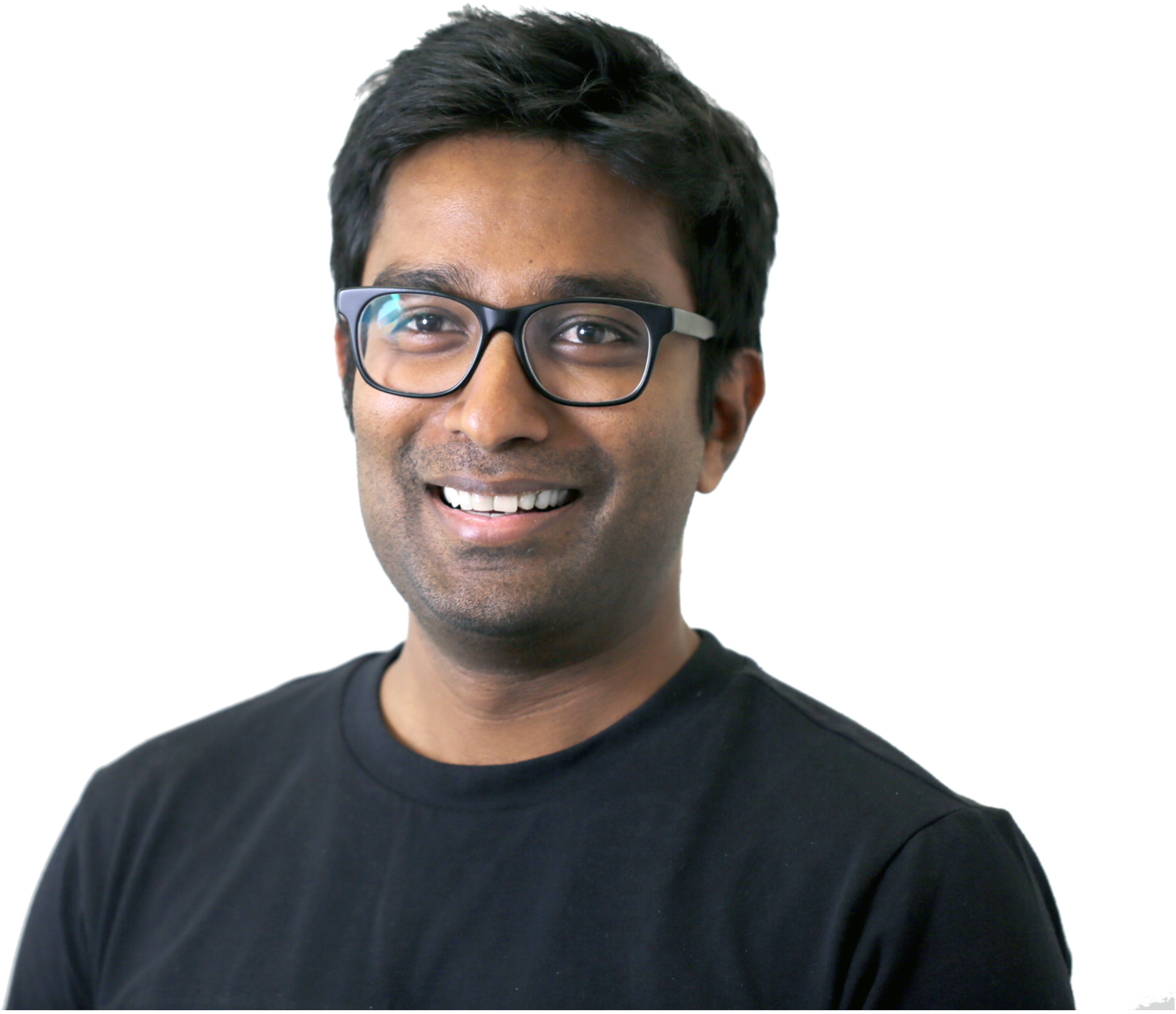
OK Google, Build Me a Phishing Campaign

armorblox.com/blog/ok-google-build-me-a-phishing-campaign/

Back



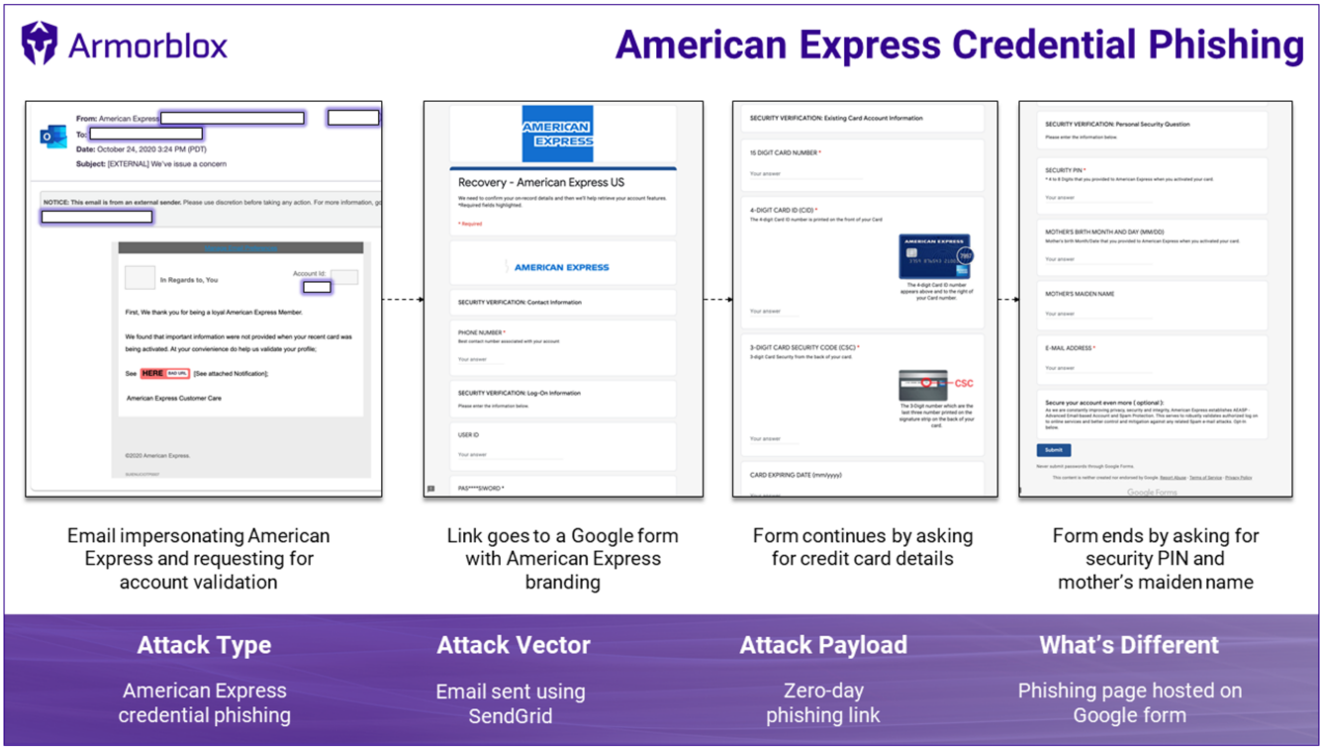
Written by Arjun Sambamoorthy

Threat Research / 11.19.20

Google's mail, workplace productivity, and other business services have helped millions of people simplify and share their work. Open APIs, extensible integrations, and developer-friendly tools mean that entire virtual offices - complete with virtual workflows - can exist in a Google ecosystem. Unfortunately, Google's open and democratized nature is being exploited by cybercriminals to defraud individuals and organizations of money and sensitive data.

The Armorblox threat research team has seen a sharp uptick in attackers using Google services to help them get emails past binary security filters based on keywords or URLs. In this blog, we will outline five targeted phishing campaigns that weaponize various Google services during their attack flow. These attacks are representative but in no way exhaustive - they are the tip of a deep iceberg. If successful, these email attacks using Google services could have potentially impacted tens of thousands of mailboxes within Armorblox customer environments alone.

1. American Express Credential Phishing



American Express Credential Phishing

From: American Express [redacted] [redacted]
To: [redacted]
Date: October 24, 2020 3:24 PM (PDT)
Subject: [EXTERNAL] We've issue a concern

NOTICE: This email is from an external sender. Please use discretion before taking any action. For more information, go
[redacted]

In Regards to, You

Account Id: [redacted]

First, We thank you for being a loyal American Express Member.

We found that important information were not provided when your recent card was being activated. At your convienience do help us validate your profile;

See HERE BAD URL [See attached Notification];

American Express Customer Care

©2020 American Express.

Email impersonating American Express and requesting for account validation

Recovery - American Express US

We need to confirm your on-record details and then we'll help retrieve your account features.
*Required fields highlighted.

* Required

SECURITY VERIFICATION: Contact Information

PHONE NUMBER *
Best contact number associated with your account
Your answer

SECURITY VERIFICATION: Log-On Information
Please enter the information below.

USER ID
Your answer

PAS****SWORD *

Link goes to a Google form with American Express branding

SECURITY VERIFICATION: Existing Card Account Information

15 DIGIT CARD NUMBER *
Your answer

4-DIGIT CARD ID (CID) *
The 4-digit Card ID number is printed on the front of your Card
The 4-digit Card ID number appears above and to the right of your Card number.
Your answer

3-DIGIT CARD SECURITY CODE (CSC) *
3-digit Card Security from the back of your card.

The 3-Digit number which are the last three number printed on the signature strip on the back of your card.
Your answer

CARD EXPIRING DATE (mm/yyyy)

Form continues by asking for credit card details

SECURITY VERIFICATION: Personal Security Question
Please enter the information below.

SECURITY PIN *
* 4 to 8 Digits that you provided to American Express when you activated your card.
Your answer

MOTHER'S BIRTH MONTH AND DAY (MM/DD)
Mother's birth Month/Date that you provided to American Express when you activated your card.
Your answer

MOTHER'S MAIDEN NAME
Your answer

E-MAIL ADDRESS *
Your answer

Secure your account even more (optional):
As we are constantly improving privacy, security and integrity, American Express establishes AEASP - Advanced Email-based Account and Spam Protection. This serves to robustly validates authorized log on to online services and better control and mitigation against any related Spam e-mail attacks. Opt-in below.

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Form ends by asking for security PIN and mother's maiden name

Attack Type	Attack Vector	Attack Payload	What's Different
American Express credential phishing	Email sent using SendGrid	Zero-day phishing link	Phishing page hosted on Google form

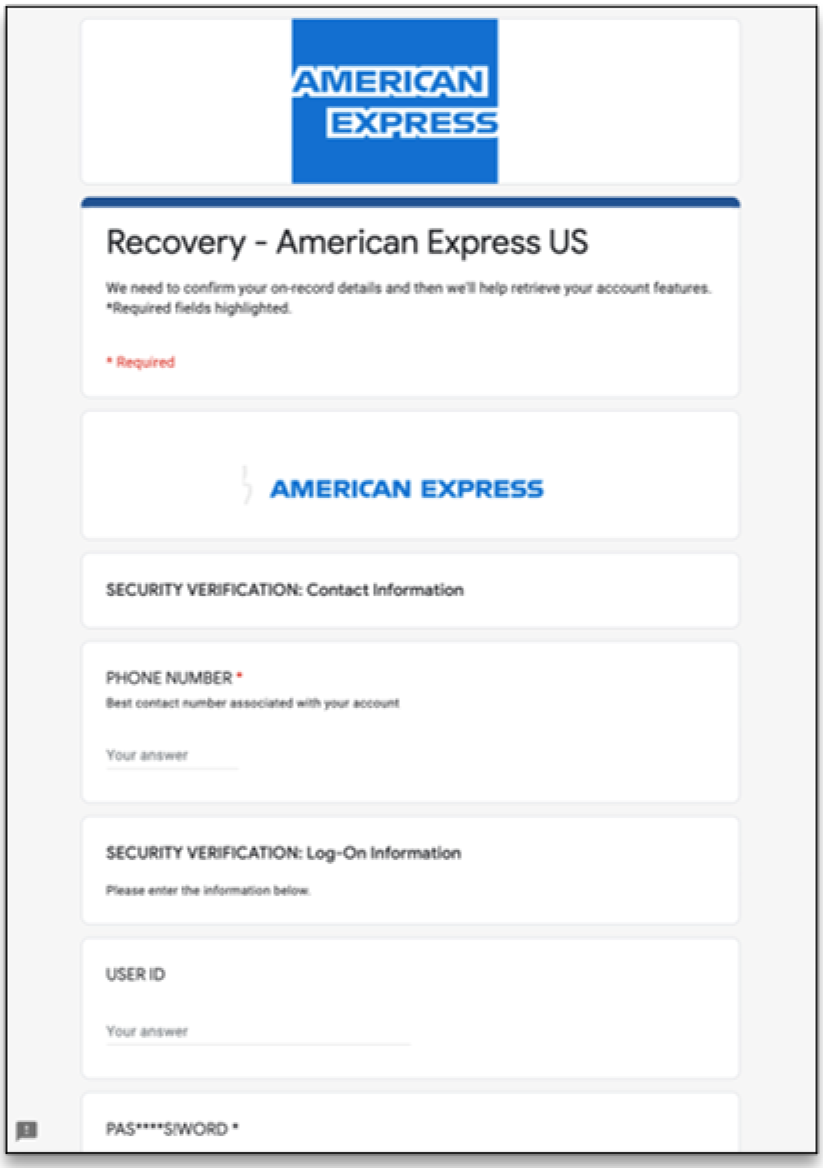
Fig: Summary of the American Express credential phishing attack

Attack summary

A credential phishing email impersonating American Express Customer Care that informs readers that they left out providing some information while validating their card. The email includes a link where readers can fill in this information and validate their card.

Google service used

The phishing page in the email is hosted on a **Google form** with a smattering of American Express branding. This fairly long form asks victims for their American Express login credentials, card details, and even their mother's maiden name (which is a common security question).



AMERICAN EXPRESS

Recovery - American Express US

We need to confirm your on-record details and then we'll help retrieve your account features.
*Required fields highlighted.

* Required

AMERICAN EXPRESS

SECURITY VERIFICATION: Contact Information

PHONE NUMBER *
Best contact number associated with your account

Your answer

SECURITY VERIFICATION: Log-On Information

Please enter the information below.

USER ID

Your answer

PAS****S!WORD *

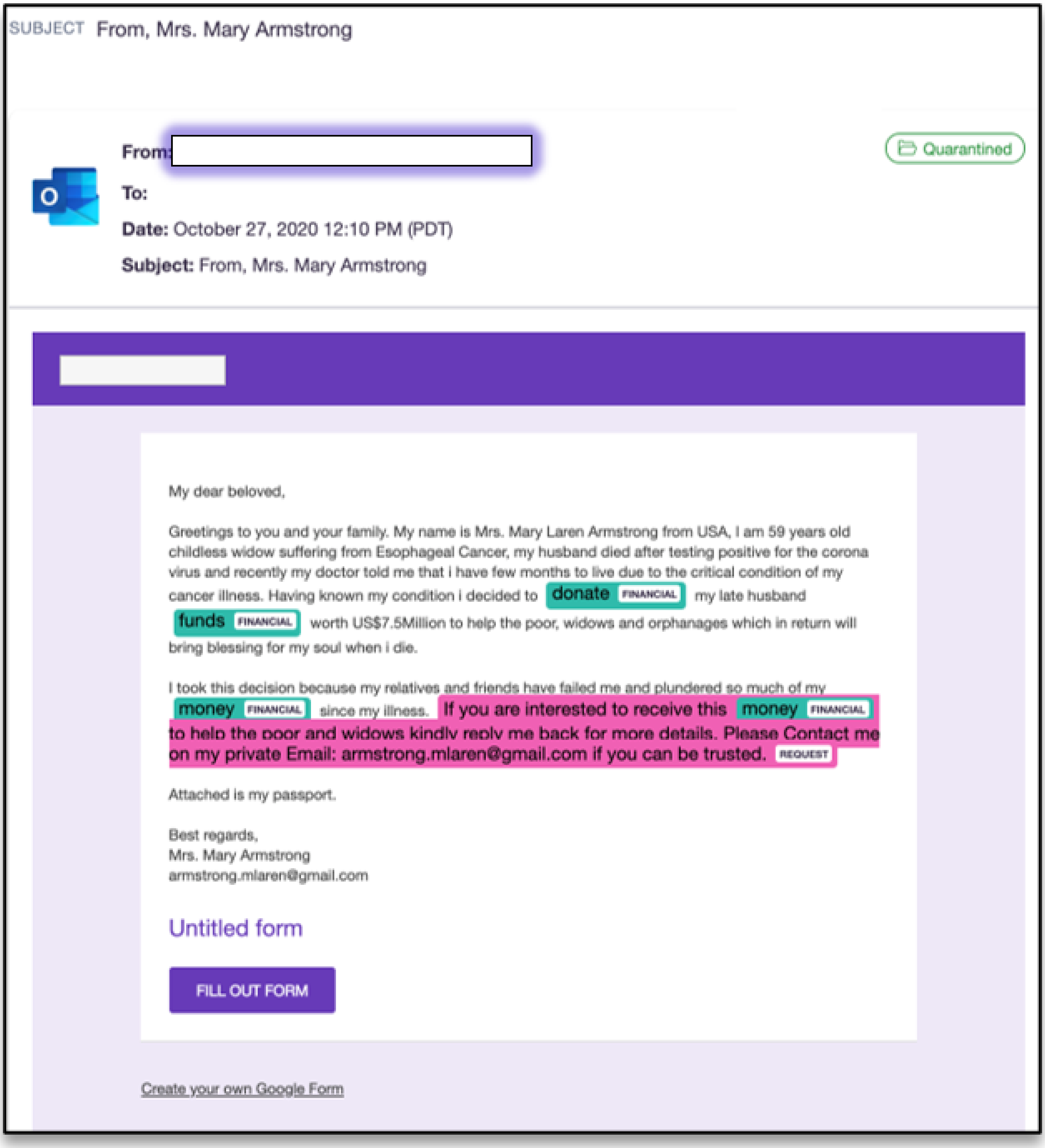
Fig: Phishing page for the AmEx attack was hosted on a Google form

Hosting the phishing page on a Google form helps the initial email evade any security filters that block known bad links or domains. Since Google’s domain is inherently trustworthy and Google forms are used for several legitimate reasons, no email security filter would realistically block this link on day zero.

Other techniques used

- Impersonation: American Express Customer Care
- Social engineering: Time-bound request to validate AmEx card by providing personal information

2. Benefactor Scam Reconnaissance



SUBJECT From, Mrs. Mary Armstrong

From: [redacted]

To:

Date: October 27, 2020 12:10 PM (PDT)

Subject: From, Mrs. Mary Armstrong

[redacted]

My dear beloved,

Greetings to you and your family. My name is Mrs. Mary Laren Armstrong from USA, I am 59 years old childless widow suffering from Esophageal Cancer, my husband died after testing positive for the corona virus and recently my doctor told me that i have few months to live due to the critical condition of my cancer illness. Having known my condition i decided to donate my late husband funds worth US$7.5Million to help the poor, widows and orphanages which in return will bring blessing for my soul when i die.

I took this decision because my relatives and friends have failed me and plundered so much of my money since my illness. If you are interested to receive this money to help the poor and widows kindly reply me back for more details. Please Contact me on my private Email: armstrong.mlaren@gmail.com if you can be trusted.

Attached is my passport.

Best regards,
Mrs. Mary Armstrong
armstrong.mlaren@gmail.com

Untitled form

FILL OUT FORM

Create your own Google Form

Fig: Benefactor scam email with a Google form link

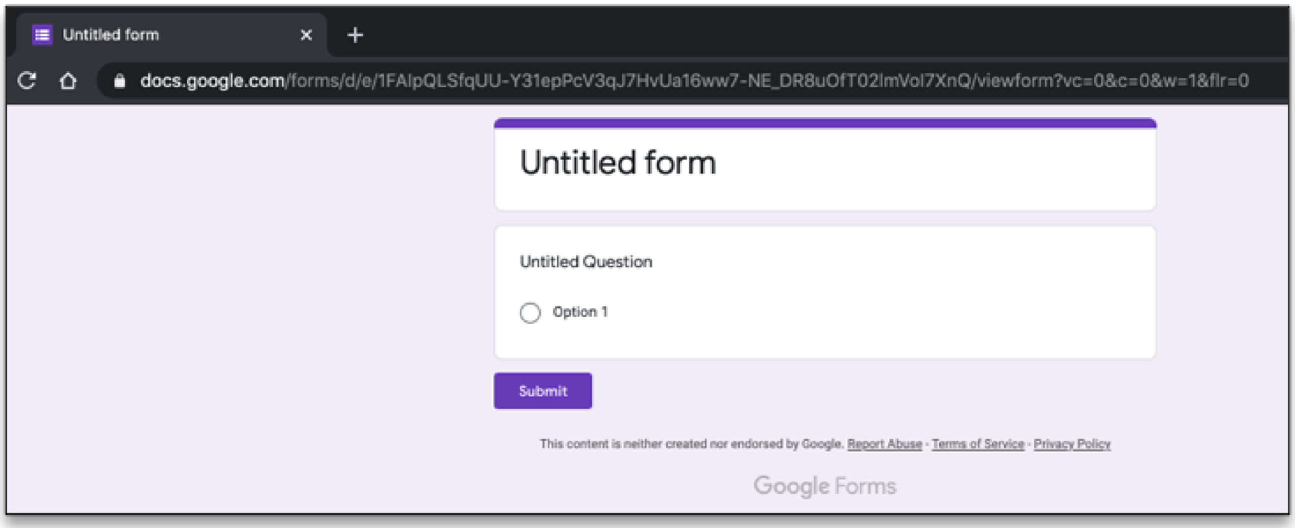
Attack summary

Cybercriminals impersonate a childless widow who wants to part with large sums of money but has nowhere to disburse it. The email asks people interested to receive money to either click the link in the email or send a reply to the address included in the email body.

Google service used

The link in the email leads to a seemingly empty **Google form** with an untitled question and one answer option (Option 1). At first glance, it seems the attackers have been lazy or negligent, but this is a **common reconnaissance technique** employed at the start of targeted email attacks.

Many people will feel the email is suspicious after going through the content and visiting this dummy form. But some people will submit the only option allowed by the form, or they will send a reply to the address provided in the email. This allows attackers to shortlist the most naive and emotionally susceptible email recipients, who will be prime targets for follow-up emails from the childless widow.



docs.google.com/forms/d/e/1FAIpQLSfqUU-Y31epPcV3qJ7HvUa16ww7-NE_DR8uOfT02lmVol7XnQ/viewform?vc=0&c=0&w=1&flr=0

Untitled form

Untitled Question

○ Option 1

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Fig: Empty Google form used as a reconnaissance technique

Just like the earlier American Express credential phishing attack, hosting the phishing page on a Google form here helps the initial email evade any security filters that block known bad links or domains.

Other techniques used

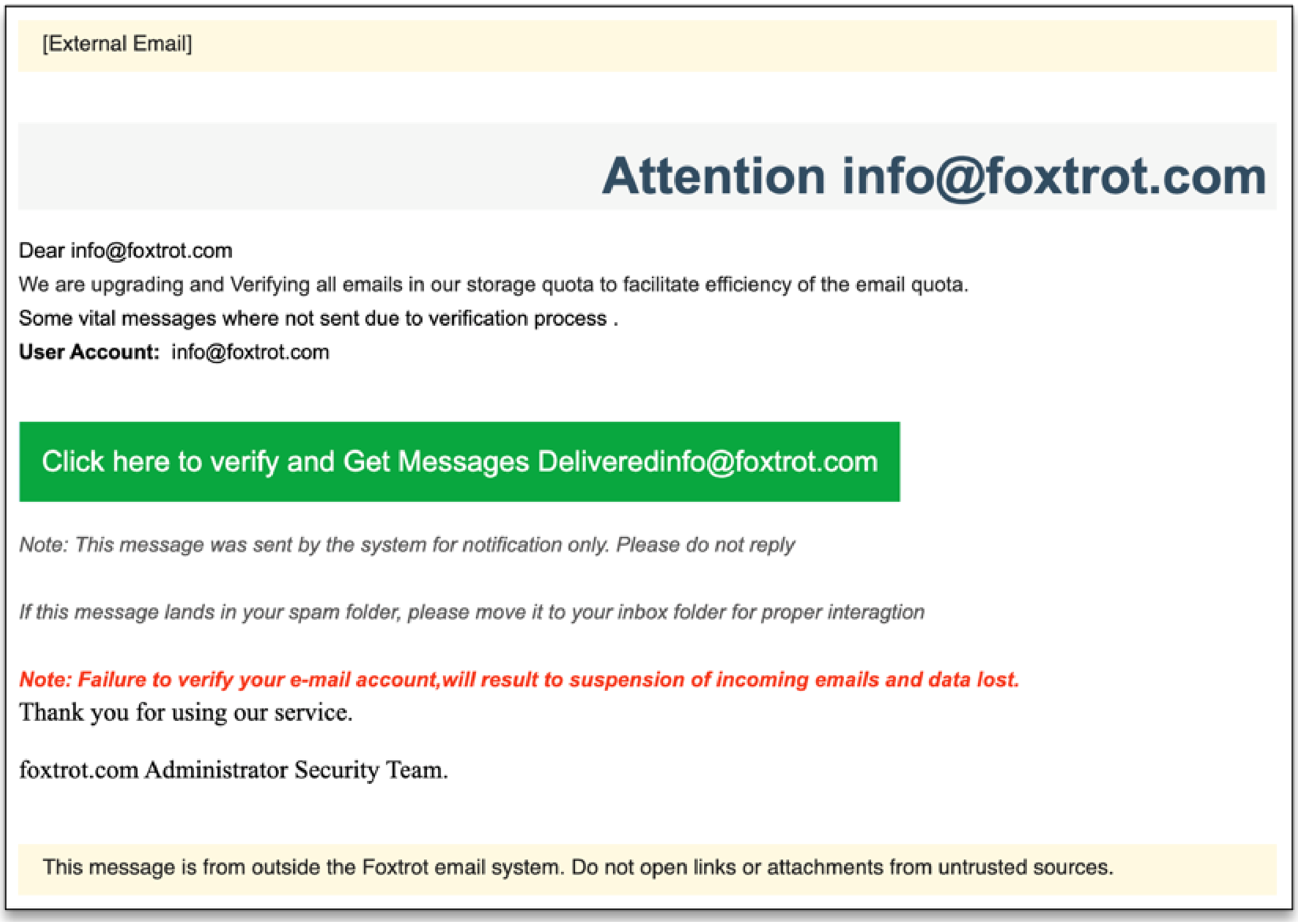
- Impersonation
- Social engineering: Emotional request from a widow, temptation of large sums of money.

3. Security Team Impersonation

Attack summary

Cybercriminals impersonate an organization’s security administrator team with an email that informs readers that they haven’t received some ‘vital’ emails because of a storage quota issue. The mail body includes a link for readers to verify their information and resume email delivery.

A snapshot of the email is given below. We have used a fictional organization called Foxtrot to showcase this email.



[External Email]

Attention info@foxtrot.com

Dear info@foxtrot.com
We are upgrading and Verifying all emails in our storage quota to facilitate efficiency of the email quota.
Some vital messages where not sent due to verification process .
User Account: info@foxtrot.com

Click here to verify and Get Messages Deliveredinfo@foxtrot.com

Note: This message was sent by the system for notification only. Please do not reply

If this message lands in your spam folder, please move it to your inbox folder for proper interagtion

Note: Failure to verify your e-mail account,will result to suspension of incoming emails and data lost.
Thank you for using our service.

foxtrot.com Administrator Security Team.

This message is from outside the Foxtrot email system. Do not open links or attachments from untrusted sources.

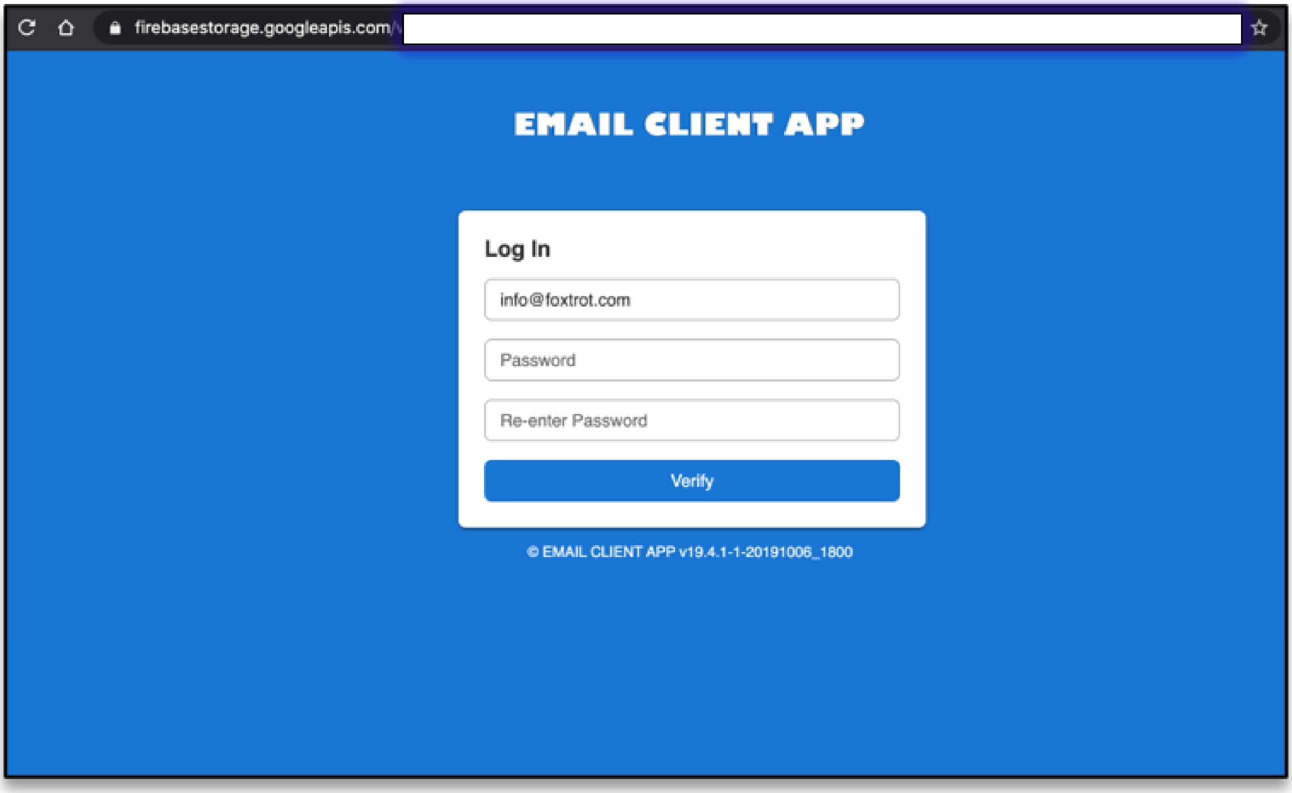
Fig: Email impersonating the security team with an email delivery failure message

Google service used

The link in the email leads to a fake login page hosted on **Firebase,** Google's mobile platform that enables users to create apps, host files and images, and serve user-generated content.

The parent URL of the page - https://firebasestorage.googleapis.com - won't be blocked by any security filters due to its inherent legitimacy.

The login screen is simple, with the email address of the victim pre entered into the first field. Imitating 'quick fill' techniques used by forms on legitimate websites is commonly used by cybercriminals to lull victims into a false sense of security.



firebasestorage.googleapis.com/[redacted]

EMAIL CLIENT APP

Log In

info@foxtrot.com

© EMAIL CLIENT APP v19.4.1-1-20191006_1800

Fig: Phishing page hosted on Firebase Storage

Other techniques used

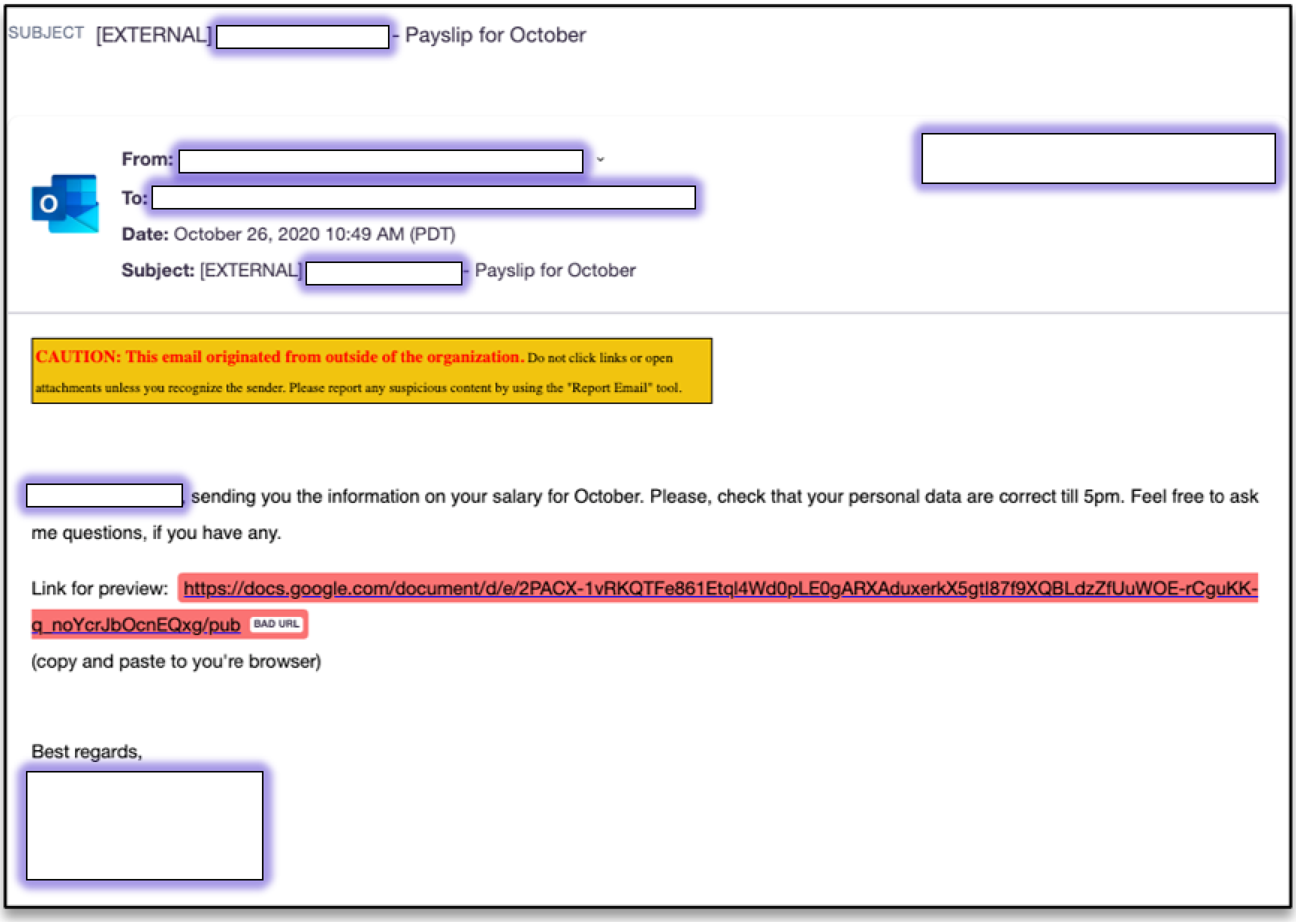
- Impersonation: security administrator team.
- Social engineering: Email focuses on failure to deliver ‘vital’ messages and includes a link to resume email delivery. The email body includes negative repercussions for lack of action (*failure to verify your email account will lead to suspension and lost data*).
- Link redirections: the URL in the email goes through one redirection before landing on the Firebase hosted page, obfuscating the attack flow for any security technology that attempts to follow the URL to its final destination.

4. Payslip Scam

Attack summary

Cybercriminals impersonate an organization’s payroll team and send an email with payslip details to victims. The email points readers to a link for them to check if their personal information for the payslip is accurate. A time-bound request to check the email link adds urgency and is likely to make victims click without thinking.

This is a variant of the more classic payroll diversion fraud, where cybercriminals impersonate employees and try to divert payroll funds to their own accounts.



SUBJECT [EXTERNAL] [redacted] - Payslip for October

From: [redacted]

To: [redacted]

[redacted]

Date: October 26, 2020 10:49 AM (PDT)

Subject: [EXTERNAL] [redacted] - Payslip for October

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender. Please report any suspicious content by using the "Report Email" tool.

[redacted], sending you the information on your salary for October. Please, check that your personal data are correct till 5pm. Feel free to ask me questions, if you have any.

Link for preview: https://docs.google.com/document/d/e/2PACX-1vRKQTFe861Etql4Wd0pLE0gARXAduxerkX5gtl87f9XQBLdzZfUuWOE-rCguKK-q_noYcrJbOcnEQxg/pub BAD URL

(copy and paste to you're browser)

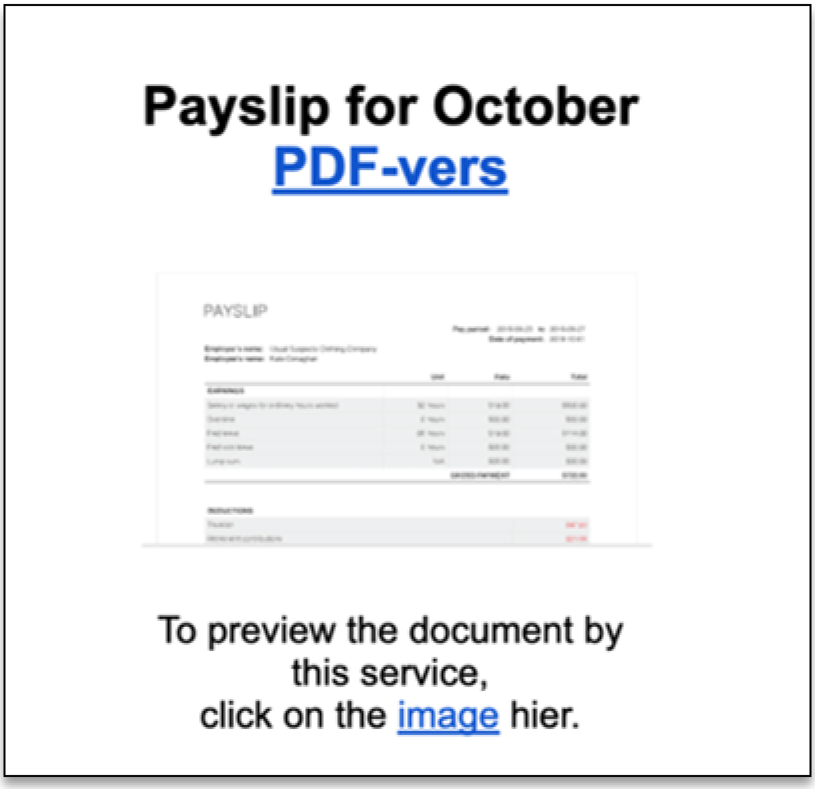
Best regards,

[redacted]

Fig: Payslip scam email with a Google Docs link

Google service used

The link in the email leads to a page hosted on **Google Docs.** Since Google Docs is ever present in our daily lives, the average recipient wouldn't be surprised to see a Google Docs link in an email from a colleague. It won't be blocked by any email security filter either - not on Day 0, at any rate. Using a Google Doc in this email is meant to trick both the recipient's eye test and traditional security layers.



Payslip for October

PDF-vers

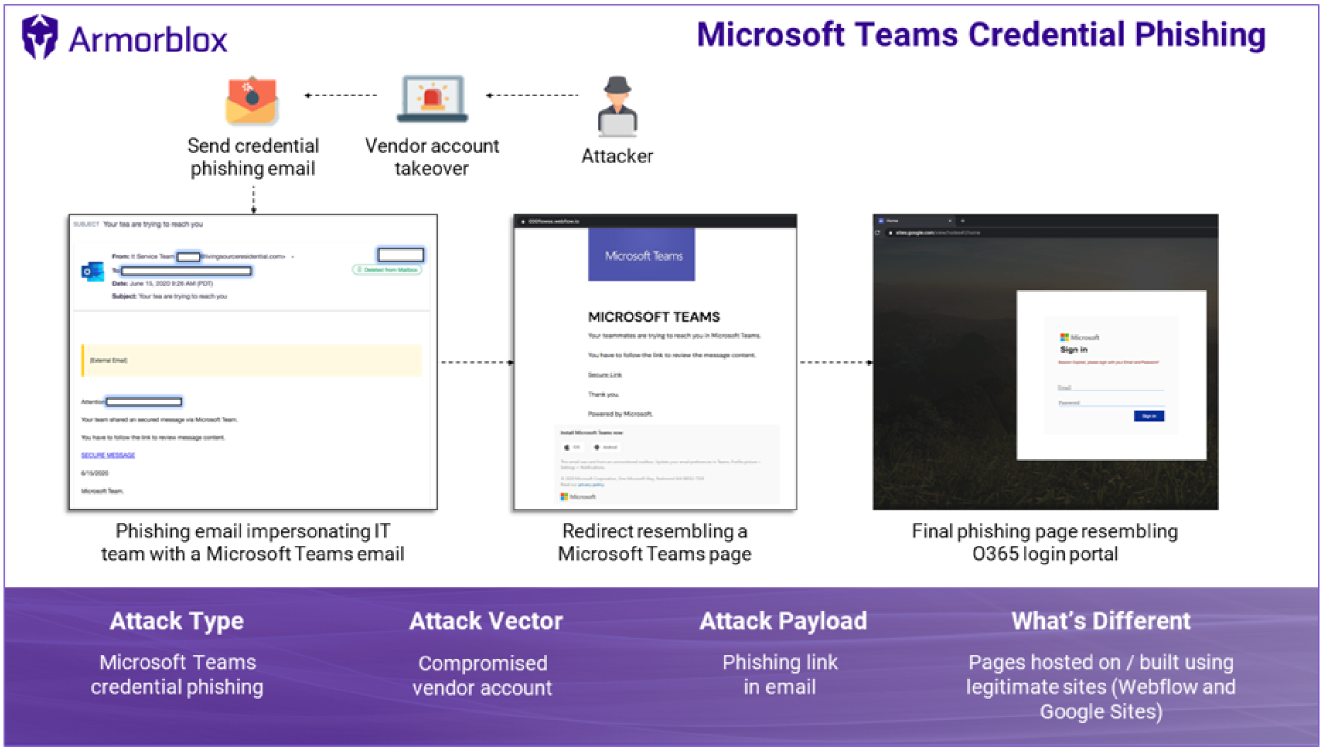
To preview the document by this service,
click on the image hier.

Fig: The link in the email leads to a Google Doc that claims to contain payslip information

Other techniques used

- Impersonation: Payroll team.
- Targeted email: The email title and body have the recipient’s name to increase legitimacy.
- Social engineering: Finance-related email with a time-bound request to take action (*check if your personal data is correct by 5pm*).
- Link redirections: The email links to the Google Doc, which further redirects to the final phishing page (which has now been taken down). These redirections obfuscate link detection technologies from identifying the URL as malicious.

5. Microsoft Teams Credential Phishing


Armorblox
Microsoft Teams Credential Phishing
Send credential phishing email
Vendor account takeover
Attacker
Phishing email impersonating IT team with a Microsoft Teams email
Redirect resembling a Microsoft Teams page
Final phishing page resembling O365 login portal
Microsoft Teams
Microsoft
Sign in
Email
Password
Sign in
iOS
Android
Deleted from Mailbox

SUBJECT Your tea are trying to reach you

From: It Service Team [redacted]@livingsourceresidential.com>
To: [redacted]
Date: June 15, 2020 9:26 AM (PDT)
Subject: Your tea are trying to reach you

[External Email]

Attention: [redacted]

Your team shared an secured message via Microsoft Team.

You have to follow the link to review message content.

SECURE MESSAGE

6/15/2020

Microsoft Team.

MICROSOFT TEAMS

Your teammates are trying to reach you in Microsoft Teams.

You have to follow the link to review the message content.

Secure Link

Thank you.

Powered by Microsoft.

Install Microsoft Teams now

Attack Type	Attack Vector	Attack Payload	What's Different
Microsoft Teams credential phishing	Compromised vendor account	Phishing link in email	Pages hosted on / built using legitimate sites (Webflow and Google Sites)

Fig: Summary of the Microsoft Teams credential phishing attack

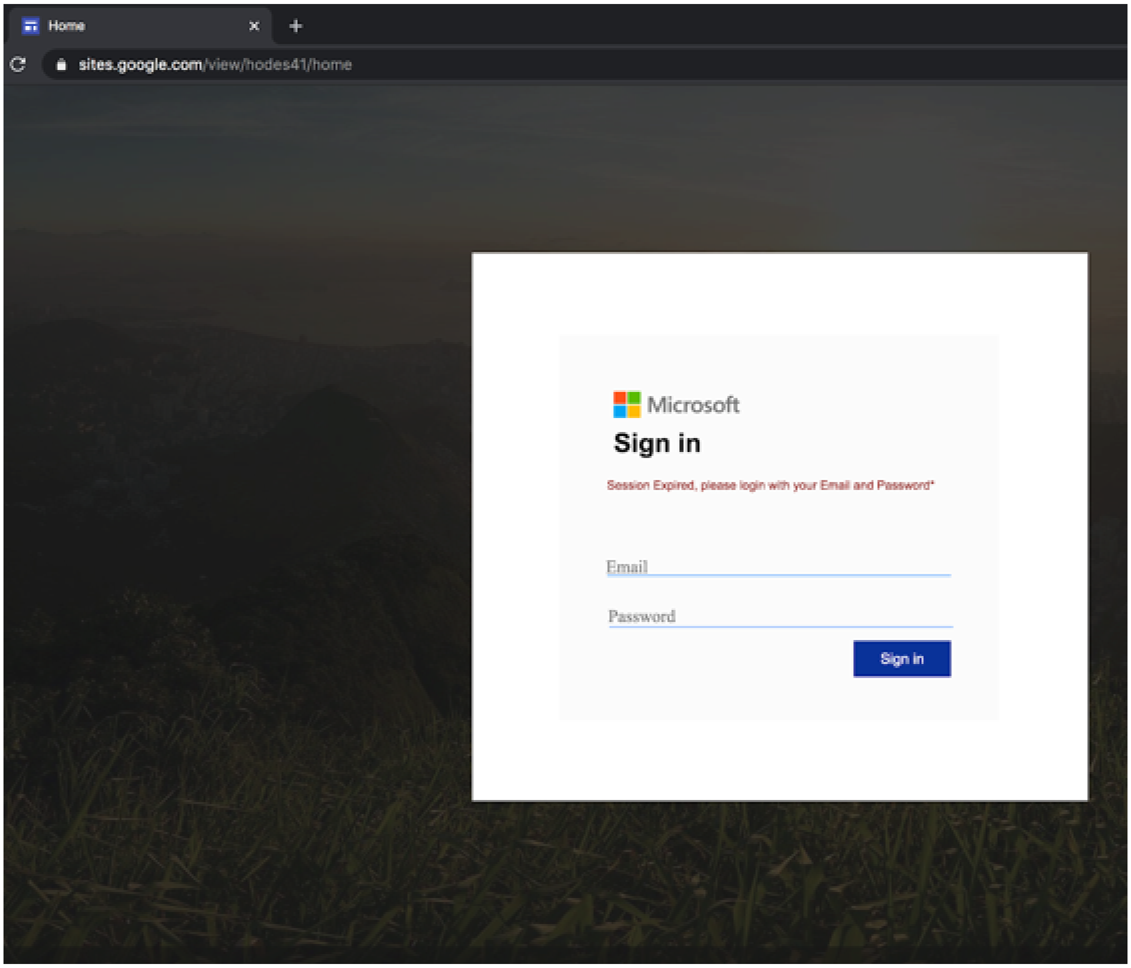
Attack summary

This email claimed to come from the company's IT team and asked readers to review a secure message their colleagues had shared over Microsoft Teams, a popular business collaboration solution. Clicking the link took the targets to a page resembling Microsoft Teams, which further redirected to the credential phishing site resembling the Office 365 login portal.

Visit this link if you'd like to learn more about this credential phishing attack.

Google service used

The Office 365 login portal was hosted on **Google Sites**, a wiki and web page creation tool that lowers the skill bar needed to create websites. The malice of the page's intent was hidden behind the legitimacy of the page's domain. This page would pass most eye tests during busy mornings (which is when the email was sent out), with people happily assuming it to be a legitimate Microsoft page.



Sign in

Session Expired, please login with your Email and Password*

Fig: Phishing page for the Microsoft Teams attack was hosted on Google Sites

Other techniques used

- Impersonation: IT team + Microsoft Teams
- Social engineering: Request to view ‘secure’ messages sent over Microsoft Teams

Guidance and Recommendations

1. Follow 2FA and password management best practices

Since all workplace accounts are so closely interlinked, losing access to your Google account can prove to be very dangerous as cybercriminals send emails in your name to your customers, partners, and loved ones. If you haven’t already, follow these hygiene best practices:

- Deploy two-factor authentication (2FA) on all possible business and personal accounts.
- Use a password manager to store your various account passwords.
- Don’t repeat passwords across accounts or use generic passwords such as your birth date, ‘password123’, ‘YourName123’ etc.

2. Subject sensitive emails to rigorous eye tests

Whenever possible, engage with emails related to money and data in a rational manner. Subject the email to an eye test that includes inspecting the sender name, sender email address, language within the email, and any logical inconsistencies within the email (*e.g. why is this childless widow willing to send me millions of dollars?*).

3. Create your own lines of authentication

You should try to replicate 2FA, even if in a loose sense, for any email that makes unusual requests related to money or data. For example, did your HR rep just email you some payroll details with a Google Doc requesting more information urgently? Call or text the HR rep and confirm that they sent the email. Even if your colleagues are very busy, they will understand and appreciate your caution.

4. Augment native email threat detection with additional controls

To augment existing email security capabilities (e.g. Exchange Online Protection for Office 365 or the Advanced Protection Program for G Suite), organizations should invest in technologies that take a materially different approach to threat detection. Rather than searching through static lists and blocking known bad domains, these technologies should learn from custom organizational data and be able to stop socially engineered threats that contain zero-day payloads like Google Forms, Docs, or pages built on Google Sites.

For more email security threat research, news, and industry guidance, sign up for email updates from Armorblox below. We promise to only email you useful information. We also promise not to include any Google Docs or Forms in these emails that ask for your personal information, although that should go without saying :-)

Join Armorblox Mailing List