Competitive Cyber Security Organization
AT PENN STATE

CARE Lab Social Engineering Competition

Day Two Deliverables

Authors:
Liam Geyer (lfg5289@psu.edu)
Jenna Fox (jef5600@psu.edu)
Brendan McShane (bbm5360@psu.edu)
Jonathan Skeete (jxs7245@psu.edu)

April 20, 2024

Table of Contents

1 Executive Summary

The CARE Lab Fraud Fighters Team continued efforts to assist Sam with her hiring process and determining the legitimacy of her offer. During the second day of the engagement, the team met with Sam to provide guidance throughout a text-based job interview conducted on Microsoft Teams. There were a number of red flags encountered during the interview as well as discrepancies between the information provided within the interview and the initial email. The most notable of these discrepancies was that Mr. David W. Bondeson did not conduct the interview as previously mentioned and that the company Omnicell, Inc was used interchangeably with HealthComp, LLC despite no relation.

Afterwards, the team sat in on a follow up text based meeting with Sam during which she received a job offer email from the prospective employer/scammer. This email contained several red flags potentially indicating it as a phishing email. As part of the on boarding process Sam was asked to fill out a job application form, W4, and provide a passport photo.

The team has compiled a comprehensive report detailing OSINT findings, potential red flags, a comprehensive timeline with MITRE ATT&CK Mappings, NIST Phish Scale evaluations of Sam's emails, as well as a to-do list and game plan for Sam moving forward. The compiled evidence indicates that this employment opportunity is extremely likely to be a scam; the team has prepared a comprehensive brief to communicate the red flags, and risks of moving forward to Sam.

2 OSINT Findings

2.1 BBB Scam Report

The team found a report submitted to the Better Business Bureau which fits the exact description of Sam's interactions with the prospective employer.

> *"I was sent an email about a potential job offer for HealthComp I then got instructions to conduct an interview on Microsoft Team then they so called hired me and had me fill out paper work including a W4 form that had my ssn number then after that I told them I had finished filling out the paper work and then they started asking if I was going to be using a credit card to accept my payments and I said no then they said I need one so they can process faster then that's when I realized it was a scam"*
>
> *— BBB Scam ID #772647 (Better Business Bureau, 2023)*

The BBB Scam Report lists the same davidbondeson@healthcomp.live email address referenced in Sam's interview offer. With this in mind, it's extremely likely that Sam's job opportunity is not legitimate.

2.2 Employer Information

- HealthComp signed a merger with Virgin Pulse to create Personify Health. Omnicell is not affiliated with HealthComp or Personify Health whatsoever.
- All positions offered to Sam are not posted on Personify Health's or Omnicell's internal job board (See Figure 1).

2.3 Interviewer Information

- As of Nov. 2023, Mr. Manley has left Omnicell, Inc. He is now employed as a Senior Enterprise Account Executive at Docusign, Inc. (See Figure 2).
- Mr. Manley's LinkedIn profile indicates that he received a Bachelor of Science in Business Administration from the University of Central Florida (See Figure 3).
- During his time at Omnicell, Mr. Manley was a Medical Account Executive.
- David W. Bondeson is not an Interview Manager but the Director of Stop Loss Sales (See Figure 4).

2.4 Domain Information

- Mr. David W. Bondeson should uses a healthcomp.com domain instead of healthcomp.live (See Figure 5).
- The healtcomp.live domain was registered in 2023, whereas the healthcomp.com domain was registered in 2001 (See Figure 6).

2.5 OSINT Evidence

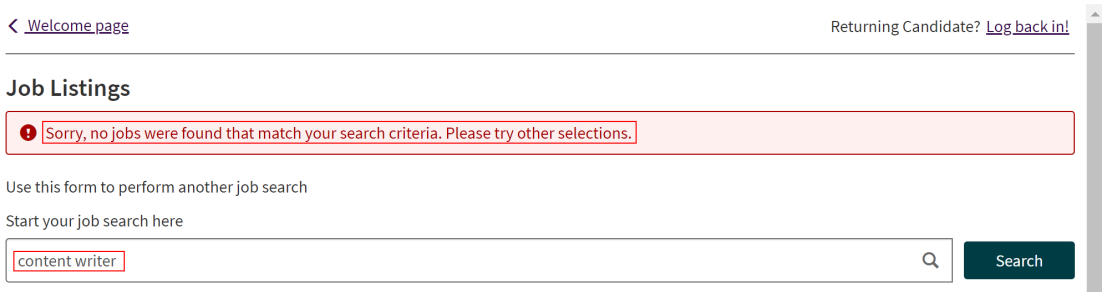


Figure 1: The job listings for Healthcomp do not have the offered position of content writer available.

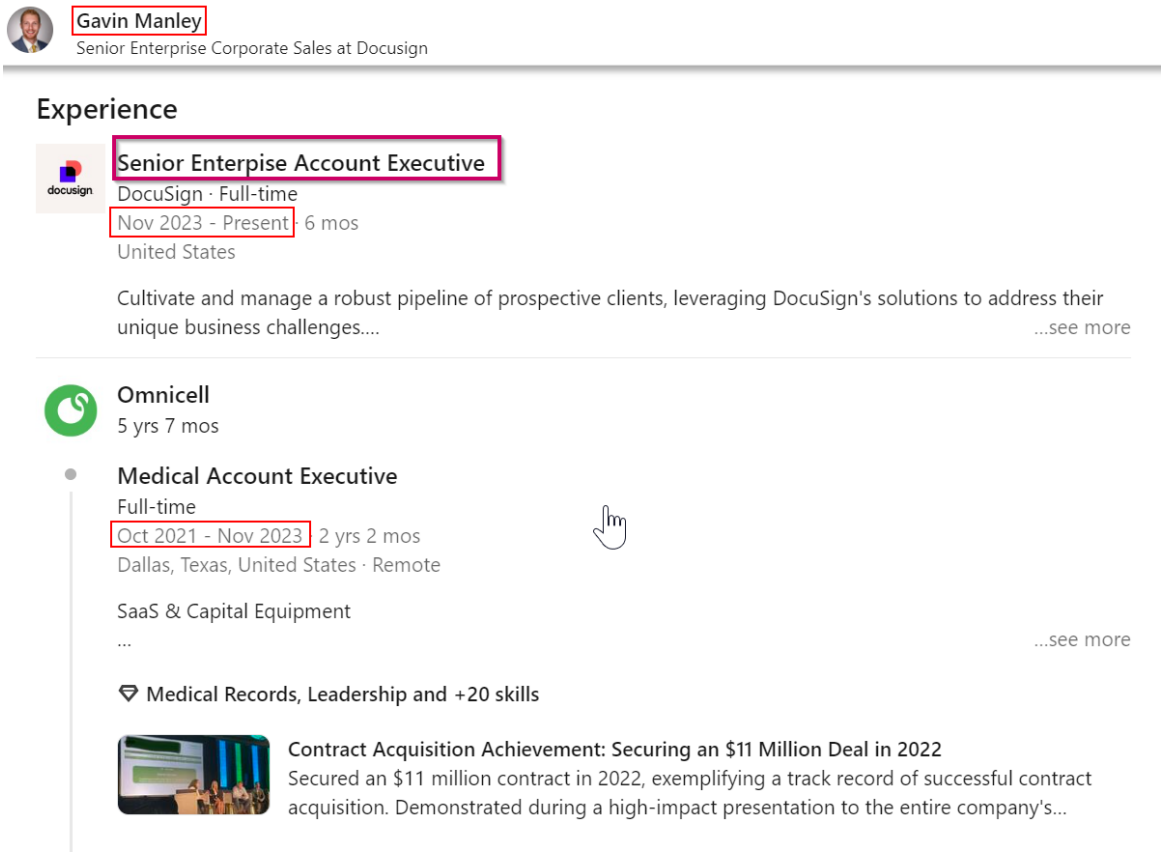


Figure 2: Gavin Manley's LinkedIn profile showing his employment at Omnicell, Inc ended in November 2023 due to his transition to DocuSign as a Senior Enterprise Account Executive.

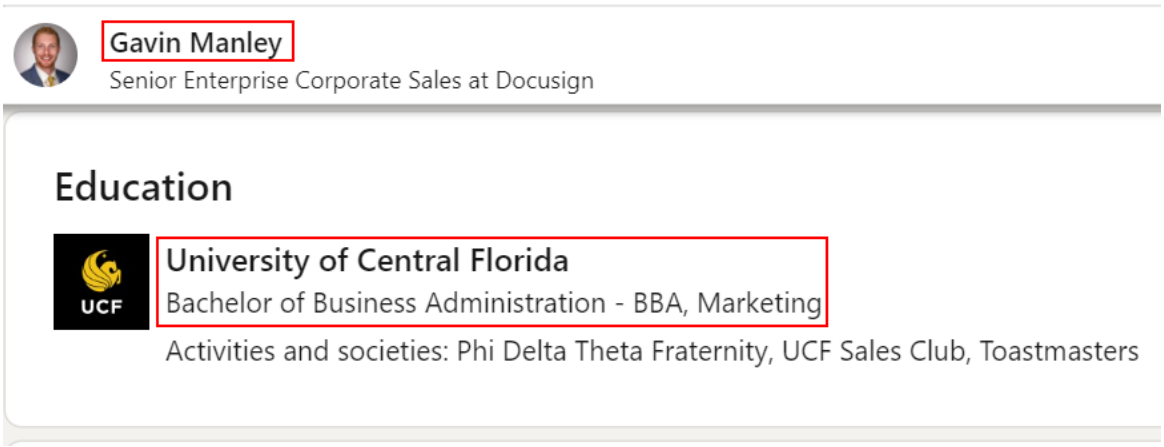


Figure 3: Gavin Manley's LinkedIn profile showing he graduated from the University of Central Florida.

Figure 4: David W. Bondeson is listed as Director of Stop Loss Sales at Personify Health.

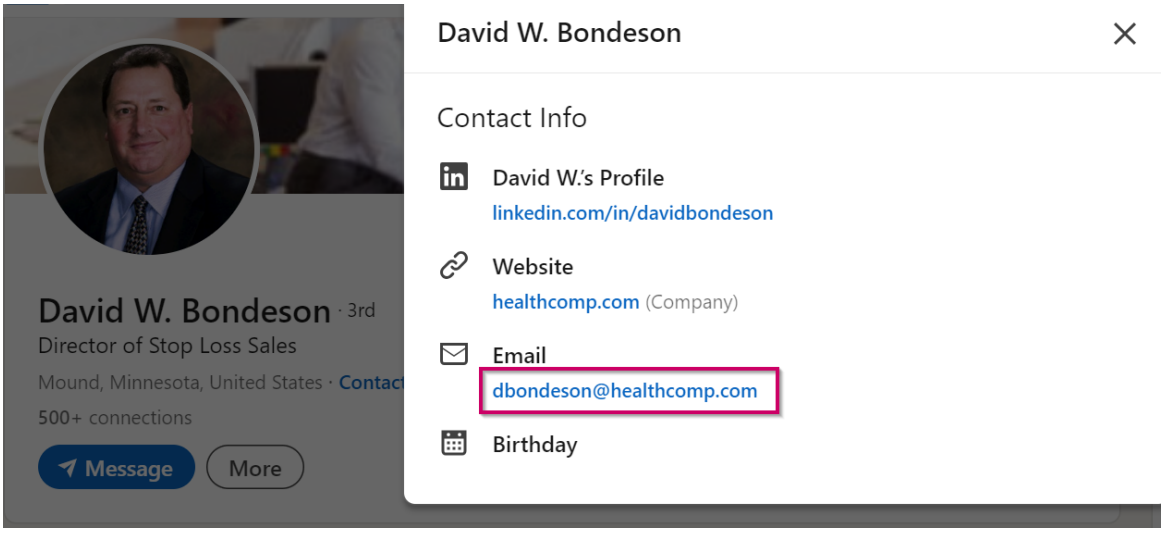
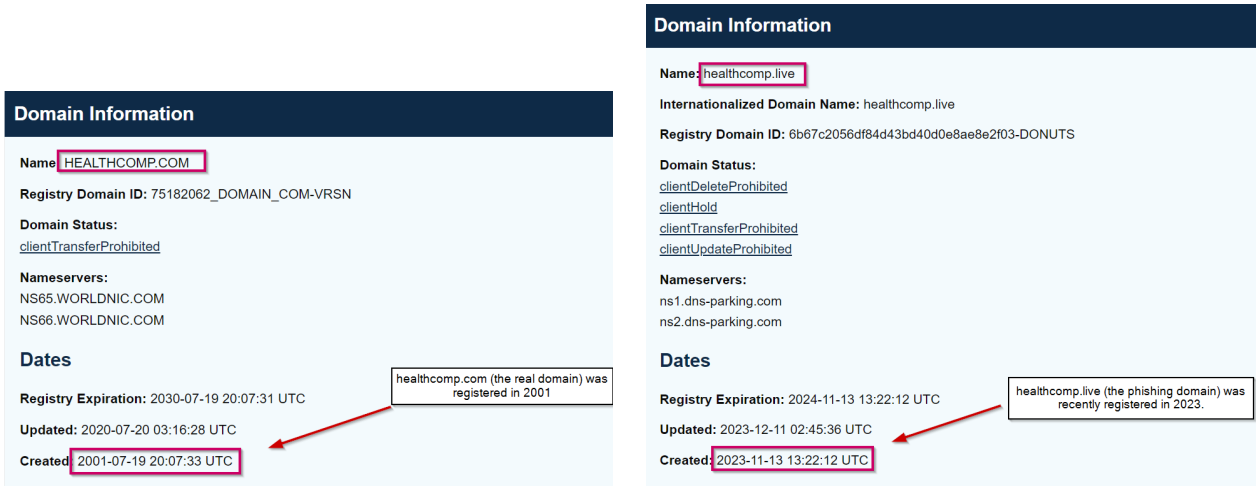


Figure 5: David W. Bondeson's contact information on LinkedIn.



(a) healthcomp.com Domain Registration (2001)

(b) healthcomp.live Domain Registration (2023)

Figure 6: Two different domains for the same company

3 Red Flags

1. **Potential AI Chat-bot**
   - The interviewer, who is claiming to be human, is responding in a time frame that is unrealistic to expect from a real person.
   - When texting Sam was asked for certain keywords which would serve as a prompt for the chat-bot to generate text tailored to their current conversation (See Figure 7).
2. **Inconsistent Information**
   - Neither Mr. Bondeson, Mr. Manly, or Ms. McDaniel ever refer to HealthComp by it's new name, Personify Health.
   - The original interview offer Sam received was from HealthComp, LLC. Upon entering the interview, it was revealed that she was actually interviewing for a company called Omnicell (See Figure 8). After reviewing public records, the team concluded that Omnicell is not affiliated with HealthComp or Personify Health whatsoever.
   - In the beginning of the interview, Mr. Manley introduces himself to be from Omincell, Inc., but later switches to HealthComp, LLC. (See Figure 9).
   - The job offer letter Sam received was for HealthComp, which was consistent with the initial email, but not with the text based interview.
3. **Point of Contact Discrepancies**
   - As stated in the email sent from HealthComp, LLC, the point of contact for this interview was supposed to be Mr. David W. Bondeson; however, the interviewer introduces himself as Mr. Gavin Manley from Omnicell, Inc. despite having the contact name "david donbenson" in Teams (See Figure 10).

- In the interview, Mr. Manley Introduces himself to be from Omnicell, Inc., but according to his Linkedin profile, he's currently employed at Docusign as a Senior Enterpise Account Executive (See Figure 2).
- When introducing himself, Mr. Manley states that he received his Bachelor of Science in Electrical Engineering from the Swiss University of Applied Science, Winterthur (See Figure 11). This information is inconsistent with Mr. Manley's LinkedIn profile indicates that he received a Bachelor of Science in Business Administration from the University of Central Florida (See Figure 3).
- During his time at Omnicell, Mr. Manley was a Medical Account Executive and not on the board of directors as he claims in the interview (See Figure 2).
- Mr. Bondeson's title at HealthComp, LLC. is Director of Stop Loss sales and not Interview Manager (See Figure 4).
- Kellie McDaniel is not listed as a HealthComp employee
- Email requests all communication be sent through a @healthcomp.live domain instead of the official @healthcomp.com domain listed on their Linkedin and website (See Figure 5).

4. **Professionalism**

- Numerous grammar (See Figures 12-13), spelling (See Figure 14), and convention errors (See Figure 15).
- Does not address recipient of email in interview offer letter and instead refers to Sam as Candidate and uses a verification code to track her application (See Figure 16).
- Email signed by HealthComp instead of the sender or an HR Representative (See Figure 16).
- Lack of branding on throughout all contact, most companies will usually include a header, footer, and logo in their emails.
- The contact name on the Microsoft Teams chat reads, "david donbenson" and not "David Bondeson," lacking proper capitalization and spelling of the last name provided in the original email (See Figure 17).

5. **Lure**

- Offer letter states Sam will have to purchase her own office equipment from a supplied vendor and will be reimbursed, which is a common scam acknowledged by the Federal Trade Commission. The vendor could be one the scammers created themselves to have payment redirected towards them, and you wont receive the products ordered
- Employer requests a photo of Sam, which could be used for identity theft

3.0.1 Red Flag Evidence

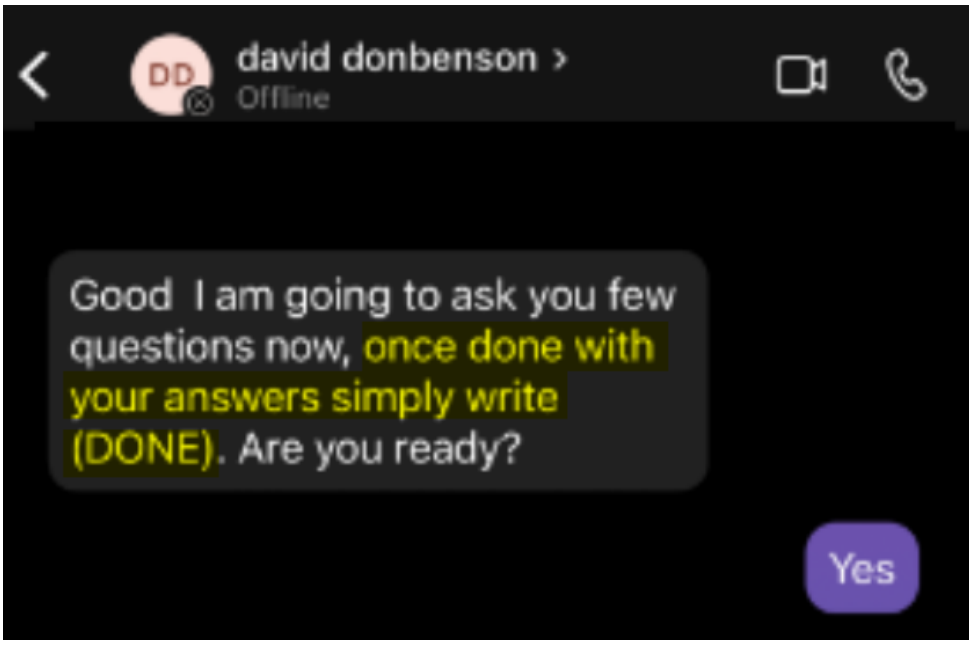
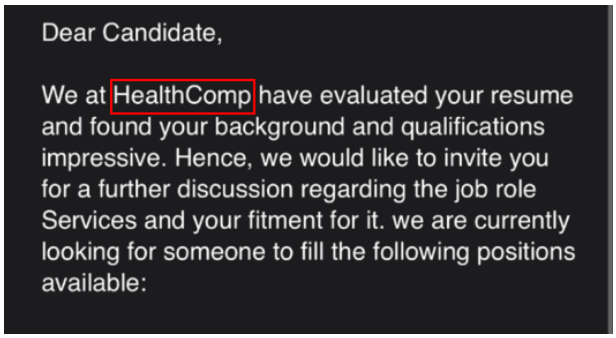
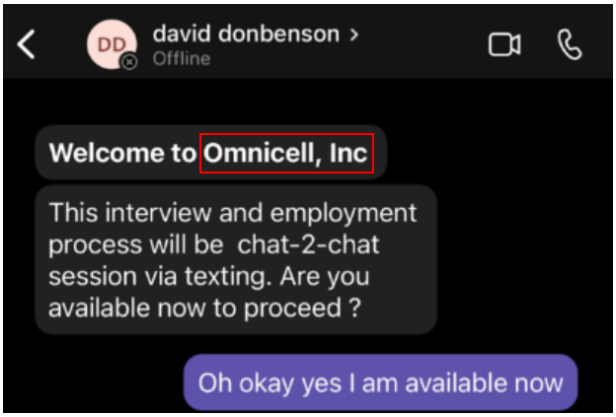


Figure 7: The interviewer asked Sam to reply with "DONE" or other cue words at several points.

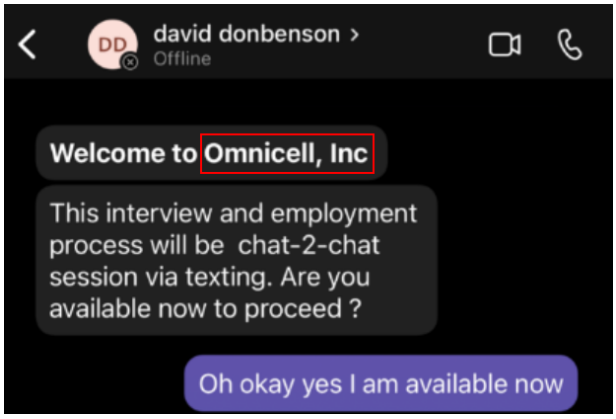


(a) Initial Email from HealthComp, LLC.

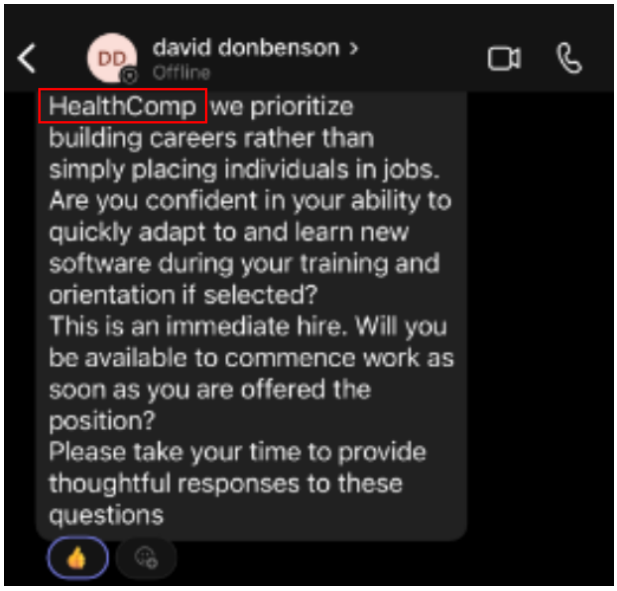


(b) Interview introduction as Omnicell, Inc.

Figure 8: Discrepancy in the company offering the job.



(a) Interview introduction as Omnicell, Inc.



(b) HealthComp used later in the interview.

Figure 9: The interviewer switches between HealthComp and Omnicell.

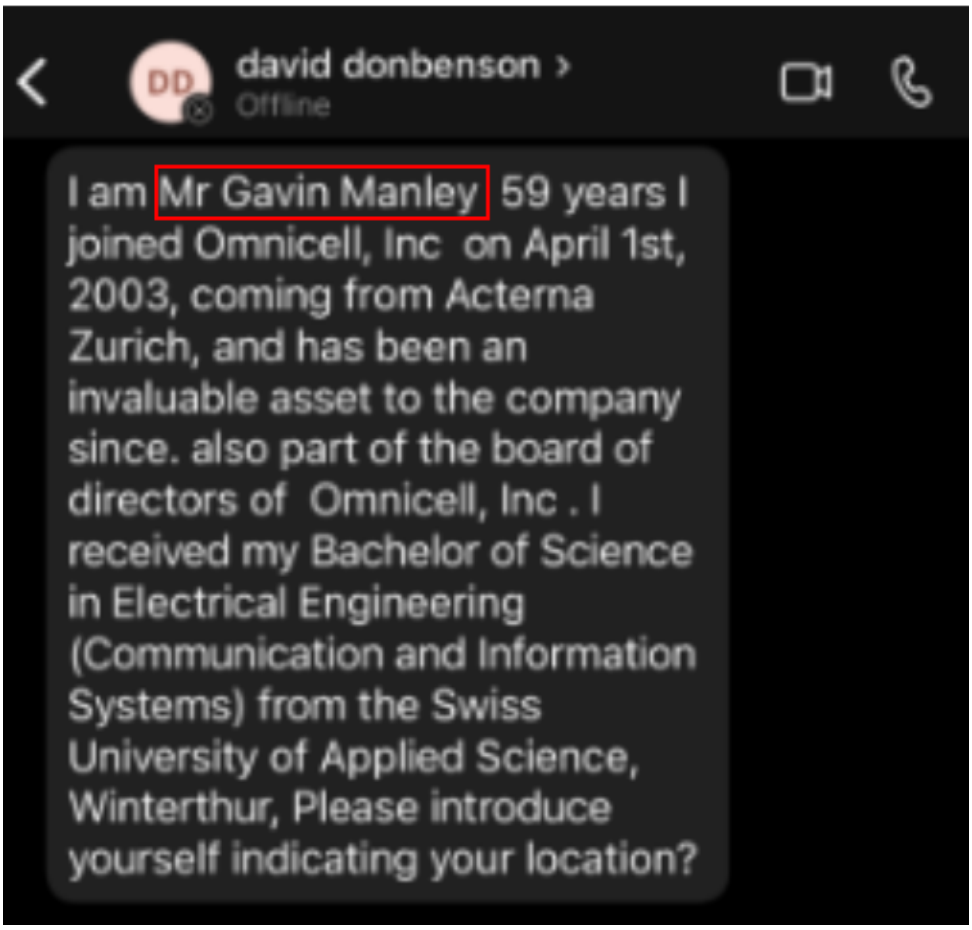


Figure 10: The interviewer introduces himself as Mr. Gavin Manley.

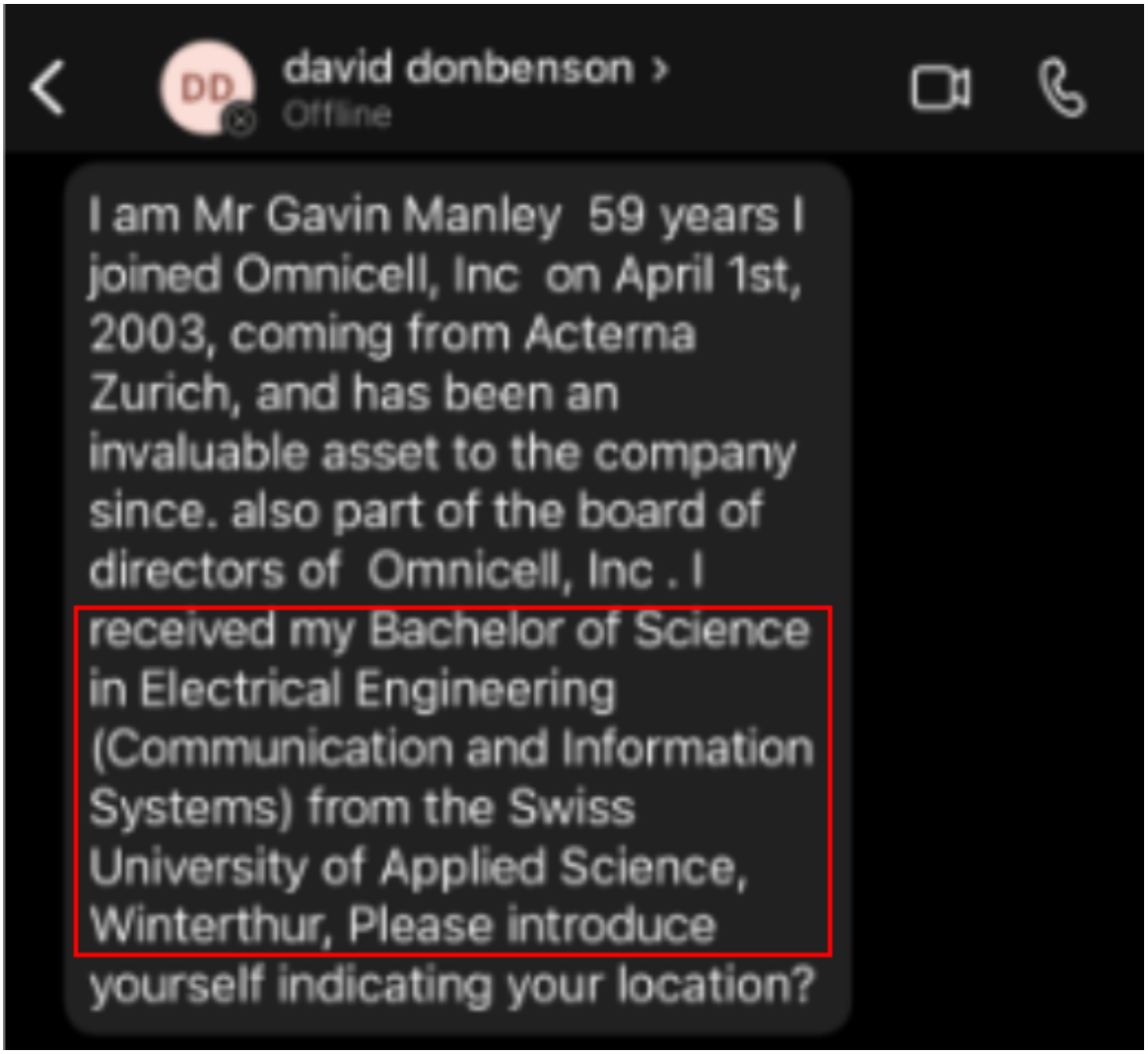


Figure 11: Mr. Manley claimed to have graduated from the Swiss University of Applied Science.

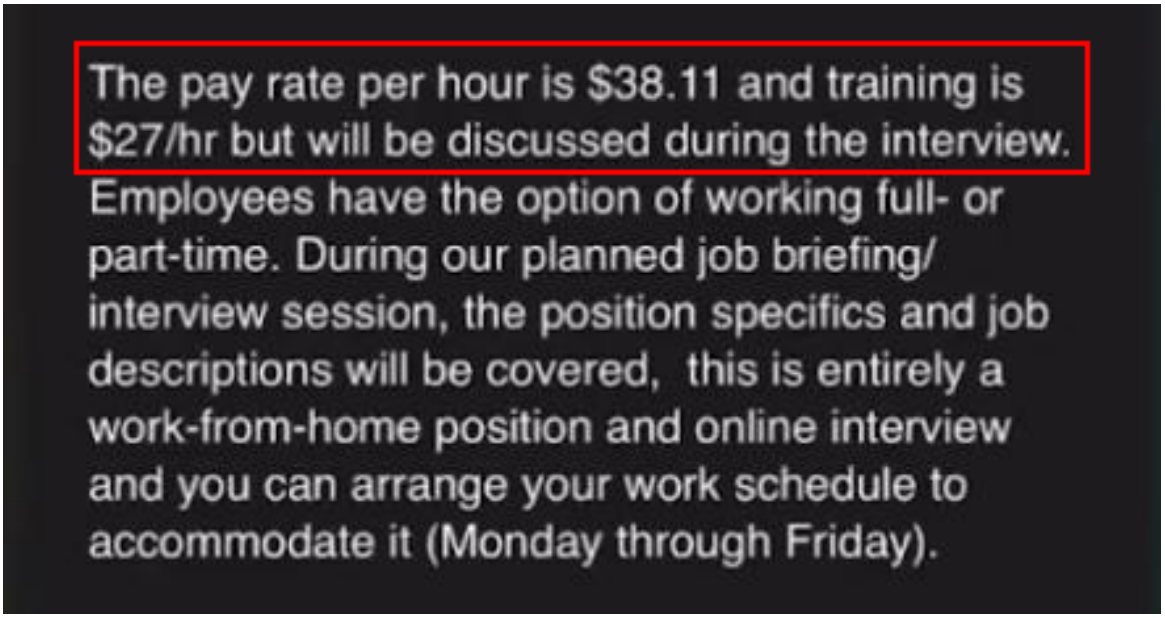


Figure 12: There should be a comma following "$27/hr" and before "but"

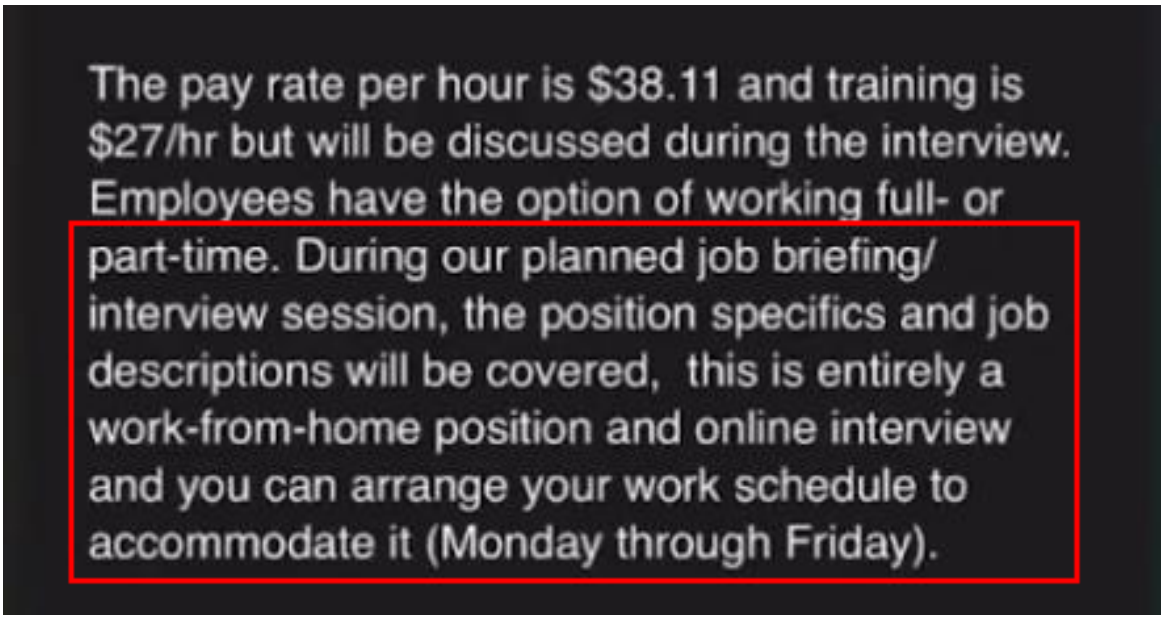


Figure 13: This is a run-on sentence that should be broken up into two or three separate sentences.

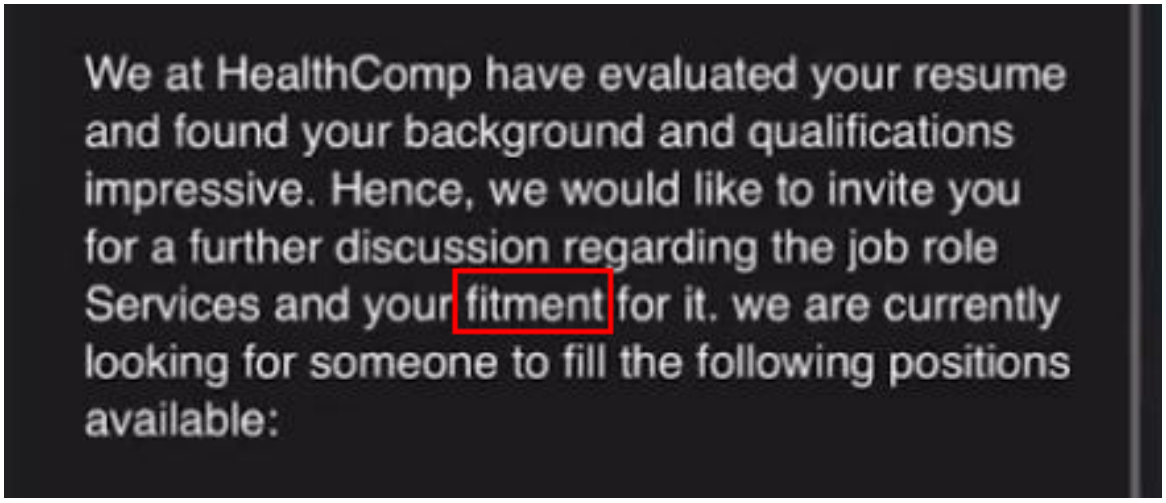


Figure 14: Misspelling of "fitment". It should just say "fit".

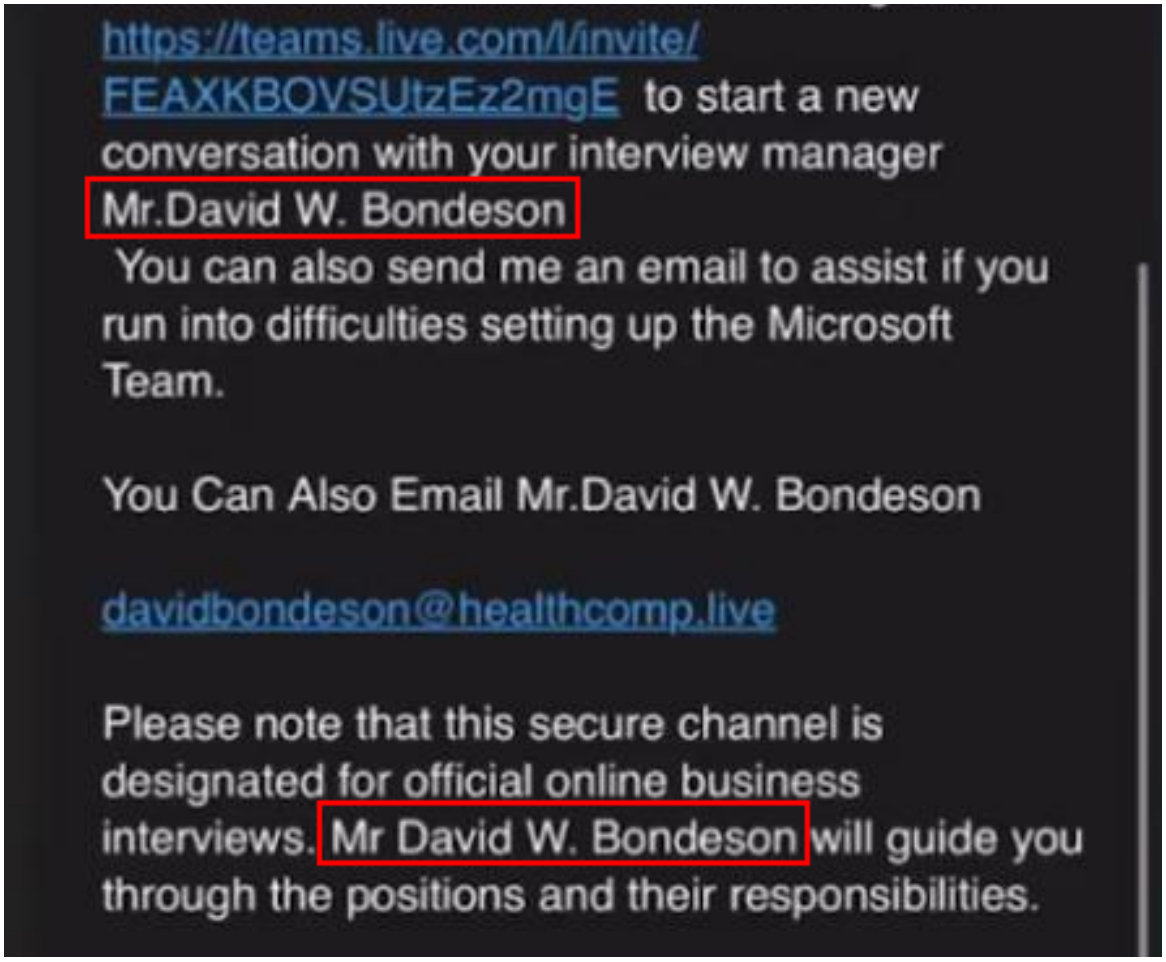


Figure 15: Discrepancy between "Mr.David W. Bondeson" compared to "Mr David W. Bondeson".

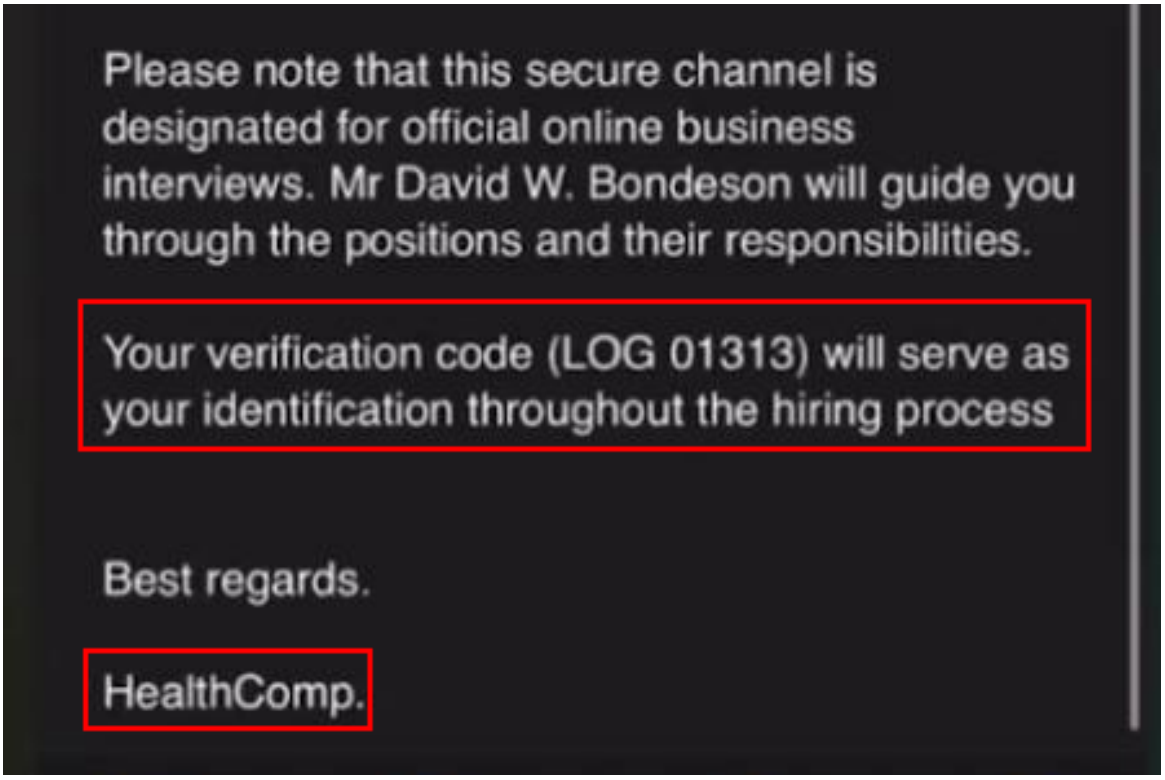
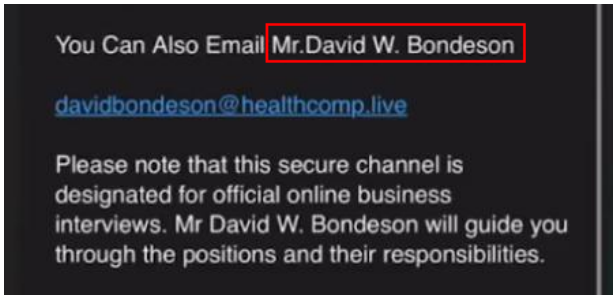
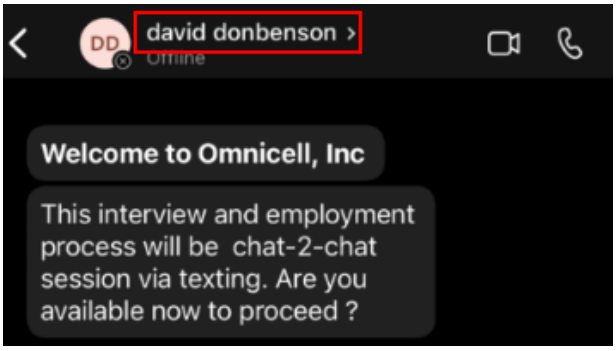


Figure 16: Verification code to be used as identification and email signature from HealthComp



(a) Original email with correct spelling.



(b) Misspelled name in Microsoft Teams interview.

Figure 17: There is a clear misspelling between the point of contact and the Teams account hosting the interview.

4 Timeline & ATT&CK Mappings

4.1 Timeline

4.2 MITRE ATT&CK Framework Mappings

1. **Resource Development: Acquire Infrastructure T1583**

   On Nov 13, 2023 the healthcomp.live domain is registered for use in later scams and phishing campaigns. This maps closely with the first reported HealthComp scam which was reported the next day.

2. **Reconnaissance: Search Open Websites & Domains T1593**

   Sam posted her resume to a public job-seeking site somewhere between April 15-18, 2024. She was contacted shortly offer with the interview offer from Kellie McDaniel. The scam perpetrators likely utilized open source intelligence techniques to find her job site posting and identify her as a target for their scam.
3. **Initial Access: Phishing T1566**

   On either April 17 or 18, 2024 Sam was sent what the team believes to be a phishing email, specifically a job scam. This serves as the point of initial access for future exploitation of the target.
4. **Initial Access: Trusted Relationship T1199**

   On April 20, 2024 Sam completed a text interview with what the team believes to be a job scam posing as the company HealthComp, LLC. This interview built trust with Sam as she considered the interview to be a legitimate part of her job search. With this established trust, a potential job scam could exfiltrate personally identifiable or financial information from Sam.
5. **Exfiltration: Exfiltration Over Web Service T1567**

   On April 20, 2024 Sam received a job offer following her interview. This job offer was sent over email and required her to fill out forms and provide both personally identifiable and financial information. Should Sam submit the forms and information, the job scammer will have successfully exfiltrated her data.
6. **Impact: Financial Theft T1657**

   Should Sam accept the job offer, she must purchase office supplies from HealthComp's vendor by April 22, 2024 at 8:00am. If this is a job scam like the team suspects, the money Sam would send to the vendor would likely be sent to the scammer for a profit and not actual office supplies.

5 NIST Phish Scale

The NIST Phish Scale is a tool developed by NIST to assist with the identification of Phishing scams (Dawkins, 2023). The team has applied the NIST Phish Scale worksheet to Sam's initial employment email to help determine its legitimacy.

5.1 Interview Offer Email

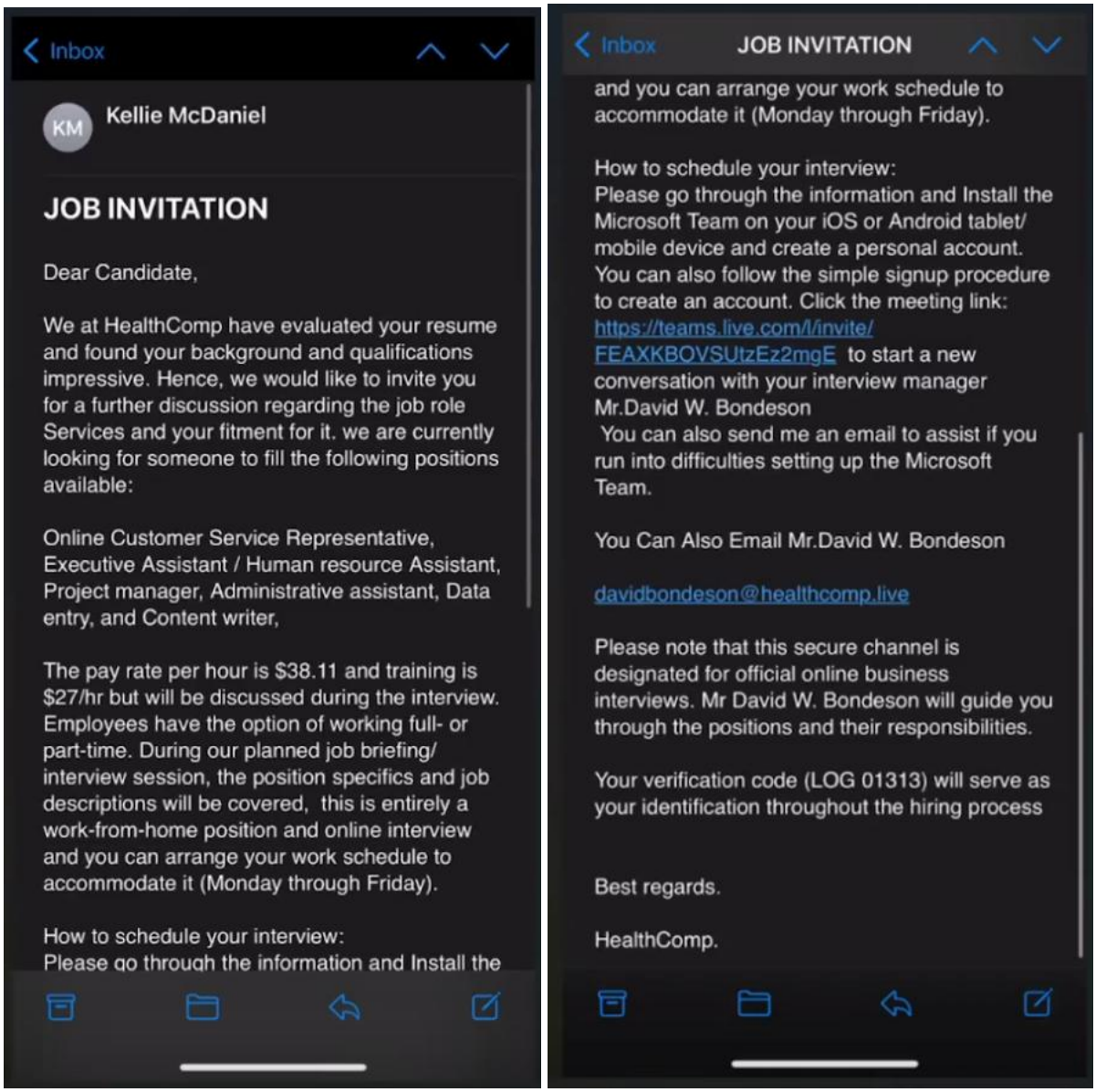


Figure 18: Sam's invitation to interview with "HealthComp"

5.1.1 Email Cues

Part 1: Answer "yes" or "no" to the following questions

Technical Indicators

Q: Is the sender's name unrelated to the sender's email address, including "reply-to" address?

A: **Yes** - The email is sent from Kellie McDaniel, who is not referenced at all throughout the interview and hiring process.

Q: Is a domain name used in the sender's email address plausibly similar to a recognizable entity's domain?

A: **Yes** - Although we don't have Kellie McDaniel's email address, the email later references davidbbondeson@healthcomp.live, which is similar to the real healthcomp.com domain.

Visual Presentation Indicators

Q: Are appropriate branding elements (text or logos) missing?

A: **Yes** - The email does not contain any logos or branding other than the use of the HealthComp name.

Q: Do the design and formatting of the email appear unprofessional?

A: **Yes** - The email doesn't utilize professional formatting, it has a number of grammatical errors and is not in line with what's expected from a typical employer.

Language and Content

Q: Is the email missing a generic greeting, such as a formal or informal salutation?

A: **No** - The email begins with "Dear Candidate", and ends with "Best regards"

Q: Is the email missing personalization?

A: **Yes** - The email is addressed to "Candidate", and doesn't refer to Sam by name at all.

Q: Is the message missing detail about the sender, such as sender or contact information?

A: **Yes** - The email does not mention the sender at all, it's signed from "HealthComp" and doesn't reference Kellie McDaniel.

Common Tactics

Q: Does the message appear to be a work or business-related process?

A: **Yes** - The message appears to be related to an interview offer at HealthComp.

Q: Does the message appear to be from a friend, colleague, boss, other authority entity, or other reputable authority entity?

A: **No** - No real information is provided about the sender of the email, Kellie McDaniel, and it's generically signed "HealthComp".

Total number of "yes" responses: **7**

Part 2: Tally the total number of times the following appear in the email

Errors

- How many spelling errors are in the email? **1**
- How many grammar errors are in the email, including mismatched plurality? **16**
- How many inconsistencies are in the email? **3**

Technical Indicators

- How many potentially dangerous attachments are included? **0**

- How many times does text hide the true URL in a hyperlink? **0**
- How many links have a domain name plausibly similar to a to a recognizable entity's domain? **1**

Visual Presentation Indicators

- How many branding elements (text or logos) appear to be an imitation? **0**
- How many branding elements (text or logos) appear to be out-of-date? **0**
- How many inappropriate security indicators or security icons are in the email? **2**

Language and Content

- How many times is legal language used in the message, such as copyright information, disclaimers, or tax information? **0**
- How many detailed aspects that are not central to the content are in the message? **2**
- How many requests for sensitive information are in the email, including personally identifying information or credentials? **0**
- How many times does the email express time pressure, including implied? **0**
- How many threats are included in the message, including implied threats? **0**

Common Tactics

- How many appeals does the email make to help others? **0**
- How many times does the email offer something that is too good to be true, such as having won a contest, lottery, free vacation and so on? **1**
- Does the email offer anything personalized and unexpected just for you? **Yes (1)**
- How many times does the email offer something for a limited time? **0**

Sum of tallied cues: **27**

Total cue count from Part 1 and Part 2: **34**

Total Cue Count	Cue Category
1 – 8 cues	Few (more difficult)
9 – 14 cues	Some
15 or more cues	Many (less difficult)

Table 1: Cue Category Mapping

Cue Category: **Many (less difficult)**

5.1.2 Premise Alignment

- How applicable is the email to workplace processes or practices for the target audience? **6**
- How pertinent is the email's premise to the roles and responsibilities of the target audience? **0**

- How well does the email align to other situations or events, even those external to the workplace? **6**
- How applicable is the email to concerns over potentially harmful ramifications for not clicking the links or attachments? **0**
- How applicable is the email's reflection of targeted training effects that would lead to premise detection? Care must be taken to appropriately incorporate the training or warning specificity, as transfer of learning is quite difficult. **8**

Applicability Scale	Applicability Score
Extreme applicability, alignment, or relevancy	8
Significant applicability, alignment, or relevancy	6
Moderate applicability, alignment, or relevancy	4
Low applicability, alignment, or relevancy	2
Not applicable, no alignment, or no relevancy	0

Table 2: Applicability Scale

Premise Alignment Rating: **4**

Premise Alignment Rating	Premise Alignment Category
10 and below	Weak
11 – 17	Medium
18 and higher	Strong

Table 3: Premise Alignment Category Mapping

Premise Alignment Category: **Weak**

5.1.3 Detection Difficulty

Cues Category	Premise Alignment Category	Detection Difficulty
Few (more difficult)	Strong	Very difficult
	Medium	Very difficult
	Weak	Moderately difficult
Some	Strong	Very difficult
	Medium	Moderately difficult
	Weak	Moderately to Least difficult
Many (less difficult)	Strong	Moderately difficult
	Medium	Moderately difficult
	Weak	Least difficult

Table 4: Detection Difficulty Mapping

Overall Detection Difficulty Rating: **Least difficult**

5.2 Job Offer Email

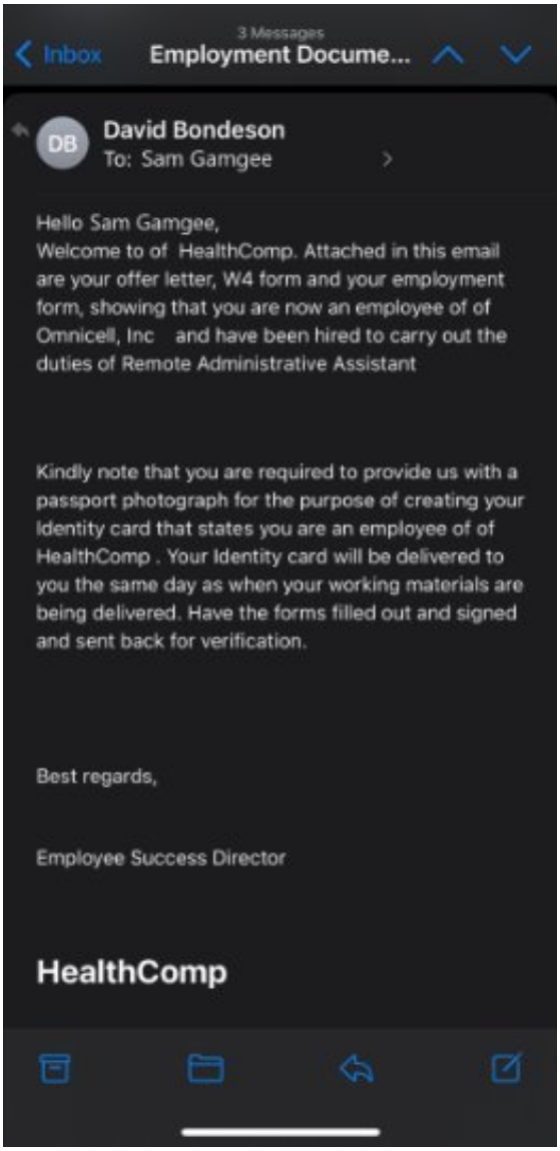


Figure 19: Sam's job offer email

5.2.1 Email Cues

Part 1: Answer "yes" or "no" to the following questions

Technical Indicators

Q: Is the sender's name unrelated to the sender's email address, including "reply-to" address?

A: **Yes** - The email is sent from David Bondeson, although this was the initial point of contact for the interview, the individual conducting the text based interview was Gavin Manley.

Q: Is a domain name used in the sender's email address plausibly similar to a recognizable entity's domain?

A: **Yes** - davidbbondeson@healthcomp.live, is similar to the real healthcomp.com domain.

Visual Presentation Indicators

Q: Are appropriate branding elements (text or logos) missing?

A: **Yes** - The email does not contain any logos or branding other than the use of the HealthComp name.

Q: Do the design and formatting of the email appear unprofessional?

A: **Yes** - The email doesn't utilize professional formatting, it has a number of grammatical errors and is not in line with what's expected from a typical employer.

Language and Content

Q: Is the email missing a generic greeting, such as a formal or informal salutation?

A: **No** - The email begins with "Hello Sam Gamgee", and ends with "Best regards"

Q: Is the email missing personalization?

A: **No** - The email is addressed to Sam specifically.

Q: Is the message missing detail about the sender, such as sender or contact information?

A: **Yes** - No contact information or sender name is indicated in the email.

Common Tactics

Q: Does the message appear to be a work or business-related process?

A: **Yes** - The message appears to be related to a job offer at HealthComp.

Q: Does the message appear to be from a friend, colleague, boss, other authority entity, or other reputable authority entity?

A: **Yes** - The message appears to be from the "Employee Success Director" at HealthComp.

Total number of "yes" responses: **7**

Part 2: Tally the total number of times the following appear in the email

Errors

- How many spelling errors are in the email? **0**
- How many grammar errors are in the email, including mismatched plurality? **9**
- How many inconsistencies are in the email? **3**

Technical Indicators

- How many potentially dangerous attachments are included? **2**
- How many times does text hide the true URL in a hyperlink? **0**

- How many links have a domain name plausibly similar to a to a recognizable entity's domain? **0**

Visual Presentation Indicators

- How many branding elements (text or logos) appear to be an imitation? **0**
- How many branding elements (text or logos) appear to be out-of-date? **0**
- How many inappropriate security indicators or security icons are in the email? **0**

Language and Content

- How many times is legal language used in the message, such as copyright information, disclaimers, or tax information? **0**
- How many detailed aspects that are not central to the content are in the message? **0**
- How many requests for sensitive information are in the email, including personally identifying information or credentials? **2**
- How many times does the email express time pressure, including implied? **0**
- How many threats are included in the message, including implied threats? **0**

Common Tactics

- How many appeals does the email make to help others? **0**
- How many times does the email offer something that is too good to be true, such as having won a contest, lottery, free vacation and so on? **1**
- Does the email offer anything personalized and unexpected just for you? **Yes (1)**
- How many times does the email offer something for a limited time? **0**

Sum of tallied cues: **18**

Total cue count from Part 1 and Part 2: **25**

Total Cue Count	Cue Category
1 – 8 cues	Few (more difficult)
9 – 14 cues	Some
15 or more cues	Many (less difficult)

Table 5: Cue Category Mapping

Cue Category: **Many (less difficult)**

5.2.2 Premise Alignment

- How applicable is the email to workplace processes or practices for the target audience? **8**
- How pertinent is the email's premise to the roles and responsibilities of the target audience? **8**

- How well does the email align to other situations or events, even those external to the workplace? **6**
- How applicable is the email to concerns over potentially harmful ramifications for not clicking the links or attachments? **4**
- How applicable is the email's reflection of targeted training effects that would lead to premise detection? Care must be taken to appropriately incorporate the training or warning specificity, as transfer of learning is quite difficult. **6**

Applicability Scale	Applicability Score
Extreme applicability, alignment, or relevancy	8
Significant applicability, alignment, or relevancy	6
Moderate applicability, alignment, or relevancy	4
Low applicability, alignment, or relevancy	2
Not applicable, no alignment, or no relevancy	0

Table 6: Applicability Scale

Premise Alignment Rating: **20**

Premise Alignment Rating	Premise Alignment Category
10 and below	Weak
11 – 17	Medium
18 and higher	Strong

Table 7: Premise Alignment Category Mapping

Premise Alignment Category: **Strong**

5.2.3 Detection Difficulty

Cues Category	Premise Alignment Category	Detection Difficulty
Few (more difficult)	Strong	Very difficult
	Medium	Very difficult
	Weak	Moderately difficult
Some	Strong	Very difficult
	Medium	Moderately difficult
	Weak	Moderately to Least difficult
Many (less difficult)	Strong	Moderately difficult
	Medium	Moderately difficult
	Weak	Least difficult

Table 8: Detection Difficulty Mapping

Overall Detection Difficulty Rating: **Moderately difficult**

6 Identifying Employment Scams & Tax Scams

Scams such as employment scams and tax scams are becoming increasingly common and more sophisticated then ever before. In fact, the FTC recorded over 105,000 "business and job opportunity" scams in 2023. This is more than a five-fold increase over the past five years (Heath, 2024).

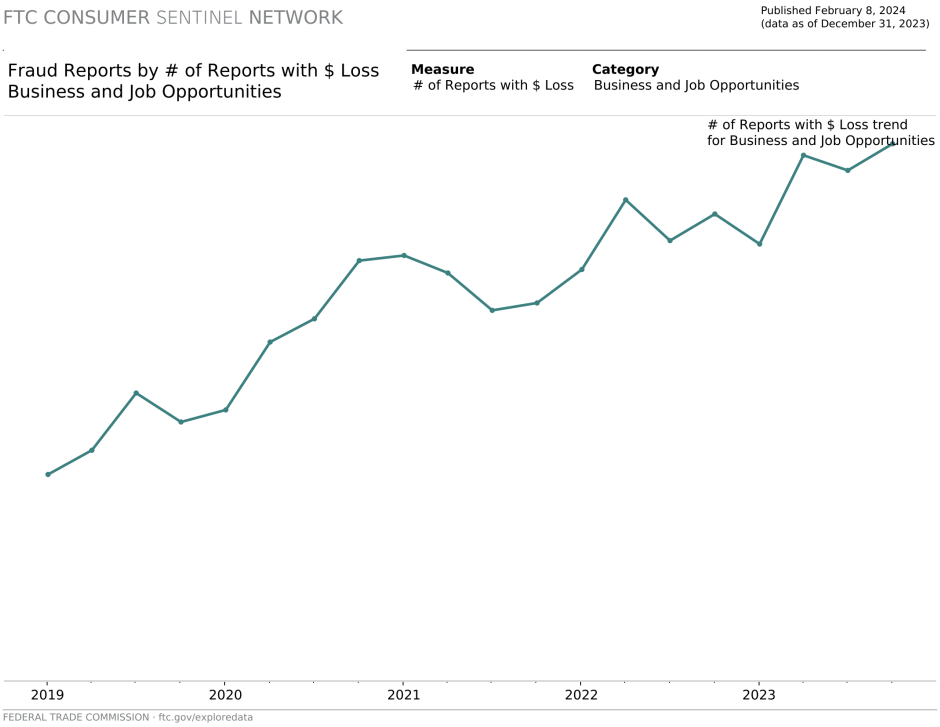


Figure 20: Number of fraud reports to the FCC with financial loss over time, FCC Tableau

6.1 General Scam Identification Steps

Scams usually attempt to exploit people for money or personal information such as a social security number. While there are various means and types of scams, the following are usually elements in a scam:

1. **Pretending to be from a Common Organization**: A scammer may pretend to work for a large company or governmental entity that people know of to build trust.
2. **Problem or Prize**: Scammers may pretend that the victim has a problem, such as jail time or debt. They also may tell the victim that there is a prize for completing the requested actions.
3. **Pressure to Act**: Scammers want victims to act before they can think about the scam and identify it. They may threaten large fines or jail time.
4. **Odd Payment Means**: Scammers may request payment through gift cards, cryptocurrency, or wire. These means are usually untraceable and you wont be able to be refunded or cancel the transaction.

6.2 Employment Scam Identification

Job scams can be hard to spot as the scammer usually identify people on legitimate job posting websites. They may also put targets through interview processes and have the target perform other tasks to build trust. Then, they will attempt to exploit the target for information or money.

The following are red flags of a job scam:

- **Contacted from a Personal Email**: A job scam is likely when a recruiter contacts you from a personal email instead of one from a company. For example, if you received an email from a @gmail.com domain, it is likely that it is a job scam.
- **Requests Payments**: When a person posing as a job recruiter requests payment for work items or training, it is likely a job scam. Particularly if the employer promises to repay for the items.
- **Asking For Personal Information Upfront**: When an employer asks for personal information upfront, such as bank account information or social security numbers, a scam is likely.

If you are ever unsure that you are dealing with the recruiter or a scammer, find the companies contact information on the internet and call or email them to ensure that you are speaking to one of their recruiters (Lazarus, 2023).

6.3 Tax Season Scams Identification

During tax season, many scammers are working hard to steal money or personal information posing as the IRS. These scams can be conducted over various communication channels such as email, SMS, social media, or phone (FCC Consumer and Governmental Affairs, 2024).

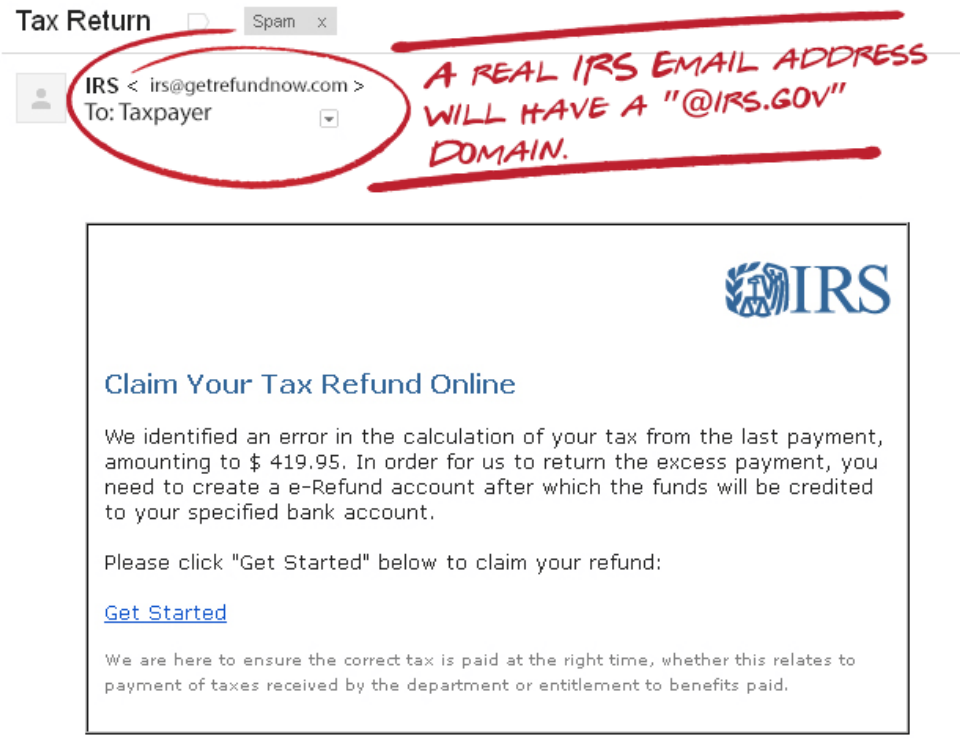


Figure 21: Common example of a tax scam, Michigan Consumer Protection.

Signs of a tax season scam include:

- **Phone Number Spoofing**: Scammers may use robocalls and phone number spoofing to make it appear that they are calling from a legitimate IRS phone number.
- **SMS Messages**: The IRS will not initiate contact with taxpayers via SMS. These messages often appear as urgent notifications with links.
- **Emails**: The IRS will not initiate contact with taxpayers via email. Any emails sent from the IRS will contain a .gov domain in the email address. Personal email addresses are never used for official contact.

To validate if the IRS is contacting you or if it is a scam, contact the IRS using the phone numbers listed on the official IRS website. If the medium of contact is an email, you can forward it to phishing@irs.gov.

7 Victim To-Do Checklist

If one has, or is believed to have fallen victim to an employment or tax fraud scam, it's imperative to take the proper steps to minimize resulting losses. The fraud fighters team has compiled the following checklists to assist those who have fallen victim to scams:

7.1 Sam's Next Steps

1. Cease contact with anyone claiming to be from Omnicell or HealthComp.
2. Do not provide the employer with any payment information or personally identifiable information (PII) such as your address, social security number or photo.
   – A remote position should not require you to have an employee identification card. Providing a scammer with a picture as well as other forms of PII such as a social security number or address opens pathways to multiple forms of identity theft.
3. Do not pay for any items which the company says it will reimburse you for as this matches with a common scam profile acknowledged by the Federal Trade Commission

   > *"No honest potential employer will ever send you a check to deposit and then tell you to send on part of the money, or buy gift cards with it. That's a fake check scam. The check will bounce, and the bank will want you to repay the amount of the fake check."*
   >
   > *— Federal Trade Commission (Hebert et al., 2024)*

4. Since minimal information has been provided, the likeliness of identity fraud occurring is slim, but not null; consider investing in a identity theft protection such as Aura or Norton Security's Lifelock.
5. Report phishing scam to phishing@irs.gov and report this incident to the Federal Trade Commission

7.2 Employment Scam Victim To-Do Checklist

1. Stop all forms of communications with scammer. However do not delete any emails or texts messages sent to you as it can help serve as evidence when building a case with your local police
2. Report the employer on the job board platform which you were solicited.
3. If scam involved impersonation of a real company, contact their HR department to inform them of the scam.
4. Monitor common signs of identity theft including:
   - Credit cards opened in your name.
   - Loan application denials sent your home.
   - Debt Collection notices via mail or phone.
   - Tax Return already filed by someone other than yourself.
5. Help the government build a case and track down scammers by reporting your incident to the Federal Trade Commission (FTC).
6. If payment was involved, contacted the involved financial institution ASAP to increase chances of conflict resolution.
7. Close all new accounts opened in your name.
8. Report all phishing scams to phishing@irs.gov
9. Report all monetary loss to the Treasury Inspector General Administration and the Federal Trade Commission
10. Submit an IRS Identity Theft Affidavit (Form 14039).
11. Initiate a credit freeze.
12. Update online security measures.
13. Identity theft monitoring.
14. Seek legal advice.

8 Gameplan

8.1 Goal

The goal for tomorrow is to inform Sam of the evidence that we collected, and how it relates to their job offer. Ultimately, we would like Sam to understand the risks of proceeding with the job offer knowing that it is likely a scam.

8.2 Current Situation

In the current situation, we realize that the job offer is more than likely a scam. Knowing this information, we have requested that Sam hold off on continuing sending the potential employer information.

For meeting with Sam tomorrow, we believe that we have the following strengths, weaknesses, opportunities, and threats (SWOT) leading up to our meeting:

8.2.1 Strengths

Going into the meeting, we find that there is more than conclusive evidence that points towards this being a job offer scam. Particularly, we find that the report of the BBB scam listing, our rating of the communications on the NIST phish scale, and our other evidence is convincing for one to understand that the job is likely a scam.

We also requested that Sam wait until tomorrow before proceeding with communication with the potential employer. We believe that this may wear down some of the excitement that she has and allow her to think about the red flags that we informed her of during the interview. If this does occur, we will be in a stronger position to inform her of the risks associated with continuing in this employment opportunity.

8.2.2 Weaknesses

We realize that Sam is very excited to get a high paying job with great benefits. The potential reward may blind her from understanding the facts of the situation and realizing that this is more than likely a phishing scam.

8.2.3 Opportunities

Since we have analysed and compiled information about many of the job scams and applied it to her experience in the hiring process with her potential employer, we believe that this puts us in a strong position to persuade her that this opportunity is a scam.

8.2.4 Threats

It is possible that Sam receives a message from the employer that requests that she urgently completes a task for them. Should this happen, she may panic and send personally identifiable information or money to the scammers before we are able to intervene.

8.3 Strategies

We recognize that Sam is excited to receive a high paying job and will be disappointed when we inform her that the job is likely a scam. She may also choose to not believe us and proceed.

Knowing this, we will proceed with the following strategies:

8.3.1 Empathy

We plan on approaching Sam with empathy and understanding. We have her best interests at heart and will try to prevent her from being harmed by the scammers.

8.3.2 Evidence

In order to convince Sam that the job is a scam, we will use all of the evidence that we compiled and present it to Sam in a persuasive way.

8.3.3 Train

Since Sam may be targeted by a scam in the future, we will train her on how to identify scams. Knowing this information, she should be able to better spot scams moving forward.

8.3.4 Provide Resources

We will provide Sam with resources to keep up to date on the current scams. We will also provide her with resources should she have had any data compromised in this incident or in any future incidents. These resources include the victim checklist that we developed. She can use this to minimize the risk of any potential identity fraud or financial loss.

8.4 Communication Plan

Knowing our where we currently stand and what strategies that we should employ, we will take the following actions to communicate out points to Sam:

8.4.1 Build Trust

In order for Sam to believe us, we must establish trust with her so that she considers our points. In order to do this, we will inform her that we are experts in the field of cybersecurity and have studied many scam cases.

8.4.2 Understand Perspective

We understand that Sam really want to get a job and doesn't believe that she is part of a scam. In order to bring our points across to her, we will use the evidence that we acquired and question why she thinks that it is not a scam. From there, we can then provide her with resources to find a legitimate job.

8.4.3 Share Evidence

Once we build trust and recognize that we understand her perspective, we will then share the evidence that we acquired for this case. This will then allow her to form her own opinion on the case.

8.4.4 Provide Resources

We will provide Sam with resources that inform her on what she should do now to resolve any potential breaches related to this scam and also provide her with resources to learn about scams and prevent her from being scammed in the future.

8.4.5 Encourage Caution

Should Sam choose to move forward with the job against our wishes, we will encourage her to exercise caution before performing any tasks for the potential employer. In particular, we will encourage her to thoroughly think over the situation before spending money or sharing personal information.

References

Better Business Bureau. (2023, November). Bbb scam tracker | scam id #772647. https://www.bbb.org/scamtracker/lookupscam/772647

Dawkins, S. (2023). *NIST Phish Scale User Guide*. https://doi.org/10.6028/nist.tn.2276

FCC Consumer and Governmental Affairs. (2024, April). Tax season scams and taxpayer id theft. https://www.fcc.gov/tax-season-phone-scams-and-taxpayer-id-theft

Heath, R. (2024, January). Job scams skyrocket. https://www.axios.com/2024/01/30/job-scams-employment-fake-offers

Hebert, A., Tressler, C., Rayo, A., & Puig, A. (2024, March). Job scams. https://consumer.ftc.gov/articles/job-scams#what%20to%20do

IBM. (n.d.). What is the mitre att&ck framework? https://www.ibm.com/topics/mitre-attack

Lazarus, A. (2023, December). How to spot the latest job scams. https://consumer.ftc.gov/consumer-alerts/2023/12/how-spot-latest-job-scams

Appendices

A NIST Phish Scale

The NIST Phish scale was developed by NIST to identify phishing attacks and evaluate the effectiveness of training to combat these attacks. The scale evaluates the complexity and quality of a phishing attack so that organizations can better train their employees and/or clients to identify these attacks (Dawkins, 2023).

NIST considers the following criteria in an email when assessing a phishing attack:

1. **Error**: Spelling errors, grammatical errors, and inconsistencies.
2. **Technical Indicator**: Attachment types, sender email, sender information, hyperlinks, and domains used.
3. **Visual Presentation Indicator**: Professionalism of the email, company logos, and other visual elements that would be expected in a cooperate email.
4. **Language and Content**: Threats presented by the email writer, urgency, lack of details, and/or irrelevant details.
5. **Common Tactic**: Such as too good to be true offers, special treatment, and/or posing as a friend/colleague/employer.

NIST also considers the premise alignment of the communications to indicate how difficult it is for a victim to detect. Premise alignment is a measure of how closely an email matches the work roles or responsibilities of an email's recipient or organization. The stronger an email's premise alignment, the more difficult it is to detect as a phish. Inversely, the weaker an email's premise alignment, the easier it is to detect as a phish (Dawkins, 2023).

The following premise alignment attributes are assessed on the NIST phish scale:

1. **Mimics a Workplace Process or Practice**: The closer a phishing email mimics how an organization acts, the more likely the target is to fall for the phishing attack.
2. **Has Workplace Relevance**: If the attack takes the target's job position and workplace access into account, they target is more likely to find the email legitimate.
3. **Aligns With Situations or Events**: Should the message be timely to events occurring in the target's life or organization, the target is more likely to believe that the message is legitimate.
4. **Engenders Concern Over Consequences**: If the email is threatening the target to take action or face consequences, the target is more likely to perform the requested actions in order to avoid the consequences, even if the consequences do not exist.
5. **Training/Experience of Recipient With Phishing Emails**: When the target is trained in identifying phishing attacks, or has previously been a victim to phishing attacks, they are more likely to identify the attack and stop it.

B MITRE ATT&CK Framework

The MITRE ATT&CK Framework catalogs cybercriminal's tactics, techniques and procedures in each phase of their attack. This allows defenders to identify such attack methods and ensure that their defenses are capable of stopping such attacks (IBM, n.d.).

The attack framework is ordered chronologically, with 1 being the first phase of the attack and 14 being the last phase of the attack. Each phase of the MITRE ATT&CK Framework is as follows:

1. **Reconnaissance**: gather information about the target to plan for an attack.
2. **Resource Development**: build and acquire resources to carry out the attack. This can include domains, web sites, and email servers.
3. **Initial Access**: Exploit the target to get initial access to their environment.
4. **Execution**: Run malware or malicious code on the exploited system.
5. **Persistence**: Setup access to the system that will withstand reboots or system reconfiguration.
6. **Privilege Escalation**: Gain access to accounts with higher privileges, such as an administrator.
7. **Defense Evasion**: Avoid detection, such as anti-virus or intrusion detection systems.
8. **Credential Access**: Gather usernames, passwords, and other credentials to expand access.
9. **Discovery**: Explore and research the target's system to find systems that can be accessed or controlled to support an attack.
10. **Lateral Movement**: Gain access to other resources in the environment.
11. **Collection**: Gather target's data in the environment related to the goal.
12. **Command and Control**: Establish covert/undetectable communications from the target's systems to the attacker that enable control over the target's system.
13. **Exfiltration**: Steal data from the target's system.
14. **Impact**: Interrupt the business' function and data.