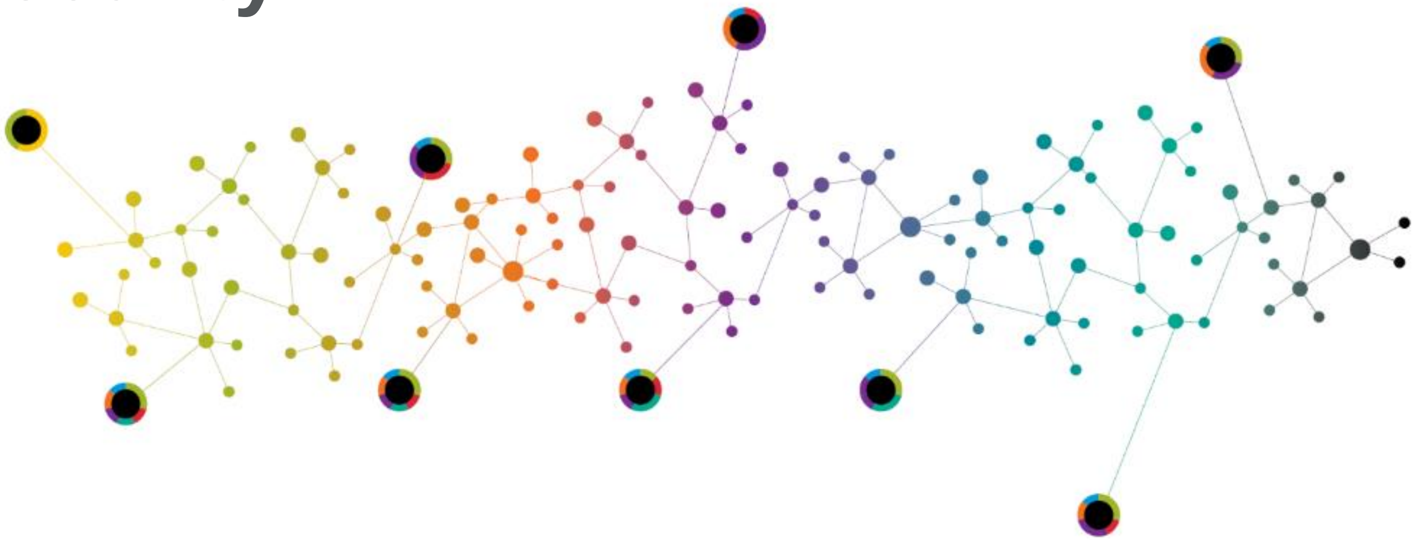
BakerHostetler

CALIFORNIA
J · P · I · A

Introduction to Cyber Security



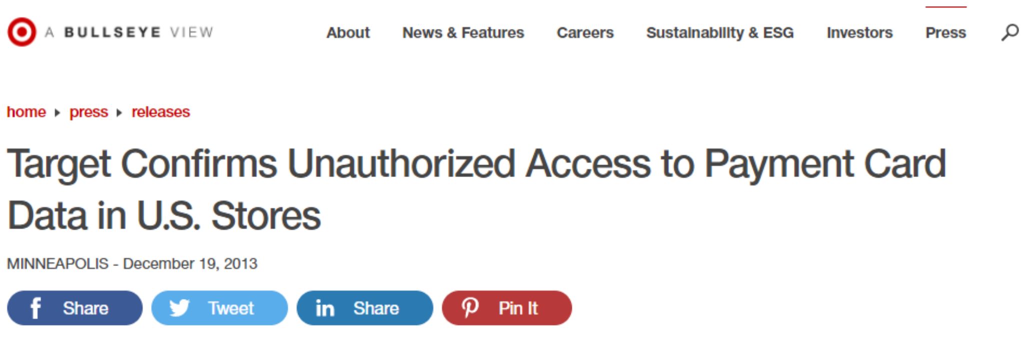
M. Scott Koller, CISSP, CIPP | Partner

Introduction

M. Scott Koller, CISSP, CIPP
Partner, Digital Risk Advisory and Cybersecurity Team
Baker & Hostetler, LLP

- Advised companies in more than 1,000 privacy and data security incidents involving malware, network intrusions, phishing, inadvertent disclosures and ransomware.
- Defends clients on data protection issues and regulatory investigations (Office for Civil Rights (OCR), Financial Industry Regulatory Authority, Securities and Exchange Commission, the Federal Trade Commission (FTC), and various state Attorneys General)

Cyber Security



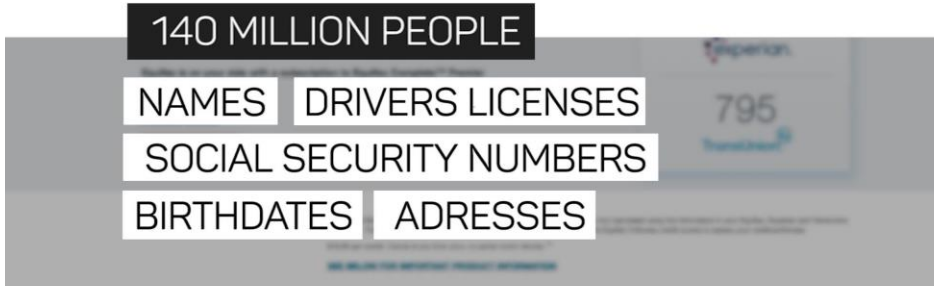
Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

MINNEAPOLIS - December 19, 2013

Target tod... confirmed it is aware of unauthorized access to payment card data that may have impacted working c the issue.

"Target's this issue said Greg very seri

EQUIFAX®

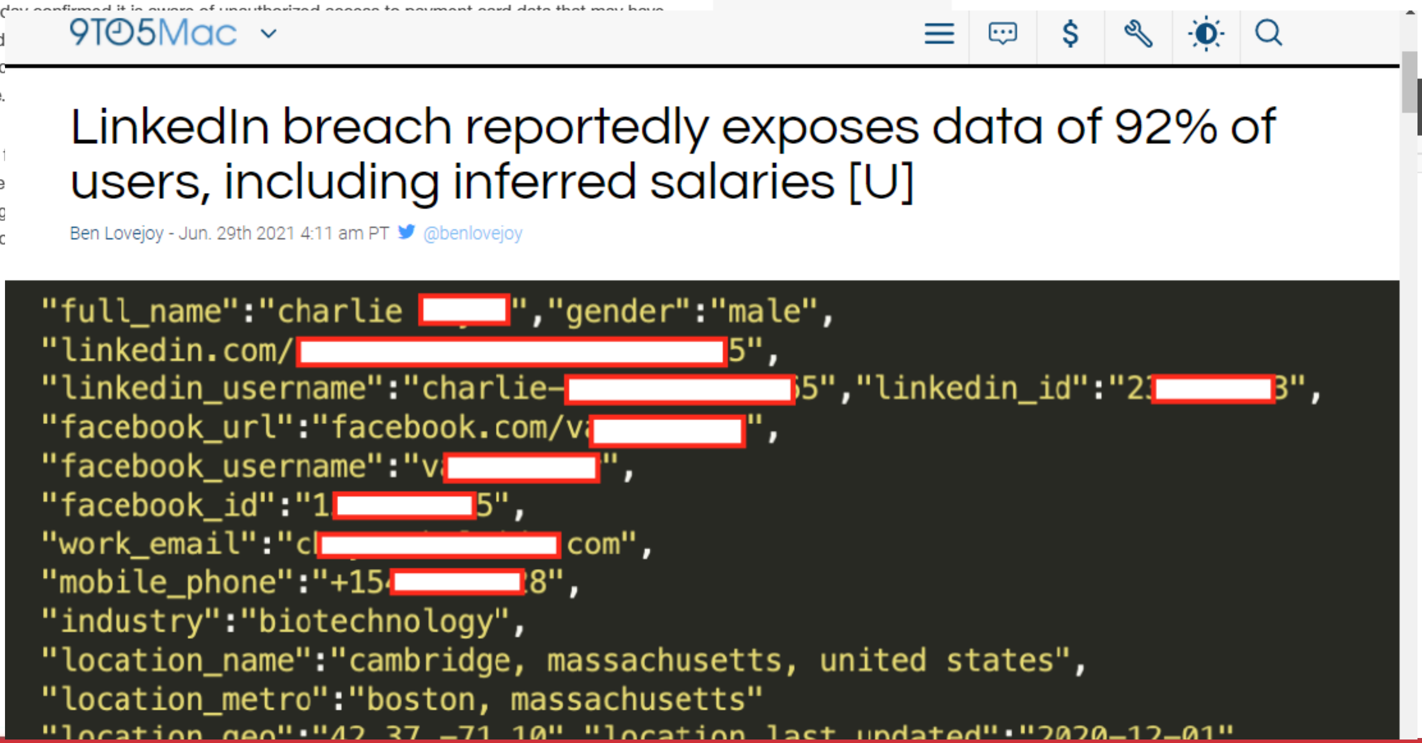


140 MILLION PEOPLE

NAMES DRIVERS LICENSES

SOCIAL SECURITY NUMBERS

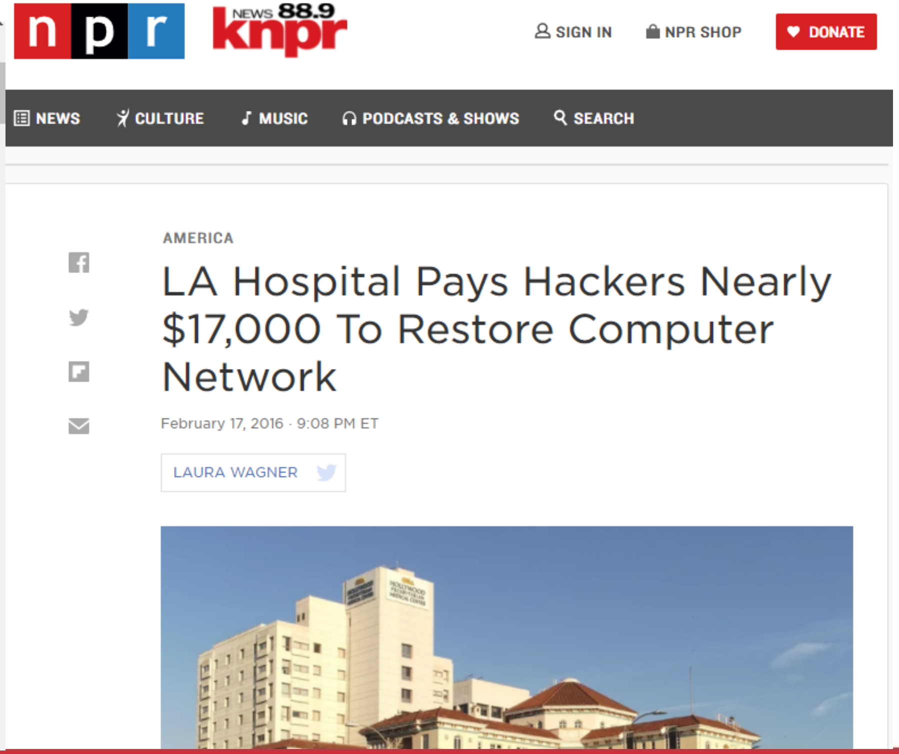
BIRTHDATES ADRESSES



LinkedIn breach reportedly exposes data of 92% of users, including inferred salaries [U]

Ben Lovejoy - Jun. 29th 2021 4:11 am PT @benlovejoy

```
"full_name":"charlie [redacted]","gender":"male",
"linkedin.com/[redacted]5",
"linkedin_username":"charlie-[redacted]5","linkedin_id":"2[redacted]3",
"facebook_url":"facebook.com/v[redacted]",
"facebook_username":"v[redacted]",
"facebook_id":"1[redacted]5",
"work_email":"c[redacted]com",
"mobile_phone":"+15[redacted]8",
"industry":"biotechnology",
"location_name":"cambridge, massachusetts, united states",
"location_metro":"boston, massachusetts"
"location_geo":"42.37,-71.10","location_last_updated":"2020-12-01"
```



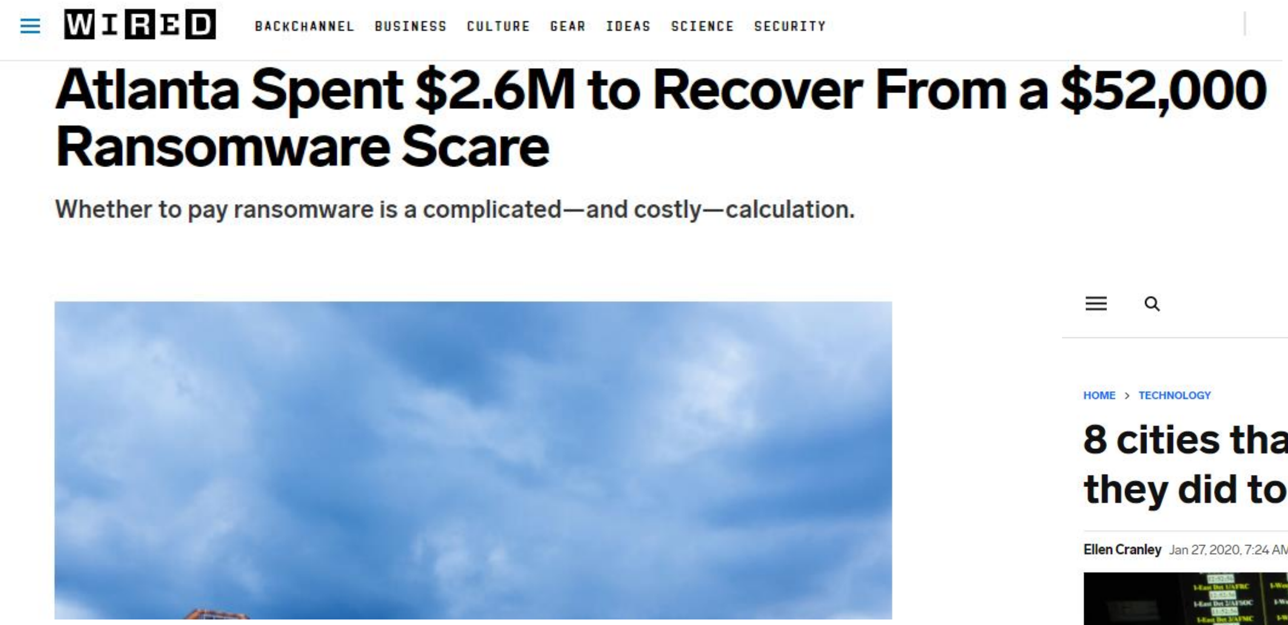
AMERICA

LA Hospital Pays Hackers Nearly $17,000 To Restore Computer Network

February 17, 2016 · 9:08 PM ET

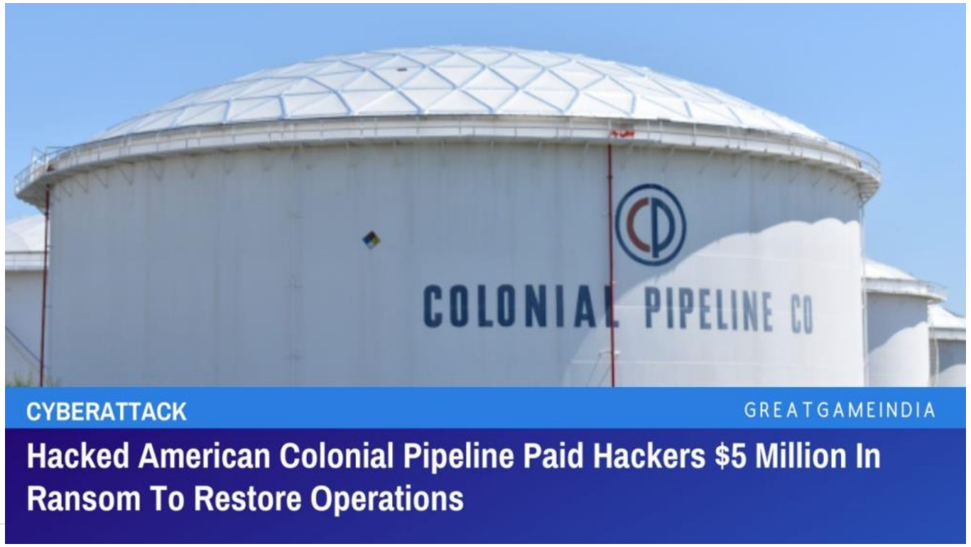
LAURA WAGNER

Cyber Security



Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare

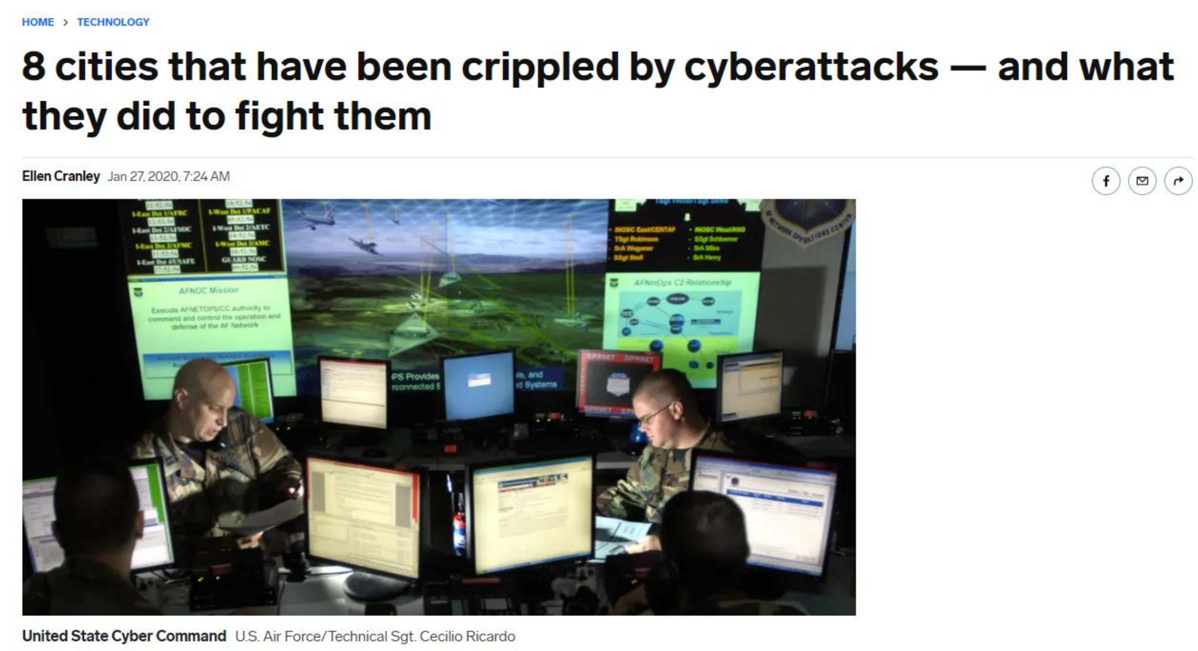
Whether to pay ransomware is a complicated—and costly—calculation.



CYBERATTACK

GREATGAMEINDIA

Hacked American Colonial Pipeline Paid Hackers $5 Million In Ransom To Restore Operations

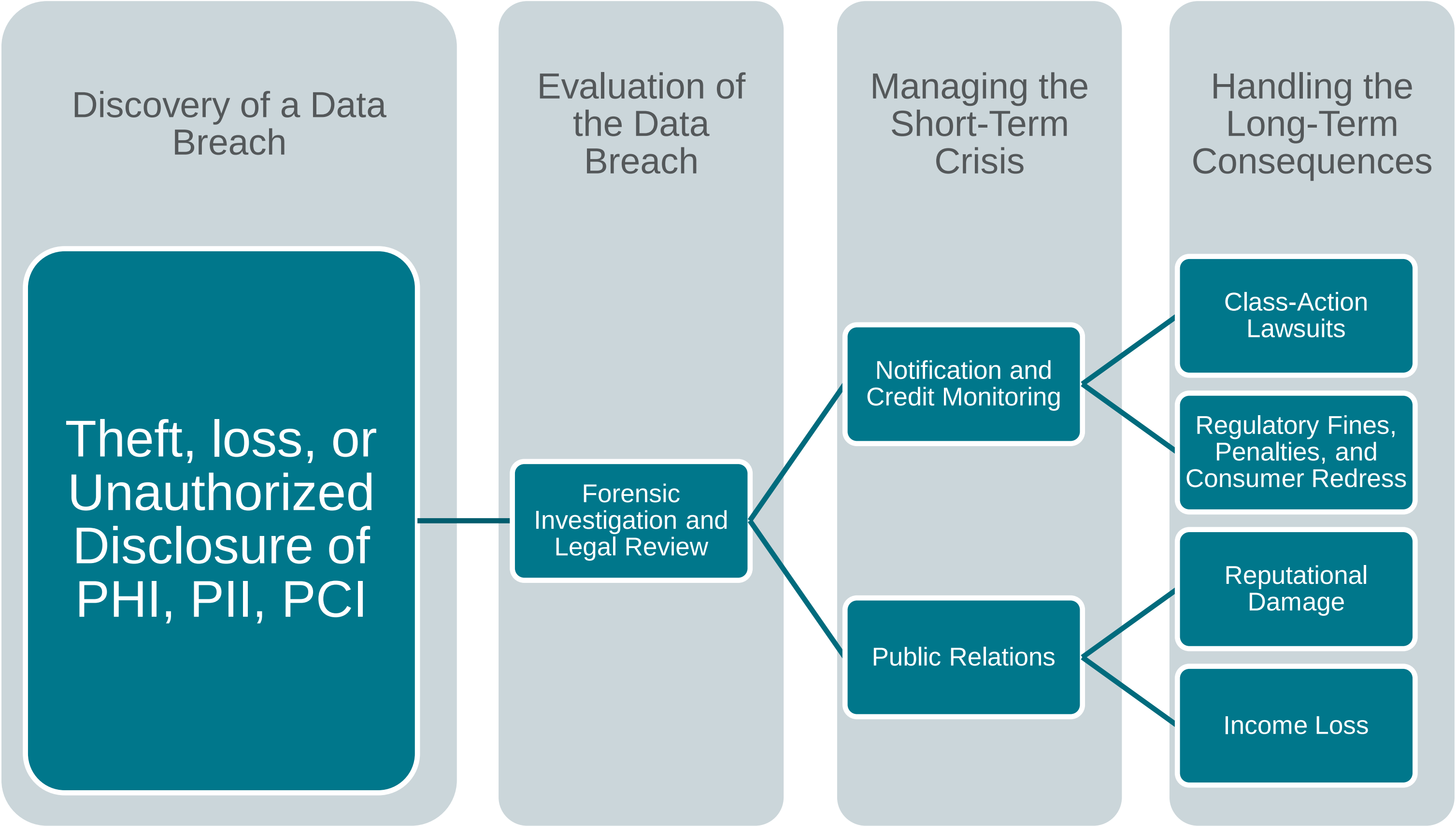


8 cities that have been crippled by cyberattacks — and what they did to fight them

Ellen Cranley Jan 27, 2020, 7:24 AM

United State Cyber Command U.S. Air Force/Technical Sgt. Cecilio Ricardo

A Simplified View of a Data Breach



Discovery of a Data Breach
Evaluation of the Data Breach
Managing the Short-Term Crisis
Handling the Long-Term Consequences
Theft, loss, or Unauthorized Disclosure of PHI, PII, PCI
Forensic Investigation and Legal Review
Notification and Credit Monitoring
Public Relations
Class-Action Lawsuits
Regulatory Fines, Penalties, and Consumer Redress
Reputational Damage
Income Loss

What Kinds of Information are at Risk?

Information of Residents

- Social Security numbers
- Driver’s License Numbers, Passport Numbers, State Issued ID Numbers.
- Credit cards, debit cards, and other payment information
- Financial information such as account balances, loan history, and credit reports
- Protected healthcare information (PHI), including medical records, test results, appointment history, and insurance information
- Non-PI, like email addresses, phone lists, and home addresses that may not be independently sensitive, but may be more sensitive with one or more of the above

Employee Information

- Employers have at least some of the above information on all of their employees

Business Partners

- Any of the above with respect to Business Associates and/or Vendors

Where are the Threats?

External Threats

- Hackers
  - Financially Motivated
  - State-Sponsored Attacks
  - “Hacktivists” (Anonymous)
- Corporate Espionage
  - Domestic and foreign commercial rivals
  - Domestic and foreign start-up companies
- Organized Crime
- Vendors

rity rootkit phishing malware worm trojan virus spam hackers spyware security rootkit

Where are the Threats?

$40 REWARD!

LOST PHONE!

Lost while on circle link or Bingham 204

Contact me ASAP PLEASE

SMITH 418

Blue T-Mobile Sidekick 2008[w/Red Garra Phone Charm]

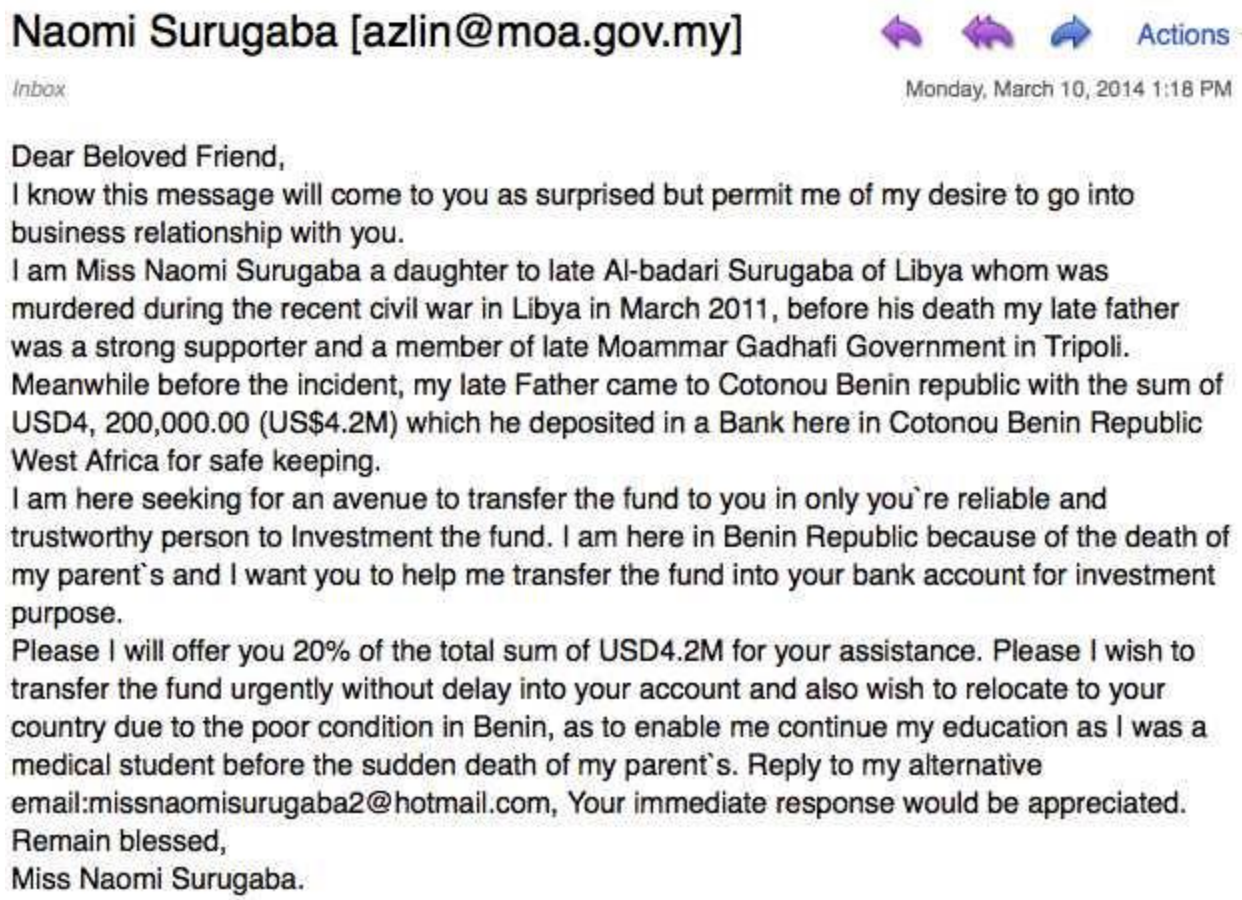
Internal Threats

- Employee Negligence
  - Security failures
  - Lost mobile devices
- Employee Ignorance
  - Improper disposal of personal information (dumpsters)
  - Lack of education and awareness
- Malicious Employees

Most Common Types of Attacks

- Phishing Attacks
- Network Intrusion
- Lost or Stolen Records
- Inadvertent Disclosures

Phishing Examples



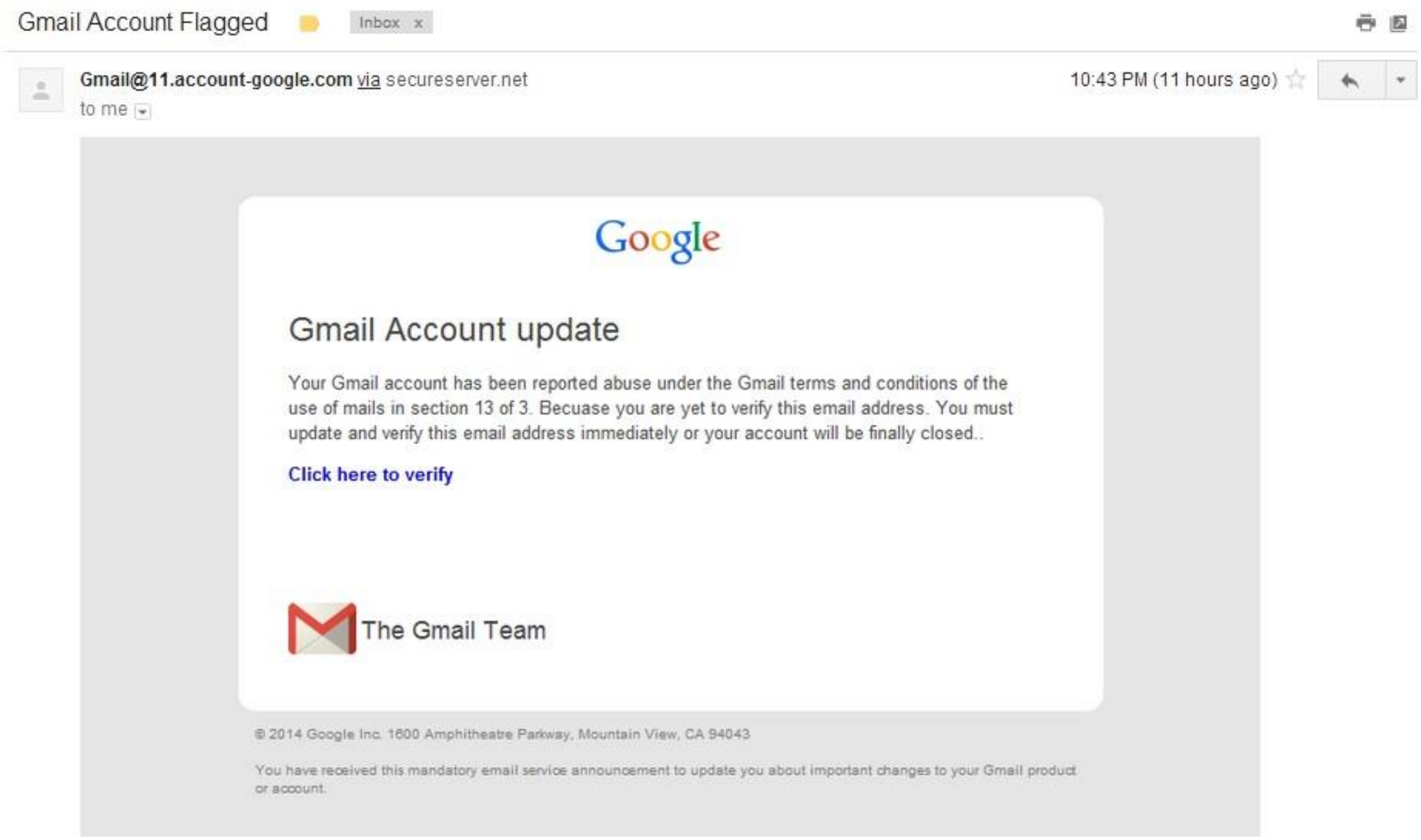
Naomi Surugaba [azlin@moa.gov.my]

Inbox

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli. Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Phishing Examples



Gmail Account Flagged

Gmail@11.account-google.com via secureserver.net
to me

10:43 PM (11 hours ago)

Gmail Account update

Your Gmail account has been reported abuse under the Gmail terms and conditions of the use of mails in section 13 of 3. Becuase you are yet to verify this email address. You must update and verify this email address immediately or your account will be finally closed..

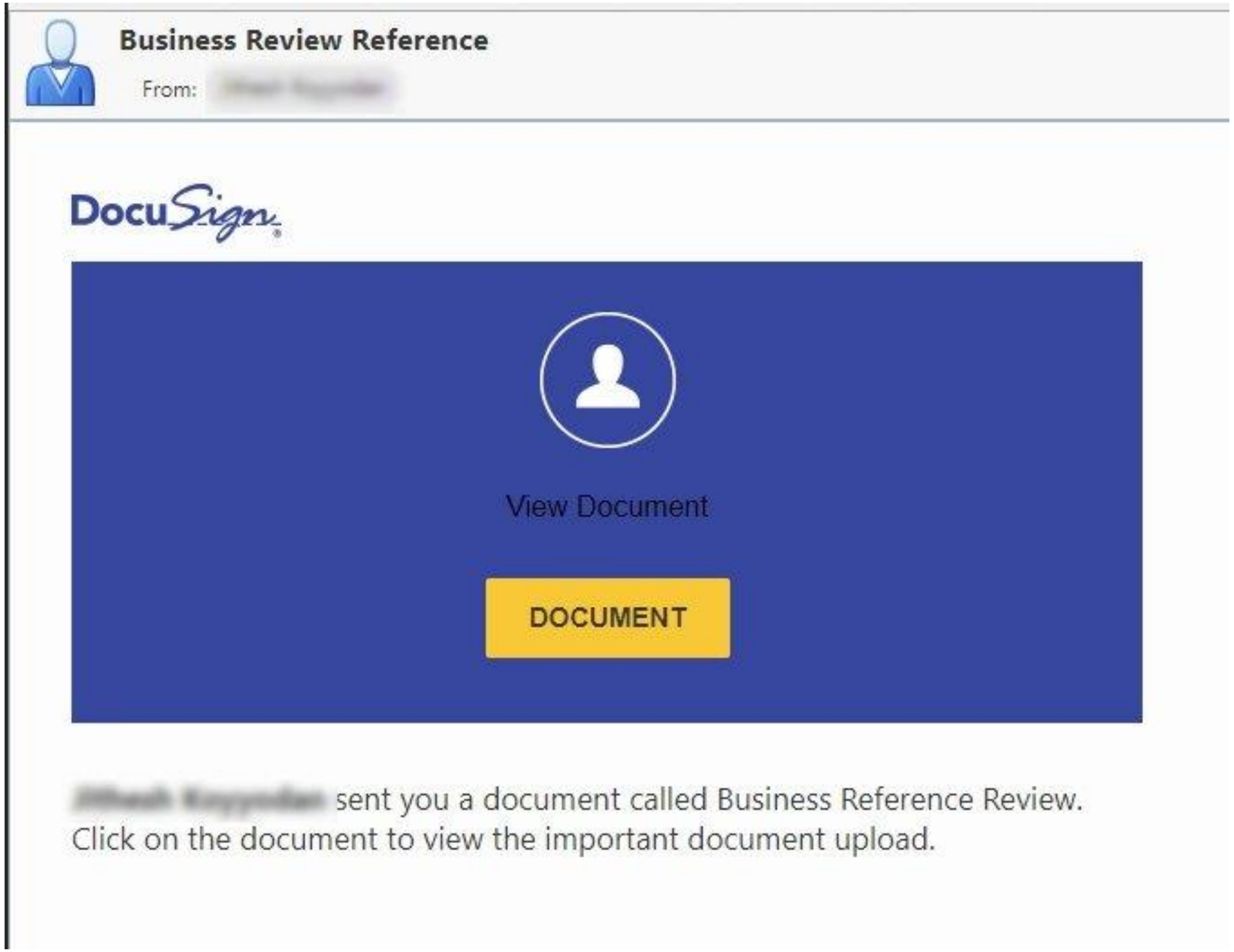
Click here to verify

The Gmail Team

© 2014 Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043

You have received this mandatory email service announcement to update you about important changes to your Gmail product or account.

Phishing Examples

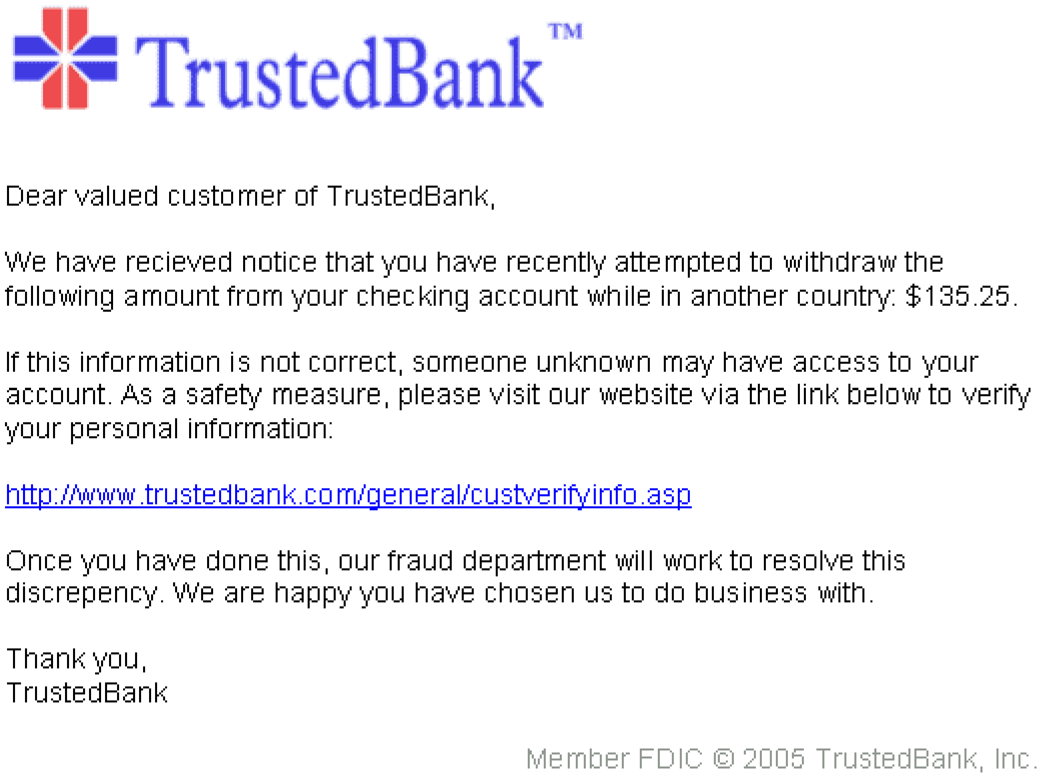


Business Review Reference

From: [redacted]

[redacted] sent you a document called Business Reference Review. Click on the document to view the important document upload.

Phishing Examples



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

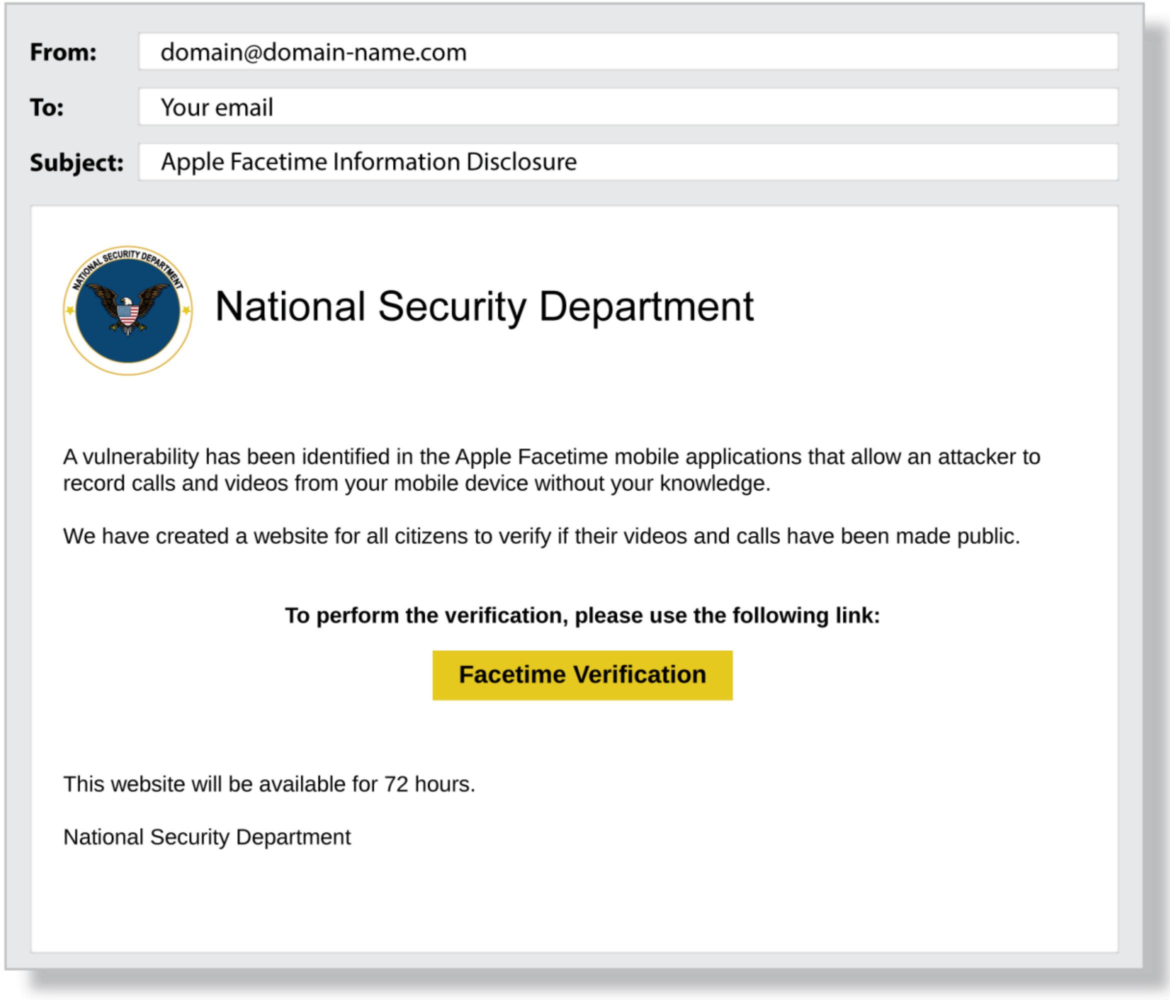
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Phishing Examples



From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

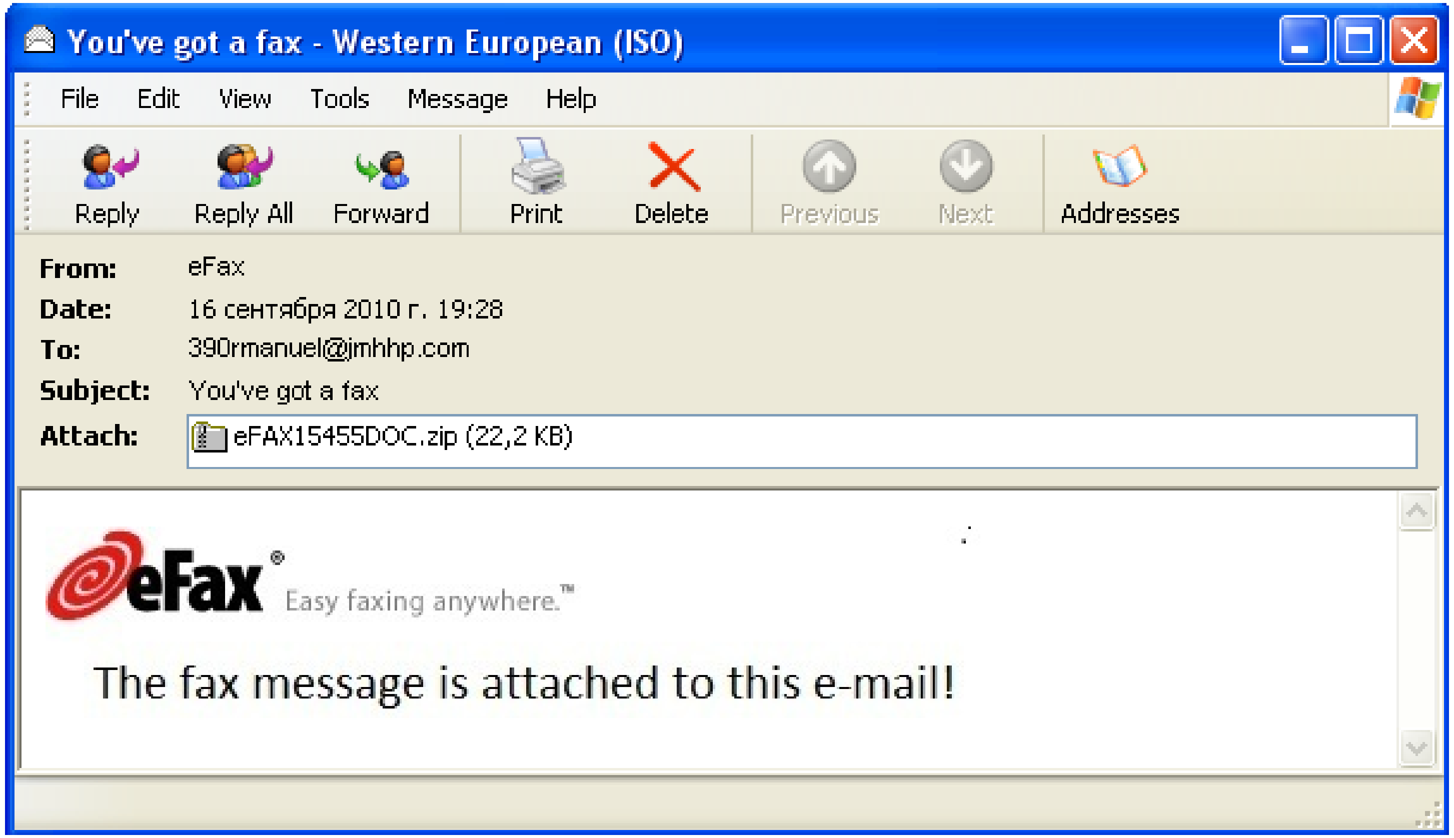
To perform the verification, please use the following link:

This website will be available for 72 hours.

National Security Department

Goals of Phishing Emails

- Execute Malware
  - Steals Credentials
  - Remote Access
  - Ransomware

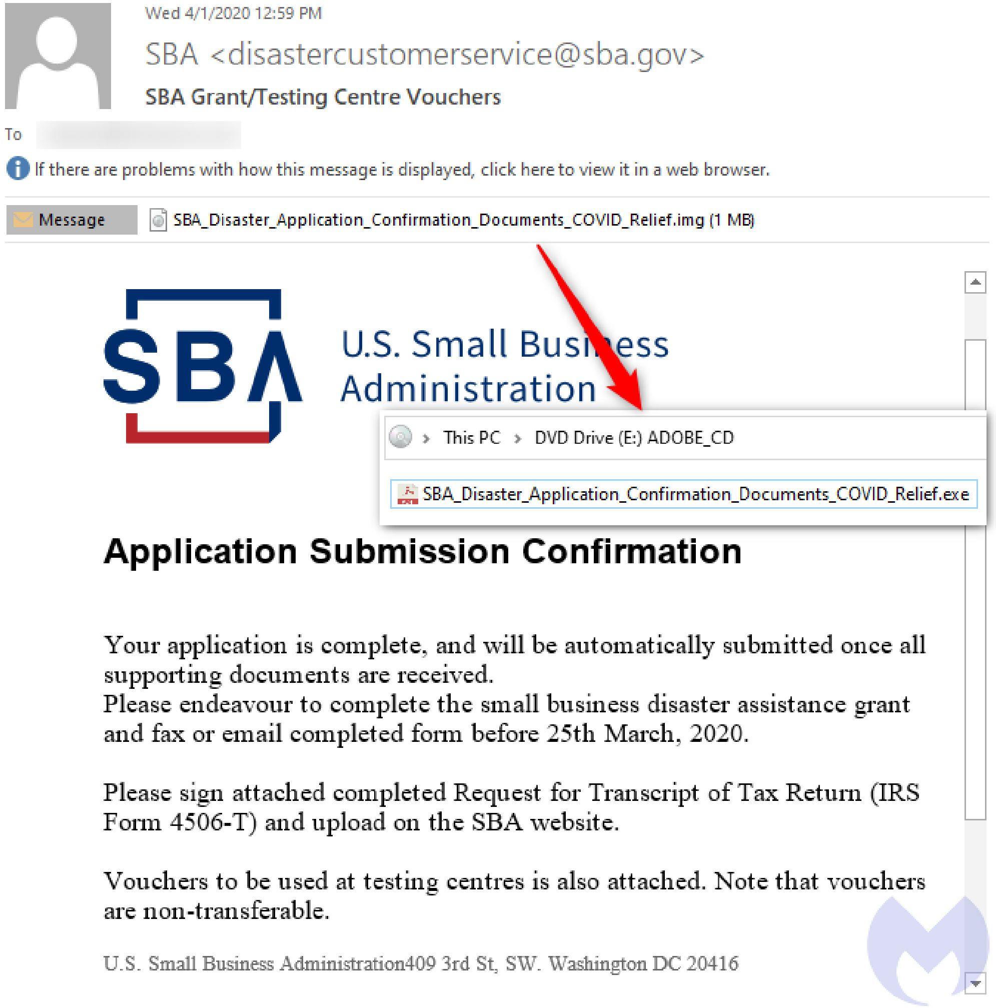


From: eFax
Date: 16 сентября 2010 г. 19:28
To: 390rmanuel@jmhhp.com
Subject: You've got a fax
Attach: eFAX15455DOC.zip (22,2 KB)

The fax message is attached to this e-mail!

Goals of Phishing Emails

- Execute Malware
  - Steals Credentials
  - Remote Access
  - Ransomware



Wed 4/1/2020 12:59 PM

SBA <disastercustomerservice@sba.gov>

SBA Grant/Testing Centre Vouchers

To [redacted]

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

Message | SBA_Disaster_Application_Confirmation_Documents_COVID_Relief.img (1 MB)

SBA U.S. Small Business Administration

This PC › DVD Drive (E:) ADOBE_CD

SBA_Disaster_Application_Confirmation_Documents_COVID_Relief.exe

Application Submission Confirmation

Your application is complete, and will be automatically submitted once all supporting documents are received.
Please endeavour to complete the small business disaster assistance grant and fax or email completed form before 25th March, 2020.

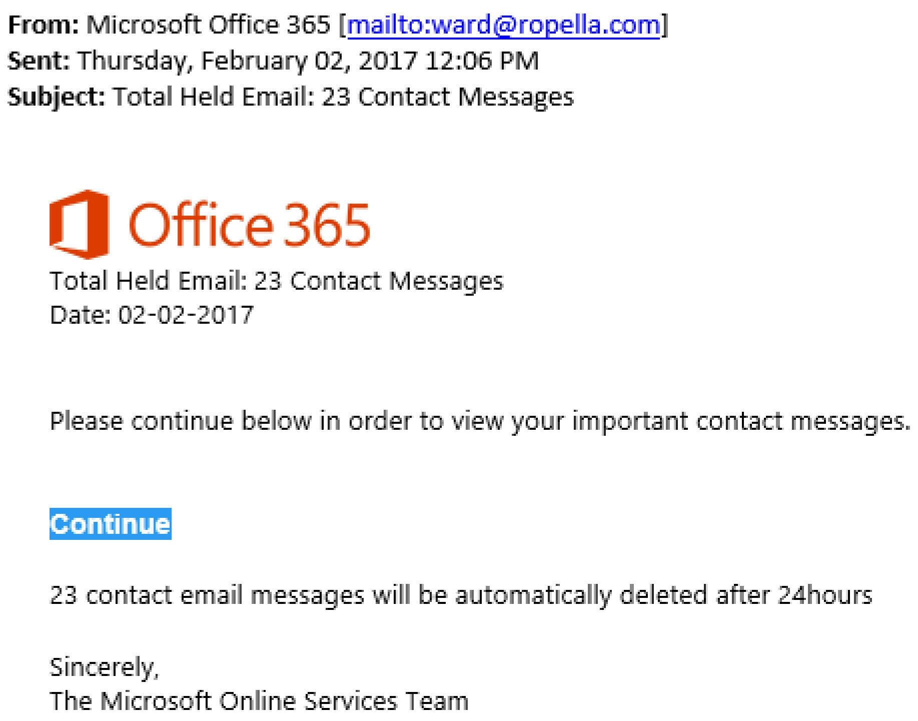
Please sign attached completed Request for Transcript of Tax Return (IRS Form 4506-T) and upload on the SBA website.

Vouchers to be used at testing centres is also attached. Note that vouchers are non-transferable.

U.S. Small Business Administration409 3rd St, SW. Washington DC 20416

Goals of Phishing Emails

- Disclose Credentials
  - Account Takeover
  - Execute Malware
  - Used to Send Phishing Emails



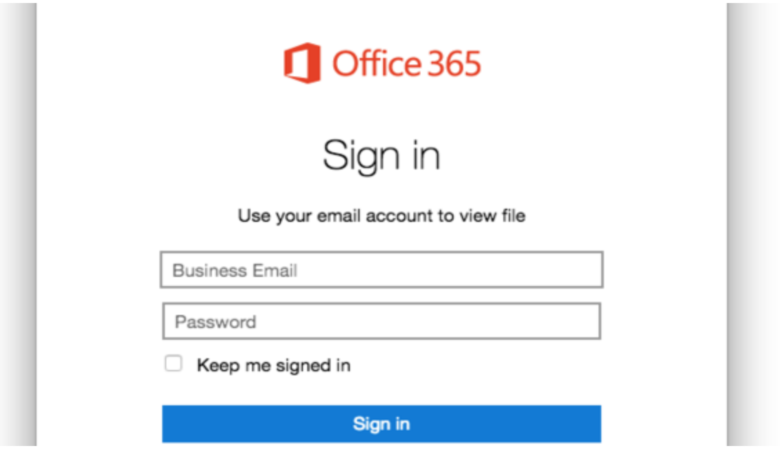
From: Microsoft Office 365 [mailto:ward@ropella.com]
Sent: Thursday, February 02, 2017 12:06 PM
Subject: Total Held Email: 23 Contact Messages

Total Held Email: 23 Contact Messages
Date: 02-02-2017

Please continue below in order to view your important contact messages.

23 contact email messages will be automatically deleted after 24hours

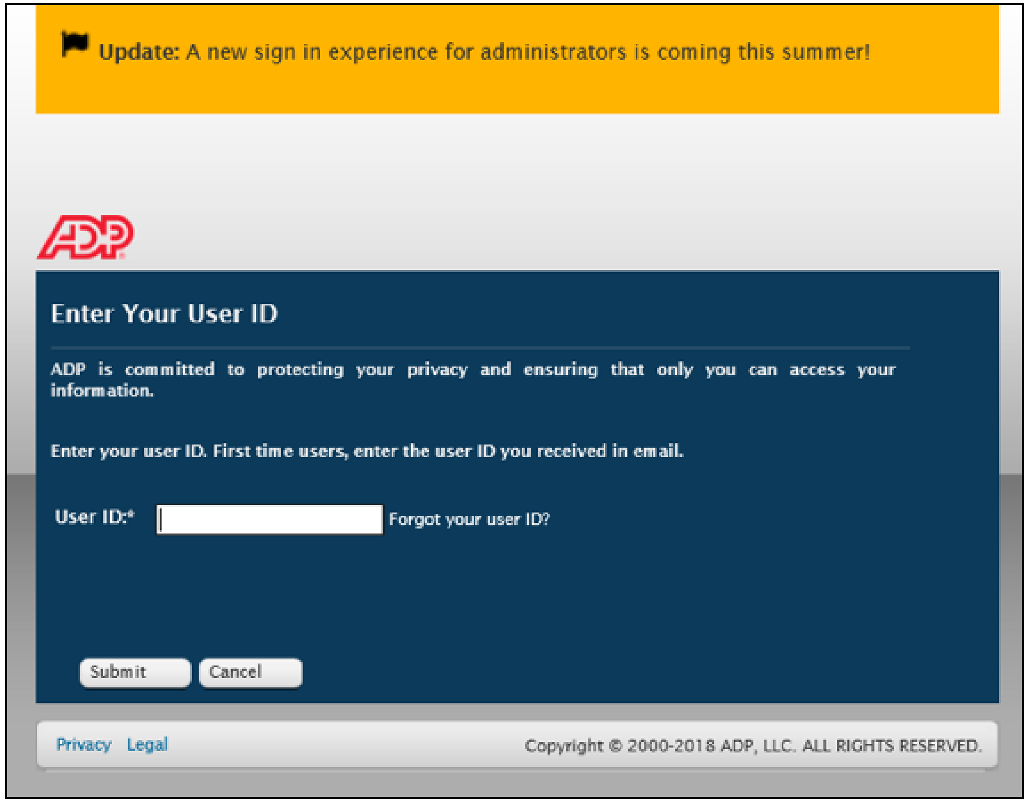
Sincerely,
The Microsoft Online Services Team



Use your email account to view file

Goals of Phishing Emails

- Disclose Credentials
  - Account Takeover
  - Execute Malware
  - Used to Send Phishing Emails



Update: A new sign in experience for administrators is coming this summer!

Enter Your User ID

ADP is committed to protecting your privacy and ensuring that only you can access your information.

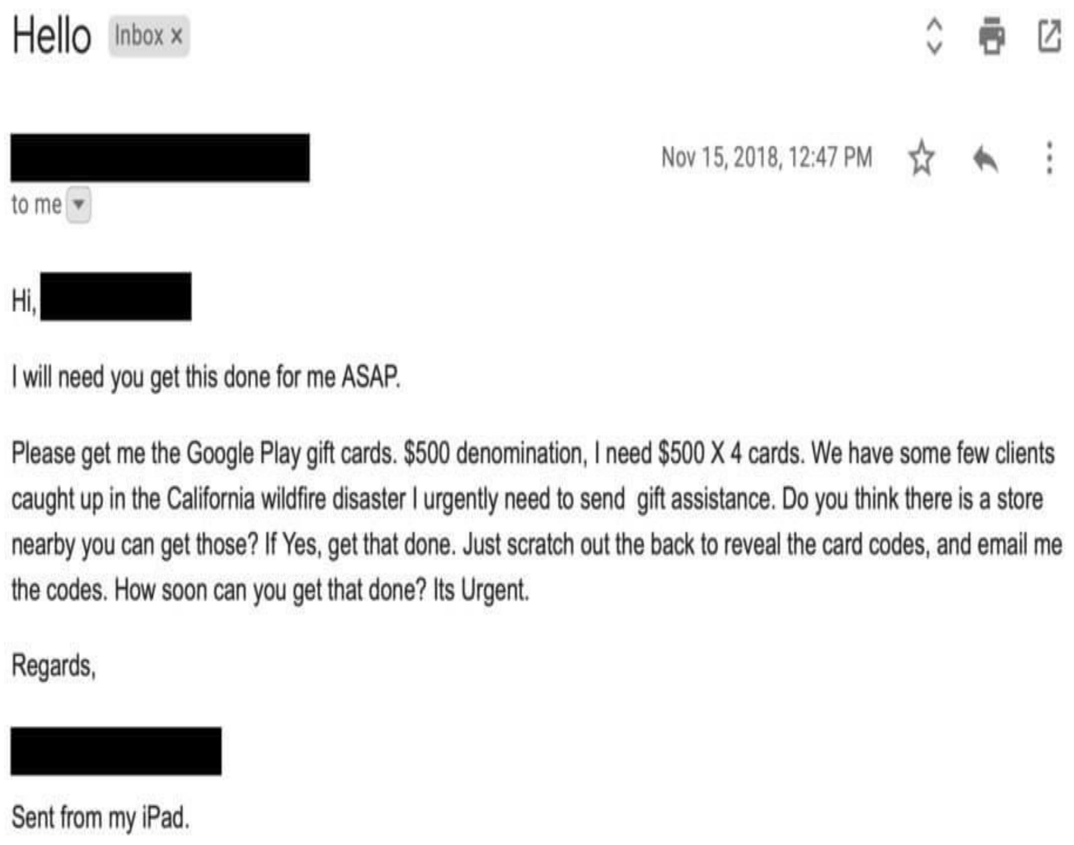
Enter your user ID. First time users, enter the user ID you received in email.

User ID:* Forgot your user ID?

Copyright © 2000-2018 ADP, LLC. ALL RIGHTS RESERVED.

Goals of Phishing Emails

- Social Engineering
  - Gift Card Scam
  - W2 Scam
  - Wire Fraud / Invoice Scam



Hello

[redacted]
to me

Nov 15, 2018, 12:47 PM

Hi, [redacted]

I will need you get this done for me ASAP.

Please get me the Google Play gift cards. $500 denomination, I need $500 X 4 cards. We have some few clients caught up in the California wildfire disaster I urgently need to send gift assistance. Do you think there is a store nearby you can get those? If Yes, get that done. Just scratch out the back to reveal the card codes, and email me the codes. How soon can you get that done? Its Urgent.

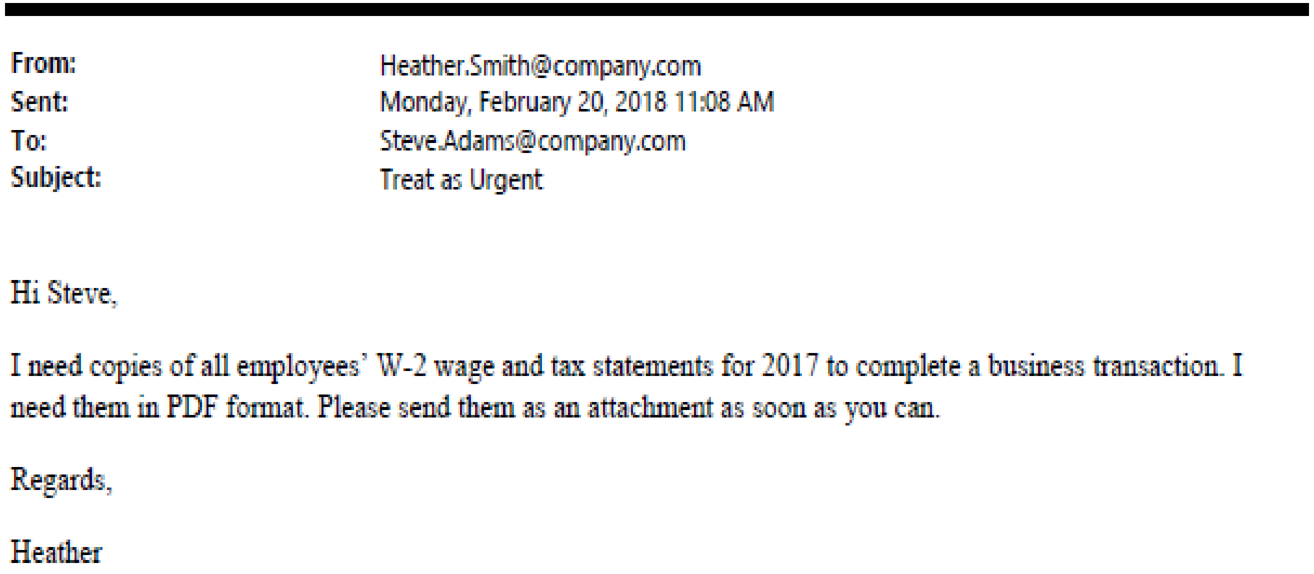
Regards,

[redacted]

Sent from my iPad.

Goals of Phishing Emails

- Social Engineering
  - Gift Card Scam
  - W2 Scam
  - Wire Fraud / Invoice Scam



From: Heather.Smith@company.com
Sent: Monday, February 20, 2018 11:08 AM
To: Steve.Adams@company.com
Subject: Treat as Urgent

Hi Steve,

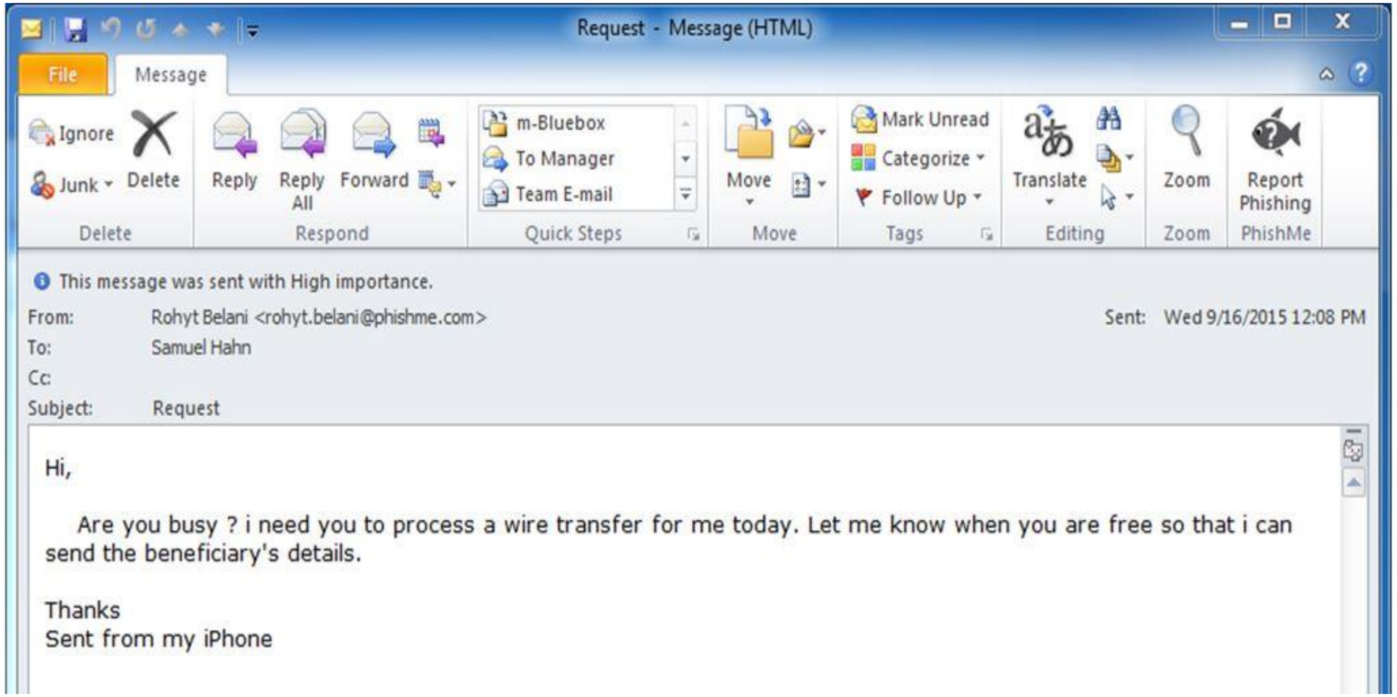
I need copies of all employees' W-2 wage and tax statements for 2017 to complete a business transaction. I need them in PDF format. Please send them as an attachment as soon as you can.

Regards,

Heather

Goals of Phishing Emails

- Social Engineering
  - Gift Card Scam
  - W2 Scam
  - Wire Fraud / Invoice Scam



This message was sent with High importance.

From: Rohyt Belani <rohyt.belani@phishme.com>

Sent: Wed 9/16/2015 12:08 PM

To: Samuel Hahn

Cc:

Subject: Request

Hi,

Are you busy ? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

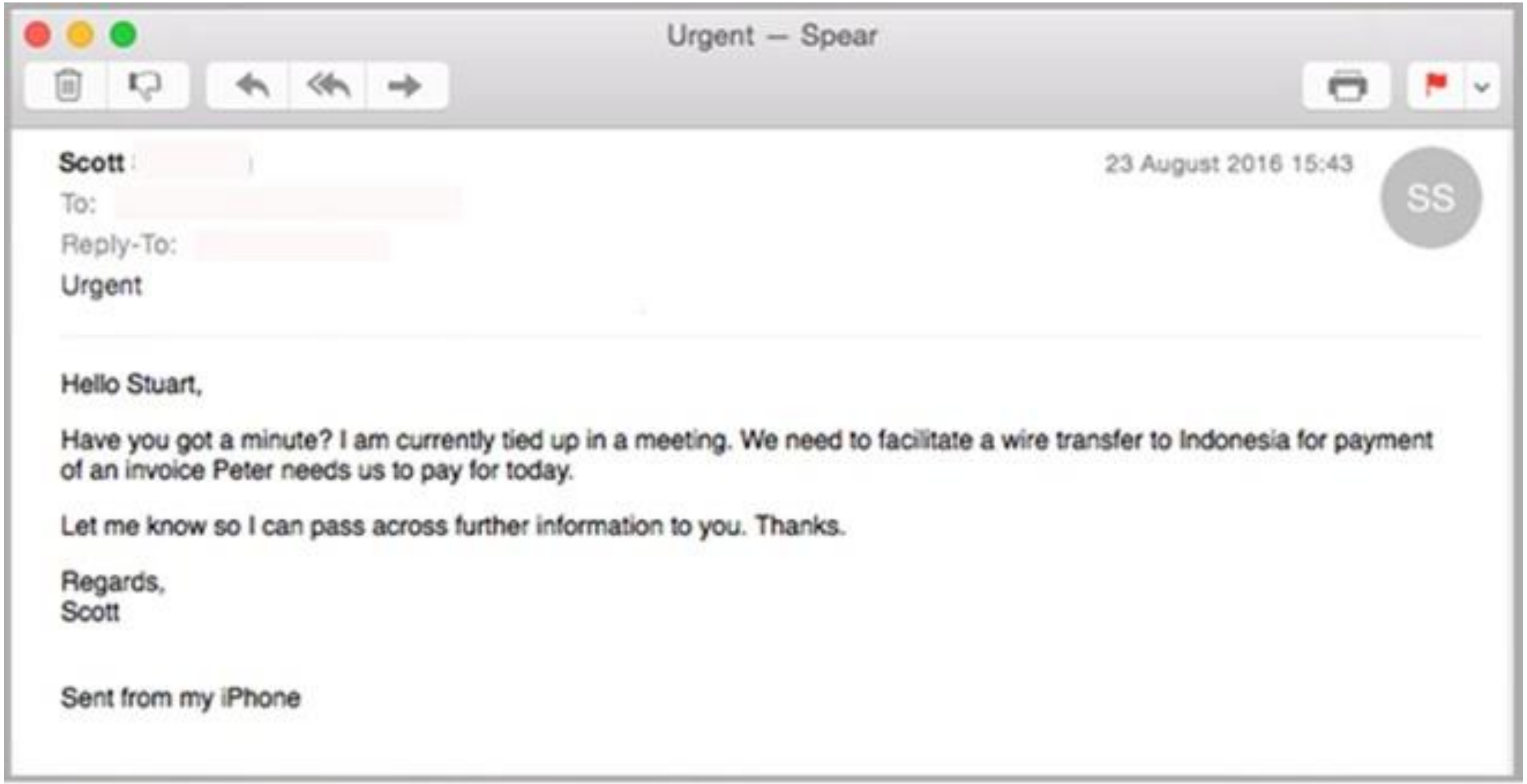
Thanks
Sent from my iPhone

Phishing vs. Spear Phishing

***Spear phishing*:**

the scammer customizes the email with personal information of the recipient such as the recipient’s name, position, phone number, etc., to *trick* the recipient into believing there is a personal connection.

Phishing vs. Spear Phishing



Scott [redacted]

To: [redacted]

Reply-To: [redacted]

Urgent

23 August 2016 15:43

Hello Stuart,

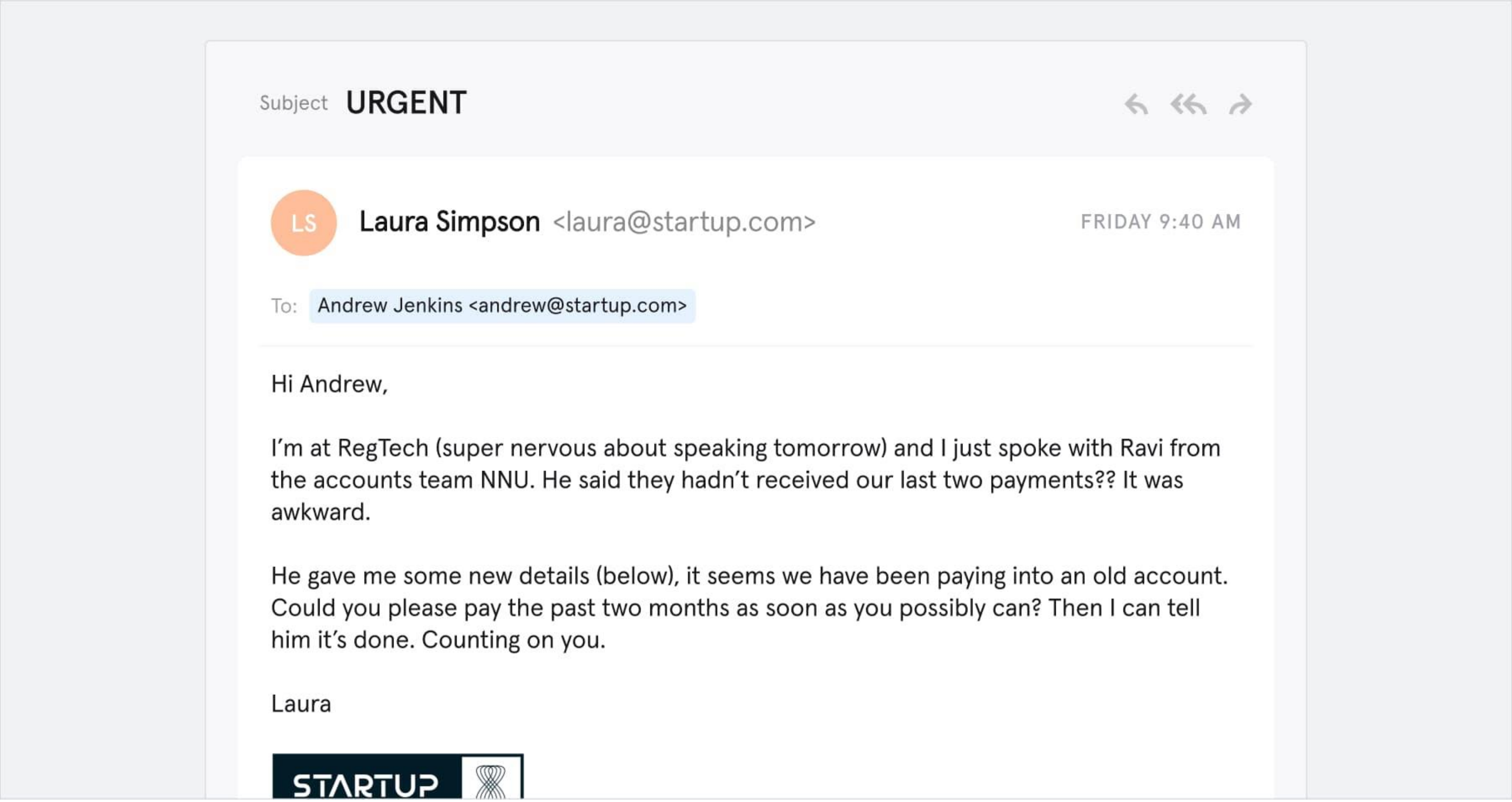
Have you got a minute? I am currently tied up in a meeting. We need to facilitate a wire transfer to Indonesia for payment of an invoice Peter needs us to pay for today.

Let me know so I can pass across further information to you. Thanks.

Regards,
Scott

Sent from my iPhone

Phishing vs. Spear Phishing



Subject URGENT

Laura Simpson <laura@startup.com>

FRIDAY 9:40 AM

To: Andrew Jenkins <andrew@startup.com>

Hi Andrew,

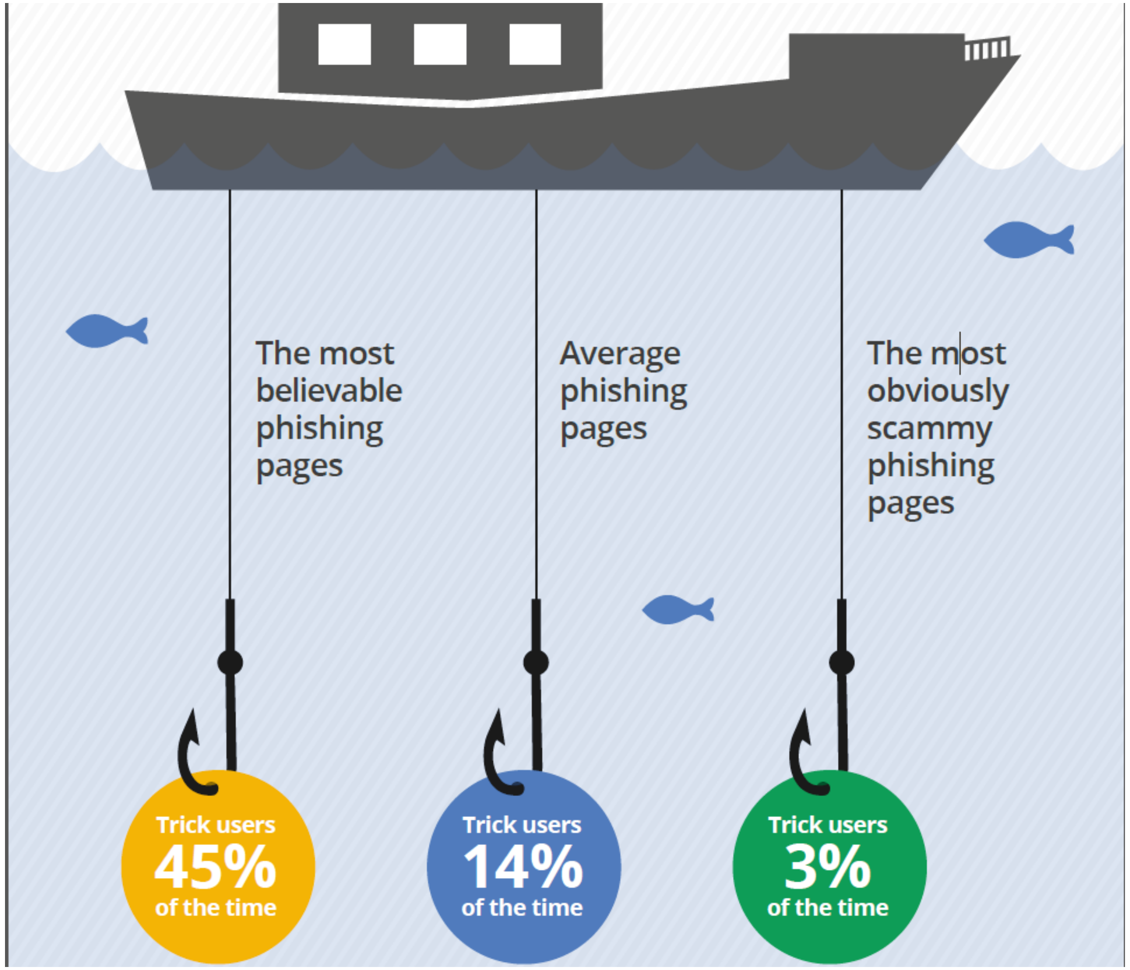
I’m at RegTech (super nervous about speaking tomorrow) and I just spoke with Ravi from the accounts team NNU. He said they hadn’t received our last two payments?? It was awkward.

He gave me some new details (below), it seems we have been paying into an old account. Could you please pay the past two months as soon as you possibly can? Then I can tell him it’s done. Counting on you.

Laura

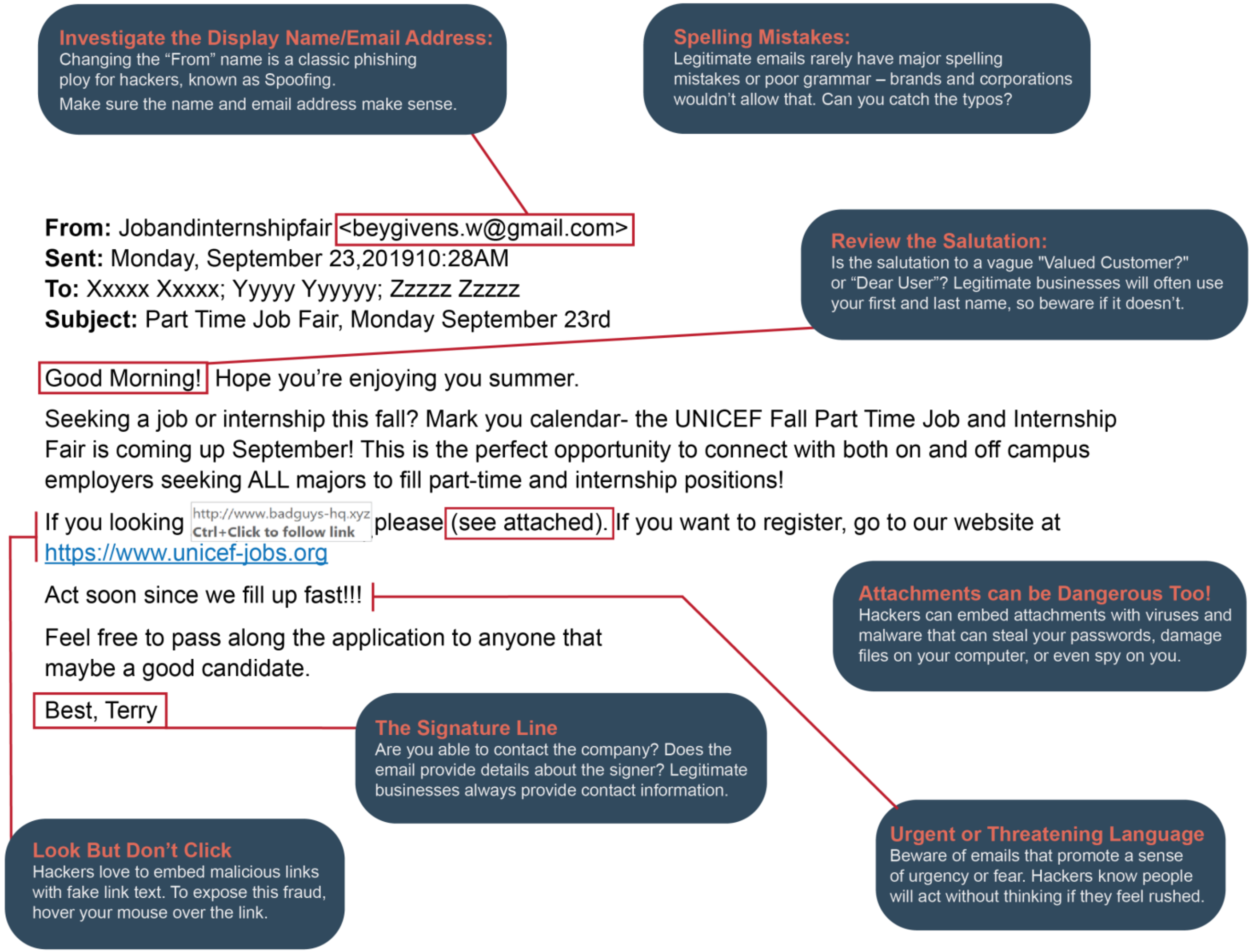
BakerHostetler

Phishing Emails



Source: Google, *Behind Enemy Lines in our war against account hijackers* (Nov. 2014)

How to Spot Phishing Emails



Investigate the Display Name/Email Address:
Changing the "From" name is a classic phishing ploy for hackers, known as Spoofing.
Make sure the name and email address make sense.

Spelling Mistakes:
Legitimate emails rarely have major spelling mistakes or poor grammar – brands and corporations wouldn't allow that. Can you catch the typos?

From: Jobandinternshipfair <beygivens.w@gmail.com>
Sent: Monday, September 23,201910:28AM
To: Xxxxx Xxxxx; Yyyyy Yyyyyy; Zzzzz Zzzzz
Subject: Part Time Job Fair, Monday September 23rd

Review the Salutation:
Is the salutation to a vague "Valued Customer?" or "Dear User"? Legitimate businesses will often use your first and last name, so beware if it doesn't.

Good Morning! Hope you're enjoying you summer.

Seeking a job or internship this fall? Mark you calendar- the UNICEF Fall Part Time Job and Internship Fair is coming up September! This is the perfect opportunity to connect with both on and off campus employers seeking ALL majors to fill part-time and internship positions!

If you looking http://www.badguys-hq.xyz Ctrl+Click to follow link please (see attached). If you want to register, go to our website at https://www.unicef-jobs.org

Act soon since we fill up fast!!!

Feel free to pass along the application to anyone that maybe a good candidate.

Best, Terry

Attachments can be Dangerous Too!
Hackers can embed attachments with viruses and malware that can steal your passwords, damage files on your computer, or even spy on you.

The Signature Line
Are you able to contact the company? Does the email provide details about the signer? Legitimate businesses always provide contact information.

Look But Don't Click
Hackers love to embed malicious links with fake link text. To expose this fraud, hover your mouse over the link.

Urgent or Threatening Language
Beware of emails that promote a sense of urgency or fear. Hackers know people will act without thinking if they feel rushed.

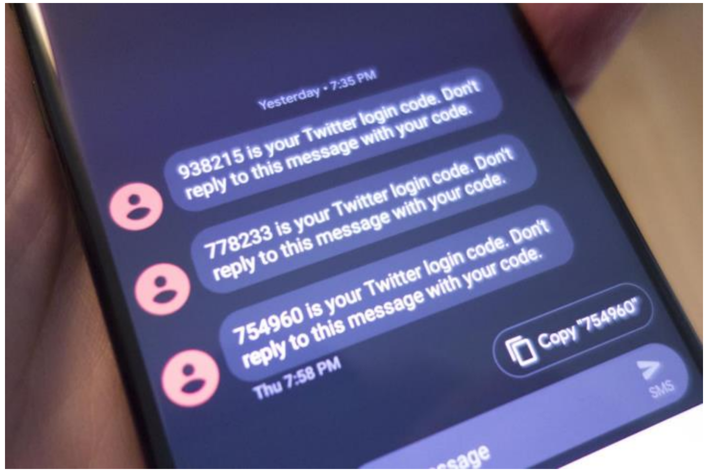
Source: https://it.ucmerced.edu/phishing

Best Defense Against Phishing

- Learn to Recognize Common Phishing Scams
- Be Careful With Attachments and Links
- Verify unusual requests by phone
- Implement Multifactor Authentication

Evolving Phishing Attacks

- More Sophisticated
- Voicemail / SMS / Automated Dialers
- Targeting MFA



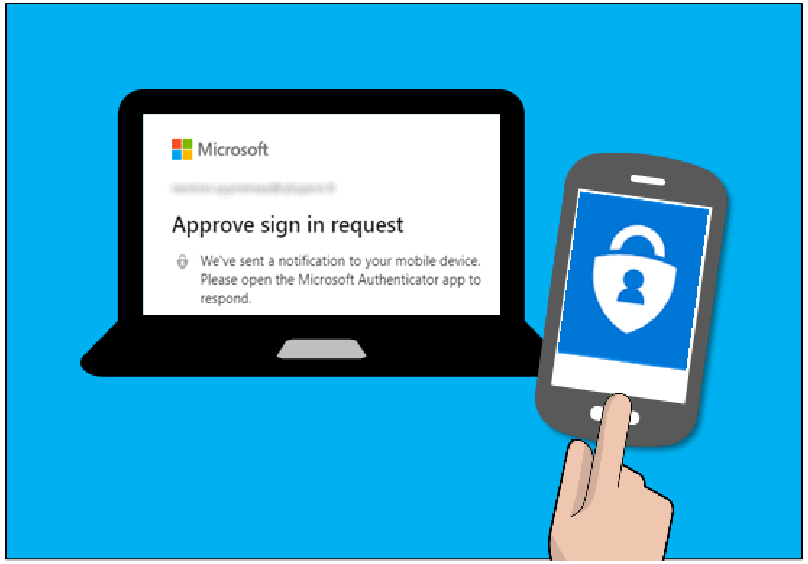
Yesterday • 7:35 PM

938215 is your Twitter login code. Don't reply to this message with your code.

778233 is your Twitter login code. Don't reply to this message with your code.

754960 is your Twitter login code. Don't reply to this message with your code.

Thu 7:58 PM



Microsoft

Approve sign in request

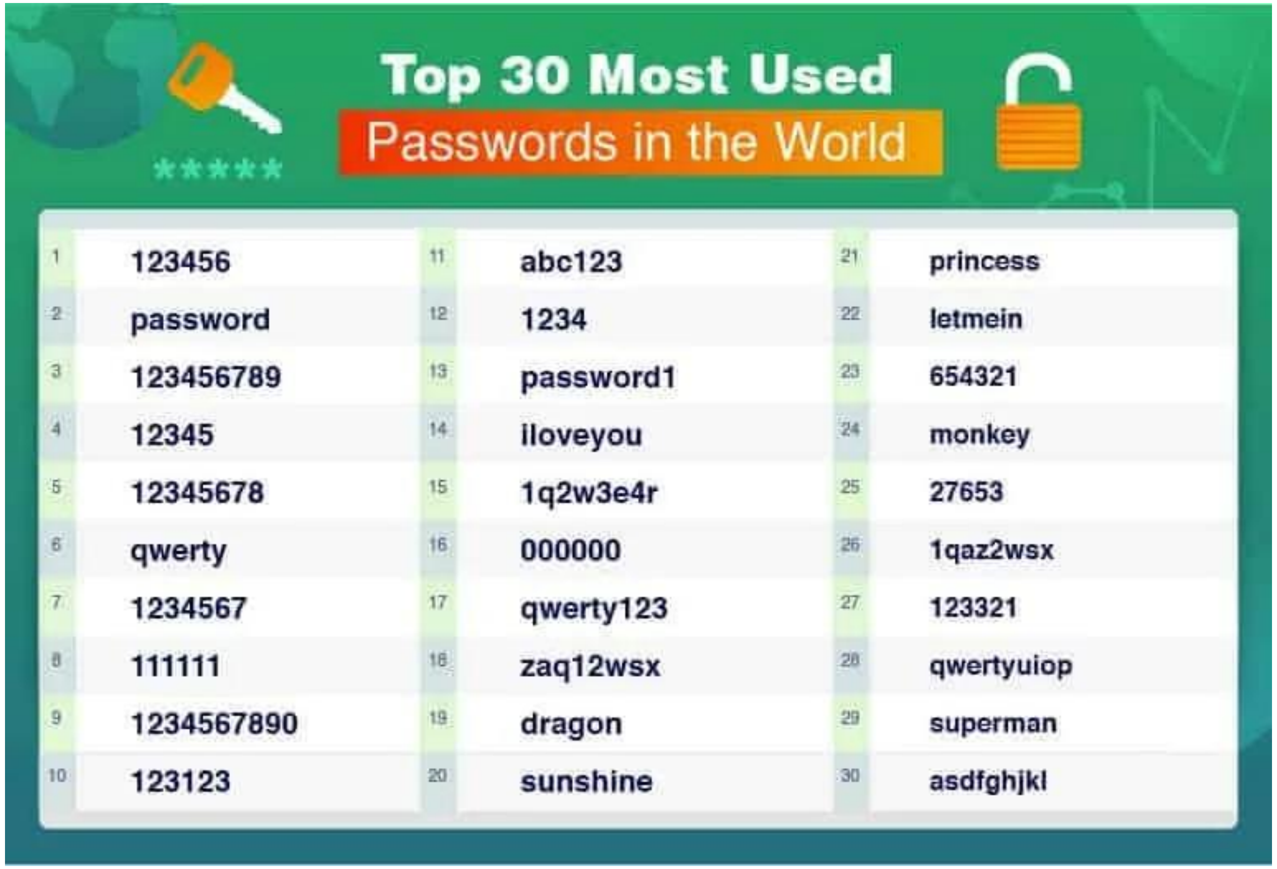
We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Network Intrusion

Involves Unauthorized Access to a Network Device or Cloud Asset

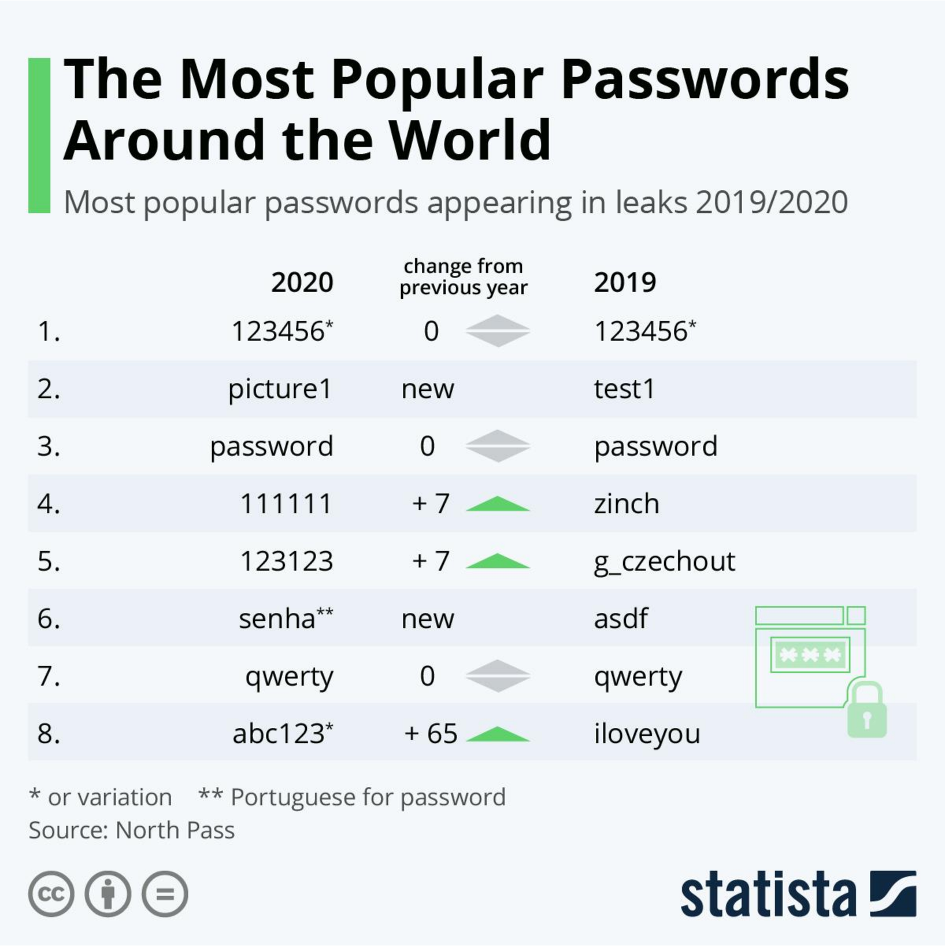
- Vulnerability
  - Log4J
  - SolarWinds
- Configuration Error
  - User Error (public vs. private AWS)
- Compromise of Credentials
  - Via Phishing
  - Brute Force
  - Credential Stuffing

Compromised Credentials – Brute Force



Top 30 Most Used Passwords in the World

1	123456	11	abc123	21	princess
2	password	12	1234	22	letmein
3	123456789	13	password1	23	654321
4	12345	14	iloveyou	24	monkey
5	12345678	15	1q2w3e4r	25	27653
6	qwerty	16	000000	26	1qaz2wsx
7	1234567	17	qwerty123	27	123321
8	111111	18	zaq12wsx	28	qwertyuiop
9	1234567890	19	dragon	29	superman
10	123123	20	sunshine	30	asdfghjkl



The Most Popular Passwords Around the World

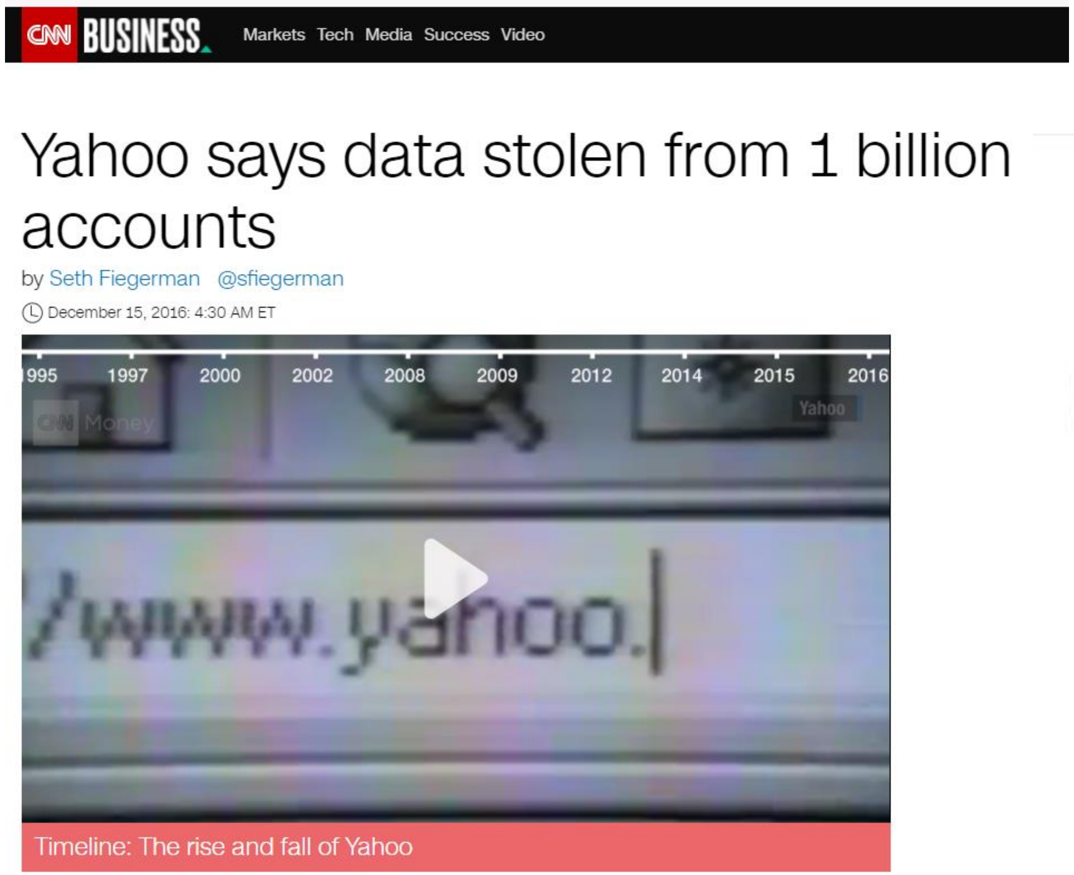
Most popular passwords appearing in leaks 2019/2020

	2020	change from previous year	2019
1.	123456*	0 ◆	123456*
2.	picture1	new	test1
3.	password	0 ◆	password
4.	111111	+ 7 ▲	zinch
5.	123123	+ 7 ▲	g_czechout
6.	senha**	new	asdf
7.	qwerty	0 ◆	qwerty
8.	abc123*	+ 65 ▲	iloveyou

* or variation ** Portuguese for password

Source: North Pass

Compromised Credentials – Credential Stuffing



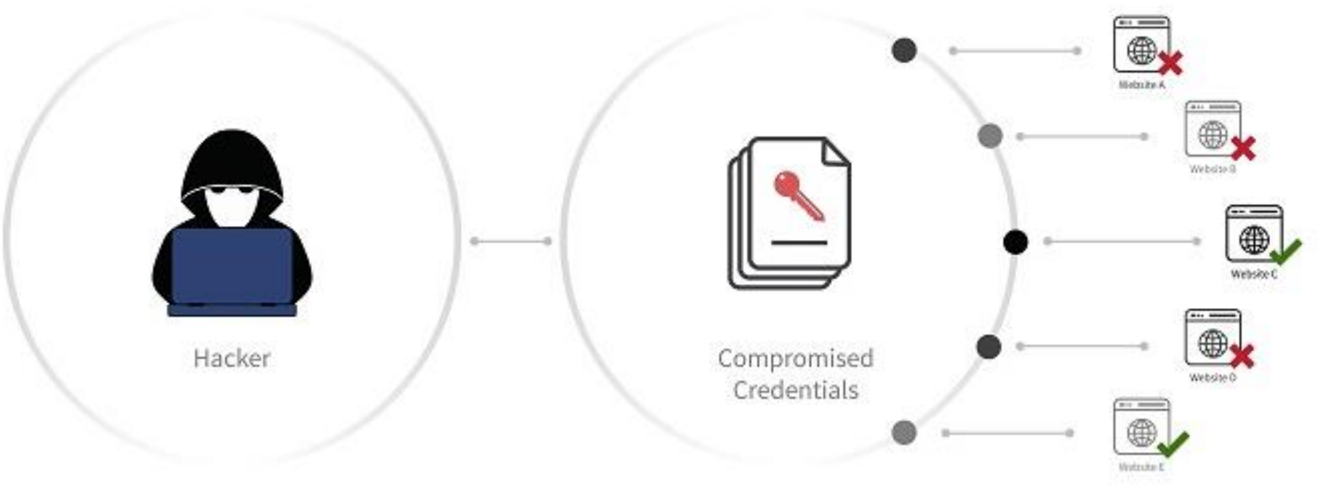
CNN BUSINESS Markets Tech Media Success Video

Yahoo says data stolen from 1 billion accounts

by Seth Fiegerman @sfiegerman

December 15, 2016: 4:30 AM ET

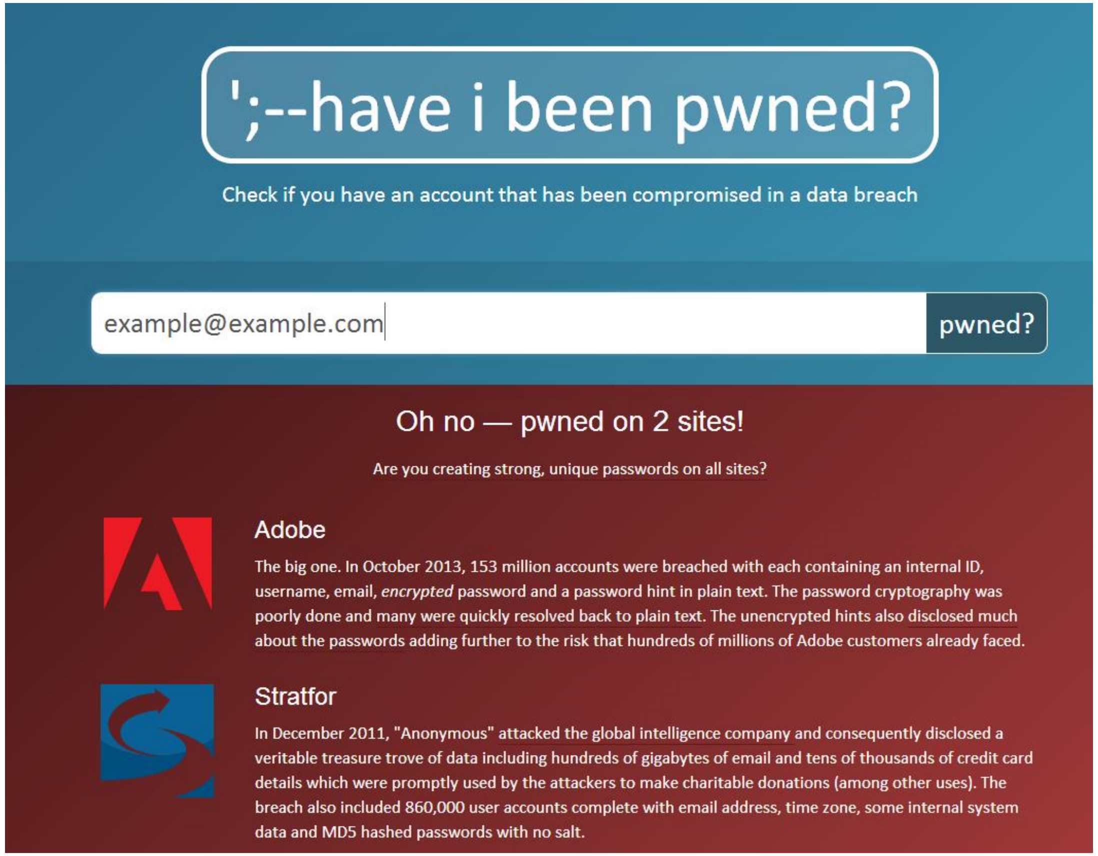
Timeline: The rise and fall of Yahoo



Attacker can test out the same credentials against many different sites, applications or services

Best Defense Against Credential Stuffing

- Use a password manager such as 1Password or LastPass.
- Change Passwords on a regular basis.
- Consider Checking “HaveIbeenpwned.com” for compromised passwords.



Check if you have an account that has been compromised in a data breach

Oh no — pwned on 2 sites!

Are you creating strong, unique passwords on all sites?

Adobe

The big one. In October 2013, 153 million accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Stratfor

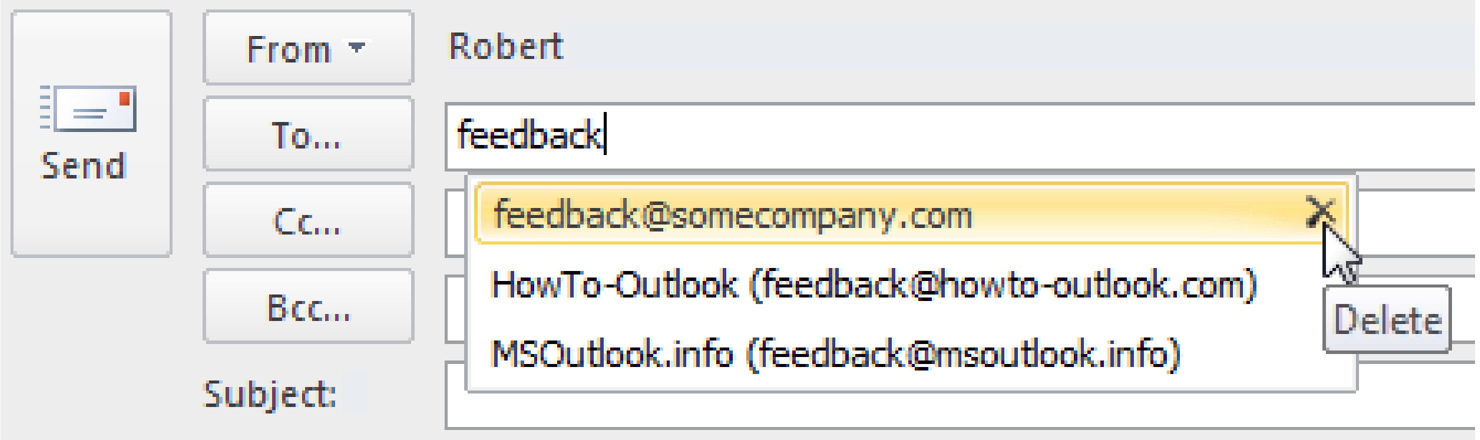
In December 2011, "Anonymous" attacked the global intelligence company and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Lost or Stolen Devices

- According to the FBI, a laptop is stolen every 53 seconds in the United States.
- Be Careful where you park.
- Apply these same measures to laptops, USB sticks, and portable hard drives.
- Where possible, ensure all Portable Devices Are Encrypted.

Inadvertent Disclosures

- Double Check the Recipient when sending emails or faxes.
- Avoid sending sensitive information via email.



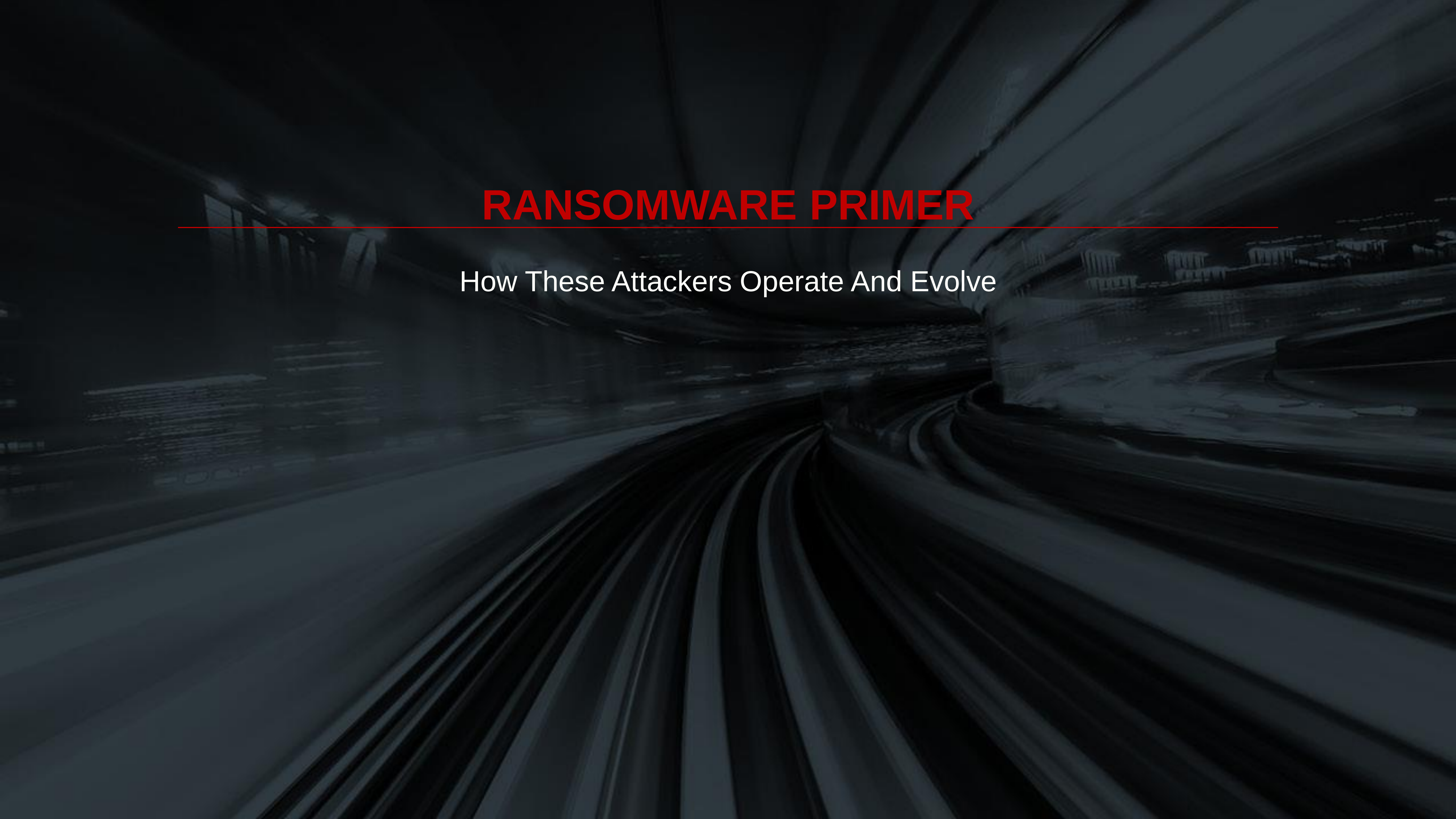
From ▾ Robert

To... feedback

feedback@somecompany.com ✕

HowTo-Outlook (feedback@howto-outlook.com)

MSOutlook.info (feedback@msoutlook.info)

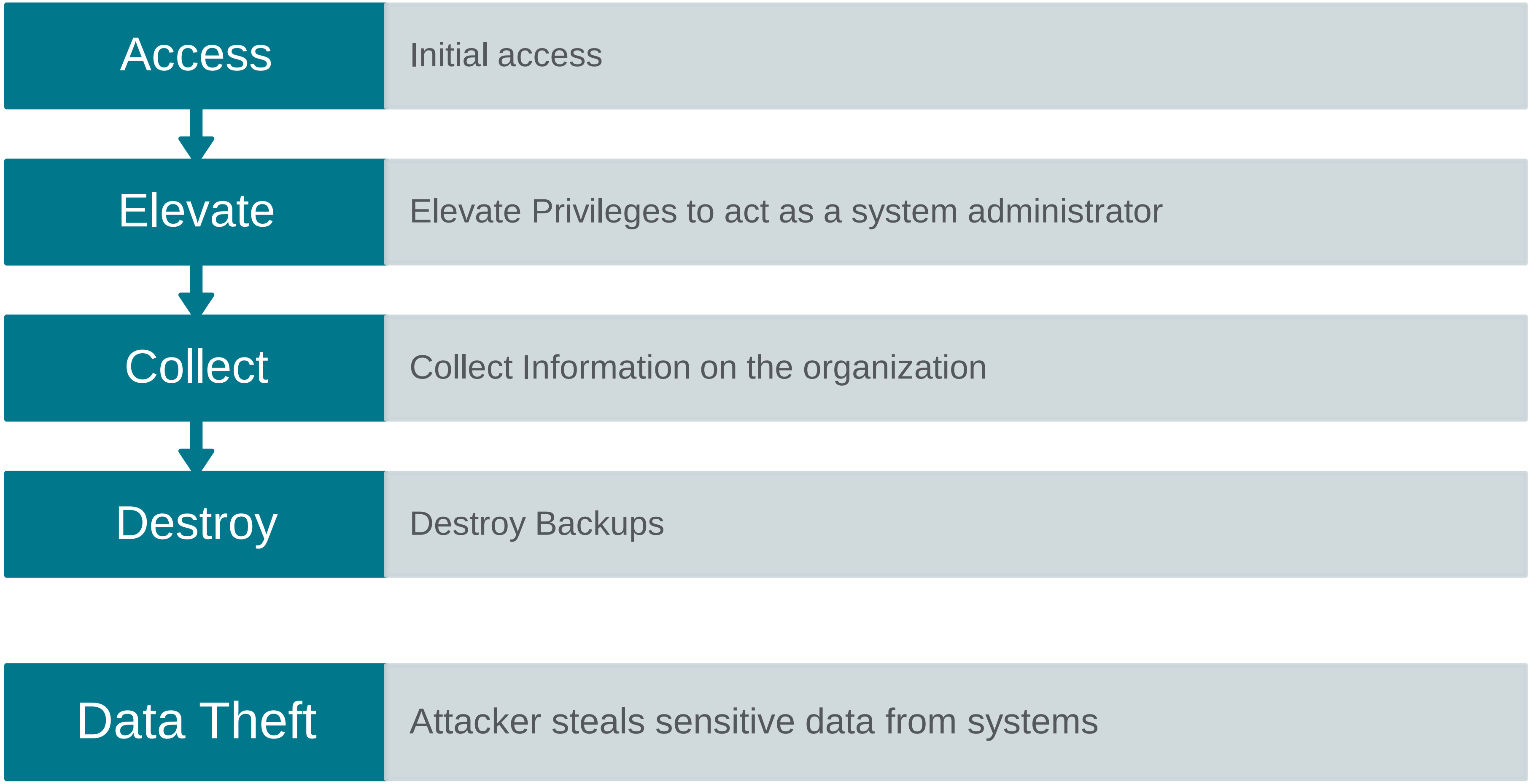


RANSOMWARE PRIMER

How These Attackers Operate And Evolve

YOUR PERSONAL FILES
ARE ENCRYPTED
Make payment or private key
will be destroyed in
12 Hours 01:34

Anatomy of an Attack – Phase 1



Access	Initial access
Elevate	Elevate Privileges to act as a system administrator
Collect	Collect Information on the organization
Destroy	Destroy Backups
Data Theft	Attacker steals sensitive data from systems

Anatomy of an Attack – Phase 2

Attacker deploys ransomware

Waits for contact

Negotiates payment

How to Respond to a Security Incident

- Learn to Identify Common Security Incidents
- Be Wary of Suspicious Emails and Attachments
- Verify Changes to Account Numbers or Payment Methods
- Don’t ignore suspicious activity. If you see something, say something.
- Be familiar with the breach reporting process at your organization and report potential incidents.
- Not just an IT Issue. Everyone is responsible for keeping the organization’s systems and data secure.

Q&A
You have
Questions
We have
Answers

BakerHostetler
bakerlaw.com

Atlanta | Chicago | Cincinnati | Cleveland | Columbus | Costa Mesa

Dallas | Denver | Houston | Los Angeles | New York | Orlando

Philadelphia | San Francisco | Seattle | Washington, D.C. | Wilmington

M. Scott Koller
mskoller@bakerlaw.com
310-928-7524

These materials have been prepared by Baker & Hostetler LLP for informational purposes only and are not legal advice. The information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel. You should consult a lawyer for individual advice regarding your own situation.