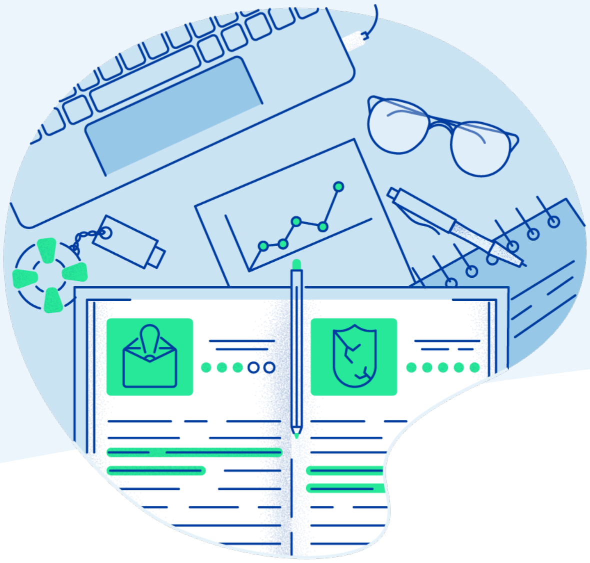
BLOG

Claims in the time of Coronavirus

Written by Catherine Lyle



On any regular day, scammers and fraudsters (aka, bad actors) are out in force. During COVID-19 they have ramped up efforts to take advantage of all aspects of the pandemic. While Coalition's claims team sees a variety of cyber events on a daily basis, we understand that the quickest way to monetize the crime will always be the most common. During the COVID-19 pandemic, the crime of choice is funds transfer fraud by way of email intrusion.

Email intrusion and funds transfer fraud

Email attacks have long been on the rise. Last month, Google revealed that they had blocked 18 million malware and phishing emails related to COVID-19, **per day**. While many think that spam is a mere annoyance, in reality, it poses a serious risk to businesses. Spam is just a phishing scheme in disguise trying to lure an employee into providing his or her credentials. While providing a password to email may seem innocuous, it effectively opens a window for a bad actor to view the entire internal operation of your company.

This window into the inner workings of your company allows a bad actor to figure out:

- Who reports to whom
- Who receives invoices
- Who pays invoices
- Who owes payment to your company
- To whom your company owes payment

And most importantly, how to use that information to steal money from you.

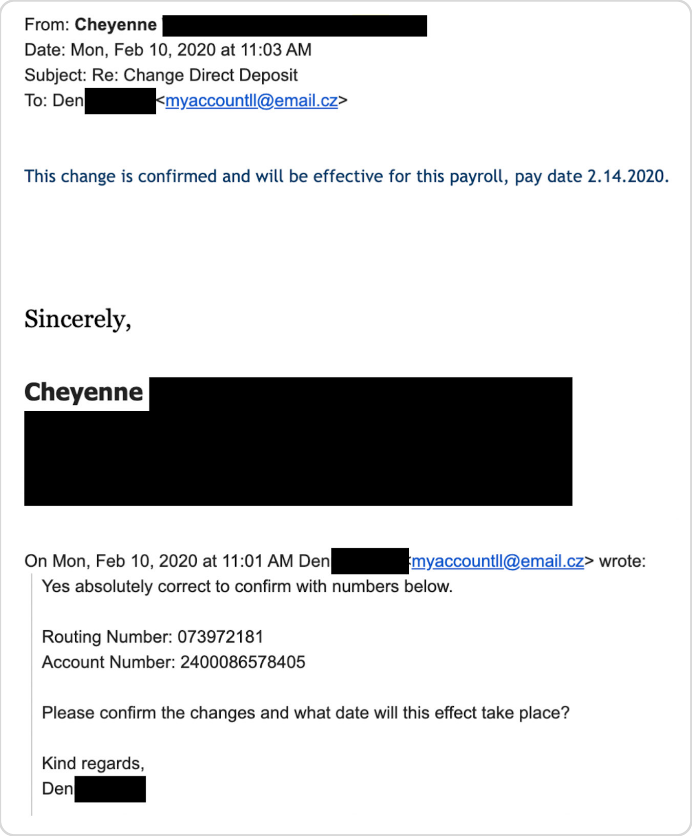
Executing an attack

How does this happen? With just a password, entry into an email account, and a little research, the bad actor now has enough information to insert themselves into any email conversations and all transactions. And while not all funds transfer fraud starts with email, at Coalition we've seen phishing emails as the root cause of 75% of funds transfer cases.

Don’t think it is possible to fall prey to this attack? In 2020 alone, Coalition has seen companies and nonprofits transfer millions of dollars to bad actors, with individual incidents well above $1 million. This doesn’t just impact large companies -- small companies and nonprofits are just as likely to be victims. While Coalition has recovered over 60% of all funds lost by its policyholders, the headache for those companies is not easily forgotten.

One of the reasons phishing attacks are so effective is hackers are able to very closely imitate legitimate company emails. Let’s look at some recent examples of spoofed emails that resulted in an incident:

Example 1
Spoofed email asking internal HR team member to update payroll with fraudulent account details. HR did not notice the spoofed email, only the reply to name and moved forward with the change.



From: **Cheyenne** [redacted]
Date: Mon, Feb 10, 2020 at 11:03 AM
Subject: Re: Change Direct Deposit
To: Den[redacted]<myaccountll@email.cz>

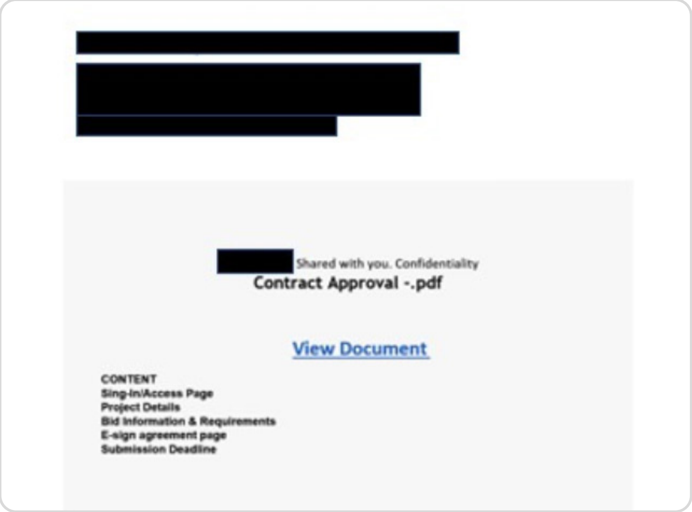
This change is confirmed and will be effective for this payroll, pay date 2.14.2020.

Sincerely,

Cheyenne [redacted]

On Mon, Feb 10, 2020 at 11:01 AM Den[redacted]myaccountll@email.cz> wrote:

> Yes absolutely correct to confirm with numbers below.
>
> Routing Number: 073972181
> Account Number: 2400086578405
>
> Please confirm the changes and what date will this effect take place?
>
> Kind regards,
> Den[redacted]



[redacted]

[redacted] Shared with you. Confidentiality
Contract Approval -.pdf

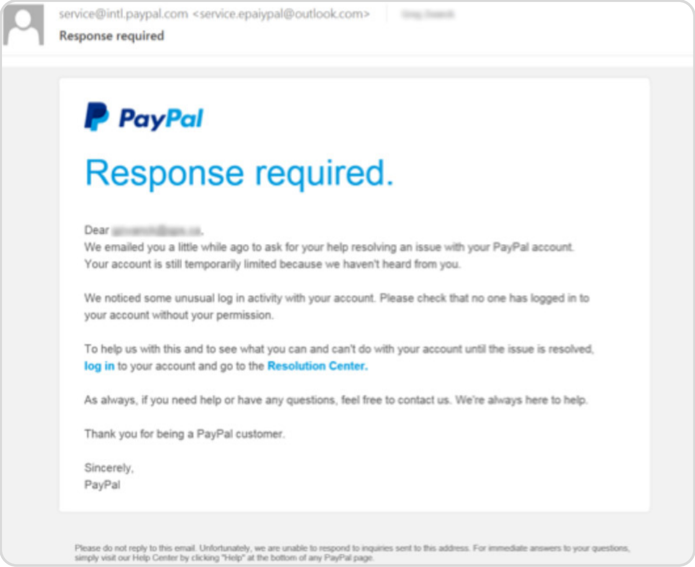
View Document

CONTENT
Sing-In/Access Page
Project Details
Bid Information & Requirements
E-sign agreement page
Submission Deadline

Example 2
Phishing link embedded in an email. Once the “View Document” link is clicked, the user is taken to a page to enter their credentials. The credentials are then harvested by a bad actor and used for future compromise.

Example 3

Phishing link embedded in an email. Once the "log in" link is clicked, the user is taken to a page to enter their credentials. The credentials are then harvested by a bad actor and used for future compromise.



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted]

Response required

PayPal

Response required.

Dear [redacted].
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Securing your organization

Thankfully, there are several basic security hygiene steps your organization can take to prevent being the victim of an attack:

1. Never rely on wiring instructions sent via email or in attachments. Whenever receiving a new instruction or a request to change an existing one, be sure to use a dual-control method to confirm the instruction (e.g., if you received it via email, make a phone call to a known good phone number to verify).

2. Always verify with your bank that the name of the organization you are transferring funds to matches the name associated with the account number provided to you (if it's fraudulent, it often won't).

3. Always use 2-factor authentication. That way, if someone in your organization is ever tricked into disclosing their credentials, the hacker will be missing the 2nd factor to gain account access.

4. Configure SPF and DMARC records to avoid email address spoofing — there is no cost to do so, and we've provided some guides to configure this in our cybersecurity help center.

5. Consider using an anti-phishing solution, or configuring your email client to notify you when you are receiving an email from outside of your organization.

Finally, if you believe you've experienced a funds transfer fraud incident, please contact us immediately. Coalition's Security & Incident Response Team (SIRT) is available to assist you, and has recovered millions in stolen funds -- but the faster you contact us, the easier it is to recover stolen funds. We are your cyber 911!

From all of us at Coalition: Stay safe! We are an email, phone call, or online chat away at all times.

Read More on Our Blog

Coalition, Inc. · 1160 Battery Street, Suite 350, San Francisco, CA 94111 · coalitioninc.com
Insurance products underwritten by Coalition Insurance Solutions, Inc. (CA License # 0L76155)