

# Ichthyology: Phishing as a Science

@tetrakazi

stripe



Let's talk.

Dear Sir,

I would like to offer you a large sum  
of money...

## System 1

Fast

Instinctive

Emotional

Gullible

## System 2

Slow

Methodical

Rational

Skeptical



# Information Overload



Action



Exploit



Credential

Hook

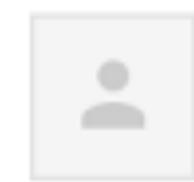


Phishing site



Trail out

# [Slack] Email verification enabled



Slack <no-reply@slack.com>

to me ▾



## Email verification enabled

Your team administrator at **Stripe** has enabled email verification for your team.

[Verify your email](#)

You'll need to verify your email address before you can continue using Slack.

All you need to do is connect your Slack account to your email. You can do that right now at this link: <https://slack.com/z-sso-3957295028-4967528491-zz30297693>

That's all, thanks!  
- Team Slack

## [Slack] Single sign-on enabled



Slack <no-reply@slack.com>

to me ▾



### Single sign-on enabled

Your team administrator at **Stripe** has enabled Single sign-on (SSO for short!) for your team.

[Authenticate your account](#)

What does this mean for you?

1. You'll no longer need to remember a separate Slack email address and password to sign in.
2. Now when you sign in to Stripe, you can do so using your SSO account.

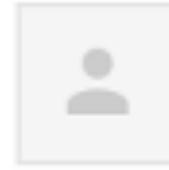
All you need to do is connect your Slack account to your SSO account.

You can do that right now at this link: <https://slack.com/z-sso-2151146308-3268585021-zzw15NyOWO>

That's all, thanks!

– Team Slack

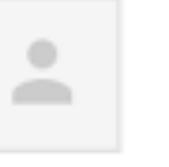
## [Slack] Single sign-on enabled



Slack <no-reply@slack.com>

to me ▾

## [Slack] Email verification enabled



Slack <no-reply@slack.com>

to me ▾

### [Slack] Single sign-on enabled

Slack <no-reply@slack.com>  
to me ▾



#### Single sign-on enabled

Your team administrator at **Stripe** has enabled Single sign-on (SSO for short!) for your team.

[Authenticate your account](#)

What does this mean for you?

1. You'll no longer need to remember a separate Slack email address and password to sign in.
2. Now when you sign in to Stripe, you can do so using your SSO account.

All you need to do is connect your Slack account to your SSO account. You can do that right now at this link: <https://slack.com/z-sso-2151146308-3268585021-zzw15NyOWO>

That's all, thanks!  
- Team Slack

### [Slack] Email verification enabled

Slack <no-reply@slack.com>  
to me ▾



#### Email verification enabled

Your team administrator at **Stripe** has enabled email verification for your team.

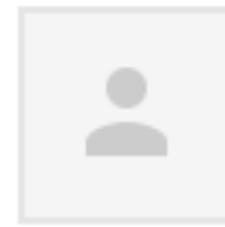
[Verify your email](#)

You'll need to verify your email address before you can continue using Slack.

All you need to do is connect your Slack account to your email. You can do that right now at this link: <https://slack.com/z-sso-3957295028-4967528491-zz30297693>

That's all, thanks!  
- Team Slack

## [GitHub] Please audit your SSH key



**GitHub <noreply@github.com>**  
to me



### ⚠ Please audit your GitHub SSH key

One of your organizations has blocked access for SSH keys created by untrusted third-party applications. If you created and imported this key yourself, you can approve it for access to your organization repositories. **You will not be able to commit using this key until it is approved.** If you have any doubts about this key, you should delete it and [upload a new one](#).

[Get help verifying fingerprints.](#)



**karla@stripe.com**

1f:5a:4e:ed:8b:7b:f9:b7:c2:70:fb:8b:ab:f4:92:a7

Last used on Feb 18, 2015

[Approve](#)

[Delete](#)

Plaintext or  $\mathcal{HTM}$

 GitHub, Inc. [US] | <https://github.com/settings/security>

Confirm password to continue

**Password** [Forgot password?](#)

**Confirm password**

Alternatively, press the button on your security key...

Tip: You are entering [sudo mode](#). We won't ask for your password again for a few hours.

[Terms](#) [Privacy](#) [Security](#) [Contact GitHub](#)

 Secure | <https://logIn.github.io/>

Confirm password to continue

**Password** [Forgot password?](#)

**Confirm password**

Alternatively, press the button on your security key...

Tip: You are entering [sudo mode](#). We won't ask for your password again for a few hours.

[Terms](#) [Privacy](#) [Security](#) [Contact GitHub](#)



Search GitHub

Pull requests Issues Marketplace Gist



## Personal settings

Profile

Account

Emails

Notifications

Billing

**SSH and GPG keys**

Security

Blocked users

Repositories

Organizations

Saved replies

Authorized OAuth Apps

## SSH keys

New SSH key

This is a list of SSH keys associated with your account. Remove any keys that you do not recognize.



karla@stripe.com

Fingerprint: 1f:5a:4e:ed:8b:7b:f9:b7:c2:70:fb:8b:ab:f4:92:a7

Last used within the last 7 days

Delete

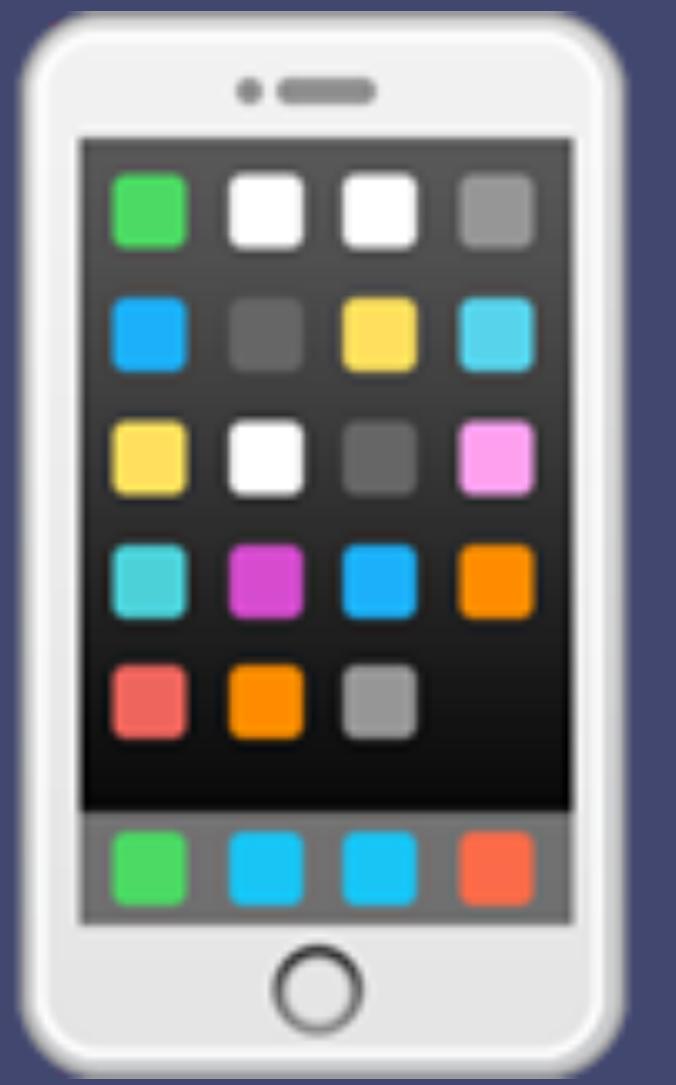
Check out our guide to [generating SSH keys](#) or troubleshoot [common SSH Problems](#).

## GPG keys

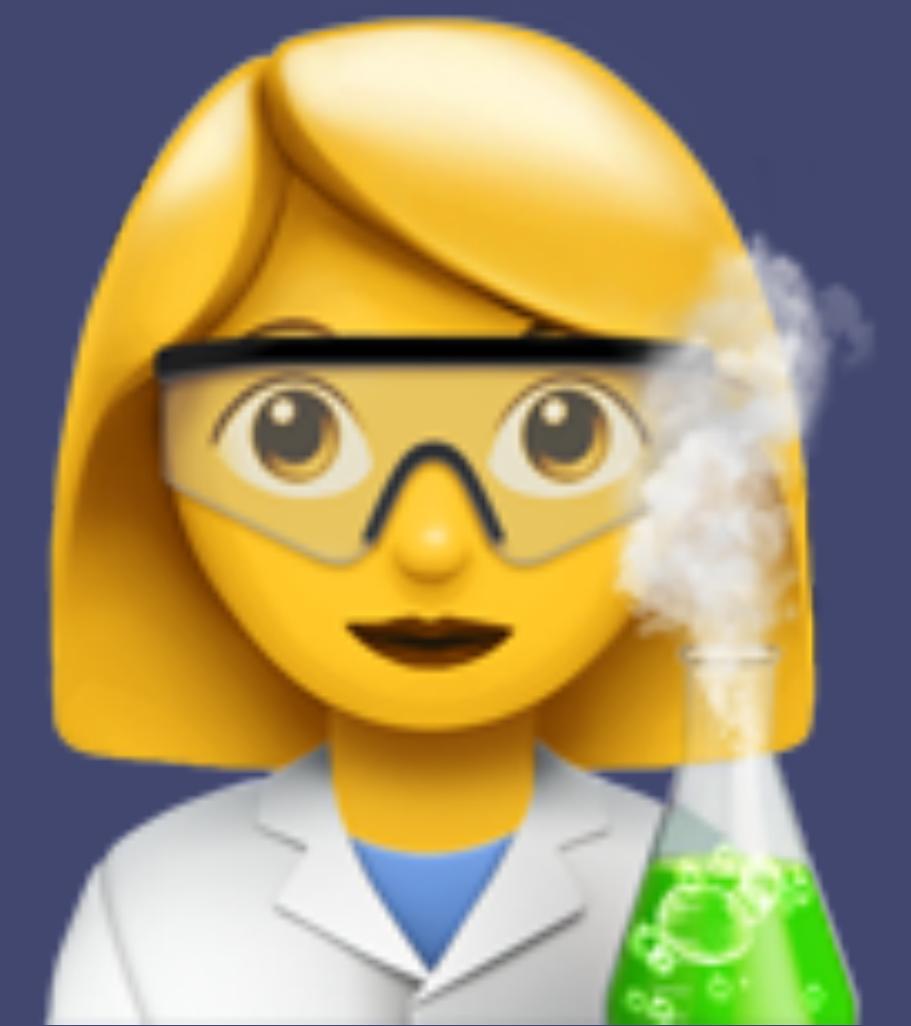
New GPG key

There are no GPG keys with access to your account.

Learn how to [generate a GPG key](#) and add it to your account.



# 2FA



# Science

Secure | <https://us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz->



Account: stripe

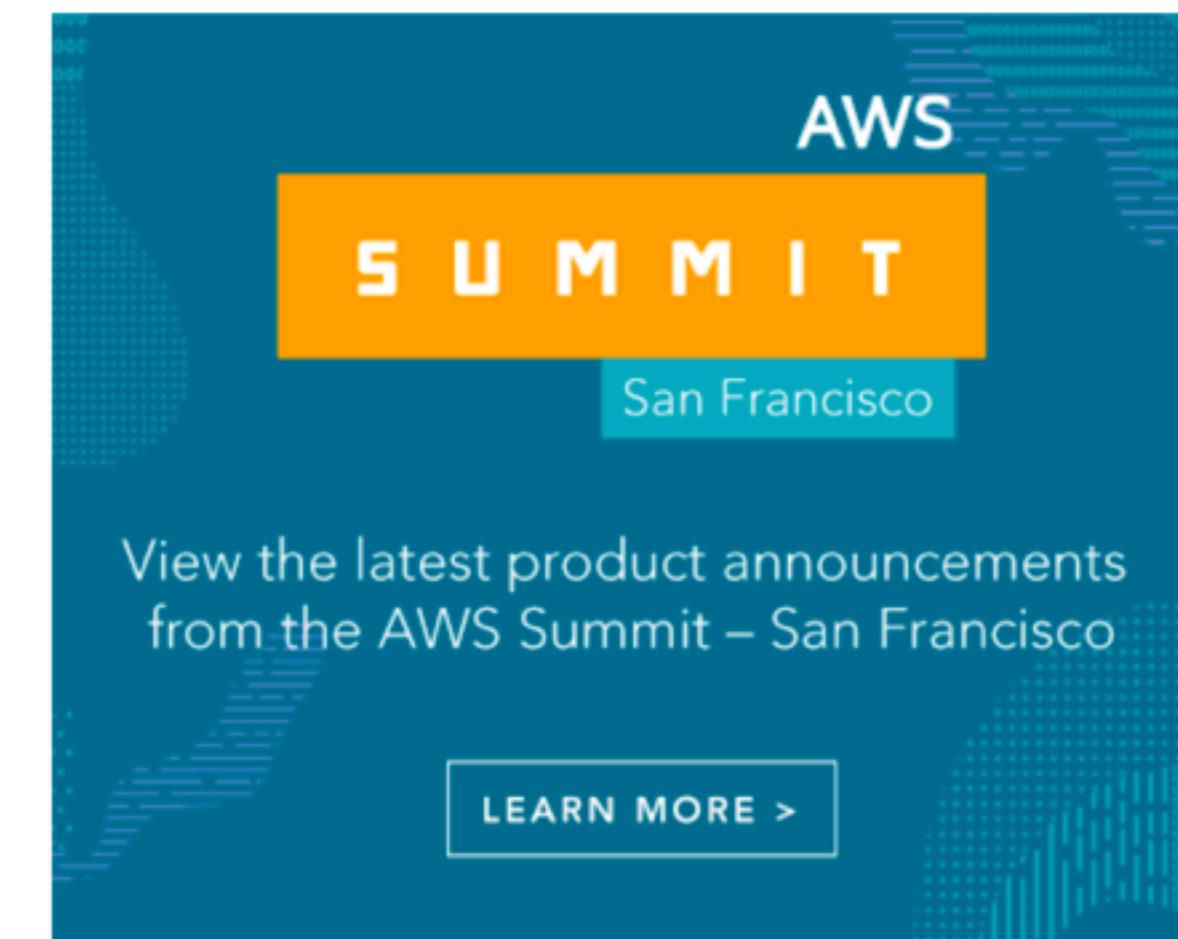
User Name:

Password:

MFA users, enter your code on the next screen.

[Sign In](#)

[Sign-in using root account credentials](#)



English

[Terms of Use](#) [Privacy Policy](#) © 1996-2017, Amazon Web Services, Inc. or its affiliates.

 Secure | <https://us-east-1.signin.aws.amazon.com/oauth?SignatureVersion=4&X-Amz->



Account: stripe

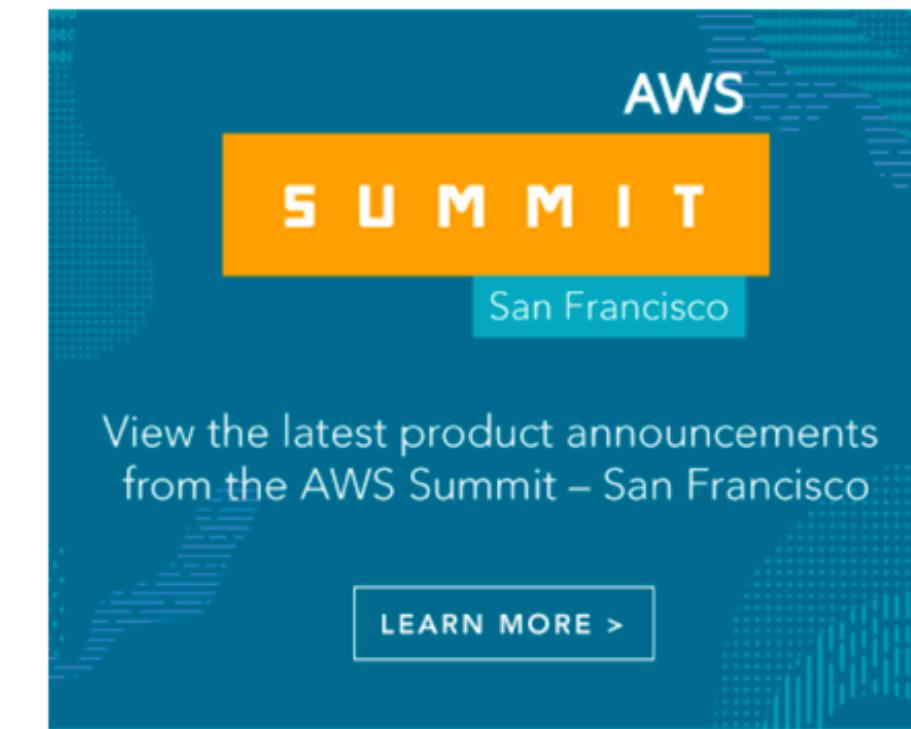
User Name:

Password:

MFA users, enter your code on the next screen.

[Sign In](#)

[Sign-in using root account credentials](#)



English 

[Terms of Use](#) [Privacy Policy](#) © 1996-2017, Amazon Web Services, Inc. or its affiliates.

 Secure | <https://us-east-1.console.awssignin.com/oauth?SignatureVersion=4&X-Amz->



Account: stripe

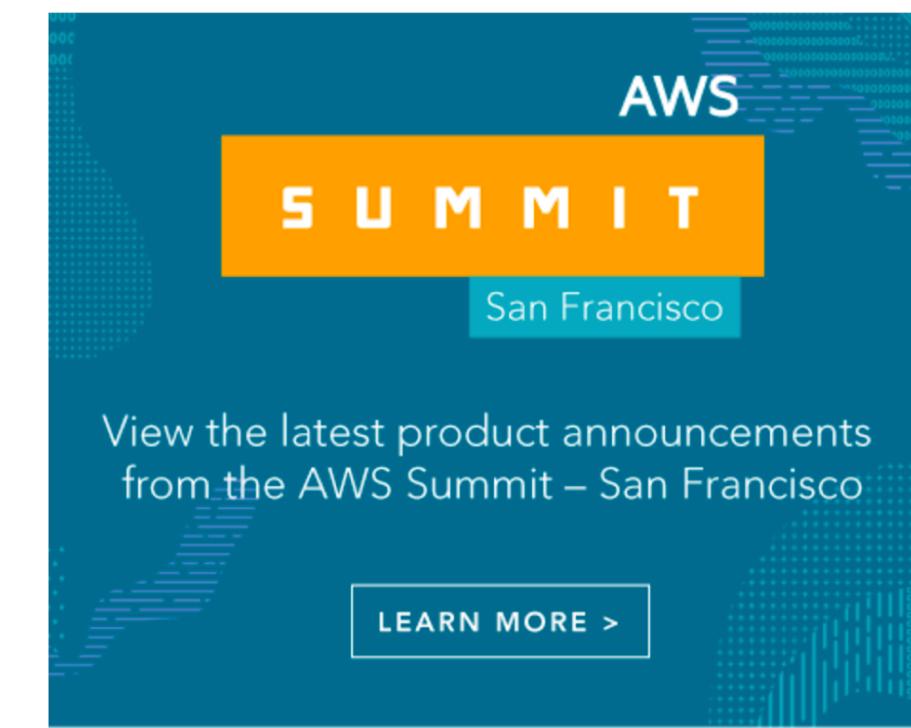
User Name:

Password:

MFA users, enter your code on the next screen.

[Sign In](#)

[Sign-in using root account credentials](#)



English 

[Terms of Use](#) [Privacy Policy](#) © 1996-2017, Amazon Web Services, Inc. or its affiliates.



What now?

Have

Know

Are

# Authentication Factors



# Client certificates





# U2F



# Single Sign On



Panacea?



Hi Karla

K

Google Docs would like to



Read, send, delete, and manage your email



Manage your contacts



By clicking Allow, you allow this app and Google to use your information in accordance with their respective [terms of service](#) and [privacy policies](#). You can change this and other [Account Permissions](#) at any time.

DENY

ALLOW

Patrick Collison invited you to [Draft] Compensation Adjustments ➤



Quip <noreply+GKFAEAFTyt@quip-sso.com>  
to me ▾



You were added to  
[Draft] Compensation Adjustments



Patrick Collison invited Karla Burnett to view

## [Draft] Compensation Adjustments

Hey folks,

In the lead up to Q3 we decided to review our compensation policy to bring us in line with the rest of the market. Over the last several weeks we've solicited feedback from across the company and the industry, and will be adjusting our internal compensation accordingly.

These changes will take effect at the beginning of Q3.

[View](#)

[Unsubscribe](#) from these notifications or change your [email preferences](#).

Quip Inc.

988 Market St. 7th Floor  
San Francisco, CA 94102

Google

Hi Karla

K

Quip would like to



Read, send, delete, and manage your email



Manage your contacts



By clicking Allow, you allow this app and Google to use your information in accordance with their respective [terms of service](#) and [privacy policies](#). You can change this and other [Account Permissions](#) at any time.

DENY

ALLOW

# So, phishing?

- Forbidding phishing in red team exercises is sticking your head in the sand.
- Phishing training is ineffective, because you're likely to fall for phishing emails too.
- But there are technical solutions that prevent or mitigate many types of phishing - use them!

# Questions!

@tetrakazi

karla@stripe.com