Competitive Cyber Security Organization
AT PENN STATE

CARE Lab Social Engineering Competition

Day One Deliverables

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

April 19, 2024

Table of Contents

1 Executive Summary

The CARE Lab fraud fighters team was solicited to assist a young student, Sam, with determining the legitimacy of a job opportunity she recently received. During the first day of the engagement the team met with Sam's friends to gather background information on both the employment opportunity and Sam.

Sam initially posted her resume on an online job seeking site, after which she was quickly contacted by Kellie McDaniel. McDaniel claimed to be from HealthComp, a healthcare solutions company. Sam received an offer to interview for six different positions with David W. Bondeson who was identified as the "Interview Manager". The positions were offered as either full or part time, and fully remote.

The team built a comprehensive profile of the prospective employer, assembled a timeline of events, identified a number of potential red flags, and created a plan to assist Sam throughout the rest of the job seeking process. Notably, the team identified a number of red flags, and a Better Business Bureau scam report consistent with the profile of Sam's prospective employer. With this in mind, the team recommends that should Sam choose to move forward she do so hesitantly, and should consult with the fraud fighting team before disclosing any sensitive information.

2 Employer/Scammer Profile

2.1 Employer Profile

HealthComp is a third-party administrator for healthcare solutions founded in 1994 which helps employers make informed financial decisions regarding self-funded health plans for employees. HealthComp and Virgin Pulse, another healthcare solutions company, merged in November of 2023 in a $3 billion deal to create a company that uses technology and AI to create health plan designs that improve member health and lower costs (Virgin Pulse, 2023). Beginning February of 2024 the merger between Virgin Pulse and HealthComp started its transition to the Personify Health name and brand (Personify Health, 2024).

HealthComp utilizes an online careers portal under the banner of Personify Health for its job postings and applications. All of their currently posted remote job listings are full time, and provide a salary range along with detailed descriptions of needed qualifications and duties (Virgin Pulse, 2024). The team found no indication that HealthComp commonly solicits interviews without an application.

2.2 Scammer Profile

As it pertains to Sam's employment, all emails received only reference HealthComp with no mention of the new brand name, Personify Health. Additionally, the email provided to contact, Mr. David W. Bondeson, is directed towards the email domain @healthcomp.live; however, all contact within the company comes from the @healthcomp.com domain, as

seen through the real David W. Bondeson's Linkedin page.

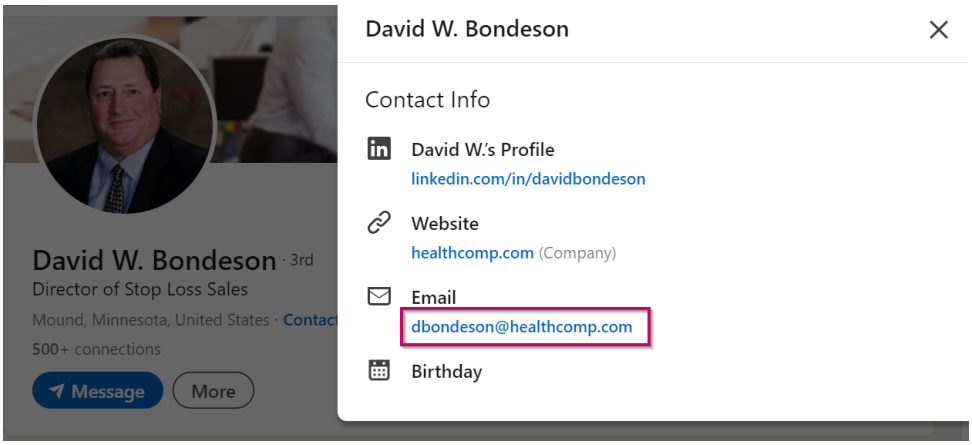

Figure 1: David W. Bondeson's LinkedIn contact information which utilizes the healthcomp.com domain as opposed to the provided healthcomp.live

The message from McDaniel promises flexibility that is not found within the Personify Health job listings. It is also worth noting that the positions referenced in the email: Customer Service Representative, Executive Assistant, Human Resource Assistant, Project Manager, Administrative Assistant, Data Entry, and Content Writer, do not appear on either LinkedIn or the internal job board as well for Personify Health.

3 Timeline of Events

3.1 Persuasive Techniques

1. **Recognizance of Achievements**

   The email received by Sam begins with HR stating they found her background and qualifications impressive. Beginning with flattery may be an attempt to lower the guard of the recipient, and is usually followed by promises that seem too good to be true.

2. **Too Good to be True**

   The advertised pay rate is generalized at $38.11/hr for all six roles which is uncommon since each role would require a different skill set and therefore the salary for each position should be different. The generalization of such a high pay rate is likely a lure so applicants are inclined to follow up with the job offer.

   The email sent to Sam offers a work from home opportunity as well as a part-time, flexible schedule; However, all remote positions listed on Personify Health's LinkedIn and internal job board are for full-time employees.

3. **Authority**

   Sam's point of contact for the interview is Mr. David W. Bondeson, and although not stated in the email, a google search shows that he's the Director of Stop Loss Sales

at Personify Health. Scheduling an interview with an executive at such a high level may make potential employees feel special and reassured about the legitimacy of the opportunity.

4. **Masquerade**

   Posing as a legitimate company builds trust between the employer and interviewee. If the job offer was sent from a company with little to no online presence, potential victims would be more wary in continuing contact with Human Resources.

3.2 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 15th-18th 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 Red Flags

During the course of the initial interview with Sam's friends, the fraud fighting team identified a number of potential red flags with the HealthComp job opportunity.

4.1 Email Red Flags

The email that Sam received contains multiple red flags that indicate that it may be a phishing email. These include:

- Numerous grammatical errors (NIST Phish Scale Cue Type: Error)
  - Several misspelled words (See Figure 2)
  - Several missed commas (See Figure 3)
  - Several run on sentences (See Figure 4)
  - Discrepancies with how David Bondeson is titled (See Figure 5)
- Email address referenced in email is healthcomp.live (NIST Phish Scale Cue Type: Technical Indicators)

  - healthcomp.live is not utilized by HealthComp, the company uses healthcomp.com for email communication
  - The healthcomp.live domain was recently registered
- Sender Kellie McDaniel is not listed as a HealthComp employee (NIST Phish Scale Cue Type: Technical Indicators)
- Email signed by HealthComp instead of the sender or an HR Representative (NIST Phish Scale Cue Type: Language and Content)
- Email is generically addressed to "Candidate" as opposed to Sam (NIST Phish Scale Cue Type: Language and Content)
- Utilizes a "verification code" as opposed to applicant name

4.1.1 Grammatical Errors

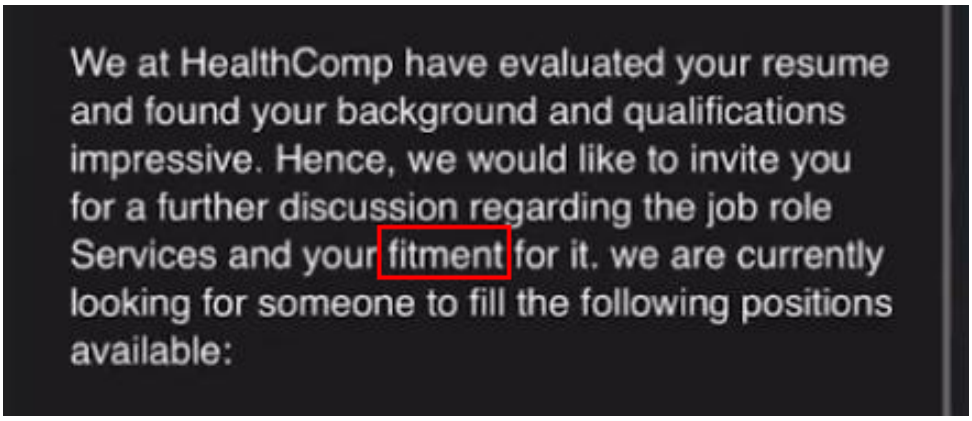

Figure 2: Misspelling of "fitment". It should just say "fit".

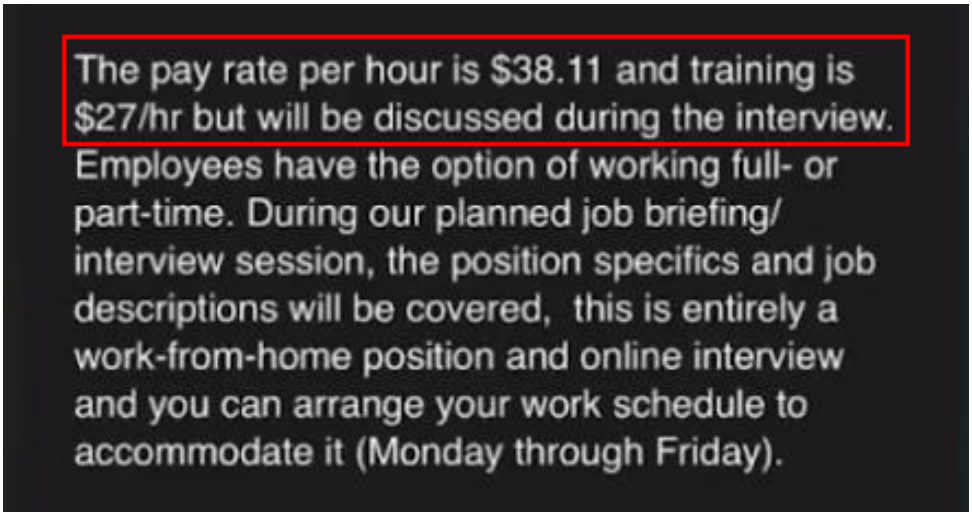

Figure 3: There should be a comma following "$27/hr" and before "but".

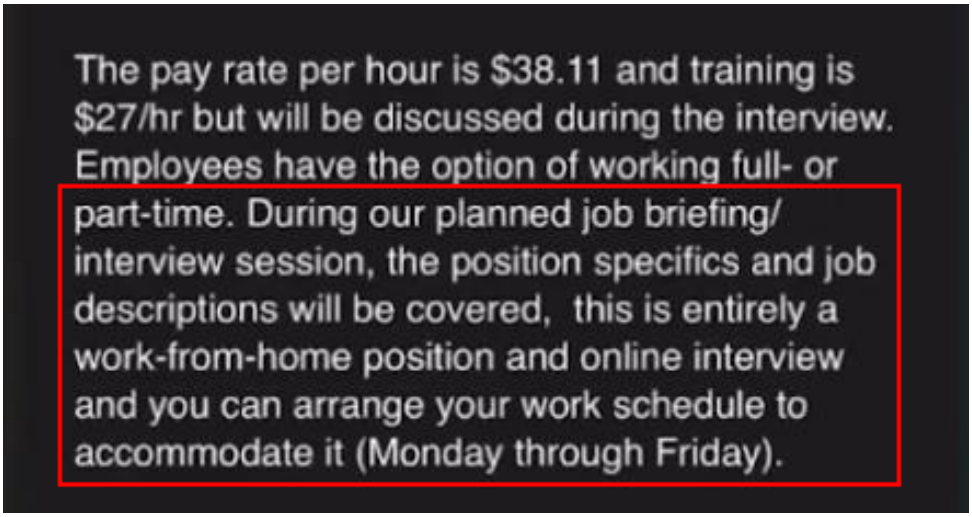

Figure 4: This is a run-on sentence that should be broken up into two or three separate sentences.

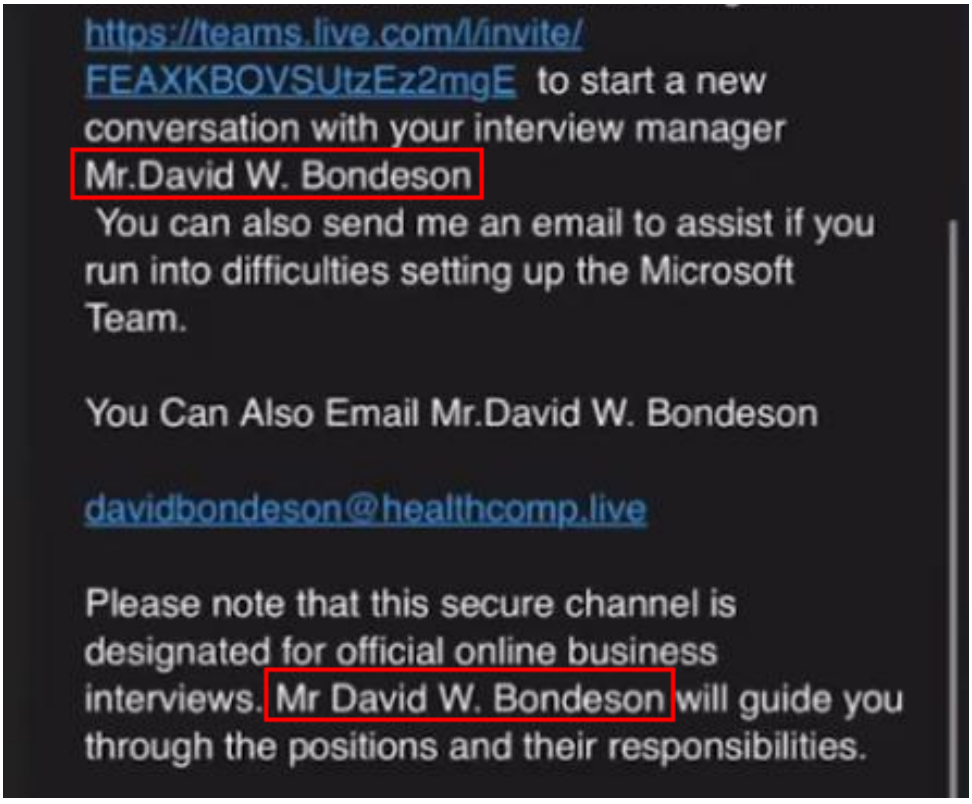

Figure 5: Discrepancy between "Mr.David W. Bondeson" compared to "Mr David W. Bondeson".

4.2 Job Red Flags

The job posting includes various red flags. These include:

- Job interview is for 6 different positions
  - All jobs have the same pay rate despite different duties and skill levels (See Figure 6)

  - All jobs are fully remote and create your own schedule (See Figure 7)
  - None of the jobs are listed on the HealthComp careers website (See Figure 8)
- Interview is scheduled through a text based chat instead of phone, video, or in person.
- On LinkedIn, David is listed as "Director of Stop Loss Sales", a director is not likely to conduct an interview for an entry level position (See Figure 1)

4.2.1 Job Posting Evidence

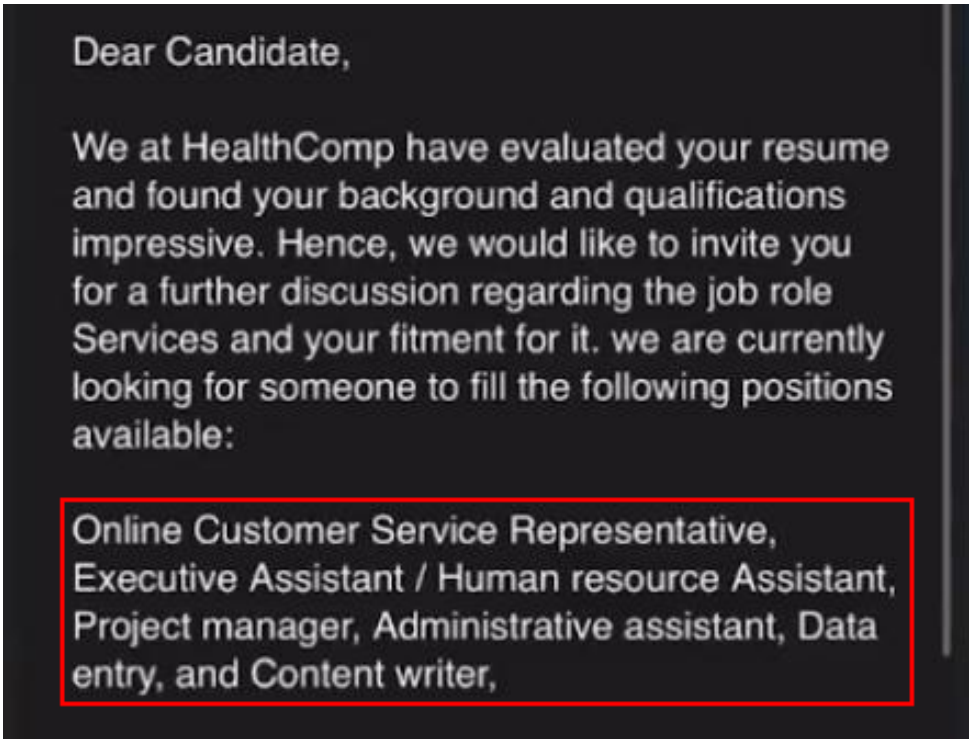

Figure 6: The email specifies these six job positions as available.

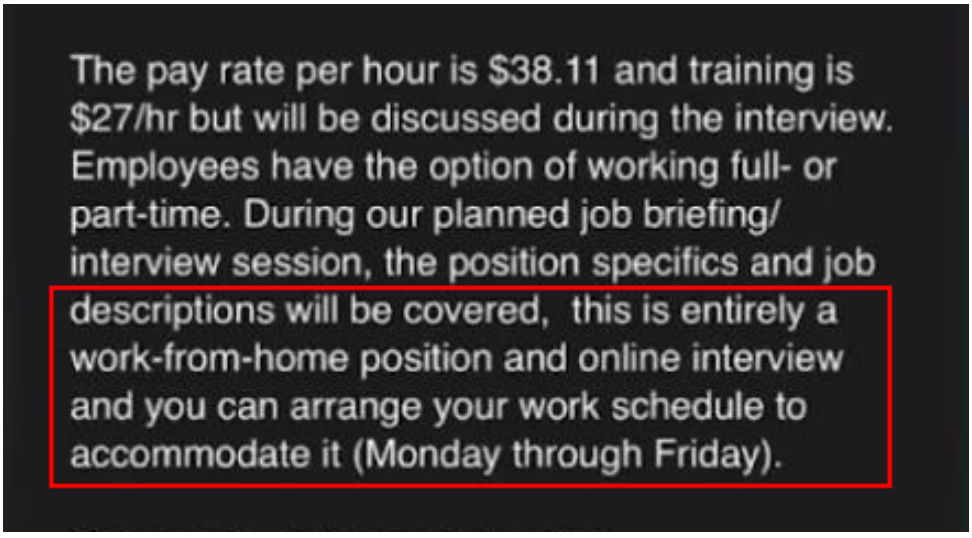

Figure 7: The email specifies all jobs are work-from-home and have custom schedules.

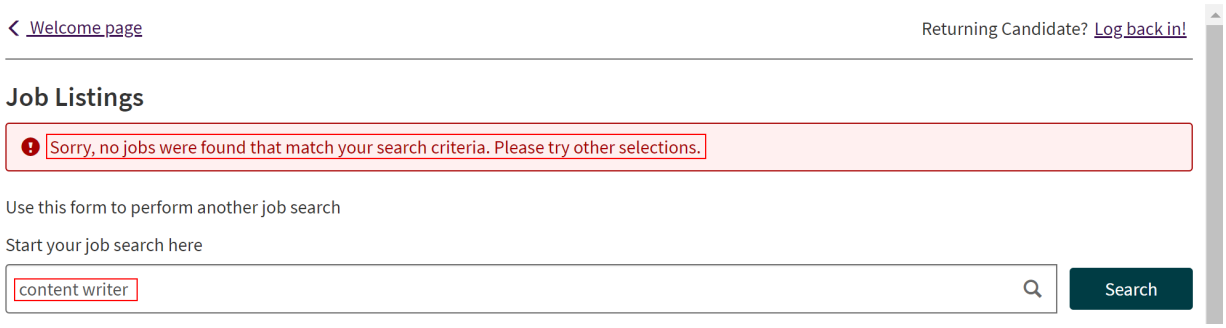

Figure 8: The job listings for HealthComp do not have the offered position of content writer available

4.3 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.

5 Gameplan

The team's goal is to help guide Sam through this potential job scam using the evidence collected from OSINT and today's preliminary interview. During the rest of Sam's hiring process the team intends to guide her through the interview, and prevent Sam from falling victim to an employment scam.

During the interview the team will continue to evaluate the interaction to see if it is consistent with the characteristics of a job scam. Specifically, it's imperative to see if the inter-

view and hiring process follow the same formula outlined in the BBB Scam Report. If this is the case, the team will advise Sam not to disclose any sensitive or personal information in order to avoid both financial loss and identity theft.

Additionally, the team plans to educate Sam on the different types of common job scams to better equip her for the rest of her job search. The team will develop a guide on identifying scams and fraud, and checklists for victims of scams that Sam can utilize in the future. It's encouraged that Sam take a proactive approach to preventing these scams in the future, by scrutinizing suspicious opportunities, and avoiding posting publicly.

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

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

Personify Health. (2024, February). Virgin pulse and healthcomp introduce combined company as personify health. https://www.prnewswire.com/news-releases/virgin-pulse-and-healthcomp-introduce-combined-company-as-personify-health-302055387.html

Virgin Pulse. (2023, November). https://www.virginpulse.com/press-releases/virgin-pulse-and-healthcomp-complete-merger/

Virgin Pulse. (2024, April). Virgin pulse career center. https://careers-virginpulse.icims.com/jobs/intro

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.