



Phishing 2.0: The Rise of Artificial Intelligence

Rachel Kang

Manager, Digital Forensics and
Incident Response

Aon Cyber Solutions

WiCyS 2024

April 13, 2024



Current Cyber Threat Landscape

2023 Phishing Statistics

Email is by far the **most exploited** business application.

Many current scams still require humans to establish rapport with victims...

...but AI will bridge this gap with its ability to **simulate human interactions**.

Effective phishing attacks are typically conducted by sophisticated cybercriminals...

...but AI opens the doors for **novice attackers** to conduct similar campaigns.

Spam emails sent daily in United States¹

347 billion

As of January 2023

% of threats attributed to deceptive links¹

35.6%

As of May 2023

Financial Losses in 2022²

\$43.3 billion

Source: FBI

Financial Losses in 2023³

\$50.8 billion

Source: FBI

Advent of AI across Phishing Landscape



Phishing-As-A-Service (PhaaS)

- Cybercriminals have now become **service providers**, selling **subscription models** for phishing on the dark web
 - Continued full service with monthly/yearly payments
 - Flat fee options for one phishing kit (phish-kits)
- Selling AI tools that generate the following elements into a ready-to-deploy **“phishing kit”**⁴ :
 - phishing email templates
 - spoofed company logos on fraudulent login pages
 - victims’ email addresses pre-filled into login prompts

Generative AI in Phishing



- Several gaps in current social engineering scams can be addressed with **AI generated content**, including emails
- 71.4% of email attacks created using AI go **undetected**⁵
 - Near-perfect verbiage and sentence structures
 - Localized phishing pages based on victim’s native language
 - Large Language Models (LLM) allow for phishers to better obfuscate the intended sender

Advent of AI across Phishing Landscape



Phishing-As-A-Service (PhaaS)

- Cybercriminals have now become **service providers**, selling **subscription models** for phishing on the dark web
 - Continued full service with monthly/yearly payments
 - Flat fee options for one phishing kit (phish-kits)
- Selling AI tools that generate the following elements into a ready-to-deploy “**phishing kit**”⁴ :
 - phishing email templates
 - spoofed company logos on fraudulent login pages
 - victims’ email addresses pre-filled into login prompts

Lowered barrier of entry for cybercriminals to conduct phishing campaigns



Generative AI in Phishing

- Several gaps in current social engineering scams can be addressed with **AI generated content**, including emails
- 71.4% of email attacks created using AI go **undetected**⁵
 - Near-perfect verbiage and sentence structures
 - Localized phishing pages based on victim’s native language
 - Large Language Models (LLM) allow for phishers to better obfuscate the intended sender

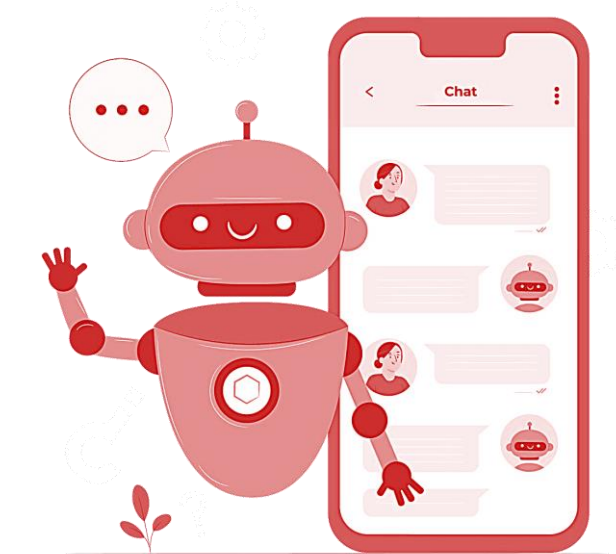
Broadened reach of cybercriminals' phishing campaigns

Features of AI-generated phishing

Cybercriminal v. Victim Perspective

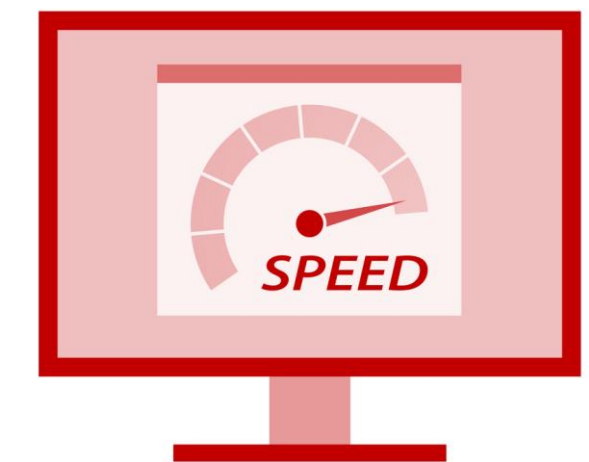
1. Convenience

- **Hand-holding** through the phishing campaign creation process
- Lack of **ethical guardrails** in LLM chatbots (FraudGPT/WormGPT)



2. Speed

- Automated campaigns travel at a much **faster rate** than humans could ever conduct
- Increased **surface area** of such attacks

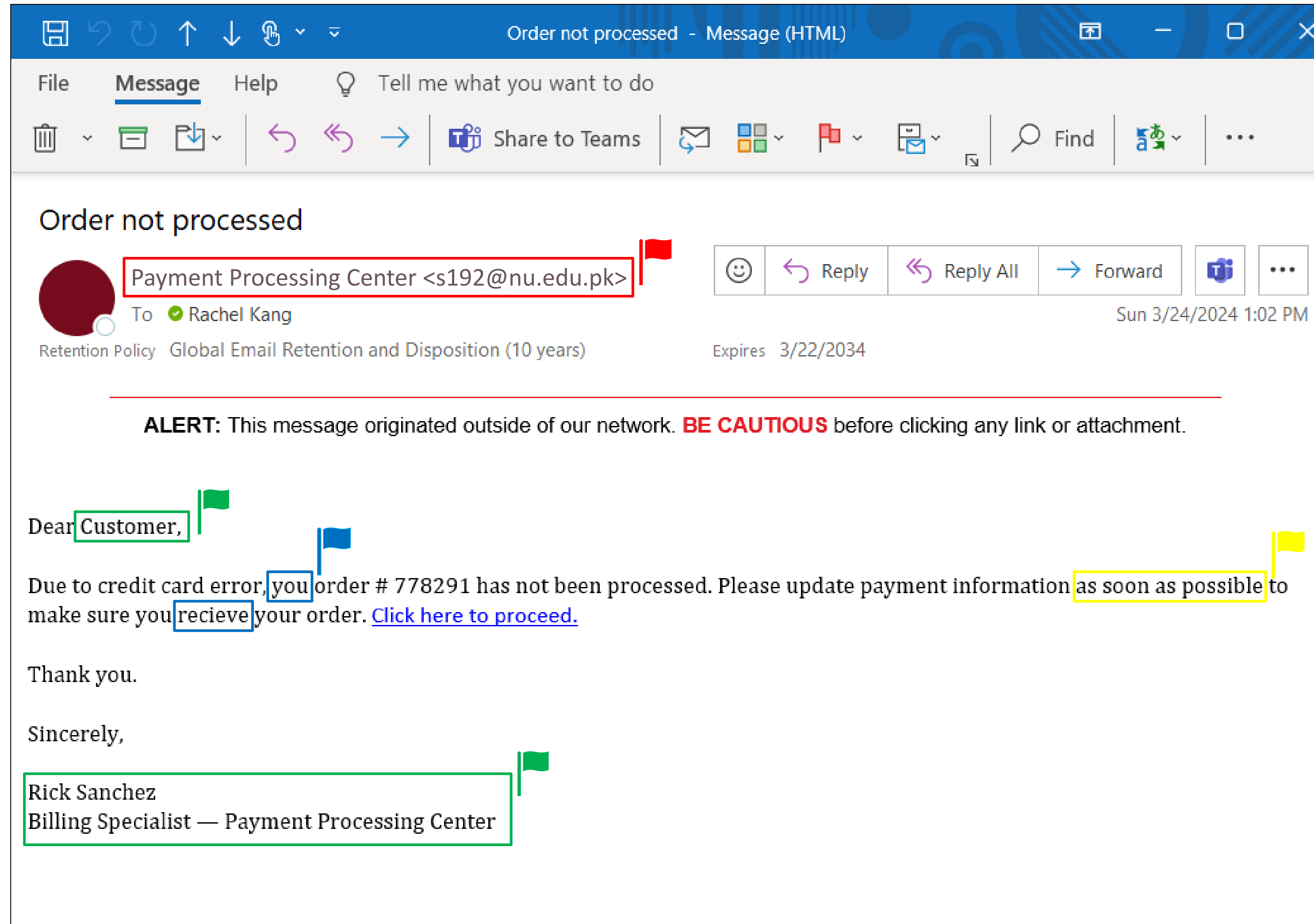


3. Effectiveness





- Credible call to action → real-time information absorbed into LLM chatbots, allowing criminals to incorporate **of-the-moment details** and contextually relevant information into phishing emails
- Highly personalized, mimicking the victim's **profession, interests, and habits**
- Lack of spelling errors, grammatical mistakes, and odd sentence structures
 - Typos indicate human-generated content!

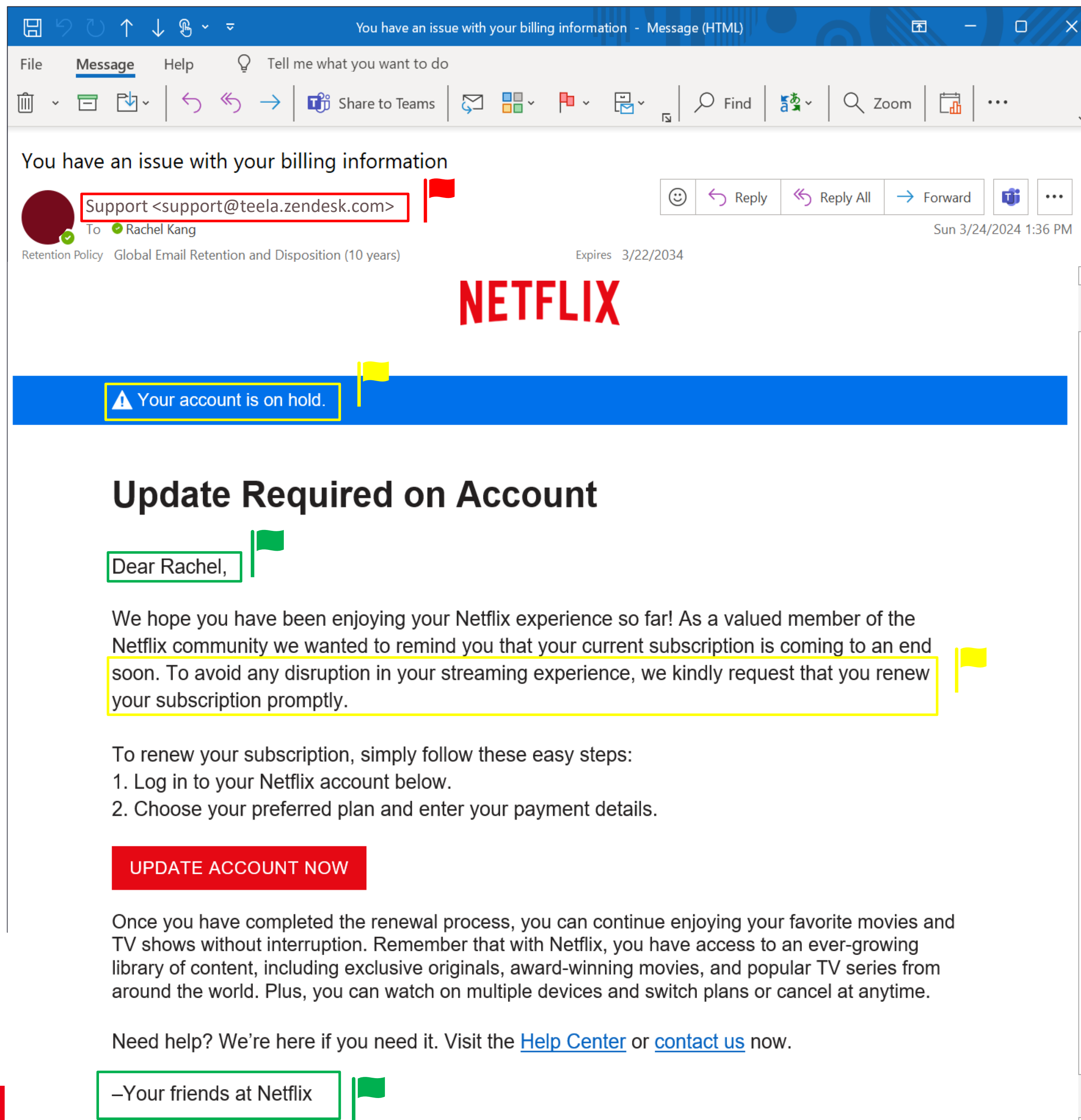


Human Generated Phish







Red Flags Noted

-  Inconsistencies in sender's email address and/or domain.
-  Generic greeting and signatures.
-  Typos in content, vocabulary, and font.
-  Sense of urgency in an unexpected/unsolicited email.



AI Generated Phish

Red Flags Addressed

-  Sender's domain is obfuscated with authentic helpdesk domain.
-  Custom greeting and expected signature.
-  No typos nor grammatical errors.
-  Credible sense of urgency.

You have an issue with your billing information - Message (HTML)

AI-Generated

You have an issue with your billing information

Support <support@teela.zendesk.com>
To Rachel Kang
Expires 3/22/2034

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

Reminder: update required due to payment issue - Message (HTML)

Real

Reminder: update required due to payment issue

Netflix <info@mail.netflix.com>
To Rachel Kang
Fri 5/29/2020 11:40 AM

NETFLIX

⚠ Your account is on hold.

Reminder: update your payment details

Hi Mom,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

UPDATE ACCOUNT NOW

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

—Your friends at Netflix

Endnotes

[1] “2023 Phishing Threats Report.” CloudFlare.com, August 16, 2023.

<https://blog.cloudflare.com/2023-phishing-report>

[2] “Business Email Compromise: The \$43 Billion Scam.” IC3.gov, May 4, 2022.

<https://www.ic3.gov/Media/Y2022/PSA220504>

[3] “Business Email Compromise: The \$50 Billion Scam.” IC3.gov, June 9, 2023.

<https://www.ic3.gov/Media/Y2023/PSA230609>

[4] “The Evolution of Phishing Campaigns” Aon.com, September 11, 2023.

https://www.aon.com/cyber-solutions/aon_cyber_labs/the-evolution-of-phishing-campaigns/

[5] “AI-Generated Phishing Emails Almost Impossible to Detect, Report Finds”

infosecurity-magazine.com, October 3, 2023. [https://www.infosecurity-](https://www.infosecurity-magazine.com/news/ai-phishing-emails-almost/)

[magazine.com/news/ai-phishing-emails-almost/](https://www.infosecurity-magazine.com/news/ai-phishing-emails-almost/)

[6] “Phishing as a Service Stimulates Cybercrime.” TrendMicro.com, March 2,

2023. [https://www.trendmicro.com/en_se/ciso/23/c/phishing-as-a-service-](https://www.trendmicro.com/en_se/ciso/23/c/phishing-as-a-service-phaas.html)

[phaas.html](https://www.trendmicro.com/en_se/ciso/23/c/phishing-as-a-service-phaas.html)

[icon] https://www.horsesforsources.com/as-a-service-economy-defined_080915/

[icon]

<https://www.postermywall.com/index.php/art/template/8be7e4b10ff1342cb85d8>

[2dbb3719d55/scam-alert-design-template](https://www.postermywall.com/index.php/art/template/8be7e4b10ff1342cb85d82dbb3719d55/scam-alert-design-template)

[icon] [https://www.freepik.com/free-vector/chat-bot-concept-](https://www.freepik.com/free-vector/chat-bot-concept-illustration_13317063.htm#query=bot&position=0&from_view=keyword&track=sp)

[illustration_13317063.htm#query=bot&position=0&from_view=keyword&track=sp](https://www.freepik.com/free-vector/chat-bot-concept-illustration_13317063.htm#query=bot&position=0&from_view=keyword&track=sp)

[h&uuid=e2bf3e2e-cb93-4a2f-8ecf-5b8f7bc99909](https://www.freepik.com/free-vector/chat-bot-concept-illustration_13317063.htm#query=bot&position=0&from_view=keyword&track=sp&uuid=e2bf3e2e-cb93-4a2f-8ecf-5b8f7bc99909)

[icon] [https://www.dreamstime.com/high-speed-internet-computer-test-screen-](https://www.dreamstime.com/high-speed-internet-computer-test-screen-illustration-image136858390)

[illustration-image136858390](https://www.dreamstime.com/high-speed-internet-computer-test-screen-illustration-image136858390)

[icon] [https://www.pngkit.com/view/u2r5a9w7r5r5q8i1_real-time-information-](https://www.pngkit.com/view/u2r5a9w7r5r5q8i1_real-time-information-real-time-icon-png/)

[real-time-icon-png/](https://www.pngkit.com/view/u2r5a9w7r5r5q8i1_real-time-information-real-time-icon-png/)

Questions & Answers