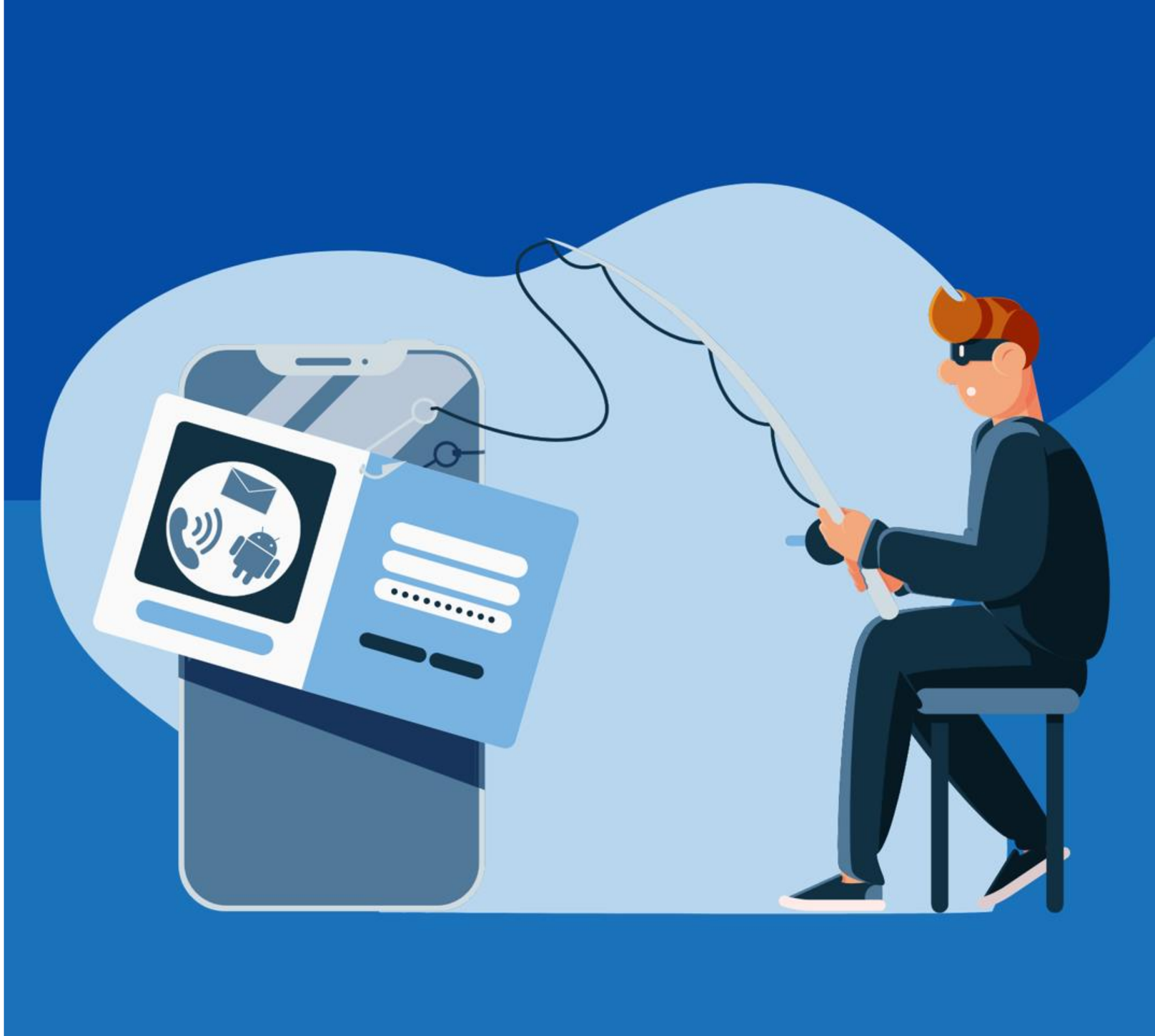
The New Generation of Phishing: Beyond the Mailbox

Rachel Kang

Manager, Digital Forensics and Incident Response

BSidesPGH 2024

July 12th, 2024



About Me

Rachel Kang

Manager – DFIR

Chicago, IL

~5 years in Digital Forensics + Incident Response (DFIR) industry

Presented at WiCyS 2024

Certifications: GCFE, GCFA, GCFR, GCIA, AZ-900

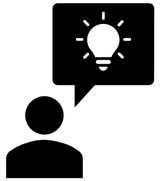
Interests: Microsoft/Azure, business email compromises, cloud forensics

OOO Interests: Rock climbing, Legos, concerts, looking at pictures of animals

AON

Agenda

What to expect from today's talk



Introduction

A Brief History

Cyber Threat Landscape

Should you BYOD?

Mobile-based phishing attacks

Smishing, Vishing, Quishing, SIM swap

Case Studies

Hiding Behind Brands

Brand Impersonation

Consent Phishing

Case Studies

What's Next?

AI in Phishing

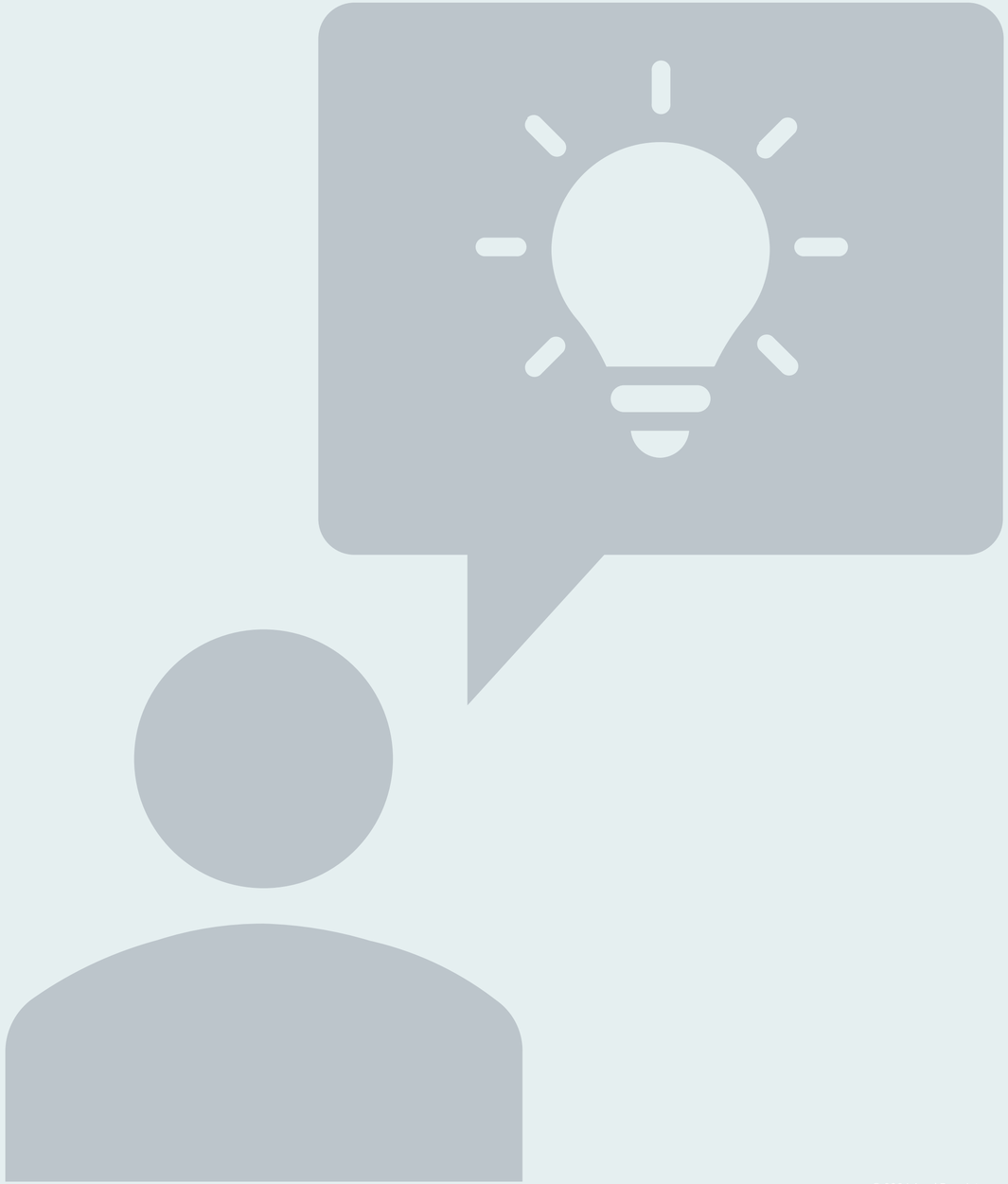
Phishing-As-A-Service

1

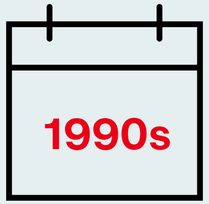
Introduction

A Brief History

Cyber Threat Landscape



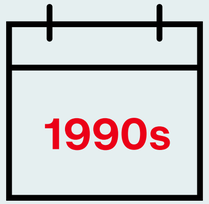
A Brief History



1. Advent of global communication

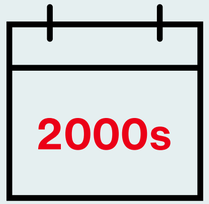
- Dial-up Internet
- Pagers, fax machines

A Brief History



1. Advent of global communication

- Dial-up Internet
- Pagers, fax machines



2. Burgeoning global communication

- AOL Mail, MySpace
- Smartphones
- Love Bug virus[1]

A Brief History

1990s

1. Advent of global communication

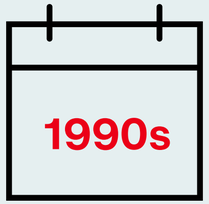
- Dial-up Internet
- Pagers, fax machines

2000s

2. Burgeoning global communication

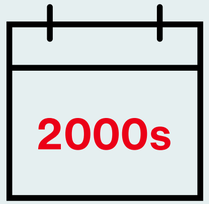
- AOL Mail, MySpace
- Smartphones
- Love Bug virus[1]

A Brief History



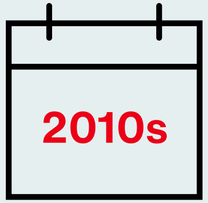
1. Advent of global communication

- Dial-up Internet
- Pagers, fax machines



2. Burgeoning global communication

- AOL Mail, MySpace
- Smartphones
- Love Bug virus[1]



3. Established global communication

- Gmail, Facebook
- iPads + tablets
- Yahoo! Mail[2], Equifax data breach[3]

A Brief History

1990s

1. Advent of global communication

- Dial-up Internet
- Pagers, fax machines

2000s

2. Burgeoning global communication

- AOL Mail, MySpace
- Smartphones
- Love Bug virus[1]

2010s

3. Established global communication

- Gmail, Facebook
- iPads + tablets
- Yahoo! Mail[2], Equifax data breach[3]

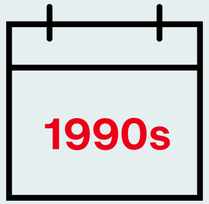
Gmail™ by Google

Equifax Data Breach Impacts 143 Million Americans

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

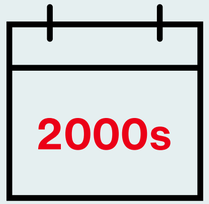
AON

A Brief History



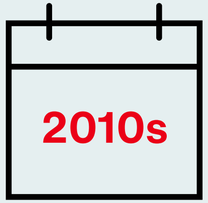
1. Advent of global communication

- Dial-up Internet
- Pagers, fax machines



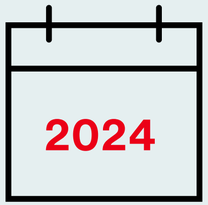
2. Burgeoning global communication

- AOL Mail, MySpace
- Smartphones
- Love Bug virus[1]



3. Established global communication

- Gmail, Facebook
- iPads + tablets
- Yahoo! Mail[2], Equifax data breach[3]



4. Advanced communication and technologies

- Google Workspace, M365, Meta Platforms
- Devices have become our “identity” in MFA (ex. “something the user has”)

AON

A Brief History

1990s

1. Advent of global communication

- Dial-up Internet
- Pagers, fax machines

2000s

2. Burgeoning global communication

- AOL Mail, MySpace
- Smartphones
- Love Bug virus[1]

2010s

3. Established global communication

- Gmail, Facebook
- iPads + tablets
- Yahoo! Mail[2], Equifax data breach[3]

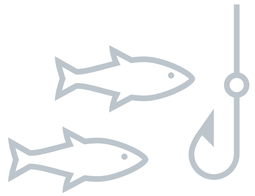
2024

4. Advanced communication and technologies

- Google Workspace, M365, Meta Platforms
- Devices have become our “identity” in MFA (ex. “something the user has”)

Current Phishing Threat Landscape

Evolution of Phishing Campaigns



In 2023, 71% of all security incidents involved a phishing link and/or phishing attack[4].

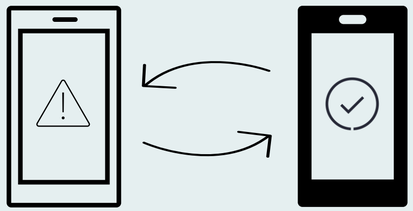
- Remains the **#1** tactic for threat actors across initial access-related incidents
- Relies on the **human factor** to facilitate attack → “social engineering”
- Email is by far the **most exploited** business application
- Novel phishing attacks targeting alternative mediums outside of email

Current Phishing Threat Landscape

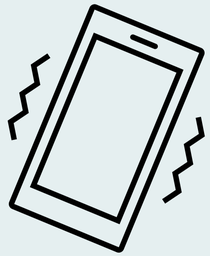
Evolution of Phishing Campaigns

In 2023, 71% of all security incidents involved a phishing link and/or phishing attack[4].

- Remains the **#1** tactic for threat actors across initial access-related incidents
- Relies on the **human factor** to facilitate attack → "social engineering"
- Email is by far the **most exploited** business application
- Novel phishing attacks targeting alternative mediums outside of email



SIM swapping



SMS text message phishing (Smishing)

Impersonating trusted services (ex. Microsoft, Amazon, Google)

AI in Phishing

How do we protect ourselves when phishing transcends to SMS, social media, and third-party territory?

2

Should you BYOD?

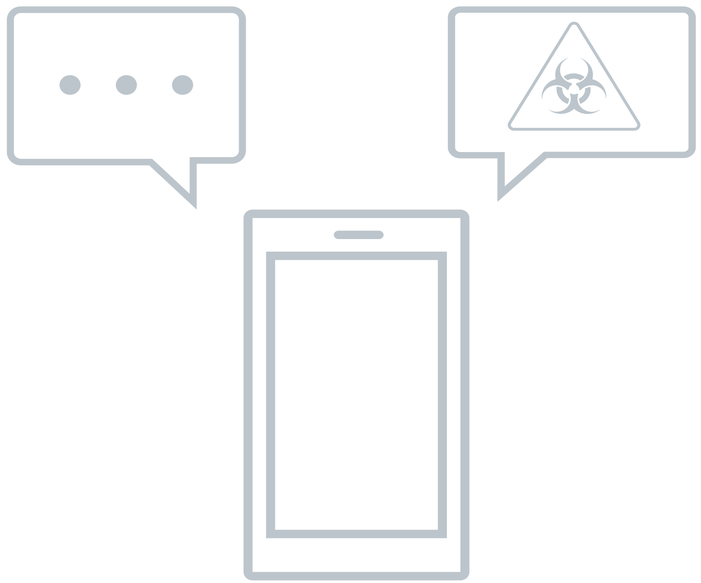
Mobile-based phishing attacks

Smishing, Vishing, Quishing, SIM swap

Case Studies

Mobile Phishing Attacks

Emerging “-ishing” Trends

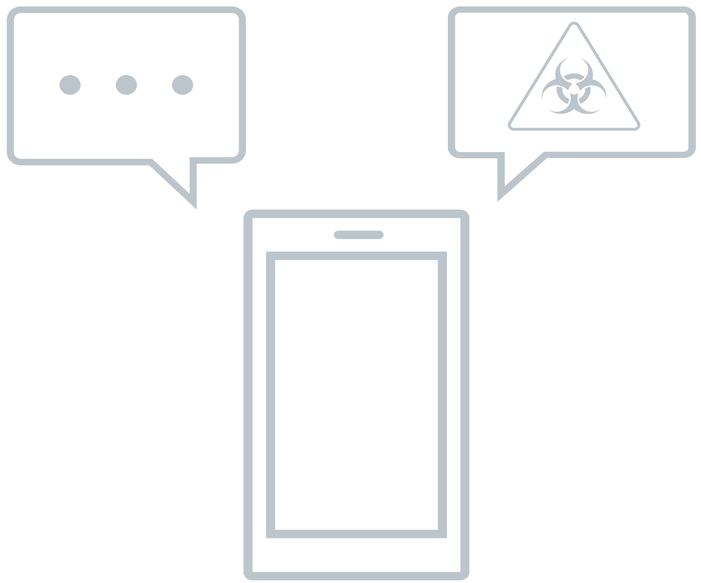


Check out “**Attacks that Smish, Phish, and Vish Their Way around MFA**[5]” on Aon’s Case Studies

-ishings

Mobile Phishing Attacks

Emerging “-ishing” Trends



Check out “**Attacks that Smish, Phish, and Vish Their Way around MFA**[5]” on Aon’s Case Studies

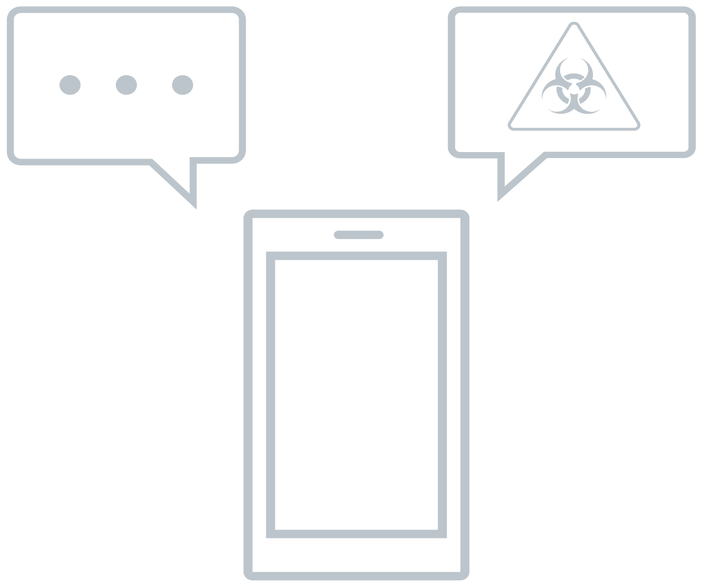
-ishings

Smishing (SMS Text Message Phishing)

- Any *messaging-based* social engineering attack
- Little to no security + auditing across messaging platforms
- Device fragmentation and mobile device management

Mobile Phishing Attacks

Emerging “-ishing” Trends



Check out “**Attacks that Smish, Phish, and Vish Their Way around MFA**[5]” on Aon’s Case Studies

-ishings

Smishing (SMS Text Message Phishing)

- Any *messaging-based* social engineering attack
- Little to no security + auditing across messaging platforms
- Device fragmentation and mobile device management

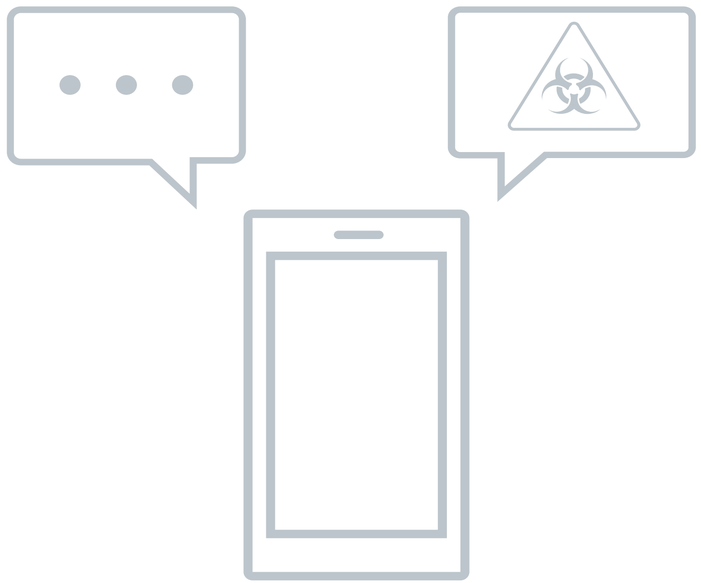
Vishing (Voice Phishing)

- Any *voice/phone-based* social engineering attack
- Spoof caller ID to trusted source
- Lack of digital footprint and logging

AON

Mobile Phishing Attacks

Emerging “-ishing” Trends



Check out “**Attacks that Smish, Phish, and Vish Their Way around MFA**[5]” on Aon’s Case Studies

-ishings

Smishing (SMS Text Message Phishing)

- Any *messaging-based* social engineering attack
- Little to no security + auditing across messaging platforms
- Device fragmentation and mobile device management

Vishing (Voice Phishing)

- Any *voice/phone-based* social engineering attack
- Spoof caller ID to trusted source
- Lack of digital footprint and logging

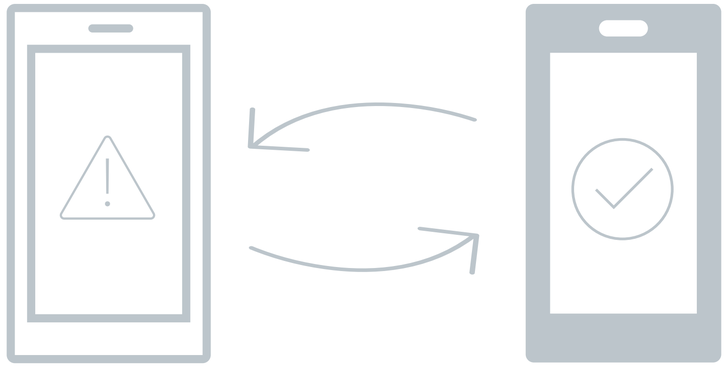
Quishing (QR Code Phishing)

- *QR code-based* social engineering attack
- Alternative to malicious links or email attachment
- Evades standard anti-phishing filters

AON

Mobile Phishing Attacks

SIM Swapping



Threat actor identifies and researches information on victim

Threat actor manipulates carrier for SIM Swap

Victim's phone loses cell network connectivity

Threat actor controls victim's phone number

- Social engineer mobile carriers to gain access into victims' mobile device and access accounts, virtual currency funds, among other personal data
- In 2021, FBI reported on adjusted losses of $68 million attributed to SIM swapping incidents [6]
- Inherently bypasses MFA and victim's credentials

Check out "**A SIMple Attack: A Look Into Recent SIM Swap Attack Trends**[7]" on Aon's Cyber Labs

AON

Case Study #1 – SSO Smishing

High Level Overview

Threat actor sends text messages containing a phishing link to employees at Company X. The link redirects to a fake, attacker-controlled website that mimics company X’s legitimate login page.

Case Study #1 – SSO Smishing

High Level Overview

Threat actor sends text messages containing a phishing link to employees at Company X. The link redirects to a fake, attacker-controlled website that mimics company X's legitimate login page.

Malicious website is configured to capture and forward victims' credentials to be entered onto Company X's legitimate login page, triggering a legitimate MFA prompt to the victim.

Case Study #1 – SSO Smishing

High Level Overview

Threat actor sends text messages containing a phishing link to employees at Company X. The link redirects to a fake, attacker-controlled website that mimics company X's legitimate login page.

Malicious website is configured to capture and forward victims' credentials to be entered onto Company X's legitimate login page, triggering a legitimate MFA prompt to the victim.

Malicious website also prompts victim to enter MFA one-time password ("OTP"), which the threat actor will then forward to the legitimate site, thereby gaining control of the victim's account.

AON

Case Study #1 – SSO Smishing

High Level Overview

Threat actor sends text messages containing a phishing link to employees at Company X. The link redirects to a fake, attacker-controlled website that mimics company X's legitimate login page.

Malicious website is configured to capture and forward victims' credentials to be entered onto Company X's legitimate login page, triggering a legitimate MFA prompt to the victim.

Malicious website also prompts victim to enter MFA one-time password ("OTP"), which the threat actor will then forward to the legitimate site, thereby gaining control of the victim's account.

Threat actor has full access to all applications integrated with the company's single sign-on ("SSO") portal, which frequently includes commercial applications like Salesforce, Workday, Slack, Jira, and Confluence, in addition to company-specific proprietary apps.

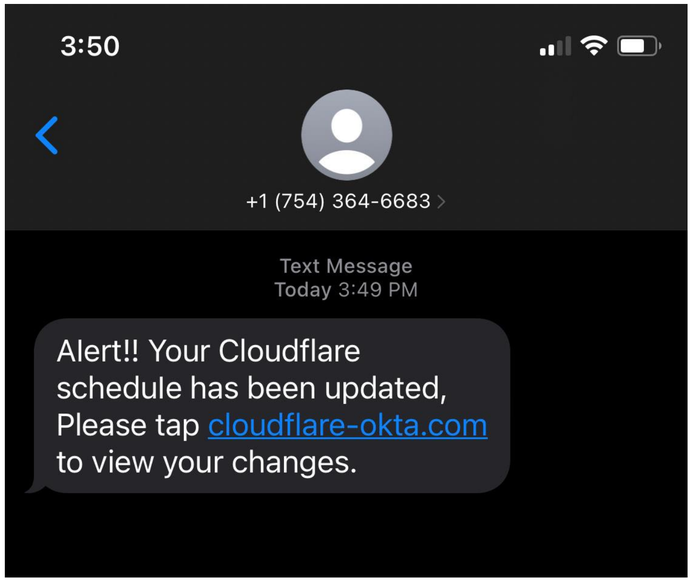
AON

Case Study #1 – SSO Smishing

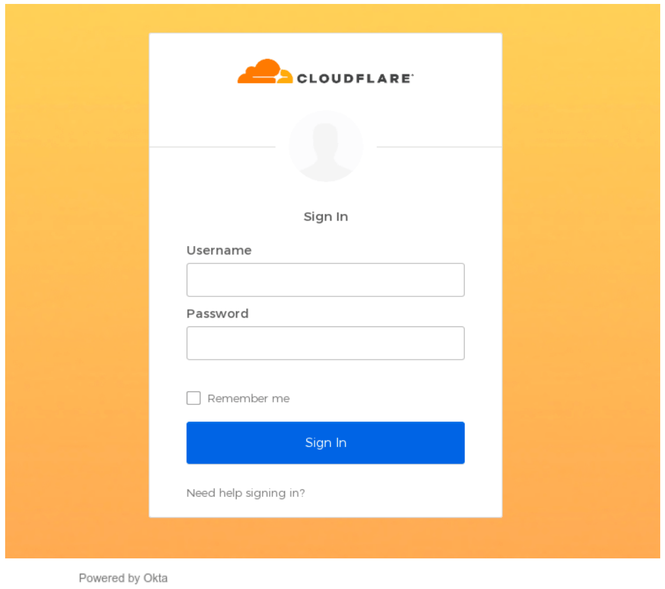
ScatterSwine Attack

In mid-2022, a major Identity and Access Management (IAM) provider was the target of a massive, persistent phishing campaign, affecting over 130 U.S-based IT, software, and cloud service companies

- Targeted customers and employees with smishing attacks using links like “company-sso.com” or “company-2fa.com”
- Targeted mailing lists + customer-facing systems to conduct supply-chain attacks [8], further broadening the reaches of the campaign



Smishing link received by employees at CloudFlare[9]

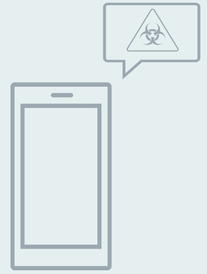


Fraudulent login page, mimicking CloudFlare’s legitimate login prompt[9]

Case Study #1 – SSO Smishing

ScatterSwine Impact

Organically evades multi-factor authentication, as well as and other security protection tools



Smishing links sent to employee's personal phones where the company lacks access to

Threat actor has wholesale access to account and obtains information w/o using malware, scripts, or other actions that would trigger AV or EDR alerts

Access to services under legitimate accounts that evades analytics tools tracking anomalous user behavior

Protections For BYOD Usage

82% of organizations have some form of a BYOD policy in place.[11]

Combat attacks by strengthening BYOD policies and promoting “smart” mobile device usage via:

Technical Controls

- Mobile Device Management (MDM) and device compliance monitoring to enforce security policies across BYOD devices
- Stronger authentication protocols using FIDO2 or biometric authentication

Employee Training

- Routine security awareness training and phishing simulations
- Personal security hygiene across devices (ex. Password resets, software updates)

Policy Enhancement

- Comprehensive and clear BYOD policies, including compliance regulations and employee responsibilities
- Role-based access control (RBAC) and usage of conditional access policies
- Established procedures and response plans for BYOD security incidents

AON

3

Hiding Behind the Big Brands

Brand Impersonation

Consent Phishing

Case Studies

Phishing across Third-party Services

Weaponizing Trusted Services

Microsoft

Google

amazon

Microsoft's Azure

Microsoft 365

Google Cloud Platform

Google Workspace

aws

Amazon Web Services

Dropbox

docusign

box

Exploiting the Trust of Brands

- Relies on the **established trust** between the organization and their vendors + service providers
- Increased risk factor for services offering **productivity suites**
- Increased risk factor for services that inherently involve users **clicking on external links**
- Deceive victims by **disguising attack** as a routine Google notification or a shared OneDrive document, as opposed to creating emotional lures

AON

Phishing across Third-party Services

Weaponizing Trusted Services

Microsoft

Google

amazon

Microsoft's Azure

Microsoft 365

Google Cloud Platform

Google Workspace

aws

Amazon Web Services

Dropbox

docusign

box

Exploiting the Trust of Brands

- Relies on the **established trust** between the organization and their vendors + service providers
- Increased risk factor for services offering **productivity suites**
- Increased risk factor for services that inherently involve users **clicking on external links**
- Deceive victims by **disguising attack** as a routine Google notification or a shared OneDrive document, as opposed to creating emotional lures

AON

Phishing across Third-party Services

Weaponizing Trusted Services

Microsoft

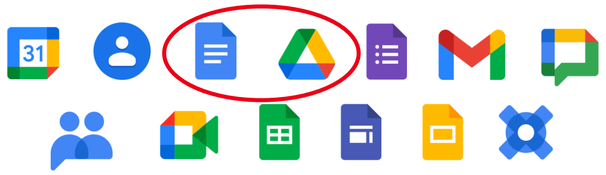
Google

amazon

Microsoft's Azure

Microsoft 365

Google Cloud Platform



Google Workspace

aws

Amazon Web Services

Dropbox

docusign

box

Exploiting the Trust of Brands

- Relies on the **established trust** between the organization and their vendors + service providers
- Increased risk factor for services offering **productivity suites**
- Increased risk factor for services that inherently involve users **clicking on external links**
- Deceive victims by **disguising attack** as a routine Google notification or a shared OneDrive document, as opposed to creating emotional lures

AON

Phishing across Third-party Services

Weaponizing Trusted Services

Microsoft

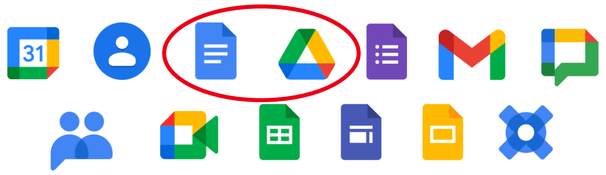
Google

amazon

Microsoft's Azure

Microsoft 365

Google Cloud Platform



Google Workspace

aws

Amazon Web Services

Dropbox

docusign

box

Exploiting the Trust of Brands

- Relies on the **established trust** between the organization and their vendors + service providers
- Increased risk factor for services offering **productivity suites**
- Increased risk factor for services that inherently involve users **clicking on external links**
- Deceive victims by **disguising attack** as a routine Google notification or a shared OneDrive document, as opposed to creating emotional lures

AON

Case Study #2 – Brand Impersonation

High Level Overview

Using perceived legitimacy of big brands, a threat actor creates and sends phishing link pointing to a threat actor-controlled, Microsoft SharePoint document to a victim.

Case Study #2 – Brand Impersonation

High Level Overview

Using perceived legitimacy of big brands, a threat actor creates and sends phishing link pointing to a threat actor-controlled, Microsoft SharePoint document to a victim.

The victim clicks on the phishing link and is redirected to a fraudulent SharePoint page that requests the victim's credentials.

The victim clicks on a legitimate SharePoint link** and is redirected to a document containing instructions to enter credentials onto a fraudulent login page.

**bypasses spam filters

AON

Case Study #2 – Brand Impersonation

High Level Overview

Using perceived legitimacy of big brands, a threat actor creates and sends phishing link pointing to a threat actor-controlled, Microsoft SharePoint document to a victim.

The victim clicks on the phishing link and is redirected to a fraudulent SharePoint page that requests the victim's credentials.

The victim clicks on a legitimate SharePoint link** and is redirected to a document containing instructions to enter credentials onto a fraudulent login page.

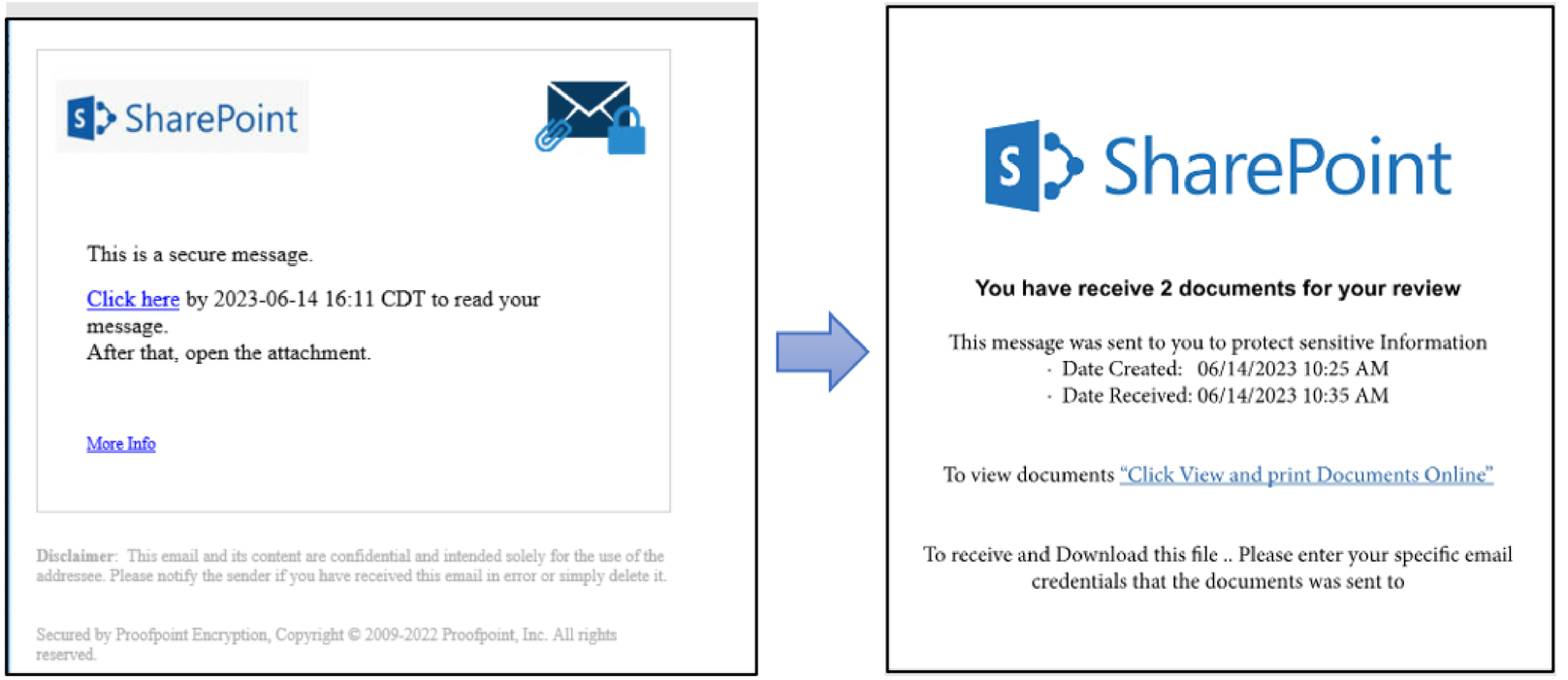
**bypasses spam filters

Threat actor captures the victims' credentials.

AON

Case Study #2 – Brand Impersonation

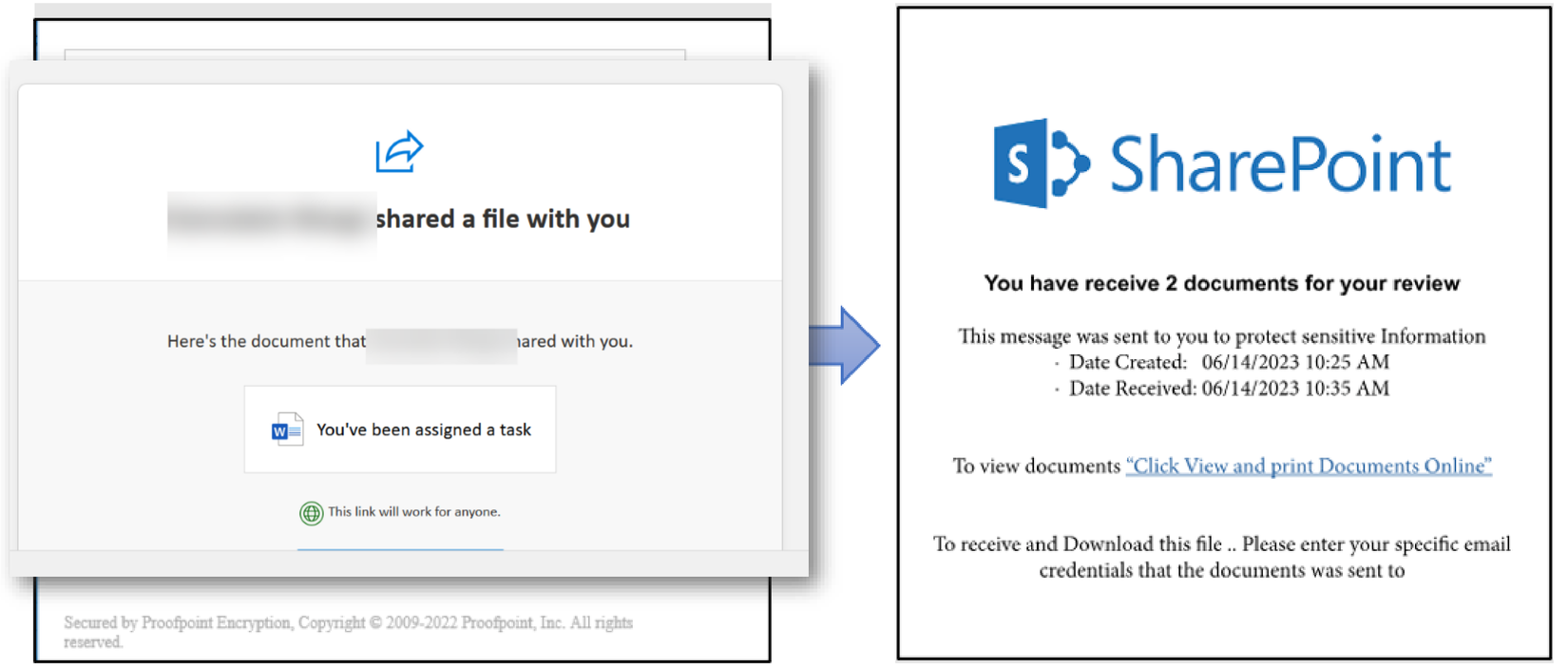
Malicious Email



Phishing email and linked webpage imitating SharePoint notification[12].

Case Study #2 – Brand Impersonation

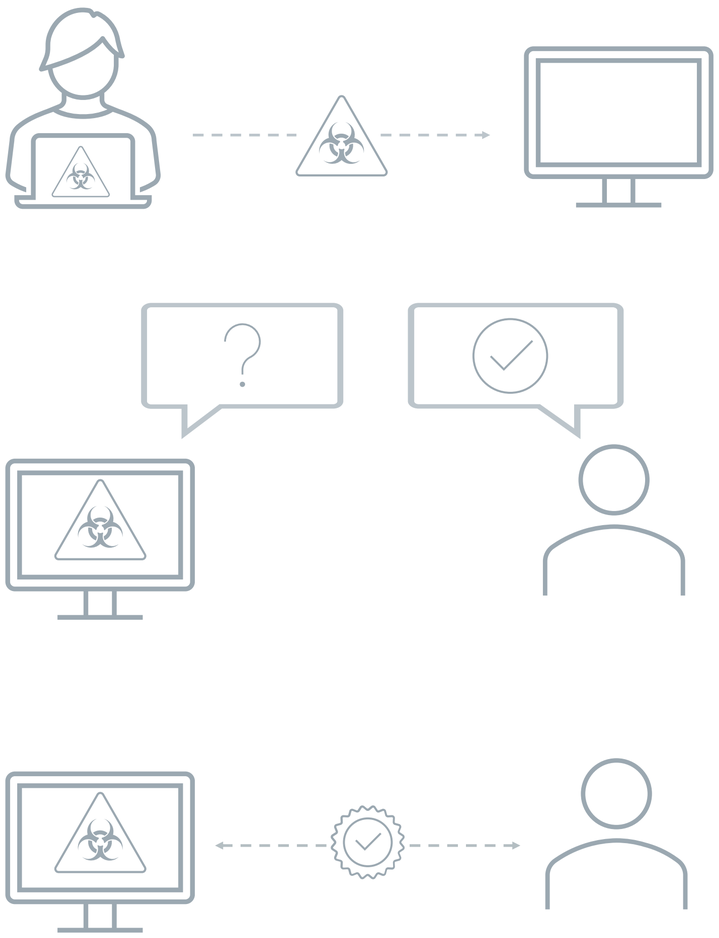
Malicious Email



Phishing email and linked webpage imitating SharePoint notification[12].

Phishing across Third-party Services

Consent Phishing



Malicious application is registered with a legitimate OAuth 2.0 provider

Application is registered with the target platform
(ex. Azure Marketplace, Google Workspace)

Victim receives and falls for a phishing email with request to grant permission to the malicious application

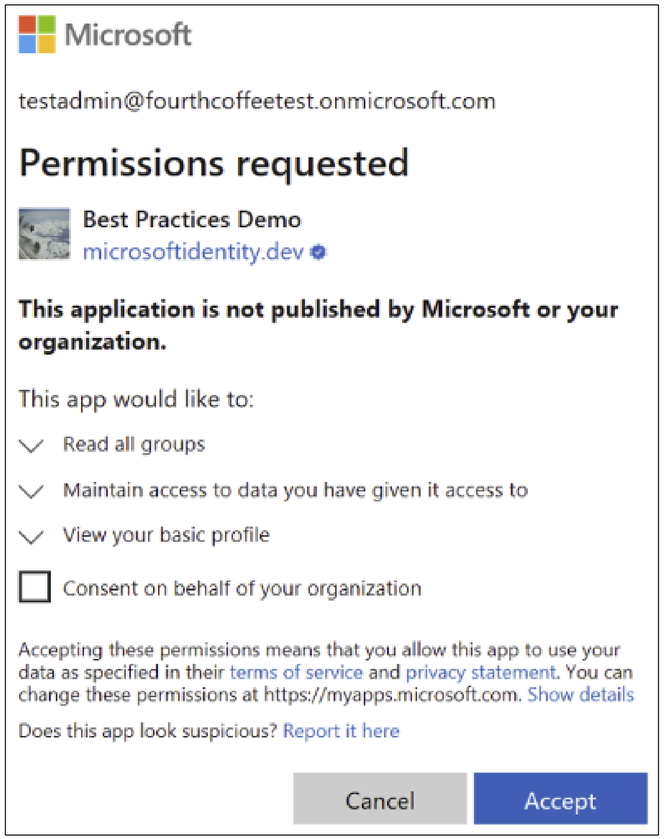
Threat actor has wholesale access to victim's data

- Successful consent phishing can result in ***wholesale access*** to mailbox
- Resistant to password resets and traditional security measures
  - Bypasses entire MFA process, relying on tokens in lieu of credentials
  - Evades anti-spam gateway + URL filtering due to lack of malicious link
- Raises little suspicion to both employees and security teams

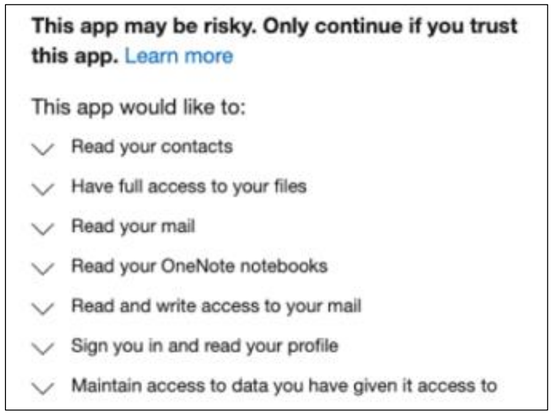
AON

Case Study #3 – Consent Phishing

Malicious Permissions



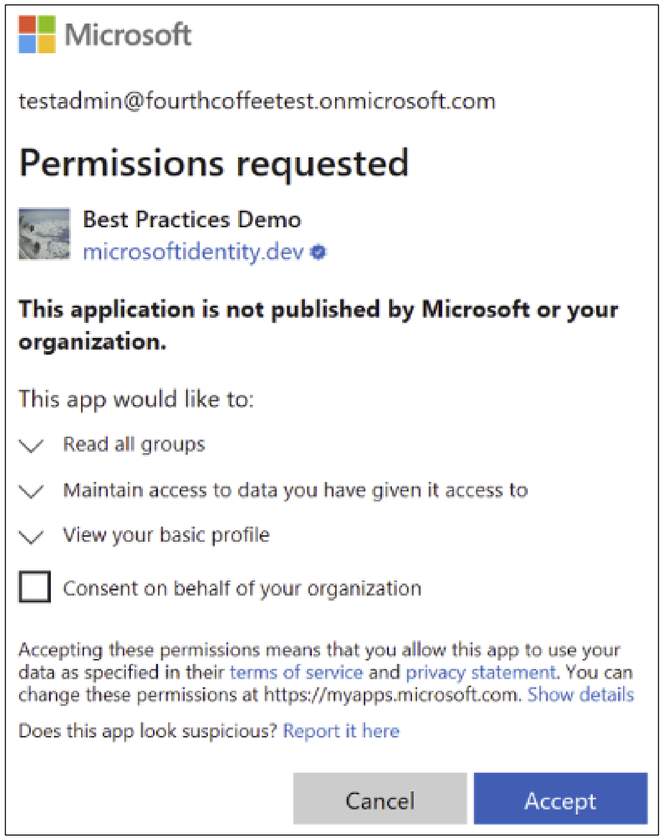
Unverified OAuth application requesting a broad set of permissions[12]



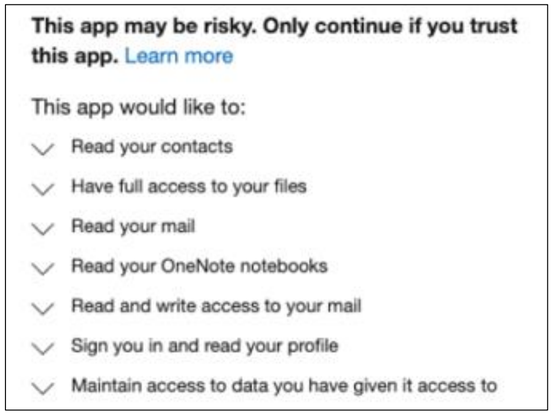
Additional potential permissions requested by unverified OAuth applications [13]

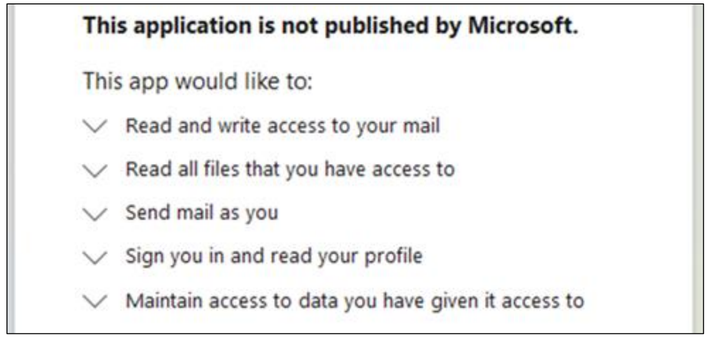
Case Study #3 – Consent Phishing

Malicious Permissions

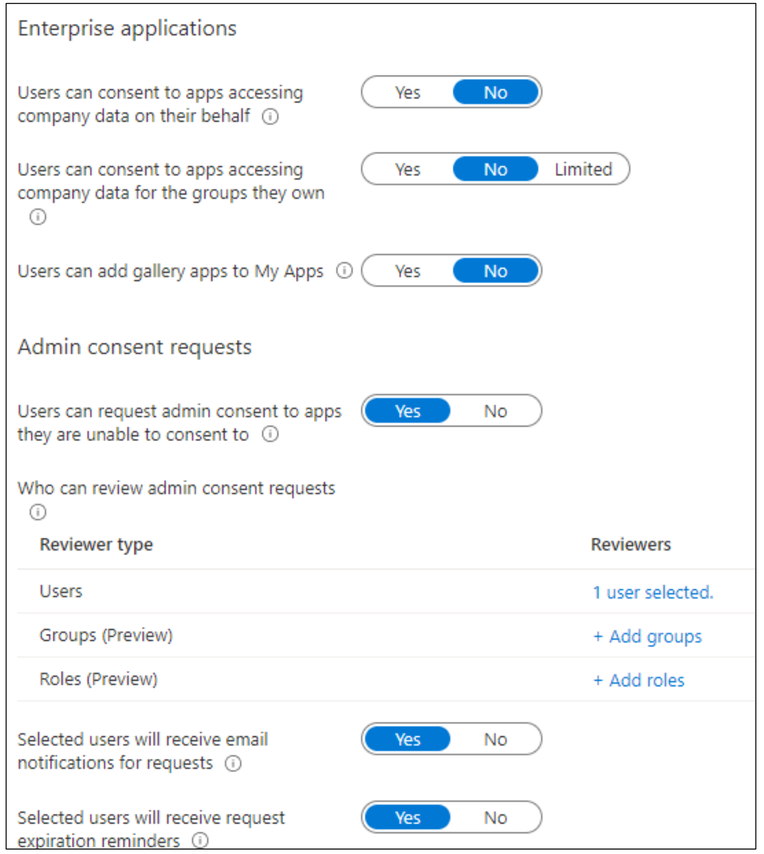


Unverified OAuth application requesting a broad set of permissions[12]





Additional potential permissions requested by unverified OAuth applications [13]



Azure AD Portal → Enterprise Application → User settings[13]

Protections Against Third-Party Attacks

Attacks that evade traditional security measures

Employee Training

- Clear protocols and communication channels surrounding external sharing of sensitive information
- Frequent security awareness training on phishing detection and concept of malicious applications

Access Controls

- Apply the principle of least privilege to all third-party integrations, ensuring *minimum* necessary access
- Limit user ability to approve OAuth application connections; routinely audit consented permissions across existing OAuth applications
- Implement RBAC across access to sensitive data and systems

Advanced Measures

- Utilize brand monitoring services to detect unauthorized usage of brand across phishing
- Leverage threat intelligence platforms and SIEMs to enhance detection capabilities
- Consider AI-based security solutions to spot behavioral-based alerts (over signature-based alerts)

AON

4

A Changing Landscape: What comes next?

AI in Phishing

Phishing-As-A-Service

Artificial Intelligence in Phishing Campaigns

Advanced Email Phishing

Threat actors view **AI technologies** as a gold mine for phishing.

Human-based Phishing

Phishing with Gen AI

Artificial Intelligence in Phishing Campaigns

Advanced Email Phishing

Threat actors view **AI technologies** as a gold mine for phishing.

Human-based Phishing

- × Typos in content, vocabulary, and font; poor grammatical errors or sentence structures
- × Inconsistencies in sender's email address and/or domain
- × Generic greetings and signatures
- × Sense of urgency within unexpected or unsolicited emails

Generally caught by anti-phishing filters

Phishing with Gen AI

AON

Artificial Intelligence in Phishing Campaigns

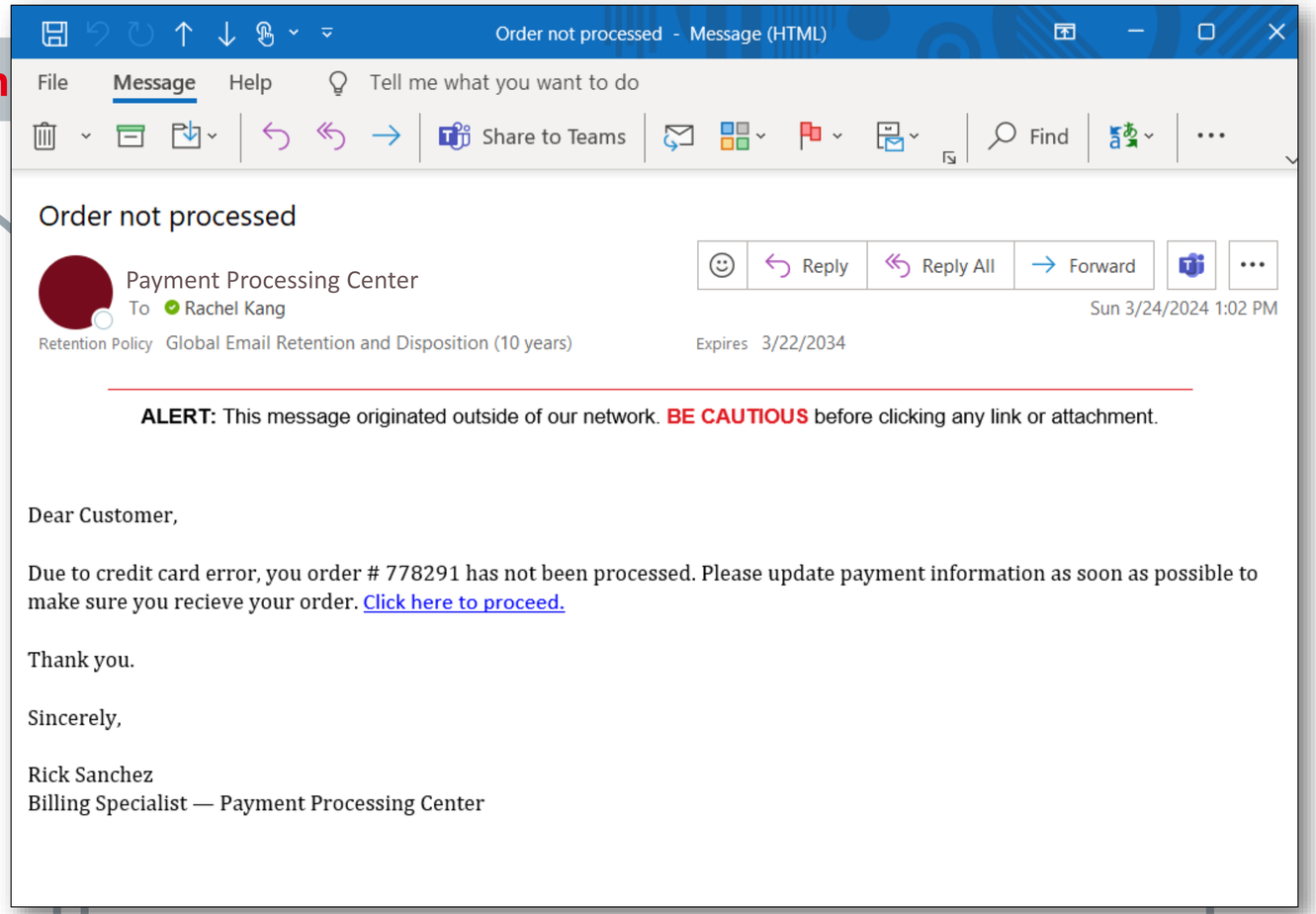
Advanced Email Phishing

Threat actors view **AI techn**

Human-based Phishing

- × Typos in content, vocabulary, and font; poor grammatical errors or sentence structures
- × Inconsistencies in sender's email address and/or domain
- × Generic greetings and signatures
- × Sense of urgency within unexpected or unsolicited emails

Generally caught by anti-phishing filters



Artificial Intelligence in Phishing Campaigns

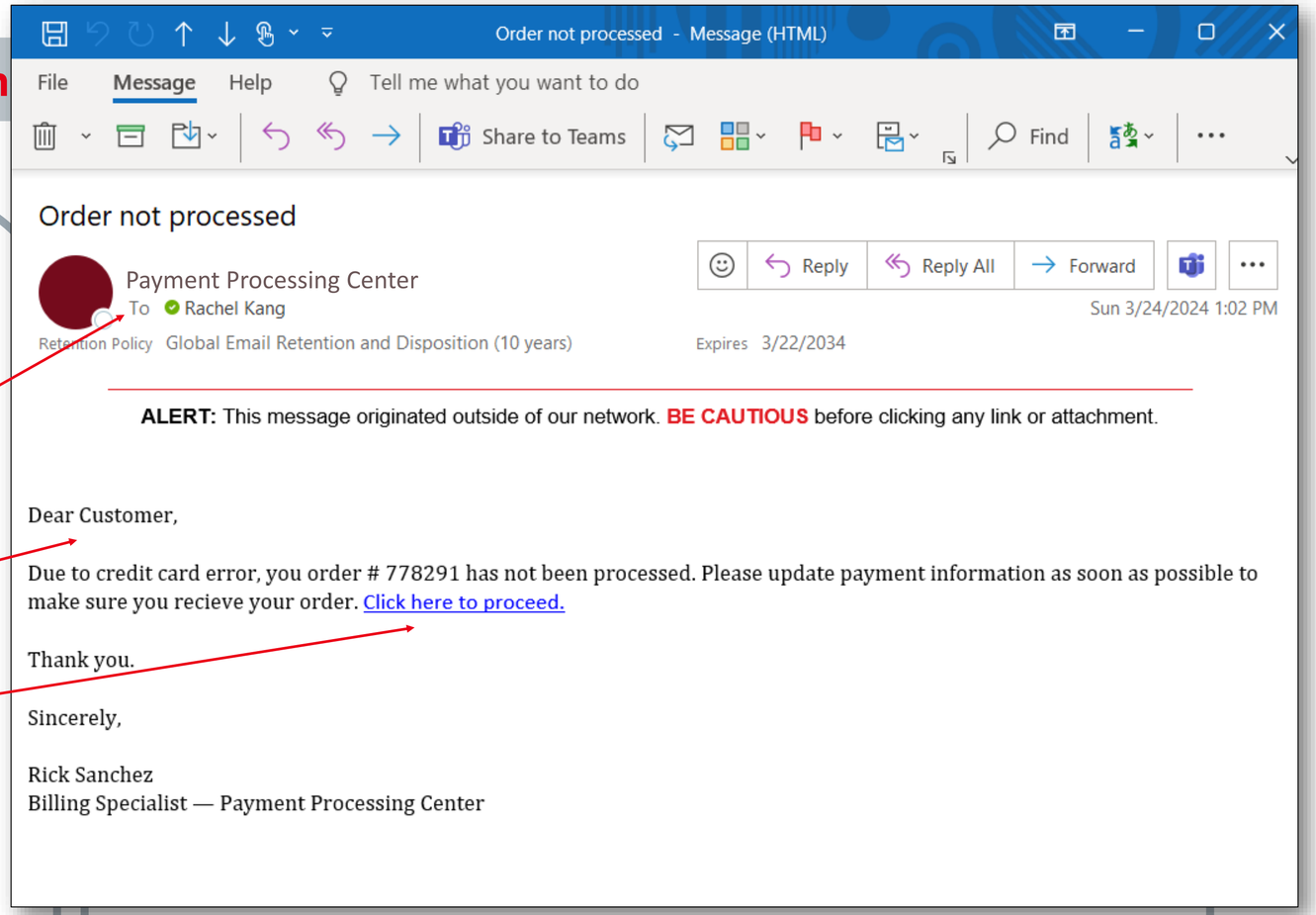
Advanced Email Phishing

Threat actors view **AI techn**

Human-based Phishing

- × Typos in content, vocabulary, and font; poor grammatical errors or sentence structures
- × Inconsistencies in sender's email address and/or domain
- × Generic greetings and signatures
- × Sense of urgency within unexpected or unsolicited emails

Generally caught by anti-phishing filters



Artificial Intelligence in Phishing Campaigns

Advanced Email Phishing

Threat actors view **AI technologies** as a gold mine for phishing.

Human-based Phishing

- × Typos in content, vocabulary, and font; poor grammatical errors or sentence structures
- × Inconsistencies in sender's email address and/or domain
- × Generic greetings and signatures
- × Sense of urgency within unexpected or unsolicited emails

Generally caught by anti-phishing filters

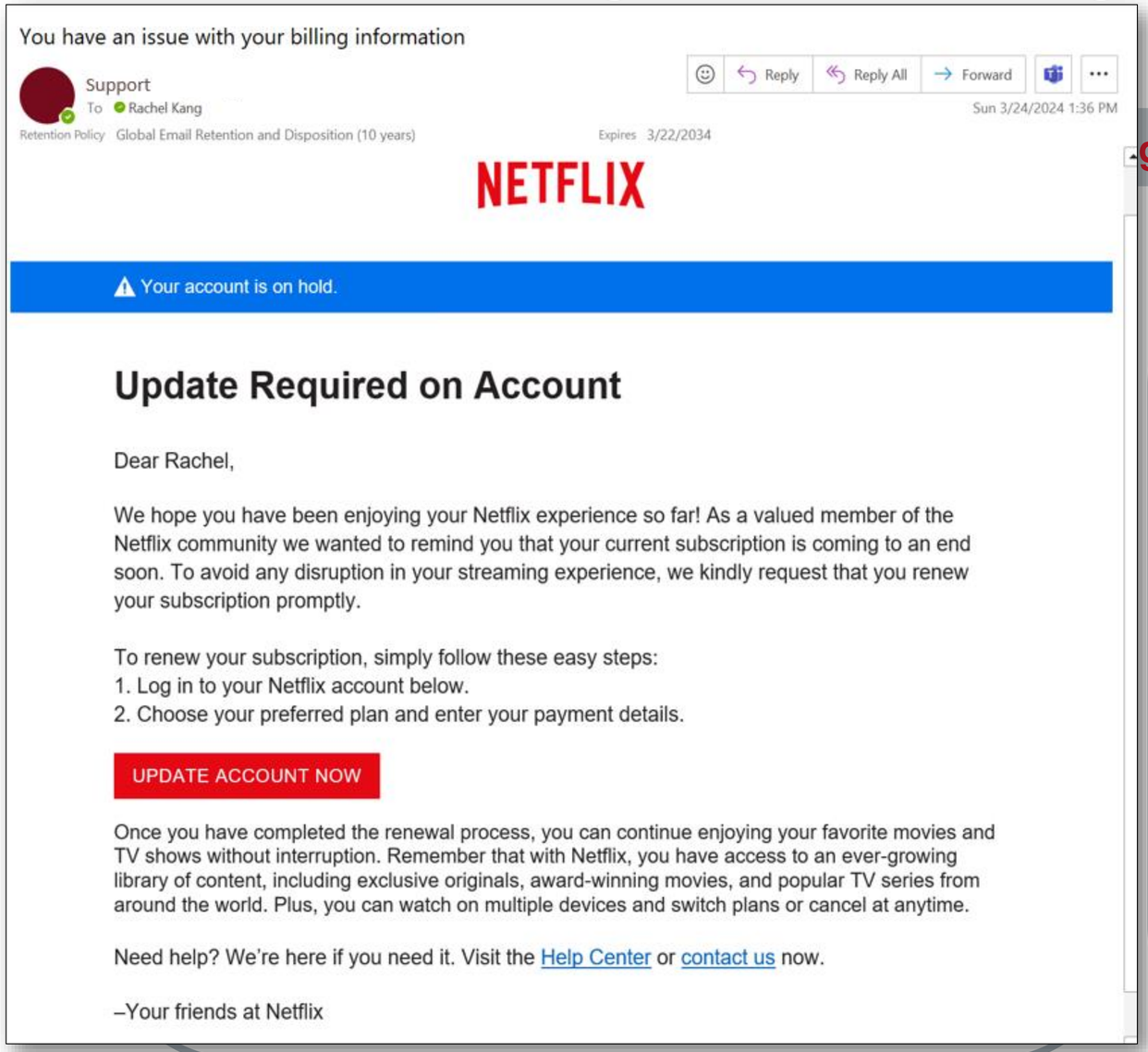
Phishing with Gen AI

- ✓ Near perfect verbiage, with no typos nor grammatical errors
- ✓ Obfuscated senders
- ✓ Custom greeting and expected signatures
- ✓ Credible sense of urgency

May or may not evade anti-phishing filters

AON

Artificial Intelligence in Phishing Campaigns



You have an issue with your billing information

Support
To Rachel Kang
Retention Policy Global Email Retention and Disposition (10 years) Expires 3/22/2034

Reply | Reply All | Forward
Sun 3/24/2024 1:36 PM

NETFLIX

⚠ Your account is on hold.

Update Required on Account

Dear Rachel,

We hope you have been enjoying your Netflix experience so far! As a valued member of the Netflix community we wanted to remind you that your current subscription is coming to an end soon. To avoid any disruption in your streaming experience, we kindly request that you renew your subscription promptly.

To renew your subscription, simply follow these easy steps:
1. Log in to your Netflix account below.
2. Choose your preferred plan and enter your payment details.

UPDATE ACCOUNT NOW

Once you have completed the renewal process, you can continue enjoying your favorite movies and TV shows without interruption. Remember that with Netflix, you have access to an ever-growing library of content, including exclusive originals, award-winning movies, and popular TV series from around the world. Plus, you can watch on multiple devices and switch plans or cancel at anytime.

Need help? We're here if you need it. Visit the Help Center or contact us now.

–Your friends at Netflix

gies as a gold mine for phishing.

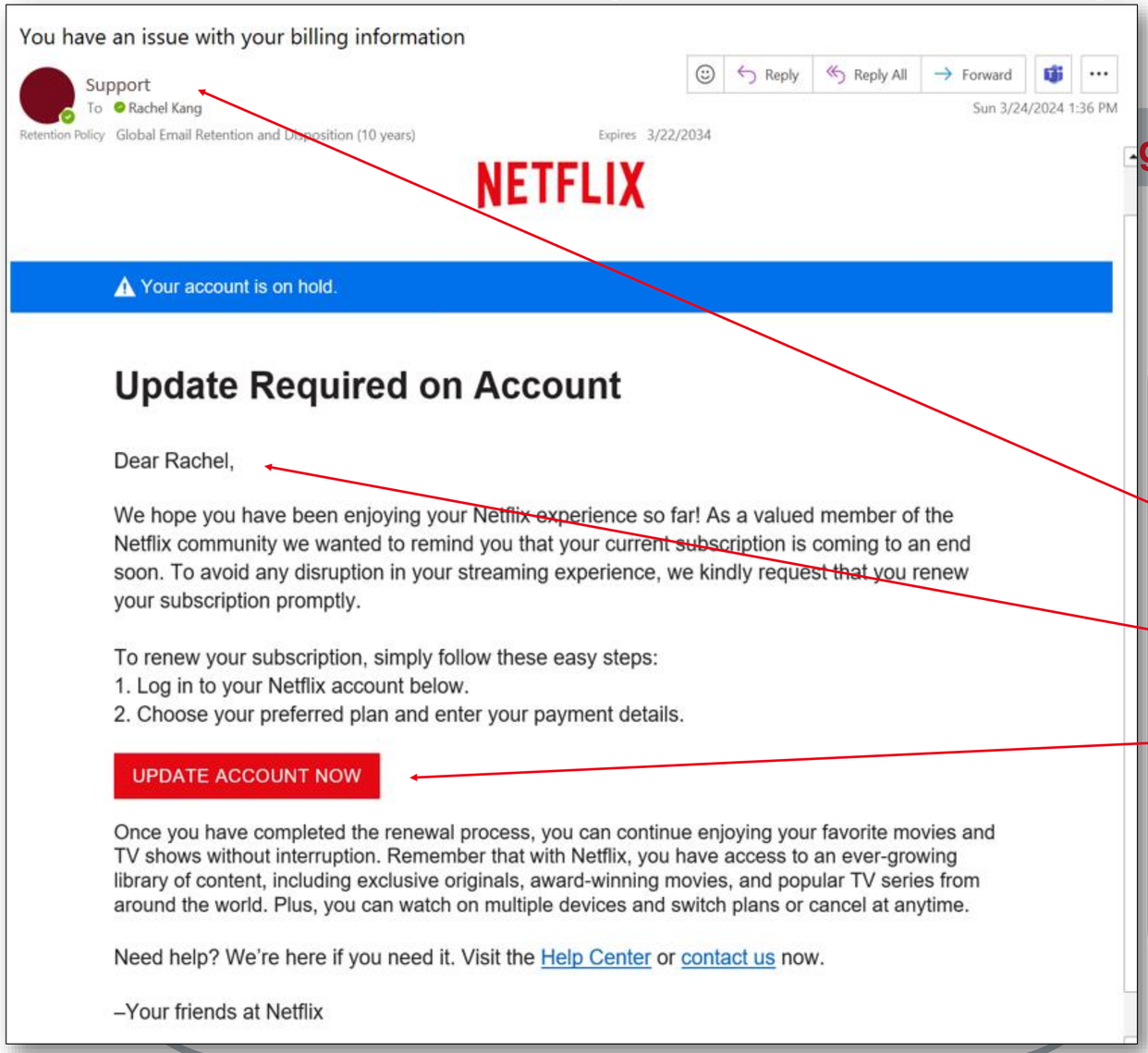
Phishing with Gen AI

- ✓ Near perfect verbiage, with no typos nor grammatical errors
- ✓ Obfuscated senders
- ✓ Custom greeting and expected signatures
- ✓ Credible sense of urgency

May or may not evade anti-phishing filters

AON

Artificial Intelligence in Phishing Campaigns



You have an issue with your billing information

Support
To Rachel Kang
Retention Policy Global Email Retention and Disposition (10 years) Expires 3/22/2034

Reply | Reply All | Forward
Sun 3/24/2024 1:36 PM

NETFLIX

⚠ Your account is on hold.

Update Required on Account

Dear Rachel,

We hope you have been enjoying your Netflix experience so far! As a valued member of the Netflix community we wanted to remind you that your current subscription is coming to an end soon. To avoid any disruption in your streaming experience, we kindly request that you renew your subscription promptly.

To renew your subscription, simply follow these easy steps:
1. Log in to your Netflix account below.
2. Choose your preferred plan and enter your payment details.

UPDATE ACCOUNT NOW

Once you have completed the renewal process, you can continue enjoying your favorite movies and TV shows without interruption. Remember that with Netflix, you have access to an ever-growing library of content, including exclusive originals, award-winning movies, and popular TV series from around the world. Plus, you can watch on multiple devices and switch plans or cancel at anytime.

Need help? We're here if you need it. Visit the Help Center or contact us now.

–Your friends at Netflix

gies as a gold mine for phishing.

Phishing with Gen AI

- ✓ Near perfect verbiage, with no typos nor grammatical errors
- ✓ Obfuscated senders
- ✓ Custom greeting and expected signatures
- ✓ Credible sense of urgency

May or may not evade anti-phishing filters

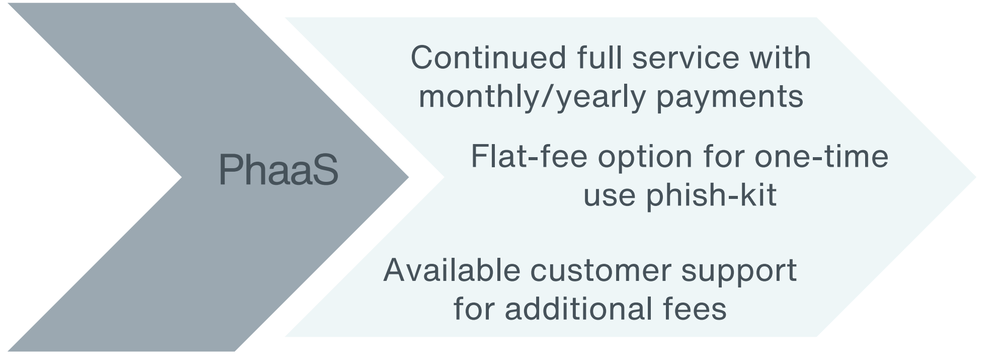
AON

Artificial Intelligence in Phishing Campaigns

The Future of Phishing Campaigns

71.4% of email attacks created using AI go undetected [14]

- Cybercriminals have now become **service providers**, selling **subscription models** for phishing on the dark web, also known as “Phishing-as-a-Service”/“PhaaS”



Artificial Intelligence in Phishing Campaigns

The Future of Phishing Campaigns

71.4% of email attacks created using AI go undetected [14]

- Cybercriminals have now become **service providers**, selling **subscription models** for phishing on the dark web, also known as “Phishing-as-a-Service”/“PhaaS”
- Selling AI tools that generate the elements for a phishing attack into a ready-to-deploy “**phishing kit**”[12]

PhaaS

- Continued full service with monthly/yearly payments
- Flat-fee option for one-time use phish-kit
- Available customer support for additional fees

Phishing Kit

- Phishing email templates
- Spoofed company logos on fraudulent login pages
- Pre-built victim email listing
- Anti-detection mechanisms

Artificial Intelligence in Phishing Campaigns

The Future of Phishing Campaigns

71.4% of email attacks created using AI go undetected [14]

- Cybercriminals have now become **service providers**, selling **subscription models** for phishing on the dark web, also known as “Phishing-as-a-Service”/“PhaaS”
- Selling AI tools that generate the elements for a phishing attack into a ready-to-deploy “**phishing kit**”[12]

AI addresses several challenges that threat actors face in current social engineering scams:

1. Ability to simulate human interactions
   - sophisticated emails
   - voice-cloned vishing
2. Lowers barrier of entry to conduct mass phishing campaigns via PhaaS + phishkits
3. Broaden the reach of cybercriminal’s attacks

PhaaS

- Continued full service with monthly/yearly payments
- Flat-fee option for one-time use phish-kit
- Available customer support for additional fees

Phishing Kit

- Phishing email templates
- Spoofed company logos on fraudulent login pages
- Pre-built victim email listing
- Anti-detection mechanisms

AON

Actionable Guidance

Secure both within and beyond email environment

“

Phishing attacks can vary widely across platforms in their methodology, execution, and techniques – however, they all are still attempts to achieve the same result: lure unsuspecting victims into divulging private and confidential information.

No single solution to eliminate phishing attacks from our digital landscape.

AON

Actionable Guidance

Secure both within and beyond email environment

“

Phishing attacks can vary widely across platforms in their methodology, execution, and techniques – however, they all are still attempts to achieve the same result: lure unsuspecting victims into divulging private and confidential information.

No single solution to eliminate phishing attacks from our digital landscape.

To combat advanced phishing, both organizations and individual employees can take several steps:

1. Leverage **advanced, AI-based solutions** to detect and protect against advanced phishing attacks
2. Stay educated on phishing attacks and security risks across not only email platforms, but other common mediums as well (including **third-party services**)
3. Remain vigilant against **red flags**, conducting routine audits, updates, and security assessments.

AON

Actionable Guidance

Secure both within and beyond email environment

Check out my blog "**The Evolution Of Phishing Campaigns**" on Aon's Cyber Labs!

"

Phishing attacks can vary widely across platforms in their methodology, execution, and techniques – however, they all are still attempts to achieve the same result: lure unsuspecting victims into divulging private and confidential information.

Rachel Kang ("The Evolution of Phishing Campaigns")

No single solution to eliminate phishing attacks from our digital landscape.

To combat advanced phishing, both organizations and individual employees can take several steps:

1. Leverage **advanced, AI-based solutions** to detect and protect against advanced phishing attacks
2. Stay educated on phishing attacks and security risks across not only email platforms, but other common mediums as well (including **third-party services**)
3. Remain vigilant against **red flags**, conducting routine audits, updates, and security assessments.

AON

Follow us!

X/Twitter

@StrozDFIR

Check out our Cyber Labs blog

https://www.aon.com/en/insights/collections/cyber-labs

Endnotes

[1] ""Love Bug" virus continues to wreak havoc." May 4, 2000. https://www.computerworld.com/article/1370113/love-bug-virus-continues-to-wreak-havoc.html

[2] "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack." October 3, 2017. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

[3] "Equifax Data Breach Impacts 143 Million Americans." September 7, 2017. https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/

[4] "Annual Threat Report 2024." Reliaquest.com, March 26, 2024. https://www.reliaquest.com/resources/research-reports/annual-threat-report-2024/

[5] "Attacks that Smish, Phish, and Vish Their Way around MFA." Aon.com, 2022. https://cyber.aon.com/case_studies/attacks-that-smish-phish-and-vish-their-way-around-mfa/

[6] "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public." February 08, 2022. https://www.ic3.gov/Media/Y2022/PSA220208

[7] "A SIMple Attack: A Look Into Recent SIM Swap Attack Trends." Aon.com, October 14, 2023. https://cyber.aon.com/aon_cyber_labs/a-simple-attack-a-look-into-recent-sim-swap-attack-trends/

[8] "Roasting 0ktapus: The phishing campaign going after Okta identity credentials" Group-IB.com, August 25, 2022. https://www.group-ib.com/blog/0ktapus/

[9] "The mechanics of a sophisticated phishing scam and how we stopped it" cloudflare.com, August 9, 2022. https://blog.cloudflare.com/2022-07-sms-phishing-attacks/

[10] "Incident Report: Employee and Customer Account Compromise" twilio.com, October 27, 2022. https://www.twilio.com/en-us/blog/august-2022-social-engineering-attack

[11] "BYOD SECURITY REPORT" Cybersecurityinsiders.com, 2021. https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q2BYOD2021.pdf

[12] "The Evolution of Phishing Campaigns" Aon.com, September 11, 2023. https://www.aon.com/cyber-solutions/aon_cyber_labs/the-evolution-of-phishing-campaigns/

[13] "Consent (OAuth) phishing...from attack to detect to prevent with Microsoft Defender for Cloud Apps" medium.com, November 17, 2021. https://derkvanderwoude.medium.com/consent-oauth-phishing-from-attack-to-detect-to-prevent-with-microsoft-defender-for-cloud-apps-86bfa660ad82

[14]"AI-Generated Phishing Emails Almost Impossible to Detect, Report Finds" infosecurity-magazine.com, October 3, 2023. "https://www.infosecurity-magazine.com/news/ai-phishing-emails-almost/

[slide 1] https://media.licdn.com/dms/image/D5612AQFhilfds0Ju8w/article-cover_image-shrink_720_1280/0/1673314206179?e=1725494400&v=beta&t=dyXcAUnB7pKqmBpBi0MFfBoDYNkz0H1pxGOBcZyX7Ho

[slide 7] https://1000logos.net/myspace-logo/

https://miro.medium.com/v2/resize:fit:828/format:webp/1*JW9qFdQXL6YfXrumaTz4jQ.jpeg

https://www.macworld.com/article/230231/original-2007-iphone-photo-album.html

[slide 9] https://www.theverge.com/2012/1/26/2742560/gmail-logo-designed-night-before-service-launched

https://www.brandcrowd.com/blog/facebook-logo-history/

https://www.macrumors.com/2017/01/27/seven-years-ago-the-ipad/

[slide 11] https://en.m.wikipedia.org/wiki/File:Google_Workspace_Logo.svg

https://commons.wikimedia.org/wiki/File:Meta-Logo.png

https://www.criticalpathsecurity.com/announcing-new-office-microsoft-365-hardening-audits-at-critical-path-security/

https://en.m.wikipedia.org/wiki/File:Google_Authenticator_(April_2023).svg

https://microsoft.fandom.com/wiki/Microsoft_Authenticator

https://commons.wikimedia.org/wiki/File:Google_Authenticator_for_Android_icon.svg

https://brandfetch.com/duosecurity.com

https://1000logos.net/okta-logo/

[slide 20 - 23] https://www.hatchwise.com/resources/the-history-of-the-amazon-logo

https://blogs.microsoft.com/blog/2012/08/23/microsoft-unveils-a-new-look/

https://en.m.wikipedia.org/wiki/File:Google_Cloud_logo.svg

https://commons.wikimedia.org/wiki/File:Dropbox_logo_2017.svg

https://en.m.wikipedia.org/wiki/File:Box,_Inc._logo.svg

https://www.docusign.com/en-gb/ip/trademark-brand-guide

https://commons.wikimedia.org/wiki/File:Amazon_Web_Services_Logo.svg

https://en.wikipedia.org/wiki/File:Microsoft_Azure_Logo.svg

[slide 42] https://www.creativebloq.com/news/twitter-logo-history

**Memes created using Mematic app

Questions & Answers

Special Thanks To:

Anthony Mussario

Carly Battaile

Partha Alwar

AON