



digital defense fund

Phishing: The Most Common Attack

Last updated 7/13/22

Phishing is the most common attack on nonprofits!

INCIDENT TYPE	COUNT OF INCIDENTS	COUNT OF SAMPLE	% OF SAMPLE EXPERIENCE INCIDENT
1. Email Phishing	140	41	26%
2. Malware	54	39	25%
3. Account Compromise	20	18	12%
4. Business Email Compromise	14	13	8%
5. Wire fraud	3	3	2%
6. Virus	1	1	1%
7. Advanced Persistent Threat	1	1	1%
8. Supply Chain	0	0	0%
9. Ransomware	0	0	0%
Grand Total	233	116	50%



Top 10 incident types from Community IT's 2018 Non-profit Cybersecurity Incidents Report
<https://www.communityit.com/wp-content/uploads/2019/03/NonprofitCybersecurityIncidentReport.pdf>

Solutions: Learn to identify phishing & email scam attempts



What is phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

Phishing can also tempt you to download and install malware.

Source: Wikipedia



What are phishing email scams?

Phishing can also simply try to get money or assets by disguising as a trustworthy entity in an electronic communication.

For email scams, the attacker doesn't even want or need your password! Often, they just try to pretend to be your boss or someone offering you an opportunity.



Why do people phish?

- To get your password
- To get your money
- To get confidential information
- To get you to execute code or download malware on your computer



Why does phishing work?

Phishers capitalize on our:

- Urge to be polite
- Urge to be helpful
- Fear of being embarrassed
- Panic about urgent messages

+ The only way to truly prevent it is to double check *everything* in another communication channel. We're too busy for that!!



Examples of phishing:

You may have experienced these already!

No shame

👉 Remember, people phish because it works, and it works because we're busy people who want to help people who contact us!



The fake boss gift card scam

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

From: [redacted]

Date: Tue, Jul 14, 2020 at 6:12 AM

Subject: Urgent

To: [redacted]

CC: [redacted]

Hi [redacted]

Visualizing my inner self-thinking of someone in the office who might be wonderful and honesty to run a personal errand for me. Imaging your accomplishments I pictured you. Kindly send me your cell and wait for my instructions.

Thanks

[redacted]

--



Display name set to boss's name



If you open on mobile, you won't see the real (random) email address



From: [redacted] <ashly👮🏻👮🏻4@gmail.com>

Sent: Monday, July 20, 2020 9:05 AM

To: [redacted]

Subject: INSTANT ASAP!!!

Hi Megan,

Would it be possible for you to complete a task for me before this conference ends ?

Please give me your personal number.

Thanks,

[redacted]

Sent from my iPhone.



Next step in the scam (if you take the bait)

From: [REDACTED]
To: [REDACTED]
Subject: RE: Vice President of [REDACTED] Task [REDACTED].
Date: Tuesday, November 6, 2018 11:43:21 AM

OK! This is what I need is AMAZON GIFT CARDS OR GOOGLE PLAY GIFT CARDS of \$100 or \$200 face value. I need 20 of Each card. That's $\$100 \times 20 = \2000 . Scratch the back out and Email me the codes or pictures of the codes. Let me know how soon you can get this done.

Regards
Sent from my iPhone



How do the scammers do this?

- Use data from LinkedIn (breach or current profiles) or emails & organization structure scraped from website to figure out who is the boss & who reports to them
- Get an email & pretend to be the boss!
 - Make a new free email account with boss's name
 - Or use an email from a breach list and change the display name to the boss's name
- **This scam is becoming more common over SMS as well!**
 - Scammers find phone number data online (data aggregators) or in breach data



Breach lists with emails & passwords can be used for scams!

- Breach lists of usernames, emails, and passwords become available when a website or company doesn't adequately protect their user information database and a cybercriminal hacks the company and steals this data
- Scammers can use your email & password to try to hack your accounts, but also for scams
- If you don't realize your password is out there (check if it is at [www.haveibeenpwned.com!](http://www.haveibeenpwned.com)), this can be really disconcerting



Delete Not junk ▾ Block ...

I know everything - proof

 This message was identified as spam. We'll delete it after 9 days. [It's not spam](#)



[Redacted]
Sun 4/28/2019 12:35 AM

You ↵



Hi!

I know that: D3[Redacted]ld - is your password!

Also as you may have noticed, I sent this email from your email account (if you didn't see, check the from Sender email ID.)

I infected you with my private malware, RAT, (Remote Administration Tool) some time ago.

The malware gave me full access and control over your computer, meaning, I got access to all your accounts and I can see everything on your screen, even turn on your camera or microphone and you won't even notice about it.

I made a video showing both you (through your webcam) and the video you were watching (on the screen) while satisfying yourself!

I can send this video to all your contacts (email, social network)!



This is a scam! How did they do it?

- They got your email & password from a breach list
- They use software to spoof your email address (make it look like they are sending from your email address) or just change the display name of a random email address

**HACKER
BLACKMAIL
WHO CRACKED
YOUR EMAIL
SCAM**

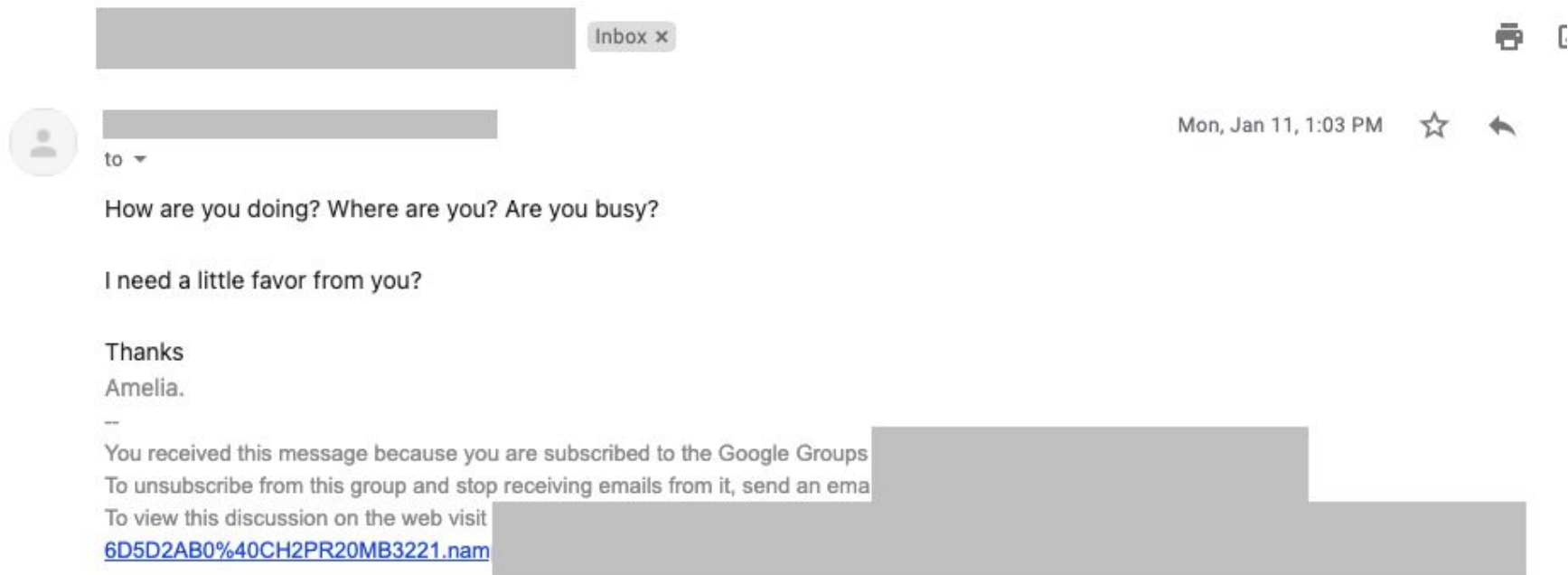


Password breaches can also be used to access accounts.

Once the attacker gains access to an email account, they can send scam attempts to all of the contacts associated with that account.



Gift card scam: after they hack an email



If you respond...

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

From: [REDACTED]

Date: Mon, Jan 11, 2021 at 12:39 PM

Subject: Re: [REDACTED]

To: [REDACTED] >

Good to hear from you, I hope all is well with you? I need you to help me get an Apple gift card for my Niece, It's her birthday but I can't do this now because I was involved in a car crash few days ago and i'd promised to get the card for her today. I have a fracture of my lumbar L1 and fracture of my right wrist.. Can you get it from any store around? Or you can help me purchase online. I'll pay back next week when I get home.

Please let me know if that would be possible?

Amelia.



Phishing for Passwords

- Email will pretend to be from a service you use, and lead you to a fake login page

Mustafa Al-Bassam @musalbas · Sep 9, 2018
Quick phishing demo. Would you fall for something like this?

Gmail - Chromium
Secure | <https://accounts.google.com.secure.computer.shop/#!...>

demo.html#
Google
file:///home/mus/Code/popup-phishing-demo/demo.f

One account. All of Google.

Sign up with Google

Enter your email

Next

Find my account

Create account

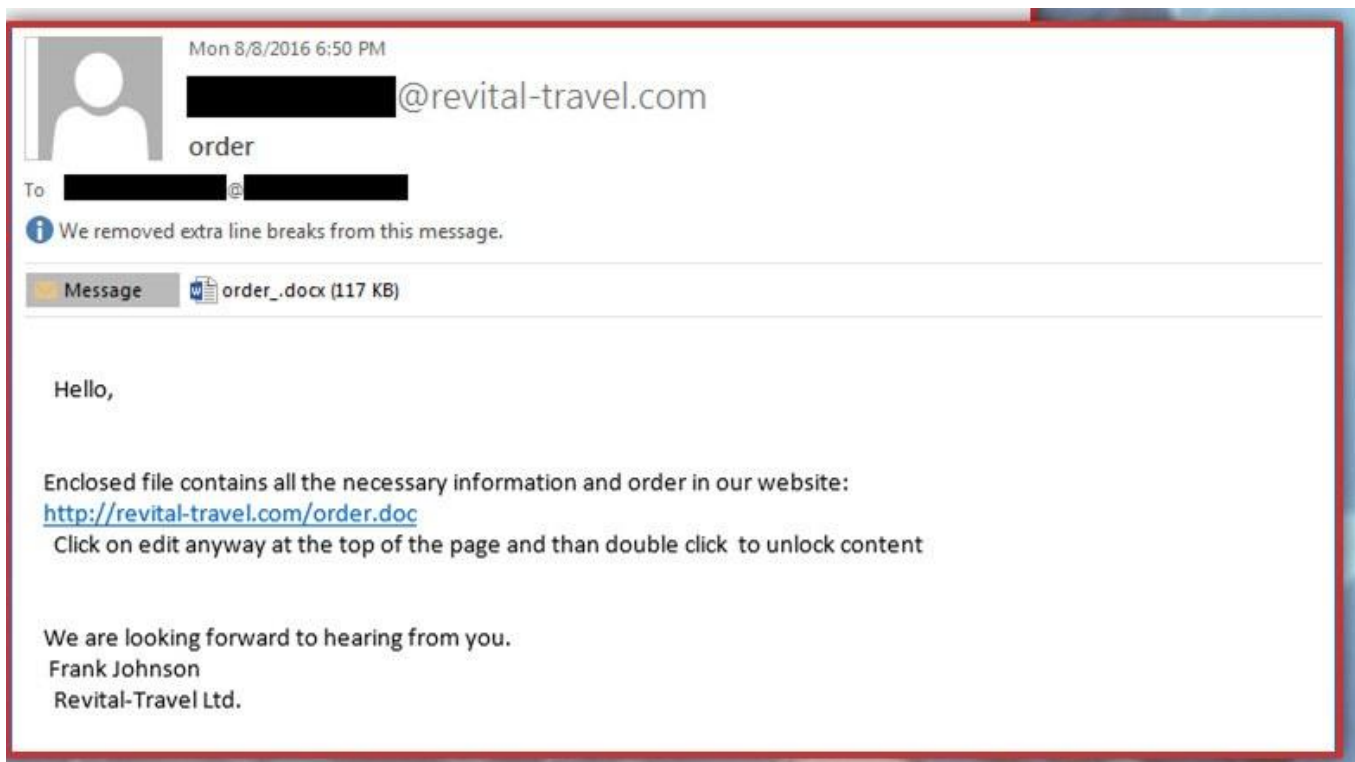
One Google Account for everything Google

0:02 485.1K views

373 4.8K 7.9K

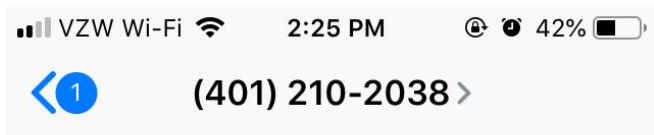
Phishing to add malware to your device

- Email will try to convince you to download something



<https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/>

Not just emails: phishing texts, DMs, phone calls...

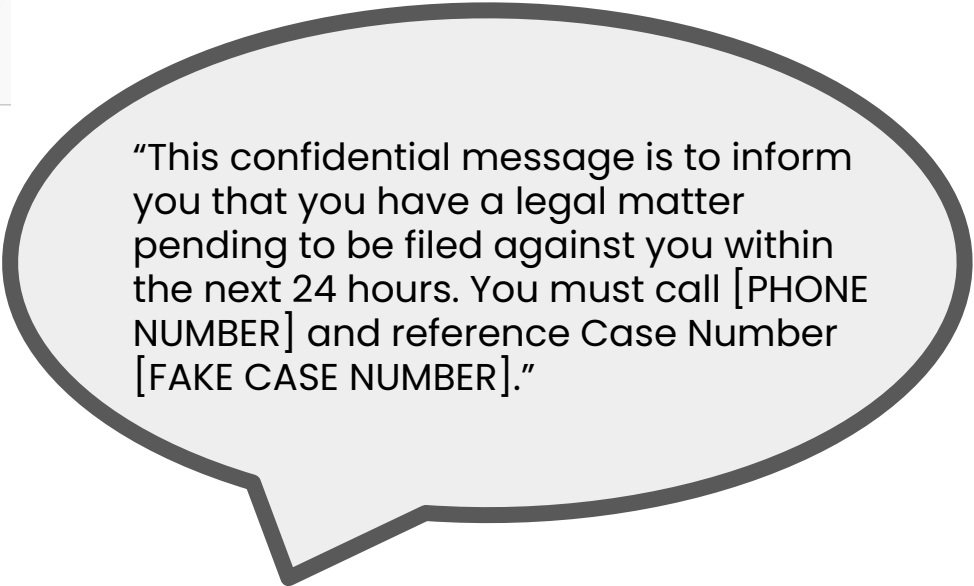


Text Message
Today 2:19 PM

Hi Amanda, this is your delivery man. I was at your home earlier, but noone was at home. Confirm now: <http://8xuwajt.top/jpw6xw>

The sender is not in your contact list.

[Report Message](#)



"This confidential message is to inform you that you have a legal matter pending to be filed against you within the next 24 hours. You must call [PHONE NUMBER] and reference Case Number [FAKE CASE NUMBER]."

Facebook messages:



Page Policy

Assign conversation ▼



Help Center

copyright-case105426.site

We have received reports that your page published posts that doesn't comply with our policy. Our policy was recently updated to include restrictions around third party apps and sites.

Using copyright content will result in removing it from your page, in the worst case deleting your page permanently. If you think that this was a mistake, you should submit an appeal.

<https://copyright-case105426.site/contact/id=21058/>

Note: If within 48 hours, you have not submitted an appeal on our link, then you have ignored our notifications and your page will be suspended.

Sincerely,
Helpdesk.



You are no longer able to send messages to this person. [Learn more.](#)

On the phone & social media,
the pressure to act quickly &
be helpful can be even
stronger!



We're going to walk through how you can identify phishing emails, but remember the only surefire way to prevent phishing from being successful is to double check everything (outside of email). But you can save time (and not have to double check!) by recognizing a scam right away.

To further muddy the waters: Some legitimate emails will have these red flags. But it never hurts to double check those too!



Signs of Phishing

From

To

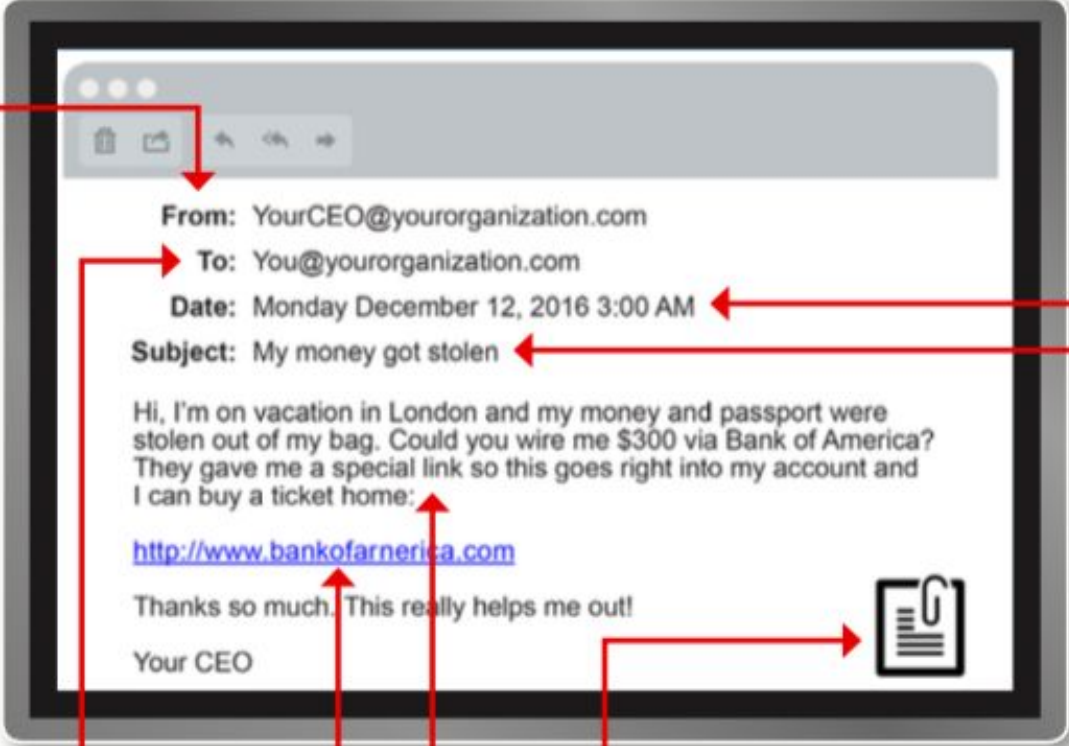
Links

Date

Subject

Content

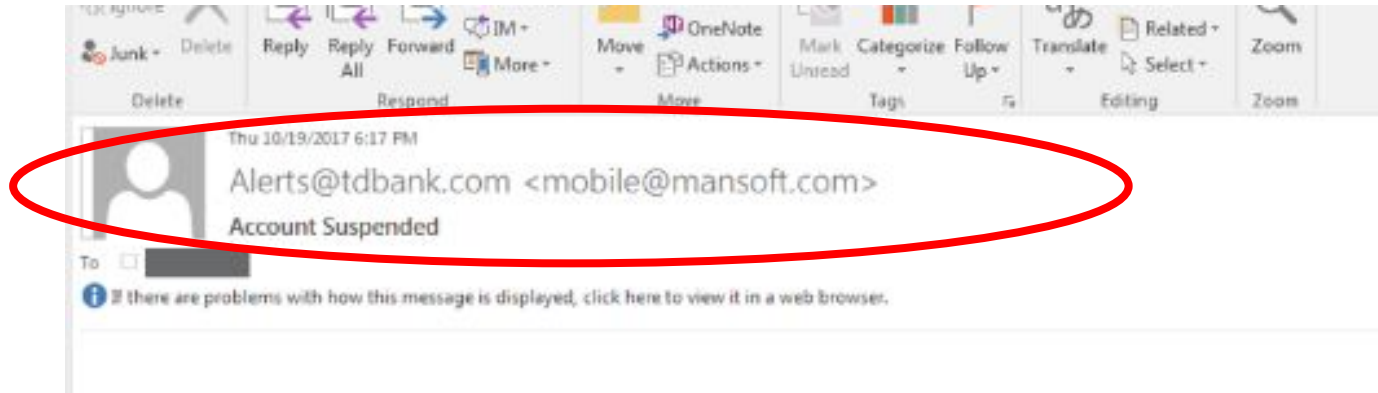
Attachments



From: Red Flags

- Don't recognize the contact
- Not work related, but sent to work email (or vice versa)
- From same domain or a known contact but content is unusual
- Domain is odd (has extra characters, spaces, or doesn't match what the contact claims - like, micorsoft.com)
- Embedded link or attachment from someone you don't regularly communicate with or weren't expecting to hear from





Note that on a mobile phone,
only the first item will display!



From: Red Flags

From: "Dropbox Notification" <dropbox.noreplay@gmail.com>
Date: Dec 7, 2016 [REDACTED]
Subject: You have 1 new file in your inbox
To: [REDACTED]
Cc:



Hi [REDACTED]

You have received a new document in your inbox, view the file "مذكرة القبض على عزة سليمان.pdf" on Dropbox.

[View file](#)



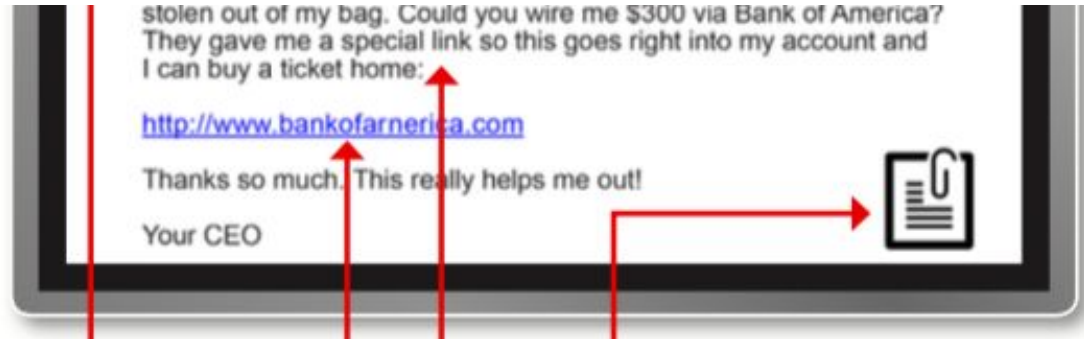
To: Red Flags

- You are cc'ed along with people you don't know
- You are cc'ed with an odd group of people - like, everyone who shares the first letter of your name



Hyperlinks: Red Flags

- Hovering over the hyperlink reveals an address that doesn't match what is displayed
- Hyperlinks are out of context or make up the whole email
- Hyperlink is misspelled - as in the example, www.bankofarnerica.com – the “m” is really two characters – “r” and “n.”



Hyperlink rule of thumb:

Never log into an account from a link sent to you in an email or text!

Instead, open a fresh tab or window, go directly to the site, and login from there.



Know your URLs

https://www.google.com/path

Subdomain SLD TLD Path

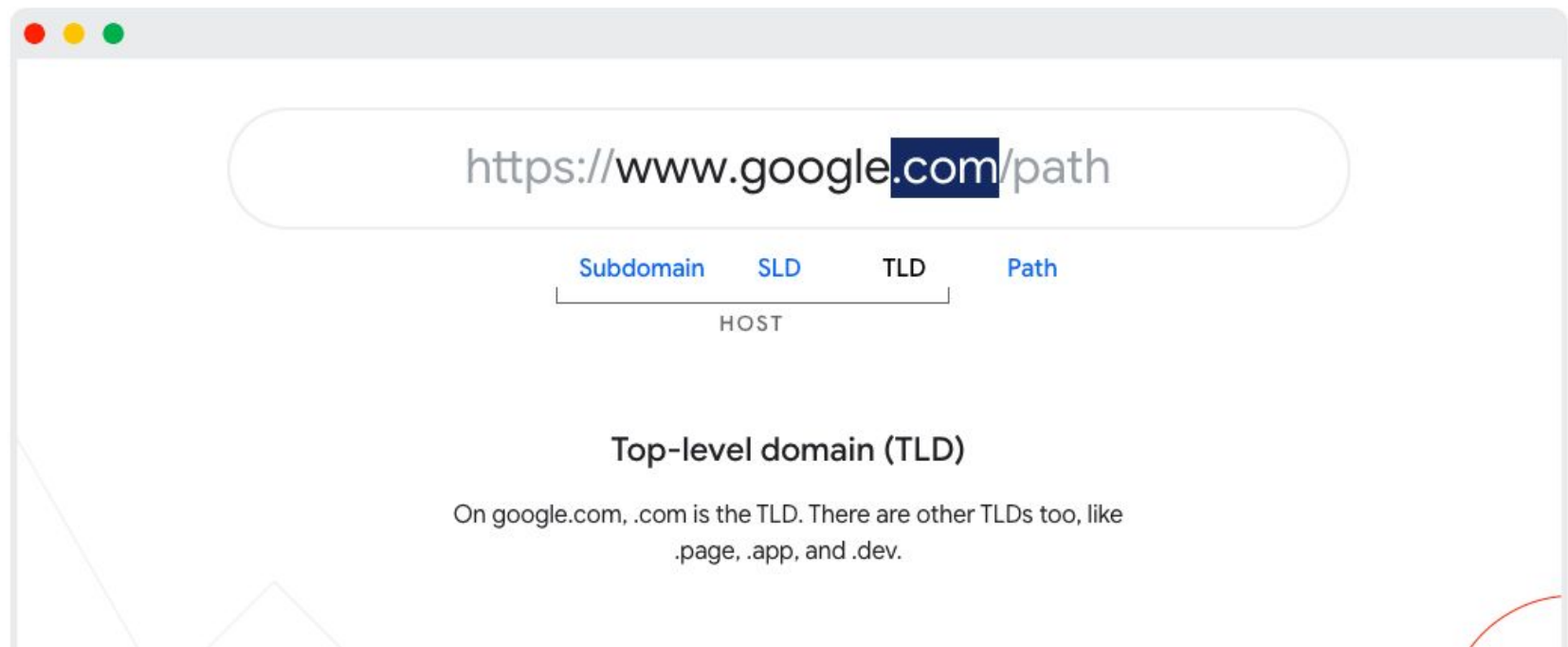
HOST

Second-level domain (SLD)

This is the part you can register and own. On www.google.com, google is the SLD. On safe.page, safe is the SLD.



Know your URLs



Know your URLs



https://www.google.com/path

Subdomain

SLD

TLD

Path

HOST

Subdomain

Once you own an SLD, you can set up a subdomain (or several), like `blog.yourdomain.page` and `my.blog.yourdomain.page`.



Hyperlinks: Trash before slash!

- The cybercriminal can buy a new domain that mimics a real one, for example:

www.google.com.info/login

spotify.com.home/favorite

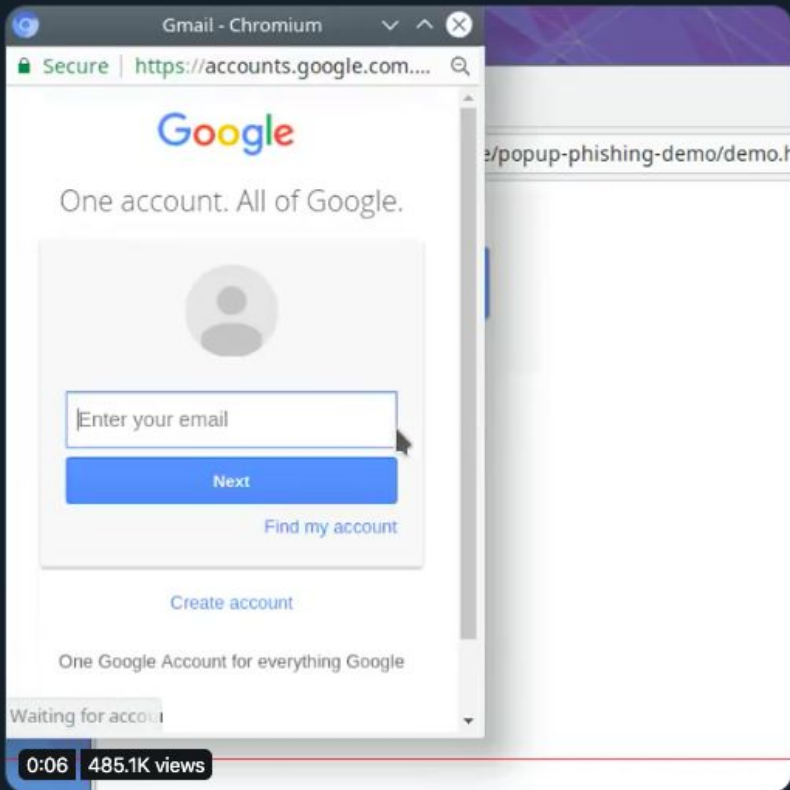
bankofamerica.us.com.webapp/





Mustafa Al-Bassam @musalbas · Sep 9, 2018

Quick phishing demo. Would you fall for something like this?



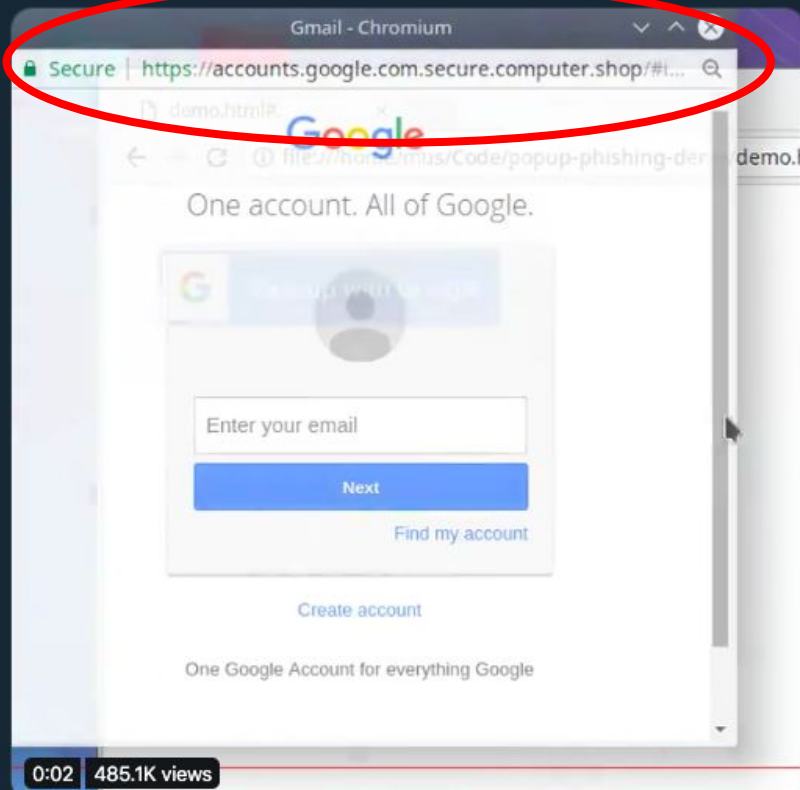
0:06 485.1K views

373 4.8K 7.9K



Mustafa Al-Bassam @musalbas · Sep 9, 2018

Quick phishing demo. Would you fall for something like this?

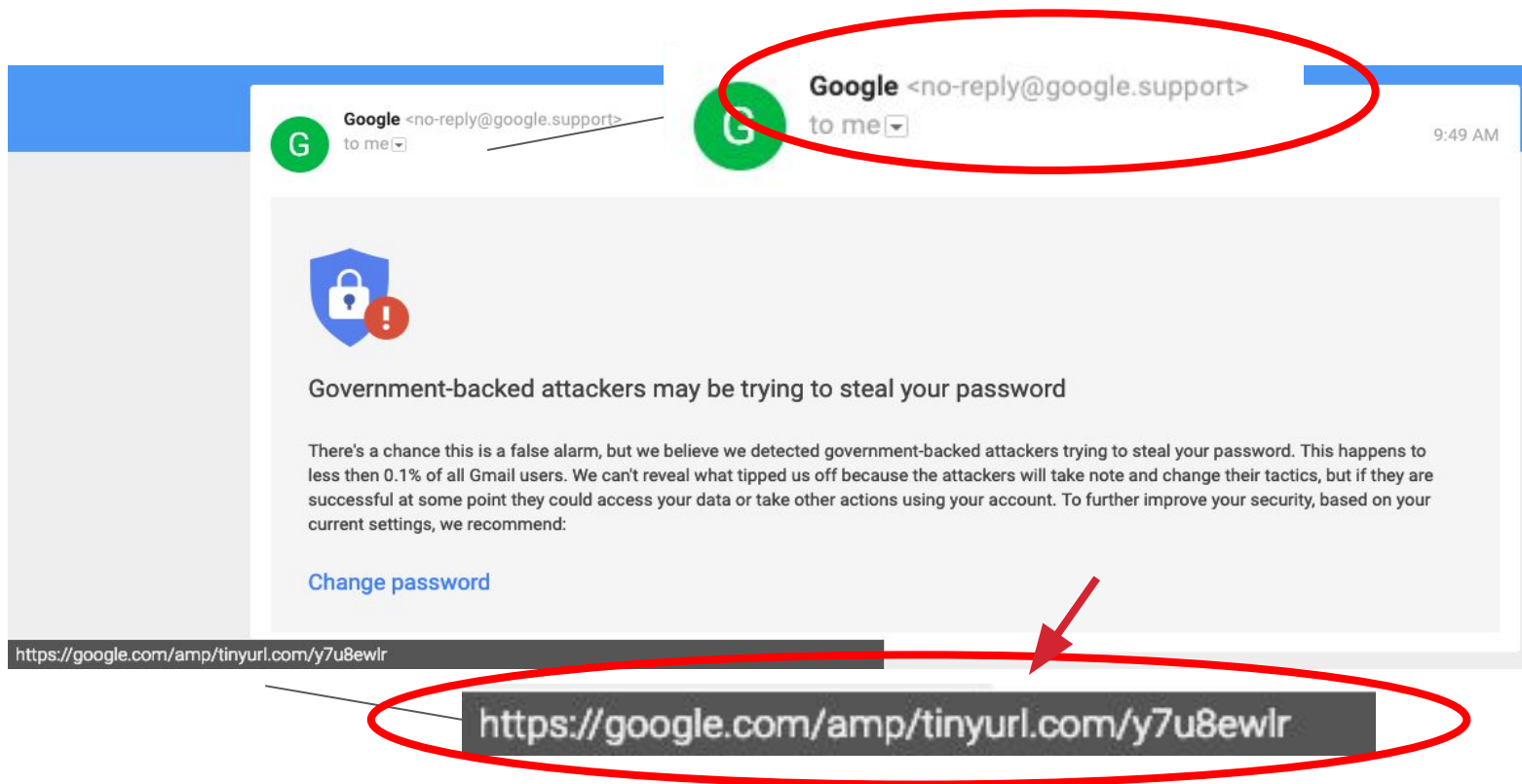


0:02 485.1K views

373 4.8K 7.9K



Hyperlinks: there's another link in the link!



How can you check a link you're unsure about, without clicking on it?

Thanks to Elle at Jane's Due Process for this screenshot!

A screenshot of a Facebook message from a page named "Page Policy". The message is from the "Help Center" and is addressed to "copyright-case105426.site". The message text reads: "We have received reports that your page published posts that doesn't comply with our policy. Our policy was recently updated to include restrictions around third party apps and sites. Using copyright content will result in removing it from your page, in the worst case deleting your page permanently. If you think that this was a mistake, you should submit an appeal." Below this is a link: <https://copyright-case105426.site/contact/id=21058/>. A note follows: "Note: If within 48 hours, you have not submitted an appeal on our link, then you have ignored our notifications and your page will be suspended." The message is signed "Sincerely, Helpdesk." At the bottom of the screenshot, a grey box contains the text: "You are no longer able to send messages to this person. [Learn more.](#)"

Page Policy
Assign conversation ▾

Help Center
copyright-case105426.site

We have received reports that your page published posts that doesn't comply with our policy. Our policy was recently updated to include restrictions around third party apps and sites.

Using copyright content will result in removing it from your page, in the worst case deleting your page permanently. If you think that this was a mistake, you should submit an appeal.

<https://copyright-case105426.site/contact/id=21058/>

Note: If within 48 hours, you have not submitted an appeal on our link, then you have ignored our notifications and your page will be suspended.

Sincerely,
Helpdesk.

You are no longer able to send messages to this person. [Learn more.](#)

Tool: urlscan.io

urlscan.io/result/2501c759-5ec1-4dca-9055-f94db4a47045/

urlscan.io Home Search Live API Blog Docs Pricing Login Sponsored by SecurityTrails

copyright-case105426.site

198.211.116.46 **Malicious Activity!**

URL: <https://copyright-case105426.site/contact/id=21058/>
Submission: On February 01 via manual (February 1st 2022, 4:54:51 pm UTC) from — Scanned from

Summary HTTP 10 Redirects Behaviour Indicators Similar DOM Content API

Summary

This website contacted **6 IPs** in **4 countries** across **5 domains** to perform **10 HTTP** transactions. The main IP is **198.211.116.46**, located in **North Bergen, United States** and belongs to **DIGITALOCEAN-ASN, US**. The main domain is **copyright-case105426.site**.
TLS certificate: Issued by R3 on February 1st 2022. Valid for: 3 months.

This is the only time *copyright-case105426.site* was scanned on urlscan.io!

urlscan.io Verdict: **Potentially Malicious**

Targeting these brands: Facebook (Social Network)

Live information

Google Safe Browsing: **Malicious** for *copyright-case105426.site*
Current DNS A record: 198.211.116.46 (AS14061 - DIGITALOCEAN-ASN, US)

Screenshot

Page Statistics

10	100 %	40 %	5	5
Requests	HTTPS	IPv6	Domains	Subdomains
6	4	103 kB	326 kB	0

Domain & IP information

IP/ASN	IP Detail	Domain	Domain Tree	Links	Certs	Frames
--------	-----------	--------	-------------	-------	-------	--------



Subject: Red Flags

- Is the subject line unrelated to the email?
- Is the subject line misspelled?
- Does it convey an urgent event that is out of context for that sender?
- Does it start with RE: but you've never talked to that person or about that topic before?
- Is it a forwarded (FW:) email you aren't expecting or from someone you don't know?



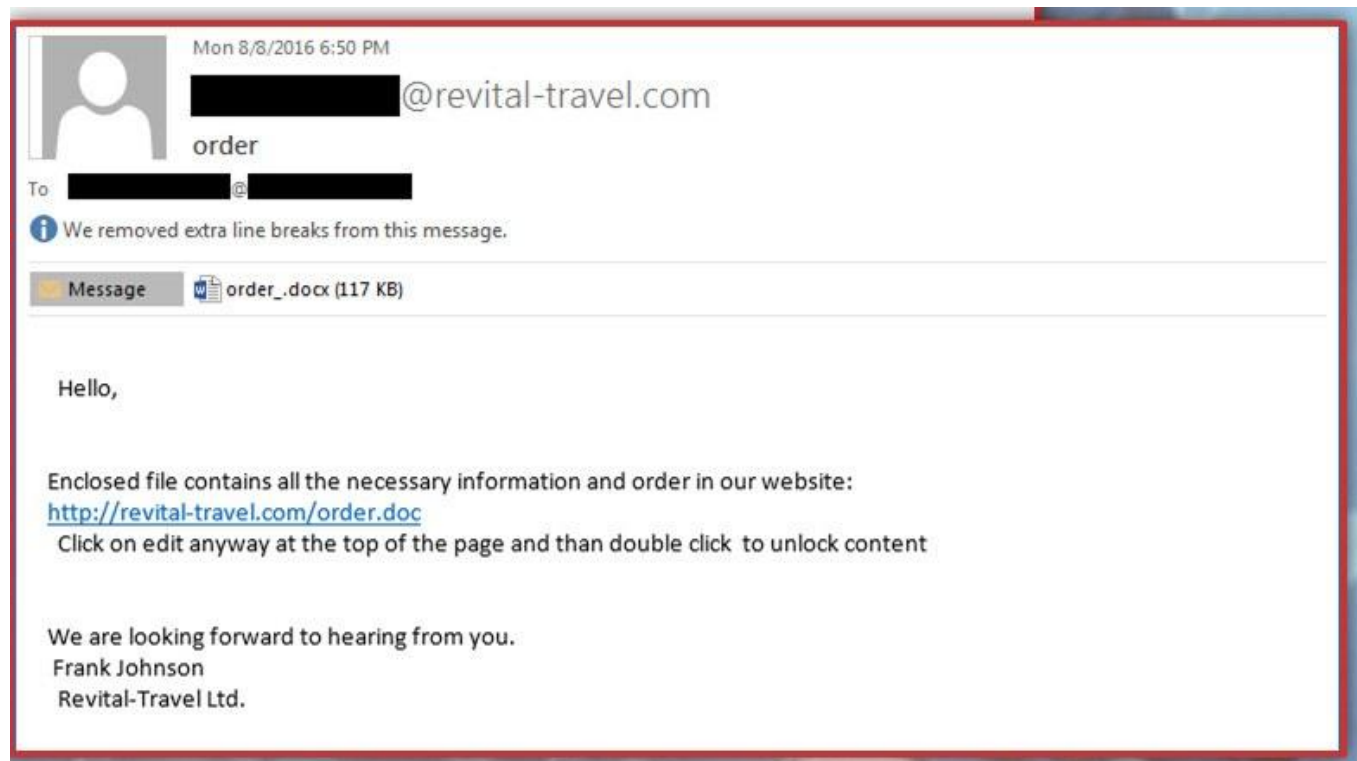
Attachments: Red Flags

Unless you expected an attachment, an attachment is always a red flag!!

- Does the attachment file type make sense in relation to the email?
- Are you instructed to enable editing or otherwise take action with the document?



Attachment: instruction to unlock content



<https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/>



Attachments: Example

Phish Fry

On or around March 27 of last year, an employee at a Red Robin Gourmet Burgers and Brews received an email from ray.donovan84@yahoo.com. The note complained about a recent experience; it urged the recipient to open the attachment for further details. They did. Within days, Fin7 had mapped Red Robin's internal network. Within a week, it had obtained a username and password for the restaurant's point-of-sale software management tool. And inside of two weeks, a Fin7 member allegedly uploaded a file containing hundreds of usernames and passwords for 798 Red Robin locations, along with "network information, telephone communications, and locations of alarm panels within restaurants," according to the DoJ.



Email compromise: sent to all contacts

Austin Diaper Bank Project Inbox x



[redacted]@austindiapers.org
to adobesharepoint@austindiapers.org ▾

Tue, Sep 28, 2:28 PM (7 days ago) ☆ ↶ ⋮

Please see attachment.

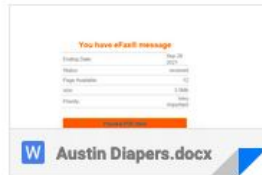
Thanks,

[redacted]

[redacted]

Austin Diaper Bank
austindiapers.org
Tel (512) 710-7242

[redacted]



Email compromise: attachment sent to all contacts

Austin Diaper Bank Project Inbox x



[Redacted]@austindiapers.org>

to adobesharepoint@austindiapers.org ▾

Please see attachment.

Thanks,

[Redacted]

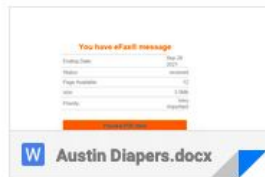
[Redacted]

Austin Diaper Bank

austindiapers.org

Tel (512) 710-7242

[Redacted]



You have eFax® message

Ending Date:	Sep 28 2021
Status:	received
Page Available:	12
size:	3.5Mb
Priority:	Very Important

[Preview PDF Here](#)

Austin Diapers.docx



Content: Red Flags

- Does the email threaten negative consequences?
- Does the email promise a reward or monetary gain?
- Is grammar and spelling off?
- Does the sender ask you to click a link or open an attachment?
- What does your gut say?
- Does the email ask you to look at something compromising or embarrassing?



What to do if you suspect phishing:

The next few slides contain screenshots of a security researcher who suspects his mother has received a phishing email. He walks through a few steps to verify if the email is real!



What to do if you suspect phishing:





Vess @VessOnSecurity · Aug 6

Replying to [@VessOnSecurity](#)

So, I do. E-mail headers look perfectly OK. It really does seem to come from the mobile provider. Is this some trick I don't know?

The message addresses me correctly by name. OK, maybe they got it from somewhere.

Message says ZIP's encrypted with a password to protect data.





Vess @VessOnSecurity · Aug 6

Password is my date of birth, YYMMDD. OK, that's not hard to find, either. But if this is an attack, it's a hell of a targeted one...

But you can see what's in the ZIP archive without entering a password; archive directory is not encrypted. It's a PDF file.

Hmm...





Vess

@VessOnSecurity



So, taking all precautions, I open the PDF file in the virtual machine with no Internet connection.

IT'S THE F**U****CKING MONTHLY BILL!!!**

It's not an attack. The idiots have sent the bill exactly as the scammers do!

That is why we can't end phishing...

10:44 AM · Aug 6, 2020 · [TweetDeck](#)





Vess @VessOnSecurity · Aug 7

They basically answered that "this is how we're doing it now", which is not surprising; customer service has no authority to make such decisions.

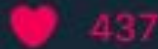
But look at the sender address.

ARE YOU F**U**CKING KIDDING ME?!



● **customerservice@a1.bg** <mtel915469@livehelpnow.net>

To: vbontchev@yahoo.com



Moral of the story:

This stuff is hard &
confusing, even for
experts!



We'll never be able to detect every phishing email, unless we verify every single email we receive.



Prevent phishing:

- Change norms: Reaching out to a peer organization or colleague to confirm the email is both appropriate and effective.
- Keep your email private.
 - Spear phishers scrape emails from websites so keep your email off your website, workplace's website, and social media accounts.
- If you get an email or text asking you to log in to a site, don't click the link! Open a new tab and log in directly on the site.
- Slow down!
- Trust your gut.
- Learn to recognize the signs and always double check for them...



If you suspect phishing

- DO NOT CLICK!
 - Do not click on links!
 - Do not open attachments!
 - Do not enable editing!
 - If you haven't already, don't open the email!
- If it's (supposedly) from someone you know:
 - Text or call to verify
- If it's from someone you don't know:
 - Forward it to a manager, security, or IT support person at work!



If you do click and realize something is wrong...

- Tell someone else at your organization immediately!
 - Even if it looks like nothing bad happened, attackers can be carrying out malicious activity in the background like...
 - Sending spam emails from your account
 - Reading/monitoring your email
 - Changing details on your account
- Monitor your account's activity
 - Check the access logs
 - Check sent & deleted messages
 - Check for forwarding rules
- Change your password!



Key takeaway:

If an email is requesting money, asking you to open an attachment, or click a link, slow down & verify the authenticity!

