



FEDERAL BUREAU OF INVESTIGATION

ANCHORAGE FIELD OFFICE

# **Business Email Compromise and Social Engineering Schemes**



## 5 Seconds to Answer

***Where would you find an expert in Marital Arts?***

- A. Magnolia Home Design Studio***
- B. Tampa Academy of Feng Shui***
- C. Abbott's Wedding Photos***
- D. OR... any respectable Karate Dojo***





## 5 Seconds to Answer

***Where would you find an expert in Marital Arts?***

- A. M**
- B. Ta**
- C. Ab**
- D. O**

**The correct answer is:**

**“C. Abbott’s Wedding photos”**

*(Marital not Martial Arts)*

- The photo of the man breaking bricks & the highlighting of answer “D” are meant to trick you.
- The **5 second time constraint** forces you to make a quick decision.





# What is Business Email Compromise (BEC)?

## *Practical Definition*

- A scam that targets businesses or individuals who perform wire transfer payments.
- Relies on social engineering deception to convince victims to send money to criminal actors.
- Initiated when a victim receives false instructions from a criminal, who is masquerading as a trusted business contact.
- In most cases, legitimate email accounts have been spoofed or compromised to lend legitimacy to the emails purporting to be from trusted contacts.



# Business Email Compromise Scenarios

## *Most Common BEC Scenarios*

- **Executive Officer Spoofing**
- **Invoice & Supply Chain**
- **Real Estate**



## How BECs Work...

### One Example of BEC Initiation

# Executive Officer Spoofing

*BEC has many variations and is constantly evolving*



# BEC Through Executive Officer Spoofing

1. A criminal actor uses information available online, a news publication or other sources to target a certain audience.

*Example: CEO / CFO*



**Bridge, Inc.** Why Freestone What We Do Our Team Blog Contact

← BACK TO ALL TEAM DOWNLOAD BIO ↓

**Bruce Jones, CPA**  
Managing Director | **Chief Operating Officer** | Seattle, WA

“Opportunity is missed by most people because it is dressed in overalls and looks like work.”  
Thomas A. Edison |

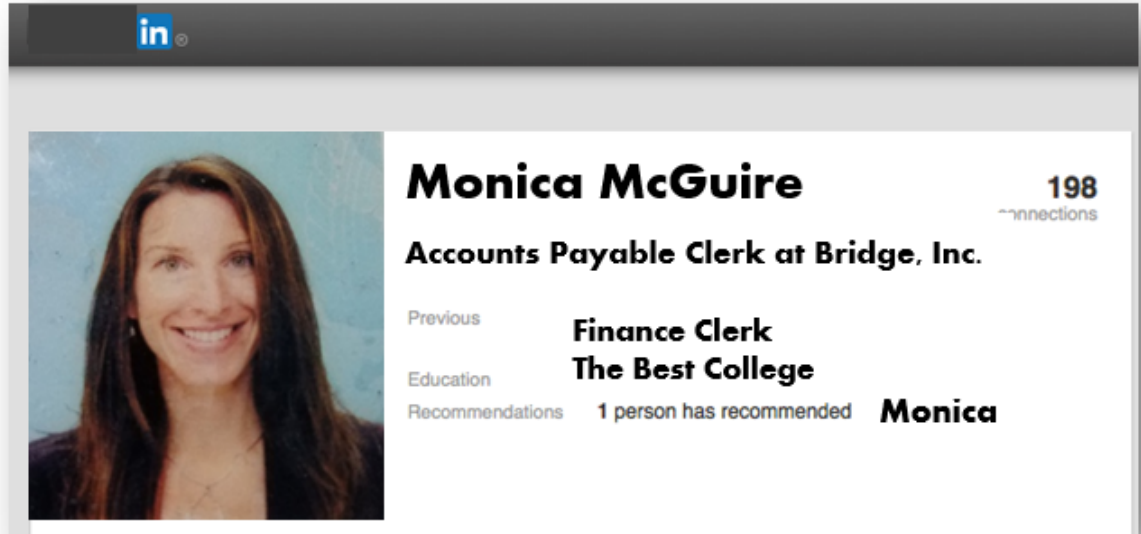
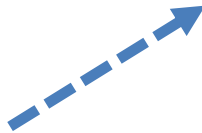
Download V-Card  
Email Bruce

P: .7365 | 800.990.3001  
F: 7399



# BEC Through Executive Officer Spoofing

*Email addresses are possibly obtained from the company's actual website and/or networking websites*



in

**Monica McGuire** 198 connections

Accounts Payable Clerk at Bridge, Inc.

Previous **Finance Clerk**

Education **The Best College**

Recommendations 1 person has recommended **Monica**



**Email Resume & Cover Letter To:**

**Monica McGuire, Accounts Payable Clerk**  
**Stone Financial**  
**Monica.M@Bridge.com**





# BEC Through Executive Officer Spoofing

2. The criminal impersonates the COO, **Bruce Jones** and sends an email to the clerk in Accounts Payable, advising of a *new client* or a *need to pay a vendor*.
  - a) The “COO” provides the **Account Number** and **Routing Number** for the transfer



**COO Bruce Jones**  
*Fake Email:*  
[Bruce.J@Bridge.com](mailto:Bruce.J@Bridge.com)  
**Display Name: “Bruce Jones”**  
*Actual:* [Bruce.J@Bridge.com](mailto:Bruce.J@Bridge.com)



**A/P Clerk**  
*Monica McGuire*  
*Actual:*  
[Monica.M@Bridge.com](mailto:Monica.M@Bridge.com)

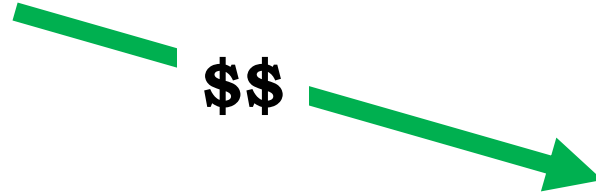


# BEC Through Executive Officer Spoofing

3. The company **employee** believes they are **communicating with the COO...**

*...they may even question the COO...*

... but the **company becomes a victim** when funds are transferred, as described in the “COO’s” email



Acct #: **4567 8910 111213**;

Routing #: **12345678**



# Executive Officer Spoofing Example

From: **Chris**  
Sent: Thursday, January 4, 2018 11:28:27 AM  
To: **David**  
Subject: wire

1

**David,**

How soon can we process an International wire transfer this morning.

Best Regards,  
**Chris**  
President / COO

From: **David**  
Sent: Thursday, January 4, 2018 12:55:10 PM  
To: **Chris**  
Subject: re: Wire

2

I can do one now, who is it for?  
Get [Outlook for Android](#)

*This is an actual example of Executive Officer Spoofing, where only the names have been changed!*



# Executive Officer Spoofing Example

**From:** Chris  
**Sent:** Thursday, January 4, 2018 1:48:17 PM  
**To:** David  
**Subject:** Re: wire

3

Professional Fees For application development and Services Agreement

Best Regards,  
**Chris**  
President / COO

**From:** David  
**Sent:** Thursday, January 4, 2018 2:09 PM  
**To:** Chris  
**Subject:** Re: Wire

4

I should be in the office in about 30 minutes my VPN connection was not it's not working. So I should have this done for you shortly and is the professional fees Marketing or sales sales?

Get Outlook for Android



# Executive Officer Spoofing Example

**From:** Chris  
**Sent:** Thursday, January 4, 2018 2:11:14 PM  
**To:** David  
**Subject:** Re: Wire

Professional fees Marketing.

Email me the wire confirmation as soon as this is completed.

Best Regards,  
**Chris**  
President / COO

5

Urgency??

Follow up questions

**From:** David  
**Sent:** Thursday, January 4, 2018 2:18 PM  
**To:** Chris  
**Subject:** re: Wire

Is this for work that was done last year or is work that is going to be done. I just wanted to make sure that I record the expense in the appropriate year

Get [Outlook for Android](#)

6



# Executive Officer Spoofing Example

**From:** Chris

**Sent:** Thursday, January 04, 2018 2:21 PM

**To:** David

**Subject:** Re: Wire

7

This was for work done last year.

Follow up request

Best Regards,

**Chris**

President / COO

**From:** David

**Sent:** Thursday, January 4, 2018 3:06 PM

**To:** Chris

**Subject:** RE: Wire

8

Can you email me a copy of the service agreement? I am sure with a wire this large at the end of the year/beginning of the year the auditors are going to want to look at it, so I just want to have it handy when they ask for it.

Thanks,

**David**





# Executive Officer Spoofing Example

**From:** Chris  
**Sent:** Thursday, January 04, 2018 3:08 PM  
**To:** David  
**Subject:** Re: Wire

9

Urgency??

Yea sure. I will forward you that tomorrow. Is the wire out?

Best Regards,  
  
Chris  
President / COO

**From:** David  
**Sent:** Thursday, January 4, 2018 3:21 PM  
**To:** Chris  
**Subject:** RE: Wire

10

Do you have their address?

Thanks,

David



# Executive Officer Spoofing Example

**From:** Chris

**Sent:** Thursday, January 04, 2018 3:23 PM

**To:** David

**Subject:** Re: Wire

11

House South Block 3 Sham Mong Rd, Central Hong Kong.

Best Regards,

Chris

President / COO

**From:** David

**Sent:** Thursday, January 4, 2018 3:25 PM

**To:** Chris

**Subject:** RE: Wire

12

Do you want me to send a confirmation to JR as well?

Thanks,

David





# Executive Officer Spoofing Example

**From:** Chris

**Sent:** Thursday, January 04, 2018 3:28 PM

**To:** David

**Subject:** Re: Wire

13

No. IF the wire is out, Email me the wire confirmation so i can forward to the Beneficiary.

Best Regards,

Chris

President / COO

Need for  
Follow up??

**From:** David

**Sent:** Thursday, January 4, 2018 3:42 PM

**To:** Chris

**Subject:** RE: Wire

14

Can you call me -313-8066

Thanks,

David



# Executive Officer Spoofing Example

From: **Chris**  
 Sent: Thursday, January 04, 2018 3:44 PM  
 To: **David**  
 Subject: Re: Wire

15

Why are you questioning the CEO??

**David,**  
 I am not available to make calls. and WHY PLEASE?

"not comfortable"

Best Regards,  
**Chris**  
 President / COO

From: **David**  
 Sent: Thursday, January 4, 2018 3:49 PM  
 To: **Chris**  
 Subject: RE: Wire

16

It's a large wire transfer at the beginning of the year for a company that was only incorporated in October. We have spent \$93k in three months with this company that I have not heard of being discussed? I feel like this is going to bite me and I am not comfortable.

Thanks,  
**David**



# Executive Officer Spoofing Example

From: **Chris**  
Sent: Thursday, January 04, 2018 3:51 PM  
To: **David**  
Subject: re: wire

17

**David,**

I think i know more right. so i do not understand what you are saying. CAN YOU PROCESS THIS YES OR NO?

Best Regards,

**Chris**

President / COO

Why are you questioning the CEO??

From: **David**  
Sent: Thursday, January 04, 2018 4:08 PM  
To: **Chris**  
Subject: re: wire  
Attachments: scan0003.pdf

18

I am not questioning you and I am not trying to be difficult, but this was company was never discussed or never came up in a conversation . . .  
The wire confirm is attached.

**David**



# Education: How to Hide A True Email Address

## People also ask

How do I hide my name when sending an email?

### How to Hide Your Name on Gmail

1. Log in to your Gmail account.
2. Click the "Settings" gear icon and select "Settings."
3. Click the "Accounts and Import" tab.
4. Click "Edit Info" next to your email address in the "Send Mail As" section.
5. Click the circle next to the blank field in the Name section and type your preferred display name.

***It's this  
simple.***

### How to Hide Your Name on Gmail | It Still Works

[https://itstillworks.com > hide-name-gmail-21114](https://itstillworks.com/hide-name-gmail-21114)



## Education: Display Name Deception (*1<sup>st</sup> Possibility*)

From: Jim

Date: January 24, 2018 at 3:08:25 PM EST

To: John Smith

Subject: Re: Escrow Clos

Display name is:

*"Jim"*

Email is actually:

*"Hackstar247@gmail.com" - Bad*

*"Jim@Realtor4you.com" - Good*

WIRING INFORMATION



## Education: Display Name Deception (2<sup>nd</sup> Possibility)

From: Jim@Realtor4you.com  
Date: January 24, 2018 at 3:08:21 PM EST  
To: John Smith  
Subject: Re: Escrow Closing

Display name is:

*"Jim@Realtor4you.com"*

Email is actually:

*"Hackstar247@gmail.com" - Bad*

WIRING



# Education: Look-Alike Domains / Spoofing

From: Jim@Reaitor4you.com  
Date: January 24, 2018 at 3:25 PM EST  
To: John Smith  
Subject: Re: Escrow Closing

Display name is:

*"Jim@Realtor4you.com"*

Email is actually:

*"Jim@RealtOr4you.com" - Bad*

*"Jim@Reaitor4you.com" - Bad*

WIRING INFO





# Reporting: Actions if Victimized

## Business Email Compromise Checklist

Have you been a victim of CEO or Wire Transfer Fraud, commonly known as Business Email Compromise (BEC)? Review the checklist below for immediate actions, as well as, ideas for prevention and recognition:

### IMMEDIATE ACTIONS

#### Reporting the Incident

- Contact your bank
  - Determine the appropriate contact at your bank, who has the authority to recall a wire transfer
  - Notify your bank you have been the victim of a Business Email Compromise
    - AND -
  - Request a wire recall or SWIFT Recall Message
    - AND -
  - Request they fully cooperate with law enforcement
- Report the incident (or attempt) to the FBI at [www.IC3.gov](http://www.IC3.gov)
  - Provide all details for the beneficiary: account numbers, contact information, names
- Contact your local FBI Field Office

#### Internal Actions

- Review all IP logs accessing the relevant infrastructure (internal mail servers or other publically accessible infrastructure) looking for unusual activity
- Scan for log-in locational data. Was there a log-in from an unknown country or location, specific to that email account?
- Review the relevant email account(s) which may have been spoofed or otherwise compromised for any rules such as “auto forward” or “auto delete”
- Inform employees/agents of the situation and require they contact clients and customers who are near the wire transfer stage
- Review all requests that asked for a change in payment type or location.

**\*\*Remain especially vigilant on transactions expected to occur immediately prior to a holiday or weekend. \*\***

### PREVENTION & RECOGNITION

- Hover your cursor over, or expand contact details on, suspicious email addresses – Looking for indications of Display Name Deception or Spoofing
  - Regularly check your email account log-in activity for possible signs of email compromise
  - Develop an intrusion detection system to identify emails from extensions that are similar to your company email.
  - Regularly check your email account for new “rules”, such as email forwarding and/or auto delete
  - Be cautious of “new” customers, suppliers, clients and/or others you don’t know who ask you to:
    - a. ...open or download any documents they send
      - OR -
    - b. ...sign into a separate window or click on a link to view an invoice or document
      - OR -
    - c. ...provide sensitive Personal or Corporate information
  - Verify the wire instructions you provide to your customers/clients are accurate for both the pertinent bank and pertinent account.
    - a. Where did you get the account data?
    - b. Is this the correct account number?
- 
- 
- Display name is: "Jim"  
What is the actual email address?
- DO NOT hover on *links* within emails, as simply hovering *may* execute commands.
  - Call a known/trusted phone number or meet in person to confirm that the wire transfer information provided to you, matches the other party’s information
  - Does the Routing Number or SWIFT Number provided to you, resolve to the expected bank used by the other party?
 

*(Example: Have you received wire information for an account at a Hong Kong bank; however, your other party only banks in the U.S?)*

Possible websites to verify a Routing or SWIFT Number:

    - a. Any reputable search engine
    - b. The Federal Reserve  
[www.FRBServices.org](http://www.FRBServices.org)
    - c. American Bankers Association  
<https://routingnumber.aba.com>





# Reporting: Actions if Victimized

## *Immediate Response*

- **Contact your bank**

- *Request a wire recall or SWIFT recall message.*

**- AND -**

<https://bec.IC3.gov>

- **Report the BEC or attempt to IC3**

- Report BEC, EAC and other Cyber-Enabled Fraud on:

- <https://bec.ic3.gov> or [www.ic3.gov](http://www.ic3.gov)

**- AND -**

- **Contact your local FBI office**





## Reporting: Actions if Victimized

### **Immediate Response**

**Be sure to...**

- ✓ **Maintain all email communications and evidence.**
- ✓ **Request your bank to fully cooperate with law enforcement.**
- ✓ **Advise your bank that you've been a victim of Business Email Compromise.**



# Recognition & Prevention: Minimize The Risk of Fraud

## *BEC Prevention*

- **Be cautious of “new”** customers, suppliers, clients, and/or others you don’t know who ask you to:
  - **Open or download** documents they send
- **-OR-**
- **Sign into a separate window or click on a link** to view an invoice or document
- **-OR-**
- **Provide sensitive** personal or corporate **information**

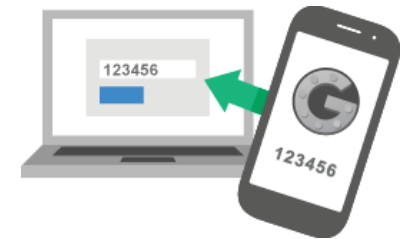
*\*\*\* Remain especially vigilant on transactions expected to occur immediately prior to a holiday or weekend \*\*\**



# Recognition & Prevention: Minimize The Risk of Fraud

## *BEC Prevention*

- Request your **employees use only** the **corporate email account**
- Request **multi-factor authentication**
  - Something you know (**password**)
  - Something you receive (**code to your phone**)
- **Hover your cursor** over, or expand contact details, for suspicious email addresses
  - Look for indications of *Display Name Deception* or *Spoofing*



*(DO NOT hover over links within emails – this may execute commands.)*



## Social Engineering

*The act of tricking someone into divulging information or taking action, usually through technology*

- ✓ Online (Social Media, Email)
- ✓ Telephonically
- ✓ In-person





## Types of Social Engineering Attacks

- ✓ **Phishing** – An untargeted fraudulent act of acquiring private and sensitive information, such as personal identification information and account usernames and passwords.
- ✓ **Spear Phishing** – A variation on phishing in which hackers send emails to groups of people with specific common characteristics or other identifiers. The email may appear to be from a trusted source within the organization..
- ✓ **Whaling** – A spear phishing attempt targeting high-ranking or senior executives or others in powerful positions or with important-sounding job titles.
- ✓ **Typosquatting** – Domains that look similar to the official email addresses of the organizations they intend to target. The domains may have a character or two misplaced, for instance “**amce\_inc.com**” (fraudulent business) vs “**acme\_inc.com.**” (legitimate business) or attackers may simply add words to masquerade as a particular department, such as “**acme\_inc\_sales.com.**”



# Phishing: How to Recognize

## Phishing

There are a lot of ways in which phishing emails can be identified:

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

[http://www.facebook.com/application\\_form](http://www.facebook.com/application_form)

Links in email

Note: If you dont fill the application your account will be permanently blocked.

Threats

Regards,

Facebook Copyrights Department.

Popular company



# Phishing: How to Recognize

The screenshot shows a web browser window with a URL bar containing "facebook.com.account.login.userek6krf3.popsi7.info/bc/fbn/security.php". The "popsi7.info" domain is circled in red. The page header features the Facebook logo and a "Sign Up" button. The main content area is titled "Facebook Login" and contains a yellow warning box that reads "You must log in to see this page." Below this, there are input fields for "Email:" and "Password:", a checked checkbox for "Keep me logged in", a "Log In" button, and a link for "Forgot your password?". At the bottom, there is a language selection menu with options for English (US), Español, Português (Brasil), Français (France), Deutsch, Italiano, العربية, and हिंदी.





# Spear Phishing

9. The hacker uses the backdoor to steal information



1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

7. A link is clicked or attachment opened.



8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/smartphone/network.



6. The email is opened because they 'know' the sender.

## ANATOMY OF A SPEAR PHISHING ATTACK



2. Following the social trail, he identifies other people the employee may know.

5. The email passes the spam filter and arrives at the employee's inbox.



3. A fake but recognizable email address is created to impersonate a colleague or boss.



4. A personalized email is sent to the employee from the fake address with a link or attachment.



# Spear Phishing: Example

From: Google <[no-reply@accounts.googlemail.com](mailto:no-reply@accounts.googlemail.com)>  
Date: March 19, 2016 at 4:34:30 AM EDT  
To: [john.podesta@gmail.com](mailto:john.podesta@gmail.com)  
Subject: Someone has your password

Google



## Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account [john.podesta@gmail.com](mailto:john.podesta@gmail.com).

### Details:

Saturday, 19 March, 8:34:30 UTC  
IP Address: 134.249.139.239  
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,  
The Gmail Team

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



# Spear Phishing: Example

## The New York Times

**From:** Charles Delavan <[cdelavan@hillaryclinton.com](mailto:cdelavan@hillaryclinton.com)>  
**Date:** March 19, 2016 at 9:54:05 AM EDT  
**To:** Sara Latham <[slatham@hillaryclinton.com](mailto:slatham@hillaryclinton.com)>, Shane Hable <[shable@hillaryclinton.com](mailto:shable@hillaryclinton.com)>  
**Subject:** Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: <https://myaccount.google.com/security> to do both. It is absolutely imperative that this is done ASAP.



# Spear Phishing: Example




Sign in - Google Account

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Ric3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Ric

Google

## One account. All of Google.

Sign in with your Google Account




**John Podesta**  
john.podesta@gmail.com

**Sign in**

[Need help?](#)

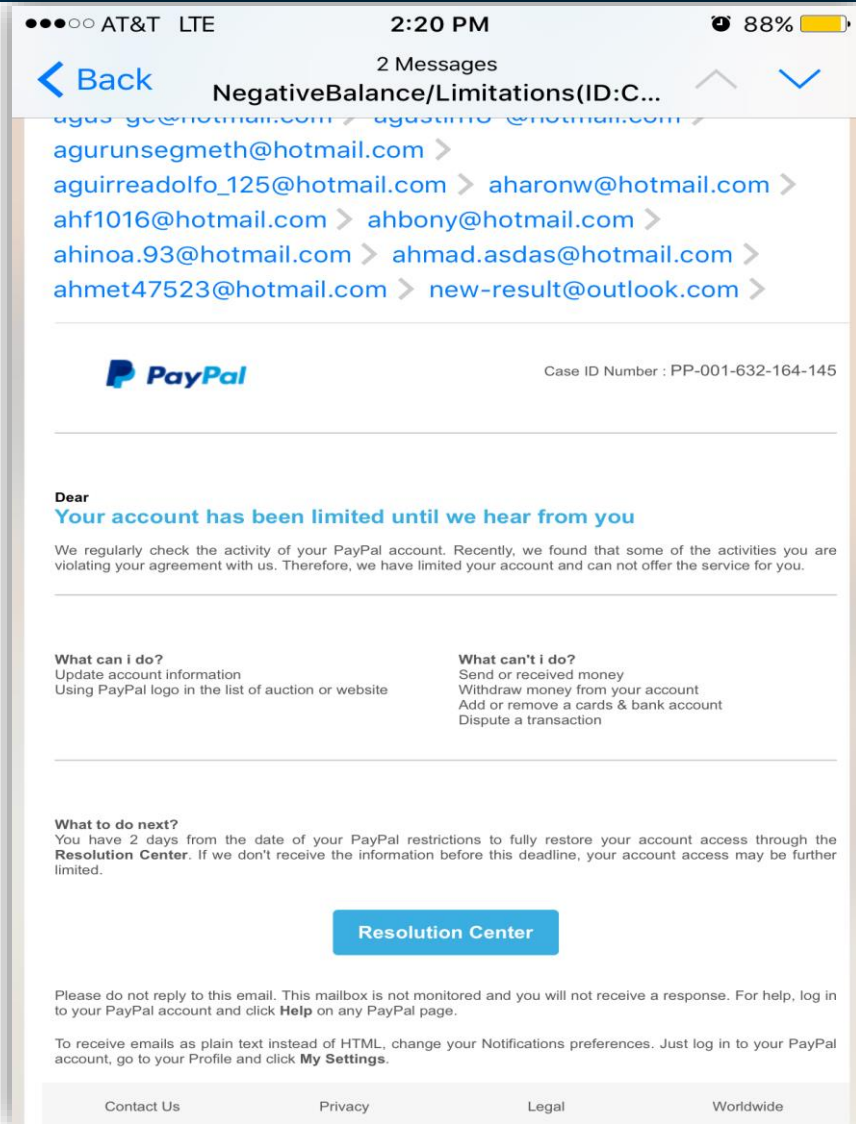
[Sign in with a different account](#)

One Google Account for everything Google



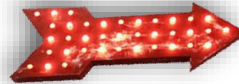


# Spear Phishing: Red Flags





# Spear Phishing: Red Flags



AT&T LTE 2:20 PM 88%

Back NegativeBalance/Limitations(ID:C... 2 Messages

agurunsegmeth@hotmail.com >  
 aguirreadolfo\_125@hotmail.com > aharonw@hotmail.com >  
 ahf1016@hotmail.com > ahbony@hotmail.com >  
 ahinoa.93@hotmail.com > ahmad.asdas@hotmail.com >  
 ahmet47523@hotmail.com > new-result@outlook.com >

---

Case ID Number : PP-001-632-164-145

---

Dear  
**Your account has been limited until we hear from you**

We regularly check the activity of your PayPal account. Recently, we found that some of the activities you are violating your agreement with us. Therefore, we have limited your account and can not offer the service for you.

---

<b>What can i do?</b> Update account information Using PayPal logo in the list of auction or website	<b>What can't i do?</b> Send or received money Withdraw money from your account Add or remove a cards & bank account Dispute a transaction
--	--

---

**What to do next?**  
 You have 2 days from the date of your PayPal restrictions to fully restore your account access through the **Resolution Center**. If we don't receive the information before this deadline, your account access may be further limited.

[Resolution Center](#)

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For help, log in to your PayPal account and click **Help** on any PayPal page.

To receive emails as plain text instead of HTML, change your Notifications preferences. Just log in to your PayPal account, go to your Profile and click **My Settings**.

Contact Us Privacy Legal Worldwide



# Spear Phishing: Test Your Skills

●●●○ AT&T LTE 2:20 PM 88%

🔒 paypal.com.sign-in.insure ↻

Email

Password

**Log In**

[Having trouble logging in?](#)

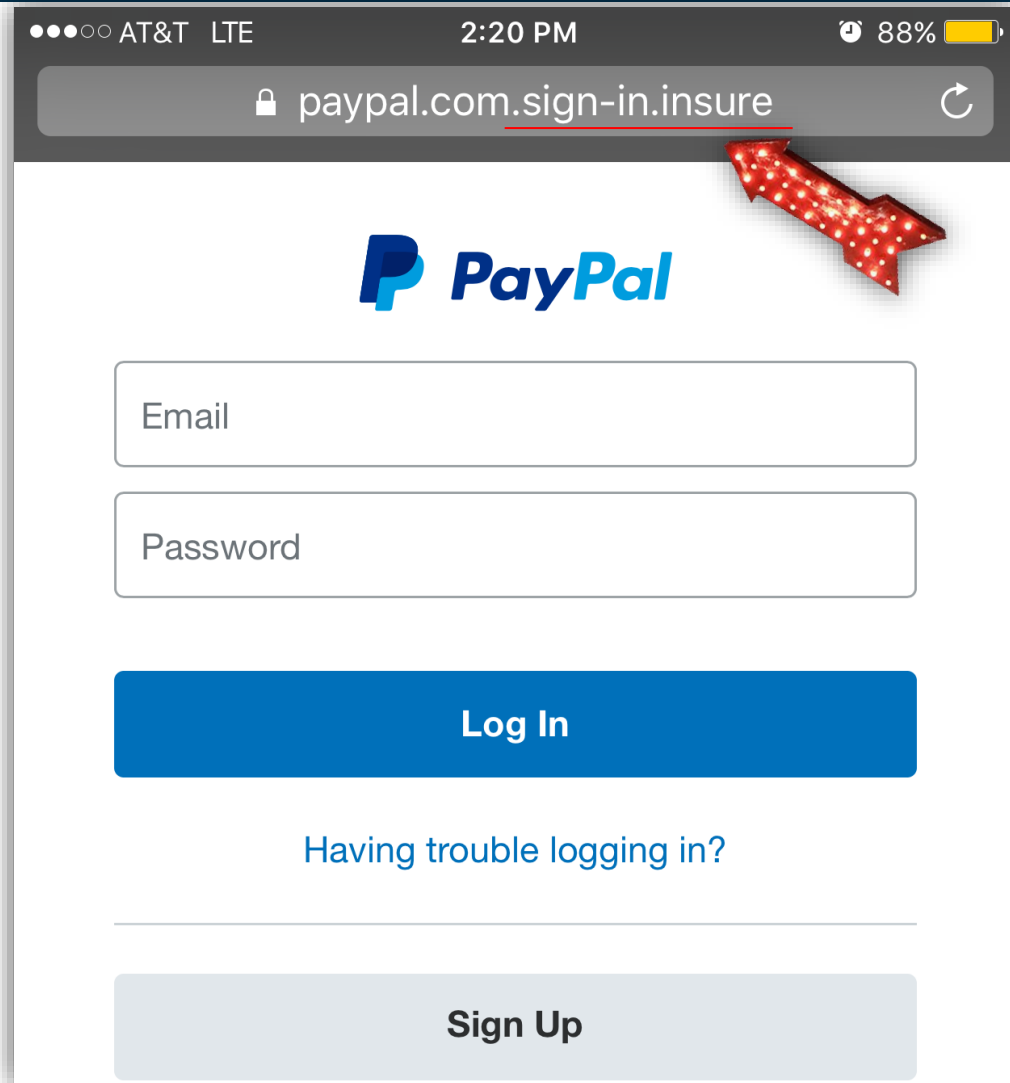
---

**Sign Up**





# Spear Phishing: Test Your Skills







# Spear Phishing: Email Addresses

## Ways in which an email address can be easily altered:

**johnsmith@gmail.com**

johnsm<sup>t</sup>ih@gmail.com

i<sup>o</sup>ohnsmith@gmail.com

joh<sup>h</sup>smith@gmail.com

johnsm<sup>l</sup>th@gmail.com

johnsmith@g<sup>n</sup>ail.com

johnsmith@gm<sup>o</sup>il.com

johnhs<sup>r</sup>nith@gmail.com



# Spear Phishing: Email Message Red Flags

## What are some red flags in this email message?

### Subject:

Urgent W2 Request

### Message body:

Hi [TARGET],

How are you today? I need you to send me the W2 of all the Company's Employees,I need it for a Quick Review

thanks [IMPERSONATED EXECUTIVE]



# Speare Phishing: Email Message Red Flags

What are some red flags in this email message?

Subject:

**Urgent W2 Request**

Message body:

Hi [TARGET],

**How are you today?** I need you to send me the **W2** of all the **C**ompany's **E**mployees,**I** need it for a

**Quick Review**

**thanks** [IMPERSONATED EXECUTIVE]

**Missing Punctuation**



# How to Avoid Being a Victim of Social Engineering

- ✓ Carefully scrutinize all communications (e-mail, social media, phone calls, text messages, etc.)
- ✓ Confirm requests for transfers of funds by using a phone call or in-person contact
- ✓ Know the habits of those with whom you are communicating
- ✓ Instead of replying to e-mails, forward responses using existing contacts in your address book
- ✓ Slow down!

**If something doesn't look right, it probably isn't right...  
report it!**

# Questions?

## Business Email Compromise and Phishing Schemes



---

ANCHORAGE FIELD OFFICE

FEDERAL BUREAU OF INVESTIGATION

---