C14: Phish Detection Agency

Saturday, December 23, 2023 4:54 PM

Difficulty: Level 2
Fitzy Shortstack on Film Noir Island needs help battling dastardly phishers. Help sort the good from the bad!

CONVERSATION w/ Elf Fitzy Shortstack	**Fitzy Shortstack (The Blacklight District)** Just my luck, I thought... A cybersecurity incident right in the middle of this stakeout. Seems we have a flood of unusual emails coming in through ChatNPT. Got a nagging suspicion it isn't catching all the fishy ones. You're our phishing specialist right? Could use your expertise in looking through the output of ChatNPT. Not suggesting a full-blown forensic analysis, just mark the ones screaming digital fraud. We're looking at all this raw data, but sometimes, it takes a keen human eye to separate the chaff, doesn't it? I need to get more powdered sugar for my donuts, so do ping me when you have something concrete on this. ** ------- Response after completing challenge ------- ** You've cracked the case! Once again, you've proven yourself to be an invaluable asset in our fight against these digital foes. From <https://2023.holidayhackchallenge.com/badge?section=conversation&id=fitzyshortstack>
HINTS	**DMARC, DKIM, and SPF, oh my!** *From: Fitzy Shortstack* *Terminal: Phish Detection* Discover the essentials of email security with DMARC, DKIM, and SPF at Cloudflare's Guide. From <https://2023.holidayhackchallenge.com/badge?section=hint&id=hintPhishing>

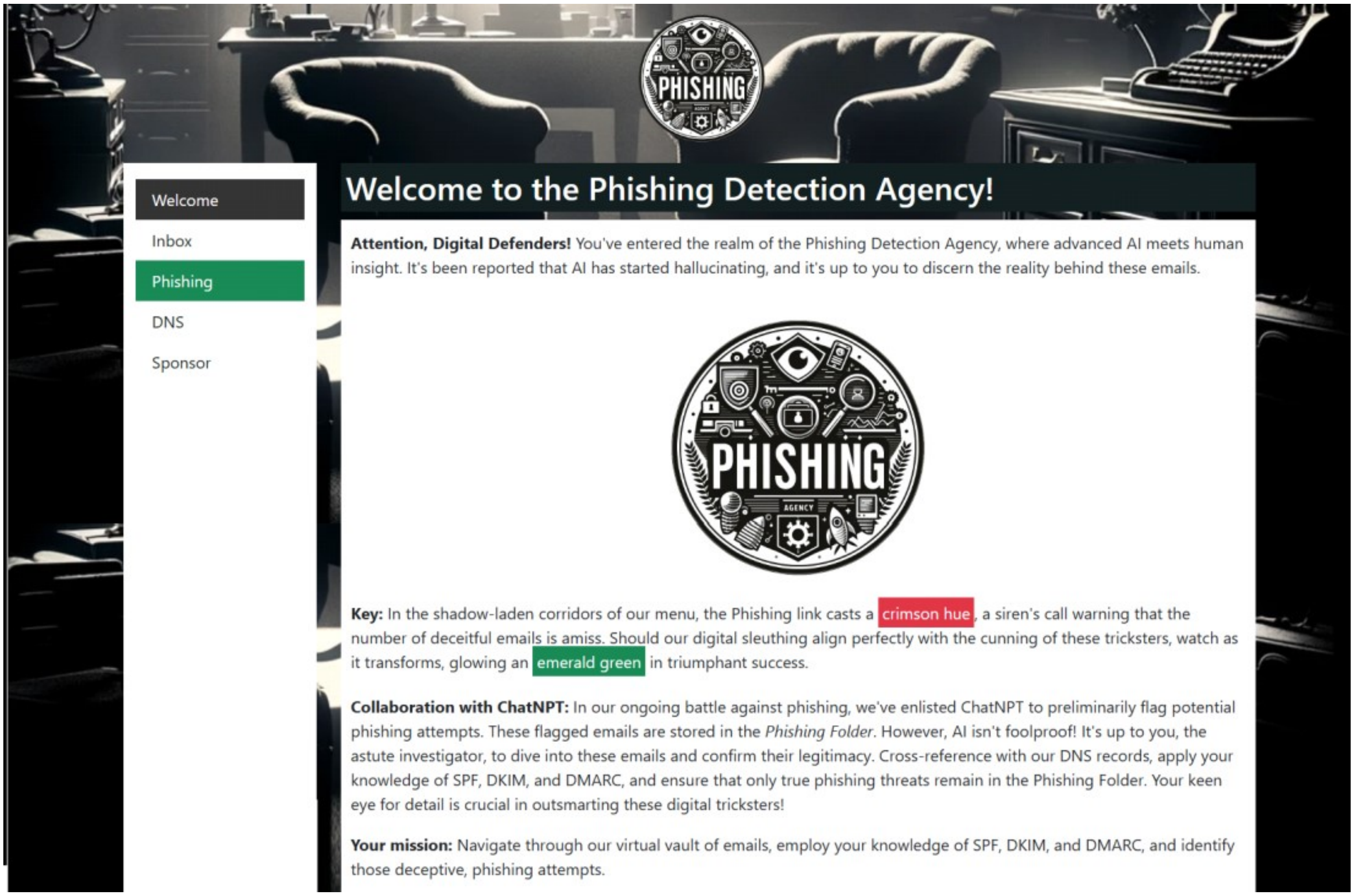
Attention, Digital Defenders! *You've entered the realm of the Phishing Detection Agency, where advanced AI meets human insight. It's been reported that AI has started hallucinating, and it's up to you to discern the reality behind these emails.*

Key: *In the shadow-laden corridors of our menu, the Phishing link casts a crimson hue, a siren's call warning that the number of deceitful emails is amiss. Should our digital sleuthing align perfectly with the cunning of these tricksters, watch as it transforms, glowing an emerald green in triumphant success.*

Collaboration with ChatNPT: *In our ongoing battle against phishing, we've enlisted ChatNPT to preliminarily flag potential phishing attempts. These flagged emails are stored in the Phishing Folder. However, AI isn't foolproof! It's up to you, the astute investigator, to dive into these emails and confirm their legitimacy. Cross-reference with our DNS records, apply your knowledge of SPF, DKIM, and DMARC, and ensure that only true phishing threats remain in the Phishing Folder. Your keen eye for detail is crucial in outsmarting these digital tricksters!*

Your mission: *Navigate through our virtual vault of emails, employ your knowledge of SPF, DKIM, and DMARC, and identify those deceptive, phishing attempts.*

From <https://hhc23-phishdetect-dot-holidayhack2023.ue.r.appspot.com/?&challenge=phishdetect&username=LadyCee&id=031e875c-c68e-4aff-9eec-f598c2d76a69&area=fni-theblacklightdistrict&location=43,13
&tokens=&dna=ATATATTAATATATATATATTAATATATATATGCATTATAATATATATATATTAATATATATATATATGCATATATATCGATATATATATATATTAATATATATATATGCAT ATATATTA>



Welcome to the Phishing Detection Agency!

Attention, Digital Defenders! You've entered the realm of the Phishing Detection Agency, where advanced AI meets human insight. It's been reported that AI has started hallucinating, and it's up to you to discern the reality behind these emails.

Key: In the shadow-laden corridors of our menu, the Phishing link casts a crimson hue, a siren's call warning that the number of deceitful emails is amiss. Should our digital sleuthing align perfectly with the cunning of these tricksters, watch as it transforms, glowing an emerald green in triumphant success.

Collaboration with ChatNPT: In our ongoing battle against phishing, we've enlisted ChatNPT to preliminarily flag potential phishing attempts. These flagged emails are stored in the *Phishing Folder*. However, AI isn't foolproof! It's up to you, the astute investigator, to dive into these emails and confirm their legitimacy. Cross-reference with our DNS records, apply your knowledge of SPF, DKIM, and DMARC, and ensure that only true phishing threats remain in the Phishing Folder. Your keen eye for detail is crucial in outsmarting these digital tricksters!

Your mission: Navigate through our virtual vault of emails, employ your knowledge of SPF, DKIM, and DMARC, and identify those deceptive, phishing attempts.

MY WORK AND ANSWER

I was rightly confident I could quickly identify the phish in this challenge without having to hack the challenge. After reading Cloudflare's Guide, I reviewed each of the 34 email messages, looking for mismatches in the address, for missing DKIM signatures, or DMARC failures. I started with the list of phishing to identify any false-positives. Then I looked at the rest to see if any should be flagged as phishing. I was successful on my first submission. This was a much needed confidence boost as I was working several challenges simultaneously.

The report shows a list of 34 emails where 10 have been identified as phishing. The remaining 24 were deemed safe.	Hint from Cloudfare DMARC, DKIM, and SPF are three email authentication methods. Together, they help prevent spammers, phishers, and other unauthorized parties from sending emails on behalf of a domain* they do not own. DKIM and SPF can be compared to a business license or a doctor's medical degree displayed on the wall of an office — they help demonstrate legitimacy. Meanwhile, DMARC tells mail servers what to do when DKIM or SPF fail, whether that is marking the failing emails as "spam," delivering the emails anyway, or dropping the emails altogether. Domains that have not set up SPF, DKIM, and DMARC correctly may find that their emails get quarantined as spam, or are not delivered to their recipients. They are also in danger of having spammers impersonate them. From <https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/>
My approach: 1. Reviewed those emails flagged as phishing for any false-positives 2. Reviewed the safe email for any false-negatives (missed phishing	Inbox From <https://hhc23-phishdetect-dot-holidayhack2023.ue.r.appspot.com/inbox> 34 emails 21 showing safe

attempts).	Success!

Success!

Congratulations, Ace Detective! You've successfully navigated the treacherous waters of deception and emerged victorious. Your sharp wits and keen eye for detail have cracked the case wide open, proving that even the most cunning phishing attempts are no match for your discerning mind.

In a world where shadows often obscure the truth, you shone a bright light on duplicity. Your unwavering commitment to truth and justice in the digital realm has kept our virtual streets safe. Thanks to your efforts, the Phishing Detection Agency stands strong, a bulwark against the tide of digital deceit.

Remember, the battle against phishing is ongoing, but with sleuths like you on the case, the internet remains a safer place. You're not just a hero; you're a guardian of the digital frontier. So here's to you, *the quintessential cyber sleuth*, a beacon of hope in these pixelated alleyways of misinformation.

Your achievement is not just a personal victory; it's a triumph for all of us in the agency.

From <https://hhc23-phishdetect-dot-holidayhack2023.ue.r.appspot.com/check/34>

A word from our sponsor...

This winter, let the Geese Islands star in your sunlit film noir; where the only thing dramatic is the sunset.

From <https://hhc23-phishdetect-dot-holidayhack2023.ue.r.appspot.com/ads>

Comments of Interest from other Players

No, it should trigger automatically when the right ones are in the phishing folder. There will be some that need to be removed from the folder and some that need to be added to the folder. I did experience a similar issue and it fixed itself when I tried it in another browser. If you try a different browser and it still doesn't work, let me know.

You need to be looking at ALL the headers, the pass or fail relates to the information in the other headers. DMARC pass/fail is not telling you if it's phishing or not, it's telling you some information that will help you understand what headers are validated and help you make a decision based on the headers and the DMARC status.

so to not be a phish, something has to pass SPF and DMARC and DKIM
to be a phish it can fail SPF OR DMARC OR DKIM

The navigation function seems to be buggy. Here is a poc. 1. Click the phishing folder. 2 search Emily and verify not found. 3. Hit next and click on the last item from Teresa.
- Click the previous button and you will see Emily's email instead of Xaviers.