

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center



Connect **to**
Protect

SESSION ID: CRWD-R03

Getting Scammed: A Security CEO's Firsthand Encounter

Tom Kemp

CEO
Centrify
@ThomasRKemp



#RSAC

CEO Fraud: A Massively Growing Scam



#RSAC

CEO Fraud aka “Business Email Compromise” (BEC) is a scam that is “carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds”

Source: FBI, <http://www.ic3.gov/media/2015/150827-1.aspx>



CEO Fraud: A Massively Growing Scam



■ Growing dramatically

- 270% year over year increase in 1H 2015
- Reported in all 50 states and 70+ countries

Source: FBI, <http://www.ic3.gov/media/2015/150827-1.aspx>

\$1.2 Billion Scammed (and that's just what has been reported)



Some FBI stats

The following BEC statistics were reported to the Internet Crime Complaint Center from **October 2013 to August 2015**:

Total U.S. Victims:	7,066
Total U.S. exposed dollar loss:	\$747,659,840.63
Total non-U.S. victims:	1,113
Total non-U.S. exposed dollar loss:	\$51,238,118.62
Combined victims:	8,179
Combined exposed dollar loss:	\$798,897,959.25

These totals, combined with those identified by international law enforcement agencies during this same time period, bring the BEC exposed loss to over \$1.2 billion.

Source: FBI, <http://www.ic3.gov/media/2015/150827-1.aspx>

But this only happens to less sophisticated companies, right?



Tech Firm Ubiquiti Suffers \$46M Cyberheist

BUSINESS FRAUD

On June 5, 2015, the Company determined that it had been the victim of a criminal fraud. The incident involved **employee impersonation and fraudulent requests** from an outside entity targeting the Company's finance department. This fraud **resulted in transfers of funds aggregating \$46.7 million** held by a Company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties. As soon as the Company became aware of this fraudulent activity it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions. As a result of these efforts, the Company has recovered \$8.1 million of the amounts transferred. Furthermore, an **additional \$6.8 million of the amounts transferred are currently subject to legal injunction** and reasonably expected to be recovered by the Company in due course. The Company is continuing to pursue the recovery of the remaining \$31.8 million and is cooperating with U.S. federal and numerous overseas law enforcement authorities who are actively pursuing a multi-agency criminal investigation. The Company may be limited in what information it can disclose due to the ongoing investigation. The ultimate amount of the loss will depend, in part, on the Company's success in recovering the funds. The Company may not be successful in obtaining any insurance coverage for this loss. The Company currently believes this is an isolated event and does not believe its technology systems have been compromised or that Company data has been exposed. While this matter will result in some additional near-term expenses, the Company does not expect this incident to have a material impact on its business or its ability to fund the anticipated working capital, capital expenditures and other liquidity requirements of its ongoing operations.

Source: Krebs on Security, SEC Filing https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

And the scam stretches from the Great Plains and across Europe



#RSAC

Impostors bilk Omaha's Scoular Co. out of \$17.2 million

Story Comments Image (2)

Print Font Size: + -

Like 177 Share

News Alerts G+

POSTED: THURSDAY, FEBRUARY 5, 2015
1:00 AM

By Russell Hubbard / World-Herald staff writer

Corporate cybercrime on an international scale has hit one of Omaha's biggest and oldest companies.

The Scoular Co., an employee-owned commodities trader founded 120 years ago, has been taken for \$17.2 million in an international email swindle, according to federal court documents.



Chuck Elisea

French businesses have lost an estimated €465m since 2010, official figures suggest, with 15,000 firms falling victim to the scam, including big names, such as Michelin, KPMG and Nestle.



Tyre maker Michelin is one of many French big-name firms who've fallen for the fraud

The biggest fraud was for €32m, and a further €830m could have been stolen if more phishing attacks had proved successful, say French police.

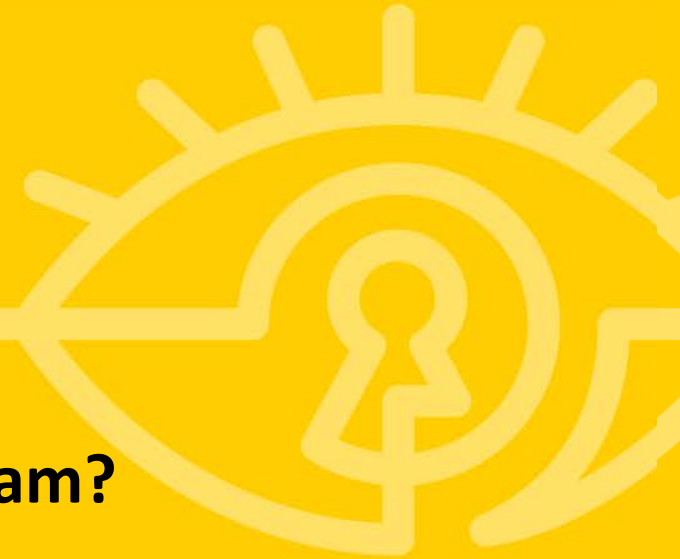


Source: http://www.omaha.com/money/impostors-bilk-omaha-s-soular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html
and <http://www.bbc.com/news/business-35250678>

RSA Conference 2016



So How Did I Get Exposed to this Scam?



February 12, 2014, 11:00 a.m.



#RSAC



Tom the CEO

CEO strolls into office at 11:00 a.m., walks by CFO office towards his office
CFO looks up, sees CEO walking by, and says:

“Hey Tom, Jennifer [Corporate Controller] is working on that wire transfer you requested this morning.”



Tim the CFO



Tom the CEO

“Huh? I did not request a wire transfer ...”

“Hmmmm ... let me look into what was sent to her”

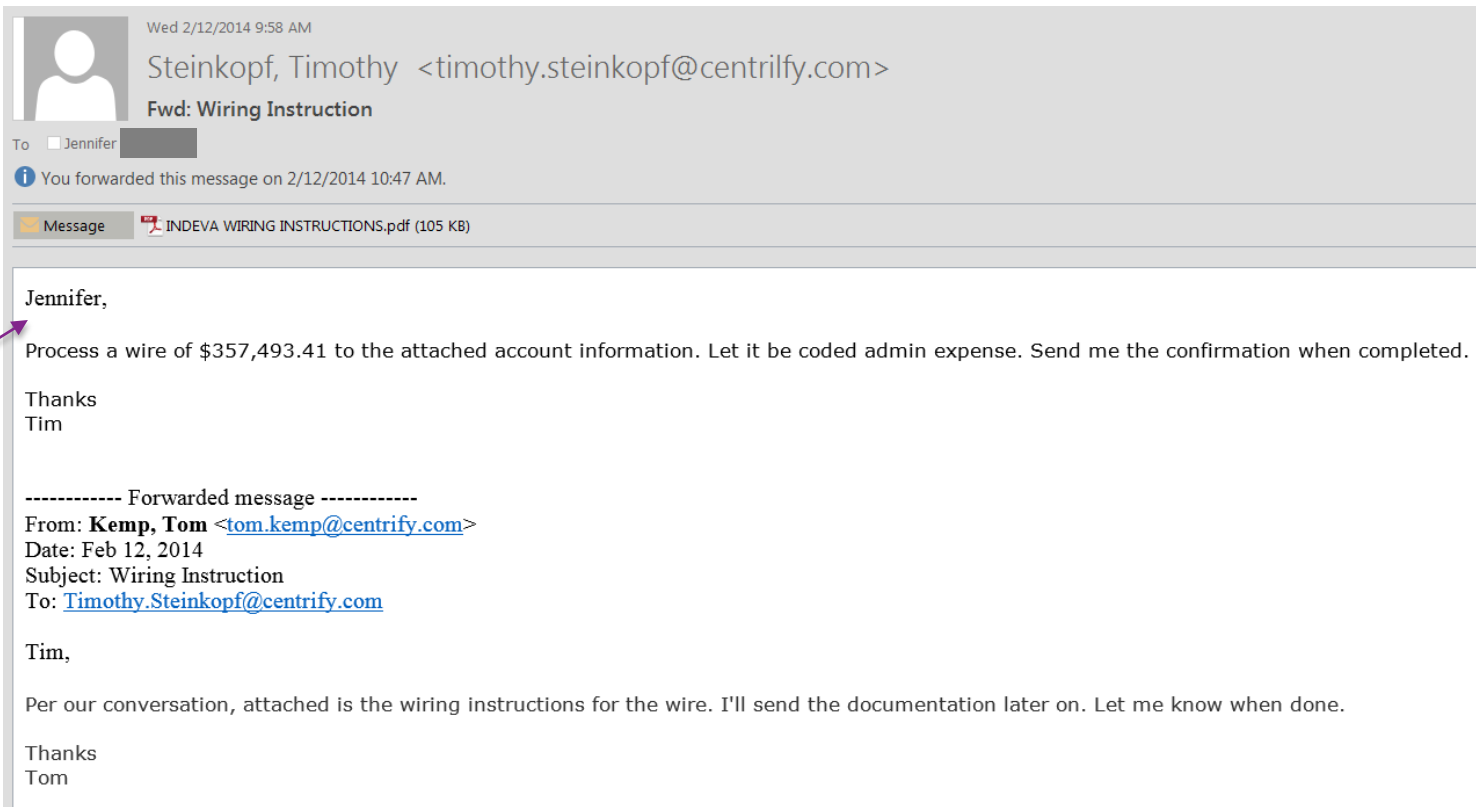


Tim the CFO

The Email Our Controller Received at 9:58 a.m.



#RSAC



Email from
CEO to CFO
forwarded to
Controller

With Attachment Going to Legit Bank



#RSAC

INDEVA WIRING INSTRUCTIONS

CITI BANK

734 Third Avenue

NEW YORK, NY 10017

Account #: 9982130330

Routing #: 021000089

Credit to: INDEVA CORPORATION

And When Controller Did Reply, Got Response



#RSAC



Wed 2/12/2014 10:34 AM

Steinkopf, Timothy <timothy.steinkopf@centrify.com>

Re: Wiring Instruction

To: Jennifer [REDACTED]

Yes. Send me the confirmation once complete.

on Feb 12, 2014, Jennifer [REDACTED]@centrify.com> wrote:

Can I send this to Flora? I normally approve the wires, not initiate.

From: Steinkopf, Timothy [<mailto:timothy.steinkopf@centrify.com>]

Sent: Wednesday, February 12, 2014 9:58 AM

To: Jennifer [REDACTED]

Subject: Fwd: Wiring Instruction

Note
separation
of duties

Accounting Was Scrutinizing the Wire Transfer Request Independent of CEO/CFO Convo



#RSAC



Wed 2/12/2014 11:12 AM

Jennifer [redacted]

FW: Wiring Instruction

To: Tim Steinkopf

Also, is there some sort of paperwork for the wire? I think for control purposes we should have something attached to a wire this size.

From: [redacted]
Sent: Wednesday, February 12, 2014 11:09 AM
To: Jennifer [redacted]
Subject: RE: Wiring Instruction

Hi Jennifer,

We need Indeva's address as the beneficiary info is a mandatory field for setting up the wiring template. Once the template is set up, it needs to be approved.

In addition, we do not have an admin GL account. The closest one I found was account 6606: outside consultants. Should we set up a new account?

Thanks,
Flora

From: Jennifer [redacted]
Sent: Wednesday, February 12, 2014 10:48 AM
To: [redacted]
Subject: FW: Wiring Instruction

Can you please process this wire and let me know when I can approve in SBV. thx

Note doc requirements

But Given CEO/CFO Convo, We Looked a Bit Closer at the Email Trail...and Voila!



Wed 2/12/2014 9:58 AM

Steinkopf, Timothy <timothy.steinkopf@centrify.com>

Fwd: Wiring Instruction

To: Jennifer

You forwarded this message on 2/12/2014 10:47 AM.

Message INDEVA WIRING INSTRUCTIONS.pdf (105 KB)

Jennifer,

Process a wire of \$357,493.41 to the attached account information. Let it be coded admin expense. Send me the confirmation when completed.

Thanks
Tim

----- Forwarded message -----

From: **Kemp, Tom** <tom.kemp@centrify.com>
Date: Feb 12, 2014
Subject: Wiring Instruction
To: Timothy.Steinkopf@centrify.com

Tim,

Per our conversation, attached is the wiring instructions for the wire. I'll send the documentation later on. Let me know when done.

Thanks
Tom

<timothy.steinkopf@centrify.com>

An "I" was inserted
into our domain name

And different fonts





Thinking there was a targeted and sophisticated attack on us...

- Bad guys created a look-a-like domain and created email accounts with our exec team members
- Figured out our org structure to send an email to our controller
- Was actively engaging with us via email
- Provided a legitimate sounding company name and a real bank (Citi) to send the money to

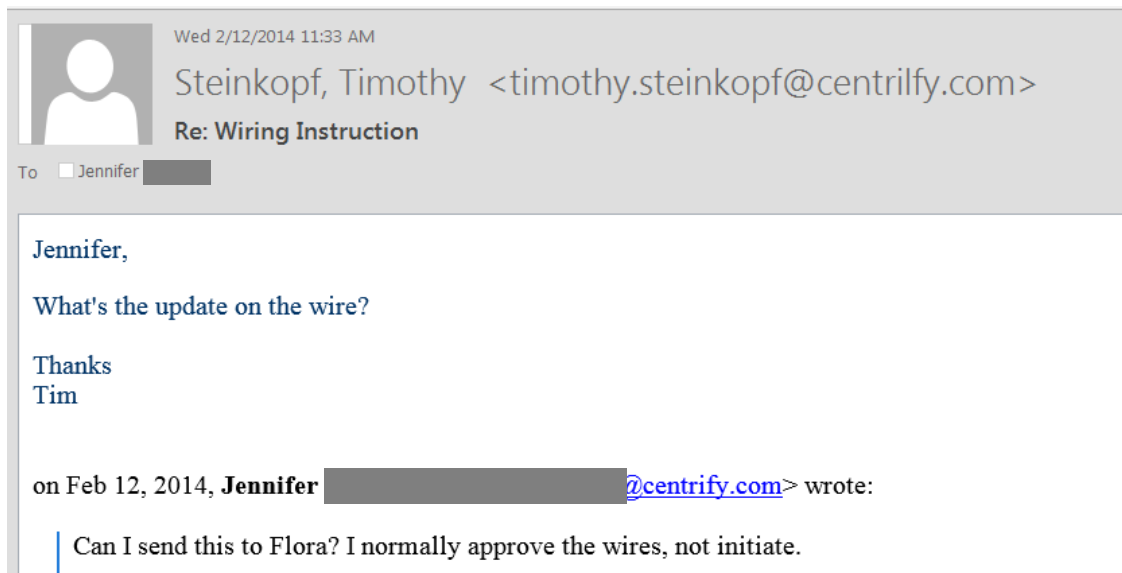
...we called the FBI while in parallel tried to track down who had centrify.com

Crooks Kept At It ...



#RSAC

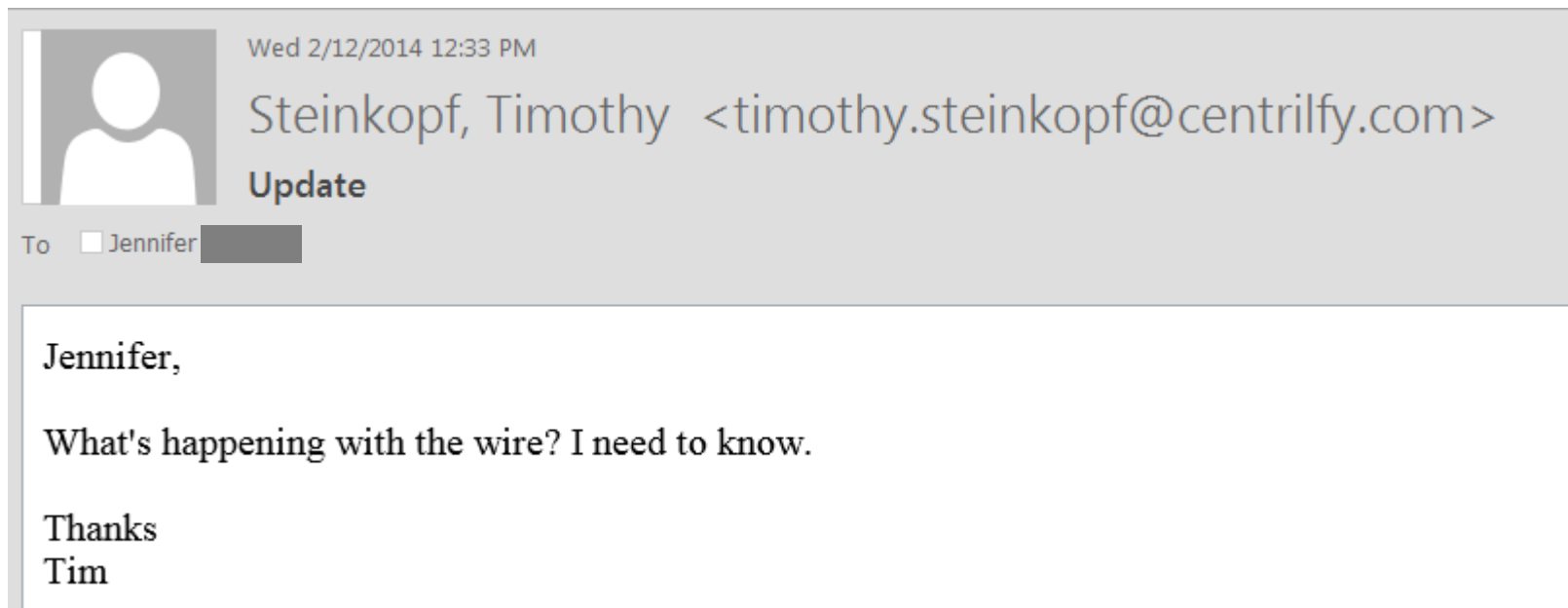
While on hold with the FBI to report a crime, the criminal at same time would contact us asking for updates



And Contacted Us Once More



#RSAC



By then we had finally got in touch with FBI and they told us not to respond

In Parallel We Raced to Track Down Who Had Created the Look-a-like Domain



#RSAC

Was created that same morning by someone using VistaPrint

Domain Name: CENTRILFY.COM
Registry Domain ID: 1846338047_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: <http://tucowsdomains.com>
Updated Date: 2014-02-12 08:22:48
Creation Date: 2014-02-12 13:22:47
Registrar Registration Expiration Date: 2015-02-12 13:22:47
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Reseller: Vistaprint
Reseller: csadmin@vistaprint.com
Reseller: 866-811-1674
Domain Status: clientTransferProhibited
Domain Status: clientUpdateProhibited
Registry Registrant ID:
Registrant Name: VistaPrint Technologies
Registrant Organization: c/o Vistaprint North American Services Corp.

We Then Experienced the Joys of Being Put on Hold by VistaPrint for a Few Hours



From: Frank [REDACTED]@centrify.com]

↑ Next ↑ Last

Sent: Wednesday, February 12, 2014 3:38 PM

To: Trademark

Subject: Urgent complaint requiring immediate action: Socially engineered fraud from VP-hosted domain

Importance: High

THIS IS NOT A TRADEMARK ISSUE. THIS IS A CURRENTLY IN-PROGRESS FRAUD EXPLOIT THAT IS ALSO BEING REPORTED TO LAW ENFORCEMENT.

Domain involved: centrify.com

Issue: We received a bogus wire request for \$350,000 specifically addressed to our accountant and including fraudulent “approvals” from the CEO and CFO. All persons were specifically named. This implies a high degree of specific targeting against our company.

We would like to ensure this domain, which is linked with illegal activity, is de-activated.

WHY THE URGENCY: The specific concern is that the same social engineering hacks may target our customers and other business associates. If they are not wary, they might be exploited.

Please advise ASAP of next steps and guidance.

Regards,

Frank [REDACTED]

Emails like this were sent





After a Few Hours Finally Were Finally Able to Talk to Someone at VistaPrint






They killed the look-a-like domain

Wed 2/12/2014 3:58 PM

 Frank 

FW: Urgent complaint requiring immediate action: Socially engineered fraud from VP-hosted domain

To  Tom Kemp;  Tim Steinkopf

 You replied to this message on 2/12/2014 3:59 PM.

Email reply from Vistaprint. She also called. Key points:

- Feel free to provide her contact information to the authorities and she will share what she knows when she receives a verifiable request from law enforcement.
- The individual is using their "free 30 day account" and has registered a number of domains. "You were not the only target" she said.

F.

And were verbally told 60+ look-like-a-like domains had been created that morning

Prologue to this CEO Fraud Attempt



- Reported to FBI but never heard back
- Similar scam attempts were publicly reported utilizing VistaPrint

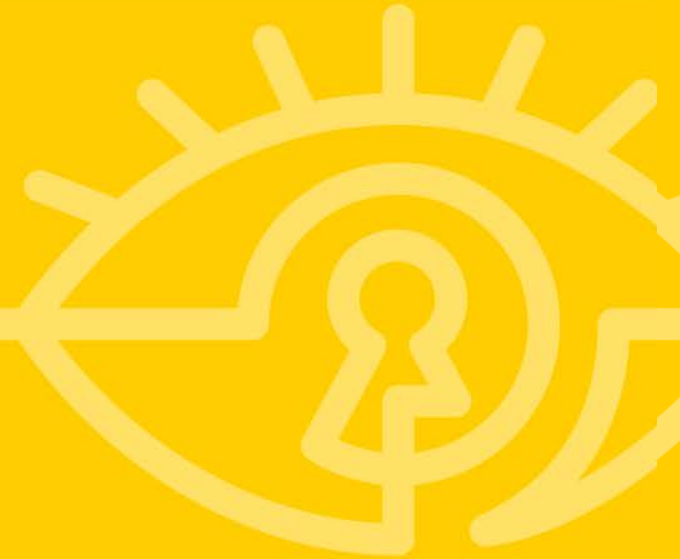
In the case of the above-mentioned Ohio manufacturing firm that nearly lost \$315,000, that company determined that the fraudsters had just hours before the attack registered the phony domain and associated email account with **Vistaprint**, which offers a free one-month trial for companies looking to quickly set up a Web site.

- PhishMe has good blog on VistaPrint

Source: Krebs on Security, <http://krebsonsecurity.com/tag/ceo-fraud/> and <http://phishme.com/vistaprint-abuse-free-phish-for-all/>



So Have the Scams Stopped?



No, Problem Getting Worse



Per my intro, growing 270%

- Thieves continue to impersonate CEOs and CFOs and email people (e.g. controller, AP clerk, etc.) in the organization that can facilitate the wire transfer
- Will have very persuasive language and appeal to employee's desire to please the CEO/CFO
 - **Use of authority:** it is an order to do this
 - **Secrecy:** The project is still secret and its success depends on this transaction
 - **Valorization:** I count on you for your efficiency and discretion
 - **Pressure:** The success of the project rests on your shoulders

Source: <http://www2.deloitte.com/lu/en/pages/about-deloitte/articles/fake-presidents.html>

And We Keep Getting Targeted



- We probably get 1-2 a month now
- Some will have variations of “Centrify” domain
- But most emails are spoofs of someone sending an email from me or the CFO and if you were to reply would go to a different email account



- Feb 4, 2015: An email from CEO to CFO asking for a wire transfer.
- Note the domain was “cenrtify.com,” the “r” and “t” of “centrify” were flipped around.

From: tomk@cenrtify.com [<mailto:tomk@cenrtify.com>]
Sent: Wednesday, February 04, 2015 5:35 AM
To: Tim Steinkopf
Subject: Fwd Wiring Instructions

Timothy,

Process a wire of **\$145,850.00USD** to the attached account information. Code it to Misc expenses.

Thanks

Another Example



- August 17, 2015: An email from CEO to CFO.
- If you were to reply, it would go to a charlyman2112 gmail account.

From: Tom Kemp [<mailto:tom.kemp@centrify.com>]
Sent: Monday, August 17, 2015 5:34 AM
To: Tim Steinkopf
Subject: Transfer

Tim, I want you to initiate a wire transfer to a client, confirm back to me so if you can now so I can provide you with the beneficiary details to transfer the funds.

Trust Me, Everyone's Getting it Now



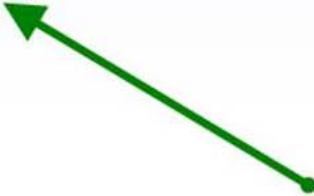
Even my Dad's 50-person leasing company in Michigan is getting this

From: John Kemp [<mailto:jkemp@laesecorp.com>]

Sent: Wednesday, January 20, 2016 11:54 AM

To: [REDACTED]

Subject: RE: Payment to process.



Can you please wire \$38,000 to the attached? Pretty urgent to have the transfer done this morning, reference payment with INV72910 and code to Admin expenses.

Notify me by email once it's done.



Suggestions for Protecting Your Company Against this Scam



Key Takeaways



#RSAC

- Immediately educate your accounting team, e.g. send entire finance department an article like
 - <http://fortune.com/2015/10/13/ceo-wire-transfer-scam/>
 - <http://blog.centrify.com/ceo-fraud-business-email-compromise/>



Key Takeaways



#RSAC

- Sit down with your CFO and make sure that proper documentation and approvals are required for all money transfers, e.g.
 - Make sure that any wire transfer is associated and maps with an actual purchase inside the accounting system
 - Determine if a separation of duties exist between initiator and approver of wire transfers
 - For large wire transfers, request that G&A add a phone call to the approval process





- Register any look-a-like domain names, e.g.
 - if you have a “i” in your domain name, buy the domain where a lower case “l” is swapped for the “i”
 - if you have an “e” in your domain name buy the domain that has a “3” for an “e” etc.

Centrify

Other Suggestions



#RSAC

- Add **multi-factor authentication** to all key apps (including financial systems), so users can confirm they really are who they claim to be (e.g. when initiating a wire transfer)



Other Suggestions



#RSAC

- Also layer on other identity controls such as **privileged session monitoring** for sensitive systems — this is in case the crooks have compromised the credentials of key employees in Finance.





- Per the FBI “create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, legitimate e-mail of *abc_company.com* would flag fraudulent e-mail of *abc-company.com*”

abc_company.com
abc-company.com

Source: FBI, <http://www.ic3.gov/media/2015/150827-1.aspx>



- “CEO Fraud” is a big problem that is growing dramatically and is impacting all sizes of companies in all regions of the world
- Feeds off of culture of:
 - (a) CEO being able to get what they want with no questions asked and...
 - (b) lack of checks and balances within accounting when it comes to wire transfers





- Educating accounting teams is critically important
- Implementing MFA and privileged account management beyond IT personnel to your finance departments is also key

Questions? DM me at ThomasRKemp