



Webinar

Protecting New Deals from Wire Fraud

April 9th, 2020

SPEAKERS AND BIOS



Chris Hueneke
Chief Information Security
Officer *RKON*
CHueneke@RKON.com

Chris Hueneke, Chief Information Security Officer at RKON, is an IT security leader with over 25 years of experience in the industry. His professional experience includes advising and implementing global IT governance, risk, compliance and security control frameworks and solutions. He has diverse IT risk and security experience protecting international organizations throughout the world for industries such as private equity, financial services, retail, manufacturing, and airlines. Chris' extensive global leadership experience includes building IT risk and security teams from the ground up and consulting on improvements in endpoint, perimeter, datacenter, and cloud security architectures. He is a visionary leader able to communicate technology strategy, compliance, architecture, and critical risks effectively to key stakeholders, executive leadership, and boards of directors.



Joe Mullarkey
Security Consultant
RKON
JoeMullarkey@RKON.com

Joe Mullarkey is an IT security professional with over 25 years of experience in the industry. He has extensive experience in messaging and identity risk management. He is a Certified Information Systems Security Professional as well as a Microsoft 365 Certified Enterprise Administrator Expert. Joe is also a Microsoft Certified Trainer with extensive presentation experience in shaping complex technology into accessible topics. He has over 20 years of experience managing SMTP systems and holds the Microsoft Certified Solutions Expert credential in messaging. Joe is currently a security consultant with RKON Technologies specializing in messaging and identity management.

SHARK TANK HOST LOSES \$400K IN EMAIL SCAM

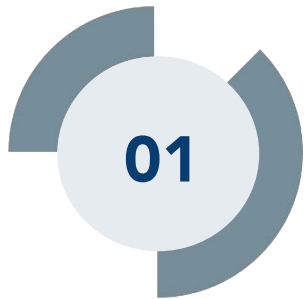


New York (CNN Business) - "Shark Tank" judge Barbara Corcoran lost nearly \$400,000 in an elaborate email scam that tricked her staff.

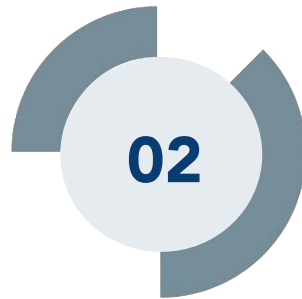
Corcoran said someone acting as her assistant sent an invoice to her bookkeeper earlier this week for a renovation payment. She told People that she had "no reason to be suspicious" about the email because she invests in real estate. So the bookkeeper wired \$388,700 to the email address.

- Hackers used publicly available information and email scam to pose as a credible source and tricked her organization into wiring money - she was not hacked into
- Hackers used "Whaling" techniques to target the executive - *"Shark Tank Judge got Whaled"*
- Barbara Corcoran may not be in the Private Equity arena, but nevertheless she fell victim to the exact same process that is being used to target newly formed organizations as a result of Merger and Acquisition activities

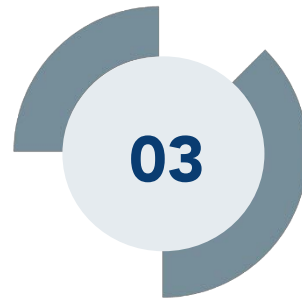
WEBINAR AGENDA



Why Attackers
Are Targeting
Private Equity



Email
Impersonation:
Primary Attack
Method



Email Fraud
Examples



Typical Wire
Fraud Steps
and Examples



Prevention
Checklist and
Best Practices



01

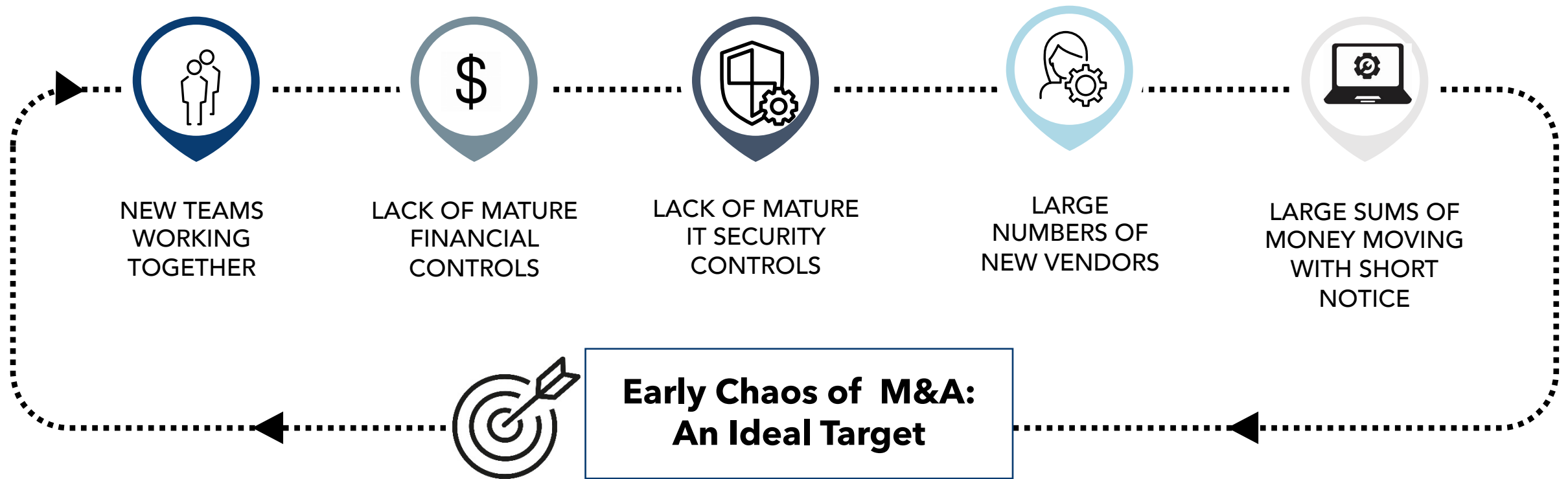
Why Are Attackers Targeting Private Equity?

Cyber Crime IS A \$26 BILLION INDUSTRY

Common Attack Scenarios

- 1. CEO Impersonation:** These scams usually involve the use of a spoofed/faked email from the CEO to a financial executive asking for funds for a new business venture or forgotten payment that is due.
- 2. Vendor or Supplier Impersonation:** These scams involve the redirection of funds from long-standing wire-transfer relationships
- 3. Payroll Redirect:** These scams involve the redirection of wage payments through a direct-deposit bank account modification
- 4. Employee Information Theft:** These newer scams involve attempts to trick HR or payroll personnel into transferring wage, W-2 forms, or other personal employee information which can be sold on the dark web
- 5. IT Impersonation:** These scams involve tricking company personnel into installing malware or revealing passwords
- 6. Attorney Impersonation:** These scams involve fraudsters pretending to be lawyers acting on behalf of the CEO and requesting confidential information

WHY ARE ATTACKERS TARGETING NEW M&A DEALS



- Attackers focus on "C" Level and Financial leaders in new M&A Transactions.
- People involved in new M&A are already prepared for the unexpected and are less likely to question things that would be red flags after normal business operations are established deeper into the hold period.

WHO IS BEING TARGETED?

Attackers are targeting specific groups within Newco's formed by recent M&A activities

01

CEO

Does the CEO know who is sending email on their behalf?

02

Financial Teams

Does the Financial Team know who they are working with on the phone and receiving email?

03

Human Resources

Does the Human Resources team know who is requesting employee W-2s?

04

IT Users

Does the IT User know who, claiming to be from the IT Help Desk, is requesting their password, personal information and credit card details?

RESULT: ITALIAN ENERGY FIRM TECNIMONT LOST \$18.6 MILLION

- Tecnimont is a \$3.6 billion Italian group with 50 operating companies in the oil and gas sector
- Attackers stole \$18.6 million by convincing local managers that the money was needed for an acquisition

SPOOFED EMAIL



Head of Tecnimont subsidiary received a spoofed email purportedly from the "global chairman"

WIRE TRANSFER



Hackers convinced the Tecnimont subsidiary head to transfer a total of \$18.6 million to Hong Kong banks

FRAUD DETECTED



Fraud was finally detected on the fourth attempted wire-transfer and stopped

SPOOFED PHONE CALLS



Hackers arranged a series of conference calls to discuss a "secretive" and "highly confidential" acquisition

MONEY COLLECTED



Money was immediately withdrawn from the bank by the attacker



02

Email Impersonation: Primary Attack Method

Business Email Compromise and Wire Fraud

Phishing: Email Impersonation **Targeting Mass Audience**

Attackers sending emails impersonating reputable parties in order to induce many employees to reveal personal information, such as passwords and credit card numbers

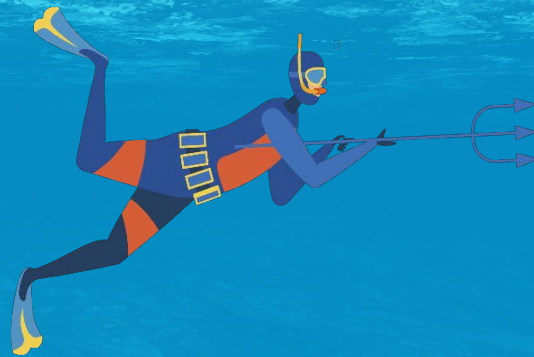
Whaling: Email Impersonation **Targeting specific high value targets**

Attackers spear phishing a specific high value target such as a C-Suite individual, usually spoofing email as a precursor to wire fraud.

Employees



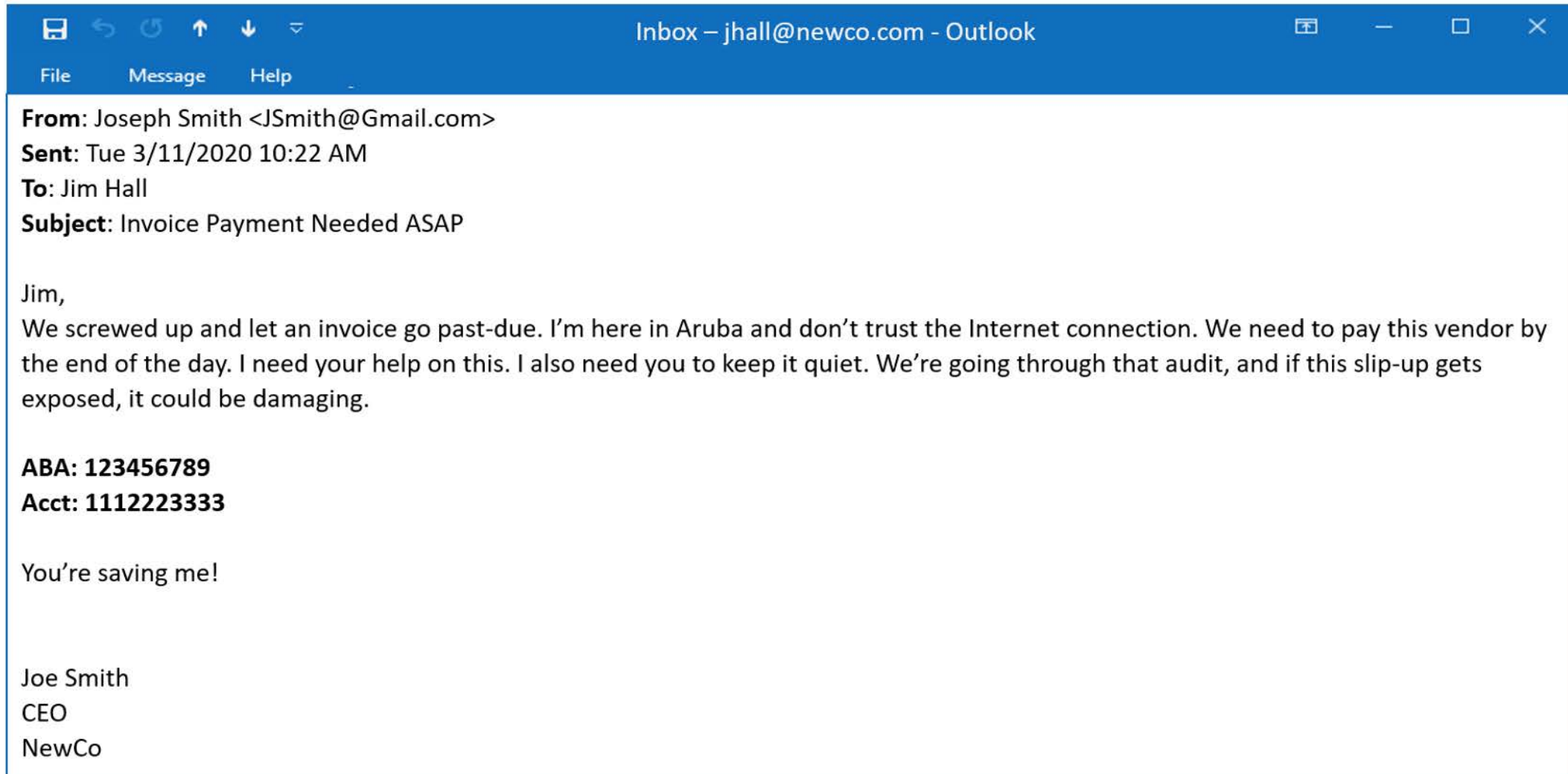
Attackers



C-Suite

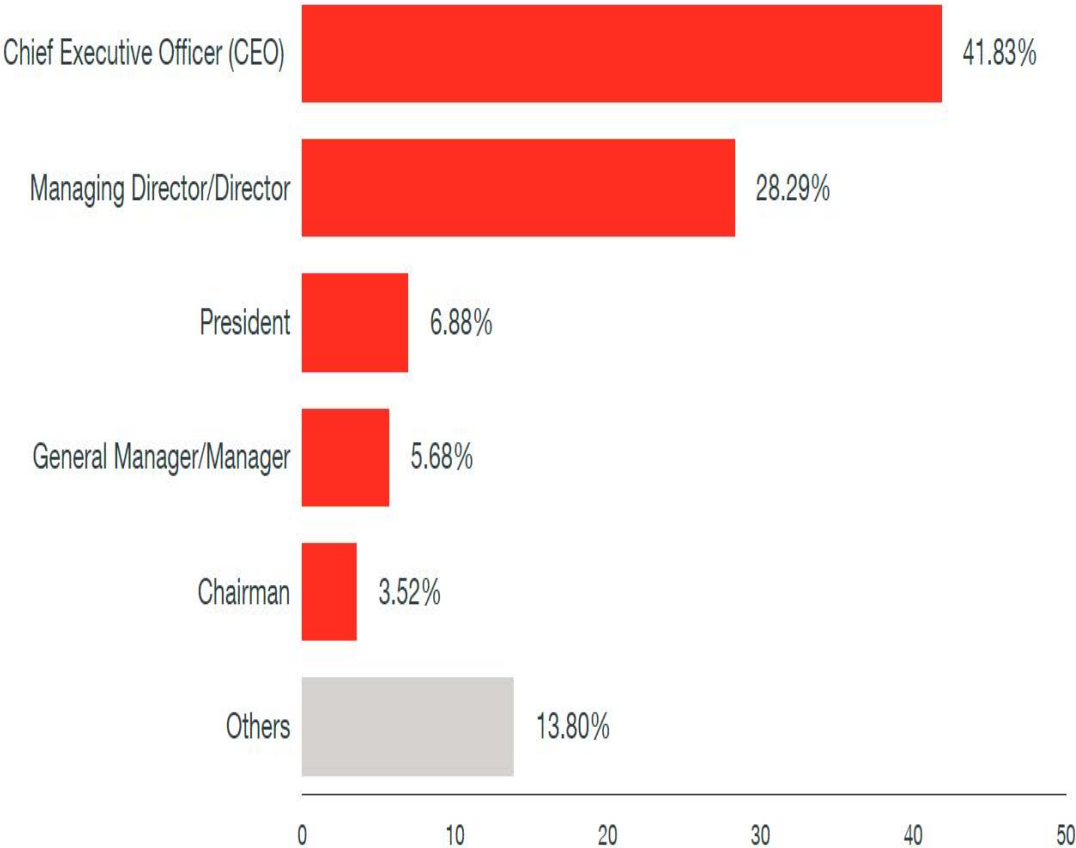


ATTACKERS IMPERSONATING CEO EMAIL

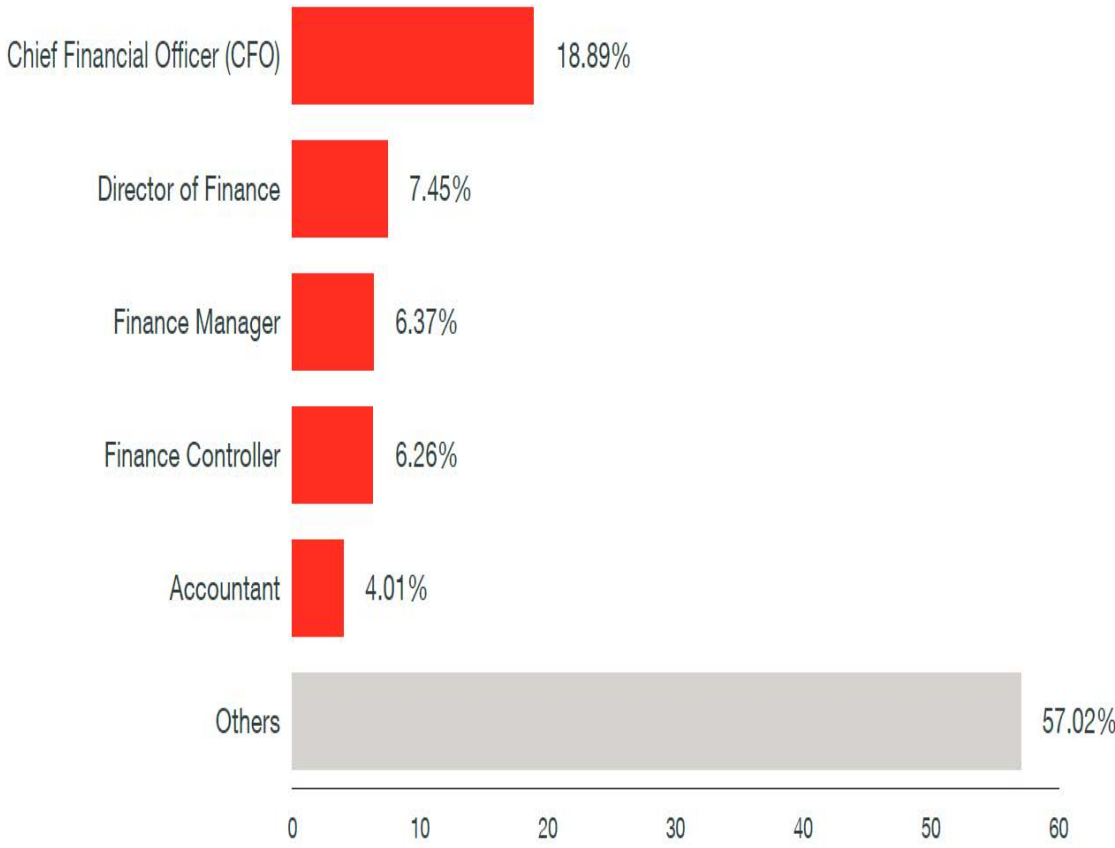


EXECUTIVE LEADERSHIP TARGETED BY ATTACKERS

Spooferd Email From:



Targeted Email To:






03

Email Fraud Examples

WIRE FRAUD SIGNS


Inbox – jhall@newco.com - Outlook

File Message Help

From: Joseph Smith <JSmith@Gmail.com>  **Personal email address**


Sent: Tue 3/11/2020 10:22 AM


To: Jim Hall

Subject: Invoice Payment Needed ASAP  **Urgency**

Jim,

We screwed up and let an invoice go past-due. I'm here in Aruba and don't trust the Internet connection. We need to pay this vendor by the end of the day. I need your help on this. I also need you to keep it quiet. We're going through that audit, and if this slip-up gets exposed, it could be damaging.

ABA: 123456789  **Secrecy**

Acct: 1112223333  **Scare Tactics**

You're saving me!

Joe Smith
CEO
NewCo

PAYROLL DEPOSIT REDIRECT SIGNS

Inbox – Sjones@newco.com - Outlook

File Message Help

From: Jim Peterson <Jim.Peterson@NewCo.com>
Sent: Thu 3/12/2020 11:35 AM
To: Sue Jones
Subject: Change in my Bank Account Number

Hi Sue,

Secrecy and favors ↙

Urgency ↘

I screwed up! (don't tell anyone, please 😊) I recently changed my bank account and forgot to put a change in. Payday is tomorrow, though, and I'm afraid my direct deposit will go to the wrong place. This could be embarrassing for me and I need your help. I have the new routing and account numbers. Normally, I know we need a test transfer of a dollar, but the way I set up my account doesn't allow that. I'm closing on a house and I need that check! I'll let you know if there's a problem on my end.

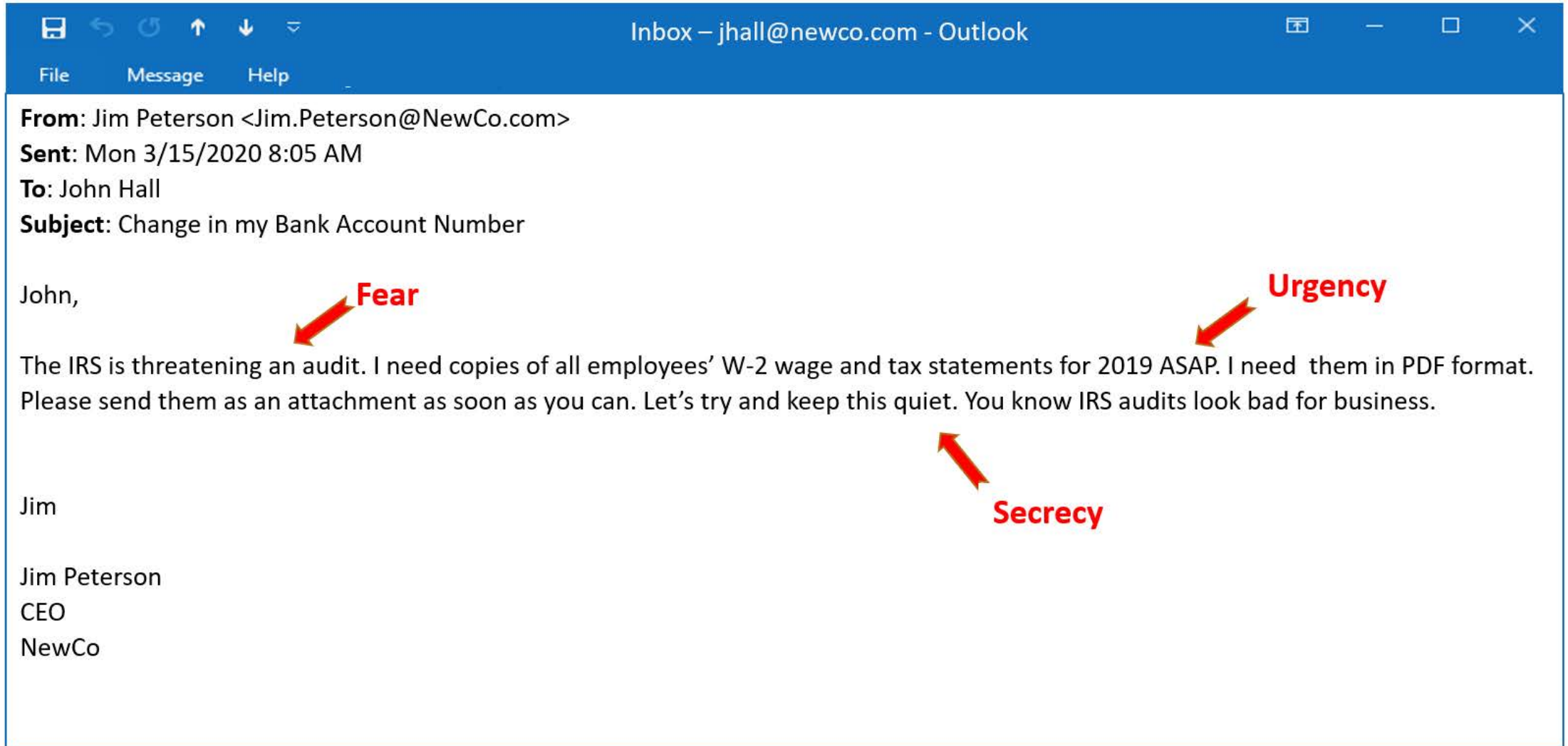
Scare tactics ↙

ABA: 123456789
Acct: 1112223333

You're saving me!

Jim Peterson
CEO
NewCo

EMPLOYEE INFORMATION THEFT SIGNS



Inbox – jhall@newco.com - Outlook

File Message Help

From: Jim Peterson <Jim.Peterson@NewCo.com>
Sent: Mon 3/15/2020 8:05 AM
To: John Hall
Subject: Change in my Bank Account Number

John,

Fear

The IRS is threatening an audit. I need copies of all employees' W-2 wage and tax statements for 2019 ASAP. I need them in PDF format. Please send them as an attachment as soon as you can. Let's try and keep this quiet. You know IRS audits look bad for business.

Urgency

Secrecy

Jim

Jim Peterson
CEO
NewCo



04

Typical Wire Fraud Steps and Examples

HOW A TYPICAL WIRE FRAUD IS CARRIED OUT

STEP 1

PUBLIC INFORMATION

Criminals become aware of the target company by using publicly available deal information

STEP 2

TARGETED RESEARCH

Criminals perform due-diligence and research on the target company

STEP 3

PLANNING

Criminals develop a plan of attack

STEP 4

EXECUTE

Criminals execute the attack






STEP 1: BEGINS WITH PUBLICLY AVAILABLE DEAL INFORMATION

Hackers are subscribing to Private Equity publications and searching for deals where a new team is likely working together for the first time (like a carve-out)

PUBLIC INFORMATION

Deal #6: IPO, \$125M, Completed; 03-Oct-2014

Deal Types	IPO, PIPE	Total Invested Equity	\$125.00M
Deal Amount	\$125.00M	Stock Split	5.8 : 1
Deal Status	Completed	Total Invested Capital	\$125.00M
Deal Date	03-Oct-2014	Pre-money Valuation	\$184.16M
Announced Date	27-Aug-2014	Post Valuation	\$309.16M ^E
Financing Status	Formerly VC-backed	CEO/Lead MGT	Thomas Wiggans  
Financing Source	Public Investment	Site	Menlo Park, CA
Raised to Date 	\$260.50M ^{**}	Business Status	Clinical Trials - Phase 3

Phone numbers, email addresses and co-workers on the leadership team gives hackers all they need to find and impersonate decision makers

EXECUTIVES

Team (17)

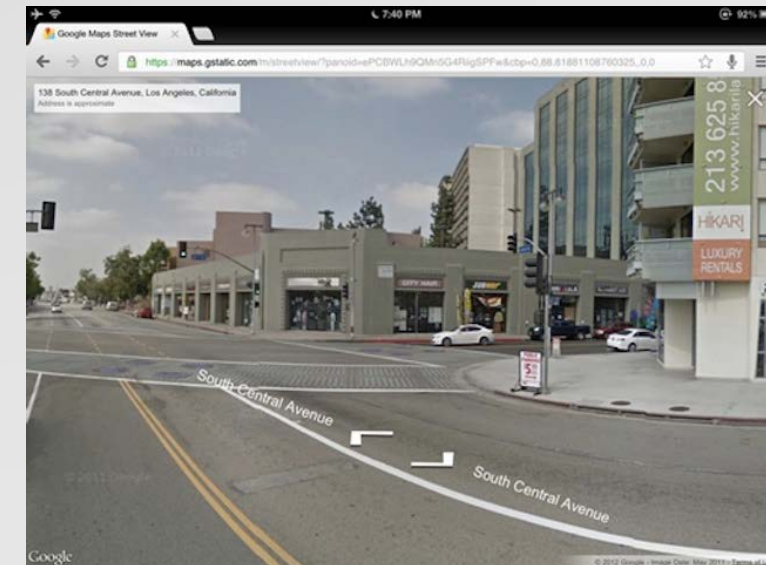
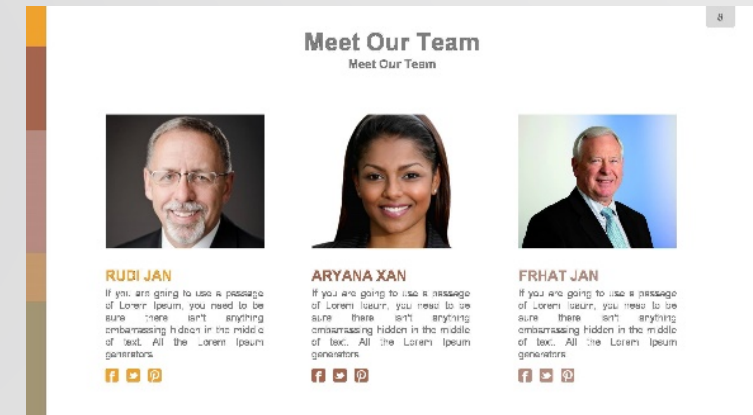
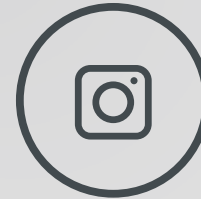
Current Team (8) Former Team (9)

Name	Title	Board Seats	Office	twiggans@dermira.com
Thomas Wiggans	Chief Executive Officer & ...	1	Menlo Park, CA	   
Andrew Guggenhime	Chief Financial Officer & ^{Text}	1	Menlo Park, CA	   
Chris Griffith	Co-Founder, Chief Busine...		Menlo Park, CA	   
Luis Peña	Co-Founder and Chief De...		Menlo Park, CA	   

STEP 2: RESEARCH OF HIGH-VALUE TARGET

- 1. Performing Internet searches to find information and news reports available on the company**
 - Merger and acquisitions taking place
 - Company leadership and organizational structure
 - Key vendors and business partners conducting transactions
- 2. Searching and combing through social media sources**
 - Friends and colleagues
 - Job history and education
 - Vacations
 - Personal likes and dislikes
- 3. Conducting physical reconnaissance**
 - Google Maps view of company office to identify areas of physical vulnerabilities and signage
 - Local coffee shop reconnaissance to perform shoulder surfing or place malicious USB drive

RESEARCH



STEP 3: ATTACK PLAN DEVELOPMENT

1. Registering look-alike web site and email domains to be leveraged in the attack
2. Identifying specific financial transactions to target identified from research
 - Vendors and business partners with focus on wire transactions
 - Payroll deposits
 - Specific mergers and acquisitions
3. Leveraging data collected from physical surveillance of leadership
 - Observations overheard within confidential conversations in airports, airplanes, and coffee shops
 - Intentional USB device drops collecting confidential data from PC
4. Preliminary spear-phishing with links and downloads designed to steal passwords
 - Attempt to steal passwords or gain visibility into device or cloud email/applications
 - Attempt to steal passwords of colleagues and contacts

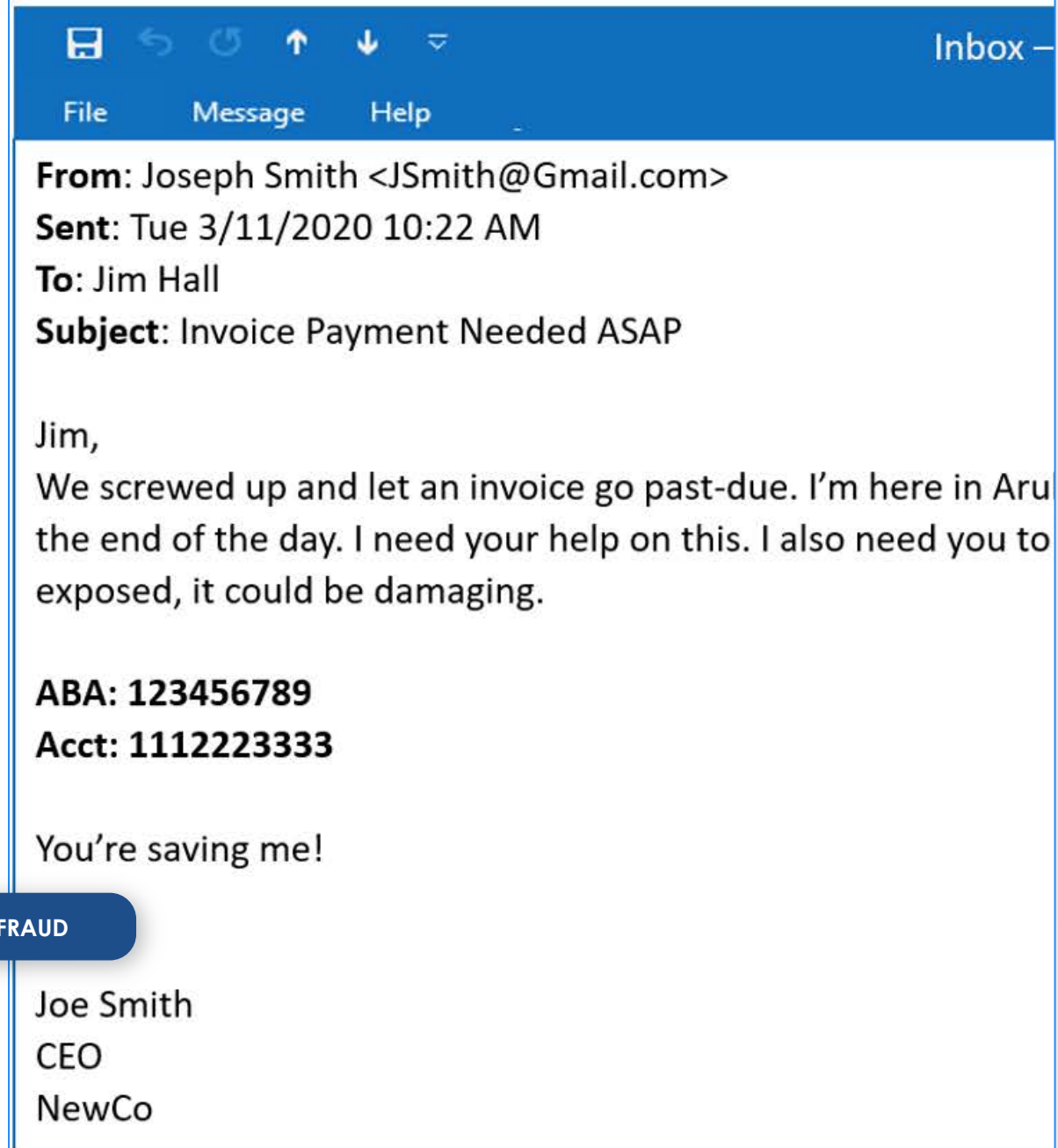
THE PLAN



STEP 4: EXECUTE ATTACK

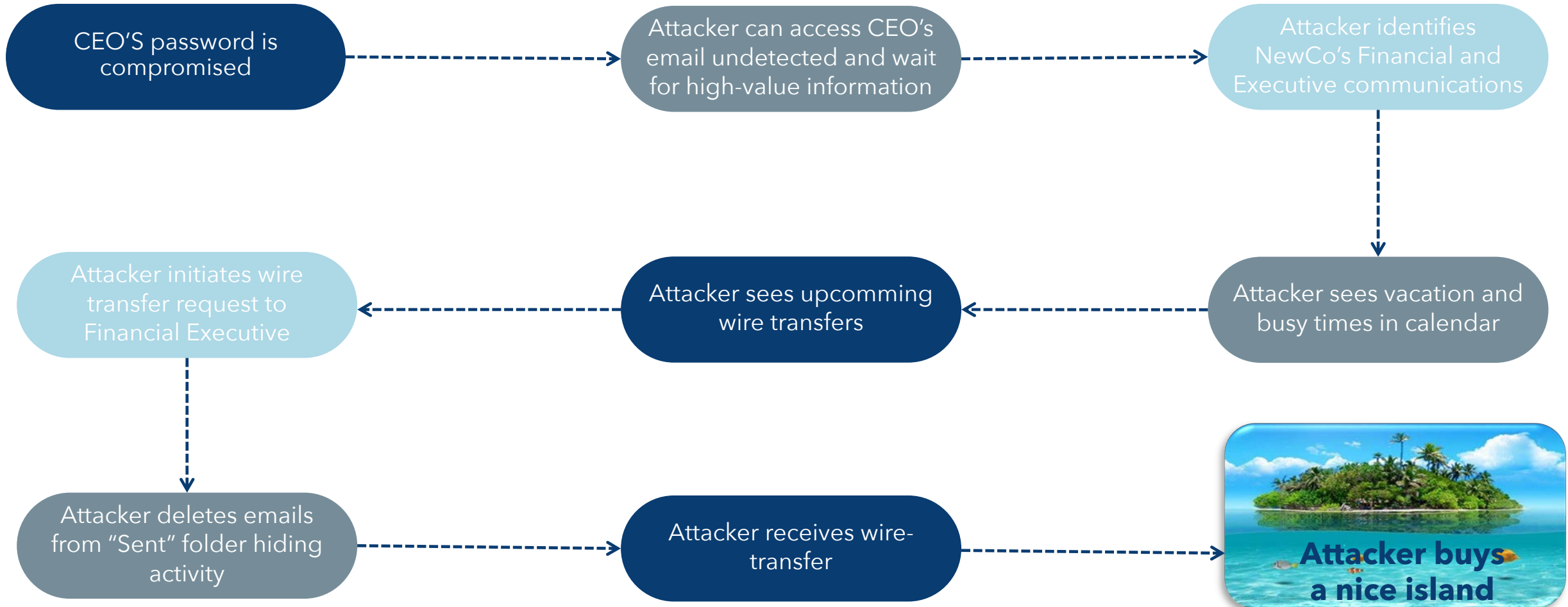
1. **CEO impersonation email** scam designed to implement financial wire-fraud
2. **HR impersonation email** scam designed to acquire employee information including W2's
3. **Executive employee impersonation email** scam designed to target Accounting to redirect payroll deposit to attacker's account
4. **IT Help Desk impersonation email and phone** scam designed to acquire control over victim's machine or steal passwords, personal information, bank account details

THE FRAUD



EXECUTION OF WIRE FRAUD VIA EMAIL

THE ISLAND PATH



CAN YOU TRUST THE **FROM** ADDRESS?

- ✓ JSmith@NewC0.com **That's a Zero!**
- ✓ Jsmith@Gmail.com **That's Gmail account!**
- ✓ Jsmith@NewCo.com **That's perfect! Uh-oh.**

Bottom line, you cannot trust the "From:" address

- Savvy attackers can directly manipulate the "From:" address
- Recipient unable to spot the discrepancy
- Sender unaware their password has been stolen
- Lack of email authentication protocol adoption

WHAT TO DO IF YOU ARE A VICTIM OF WIRE FRAUD

1. Report to executive leadership
2. Invoke Incident Response Plan if it exists
3. Contact both sending and receiving banks IMMEDIATELY and request a recall
 - Time is a factor in stopping the transfer
4. If the transfer was international, request the banks initiate a SWIFT GPI recall
 - High value SWIFT transactions may qualify for the FBI Financial Fraud Kill Chain
5. Inform business partners that were involved
6. Verify wire recall or SWIFT GPI recall has been initiated
7. Document everything
8. Report the incident to the authorities





05

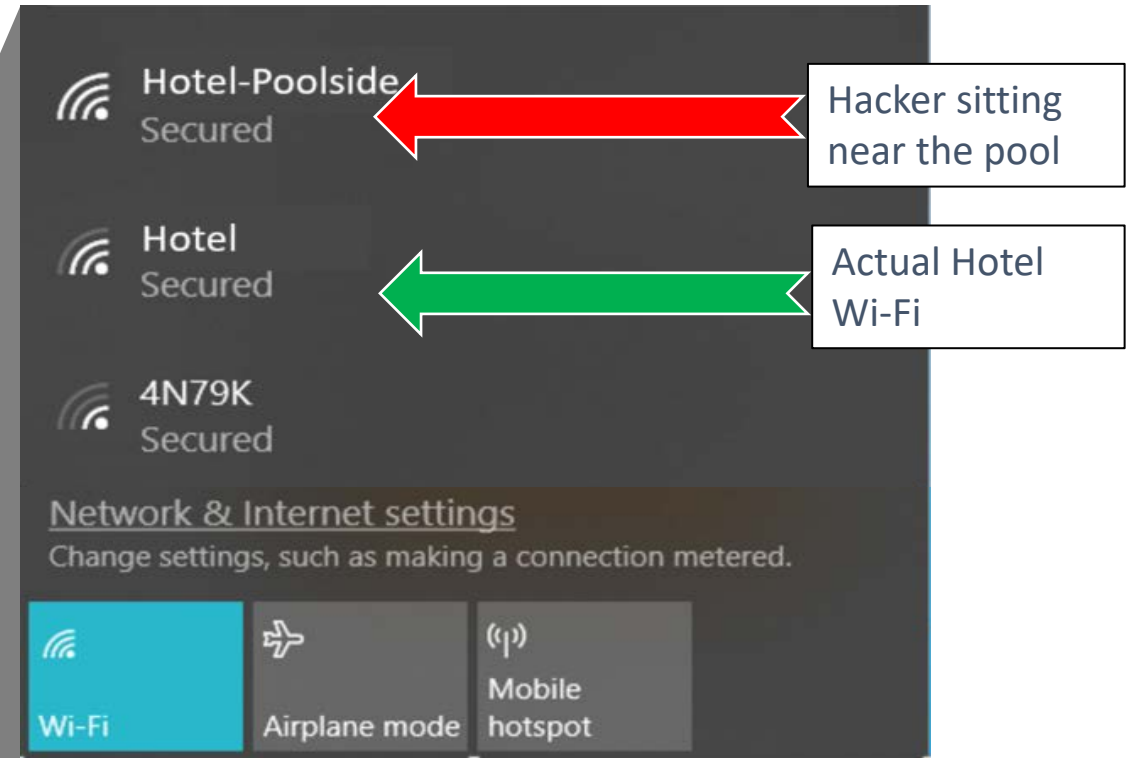
Prevention Checklist and Best Practices

DO'S AND DON'TS TO PREVENT WIRE FRAUD

WIRE FRAUD PREVENTION CHECKLIST	
✓	Implement two-step verification such as a phone call or a face-to-face visit for the following: <ul style="list-style-type: none">• New or Changed Wire Transfers, Employee Information Requests, Direct Deposit Change Requests, Vendor Payment Change Requests
✓	Limit number of people who are authorized to complete transfers and inform employees as to who is authorized to initiate transfers – establish internal department rules to follow up with phone call
✓	Never communicate to or from personal Email addresses
✓	Never give your password to personnel from the help desk or IT – use password self-service reset
✓	Be cautious when clicking on links and downloading attachments in email
✓	Don't follow links in email requesting to change passwords - visit the website by typing the address yourself
✓	Don't post company information or vacation schedules on social media
✓	Don't insert unknown USB thumb drives into any computer
✓	Be aware of the criminal presence and malicious wireless networks in public spaces

PUBLIC WIFI NETWORK RISK

- Hackers can sit quietly with their laptops nearby and create look-alike Wi-Fi networks
- Ask hotel or coffee shop for the exact name of the Wi-Fi networks



IT SECURITY SOLUTIONS TO MITIGATE WIRE FRAUD

- **Advanced Email Security**

- Email content filtering inspecting for malicious web links and attachments
- Block phishing and spoofing attempts
- End user awareness training with phishing simulations
- Block embedded email trackers (spymail)
- Reveal hidden risks within email alerting users



- **Multi-Factor Authentication**

- Something you know, have, and are
- Protect against stolen passwords

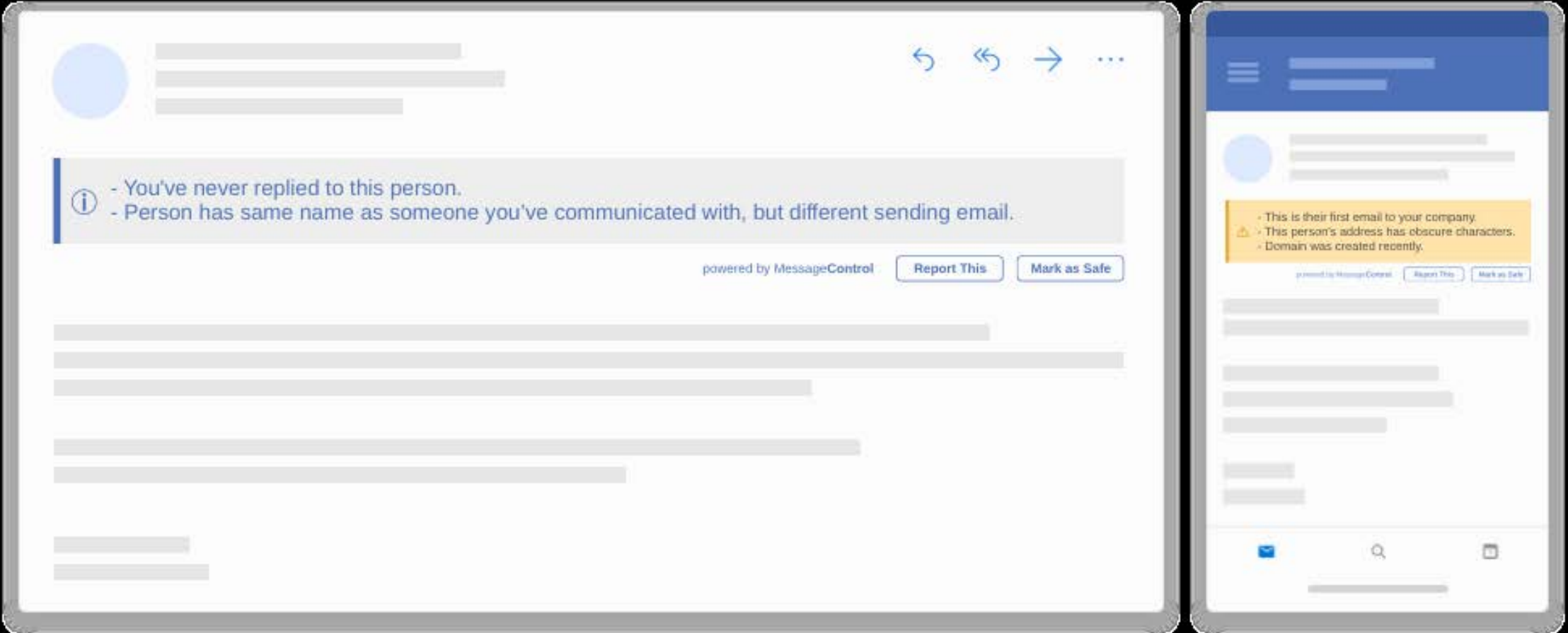


- **Conditional Access**

- Access to data based on conditions such as location, behavior, and risks detected on device
- Protect against international attackers or if virus on device

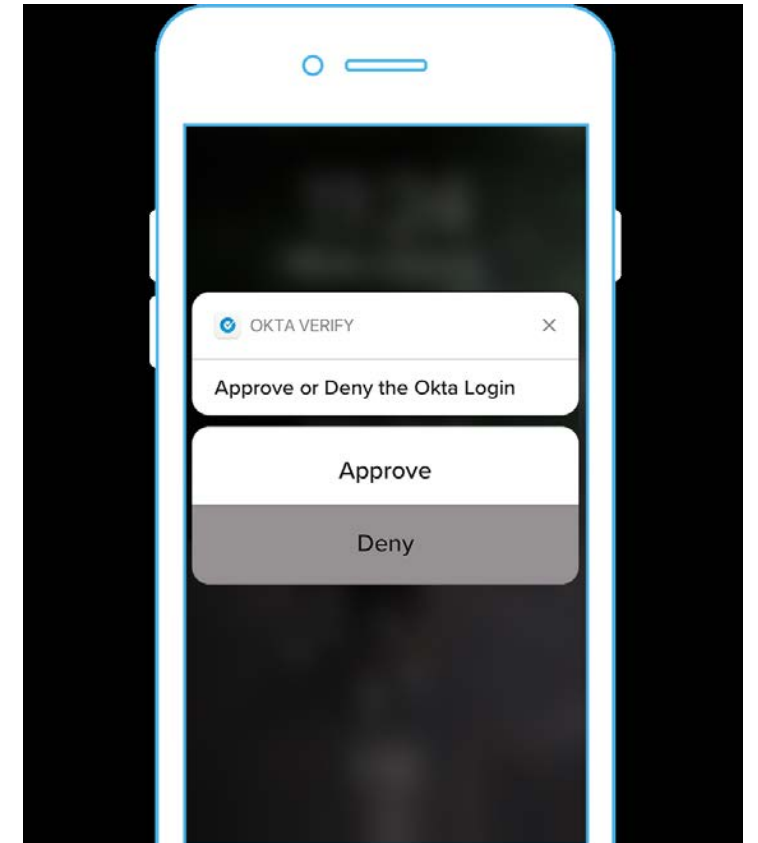
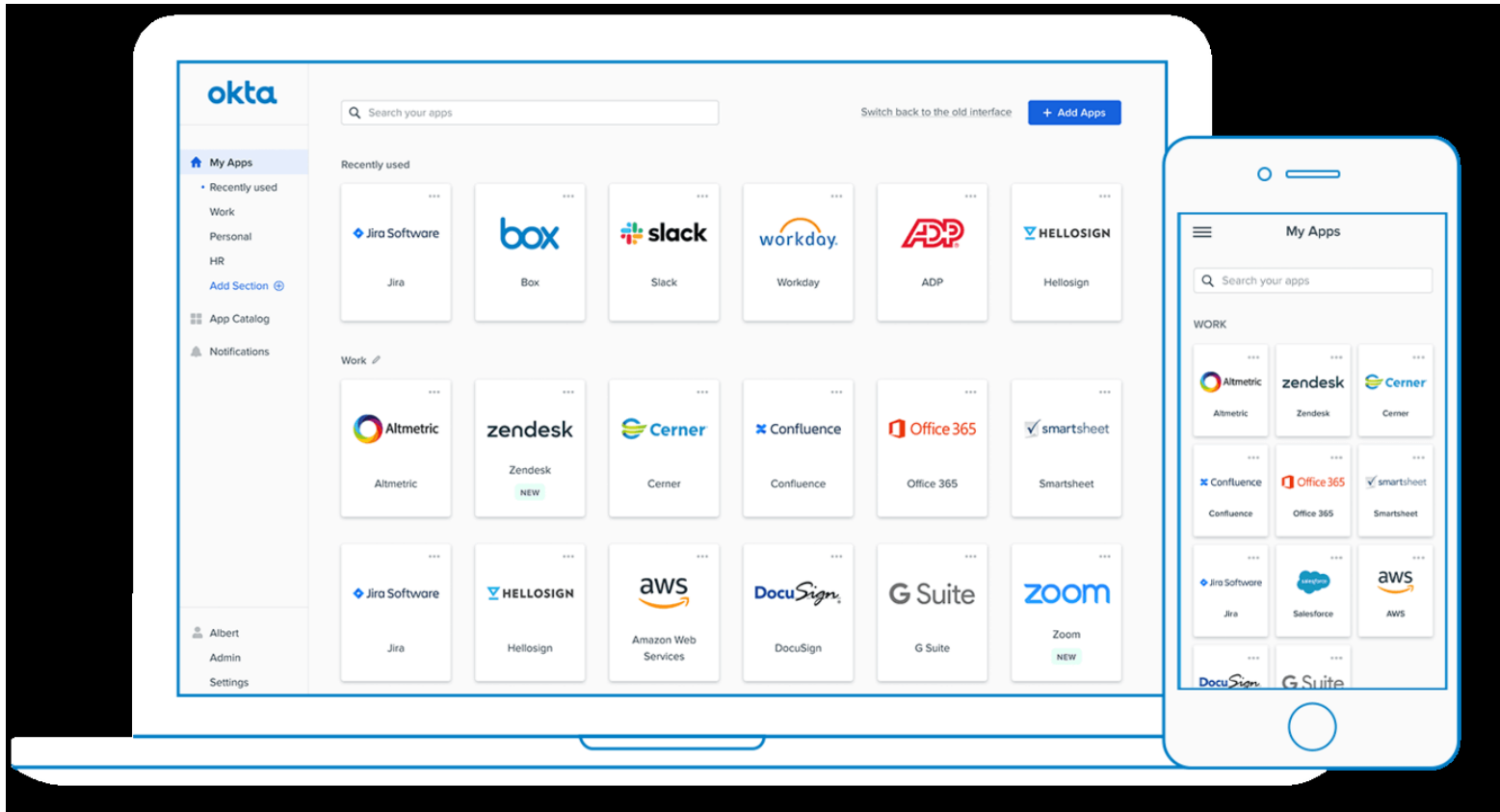


STOP SOCIAL ENGINEERING AND HUMAN IDENTITY ATTACKS



SECURE ACCESS TO YOUR ENTIRE BUSINESS

81% of data breaches involve weak or stolen credentials



IDENTITY IS THE NEW PERIMETER

Specify entire countries IP address ranges to block or allow traffic from



THREE KEY TAKEAWAYS

1. Private Equity Firms are being targeted
2. Awareness will reduce risk
3. Modern IT security solutions and properly configured mitigations will reduce risk



Thank you

Chris Hueneke
CHueneke@RKON.com

Joe Mullarkey
JoeMullarkey@RKON.com



FIVE KEY TAKEAWAYS

1. Private Equity being targeted for wire fraud with phishing emails

- Are links and downloads being inspected in real-time?
- Are inbound external emails being flagged visually so that users can easily identify them?
- Are inbound emails with look-alike domain names being flagged or rejected?
- Are email authenticity records being updated regularly?

2. Train users on security awareness on how to spot the signs

- Is that the real address of the sender?
- Should a phone call be placed to follow up on the email to see if the action is actually urgent?
- How should suspicious email be reported?

3. Implement strong security controls

- Is the email security sufficient to protect the company?
- Is Multi-Factor Authentication, Single Sign-On, and Conditional Access being used?

4. Perform Portfolio Company security and risk assessments

- Is there full visibility on the security controls of the companies within our Portfolio?
- What risk tolerance level should be accepted?

5. Vendor Risk Assessments

- Are security controls of critical vendors' being assessed?
- What access is provided to contractors and how is it being monitored?

APPENDIX A: QUESTIONS FOR IT DEPARTMENT

1. What is our current email phishing prevention toolkit?

- Are links and downloads being inspected in real-time?
- Are inbound external emails being flagged visually so that users can easily identify them?
- Are inbound emails with look-alike domain names being flagged or rejected?
- Are email authenticity records being updated regularly?

2. What is our current backup and restore policy?

- How often is a full restore tested?
- Are immutable backup copies being stored off-site?
- Is cloud-replicated storage like OneDrive being used to mitigate ransomware on users' machines?

3. Is the disaster recovery and incident response well documented?

4. Are users receiving security awareness training?

5. Are vendors being assessed for risk?

BE PROACTIVE

- Perform End User Security Awareness Training
- Implement Advanced Email Security Solutions
- Backup Critical Data
- Document Disaster Recovery Plan
- Document Incident Response Plan
- Assess Critical Vendors' Security Controls

APPENDIX B: SUMMARY OF IT RISK & SECURITY BEST PRACTICES

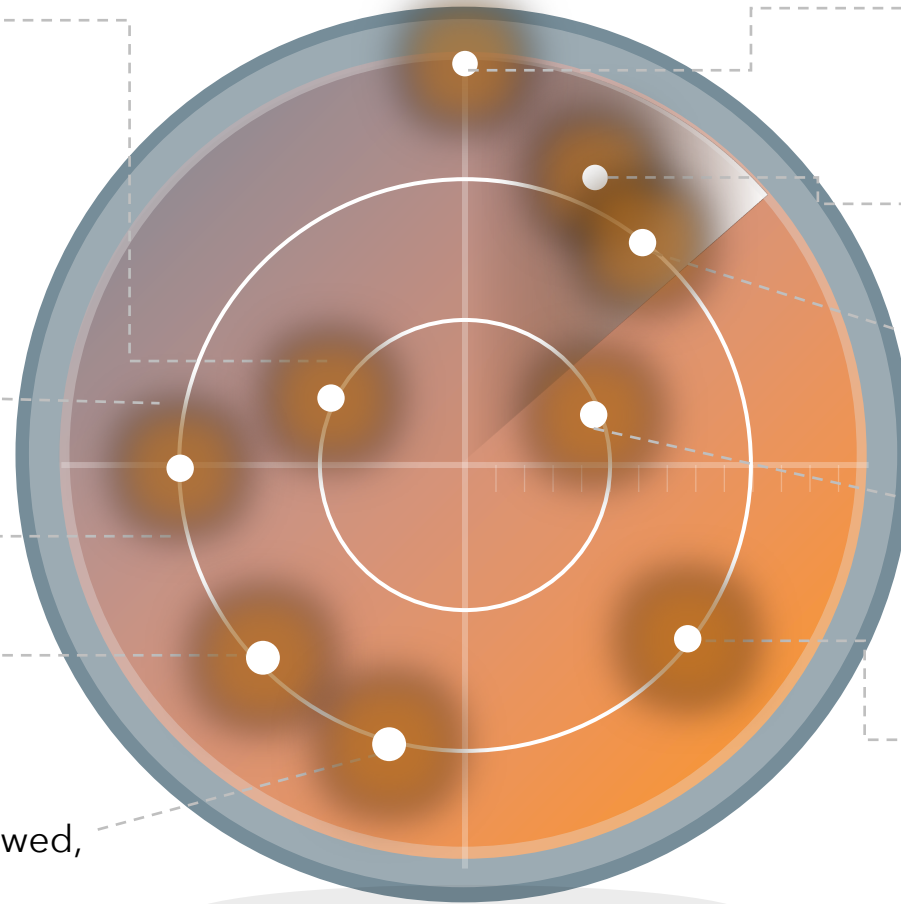
IT Security Policies documented, communicated, and accepted by users

Security Awareness Training provided to end users

Security Architecture implemented to **Identify** vulnerabilities, **Protect** against threats, **Detect** attacks, **Respond** in a timely manner and **Recover** to keep the business operational and resilient

Security Operations Center monitoring threats and vulnerabilities, reporting on performance of security controls and handling incidents

Disaster Recovery Plan documented, reviewed, accepted, and tested regularly



Virtual Chief Information Security Officer services provided by strategic partner

Risk and Security Self-Assessment performed across the business and portfolio companies

Security Architecture Review analyzing control gaps and remediation

Monitor Security and Risk Posture continually across the business

Business Continuity Plan includes Crisis Management, IT Disaster Recovery, Security Incident Response policies, processes, and subject matter experts (internal team and external partners)