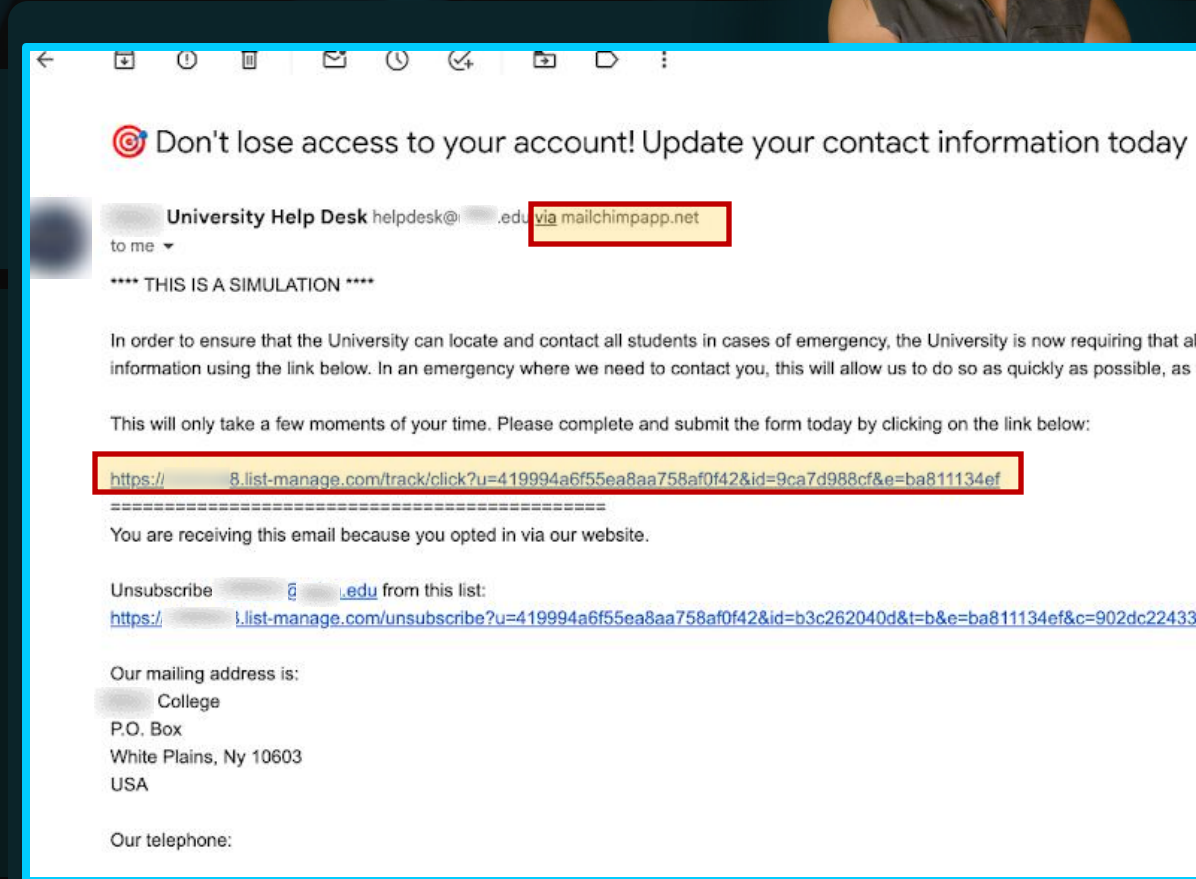


Red Flags as Technical Controls

>> 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

From University Help Desk helpdesk@i.edu
Reply To University Help Desk helpdesk@i.edu
To @i.edu
Date Mar 28, 2024 at 9:34 AM
Standard encryption (TLS)
[Learn more](#)

**** 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://us8.list-manage.com/track/click?u=419994a6f55ea8aa758af0f42&id=9ca7d988cf&e=ba811134ef>

> 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



IS THAT WHAT THEY TOLD YOU?



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