FORTRA™

SOLUTION BRIEF *(Agari)*

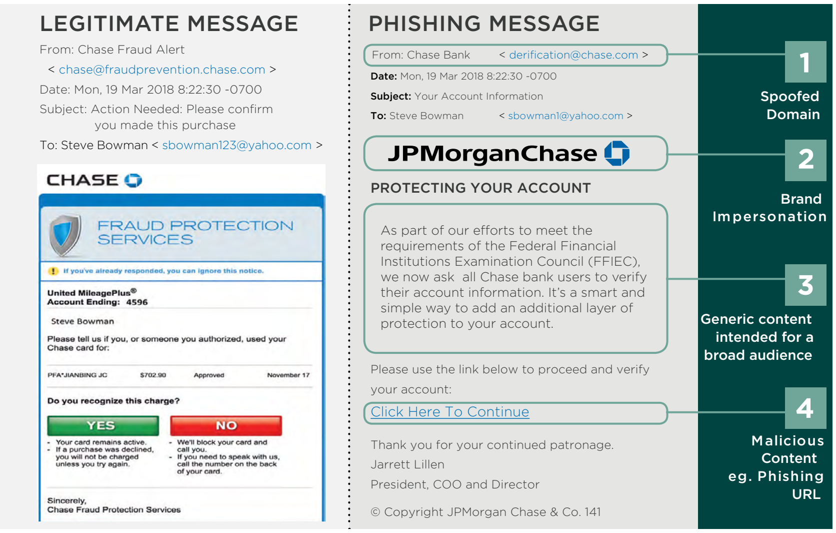
Stop Identity-Based Email Attacks

Customer Phishing, Business Email Compromise, and Account Takeover-based email attacks are three of the most damaging attacks cybercriminals are profiting from today.

Understanding The Threats

Today's modern identity-based email attacks exploit the identity of trusted colleagues and brands. However, each varies in the tactics and techniques used. Understanding the differences will be critical in being able to effectively and accurately stop these attacks.

Customer Phishing: Cybercriminals use brand impersonation techniques such as domain spoofing and malicious content such as phishing URLs to evade security controls and trick their victims. Also, keeping content generic while launching scattershot attacks allows cybercriminals to reach as many recipients as possible.



LEGITIMATE MESSAGE

From: Chase Fraud Alert
< chase@fraudprevention.chase.com >
Date: Mon, 19 Mar 2018 8:22:30 -0700
Subject: Action Needed: Please confirm you made this purchase
To: Steve Bowman < sbowman123@yahoo.com >

CHASE

FRAUD PROTECTION SERVICES

If you've already responded, you can ignore this notice.

United MileagePlus®
Account Ending: 4596

Steve Bowman

Please tell us if you, or someone you authorized, used your Chase card for:

PFA*JIANBING JC	$702.90	Approved	November 17

Do you recognize this charge?

YES
- Your card remains active.
- If a purchase was declined, you will not be charged unless you try again.

NO
- We'll block your card and call you.
- If you need to speak with us, call the number on the back of your card.

Sincerely,
Chase Fraud Protection Services

PHISHING MESSAGE

From: Chase Bank < derification@chase.com >
Date: Mon, 19 Mar 2018 8:22:30 -0700
Subject: Your Account Information
To: Steve Bowman < sbowman1@yahoo.com >

JPMorganChase

PROTECTING YOUR ACCOUNT

As part of our efforts to meet the requirements of the Federal Financial Institutions Examination Council (FFIEC), we now ask all Chase bank users to verify their account information. It's a smart and simple way to add an additional layer of protection to your account.

Please use the link below to proceed and verify your account:

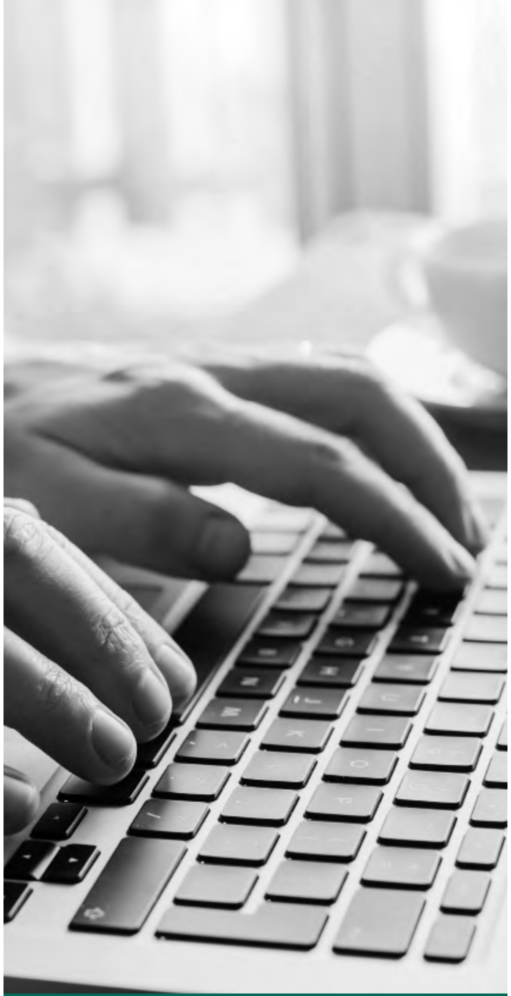
Click Here To Continue

Thank you for your continued patronage.
Jarrett Lillen
President, COO and Director

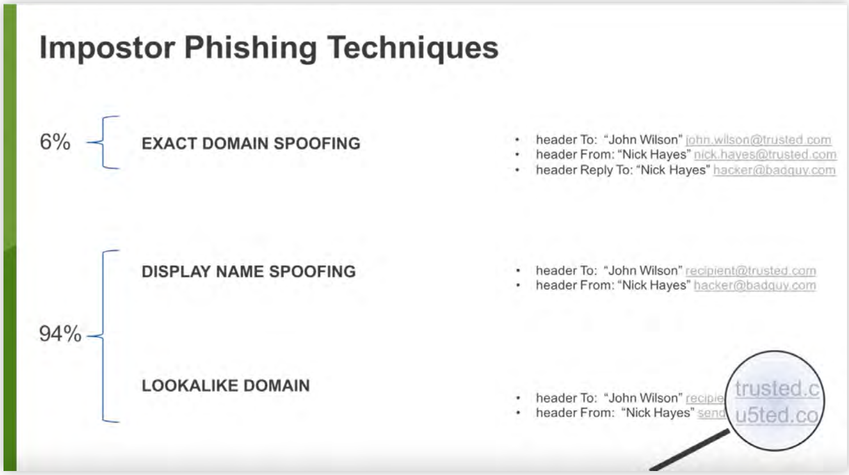
© Copyright JPMorgan Chase & Co. 141

1
Spoofed Domain
2
Brand Impersonation
3
Generic content intended for a broad audience
4
Malicious Content eg. Phishing URL

Business Email Compromise: BEC attacks differ from customer phishing by targeting employees of an organization. These targeted attacks inherently use identity deception, requiring no malicious content, such as phishing URLs or malware. BEC relies on three deception techniques: Display Name Imposter (DNI), Domain Spoofing, and Look-alike Domains. While all these routinely bypass Secure Email Gateways that by design look for malicious content, DNI-based attacks are the most effective.



> ***"Using Agari, we stopped 1.4 million potentially fraudulent emails from being delivered to customers per month."***
>
> — Security Manager, Global 500 Financial Services Company



Impostor Phishing Techniques

6% — EXACT DOMAIN SPOOFING

- header To: "John Wilson" john.wilson@trusted.com
- header From: "Nick Hayes" nick.hayes@trusted.com
- header Reply To: "Nick Hayes" hacker@badguy.com

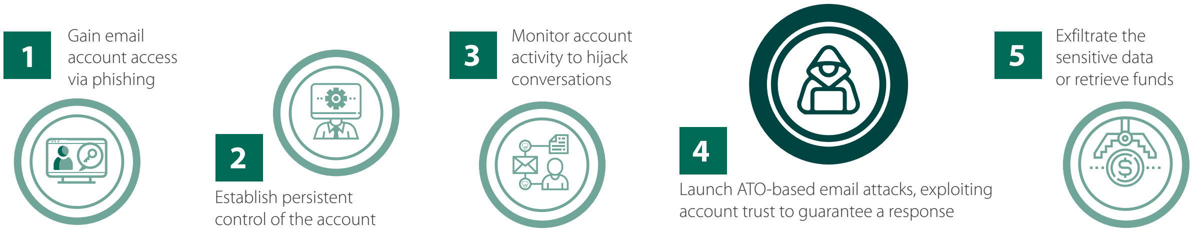
94% — DISPLAY NAME SPOOFING

- header To: "John Wilson" recipient@trusted.com
- header From: "Nick Hayes" hacker@badguy.com

LOOKALIKE DOMAIN

- header To: "John Wilson" recipie
- header From: "Nick Hayes" send

Account Takeover (ATO)-Based Email Attacks: Cybercrimals use a multi-step process that initially compromises a previously established credible email account to launch subsequent targeted attacks such as BEC, spear phishing, or ransomware. ATO-based email attacks exploit the existing trust between the compromised account and its known contacts, which increases the cybercriminal's success rate.



1 Gain email account access via phishing

2 Establish persistent control of the account

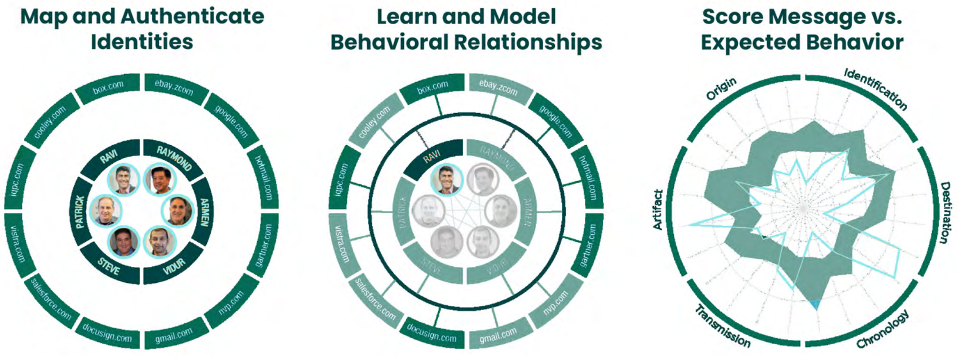
3 Monitor account activity to hijack conversations

4 Launch ATO-based email attacks, exploiting account trust to guarantee a response

5 Exfiltrate the sensitive data or retrieve funds

Fortra Advanced Email Security

Fortra Advanced Email Security is the most comprehensive email security architecture that detects, defends against, and deters advanced identity-based email attacks. With the Fortra Identity Graph at its core, the solution leverages a high-performance graph database of relationships and behavioral patterns between individuals, brands, businesses, services, and domains using hundreds of characteristics to maintain a real-time understanding of trusted communications to stop these attacks.



Map and Authenticate Identities

Learn and Model Behavioral Relationships

Score Message vs. Expected Behavior

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

FORTRA™

Fortra.com