

# Comment répondre avec efficacité aux défis actuels de la protection email ?

IA générative, QR codes...

**Loïc Guézo** – senior director, cybersecurity strategy EMEA  
VP CLUSIF, LCL (RC) COMCYBER-MI



# Cyber Crime Impacts Everyone



**Enterprise**



**SMB**



**Individuals**



**At work**



**At home**

# The Reality of Cyber Crime

Affects companies' profitability and stability



2023: Comcast Faces Lawsuits over Breach of 36M Accounts



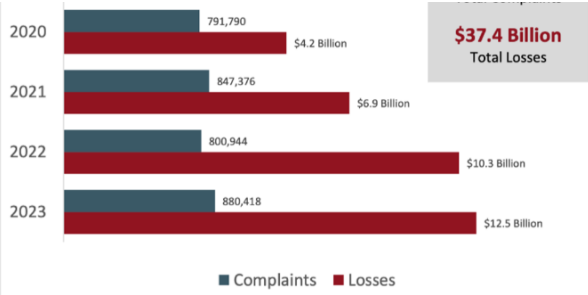
**Cyberattack cost MGM Resorts about \$100 million, Las Vegas company says**

The company said it deliberately shut down a number of services "to mitigate risk to customer information" after the hack last month.

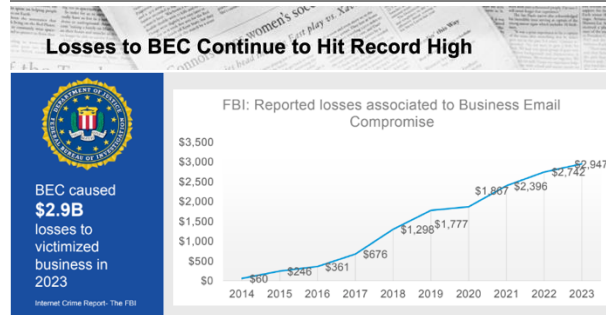


# Current Threat Landscape

## Cyber Crime



## Email Fraud



## Data Loss



**90%** of security incidents involved *human element*

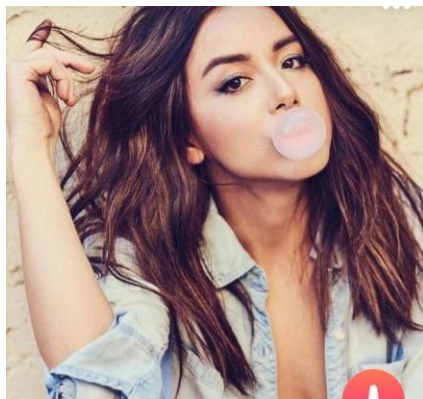


# When you think of Cyber Criminals...

You might think they gain  
access by hacking a network



# But Cyber Crime often looks like this...



Chloe, 25

Actress

11 kilometers away

Love to travel almost as much as I love my dog 🐶



They gain access by targeting people



**Bill Gates** ✓  
@BillGates

Sharing things I'm learning through my foundation work and other interests.

Seattle, WA [gatesnot.es/Pandemic-Preve...](#) Joined June 2009

368 Following 58.2M Followers

# Which of the following was the most abused brand in 2023?

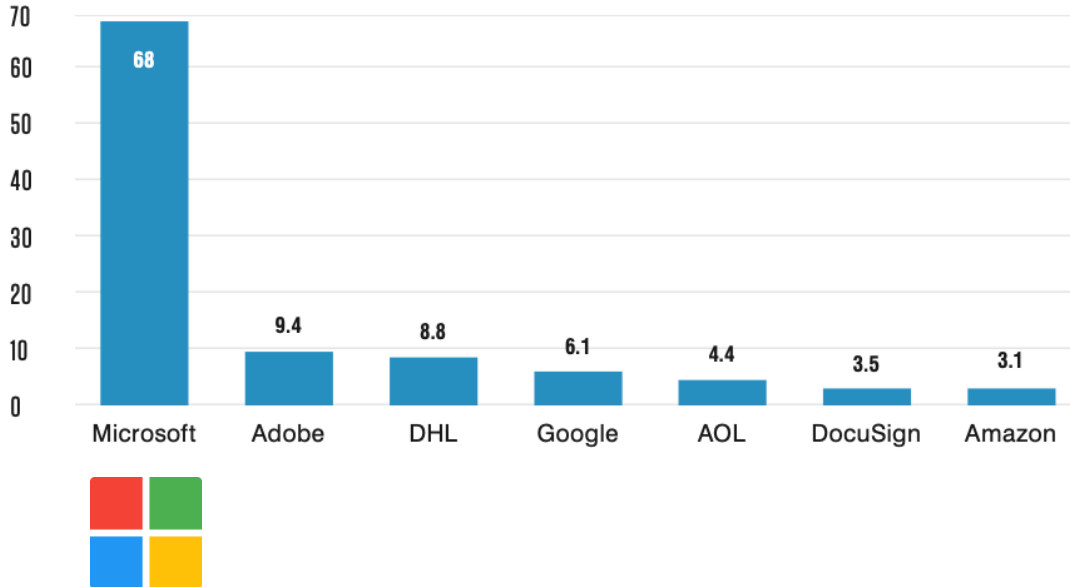


- 1) Amazon
- 2) Google
- 3) Microsoft
- 4) DocuSign

# Microsoft Remains Most-Abused Brand



Brand Abuse Threats (Million)



**68M** messages were associated with Microsoft products and brand;  
over **20M** email threats involved Office 365





# Phishing 101

How Attackers Exploit People

# It's All Social Engineering

proofpoint.

**REMEMBER:**



**PHISHING EMAILS WILL  
PULL ON YOUR HEARTSTRINGS**

# Three Parts of Social Engineering

Emotion



Trust



Timing



Used in **98%** of all cyber attacks

# Common Tactics of Social Engineering

## Emotion



Plays on  
Positive or  
Negative



Too Good to  
Be True

## Trust



Someone  
You Trust



Authority or  
Expertise

## Timing



Urgent  
Response



Offer  
Expires

# Take Actions for Attackers



**Run attackers' code**



**Give up your  
credentials**



**Transfer funds or data**

# What is Phishing?

Fishing > Phishing

Worms > Lures

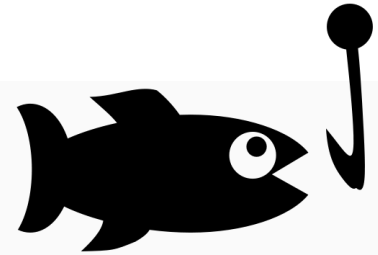
Hooked > Breached



Emails that fish for information and access



Messages that lure you in to take the bait



Once you're hooked...it's not good

# Three Primary Phishing Threats



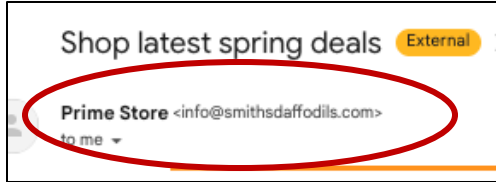
**Malicious links**

**Malicious  
attachments**

**Requests for  
sensitive data**



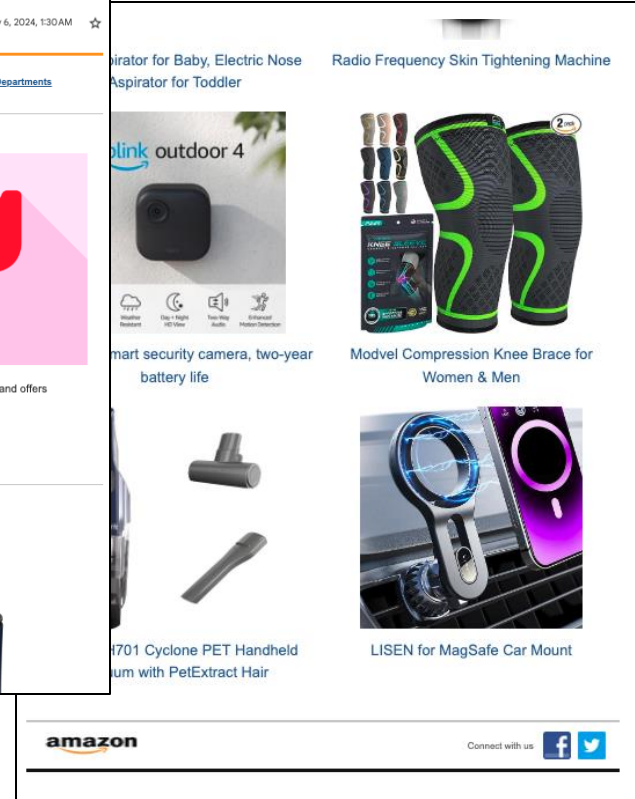
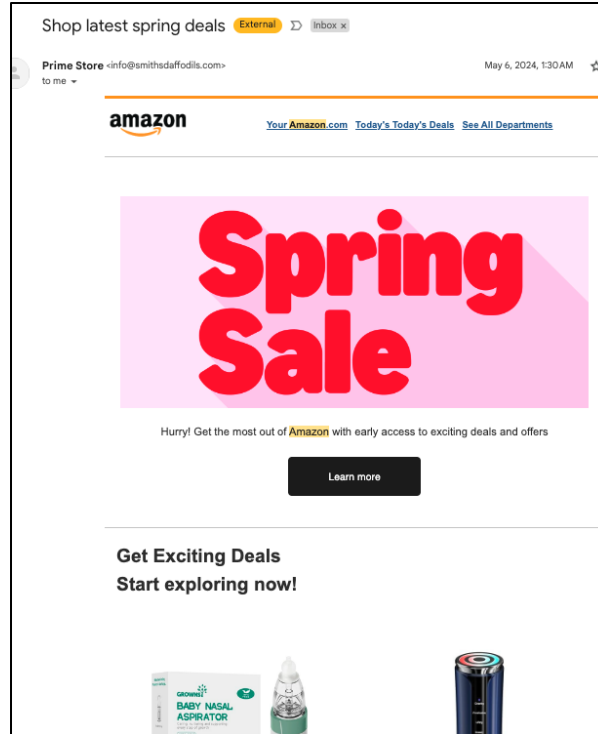
# Phishing at Home: Malicious Links



Mismatch email



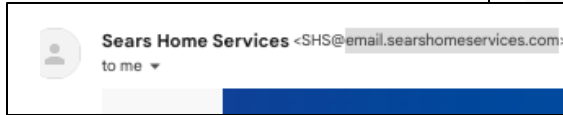
Brand looks off



# Phishing at Home: Malicious Links



mismatch email  
unbranded icon



mismatch name

© 2024 Transform SR Brands LLC, 5407 Trillium Boulevard Suite

Appliance on the fritz? We'll diagnose and repair the issue in no time

External | Inbox X

Sears Home Services <SHS@email.searshomeservices.com> to me

Thu, May 16, 2:46 PM

call 619.821.4948 to schedule not a member? join free

sears HOME SERVICES

repair home warranty home improvement clean & maintain shop parts

It's Flame Fine-tuning Season

Enjoy \$50 off Appliance Repair

Ensure your flames are even and reliable for perfect cooking every time. Our expert repairs can make it happen.

schedule repair

We'll fix it, no matter where you bought it.

Hi Valued Customer,

We noticed that your Protection Agreement for your Sears air conditioner has expired. First, let us thank you for the trust and loyalty you've shown Sears Home Services over the years. As a valued customer, here's \$50 off your next repair appointment, on us.

SPECIAL OFFER \$50 off appliance repair

SPECIAL OFFER \$50 off appliance repair now! schedule repair

Present code IHRPA50OFF to your technician.

SPECIAL OFFER \$25 off appliance repair schedule repair

Present code IHRPA25OFF to your technician.

May 31, 2024. Save \$50 on your next completed in-home repair on most kitchen or laundry appliances. Limit one service repair order. Certain appliance brands may be excluded. Determination will be made at time of service scheduling. Discount is applied before tax. Not valid on prior services, Clean & Maintain service, estimate collection Agreements, Home Warranty service, heating & cooling, electronics, lawn & garden or garage door sold in conjunction with other coupons, tech add-ons or preseason specials. Coupon is not transferable, is not for cash, and can not be combined with other offers. Additional exclusions may apply. Valid in USA and Puerto Rico in Guam or US Virgin Islands. Present this coupon to receive discount. Tech: Enter code IHRPA50OFF


May 31, 2024. Save \$25 on your next completed in-home repair on most kitchen or laundry appliances. Limit one service repair order. Certain appliance brands may be excluded. Determination will be made at time of service scheduling. Discount is applied before tax. Not valid on prior services, Clean & Maintain service, estimate collection Agreements, Home Warranty service, heating & cooling, electronics, lawn & garden or garage door sold in conjunction with other coupons, tech add-ons or preseason specials. Coupon is not transferable, is not for cash, and cannot be combined with other offers. Additional exclusions may apply. Valid in USA and Puerto Rico in Guam or US Virgin Islands. Present this coupon to receive discount. Tech: Enter code IHRPA25OFF

Sears Home Services LLC is part of Sears Home Services. The "Sears Home Services" brand and logo is used in license of Transform SR Brands LLC. This is an advertisement. All products, offers and services may not be available in all areas. Prices may vary by location. Minimum order or other restrictions may apply.

Transform SR Brands LLC, 5407 Trillium Boulevard Suite B120, Hoffman Estates, IL 60192. All rights reserved.

California Privacy Policy | License Info | Unsubscribe

# Phishing at Home: Malicious Attachment



Inv\_GT512487\_from\_Norton\_Inc\_2904.pdf  
153 KB

[Released] Fwd: Ordar Update Invoice

Debbie Rich <twinkles@wildbranches.com>  
Debbie Rich

Sat 10/22

problems with how this message is displayed, click here to view it in a web browser.  
download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.


Inv\_GT512487\_from\_Norton\_Inc\_2904.pdf  
153 KB

Dear Customer ,

Thank you for your order. Please review your payment amount below, we have attached a PDF detailing your order invoice and terms of your subscription.

Contact Support +1 888 230 8597 Reach out to us anytime between 9 AM To 6 PM EST. We'll be happy to help you.

-----Product Details: -----

GEEK SQUAD=INC. ® Network Security - Auto Renewal 3 Years subscription  
 Invoice Number: GT-512487  
 Invoice Date: 10/11/2022  
 Payment Method: Online  
 Amount: 349.99 USD

If you have any Question or Wish to cancel the Renewal, Please connect us on +1 888 230 8597 (9 AM To 6 PM EST)

Sincerely,  
 © 2022 GEEK SQUAD. All Rights Reserved  
 +1 888 230 8597

**To view attachment**  
 Open the attached PDF file. You must have [Acrobat® Reader®](#) installed to view the attachment.

**Push to open PDF**

**Incorrect grammar**

Dear Customer ,

between 9 AM To 6 PM EST.

# Phishing at Home: Malicious Attachment

Mismatch email

Re: Your Amazon Prime Account Update Information - Your Amazon Account Will Be Updated on Sunday, May 12, 2024 - [A55SR6US]

External External Spam

Customer Service <custx57-servicamzinformtliin178821120@mic5x9amz....> Sun, May 12, 5:39 AM  
to informationservice, bcc: me

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

One attachment • Scanned by Gmail

Anti-virus warning – 1 attachment contains a virus or blocked file. Downloading this attachment is d

amazon prime

Your Prime benefits are on hold due to a billing issue

Due to a problem with your card. We have been unable to

AMAZON-STATE...  
Virus found

Push to open PDF

# Phishing at Home: Request for Data

Wells Fargo Online <atmarin@calpoly.edu>  
Recipients


**Mismatch email**

are problems with how this message is displayed, click here to view it in a web browser.

Wells Fargo Online <atmarin@calpoly.edu>  
Recipients

Subject: Your Account Has Been Compromised.

---

 [wellsfargo.com](https://www.wellsfargo.com)

---

**Your Account has been restricted, unlock**

Your account has been limited for security reason to keep your account safe note all your transaction will be monitored to enhance your security.

To Unlock click on the below link and follow the security check Questions:

<http://www.welsfargo.com/secure>

Answer the security questions carefully and correctly. After you answer all the security question has been answer you dont have to do anything.

If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements online, Wells Fargo Customer Support is available 24 hours a day, 7 days a week. Call 1-800-4MYWELLS or sign on to send a [secure email](#).

[https://www.wellsfargo.com/privacy\\_security/fraud](https://www.wellsfargo.com/privacy_security/fraud)  
Click to follow link

Go to <http://www.welsfargo.com/secure>

**Incorrect website**

# Three Kinds of Non-Email Phishing



**Smishing  
(SMS Phishing)**

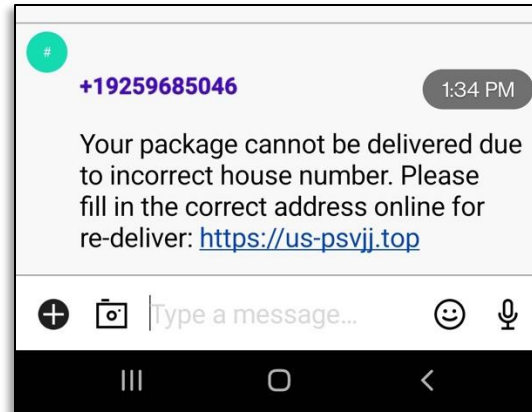
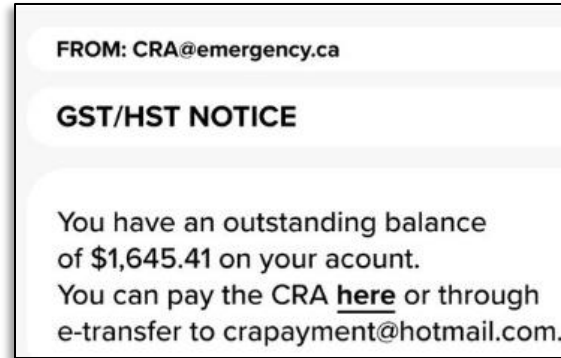
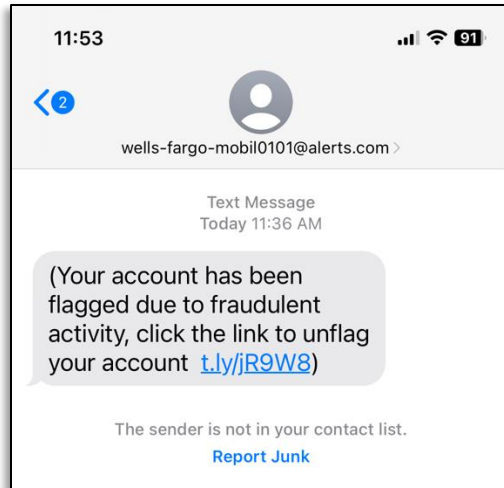


**Vishing  
(Voice Phishing)**



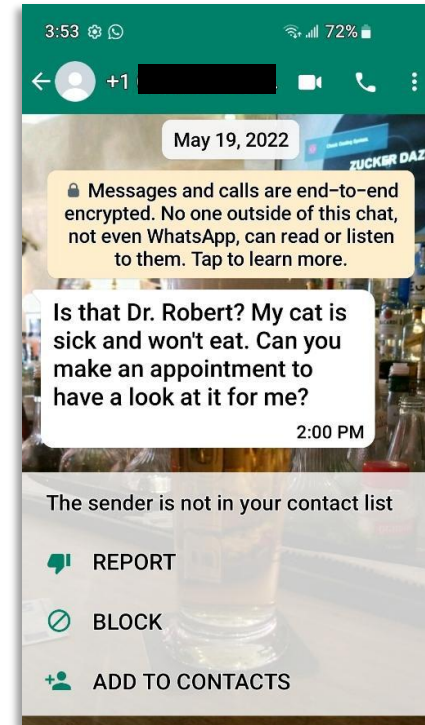
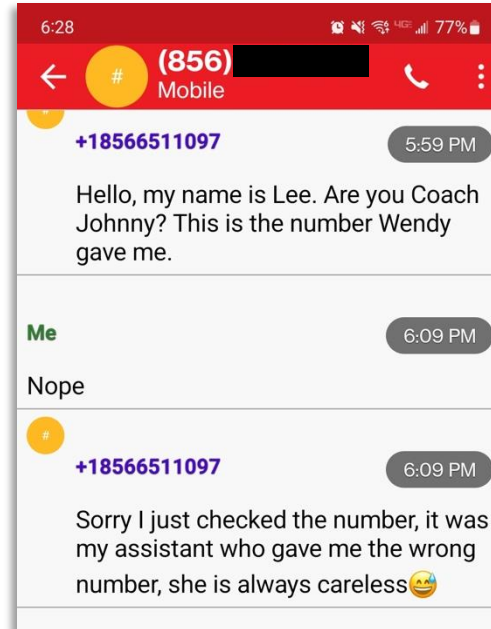
**Social Media  
Phishing**

# Smishing: Malicious Links

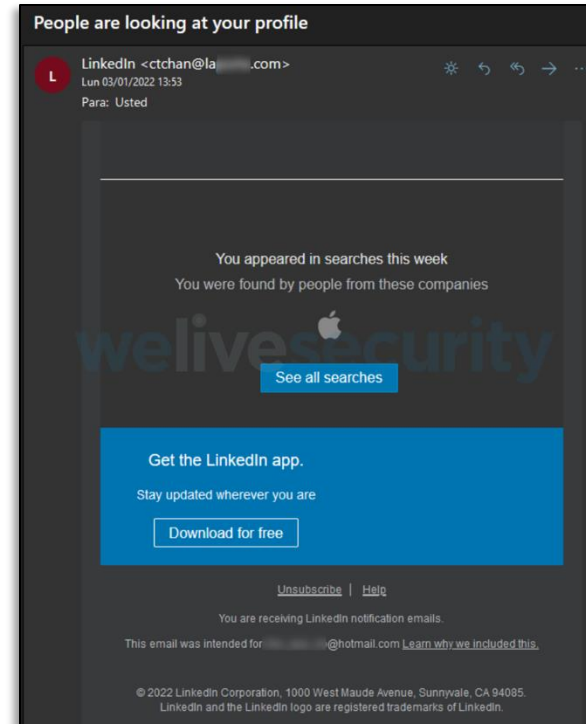
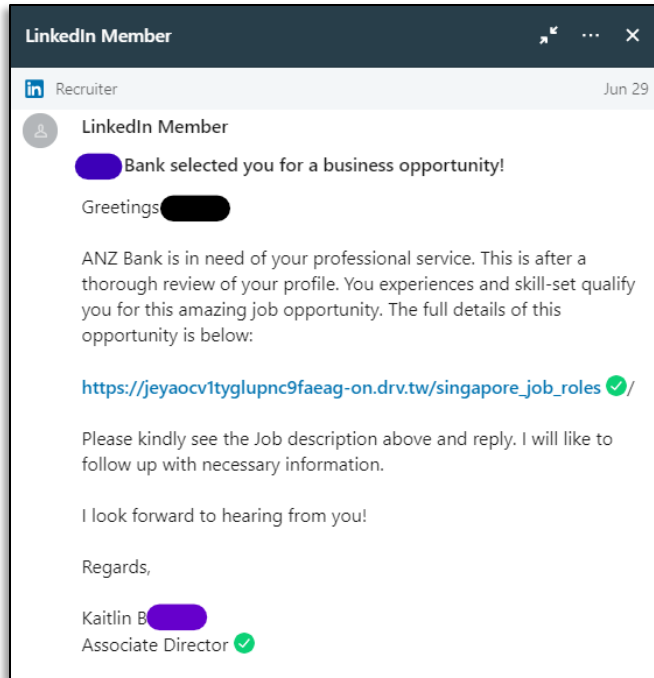




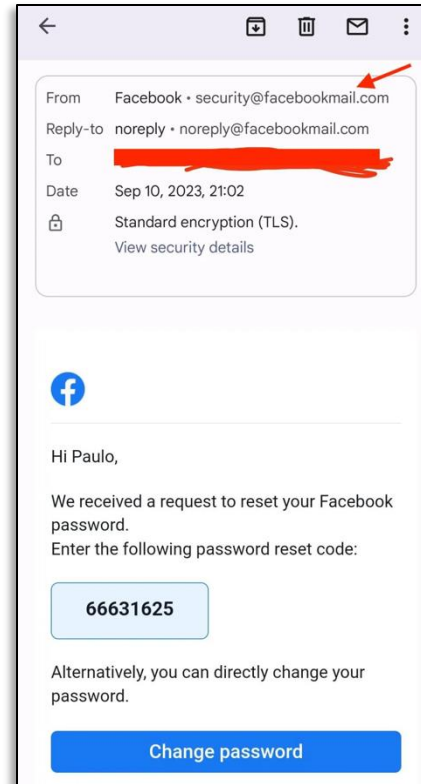
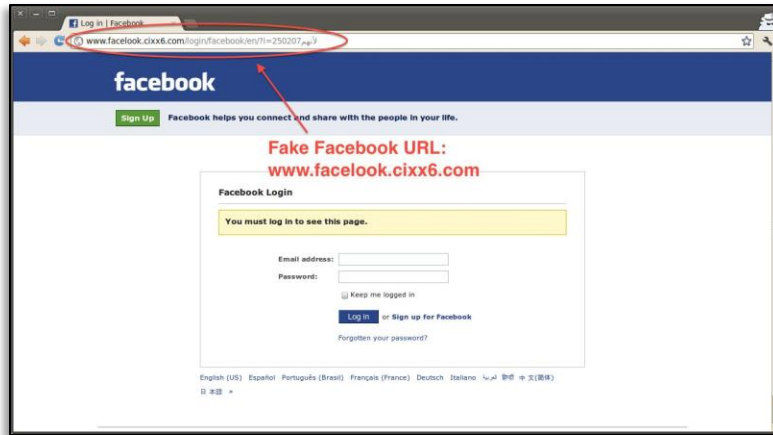
# Smishing: Conversation Scams



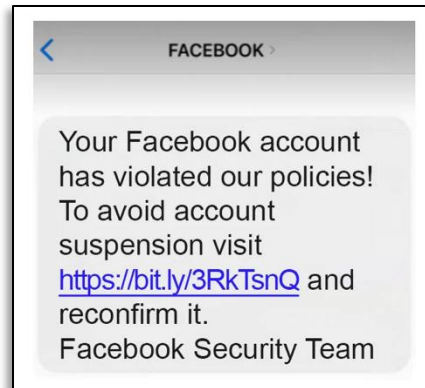
# Social Media Phishing- Examples



# Social Media Phishing- Examples



Mismatch email



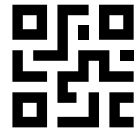


# Novel Phishing Techniques

# Novel Phishing Techniques



**BEC**



**QR Code**



**MFA Bypass**

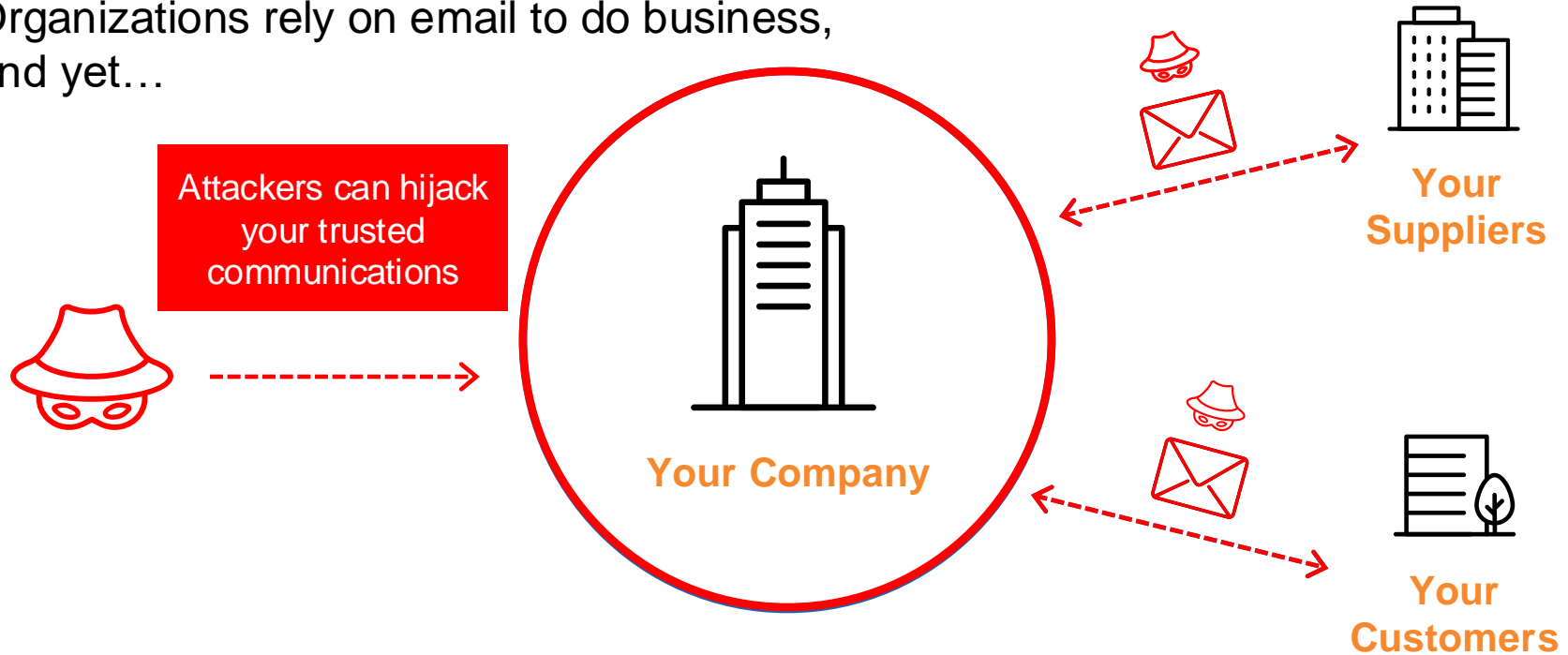


**TOAD**



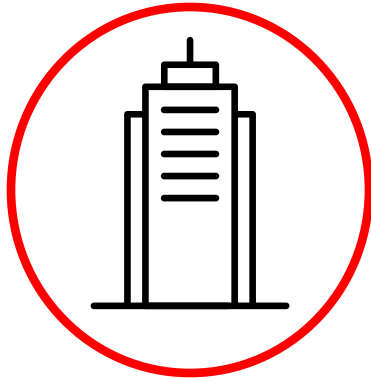
# Trusted Business Communication is Critical

Organizations rely on email to do business,  
and yet...



# Tactics to Hijack Business Communications

Either **You** or  
your **Business Partners**  
can be impersonated



## IMPERSONATION

Display Name  
Spoofing

Domain Spoofing

Lookalike Domains

Compromised  
Supplier Accounts



Your  
Suppliers



Your  
Customers



# Language no longer a barrier (Thanks GenAI)



**Gmail** 2022

**Letter of Membership**

Revived Service <abhishekvarma64w@gmail.com>  
Reply-To: abhishekvarma64w@gmail.com  
To: [REDACTED] Mon, Aug 1, 2022 at 6:42 PM

Your Subscription Resumption Attempted Successful

Thank You For Your Purchase

iMusic User: [REDACTED]

Today is your last date of your plan as it is expiring today Monday, 1st of August, 2022.

Your plan will be auto-renewed on due date 01-08-2022 with amount of \$ 77.29 from your saved card details.

Hope this musical journey gives you immense pleasure.

**MEMBERSHIP PURCHASE SUMMARY.**

APPLE ID: [REDACTED]  
Invoice Number- IN729U1691  
DUE DATE- Monday, Aug 01, 2022.  
Order ID - ORD02DB1069  
PAYMENT METHOD- Pay-Pal(Helpdesk PP-(+1(850)-542-1.8.9.1)  
Service Delivery By- Apple Inc.  
Service Received- iMusic Membership  
Service Provider- Apple In App Services  
App Renewal Fee- \$ 77.29

**Broken Language**

Fee of \$ 77.29 will be ducted on 1st August 2022 as per your chosen iMusic plan.

If you are not satisfied with our service you can request for Cancellation just reach to 542-1.8.9.1.

You can cancel your subscription just reach us on +1(850)-542-1.8.9.1.

Warm Wishes,  
The iTunes Team

2980, Peachtree Road, NE, Atlanta, 986-605, United states.

Requesting payment of USD 457 (via Razorpay) 2024

FilmyBooks <no-reply@razorpay.com>  
to me

**Payment requested by FilmyBooks**  
Payment Link Id: plink\_OA0mh6nRQA5Gs5

**Good Grammar**

We are delighted to confirm the successful renewal of your Geek Squad annual plan for \$456.87. This transaction has been processed and will soon appear on your banking statement. Your plan will be automatically renewed to ensure continued

support for your devices. If you have any questions or wish to cancel, please contact us at +1(805) 744 2764

ISSUED TO  
[twinkles@wildbranches.com](mailto:twinkles@wildbranches.com)

AMOUNT PAYABLE **USD 456.87** PROCEED TO PAY

FilmyBooks  
266 new mathnath colony hisar cannt

Sign up with [Razorpay](#) to accept payments via links for your business.  
Please report this email if you find it to be suspicious [Report Email](#)

**54%**  
CISOs think  
GenAI is a  
security risk  
in 2024

# BEC Attacks Benefit from AI



35% YoY ↑



31% YoY ↑



29% YoY ↑

**66M+** targeted BEC attacks were blocked every month on average. BEC actors have overcome the challenges of language and cultural barrier, thanks to AI.

NEWS 16 MAY 2023

## BEC Attackers Spoof CC'd Execs to Force Payment



**Phil Muncaster**

UK / EMEA News Reporter, Infosecurity Magazine

Email Phil Follow @philmuncaster



InfoSecurity Magazine, May 2023

# Impersonation tactics to pay **fake invoices**

*After initial fake invoice is sent to employee, bad actors created a sense of urgency to pay by sending **spoofed email from supervisor** requested that payment be made.*



# United Healthcare Reports Data Breach after **vendor email compromised**

Compromised supplier account communicates with United Healthcare employee regarding sensitive patient information



December 14, 2023

## UnitedHealthcare Announces Data Breach Involving Unauthorized Access to Vendor Email Account

Richard Console, Jr.  
Console and Associates, P.C.

[+ Follow](#) [Contact](#)

[in LinkedIn](#) [f Facebook](#) [X X](#) [Send](#) [Embed](#)

On December 8, 2023, UnitedHealthcare Services Inc. (“UHC”) filed a notice of data breach with the Attorney General of Montana after discovering that an unauthorized party was able to access an email account belonging to Equality Health, an Accountable Care Organization that serves some UHC members. In this notice, UHC explains that the incident resulted in an unauthorized party being able to access consumers’ sensitive information, which includes their names, dates of birth, genders, addresses, Social Security numbers, UHC member ID numbers, Medicare ID numbers, Medicare plan information, and primary care provider information. Upon completing its investigation, UHC began sending out data breach notification letters to all individuals whose information was affected by the recent data security incident.

**If you receive a data breach notification from UnitedHealthcare discussing an incident at Equality Health, it is essential you understand what is at risk and what you can do about it.** A data breach

Privacy - Terms

JD Supra Legal News, December 2023



David Bernstein of Debevoise & Plimpton. Courtesy photo

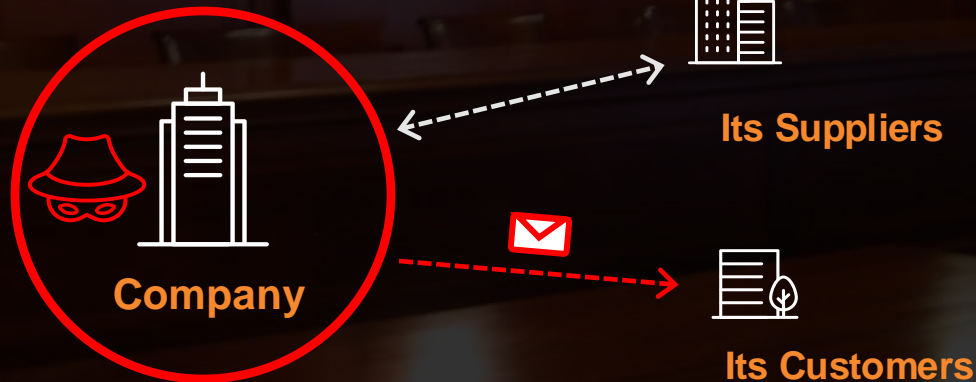
NEWS

## Debevoise Wins Cybersquatting Suit Against 2 Fraudulent Domains Impersonating Firm, Lawyers

"I think most cybercriminals realize that trying to defraud a law firm with a phishing scheme like this is not going to end well for them," said Debevoise & Plimpton's David Bernstein, the lead partner on the matter.

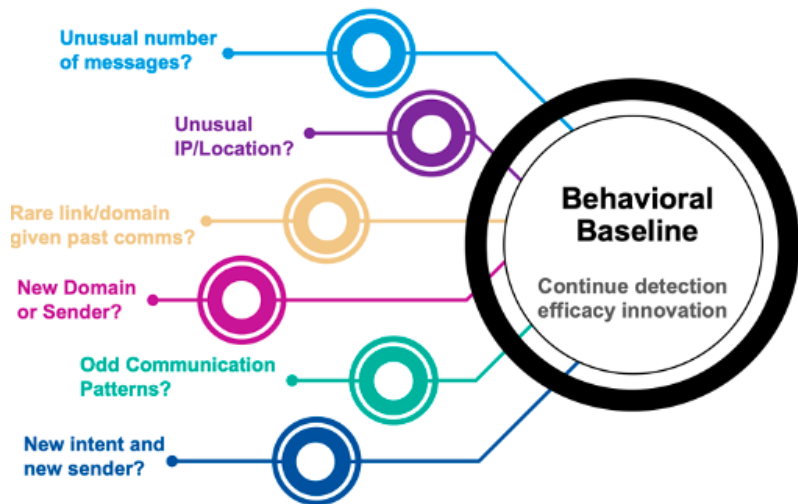
# International Law Firm Wins Legal Action After Lookalike Domains Fool Customers.

Lookalike domains spoof actual Debevoise lawyers and request "sensitive information or funds" from current customers in M&A.



# Defending against BEC

with Proofpoint Supernova





# QR Code Parking Scam



In November 2023, a 71-year-old woman was scammed out of over \$16,000 when scammers placed a fake QR code over a legitimate one on a car parking sign.

# QR Code Phishing Scam

**September 2023**

A phishing campaign attacked WashU students in an effort to gain login credentials. When the QR code in the phishing email was scanned, it redirected the victim to a fake university login page.



## Microsoft Multi-factor Authentication 2FA Set up.

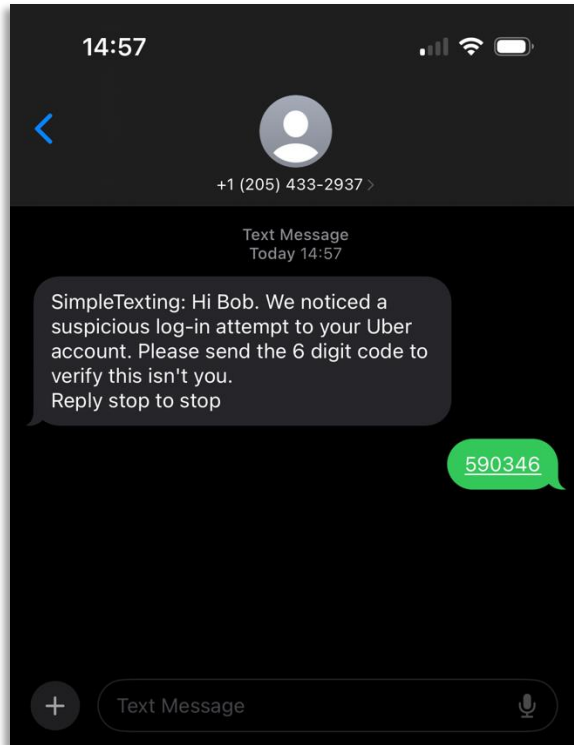
Your 2FA multi-factor settings requires review. Follow the steps below to review and verify. Quickly scan the QR Code below with your smartphone camera to re-authenticate your password security.



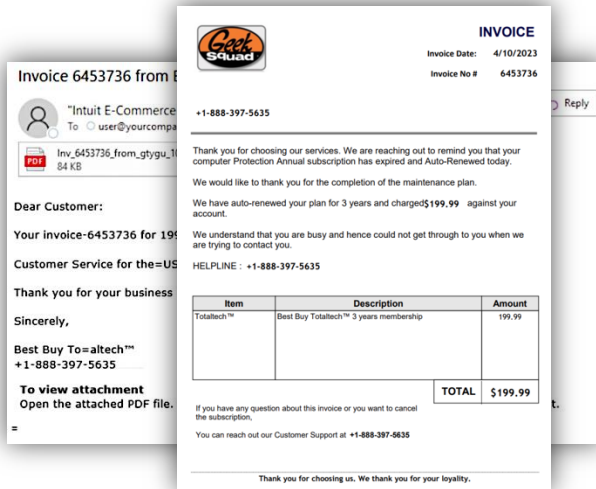
1. Scan the Microsoft QR Code using your phone camera.
2. Access your account, then go to settings.
3. Review and verify contact information and click save changes.



# MFA Bypass Scam



# TOAD Attack: Email → Phone → Attack



1

TOAD email  
received by victim

2

Victim Calls  
Support Number

3

Threat Actor Answers  
& Directs Victim

# TOAD Example: Justin Bieber

Lisa you are going to a Justin Bieber event! Your electronic ticket is ready!

Jeff Jacobsen <nitasarcdata64@aol.com>  
To: [REDACTED] Mon 8/16/2021 12:35 PM

Hi, Lisa

We're happy that you're a member of Justin Bieber JUSTICE WORLD TOUR. Make sure you get your electronic tickets below.

Your personal reference: JB205618936

Your ticket number <b>JB205618936</b> /US	T-Mobile Arena, Las Vegas, NV SUN FEB 20, 2022 - 7:30 PM SECTION - FLOOR G ROW - C SEAT - 11 Quantity - 1 FULL PRICE: 310.99 USD
---	--

**JUSTIN BIEBER**  
JUSTICE WORLD TOUR

T-Mobile AEG

This ticket can be applied as an entry pass just once, re-entry unavailable.

Be sure you get there early in order to avoid giant queues, doors for the concert will be open at 6:00 PM.

You have also applied for Missed Mondial Assistance Missed Event Insurance. A total of 10.99 USD will be charged separately by Allianz Global Assistance. You will soon receive a validation e-mail from Allianz Assistance with the policy attached.

Sadly there's a lot of illegal activity occurring, so IF YOU DIDN'T MAKE THIS TRANSACTION PLEASE CONTACT US AT +1 816 743 4566. Our customer care service will give you a hand in resolving this difficulty Monday to Friday 9:00 AM-6:00 PM.




# TOAD Example: PayPal Lure

service@paypal.com 1:47 PM  
To: PayPal User >

**If you have not ordered, reach +1 (888) 920-1081.**

Hello, PayPal User



## Invoice payment reminder

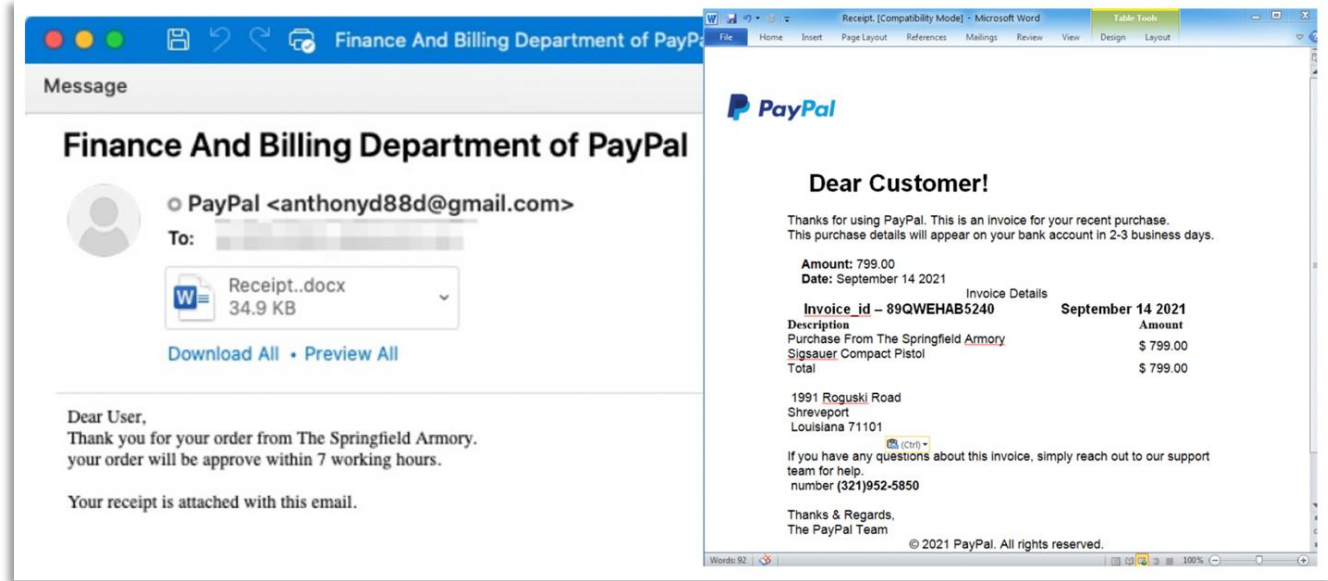
Reminder: Bill Service sent you an invoice.

Amount due: \$349.00 USD

Due on receipt

[Invoice details](#)

Amount requested



Message

**Finance And Billing Department of PayPal**

PayPal <anthonyd88d@gmail.com>

To: [Redacted]

Receipt..docx  
34.9 KB

[Download All](#) • [Preview All](#)

Dear User,  
Thank you for your order from The Springfield Armory.  
your order will be approve within 7 working hours.

Your receipt is attached with this email.

**PayPal**

### Dear Customer!

Thanks for using PayPal. This is an invoice for your recent purchase.  
This purchase details will appear on your bank account in 2-3 business days.

**Amount:** 799.00  
**Date:** September 14 2021

Invoice Details	
Invoice_id - 89QWEHAB5240	September 14 2021
<b>Description</b>	<b>Amount</b>
Purchase From The Springfield Armory	\$ 799.00
Sigsauer Compact Pistol	\$ 799.00
<b>Total</b>	<b>\$ 799.00</b>

1991 Roguski Road  
Shreveport  
Louisiana 71101

If you have any questions about this invoice, simply reach out to our support team for help.  
number (321)952-5850

Thanks & Regards,  
The PayPal Team

© 2021 PayPal. All rights reserved.

# Protecting People, Defending Data



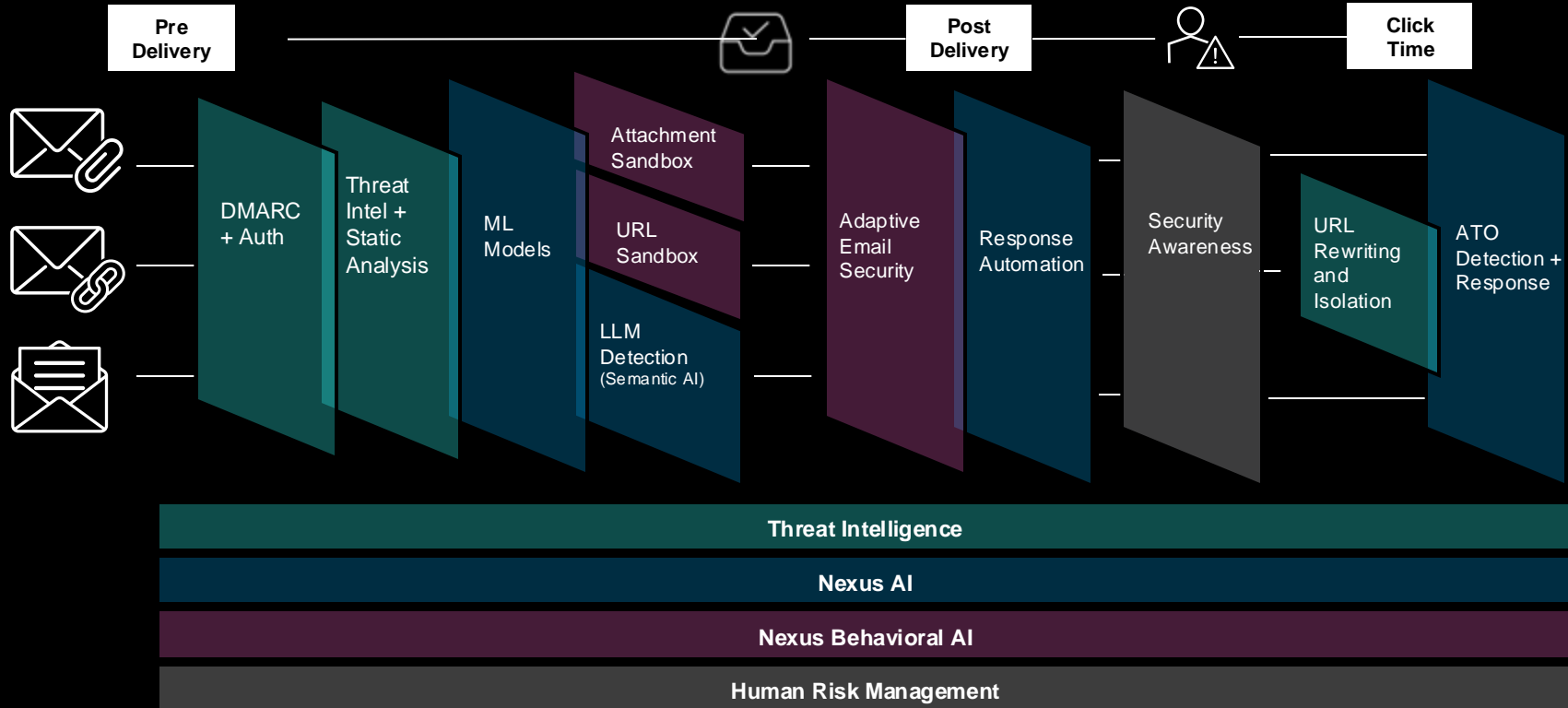
# Proofpoint

Helping over half a million customers pivot to human-centric security, including 87 of the Fortune 100.



# Proofpoint People Protection

*Redefining Email Security: End-to-end, Complete and Continuous*



# Microsoft struggles to detect phishing threats detected by Proofpoint

Active Threat Assessments behind Microsoft 2023



**Phish**

63.4% of threats detected by Proofpoint are **Phishing**



**Malware**

25.9% of threats detected by Proofpoint are **Malware**



**BEC**

6.3% of threats detected by Proofpoint are **BEC**

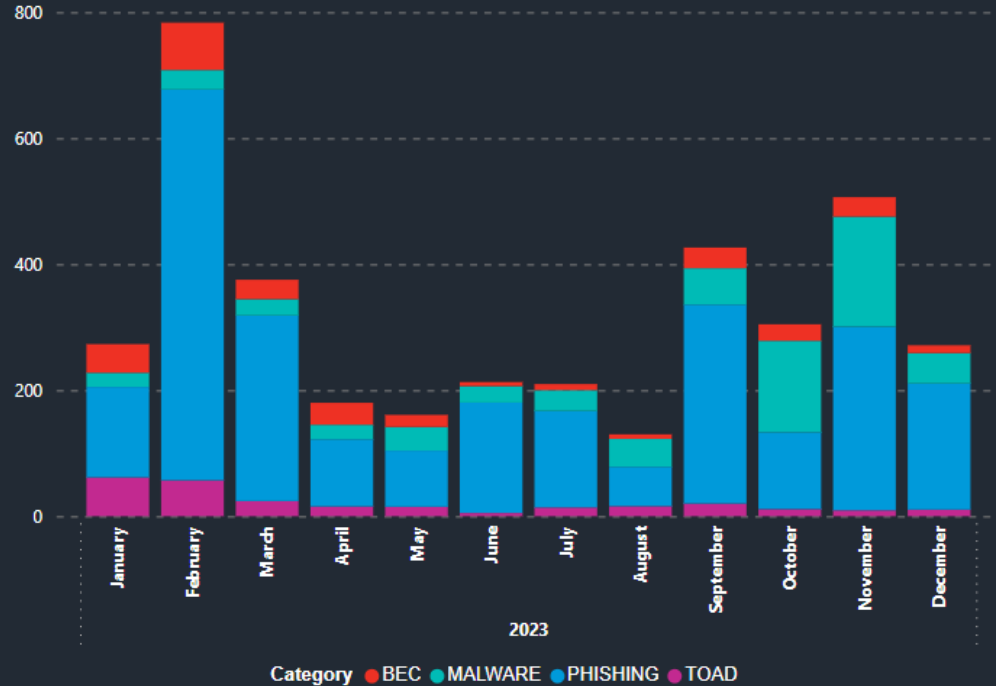


**TOAD**

4.4% of threats detected by Proofpoint are **TOAD**

Normalization: ( Total Threats Detected by Proofpoint / Sum of Unique Customer Mailboxes ) \* 1,000 mailboxes

Threats Detected by Proofpoint / 1,000 mailboxes  
Microsoft





# What's In Attackers' Playbook?



- Olympics
- Back-to-School
- COVID
- Natural disaster
- War
- Concert
- Election
- Holiday Shopping
- End of Year

The collage consists of four distinct screenshots:

- Top Left:** A charity website for disaster relief. It features a background image of a military tank and text including "MAKE A DONATION", "BECOME A VOLUNTEER", "DONATE NOW", "Our Mission: Food, Education, Medicine", and "100% DONATED".
- Top Right:** A promotional page for the Paris 2024 Olympics. It says "Welcome to the Olympics" and "Get free data packages during the Paris Olympics". It features an illustration of athletes and a "48 GB" offer. Below the illustration, it reads "To Celebrating 2024 Paris Olympics: 48GB Mobile Recharge Plans for everyone!" and "FREE 48GB DATA PLAN FOR ALL NETWORKS." with a "CLICK HERE" button.
- Bottom Left:** A Ticketmaster page for Taylor Swift's "The Eras Tour". It shows a grid of album covers and the text "TAYLOR SWIFT THE ERAS TOUR". Below the page, a news banner reads "SCAMMERS CASH IN ON TAYLOR SWIFT TICKETS".
- Bottom Right:** A news article titled "Israel-Gaza War Has Triggered More Charity Scams: Here's 4 Ways To Avoid Getting Swindled" by John F. Wasik. It includes a "Follow" button and a date of "Nov 1, 2023, 02:42pm EDT". A blue notification box says "Click to save this article. You'll be asked to sign into your Forbes account. Get it." The background of the article shows a damaged bridge.

# Protect Yourself and your Company



**Be careful what you click**



**Remember that you, your computer, your data and your services are valuable to attackers**



**Don't be shy to report your suspicions**



**Get suspicious if an email tries to elicit an emotional response**



**When in doubt – ask the security team**



# MERCI DE VOTRE ATTENTION !

**Sondage de satisfaction**  
Merci de votre feedback



**Scannez-moi**