

RSA[®]Conference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: **SOP-W06**

91% of Attacks Start with Email: Fix Your Human Firewall Flaws



#RSAC



Connect **to**
Protect

Steven Malone

Cybersecurity Strategist
Mimecast
Twitter: @Steven_Malone

Original Phishing Scams – What Do You Notice About Them?



Naomi Surugaba [a[REDACTED]@[REDACTED].gov.my]

Inbox

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.

They're Still Around And Have Gotten Creative



Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progresh supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [REDACTED] only.



Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager

[REDACTED]

[http://www.\[REDACTED\]](http://www.[REDACTED])

And They Do Not Discriminate Who They Target – No One Is Safe




  July 26 at 11:23pm · Mytilene, Greece · 🌐



Yea, you know you're an established NGO when the dead lawyers come back to life JUST to email you and request Advocates Abroad to help their clients. Oh and there's \$8.5 million in it for you because her father is a super wealthy Nigerian prince.

Honestly, dead lawyer, I'm offended. Everyone knows we're a non-profit that has never, and will never, take payment for any service provided to asylum seekers or refugees. Like, get it together.

#spammersbegone!

👍 Like 💬 Comment ➦ Share


👍 🙄  and 23 others

  Dear Friend.


How are you doing, I hope you're okay? Please I request your assistance to help my client, who lost her parents and brother during the crisis in Ivory Coast cause by Ivory Coast President (Laurent Gbagbo) . My client is currently in the refugee camp and my country is too poor to provide a good living for people in the refugee camp. My clients father is the prince in another country of Africa who had money worth \$8.5 million dollars deposited in private security company and the money was registered for safe keeping as family treasured without knowing that he would die in 2011 February 2011 when rebels hit my client father house with bomb and killed everyone in the building, including their parents business associate who is a French woman.

I want to seek help for the girl to help her move money in your country and invest her money in profitable area, I am the deceased family lawyer when he was alive. May their souls rest in peace.

Like · Reply · 🍷 3 · July 26 at 4:28pm

 Like literally. You can not make up half the crazy nonsense I have to deal with on a daily basis.

Like · Reply · 🍷 3 · July 26 at 4:29pm

 However, I do award the dead lawyer points for correctly citing the President in his term of office and that chaos. That and the mention of the refugee camp made me reread this thing, before I could dismiss it. Very irritating.

Like · Reply · 🍷 3 · July 26 at 4:32pm

They're Not Necessarily Even Sophisticated Attacks – Yet They're Still Successful



Reply-To: "[REDACTED]" <President_office@aol.com>
To:
Subject: Request
Date: Mon, 25 Apr 2016 16:12:41 -0700
Mime-Version: 1.0
X-MC-Unique: 65n_7iqPRWyrolWPbKr3GA-1
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: quoted-printable

From: [REDACTED]
Sent: Monday, April 25, 2016 6:13 PM
Subject: Request

Hi [REDACTED],
Please send me the list of W-2 copy of all employees wage and tax statement for 2015.
Kindly prepare the report in PDF and send via email.
Thanks,
[REDACTED]
PRESIDENT

You Don't Even Need To Know How To Code



Botnets & Malware

Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...



Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE

----- Stampado Ransomware ----- You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :)
Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...

Sold by [The_Rainmaker](#) - 2 sold since Jul 12, 2016

Vendor Level 1

Trust Level 5

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

“Stampado encrypts files and gives the victim 96 hours to pay a ransom. It’s advertised as fully undetectable and can be deployed in .exe, .bat, .dll, .scr and .cmd files. In an added twist, Stampado deletes a randomly selected file every six hours if the ransom is not paid.”

Source: Forbes.com - "Ransomware As A Service Being Offered For \$39 On The Dark Net" 7/15/16

“The risk doesn't go away, it just changes its nature.”



- Attackers have evolved
 - You need to evolve with them
 - Your products need to evolve even faster
- Ransomware has become RaaS
- Wire transfer scams are on the rise
- Users are preyed upon
 - Do you honestly trust your users?

Attackers Are Not Slowing Down – And They Don't Plan To Either



- In the past 18 months, 1,300% increase in identified losses in excess of \$3.1 Billion
- All 50 U.S. states
- 100+ Countries
- Fraudulent transfers sent to 79 countries

It's Not Just About Wire Transfers!



- Data Mining is incredibly valuable
 - Employee W2s
 - Insider information
 - Proprietary data
 - Upcoming changes in the company
- Think of all the variations of attacks using the data they are able to pull
 - Identity theft
 - Stock manipulation
 - Leaking inside “trade” secrets



What you think your security looks like



What your security actually looks like

You are at risk if...



- You have certain letters in your company name
- You showcase your senior employees
- You accept resumes on your website
- You have an active social presence
- Your users share on social media

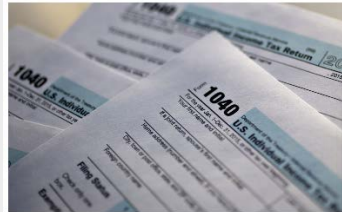


In the Headlines



Beware of This Latest IRS Phishing Scam

by Michal Adinly | @michal_adinly | MARCH 14, 2016, 6:48 PM EDT

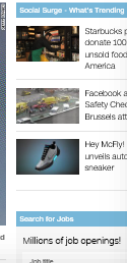
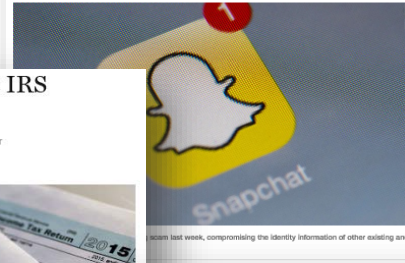


"Don't be fooled."

The IRS is warning taxpayers against scammers' newest tactic.

The agency wrote on its [website](#) that it has received reports of taxpayers being contacted by people claiming to be IRS agents, asking for personal and financial information over the phone. They use certain personal information, like the taxpayer's name and address, as well as false badge numbers and IRS titles to present themselves as legitimate agents. They have also been known to adjust their caller ID

1040 Individual Income Tax Return for the 2015 tax year
Photograph by Andrew Brown - Bloomberg via Getty



Hackers carry out \$55m cyber heist from Boeing aerospace parts manufacturer

By James Billington
January 27, 2016 20:25 GMT



Manufacturer in a \$55 million spear phishing heist (CNN)

Manufacturer that supplies engine and interior parts for the likes of Airbus and Boeing, a massive cyber attack that has seen hackers take off with \$55m (£50m), the company's accounts.

Company that has been a supplier to Airbus since 1989, revealed on its 19 January the finance department "was the target of cyber fraud and related activities involving communication and information technologies".

The company, which makes overhead cabins and engines for business and commercial jets, went on to say that extent of the hack appeared to be purely money-focussed rather than a theft of intellectual property for its designs with "the damage an outflow of approximately EUR 50 million of liquid funds".

Anthem Breach: Phishing Attack Cited

Phishing Campaigns Now Targeting Anthem Members

Anthony J. Schwartz | @anthonyj_schwartz | February 9, 2015 | 1 Comment

Twitter Facebook LinkedIn Create Egle I Get Permission



Anthem Inc. believes that the attack that compromised up to 80 million personally identifiable information may have begun with phishing e-mails sent to employees. This is just one of several options being investigated as the cause of the breach. The insurer also warned members that the data breach is being used as a tool by telephone scammers.

King Software Innovation with Secure Data as a Service

and-largest U.S. health insurer, says that the data breach likely began as



70% of attacks lead to secondary target

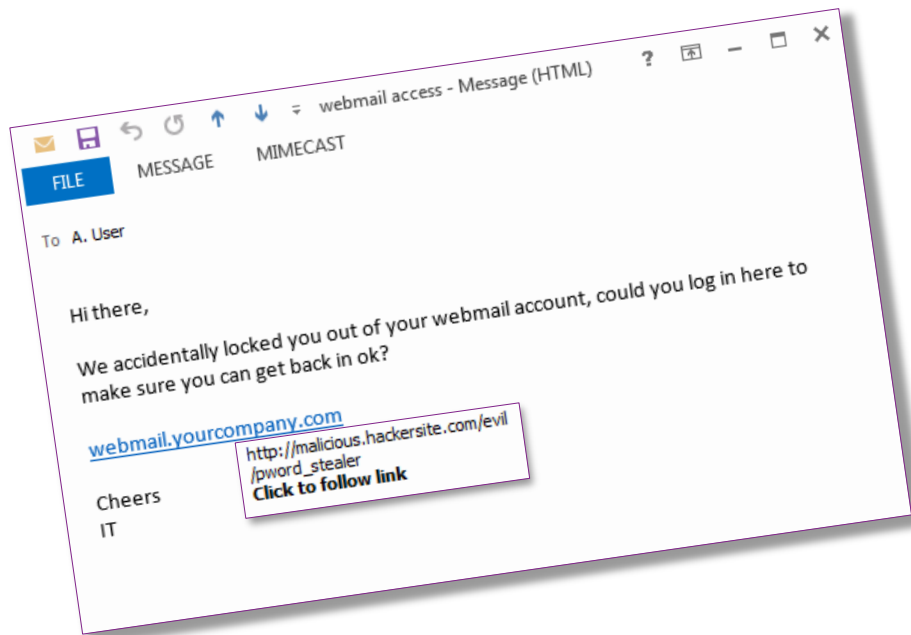
Verizon 2015 Data Breach Investigations Report (DBIR)



Which means: You could be the stepping stone or ‘pivot’

Verizon 2015 Data Breach Investigations Report (DBIR)

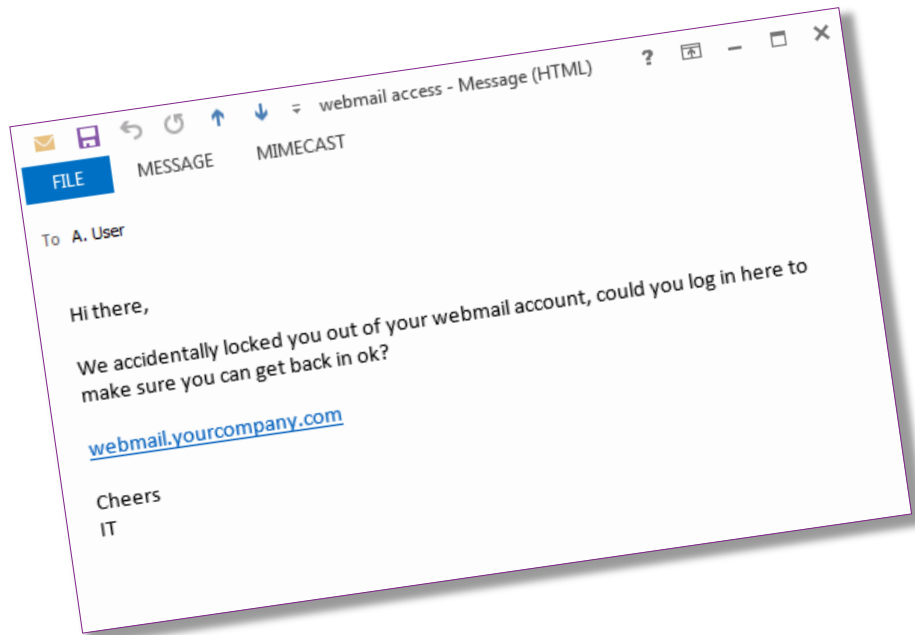
91% of all incidents start with a phish



Wired 2015

1 minute 22 seconds

a phish: median time-to-first-click



Verizon 2015 Data Breach Investigations Report (DBIR)



**23% open the
phish & click
the link**

Verizon 2013 Data Breach Investigations Report (DBIR)



13% open the
phish & run the
attachment

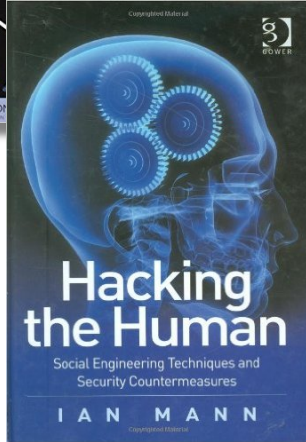
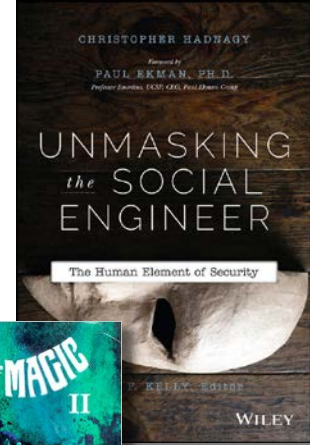
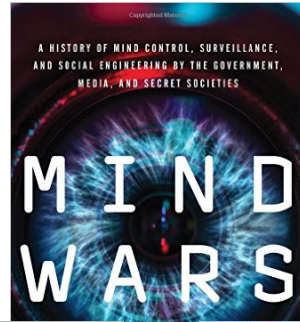
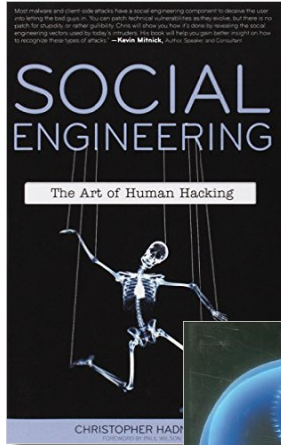
Verizon 2013 Data Breach Investigations Report (DBIR)

How are attackers targeting you?

People inherently want to help – it's in our nature – The human firewall is flawed



Targeted attacks are well researched



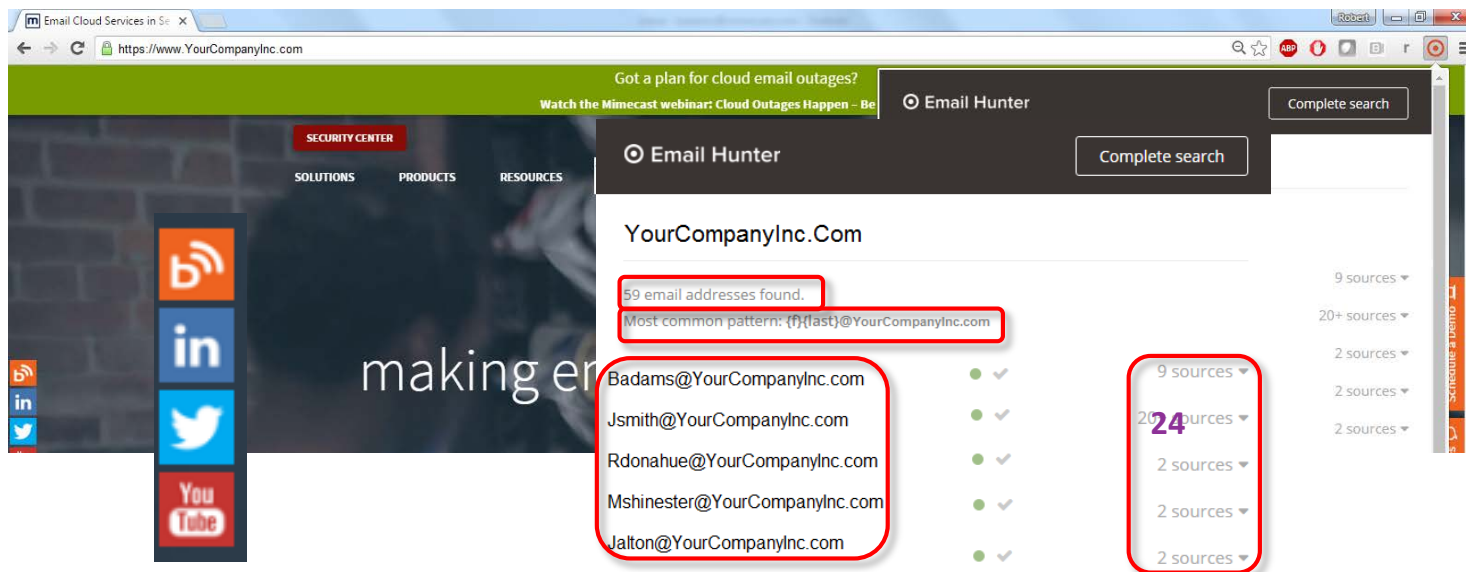
Corporate Stalking: They will learn everything they can about you



- Your company website
- Social media presence
- Leadership and High Value Targets (HVTs)
- Free tools (e.g.: Google Chrome Plugins)

Let's explore the methods of attackers and how they're gathering other, lesser known, public data

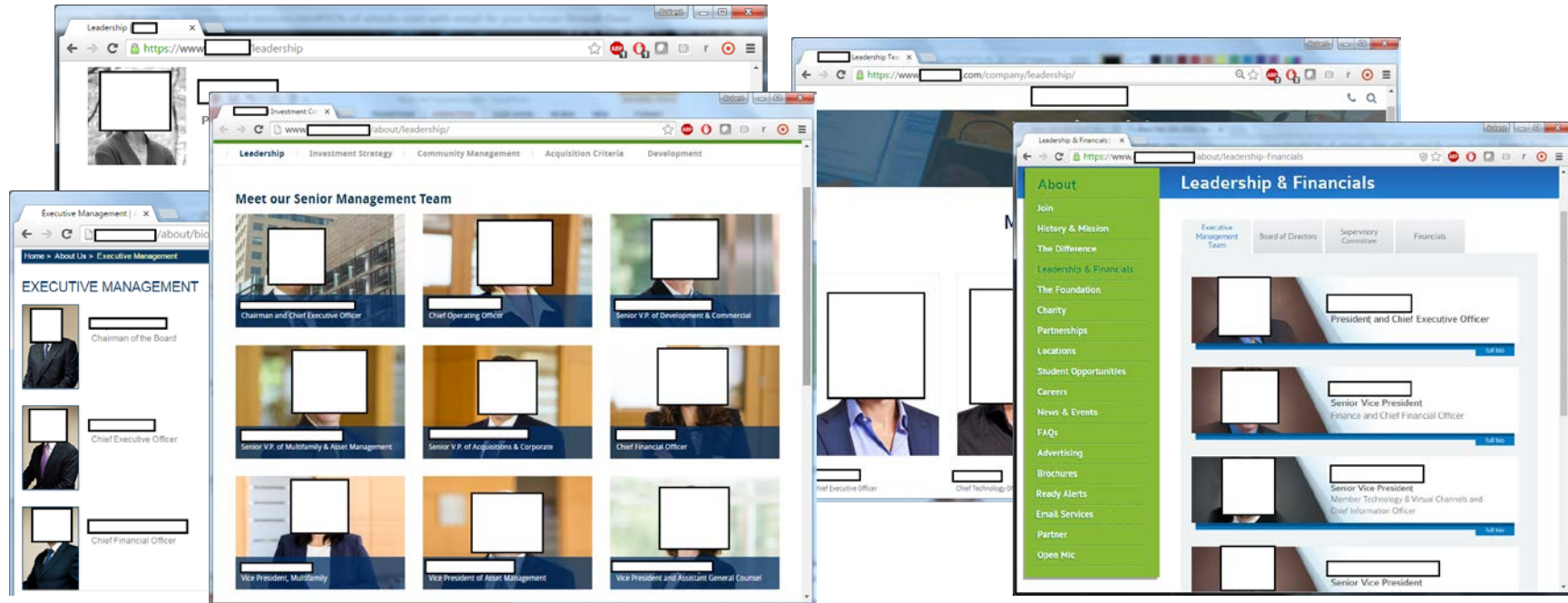
Your Website Is Their Launching Pad & Email Hunter Is Here To Help... Attackers



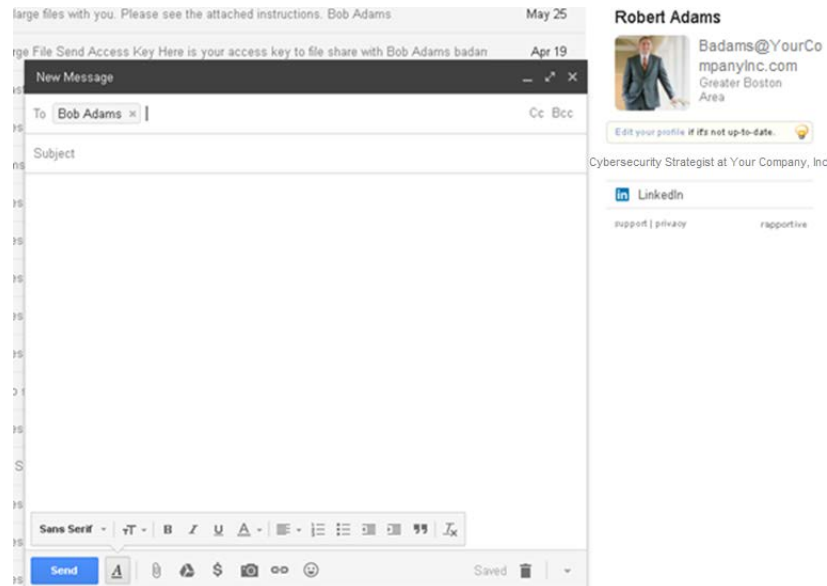
The screenshot shows the Mimecast Email Hunter interface. The search results for 'YourCompanyInc.Com' are displayed. A red box highlights the search results summary: '59 email addresses found.' and 'Most common pattern: {f}{last}@YourCompanyInc.com'. Another red box highlights a list of email addresses: 'Badams@YourCompanyInc.com', 'Jsmith@YourCompanyInc.com', 'Rdonahue@YourCompanyInc.com', 'Mshinester@YourCompanyInc.com', and 'Jalton@YourCompanyInc.com'. A third red box highlights the source counts for each email address: '9 sources', '20 sources', '2 sources', '2 sources', and '2 sources'. The number '24' is also visible next to the source counts.

Email Address	Source Count
Badams@YourCompanyInc.com	9 sources
Jsmith@YourCompanyInc.com	20 sources
Rdonahue@YourCompanyInc.com	2 sources
Mshinester@YourCompanyInc.com	2 sources
Jalton@YourCompanyInc.com	2 sources

Your Executive Team Will Be Found



Rapportive Will Confirm Your Users Address (Particularly The HVTs) And Correlate Them To Their Social Media Profile(s)



Step 1: Locate Your Company



FreeERISA

BenefitsPro FreeERISA BenefitsPRO Magazine Broker Innovation Lab BenefitsPRO Broker Expo A benefitsPRO WEBSITE

Twitter Facebook Google+ LinkedIn FreeERISA Sign Up Log in

Data Products Deluxe Search Document Retrieval myFreeERISA FAQ Support About Us

SEARCH DELUXE SEARCH adamsmimecast@gmail.com Log Out

Your Company, Inc. GO

Need help? Watch a Search Tutorial. Filter By Select... Zip Code

Home » Search Results

Search Results

Showing 1-4 of 4 Matches

Available Filings	Company	Average Assets	Average Participants
	Your Company, Inc	\$6,693,902.75	207

Send
Printer Friendly

Advertisement

Step 2: Review



Form 5500

Your Company, Inc 401(K) Savings Plan

[2014](#)[2013](#)[OLDER FILINGS](#)[View Full 5500](#)

This is a Single Employer 401(k) plan which filed its most recent 5500 in 2014. It has \$46,483,096 in assets and 596 participants. The plan's assets have increased by \$31,910,759 over the past three years, while over the same time period employer contributions per participant have increased by \$3,223.

This plan is **Active**.

Plan #	001
Plan Types	2E DC: Profit sharing 2F DC: ERISA 404(c) 2G DC: Total part. directed 2J DC: 401(k) 2K DC: 401(m) 2S Plan provides for automatic enrollment 2T Total or partial participant-directed - default investment account 3D Other: Master plan
Total Participants	596
Total Assets	\$46,483,096
Red Flags	2
Plan Score	FAIR

Step 3: Pull Out Relevant Details



Plan Name, EIN,
Business Code,
Document Signer

Form 5500 Department of the Treasury Internal Revenue Service Department of Labor Employee Benefits Security Administration Pension Benefit Guaranty Corporation		Annual Return/Report of Employee Benefit Plan This form is required to be filed for employee benefit plans under sections 104 and 4065 of the Employee Retirement Income Security Act of 1974 (ERISA) and sections 6047(e), 6057(b), and 6058(a) of the Internal Revenue Code (the Code). Complete all entries in accordance with the instructions to the Form 5500.	OMB Nos. 1210 - 0110 1210 - 0089 2014 This Form is Open to Public Inspection
Part I Annual Report Identification Information For calendar plan year 2014 or fiscal plan year beginning January 01, 2014, and ending December 31, 2014			
A a multiple-employer plan (filers checking this box must attach a list of participating employer information in accordance with the form instructions) for		<input type="checkbox"/> a multiemployer plan; <input checked="" type="checkbox"/> a single-employer plan;	
B This return/report is:		<input type="checkbox"/> the first return/report; <input type="checkbox"/> an amended return/report; <input type="checkbox"/> the final return/report; <input type="checkbox"/> a short plan year return/report (less than 12 months).	
C If the plan is a collectively-bargained plan, check here <input type="checkbox"/>		<input checked="" type="checkbox"/> Form 5558; <input type="checkbox"/> automatic extension; <input type="checkbox"/> the DFVC program; <input type="checkbox"/> special extension (enter description)	
Part II Basic Plan Information – enter all requested information.			
1a Name of plan Your Company 401(k) Investment Plan		1b Three-digit plan number (PN) 001 1c Effective date of plan January 01, 2009	
2a Plan sponsor's name and address, including room or suite number (Employer, if for a single-employer plan) Your Company, Inc. 123 Technology Dr. Boston, Ma 02124		2b Employer Identification Number (EIN) 18-5245493 2c Sponsor's telephone number 800-867-5309 2d Business code (see instructions) 452628	
Caution: A penalty for the late or incomplete filing of this return/report will be assessed unless reasonable cause is established. Under penalties of perjury and other penalties set forth in the instructions, I declare that I have examined this return/report, including accompanying schedules, statements and attachments, as well as the electronic version of this return/report, and to the best of my knowledge and belief, it is true, correct, and complete.			
Signature of plan administrator		Date 10/13/2015 John McNeil	

Step 4: Insurance Information

#RSAC



Insurance Company,
Insurance EIN,
Contract Number, etc

SCHEDULE A Form 5500 <small>Department of the Treasury Internal Revenue Service</small> <small>Department of Labor Employee Benefits Security Administration Pension Benefit Guaranty Corporation</small>		Insurance Information <small>This schedule is required to be filed under section 104 of the Employee Retirement Income Security Act of 1974 (ERISA)</small> File as an attachment to Form 5500. <small>Insurance companies are required to provide the information pursuant to ERISA section 103(a)(2).</small>		<small>OMB No. 1210 - 0110</small> 2014 This Form is Open to Public Inspection					
For the calendar plan year 2014 or fiscal plan year beginning January 01, 2014, and ending December 31, 2014									
A Name of plan Your Company, Inc 401(k) PLAN		B Three-digit plan number (PN) 001							
C Plan sponsor's name as shown on line 2a of Form 5500 Your Company, Inc		D Employer Identification Number (EIN) 27-2064493							
Part I Information Concerning Insurance Contract Coverage, Fees, and Commissions. Provide information for each contract on a separate Schedule A. Individual contracts grouped as a unit in Parts II and III can be reported on a single Schedule A.									
1 Coverage Information									
(a) Name of insurance carrier LIFE INSURANCE COMPANY (U.S.A.)									
(b) EIN 18-5245493	(c) NAIC code 65838	(d) Contract or identification number 90928	(e) Approximate number of persons covered at end of policy or contract year 84	Policy or contract year <table border="1"> <thead> <tr> <th>(f) From</th> <th>(g) To</th> </tr> </thead> <tbody> <tr> <td>01/01/2014</td> <td>12/31/2014</td> </tr> </tbody> </table>		(f) From	(g) To	01/01/2014	12/31/2014
(f) From	(g) To								
01/01/2014	12/31/2014								
2 Insurance fee and commission information. Enter the total fees and total commissions paid. List in item 3 the agents, brokers, and other persons in descending order of the amount paid.									
(a) Total amount of commissions paid \$7,717			(b) Total amount of fees paid \$1,000						
3 Persons receiving commissions and fees. (Complete as many entries as needed to report all persons).									
(a) Name and address of the agent, broker or other person to whom commissions or fees were paid INSURANCE AGENCY, INC. FINANCE DEPARTMENT MA									
(b) Amount of sales and base commissions paid \$5,550		Fees and other commissions paid <table border="1"> <thead> <tr> <th>(c) Amount</th> <th>(d) Purpose</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>		(c) Amount	(d) Purpose			(e) Organization code 3	
(c) Amount	(d) Purpose								

Step 5: Accounting Firm Information



Part III Accountant's Opinion

3 Complete lines 3a through 3c if the opinion of an independent qualified public accountant is attached to this Form 5500. Complete line 3d if an opinion is not attached.

a The attached opinion of an independent qualified public accountant for this plan is (see instructions):

(1) ☐ Unqualified (2) ☐ Qualified (3) ☒ Disclaimer (4) ☐ Adverse

b Did the accountant perform a limited scope audit pursuant to 29 CFR 2520.103-8 and/or 103-12(d)?

☒ Yes ☐ No

c Enter the name and EIN of the accountant (or accounting firm) below:

(1) Name **Adams & Adams CPAs** (2) EIN: **03-2166147**

d The opinion of an independent qualified public accountant is not attached because:

(1) ☐ This form is filed for a CCT, PSA, or MTIA. (2) ☐ It will be attached to the next Form 5500 pursuant to 29 CFR 2520.104-50.

Remember: It's Not Just About Your Company –
It's About Who Attackers Know You Work With

Complete Attack Profile Of Your Company



- **Social Media** (Company Website, Facebook, LinkedIn, Twitter, Bloomberg, etc)
- **Email Hunter addresses** (compile list and identify common format)
- **High Value Targets** (Executives, Board Members, Finance, and HR)
 - Identify likely email addresses using Email Hunter format
 - Correlate addresses/high value targets to social media profiles using Rapportive
- **Organize FreeERISA Data** - Investment, 401k, Insurance, Accounting Information

Commence Attack



- Email careers address/HR with a resume.doc loaded with ransomware
- Send link to finance/executive team referencing EIN from Form 5500 and other details asking to confirm updated terms and conditions
- Email finance as an executive asking for a wire transfer
- Identify upcoming social events employees will be at and use those details

Endpoint Protection *Is A Must* – But What About External Access Outside Your Firewall?



mimecast[®]

From: [Redacted]
Sent: Thursday, October 01, 2015 1:44 PM
To: Bob Adams <badams@mimecast.com>
Subject: Your Chase Account Has Been Compromised

CHASE 

Hello Chase Online™ Customer,

We are sorry, due to several failed attempts to access your account, we have temporarily deactivated your account for your protection. You are required to reactivate your bank account within the next 48 hours in order to continue using it.

Please logon to www.chase.com and enter your information correctly.

We apologize for any inconvenience this may have caused and look forward to taking further action with you to ensure your account remains secure.

Please do not reply to this automatically system generated email.

Sincerely,
-Your Chase Online™ Banking Team

JPMorgan Chase Bank, N.A. Member FDIC
©2012 JPMorgan Chase & Co.

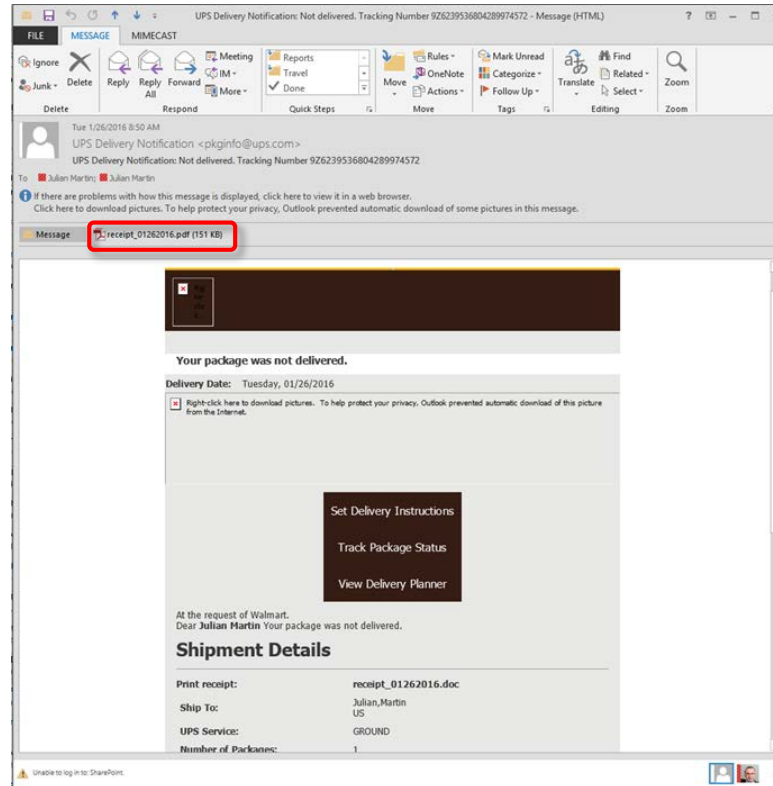
Attachment Sandboxing



Sandboxing is crucial
for every organization
– but don't forget
about file
transcription options



mimecast®



Do Not Forget About Malwareless Attacks!!!



Business Email
Compromises (aka:
Whaling Attacks) often
exploit users through a
number of methods



mimecast®

On 2015-07-29 09:31 AM, Peter Fondini wrote:

Peter,
Sent: Wednesday, July 29, 2015 12:04 PM
To: Peter Fondini
Cc: Mark O'Hare
Subject: RE: Payment Request

Is this f Nice catch. It is not me.
It is a phishing scam.
Don't pay anything
Copying Mark O'Hare on this.

Peter C

From: Peter Fondini
Sent: Wednesday, July 29, 2015 10:55 AM
To: Peter Campbell
Subject: FW: Payment Request
Importance: High

mir
Peter,

Got these two message from an email "representing " itself as you. I presume these have not come from you. Please confirm.

From: I
Sent: W
To: Peb
Subject:

From: Peter Campbell [<mailto:pcampbell@minecast.com>]
Sent: Wednesday, July 29, 2015 10:46 AM
To: Peter Fondini
Subject: RE: Payment Request

Peter,

Can w Peter,

Thank No Find attached wiring instructions for a wire of \$48,254.80. I need you to process this, code to Professional Service expenses and send me confirmation when completed.

Peter This ought to have been sent yesterday.

Thanks,

Peter

Let's examine this attack closer and
how it could have been prevented
by fixing the Human Firewall

Fixing the Human Firewall



Perform User Name
Checks – Attackers
Know Your Leadership
Team And Will
Impersonate Them!
**Remember: Everyone
Is A Potential Target**



mimecast[®]

On 2015-07-29 09:31 AM, Peter Fondini wrote:

Peter,

Is this for Nasdaq or something else?

Peter

Peter Fondini
Corporate Controller: North America

m: +1 617 584 9789
p: +1 781 996 4284

w:
www.mimecast.com
Address click [here](#)

mimecast[®]
unified email management



From: Peter Campbell (<mailto:pcampbell@mimecast.com>)
Sent: Wednesday, July 29, 2015 10:25 AM
To: Peter Fondini
Subject: Payment Request

Peter,

Can we send a wire transfer today? I'm expecting to receive instructions for wire transfer and I will forward to you soon for processing.

Thanks,

Peter

Fixing the Human Firewall



Check For Common
Keywords Used By
Attackers – e.g.: Wire
Transfer, Wire
Payment, W2, P60, etc



mimecast®

On 2015-07-29 09:31 AM, Peter Fondini wrote:

Peter,

Is this for Nasdaq or something else?

Peter

Peter Fondini
Corporate Controller: North America

m: +1 617 584 9789
p: +1 781 996 4284

w:
www.mimecast.com
Address click [here](#)

mimecast
unified email management



From: Peter Campbell [<mailto:pcampbell@mimecast.com>]
Sent: Wednesday, July 29, 2015 10:25 AM
To: Peter Fondini
Subject: Payment Request

Peter,

Can we send a **wire transfer** today? I'm expecting to receive instructions for wire transfer and I will forward to you soon for processing.

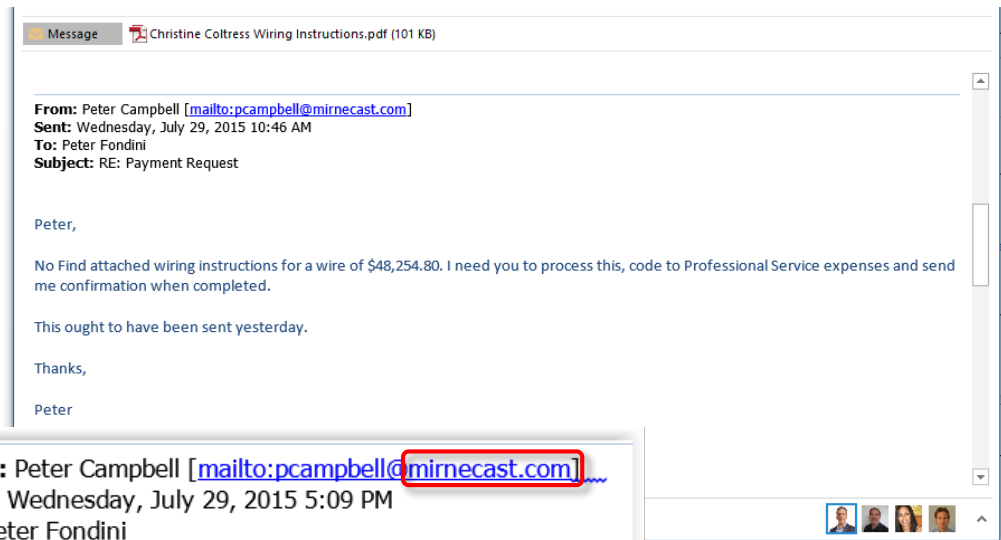
Thanks,

Peter

Fixing the Human Firewall



Check For Similar
Domains – Not Your
Spoofed Domain, But
A Slight Variation



From: Peter Campbell [<mailto:pcampbell@mirnecast.com>]
Sent: Wednesday, July 29, 2015 5:09 PM
To: Peter Fondini
Subject: RE: Payment Request

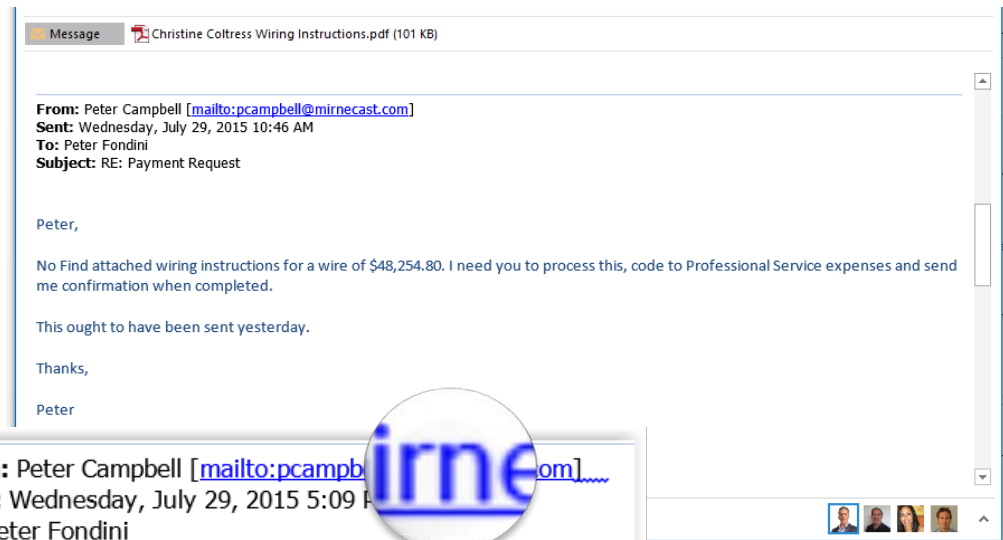
Peter--what is the update of the wire



Fixing the Human Firewall



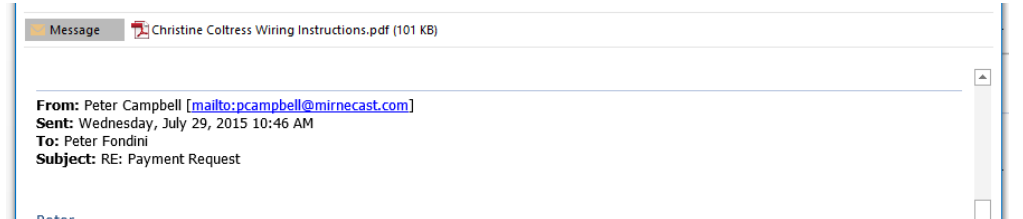
Check For Similar
Domains – Not Your
Spoofed Domain, But
A Slight Variation



Fixing the Human Firewall



Examine the Domain Age – How often do you work with new domains?



Whois Record (last updated on 2015-08-02)

Domain Name: MIRNECAST.COM
Registry Domain ID: 1949875411_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2015-07-29T13:06:40Z
Creation Date: 2015-07-29T13:06:40Z

From: Peter Campbell [mailto:pcampbell@mirnecast.com]
Sent: Wednesday, July 29, 2015 5:09 PM
To: Peter Fondini
Subject: RE: Payment Request

Peter--what is the update of the wire



Simplicity, Credibility, Psychology, And Urgency Lead To Their Success



- Emails do not go into detail
 - Need a Wire Transfer
 - Send me Employee W2s
 - Click on this link/Open this attachment
- Public information gives credible data sources to leverage
- Leverage manipulation tactics to trick users – e.g. C-Level Impersonation
- They need it done now and are often unavailable to discuss further

So what can you do?



Layer 1: The technology



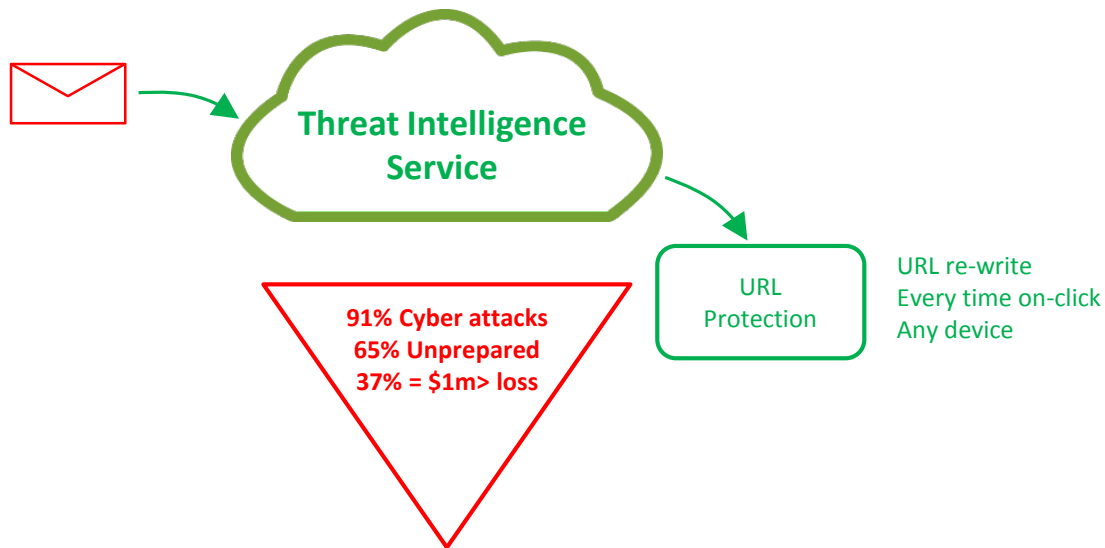
Layer 2: The people - a human firewall

So how can you **help** fix your
Human Firewall Flaws?

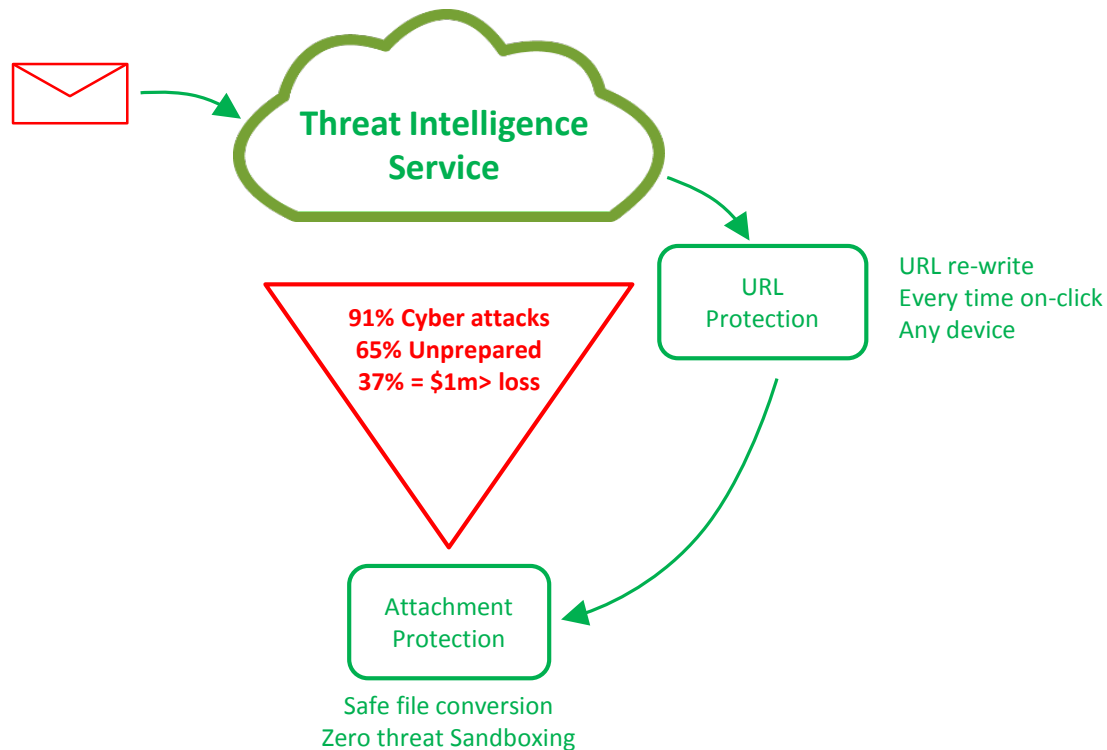
So how can you help fix your Human Firewall Flaws?



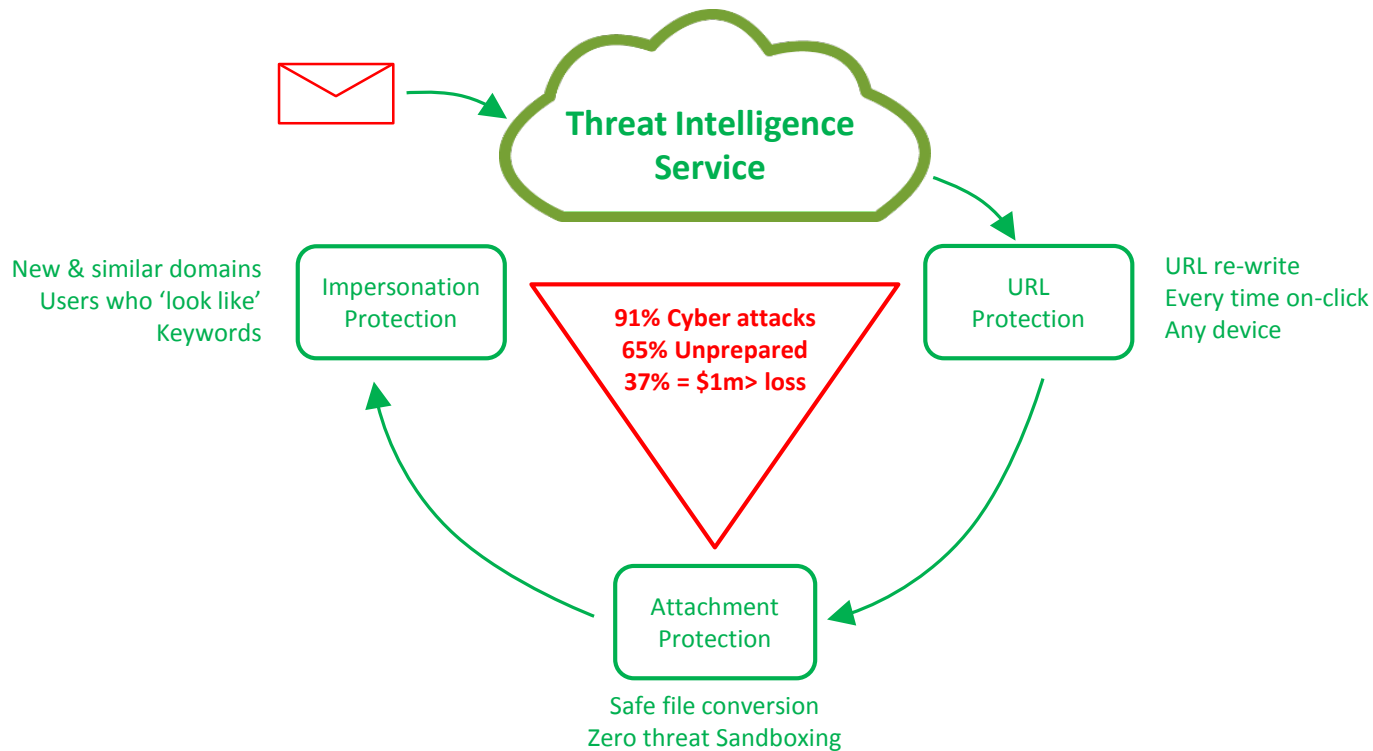
So how can you help fix your Human Firewall Flaws?



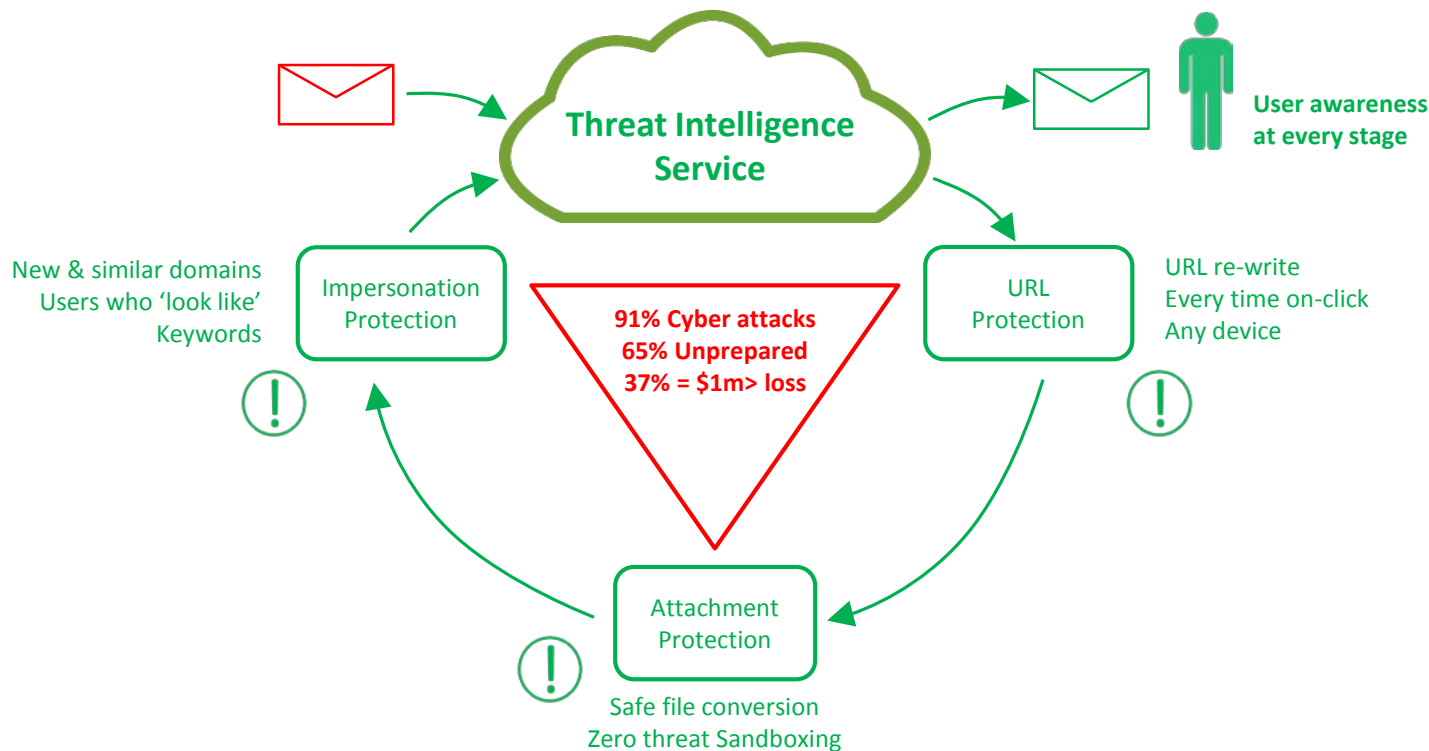
So how can you help fix your Human Firewall Flaws?



So how can you help fix your Human Firewall Flaws?



So how can you help fix your Human Firewall Flaws?





This works too

How do I apply this?



- When you get back to the office, consider:
 - Are my employees security aware?
 - Do I have the right security technology?
 - Do I have buy-in from the top?

Thank You



Email: smalone@mimecast.com

Twitter: [@Steven_Malone](https://twitter.com/Steven_Malone)