GLOBAL PHISH REPORT

2019

AVANAN

EXECUTIVE SUMMARY

One in every 99 emails is a phishing attack, using malicious links and attachments as the main vector. Of the phishing attacks we analyzed, 25% bypassed Office 365 security, a number that is likely to increase as hackers design new obfuscation methods that take advantage of zero-day vulnerabilities on the platform.

CONTENTS

INTRO

***Phishing** occurs when an attacker sends a communication — usually an email — to an individual attempting to influence them to open an infected file or click on a malicious link to a page that will request credentials or drop malware. Once the victim clicks, the criminal can upload malware and engage in other insidious acts that will enable prolonged access to the system. (2018 Verizon Data Breach Investigation Report)*

Over the past decade, phishing attacks have become the most widespread email threat to organizations around the globe. As security solutions designed to block these attacks have grown more advanced, the sophistication of these attacks have kept pace, evolving to evade detection.

Cloud based email, with all of its benefits, has ushered in a new era of phishing attacks. The nature of the cloud provides even more vectors of which hackers take advantage, and even broader access to critical data when a phishing attack is successful.

ABOUT THIS REPORT

Avanan has unique insight into the current phishing landscape due to our cloud-native architecture. Our software connects via API inside of the cloud, creating key advantages over conventional solutions to email security, which sit outside (such as email gateways). For this reason, it can detect and analyze phishing attacks that have evaded Office 365 and Gmail security. Scanning after the default security but before the inbox, the platform catches phishing emails that bypass all other existing security layers.

As our research team consistently realized that this approach offered new insights into how attacks make it to the inbox, we felt compelled to combine the data and make the following report available.

THE RESEARCH

EMAILS ANALYZED

55.5 Million

INDUSTRIES

- Finance
- Construction
- Retail
- Healthcare
- Consulting
- Education
- Manufacturing
- Government
- Technology

COMPANY SIZE

20 users → 100,000 users

PLATFORMS

Office 365

G Suite

OVERVIEW

For most organizations, phishing is the number one email security threat, outranking both malware and ransomware. We analyzed over 55 million emails to provide a clear picture of the threat landscape.

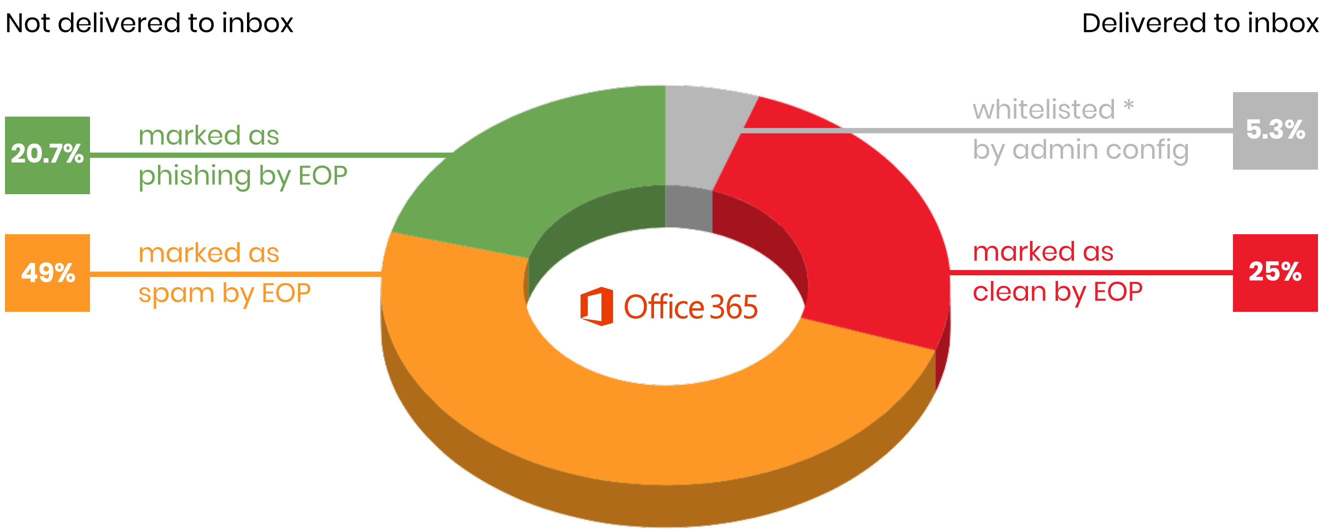
	EMAILS ANALYZED	PHISHING EMAILS	PERCENTAGE PHISHING
Office 365	52,379,886	546,247	1.04%
G Suite	3,120,114	15,700	0.5%
TOTAL	55,500,000	561,947	1.01%

One in every 99 emails is a phishing attack.

OFFICE 365 DEEP DIVE

In our analysis of over 52 million emails sent to Office 365, we scanned every email after the default security, allowing us to see not only the phishing attacks that were caught, but also those that were missed. This gave us deep data on every phishing attack caught or missed, and how they were classified.

How phishing emails were treated by Office 365 Exchange Online Protection (EOP)

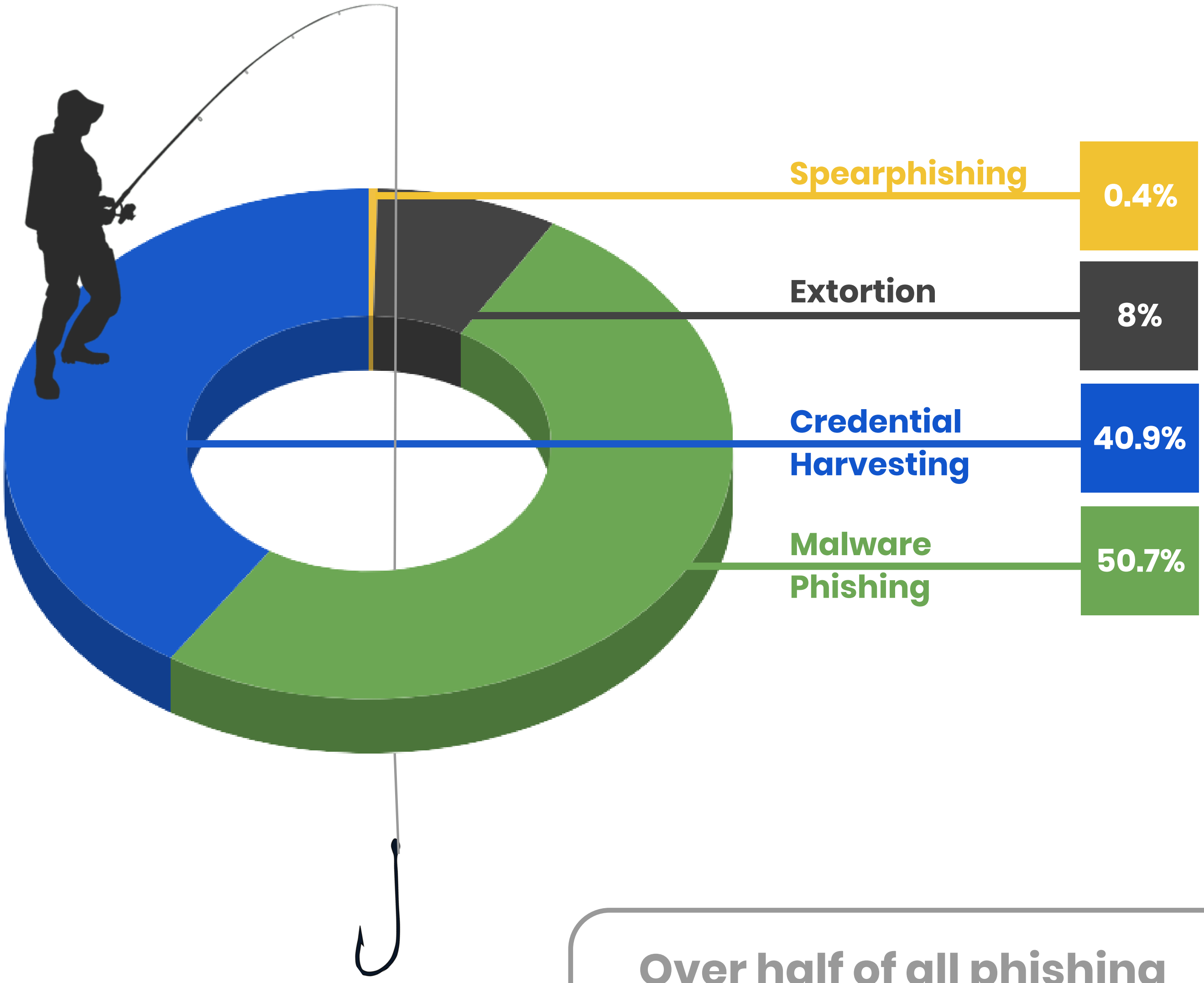


30.3% of phishing emails sent to organizations using Office 365 EOP were delivered to the inbox.

** These are phishing emails that are not blocked due to admin configurations set up by the organization that inadvertently whitelist emails that would otherwise get blocked.*

PHISHING VECTORS

What type of phishing attack is most common? We looked at 561,947 phishing attacks and broke them down into four vectors, each illustrating a different approach taken by the bad actor.



Over half of all phishing attacks contain malware.

LEARN THE PHISHING VECTORS

SPEARPHISHING (0.4% of phishing attacks)

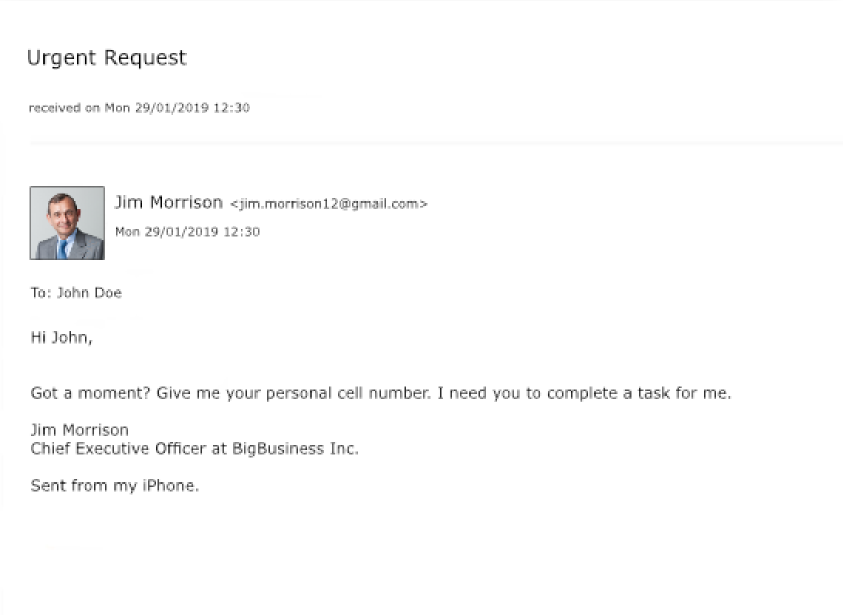
Although spearphishing is far less common than the other three vectors, it often has the largest impact. Spearphishing attacks target high level employees who have access to either company finances or other sensitive information. Their goal is to establish trust and urgency to convince the recipient to comply with the ask. These phishing attacks can also be the most difficult to detect, given the lack of attachments or links that can be flagged by anti-phishing tools. They rely on social engineering, rather than technical bypass methods, to deceive targets into surrendering a wealth of information.

COMMON TRAITS OF SPEARPHISHING EMAILS

Impersonates or sent to a senior employee (C-level/VP/HR/Accounting)

Doesn't contain a link or attachment

Sense of urgency to complete a manual task.



Urgent Request

received on Mon 29/01/2019 12:30

Jim Morrison <jim.morrison12@gmail.com>
Mon 29/01/2019 12:30

To: John Doe

Hi John,

Got a moment? Give me your personal cell number. I need you to complete a task for me.

Jim Morrison
Chief Executive Officer at BigBusiness Inc.

Sent from my iPhone.

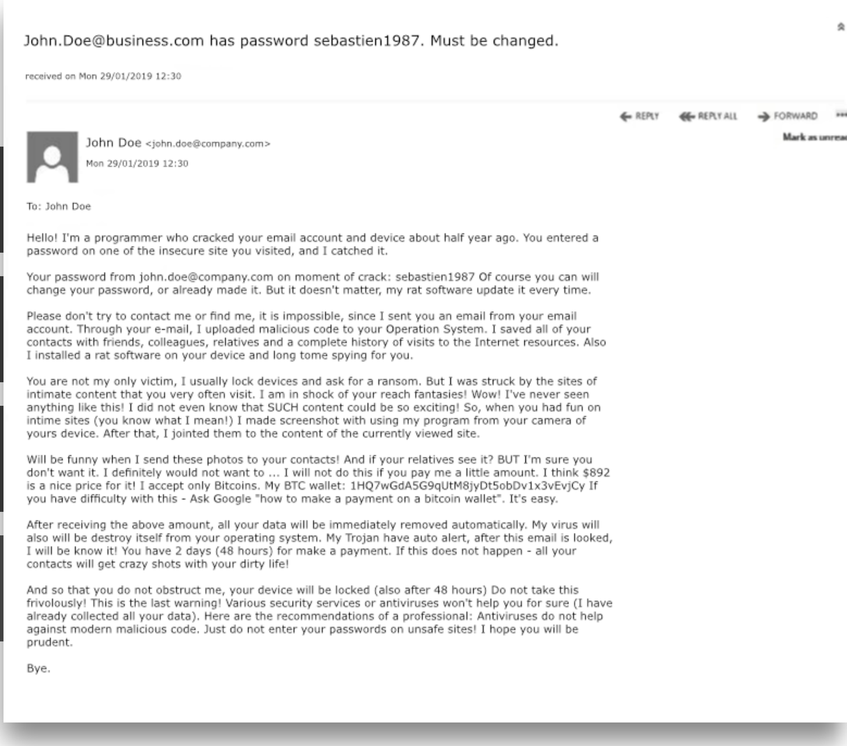
LEARN THE PHISHING VECTORS

EXTORTION (8% of phishing attacks)

The digital form of blackmail, extortion emails are almost always are after money. The sender of the phishing email will claim to have compromising information about the recipient. But unlike spearphishing, these threatening emails are usually sent en-masse, meaning that the content of the message is usually vague. In order to lend authority to their claim, the attacker typically lists the victim's current or past password that was obtained from a data leak and sold on the dark web.

COMMON TRAITS OF EXTORTION PHISHING EMAILS

- Cryptocurrency wallet address
- Threats to blackmail the recipient
- Contains recipient's password (obtained from database leak)
- Impersonates recipient



John.Doe@business.com has password sebastien1987. Must be changed.

received on Mon 29/01/2019 12:30

John Doe <john.doe@company.com>
Mon 29/01/2019 12:30

To: John Doe

Hello! I'm a programmer who cracked your email account and device about half year ago. You entered a password on one of the insecure site you visited, and I catched it.

Your password from john.doe@company.com on moment of crack: sebastien1987 Of course you can will change your password, or already made it. But it doesn't matter, my rat software update it every time.

Please don't try to contact me or find me, it is impossible, since I sent you an email from your email account. Through your e-mail, I uploaded malicious code to your Operation System. I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources. Also I installed a rat software on your device and long tome spying for you.

You are not my only victim, I usually lock devices and ask for a ransom. But I was struck by the sites of intimate content that you very often visit. I am in shock of your reach fantasies! Wow! I've never seen anything like this! I did not even know that SUCH content could be so exciting! So, when you had fun on intime sites (you know what I mean!) I made screenshot with using my program from your camera of yours device. After that, I jointed them to the content of the currently viewed site.

Will be funny when I send these photos to your contacts! And if your relatives see it? BUT I'm sure you don't want it. I definitely would not want to ... I will not do this if you pay me a little amount. I think $892 is a nice price for it! I accept only Bitcoins. My BTC wallet: 1HQ7wGdA5G9qUtM8jyDt5obDv1x3vEvjCy If you have difficulty with this - Ask Google "how to make a payment on a bitcoin wallet". It's easy.

After receiving the above amount, all your data will be immediately removed automatically. My virus will also will be destroy itself from your operating system. My Trojan have auto alert, after this email is looked, I will be know it! You have 2 days (48 hours) for make a payment. If this does not happen - all your contacts will get crazy shots with your dirty life!

And so that you do not obstruct me, your device will be locked (also after 48 hours) Do not take this frivolously! This is the last warning! Various security services or antiviruses won't help you for sure (I have already collected all your data). Here are the recommendations of a professional: Antiviruses do not help against modern malicious code. Just do not enter your passwords on unsafe sites! I hope you will be prudent.

Bye.

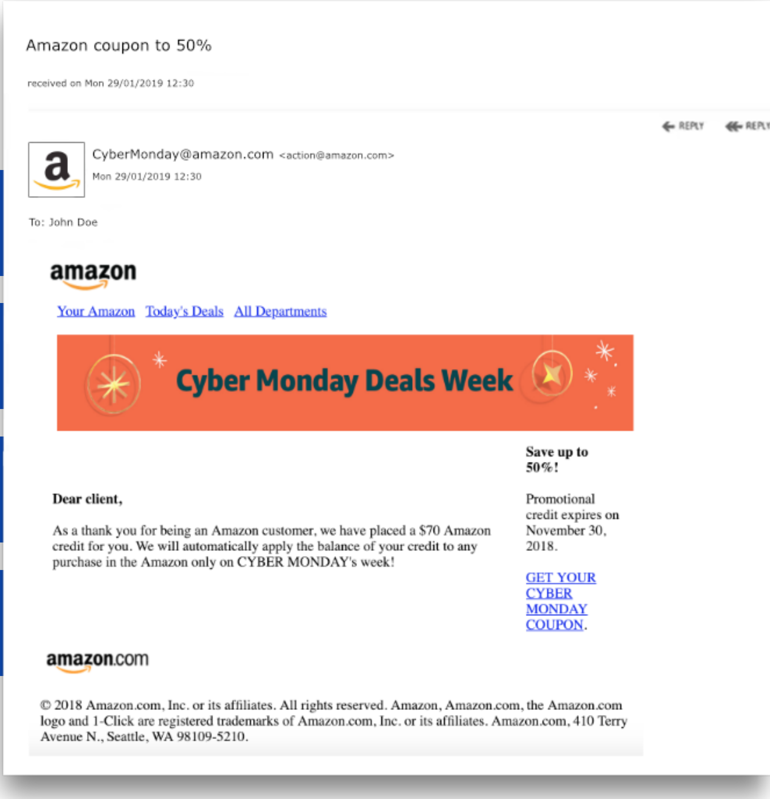
LEARN THE PHISHING VECTORS

CREDENTIAL HARVESTING (40.9% of phishing attacks)

Credential harvesting attacks lure the victim into divulging personal information that grants access to online accounts or personal finances. Credentials range from email passwords to credit card numbers. Usually, credential harvesting impersonate trusted brands like Amazon to trick the recipient into entering their username and password in a spoofed login page. With these credentials, hackers take over the victim's account or sell the information on the black market in bulk.

COMMON TRAITS OF CREDENTIAL HARVESTING PHISHING EMAILS

- Trusted brand logo
- Link in the email body or an attachment (.docx or PDF)
- Action items that create a sense of urgency to click on the link
- Link in email leads to a login page.



Amazon coupon to 50%

received on Mon 29/01/2019 12:30

CyberMonday@amazon.com <action@amazon.com>
Mon 29/01/2019 12:30

To: John Doe

Save up to 50%!

Dear client,

As a thank you for being an Amazon customer, we have placed a $70 Amazon credit for you. We will automatically apply the balance of your credit to any purchase in the Amazon only on CYBER MONDAY's week!

Promotional credit expires on November 30, 2018.

GET YOUR CYBER MONDAY COUPON.

© 2018 Amazon.com, Inc. or its affiliates. All rights reserved. Amazon, Amazon.com, the Amazon.com logo and 1-Click are registered trademarks of Amazon.com, Inc. or its affiliates. Amazon.com, 410 Terry Avenue N., Seattle, WA 98109-5210.

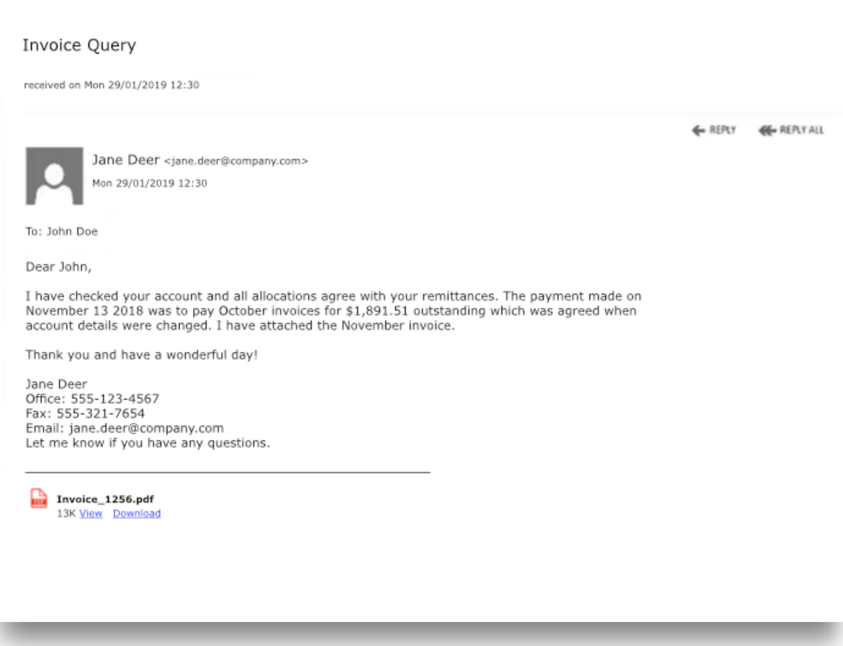
LEARN THE PHISHING VECTORS

MALWARE PHISHING (50.7% of phishing attacks)

This vector uses a phishing email to install malware on the recipient's device. These attacks often bypass traditional malware scans since the email itself is not malicious; instead, the email contains a link that triggers a download of malicious content (known as a *trojan*) or has a malicious attachment.

COMMON TRAITS OF MALWARE PHISHING EMAILS

- Has an attachment
- Contains a link that triggers a file download



Invoice Query

received on Mon 29/01/2019 12:30

Jane Deer <jane.deer@company.com>
Mon 29/01/2019 12:30

To: John Doe

Dear John,

I have checked your account and all allocations agree with your remittances. The payment made on November 13 2018 was to pay October invoices for $1,891.51 outstanding which was agreed when account details were changed. I have attached the November invoice.

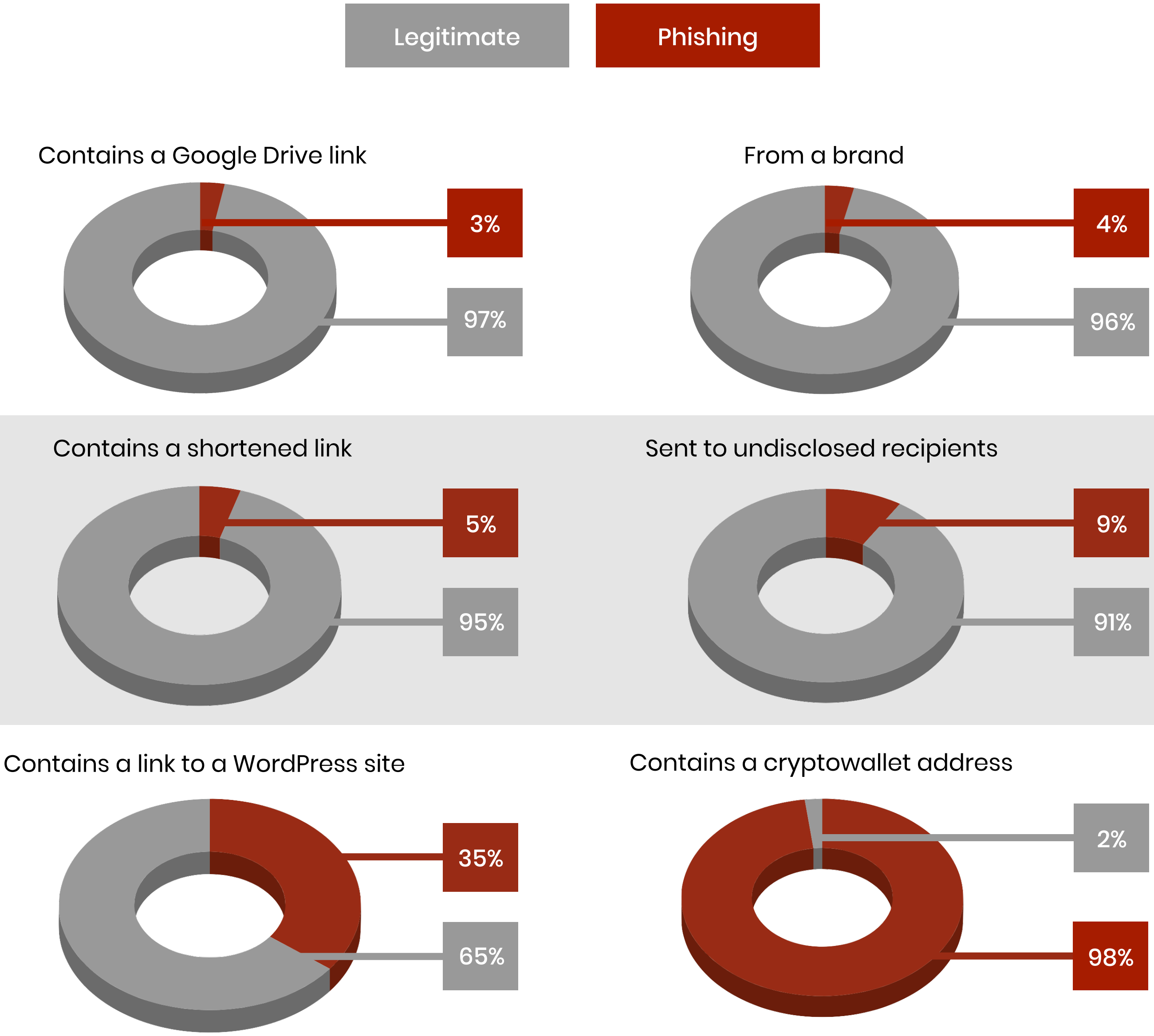
Thank you and have a wonderful day!

Jane Deer
Office: 555-123-4567
Fax: 555-321-7654
Email: jane.deer@company.com
Let me know if you have any questions.

Invoice_1256.pdf
13K

PHISHING INDICATORS

The signs of a phishing attack can be subtle and inconsistent, making them hard to detect. As you can see below, there are plenty of reasons why a legitimate email may possess traits that are common in phishing emails. This is why it is vital you use an anti-phishing solution, which can analyze these subtle traits with automated precision.



Contains a Google Drive link

From a brand

Contains a shortened link

Sent to undisclosed recipients

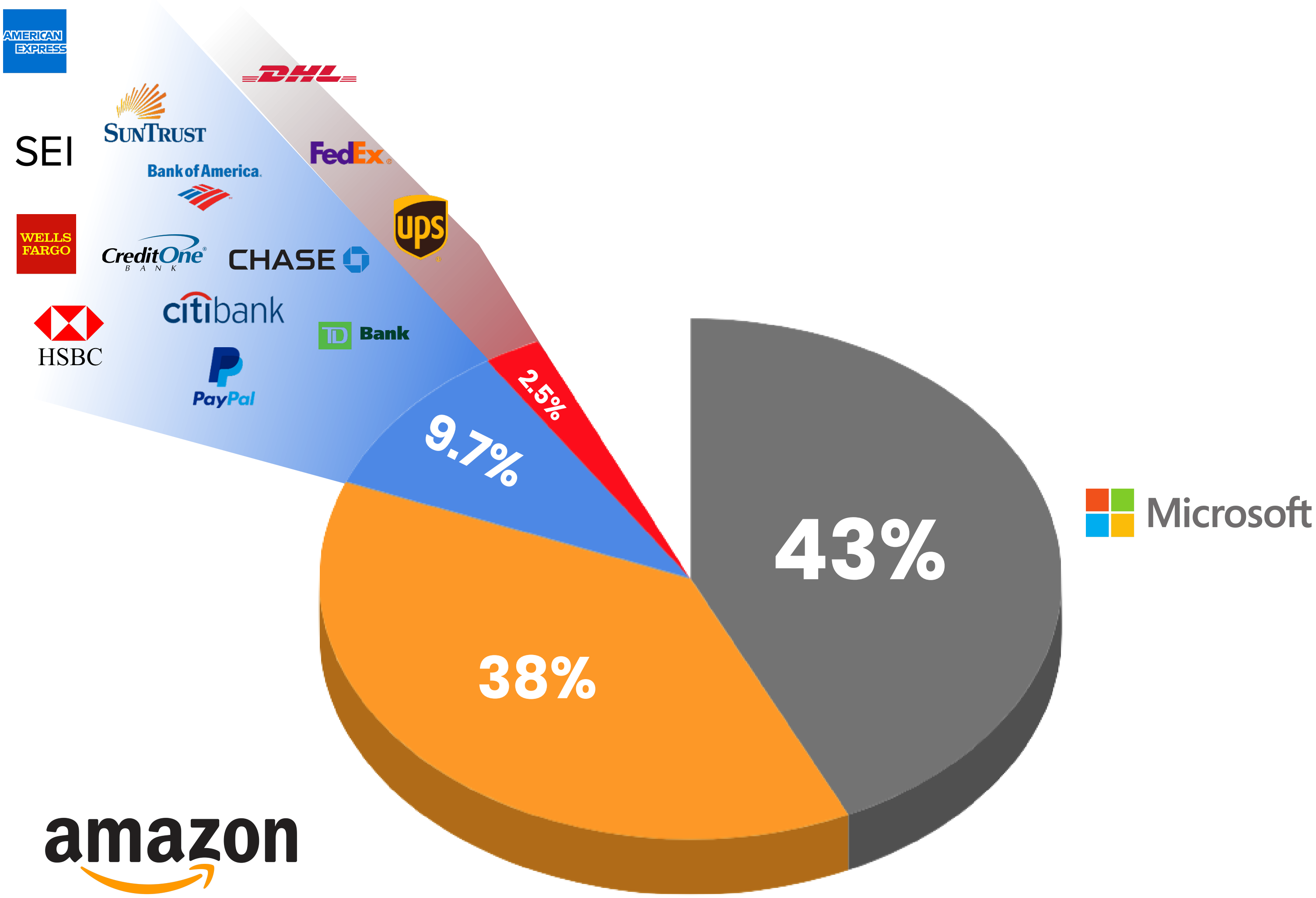
Contains a link to a WordPress site

Contains a cryptowallet address

Over 1 in 3 emails containing a link to a WordPress site is phishing.

BRAND IMPERSONATION

We discovered an alarming statistic: out of every 25 branded emails, it is likely that at least one is a phishing email. These emails impersonate trusted brands to get you to click a malicious link or surrender personal information on a spoofed landing page.



Microsoft is by far the most impersonated brand throughout the year. During the holiday season, however, Amazon surpasses Microsoft.

OBFUSCATION

Obfuscation methods are the most advanced phishing attacks, leveraging specific vulnerabilities in Office 365 security layers. Hackers obfuscate the URL, making it unrecognizable to Office 365 security, which fails to blacklist the malicious content. With this strategy, hackers can use URLs that are even known to be malicious, because Microsoft won't recognize the format of the URL. And because EOP and Advanced Threat Protection (ATP) use the same first layer of email body parsing (though ATP has a unique attachment parser), all email body obfuscation methods we tested effectively bypassed both security layers of Office 365.

URL OBFUSCATION EXAMPLE

MALICIOUS LINK

```
<a href="https://malware.com">Link</a>
```

MALICIOUS LINK OBFUSCATED WITH ZERO-WIDTH SPACES

```
<a href="https://malw&#8204are.&#8204com">Link</a>
```

Obfuscation methods make up a very small percentage of attacks — likely because hackers intentionally limit its usage in order not to expose the vulnerability. Typically, we observe these attacks use malicious login pages and links to malicious attachments that detonate malware.

Why obfuscation is effective

These methods are designed to not only fool the recipient but also systematically bypass email security scans.

Obfuscation methods have been used in some of the most notable attacks in the past year. During that time, our security team has uncovered several high-profile obfuscation methods. Most notably, the BaseStriker attack used <base> tags in the html of the email to split links into multiple parts, making them unrecognizable to Microsoft SafeLinks. Most recently, the NoRelationship attack bypassed Proofpoint and EOP by removing malicious links from the relationship file to confuse link parsers, which scan Office documents like PowerPoint, Word, and Excel.

OBFUSCATION TYPES

At their core, obfuscation attacks rely on the email being rendered to the end-user differently than how it appears to the machine-based security layer. The generalized groups of obfuscation include:

- **Rare / unused, yet legitimate email formats** that are not properly parsed by the security layer, but are presented by the email client to the end user.
- **Malformed email bodies and attachments** that confuse the security layer parsing the html, but are still presented by the email client as if the message and its contents were legitimate and safe.
- **Hidden characters in the email body and links** fool the machine-based security filter to analyze content differently than what will be presented to the end-user.

Email Body

Hackers edit the html of the email body to confuse natural language processing or hide URLs from detection technology.

Attachment

Hiding malicious links within an otherwise benign attachment to take advantage of the disconnect between email link scanning and attachment scanning technology.

CONCLUSION

Phishing attacks are becoming increasingly sophisticated and difficult for humans and machines alike to detect. Employees are bombarded with spearphishing, extortion, credential harvesting, and malware attacks. Yet Office 365 and Gmail cannot reliably block emails containing malicious language, links, or attachments.

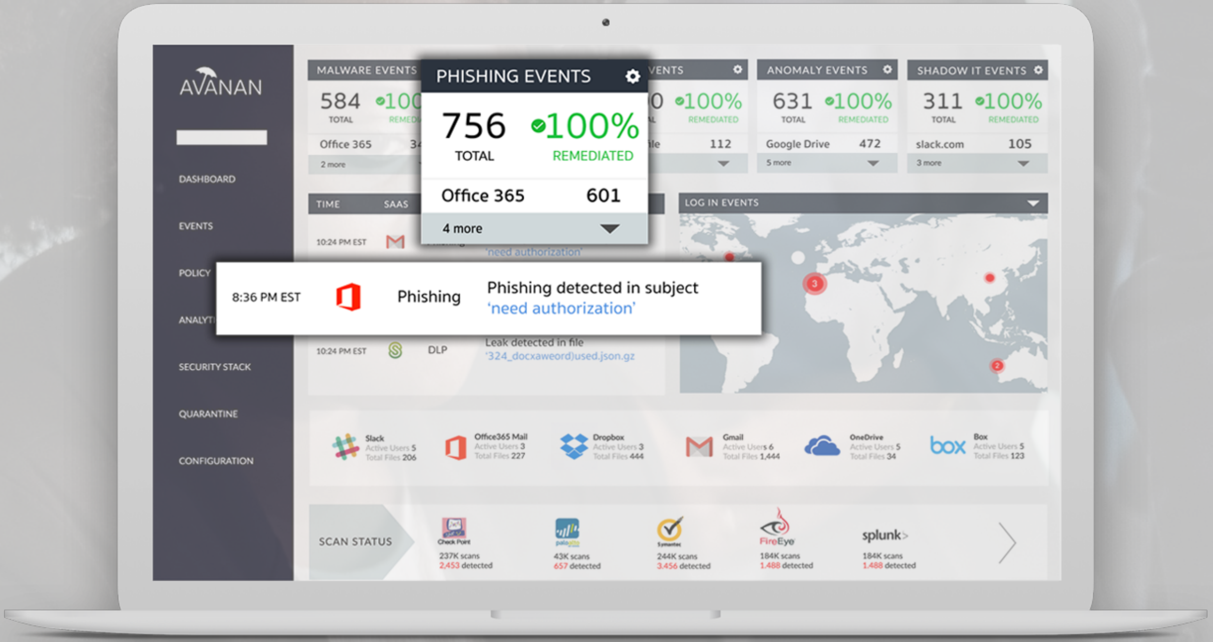
Avanan's analysis of 55.5 million emails in this report exemplifies how hackers succeed at deceiving organizations of any industry and size. At the same time, it attests to Avanan's rich insights into the phishing landscape, and how Avanan can identify the evolving methods hackers use to evade detection.

As phishing attacks continue to wreak havoc across the globe, Avanan is uniquely positioned to protect companies from the threats that Office 365 and Google miss. Unlike other email security solutions, Avanan sits inside the email provider's cloud, stopping threats after the email provider has scanned but before they reach the inbox.

Avanan is the final line of defense for global companies looking to secure their email from the unrelenting efforts of hackers.

ABOUT AVANAN

Avanan augments the security of cloud-based email, messaging, and file-sharing across enterprise platforms including Office 365™, G-Suite™, and Slack™. It deploys in minutes via API to block phishing, malware, data leakage, account takeover, and shadow IT. The cloud-native platform is a core component of leading security vendor solutions, and deploys best-of-breed technologies from trusted partners including Check Point, Lastline, and FireEye.


AVANAN
DASHBOARD
EVENTS
POLICY
ANALYTI
SECURITY STACK
QUARANTINE
CONFIGURATION
MALWARE EVENTS
584
TOTAL
Office 365
2 more
PHISHING EVENTS
756
TOTAL
100%
REMEDIATED
Office 365 601
4 more
100%
REMEDIATED
112
ANOMALY EVENTS
631
TOTAL
100%
REMEDIATED
Google Drive 472
5 more
SHADOW IT EVENTS
311
TOTAL
100%
REMEDIATED
slack.com 105
3 more
TIME
SAAS
LOG IN EVENTS
Slack Active Users 5 Total Files 206
Office365 Mail Active Users 3 Total Files 227
Dropbox Active Users 3 Total Files 444
Gmail Active Users 6 Total Files 1,444
OneDrive Active Users 5 Total Files 34
box Box Active Users 5 Total Files 123
SCAN STATUS
Check Point 237K scans 2,453 detected
paloalto 43K scans 657 detected
Symantec 244K scans 3,456 detected
FireEye 184K scans 1,488 detected
splunk 184K scans 1,488 detected

10:24 PM EST 'need authorization'

8:36 PM EST Phishing Phishing detected in subject 'need authorization'

10:24 PM EST DLP Leak detected in file '324_docxaweord)used.json.gz

Avanan is a cloud-native security platform for communications and collaboration.

Learn more at avanan.com

AVANAN