Spam, Phishing, and You.

Last updated January 17th 2023

There is likely no one who is unfamiliar with the unwanted emails and messages that we receive in our inboxes day in and day out. You're also likely familiar with attempts to educate users on how to avoid and detect fraudulent and possibly malicious messages. We have specific training that the university requires us take from time to time to help cut down the amount of users who fall victim to some of these events. Regardless of our attempts to educate users and avoid the potential consequences of falling victim to the various types of attacks we are subjected to, there are still many people who are understandably caught unaware.

Not only are the types of attacks increasing, but their sophistication is also getting advanced where it can be hard for even professionals to tell if emails and messages are legitimate. I wanted to take a quick look at some of the easy yet potentially malicious emails and messages that are out there, try to identify the ones that are harder to spot, as well as go over some tips to avoid and curtail the amount of messages that we receive.

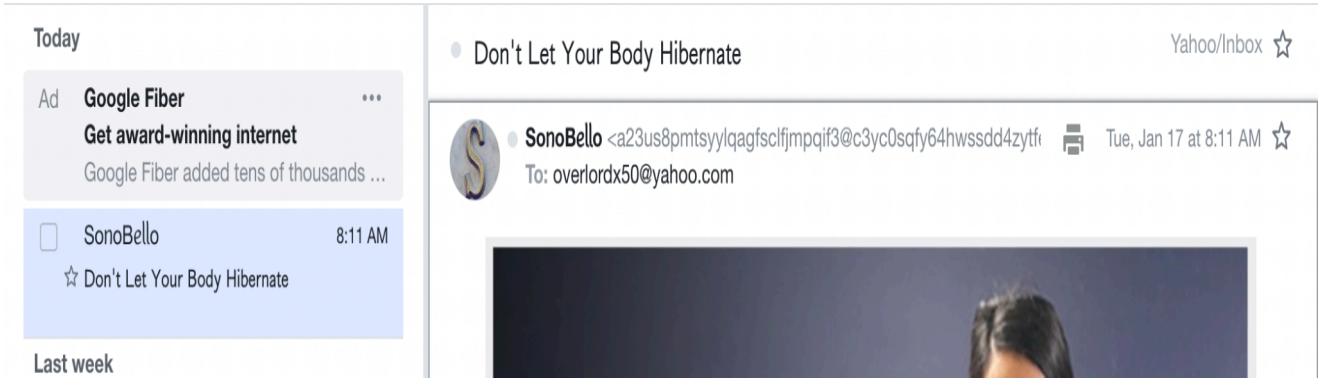
In this episode we'll be looking at Spam, and Phishing emails.

If you want to skip all my witty commentary, feel free to scroll to the bottom of the document for the TL;DR

If you're lucky, you're familiar with the salty and savory goodness that is canned meat product. I like mine fried, with a little brown sugar, throw a slice of processed cheese product on top and I've got a meal. No one likes spam email. It's annoying, clutters up your inbox, and is unfortunately one of life's little frustrations and the cost of our interconnected world. Spam messages in and of themselves are not malicious, but the difference between spam and a phishing email can be very slight. Spam emails are mainly just attempts to sell you something, or steer you to content that wants to sell you something, while phishing is an attempt to get information out of you that can be used to further access and maliciously control your accounts.

Let’s take a look at some examples… these are from a personal email account.

SPAM EMAIL

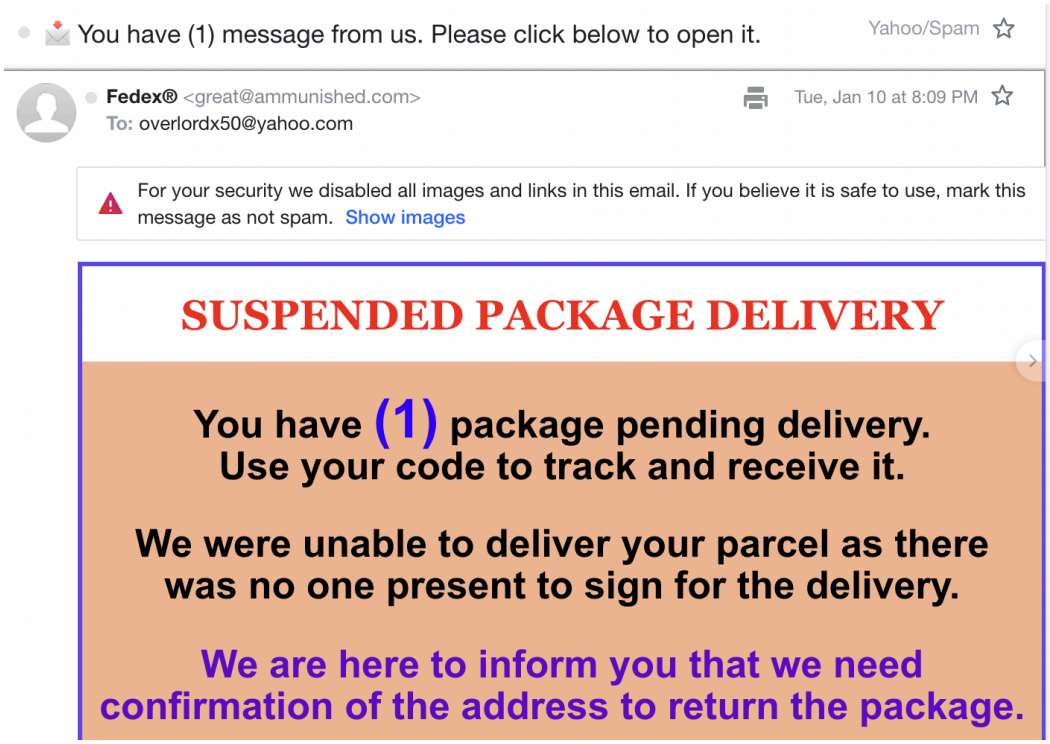


1. Notice the email header, the subject is in different fonts, different sizes, etc, all meant to draw attention to the email. SonoBello is a legit company (I think), so this is at best an affiliate attempt to get you to SonoBello’s website.
2. The email address is gibberish. **THIS IS SOMETHING TO TAKE NOTE OF ACROSS THE BOARD. Legitimate emails do not come from gibberish email addresses. If there is EVER a question if something is legit or not, step one, look at the email address it comes from.**
    - **This is not an absolute, attackers have the ability to make it look like the email comes from a legitimate source. This is called spoofing.**
3. My body is just fine. It enjoys its hibernation, thank you. But someone out there is wanting to lose weight, look better, have more stuff, etc. They are trying to get your money one way or another. I guess that’s just society.

PHISHING EMAILS

Remember phishing emails are attempting to get information from you including account names, passwords, personal information etc. If I followed the link below, it would prompt me to enter information to get the correct address this package can be sent to. That would be appropriate right? If the address is incorrect, it needs to be fixed, right?

*You may think what’s the harm in someone having my information? That’s just one more piece of the puzzle that an attacker has that they can use against you. If someone has your name and birthday, they’re already on their way to being able to open up a credit card in your name, as an example. If they were to get your address, phone number, social security number, they’ve got your identity.



There is a lot going on here, so let's break this down.

1. Vague email subject meant to pique your interest. If you saw this on your phone or mobile device you might just click it out of habit.
2. I'm not expecting a package. I know with the holidays it's easy to lose track of what's coming and going, but that's why these types of messages exist. Knowing your business and what's coming and going is an excellent habit to be in. They're trying to catch people off guard and unaware.
3. It says FedEx, but again, look at the address. Nothing to do with FedEx other than the title.

Let's look at something similar, but not an email. This is a message I received on my phone. This time they're trying to get my AppleID. If they have the account ID they can work on getting the password. If they get the password they have access to the account, and potentially they can start working on whatever means of payment I have attached to the account.

To: information-logappieaccount15_-update-ll561-8111@webspage-official05.co.za

Text Message
Sunday 4:22 AM

Your Apple ID has been locked.
We have locked your Apple ID because our service has detected two unauthorized devices.

To unlock your account, you required verify your Apple ID .
Click the link below to unlock your Apple ID.
http://s948022464.onlinehome.us/

Your account will be automatically unlock, after finishing the verification.

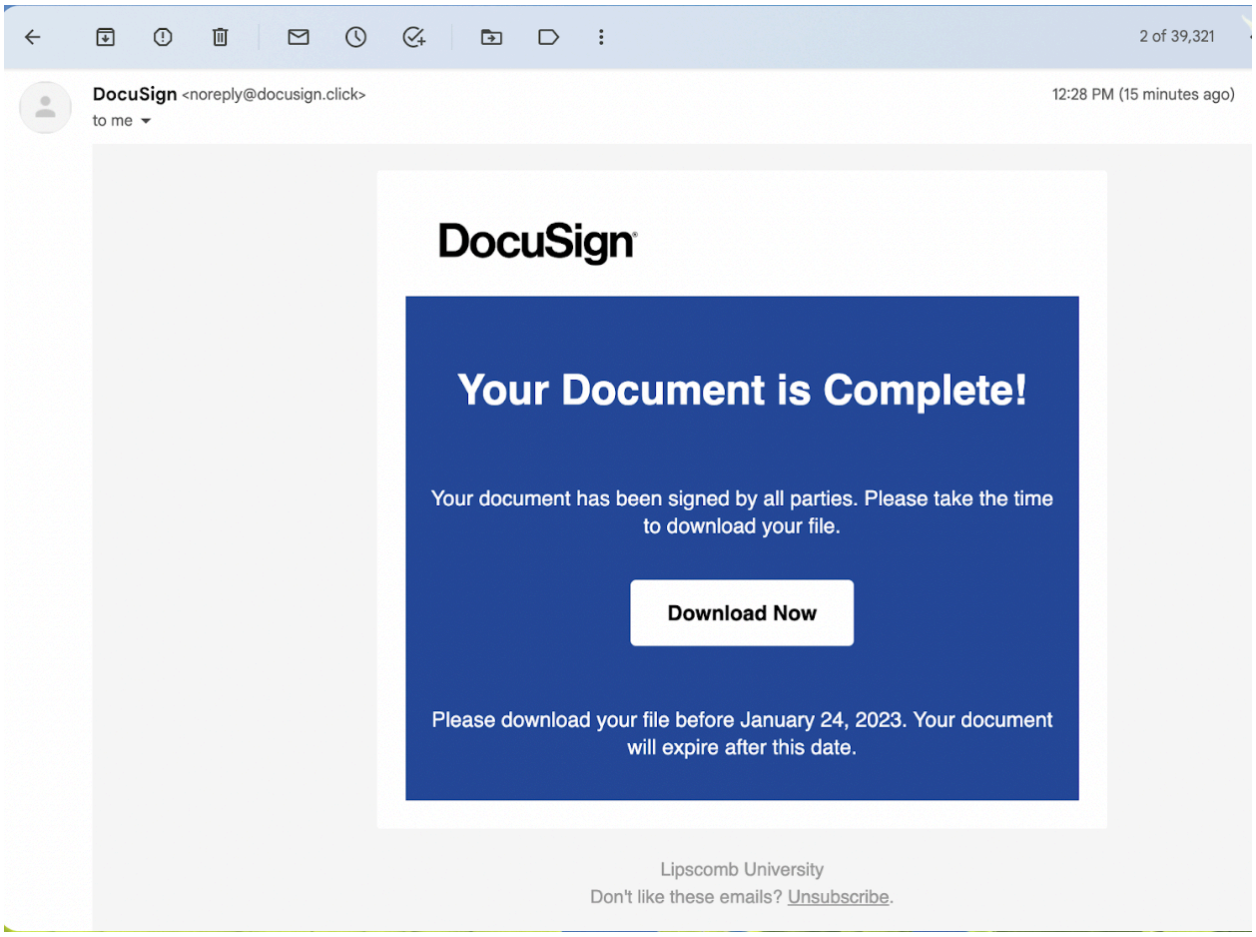
Copyright © 2023 Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Irlande.
All rights reserved.

1. Again, when my phone buzzes I look and see your account has been locked. Uh oh. I click on it immediately. Look at what time it was sent - most people are asleep at 4am. If I roll over and see that on my phone at 4am I'm likely to just click it without thinking and follow what it says.
2. Look at who it's from. Gibberish, with a vague attempt to throw the word 'apple' in there. Look at the domain name after the @, nothing about apple.
3. The link in the message has nothing to do with apple. It directs to an attack site which will record my account information and relay it to the attacker.
4. General bad spelling and grammar. This is something that signifies it's not legitimate. There is no professional company in the world that would send out a message formatted like this. The trick is that the attackers know that, it's not just a mistake. Users who don't know the difference are more likely to not catch the mistakes, so they're easier to attack.

TL;DR (too long; didn't read)
These are just some quick examples of emails and messages that are crafted and sent out in bulk. They are relatively easy to spot and avoid, as they aren't meant to be well thought out and tailored. They are meant to hit as many people as they can and catch a couple. Being vigilant is 99% of avoiding getting caught by these types of communications. Know your business, know your accounts, know that someone is always trying to get something from you. If someone was to ask me what's the number one way to keep yourself safe online, that would be my response. Vigilance. God gave us the ability to sense when something is wrong with the proverbial 'gut feeling'. Trust your gut, if something doesn't seem right there is a good chance it's not. Randy Savage says OH YEAH BROTHER, Vigilance for the WIN

(He approves this message)

*We've had this email come through the past few days, and I wanted to make a special note of it.



This is the type of email I mean that is rather sophisticated. If you look at this email, I don't see anything initially wrong… BUT… my gut… it tells me something doesn't look right.

Look at the email subject, nothing crazy. Look at the body of the email… nothing crazy. Look at the sender's domain - docusign.click… hmmm. Ideally it would be docusign.com, or something like that. Suspicious item #1.

The email is extraordinarily vague… it doesn't say who it's addressed to, just a generic hey, your document is ready. More than that, notice where it says download your file by tomorrow, or it's going to be gone. This represents an attacker trying to build a sense of urgency where you are likely to mistake something malicious as genuine. Suspicious item #2.

When I saw this email I wasn't 100% sure it was malicious, but I have since been told that it is. My initial advice was to disregard it just to be on the safe side. There is not a thing in the world wrong with deleting something you think might not be legit, or that you have a questionable feeling about.

This is where vigilance comes into play. The person who sent me this said "I use docusign, but I shouldn't have anything I'm expecting." That's a major part of spotting this as potentially malicious. For those of you who have tons and tons of documents every day that get signed, I understand completely you can't be aware of every single thing that's outstanding. But knowing your business, being cognizant of what is

coming and going, and more than anything, just being vigilant and aware of things, goes a long way in prevention. Remember what Randy says.