PHISHING

11 phishing email subject lines your employees need to recognize.

March 20, 2022 by Christine McKenzie
Share:

By now, we've all probably received an enticing email from a long-lost relative promising untold riches and wealth. In fact, there might be a few sitting in your spam box as you read this. That's because the game is up for phishers using lures like inheritance money.

These days, savvy phishers have buried the dead relative scheme in favor of urgent business messages or cybersecurity warnings. According to a recent ZDNet article, "The most common subject lines used in phishing emails targeting businesses show how cybercriminals are exploiting urgency, personalization and pressure in order to trick victims into clicking on malicious links, downloading malware or otherwise surrendering confidential or sensitive corporate information."

In other words, criminals create a false sense of urgency to trick your staff into clicking before they think. And this strategy works: 53% of organizations reported a phishing-related breach, more than any other cause. Fortunately, there are tactics you can take to empower your employees to resist phishing attempts. Teaching them how to spot the subject line of a phishing email is one of the most effective security awareness strategies you can share.

Let’s take a look at some of the top phishing email subject lines your employees need to recognize:

1. Password check required

This subject line is insidious because it taps into a commonplace occurrence in offices across the world: expired passwords. The average employee is juggling dozens of passwords, some of which have set expiration dates. So when an email pops up warning them that their password needs to be updated, it disguises itself as a friendly reminder. However, it’s anything but.

Clicking on the link will lead to a spoof site that harvests your employee’s log-in credentials. Just like that, the hacker has access to the account! And since 1 out of every 8 employees will accidentally share information on a phishing site, this poses an excellent training opportunity.

Keep an eye out for some common variations of this email subject line, including:

- Change of Password Required Immediately
- Office 365: Change Your Password Immediately
- Slack: Password Reset for Account

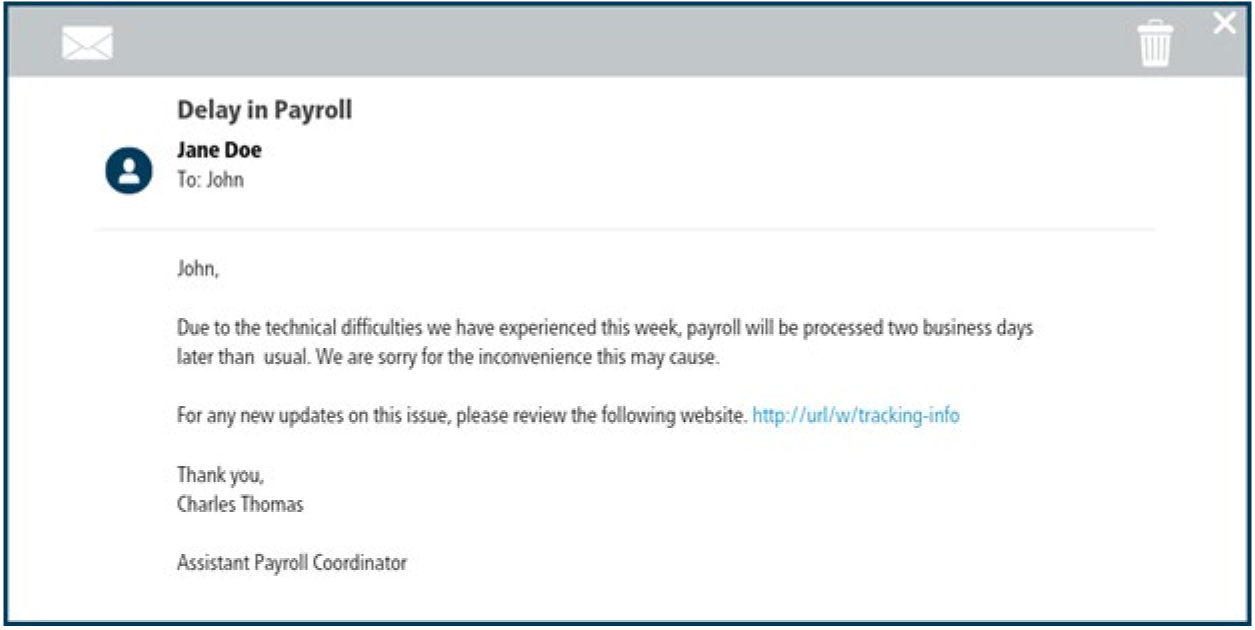
2. Billing information is out of date

Cybercriminals have been known to disguise themselves as third-party vendors to gain access to a company’s financial resources. One of these strategies involves sending an email that alleges an account’s billing information needs to be updated. An unsuspecting employee may follow the link to a spoof site and enter the billing information, therefore putting corporate credit card or bank account numbers directly into the hands of criminals.

(Source: Canadian Bankers Association)

3. Payroll has been delayed

Payroll departments should run like well-oiled machines, which is why a perceived payroll delay could have disheartened employees rushing to learn more about the situation. Their quest for an explanation will lead them to a phishing website that collects their credentials and leaves the actual payroll department none the wiser.



Delay in Payroll

Jane Doe

To: John

John,

Due to the technical difficulties we have experienced this week, payroll will be processed two business days later than usual. We are sorry for the inconvenience this may cause.

For any new updates on this issue, please review the following website. http://url/w/tracking-info

Thank you,
Charles Thomas

Assistant Payroll Coordinator

(Source: Center for Internet Security)

4. Your meeting attendees are waiting!

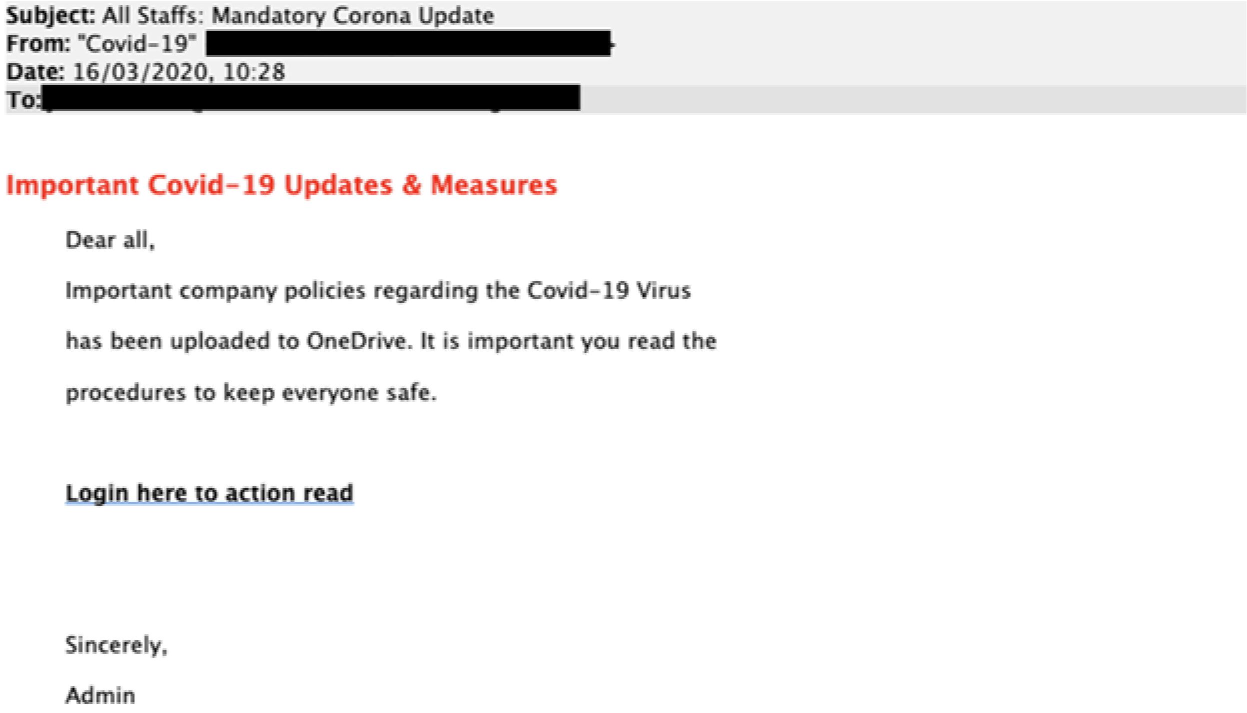
It’s human nature that we don’t like to keep people waiting. If you’ve ever been stuck in traffic minutes before a big meeting is about to begin, then you’re familiar with that sense of anxious dread.

Hackers have recreated that nightmare situation in your inbox. A subject line about meeting attendees will probably have you dashing to the link to the “meeting room,” only to get hit with a piece of malware. Watch Infosec’s Keatron Evans’ demo of how Zoom is being exploited for phishing attacks to see this attack in action.

How Zoom is being exploited for phishing attacks.

5. Office reopening schedule

Phishing emails may trick staff by disguising their contents as something important. After all, you're much less likely to scroll past an email if it sounds essential to your job. That's why it's increasingly common for scammers to use lofty-sounding subject lines. In the wake of COVID-19, this might include an office re-opening schedule or vaccination policy.



Subject: All Staffs: Mandatory Corona Update
From: "Covid-19" [redacted]
Date: 16/03/2020, 10:28
To: [redacted]

Important Covid-19 Updates & Measures

Dear all,

Important company policies regarding the Covid-19 Virus has been uploaded to OneDrive. It is important you read the procedures to keep everyone safe.

Login here to action read

Sincerely,
Admin

(Source: Risk Management Monitor)

6. Confidential information about COVID-19

Ooh, what is it? Secret vaccination info? A list of top-secret test sites? People like secrets — they make us feel exclusive and important. Plus, if the email promises to fill us in on something life-changing like COVID-19, we feel additional pressure to click on it.

If you haven't already, it may behoove you to issue a warning to your employees about COVID-19 phishing emails. They saw a 30,000 percent increase during 2020, and continue to be effective as new COVID strains stay in the news.

7. Updated vacation policy

Clever attackers may try to give their emails an air of legitimacy by disguising them as business communications from Human Resources. One of the most commonly clicked attacks is about updated employee policies regarding vacation time or other benefits.

Keep in mind that HR resources are often only accessible through an employee portal. That means hackers may try to snatch your employees' login credentials via a spoof site or portal.

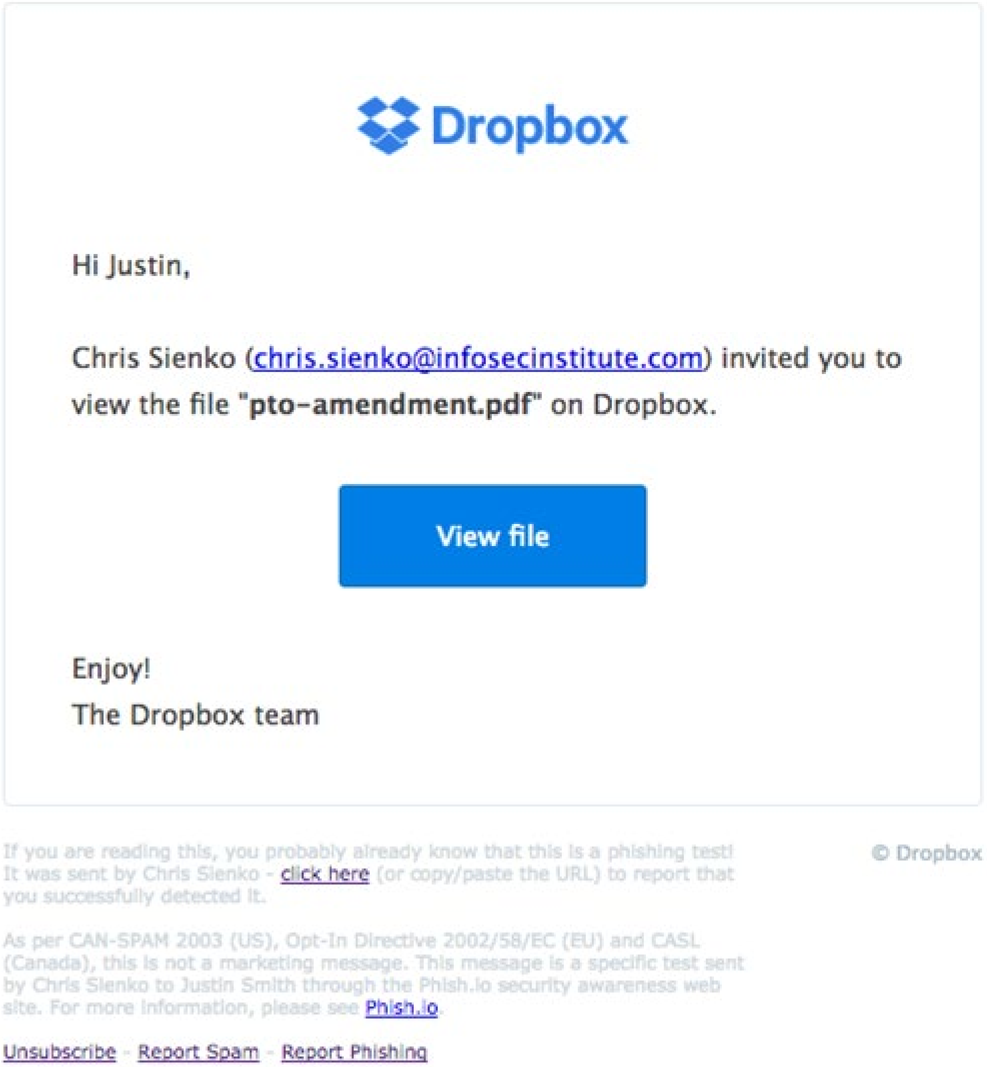
8. Employee raises

Any mention of salary is sure to grab your employees' attention, from annual raises to holiday bonuses and everything in between. One particular scam appears to come from the company HR department regarding a raise. Linked or attached is a spreadsheet claiming to detail the employee's wage increase. Unfortunately, the link leads to a spoof login page that harvests the employee's credentials. The only one walking away with a raise is the scammer!

This attack has been in the headlines recently. The website hosting company GoDaddy found itself the recipient of unwanted news coverage when it sent a fake phishing email to its employees, saying that they'd received a $600 Christmas bonus (which did not exist). The exercise raised many questions about the ethical considerations of leading one's employees with such baldly emotional material to test their security awareness.

9. Dropbox / Google / SharePoint: Document shared with you

Many companies use collaborative tools like Dropbox, Google Drive and SharePoint so that colleagues can share media like documents and images in real-time. Unfortunately, file attachments are a common vector for malware. And of users who receive infected attachments, 12% will click on them. Hackers will attempt to spread infected files by spoofing a Dropbox, Google or SharePoint email and tricking their victims into downloading the document. Often these emails appear to come from a know associate or co-worker.



Dropbox

Hi Justin,

Chris Sienko (chris.sienko@infosecinstitute.com) invited you to view the file "**pto-amendment.pdf**" on Dropbox.

View file

Enjoy!
The Dropbox team

If you are reading this, you probably already know that this is a phishing test! It was sent by Chris Sienko - click here (or copy/paste the URL) to report that you successfully detected it.

© Dropbox

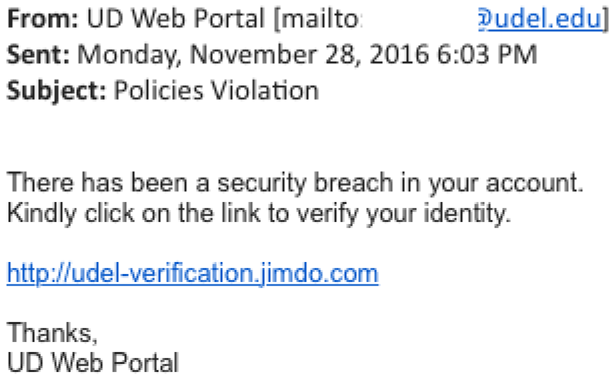
As per CAN-SPAM 2003 (US), Opt-In Directive 2002/58/EC (EU) and CASL (Canada), this is not a marketing message. This message is a specific test sent by Chris Sienko to Justin Smith through the Phish.io security awareness web site. For more information, please see Phish.io.

Unsubscribe - Report Spam - Report Phishing

(Source: Infosec Resources)

10. Attention: unusual account activity detected!

ALERT! DANGER! ACT IMMEDIATELY! That’s what this subject line screams, and it will have your employees scrambling to open the email for more details. Once they arrive at the destination, they’ll be asked to enter their credentials and the real security breach will begin.



From: UD Web Portal [mailto @udel.edu]
Sent: Monday, November 28, 2016 6:03 PM
Subject: Policies Violation

There has been a security breach in your account.
Kindly click on the link to verify your identity.

http://udel-verification.jimdo.com

Thanks,
UD Web Portal

(Source: University of Delaware)

11. Earn money working from home

In today’s gig economy, many people like to balance lucrative side hustles with their main line of work. Hackers like to prey on this by pitching fake work-from-home jobs and freelance gigs. Depending on how elaborate the scheme is, these hackers could steal anything from sensitive personal information (like Social Security numbers and bank accounts) to actual money by claiming it covers onboarding supplies like laptops and tablets.