Ian Waweru

Lucinda Wittikower

Information literacy

12/8/2022

Increased emailing scams

 There are scenarios of moral panics (MP) that occur in our society. The purpose of a moral panic is to grab the reader’s attention by writing a paper and posting it on the media, blogs, or any news sources to get people to believe in the situations that occur. Sometimes the information can be exaggerated and not qualify to be considered a moral panic. For example, if I told people that a new version of chicken pox is on the rise and it’s deadly. It could spring widespread fear in people and wanting to learn more about the situation. There’s another example of moral panic that I want to deeply investigate and it’s titled email scams. Emailing scams have been around for a while and will only worsen. To learn more about this situation I will look for articles written by cybersecurity specialties and discover the truth behind this problem. I will also look back to discover when this moral panic started and why it has become problematic to our society. There are different types of content I can use as examples to cover why this is considered a moral panic. There used to be a name given to emailing scams, known as the Nigerian prince scam. The Nigerian prince scam is an older tactic that was used to invade victims’ systems. The hacker will send an email claiming to be the Nigerian prince and from there the victim sends their banking information thinking they’ll get a reward from the hackers. The main target of these attacks are people in big businesses or people in general that carry a device like a cell phone. This strategy was once effective but nowadays that strategy wouldn’t work as well. However, emailing scams are still occurring and have gotten worst. As technology develops over time, so do cyber crimes and their strategies for an attack. Cybercriminals have found other ways of using emailing scams to commit an attack. “Instead, scammers are scouring social media, especially business-related ones like LinkedIn, to target people with tailored messages” (Oliver, Buckley). For example, businesses that used the “Linked-In” app within the first quarter of 2022, accounted for 52% of phishing scams globally. The emailing scams also known as phishing attacks will steal company data and people’s private information. This concern should be taken more seriously as it continues to become a problem for people and businesses.

 All organizations have a policy they follow when it comes to the awareness of email scams. I used *authority constructed and contextual* to discuss how the author’s expertise in this field can give readers an example of why this concern is important. Caroline Duncan is an employee of a company called desk alerts. She has a blog page that talks about what businesses should be aware of and how to organize certain things. In one of her posts, she talks about cyber-attacks through emails. In the year 2020 businesses around the world hit a record for data that was lost. This is a fact because in 2020 there was a report out that stated the average cost to businesses for a cyber-attack was 3.86 million. Caroline also highlighted another important fact: in 2020 “IDG research services had a survey and found that almost 80% of IT leaders felt that their companies do not know how to protect against these cyber-attacks” (Duncan, Caroline). Caroline talks about 6 different types of email scams that people and organizations should be aware of. The first scam attack is called Ransomware awareness email. Ransomware attacks are dangerous, they can lock an individual’s system until they pay the price a hacker is requesting. Using the authority frame I came up with a situation where a hacker can use ransomware emailing attacks to infect a system in an organization. The hacker can use this email to act as an authoritative figure to get an employee to click on its link. The best way to avoid these attacks is for employees to be aware of the emails they open. The second scam is called phishing awareness email. Phishing emails are another technique used by hackers to gain access to a system. The objective is to trick a victim into clicking a link sent via email by making an empty promise. For example, the Nigerian prince scam is considered a phishing attack and it uses authority to get the data the hacker is looking for. The next two attacks are known as whaling attacks and spam email attacks. Whaling is like phishing attacks; however, the difference is that the hacker will send an email acting as a top advisor. They will ask for private information like a password or even credit card information. Spam attacks are used by cybercriminals to trick employees into thing there important. Having a password for emails is a great idea however if a hacker can access that password, then it could get risky. All these attacks are examples of why emailing scams are a concern in cyber security. Another way I used the authority frame was to look at why someone might fall for a scam. Hackers use different techniques to trick people into falling for a scam. There are six of these techniques and they are known as; Reciprocity, consistency, social proof, liking, authority, and scarcity. The important technique that caught my attention the most was the authority technique. Scammers are imitating authoritative companies because “People are more likely to say “yes” to those seen as authorities or experts” (MPG).

 Emailing scams aren’t going away anytime soon. These attacks have been here for a while and are evolving. Even cybersecurity experts are struggling to keep up or are getting tricked themselves. I used another frame from the ACRL framework to talk about the value of the information shared by the authors. Three authors wrote an article on the dangers of email scams and how it’s progressing. I think the author's background is important and it adds value to the article. Oliver Buckley is one of the authors and he is an associate professor in cyber security. The next author is Max Eiza, and he is a senior lecturer in computer security. The final author is Gareth, Norris, a senior lecturer of psychology. The background of these authors is important because it allows the reader to believe in the information they provide. The source itself that they provided was very informal and as I was reading, I was able to understand why it was necessary to have 3 different authors. Gareth Norris has a career in teaching psychology and his information is valuable for understanding why people fall for these types of scams. He claims, “Psychologists who research obedience to authority know who we are more likely to respond to requests from people higher up in our social and professional hierarchies” (Gareth, Norris). For example, if someone saw their favorite celebrity message or emailed them, they are likelier to open them. Most cybersecurity concerns start with people or employees in an organization. Scammers use this to their advantage by making fake emails or messages that look like they came from someone else. Another important fact that was mentioned is the use. Of social media. Social media has made it easier for cybercriminals to perform spear phishing attacks. The data we share every day through social media allows cybercriminals to learn more about a person and get clues or ideas on how to proceed with an attack. It’s important to learn about these attacks before encountering them, organizations and people living their normal lives are at risk for these types of attacks. There are different ways to combat and slow down these attacks but the best way to avoid them at all is by ensuring you’re not clicking on a random email with a site tab. Another example of how I used the information has value frame was by using social media posts that talk about phishing attacks. For example, I went on Twitter and found a list of tweets that talk about the dangers of email scams. Below is an image of my Twitter search page. It shows the different types of businesses and people who have encountered emailing scams and are spreading awareness or educating their viewers.



 After researching emailing scams, I think this concern is not overblown due to moral panic for many reasons. Each year some reports come from organizations, and they talk about the amount of money and data that gets lost. These organizations need to ensure that their employees are aware of fake emails that can endanger themselves and the organization. I have a cybersecurity internship job and one of the many things I was told about was emailing scams. I have a VPN application on my work computer and it protects me from the public servers that might have a hacker behind the crowd. The reporting and public debates on cybersecurity do match up with the concern about email scams. There are reports that state that these attacks are getting more cleaver due to social media. Social media has created more possibilities for hackers to explore and use against people. I used two of the 6 frames from the ACRL framework to discuss what was being understood well and what was being understood badly. For my first frame, I used authority as contextual and I talked about how the author Caroline Duncan talked about the significance of different types of email scams. She uses her blogs to provide organizations with information that is necessary for a company. The second frame I used is the information that has value. I talked about how valuable certain information can be when it comes to learning about the concerns. There were a few things that caught my attention for example the psychology of emailing scams is an important fact that people should know. People understand how significant it can be once you get hacked however, what is not understood well is knowing the difference between a fake email and a real email. There is a lot of fake news however, Emailing scams are a real concern and they are getting trickier as technology advances.

SOURCES

1. <https://theconversation.com/email-scams-are-getting-more-personal-they-even-fool-cybersecurity-experts-186009>
2. <https://www.alert-software.com/blog/cyber-security-awareness-email-to-employees-sample>
3. <https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams-2022>
4. <https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full>
5. <https://www.sciencedirect.com/science/article/abs/pii/S1361372310700658>
6. <https://twitter.com/search?q=phishing%20attack%20was%20sent%20to%20me&src=typed_query&f=live>
7. <https://morrispsych.com/why-so-many-people-fall-for-scams-by-kenneth-freundlich-ph-d/>