



# Why are you here?

- Did you know, every week HR gets at least one real phishing email requesting to update an employee's direct deposit information.
  - If we make one slip, it could mean your paycheck is not deposited when you need it.
- It's not about how many people can we catch or a "gotcha" moment.
- While the test emails are fake, they represent real life attacks.
- The consequences are real – people have missed a paycheck as a result of hackers
  - BullsEye, of course, resolved everything in the end, but what would the immediate repercussions for you, if you:
    - Don't get paid on the day you expect to? This why all UltiPro updates are now DIY!
    - You need to reset all your passwords
    - Are the one that exposes BullsEye to a serious breach



# Recognize this email?

## \*URGENT\* BullsEye Return to Office SignUp



Carl Parkins <carl.parkins@bullseyetelecom.com>

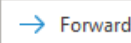
To Rob Moore



Reply



Reply All



Forward



Tue 4/5/2022 2:08 PM

## External Email ##

04/05/2022

Dear Rob Moore,

I hope this notice finds you safe and well during this unprecedented time. While we have all been working remotely over the past several months, we are pleased to announce bullseyetelecom has begun the process of returning employees to the workplace.

We will be handling returning to work in a different way this time. We are offering employees at bullseyetelecom to sign up for their preferred days. This will be done on a **first come, first serve basis**.

[Please use this link to sign up for you're preferred days of return.](#) (you may have to sign in with your bullseyetelecom email to view)

Employees will be notified by the HR department of their assigned phase/return-to-office date based off sign up results.

Safety is of the utmost importance during this return-to-office process, and we have made numerous changes to our policies and procedures. For a updated list of processes and procedure [please click this link](#) (you may have to sign in with your bullseyetelecom email to view)

We will provide more-detailed information to each group of returning employees prior to their return-to-office date. If you have a conflict or concern regarding your return to the workplace, please contact HR me directly.

Carl Parkins - Human Resources Generalist, BullsEye Telecom  
Address: 25925 Telegraph Rd #210, Southfield, MI 48033  
Phone: (877) 438-2855



# Red Flags



**\*URGENT\*** BullsEye Return to Office SignUp

CP Carl Parkins <carl.parkins@bullseyetelecom.cc>  
To Rob Moore Tue 4/5/2022 2:08 PM

## External Email ##

04/05/2022

Dear Rob Moore,

I hope this notice finds you safe and well during this unprecedented time. While we have all been working remotely over the past several months, we are pleased to announce **bullseyetelecom** has begun the process of returning employees to the workplace.

We will be handling returning to work in a different way this time. We are offering employees at **bullseyetelecom** to sign up for their preferred days. This will be done on a **first come, first serve basis**.

[Please use this link to sign up for you're preferred days of return.](#) (you may have to sign in with your bullseyetelecom email to view)

Employees will be notified by the HR department of their assigned phase/return-to-office date based off sign up results.

Safety is of the utmost importance during this return-to-office process, and we have made numerous changes to our policies and procedures. For a updated list of processes and procedure [please click this link](#) (you may have to sign in with your bullseyetelecom email to view)

We will provide more-detailed information to each group of returning employees prior to their return-to-office date. If you have a conflict or concern regarding your return to the workplace, please contact HR me directly.

Carl Parkins - Human Resources Generalist, BullsEye Telecom  
Address: 25925 Telegraph Rd #210, Southfield, MI 48033  
Phone: (877) 438-2855

1. Sense of URGENCY
2. Email address is not the usual formatting for BullsEye
3. Date in email isn't consistent with most communications
4. The email is composed to address all of BullsEye, however it has a personal beginning with the user's name
5. BullsEye Telecom isn't anywhere on the email, only "bullseyetelecom" which isn't professional and not how employees of a company would usually format their company name
6. Words in Red Highlight and underlining draw the eyes of users to that point, skipping most of the rest of the email. This is why the email is staged as Urgent, to fool user's minds to look for stand out text
7. The signature is plain, not formatted professionally, and only contains public information from Google.





Let's review some more **Red** Flags!

# Double Charged, Please Refund

**From:** jennyb@gmail.network.com

**Reply-to:** jennyb@gmail.network.com

**Subject:** double charged

📎 statement.docm

✉ Send me a test email

🚩 Toggle red flags

36248

Hi Evan, I am emailing you directly because I haven't received any reply from your Accounting department, regarding my problem. My credit card has been charged twice by bullseyetelecom.com.

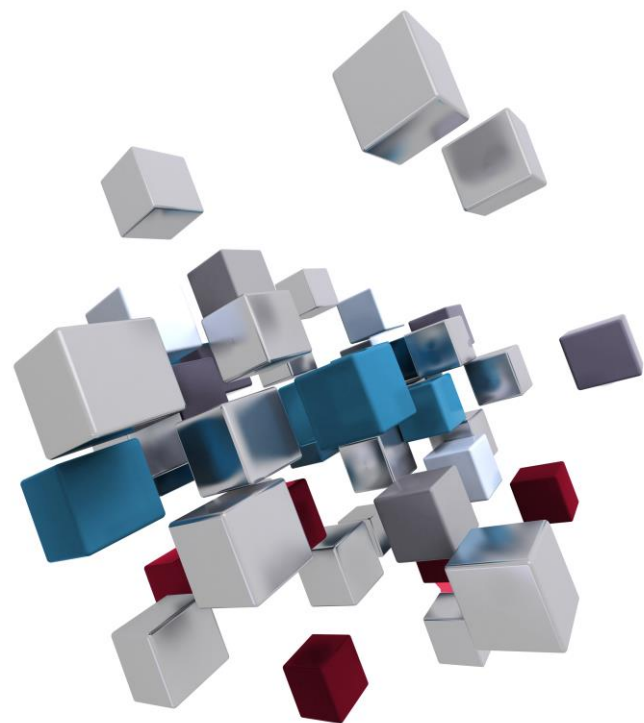
Please refund one of the charges. I am attaching my card statement as evidence.

Sincerely,

Jenny Block




# Strange Domain with attachment




**From:** [jennyb@gmail.network.com](mailto:jennyb@gmail.network.com)

**Reply-to:** jennyb@gmail.network.com

**Subject:** double charged

 [statement.docm](#)

 [Send me a test email](#)

 [Toggle red flags](#)

36248

Hi Evan, I am emailing you directly because I haven't received any reply from your Accounting department, regarding my problem. My credit card has been charged twice by bullseyetelecom.com.

Please refund one of the charges. I am attaching my card statement as evidence.

Sincerely,

Jenny Block

# Your quote is attached

**From:** jeffbarker@vccu.f1s.org  
**Reply-to:** jeffbarker@vccu.f1s.org  
**Subject:** Re: Your quote is attached.  
📎 Quote-VCCU-3.docm

[Send me a test email](#)  
[Toggle red flags](#)

Hi Evan,

The signed quote is attached. Thanks for the discount.

Sincerely,

Jeff Barker  
CEO, VCCU

--

On Friday at 2:44 PM, Evan Branstner <EBranstner@bullseyetelecom.com> wrote:

Dear Jeff,

Here is the quote we discussed on the phone. I was able to get you a substantial discount from the previous quote.

Please sign and return. Thank you for your business!

Sincerely,

Evan Branstner  
EBranstner@bullseyetelecom.com





# Replying to an email you never sent



**From:** [jeffbarker@vccu.f1s.org](mailto:jeffbarker@vccu.f1s.org)  
**Reply-to:** [jeffbarker@vccu.f1s.org](mailto:jeffbarker@vccu.f1s.org)  
**Subject:** [Re: Your quote is attached.](#)  
[Quote-VCCU-3.docm](#)

[Send me a test email](#)  
[Toggle red flags](#)

Hi Evan,

The signed quote is attached. Thanks for the discount.

Sincerely,

Jeff Barker  
CEO, VCCU

--

On Friday at 2:44 PM, Evan Branstner <[EBranstner@bullseyetelecom.com](mailto:EBranstner@bullseyetelecom.com)> wrote:

Dear Jeff,

Here is the quote we discussed on the phone. I was able to get you a substantial discount from the previous quote.

Please sign and return. Thank you for your business!

Sincerely,

Evan Branstner  
[EBranstner@bullseyetelecom.com](mailto:EBranstner@bullseyetelecom.com)



Can you find the **Red** Flags?

# RSVP to Company Event

**From:** Corporate Events Organizing Dept. <RSVP@CorporateEvents.org>  
**Reply-to:** Corporate Events Organizing Dept. <RSVP@CorporateEvents.org>  
**Subject:** RSVP Required to Company Event

**Template ID:** 36248-44  
[Send me a test email](#)  
[Toggle Red Flags](#)

Dear Employees,

This year the company has decided to throw a birthday party for our CEO. This will take place on March 8, 2019. We want you to be a part of this celebration. We felt you deserved some fun time after all the hard work you do. However this is a surprise party. That is why we are using this [RSVP Event service](#). Please keep this a secret and do not talk about it in the halls.

You must [RSVP](#) to this event, as we will need to know how much food to cater in. Please [click here](#) to RSVP and let us know how many others you will be bringing (your family members are invited).

We are trying to keep this a secret so please do not mention this to anyone else... and especially (you know who).

**As a reminder, we recommend that you:**

- Please keep this event as a secret
- [RSVP](#) as soon as possible
- Have a good time at the party!

Sincerely,

HR Department



# Many Red Flags!

- Email from outside company, strange domain
- Are emails like this normal from our HR?
- Ambiguous greeting
- Explains why you have to click the link
- Hover over the link, it does not make sense
- Sense of urgency to click the link

**From:** Corporate Events Organizing Dept. <[RSVP@CorporateEvents.org](mailto:RSVP@CorporateEvents.org)>  
**Reply-to:** Corporate Events Organizing Dept. <[RSVP@CorporateEvents.org](mailto:RSVP@CorporateEvents.org)>  
**Subject:** [RSVP Required to Company Event](#)

[Dear Employees,](#)

This year the company has decided to throw a birthday party for our CEO. This will take place on March 8, 2019. We want you to be a part of this celebration. We felt you deserved some fun time after all the hard work you do. However this is a surprise party.

[That is why we are using this](#) [RSVP Event service](#). Please keep this a secret and do not talk about it in the halls.

You must [RSVP](#) to this event, as we will need to know how much food to cater in. Please [click here](#) to RSVP and let us know how many others you will be bringing (your family members are invited).

We are trying to keep this a secret so please do not mention this to anyone else... and especially (you know who).

**As a reminder, we recommend that you:**

- Please keep this event as a secret
- [RSVP](#) [as soon as possible](#)
- Have a good time at the party!

Sincerely,

HR Department



# HR Cyber Bullying

**From:** Human Resources <hr@bullseyetelecom.com>  
**Reply-to:** Human Resources <hr@bullseyetelecom.com>  
**Subject:** Cyber-Bullying Document

**Template ID:** 36248-613048

[Send me a test email](#)

[Toggle Red Flags](#)

Human Resources has invited you to **see** the following document:

 [Cyber-Bullying Document](#)



Hey everyone this is Kelly from HR,

It has come to my attention that someone has been circulating this document around the office and I'm sure many of you have seen it already so I just wanted to get it out in the open. This kind of cyber bullying will not be tolerated at Bullseye Telecom Inc and must stop immediately. Many of the things said in it were very hurtful to all those involved. I cannot advocate this kind of behavior and if it doesn't stop soon, then disciplinary action will have to be taken.

If anybody has any knowledge as to the creation of this document please email me [here](#).

Thanks,  
Kelly

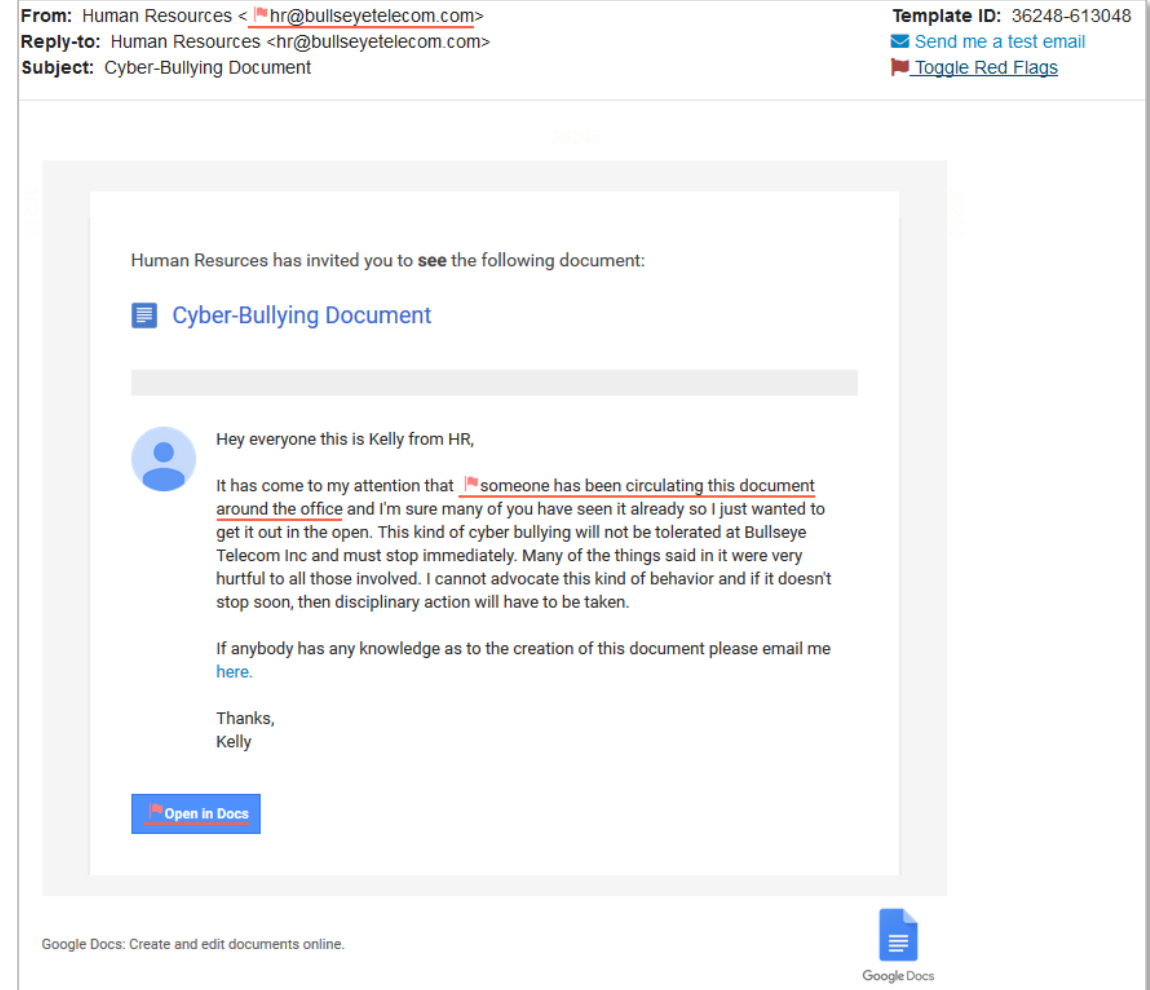
[Open in Docs](#)

Google Docs: Create and edit documents online.



# HR Cyber Bullying

- HR does not use an email address like this
- There is no Kelly in HR
- “Shocking content” to entice you to click the link
- Hover over the link, it does not make sense



# Look out for these Red Flags!

## FROM

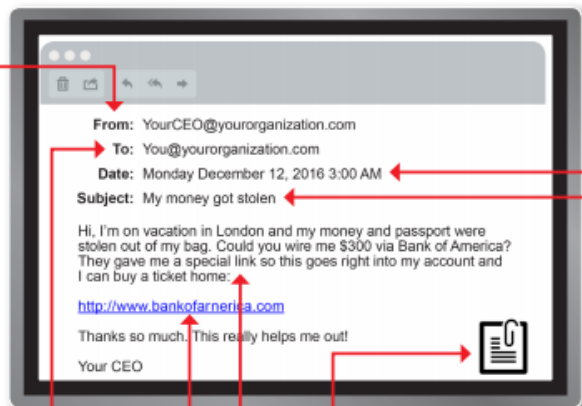
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink** or an **attachment** from someone I haven't communicated with recently.

## TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofamerica.com](http://www.bankofamerica.com) — the "m" is really two characters — "r" and "n."



## DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

## SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

## ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

# Other Security Tips to Remember

- Passphrases are better than passwords
  - Bulls3y@ - *Meh*; peachB1anketfi\$h - *Awesome!*
  - And don't reuse passphrases/passwords
- If it seems out of the ordinary, it probably is
  - Use your intuition
- Two factor authentication may seem like a nuisance but think of it as your last wall of defense.
  - Even if your credentials are compromised, hackers would still need your device or be able to convince you to allow access.
    - If you didn't initiate a log-in in the last minute and you get a 2<sup>nd</sup> factor request, do NOT accept it! Do NOT click Yes.
    - Also – even if you click No, report it because it means someone has your login credentials.
    - Change your password(s) ASAP.
- Check out <https://haveibeenpwned.com/>





# Questions?

Thank you for attending

