Evolution of Social Engineering Attacks and Prevention

Patrick Nguyen, Paige Hensley, Aneesa Bell, Logan Whaley, and Emily Wyland
College of Business, University of Louisville
CIS 481-50-4232: Intro to Information Security
Dr. Andrew Wright
April 21, 2023

Executive Summary

Social engineering is a methodology that affects confidentiality, integrity and availability. It has seen noticeable changes and expansions because of the COVID-19 pandemic and technological advancements. Traditional methods include phishing, pretexting, and baiting. Attackers manipulate victims into giving personal information by creating a credible scenario or even offering exchanges for their personal information. These traditional methods have been adapted to attack different demographics on newer platforms. Where methods like phishing typically take place over email, a new form of malicious impersonation is taking shape on social media platforms. Account cloning and Attackers can now achieve the same ends with more modern means.

In addition to the adaptations made to move social engineering to social media, the techniques were also affected by the recent global pandemic. The rapid spread of COVID-19 led to the imposition of social restrictions as a means to decrease its impact. As a result, organizations sent employees home to work remotely. This caused an increase in digital communications like video conferencing and instant messaging. Financial services and the healthcare system are examples of industries affected by the pandemic.

Social engineering poses a significant threat to organizations, so it is important that companies in all industries prepare for the attacks and actively work to prevent them. One prevention method that could be used is auto flagging software. This software can be utilized to filter emails based on the content and/or the sender of the media received by a user. Many organizations also opt to implement training and provide educational resources to make their employees aware of the risks. These prevention methods are worth the implementation costs because they significantly decrease the risk that social engineering poses to corporations.

As technology forges ahead, AI is increasingly being used for online scams, including tools like deepfaking and chatbots utilized to execute social engineering attacks. Younger people, who generally have larger presences online, are becoming the primary targets of virtual identity fraud. The potential harm of AI being able to effectively impersonate humans goes beyond intentional damage from attackers. Now even legitimate companies support bots beginning to convince users that there is a human on the other end of the line. Greater societal understanding and education around the use of AI are necessary to prevent these kinds of attacks or confusion.

Table of Contents

History of Social Engineering

Pre-Covid

Prior to the COVID-19 pandemic, the idea of living life entirely online seemed to be reserved for future generations, with many hesitant ever to let it get that far. However, the pandemic brought about an unexpected shift in our daily lives, which led to the increased adoption of technology and digital platforms.

Prior to the COVID-19 pandemic, the idea of living life entirely online seemed to be reserved for future generations, with many hesitant ever to let it get that far. However, the pandemic ended up catapulting society towards this inevitability whether we liked it or not, leading to a massive adoption of new technology and digital platforms.

Social engineering refers to a type of scam where the attacker manipulates the victim into performing specific actions or divulging confidential information. This technique has been commonplace for many years and is often used to gain access to sensitive financial information or carry out cyberattacks. Prior to the COVID-19 pandemic, social engineering tactics were conducted primarily via phishing emails or phone calls. The attacker would then impersonate an unknown, but trusted, authority figure like a bank employee and get the victim to either verbally give out sensitive information or convince them to engage with malicious links/software.

Post-Covid

The urge to resume "normalcy" during the pandemic forced both consumers and businesses to adapt to the new digital landscape quickly, and typically without much forethought to security. This opened the way for attackers to take advantage of people's vulnerabilities and lack of familiarity with online security measures. The pandemic helped opened up new avenues for attackers, from social media platforms, and messaging apps, to video conferencing software.

Cybercriminals have also used the pandemic as a pretext to create fake news and misinformation campaigns to manipulate individuals. This disinformation can be used to both prime a particular target for a scam, or just generally create an environment more receptive to social engineering tactics.

All of these things, plus the rise in employees working from home, has created untold opportunities for cybercriminals to exploit vulnerabilities in both personal and professional settings.

Approaches to Attacks

Traditional Attacks

According to Okereafor, social engineering has emerged as a serious threat in the work environment impacting cybersecurity, data confidentiality, data integrity, and data availability. The term is often described as "Human Hacking" in the sense that it tricks people into disclosing confidential information allowing the attacker to gain access to networks or personal accounts (Sushruth, Reddy, Chandavarkar et al., 2021), Reddy, Chandavarkar et al., 2021). Lack of structure and training is often a result of this occurrence in the work environment, and there are many methods used against users. Skills involved with social engineering can play a role in facilitating and preventing cyber attacks (Okereafor & Adelaiye, 2020). Cyber attacks generally use social engineering to exploit users, but some programs can educate users on how to protect themselves from falling into these scams.

To begin, we will discuss the traditional methods of social engineering. The first threat is phishing. This form of social engineering comes in many forms including spear phishing, email phishing, and vishing. Phishing is often thought of as an attack where it provides what appears to be an impersonation of a known person, brand, or high-profile personality (Okereafor & Adelaiye, 2020). However, code is embedded within the email that redirects replies to a third-party site to extract information. Propagation of malware generally occurs with this which can cause harm and undesirable outcomes to the victim's computer or digital asset. Some information gathered from this form of social engineering consists of bank information, names, addresses, social security numbers, and much more (Whiteman, 2017). As stated previously, phishing attacks do impersonate someone and seem legitimate to some users. Even so, poorly constructed emails can still cause some users to click on links or attached files (Whiteman, 2017).

Pretexting is another form of social engineering where attackers create a scenario involving an authority figure. Figures in pretexting could include government officials, IT technicians, or even higher-ups in the workplace. This impersonation needs information to confirm the target/user's identity to trick them into revealing confidential information. These attacks differ from phishing in the sense that it relies on building a false sense of trust with the victim (Whiteman, 2017). Phishing often uses fear and urgency to take advantage of users (Whiteman, 2017). Once trust is established with the victim, gathering information is much

easier for the attacker. However, the attacker must maintain credibility (Whiteman, 2017). Holes in the alias, story, or identity can make it known that a target is being scammed.

Baiting is another form of social engineering that is similar to phishing in the sense of how personal information is obtained (Whiteman, 2017). However, the attacker promises something in exchange for personal information (Lohani). Exchanges could include money, technology, and anything of value to the victim. Whiteman elaborates on an example of baiting through infected USB drives. These drives are distributed throughout the organization and allow the attacker to access machines when they are plugged into the device. Whiteman then quotes Beckers that this threat could occur with the distribution of free USB drives.

Social Media - The New Frontier

As new forms of online communication develop, attackers who employ social engineering have adapted and expanded their methodologies to attack technology users in new ways. According to a recent survey by YouGov, 35% of Internet users report that they have experienced hacking with one of their social media accounts with 13% of this group having this type of incident occur more than once (2018). One approach that attackers may take when trying to manipulate social media users is to gain access to the target's social media account and send messages and create posts while posing as that user. A hacker can access a user's account using dictionary or brute force attacks and impersonate the user to communicate with his or her followers. This attack is known as social media impersonation fraud.

Impersonation via social media is a trend that has personally affected multiple members of our team. If an individual has a public account on a social media platform, any user can view the individual's name, photos, and other personally identifiable information (PII). Those who want to take advantage of this transparency and use the information with malicious intent have started using a new exploitation tactic. The new tactic–that takes far less time and effort than hacking into an account using various password attacks–is account cloning. This attack is a form of identity theft and is used to gain the trust of individuals who have a relationship with the user being impersonated. Social media impersonation fraud occurs when an attacker creates a fake account and uses the victim's photos and content to populate the page. From there, the attacker will message people that the victim follows to either extort money or other information from

them. The attacker could also create posts on the fake account to further exploit the victim's followers or damage the victim's reputation.

Some attackers may reach beyond impersonating individuals and will pose as an organization's social media account. This can be incredibly damaging for the organization's brand image. Attackers who impersonate organizations may do so for one of two reasons: theft or activism.

The first approach is carried out with the intent of extorting money or other critical information from users who follow the company's social media account. The attackers accomplish this by creating an account with a very similar handle and exactly the same content as that of the company. This gains the trust of unsuspecting users because the differences between the real account and the fake account are not quickly noticed. From there, the attacker can create posts with links that would plant viruses or worms on users' computers to steal their information. The attacker could also create a post that prompts users to input their personal information (ie. bank account information) which can be used for financial theft.

Account cloning tends to be less damaging than impersonation fraud because these accounts can be quickly reported and are more easy to identify as fraudulent. Grainy photos, misspellings, and a stark follower-to-following ratio typically raise red flags for other social media users to be wary. However, with the changes being implemented on Twitter by Elon Musk, the line between real and fake has become more blurred.

When Elon Musk became the CEO of Twitter, he commercialized a system that once helped prove the authenticity of user accounts. The original process for receiving a verification icon required the submission of documentation and long processing times. Musk changed what it means to be a "Verified Account" by allowing users to purchase the status for a small monthly fee of $8 which gives them a blue check mark beside their account handle (Twitter Help Center). Now, fake accounts can convey status and validity without actually possessing it.

The use of account cloning in conjunction with the purchase of an account verification on Twitter invokes some of the principles of social engineering but can also help carry out agendas like a hacktivist. Attackers will create a fake account, pay the monthly fee to increase users' trust, and make posts that will damage the brand's image. Some users may identify the account as an impersonation and dismiss the claims made in its posts. However, as companies like Eli

Lilly have experienced, this type of attack can attract a lot of unwanted attention and lead to major financial losses.

Eli Lilly is a pharmaceutical giant that is known for its production of insulin. One Twitter user saw the new verification process as an opportunity to joke about the skyrocketing prices of vital medication. As Camryn Mata–staff reporter at Seattle University's student newspaper–so eloquently said, "In a nine-word post, one Twitter user brought a multi-billion dollar pharmaceutical company's stock down four percent," (2022). Although this satirical tweet was not created with the intention of stealing from people like social engineering messages, it highlights the dangers of treating credibility like a commodity. If a fake account like the one impersonating Eli Lilly had taken their attack just one step further by requesting that users log into an account or enter their payment information, it could have been even more damaging. Someone who wants to fool Twitter users by posing as a company can essentially purchase their trust and utilize the platform as a medium for social engineering.

Although the attack on Eli Lilly was not social engineering in the traditional sense, it paved the way for other attackers to use account cloning to carry out social engineering on the microblogging platform. The haphazard distribution of "verification" labels may lead to the diminished credibility of all accounts.

Target Profiling

The COVID-19 pandemic marked an unprecedented event for billions of citizens. Countries imposed social restrictions to decrease the risk of spreading the COVID-19 virus, and, as a result, the use of computers became essential for communication. Importantly, restrictions such as curfews had led to lower crime rates. However, cybercrime has risen tremendously since the beginning of the pandemic (Sushruth, Reddy, Chandavarkar et al., 2021). The widespread use of digital technology has led to several increased threats to organizations and society as a whole. Researchers Joel Chigada and Rujeko Madzinga adopted a systematic literature review regarding targeted corporations, the healthcare industry, and government agencies.

To begin, the authors created a methodology for collecting information from December 2019 to May 2020 period (Chigada & Madzinga, 2021). The methodology employed three key questions which were analyzed, synthesized, and disseminated using meta-analysis techniques with clear inclusion and exclusion in place (Chigada & Madzinga, 2021). Using systematic

research allows for a review to identify cybercrimes committed during the pandemic. Relevant evidence allows researchers to use the results to inform practice, policy, and further research (Chigada & Madzinga, 2021). Cybercrime during the pandemic targeted systems or internet-enabled devices for people working remotely, which was common during the pandemic (Chigada & Madzinga, 2021). This led to a lack of security protocols, heightened espionage, phishing campaigns, and denial of service attacks (Chigada, 2021, as cited in Quada, 2020).

Financial services were one targeted set of corporations during the COVID-19 pandemic. Global systems were attacked and the United States lost millions of dollars through cybercrime (Chigada & Madzinga, 2021). Financial services were attacked through phishing, malware, and ransomware. Financial institutions were forced to move away from physical branches to mobile services and digital communications, thus, creating exposures to risks (Chigada & Madzinga, 2021). Clients conducted business remotely and had no security protocols, firewalls, internet access controls, or routine updates. That being said, Chigada and Madzinga determined that cyberattacks and threats to financial institutions increased by more than 238% globally (Chigada & Madzinga, 2021). Out of the tactics presented, phishing was the primary source of attacks. Additionally, business-email-compromise was used against financial institutions. Chigada uses information from Dixon and Balson stating that criminals are using the pandemic as leverage to impersonate workers in companies. The First National Bank, Standard Bank, and Nedbank were identified as recent targets of this tactic leading to 1.7 million user accounts being compromised (Chigada & Madzinga, 2021).

The Healthcare system was another organization that suffered increased cyberattacks during the COVID-19 Pandemic. Healthcare organizations generally rely on Information & Communication Technologies (ICT) applications that offer e-healthcare to patients and healthcare personnel (Chigada & Madzinga, 2021). COVID-19 has exposed these services causing an overload of resources and responding workers. The World Health Organization and the Center for Disease Control were two organizations heavily affected by the pandemic (Chigada & Madzinga, 2021). Criminals initiated spear-phishing attacks, imitating the WHO and CDC, to launch malicious attacks. Attackers used the pandemic to spread malware, and ransomware, and created fraudulent websites to prey on users (Chigada, 2021, as cited in Balsom, 2020). The CDC and the WHO are crucial elements to the pandemic. Society relies on

them for information, and it makes it tremendously difficult to trust sources considering the circumstances with cybercrime.

Approaches to Prevention

Auto Flagging Software

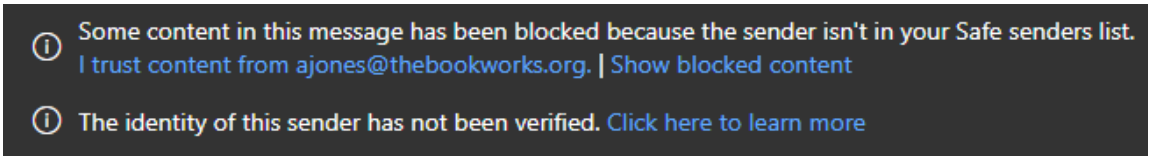
An approach to mitigate social engineering attacks is the use of auto flagging software. Organizations can use software that can flag incoming content based on predetermined standards and policies. When potentially harmful subject matter is identified, it can be sent to the appropriate security personnel for analysis. At this point, security personnel can determine whether the content poses a legitimate threat to the organization.

One way auto flagging can be implemented is through content filtering. The software scans content for specific words or phrases that are commonly used in social engineering attacks. Some examples of phrases used would be “update your healthcare info”, “verify your password”, “account has been locked”, and “important from human resources” (Ranger).
Another way auto flagging works is through contact filtering. The software filters incoming content based on the presented identity of the sender.

Furthermore, auto flagging software can also be used for educational purposes within organizations. The auto flagging software can be programmed to display warning messages to the user when suspicious content is detected. The preprogrammed message can provide information on how to identify social engineering attacks.

The University of Louisville administers contact filtering flagging through Microsoft Outlook, the university E-mail client software. If the sender is from outside of the organization and is not on an individual's “Safe Sender” list, the email will be flagged. In addition to the warnings displayed to the user, it also offers the user a few links to learn more information about phishing from Microsoft Support.

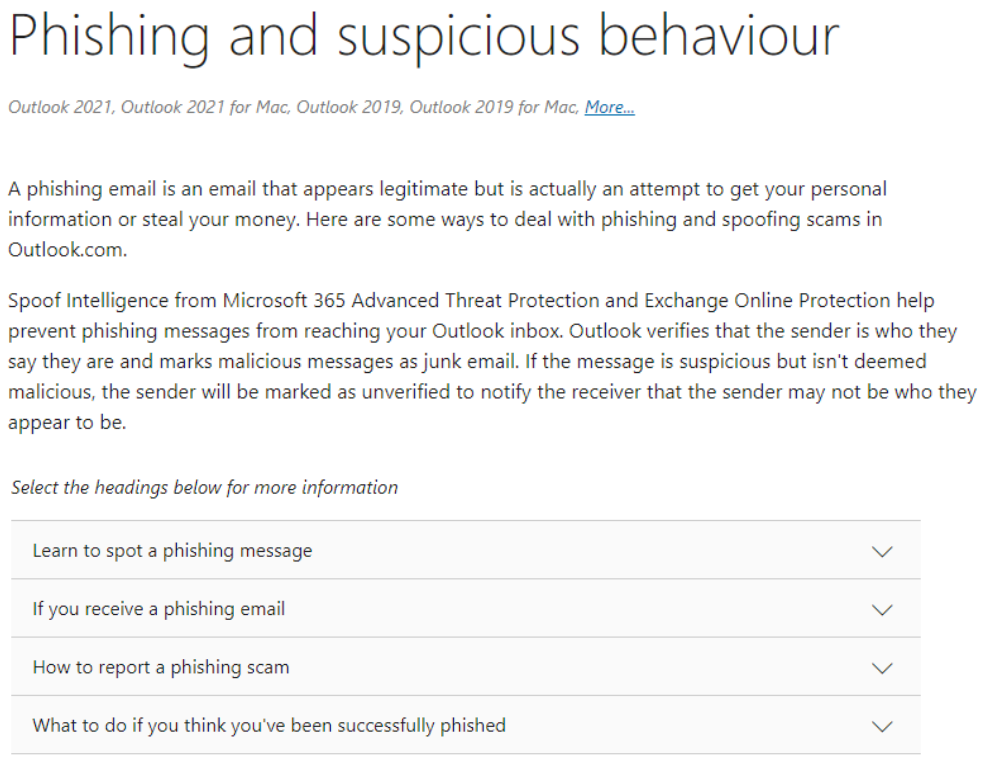
Figure 1:



(A. Bell)

Figure 1 shows how content is blocked and flagged from senders that are not on an individual's Safe Senders list. This is a screenshot from the University of Louisville Microsoft Outlook of Aneesa Bell.

Figure 2:



(Microsoft Support)

Figure 2 shows how a user can learn more through the links in the warning displayed in Figure 1

However, there are a few downsides to the use of auto flagging software in organizations. Based on experience with the University of Louisville, many "false alarms" are signaled through the Microsoft Outlook sender auto flagging system. When many harmless emails get flagged, it degrades the value of the warning to the user. When users start ignoring the warnings, the system is essentially rendered useless. Another downside is that auto flagging software cannot protect

against all types of social engineering attacks. For instance, this tactic has few viable applications to attacks that occur over the phone or an organization's video conferencing platform.

All in all, auto flagging software is merely a preventative measure. While it is valuable, it is not comprehensive enough to provide ample protection. In terms of protecting an organization, it needs to be integrated with other security measures.

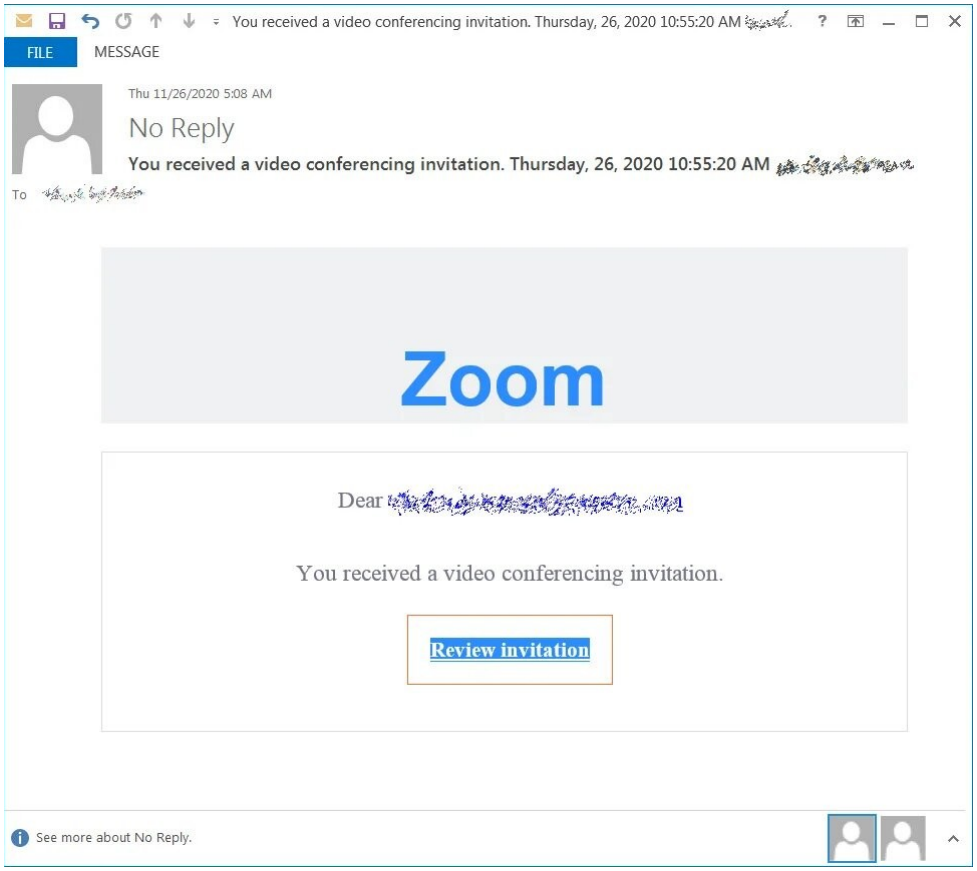
Virtual Meetings and Two Factor Authentication

Another common form of Social Engineering is Vishing. Vishing, also known as voice phishing, is most commonly associated with spam calls. One of the most terrifying things about Vishing is the absolutely absurd rate at which it occurs. Hundreds of millions of spam calls go out everyday through the world, amounting to billions of people being vulnerable to Social engineering attacks (Jones, 2022). In the past there was little to do to prevent Vishing attacks. Speaking over the phone was the main source of communication between people other than talking face to face. As technology has advanced, thankfully that isn't the case anymore, which is why our second approach to negating social engineering is the continued implementation of virtual meeting services.

In the midst of the pandemic and its decline companies have implemented virtual meetings through services like Zoom or Microsoft Teams as a substitute to in person conferences. These platforms proved to be a great help in a time where meeting face to face with one's coworkers or classmates wasn't a possibility. The ability to see, hear, and access what each person may be working on was a game changer. So much so that Teams, Zoom, and other virtual meeting platforms still are heavily used today! One of the most significant aspects of these virtual meeting platforms is the fact that there is an additional layer of trust or security compared to the typical phone call. Having the ability to see the person you are conversing with severely lowers a social engineer's chances of impersonating someone you may know. Seeing one's face, their surroundings, what they may be wearing, it all brings additional information to a party that may have to determine whether this person is really who they say they are. It may also give one the chance to ask to see the other person's ID, another form of verification that would allow them to ensure the person they are speaking with is the one they claim to be. This extra layer of security via online communication is a great start, but there are still some vulnerabilities with it.

Like with all things, eventually social engineers were able to find a weakness with virtual meetings. One of the most common ways to invite someone to a meeting is via a unique url. When the recipient then clicks on said link, it would take them to the meeting and prompt them to join. Social engineers were able to twist this user-friendly feature to their advantage, emailing people fake links that when clicked would open up malware on their computer that looked almost identical to the login screen for the service the user was trying to access.

Figure 3:



(Threatcop, 2022)

Figure 3 shows how one might be coerced into clicking a link that seems like a legitimate Zoom invite

As one might expect, this proved to be very effective and compromised sensitive information, all just by making a copycat link. That is why in addition to continuing to implement online communication via virtual teams to negate social engineering, using multi factor authentication is of equal importance. Multi factor authentication requires the user to input multiple forms of identifiers in order to access a file, app, or account. These can be two or more

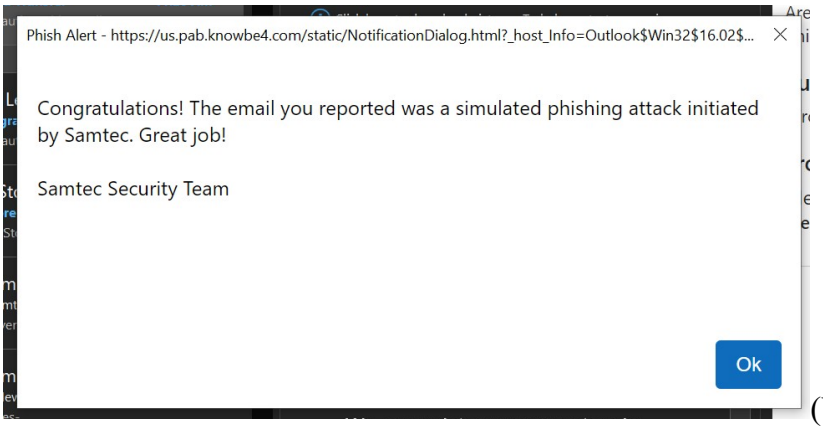
of: something the user knows, something the user has, or something the user is. A common form of multi factor authentication is inputting one's password, and then inputting a code that was received from another device, like their cell phone. The main advantage to multi factor authentication is that it prevents social engineers from being able to access one's account or files even if they are able to successfully obtain one of the multiple forms of identification. This added level of security is invaluable to everyday people and corporations alike. Both Microsoft Teams and Zoom have the option for multi factor authentication and should be enabled on any company device that has those apps installed (Zoom) (Microsoft).

Simulated Phishing Attacks

Phishing is one of the most frequently used forms of social engineering. According to some statistics published by an IT support company called AAG, "Phishing is the most common form of cyber crime, with an estimated 3.4 billion spam emails sent every day," (Griffith). Because phishing attacks are so common, it is important for organizations to ensure that their employees can identify a phishing email.

Samtec Incorporated, a local electronic interconnect solutions manufacturer, uses simulated phishing attacks to encourage its employees to be alert. When employees correctly identify a phishing attack using Microsoft Outlook's "Phish Alert Report" button, they receive a congratulatory message like the one in the figure below . If they fail to identify the simulated attack and click any of the links or attachments, they will be flagged and required to retake the company's email security training. This prevention method helps train employees to be on alert by exposing them to emails like those they might actually receive from an attacker. It also provides the company with data regarding how many employees would fall victim to an actual attack. The internal data (shown in Figure 5) gives the company a better understanding of the effectiveness of their training and the threat level that their employees pose to their information security.

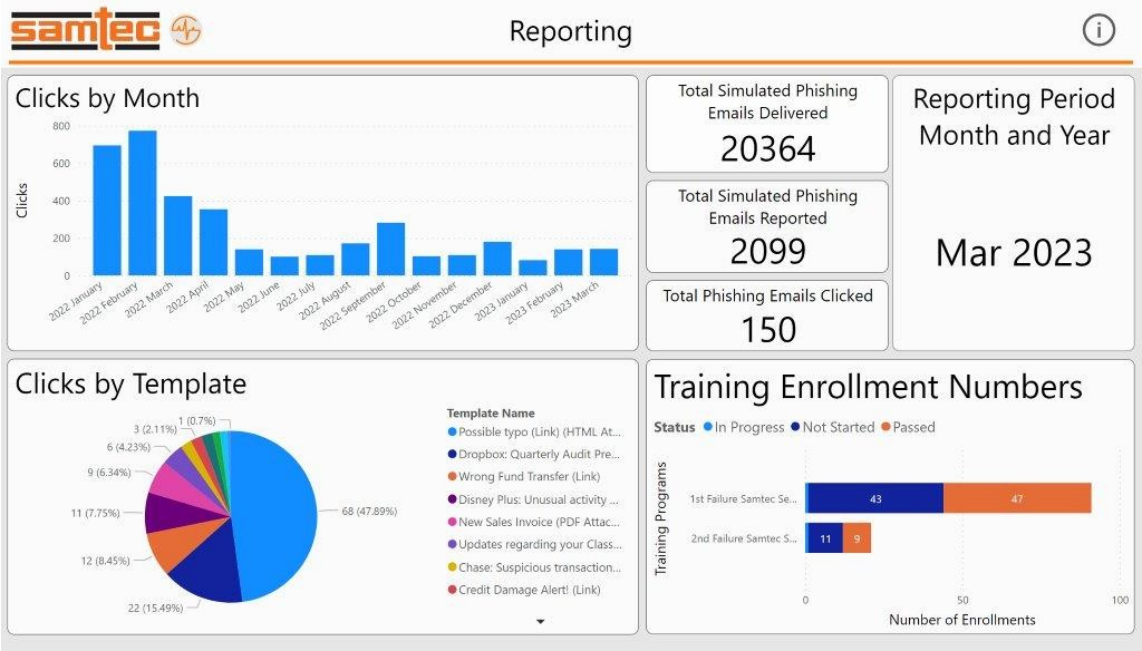
Figure 4:



(Wyland, 2023)

Figure 4 shows an example of a congratulatory message from Samtec's Security Team when a simulated phishing email is correctly identified

Figure 5:



(Hardin, 2023)

Figure 5 shows the data received from Samtec's simulated phishing email 2022-2023 campaign.

Recommended Approach to Prevention

Because it is not financially feasible or wholly practical for an organization to implement a multitude of the aforementioned prevention methods, one should be selective when making

these decisions. The company must consider the methods' effectiveness and cost when making choices that will impact its information security. It is important to find the right mix of preventative measures that best supports the company's goals and practices.

The method that is incredibly effective and the easiest to implement within an established organization is training. Creating a course that alerts employees to the threat of social engineering and informs them as to how it may appear in their work life helps to increase awareness. The training should also include the process people should follow if they were to encounter a social engineering attack. These courses can be distributed through in-person classes or online presentations making them adaptable to the structure of any organization. A great addition for companies to include in their training regimen is the simulated phishing emails tactic. This helps test the waters and gives the information security team real data regarding the effectiveness of the company's current training method. They have proven to be effective where they are being utilized at Samtec, Inc. By implementing simulated phishing attacks in their KnowBe4 security campaign, Samtec's security team caused a significant decline in clicks within one year (see Figure 5).

The next prevention method that is slightly more costly and slightly less effective is auto flagging software. Implementing new software within an organization requires money and effort. However, the benefits are typically worth the sacrifices because this software will keep potential phishing scams from entering an employee's mailbox (see Figure 2). However, Type 1 and Type 2 errors often occur with this type of software. Emails that are not social engineering attacks may be wrongly flagged or an actual attack may slip under the radar.

The final method that a company may or may not choose to implement is two-factor authentication. This method is very effective at preventing attackers from accessing accounts, information, or even video conferencing sessions that they are not supposed to. However, it can create unnecessary inconveniences when used across multiple platforms and accounts. For example, having to authorize an email account, Microsoft account, and Zoom account at every login wastes time and energy.

With that being said, an organization must find what methods are the best fit based on the processes used in its departments and the receptiveness of its employees. It is important to construct training sessions in such a way that will have the greatest impact on people. This may

mean mandatory in-person classes for some companies or simulated phishing attacks for others. It is also important to keep in mind how employees value convenience as compared to security.

Future Outlook

The conversations about the potential that AI holds for automation have largely been centered around industry/production, with some trickle-down to "AI and You" consumer lifestyle efficiency products/services. However, society is already starting to feel the negative impact of AI on crime, faster than it sometimes feels the positive.

Social Engineering has long been restricted in certain mediums, such as voice calls and visual mediums like photos and video, by the cost associated with fabricating them. One could undoubtedly hire a voice actor or perform elaborate photoshop to convince a target that their uncle really was at the beach and in desperate need of money, but the benefit often does not outweigh the cost. However, like in many other industries, AI is cutting down on the cost of business operations for online scammers.

Figure 6:

(Vedova)

The low return on investment mentioned prior is why, historically, the elderly have been the most targeted demographic of financial fraud. Considered less tech-savvy and less likely to successfully report an instance of fraud on average, the risk vs reward was skewed much more in the attacker's favor. Interestingly, as more and more of everyday life gets moved online, young people are becoming the primary targets of online financial fraud. In an annual report by CPA Canada, it was found that 63% of 18-34 year-olds have experienced being a victim of financial fraud at least in their life. This number drops to 39% for ages 35-54 and 31% for those aged 55+.

Younger people also tend to have a larger personal presence online via social media accounts. This makes them prime targets for things like deepfaking. As stated in a Federal Trade Commission consumer alert, "All [the scammer] needs is a short audio clip of your family member's voice — which he could get from content posted online — and a voice-cloning program" for them to mimic a loved one convincingly. Figure 7 below demonstrates an example of a deepfake scam call.

Aside from convincingly mimicking the voice of important figures in a target's life, AI chatbots can remove much of the legwork of traditional chat-based social engineering scams. Advancements in Chatbot capabilities have made it more difficult for users to distinguish between real and automated communications. When asked to speak on how Large Language Models like ChatGPT and LaMDA are advancing the field of AI, cognitive scientist Gary Marcus said “I don’t think it’s an advance toward intelligence, it’s an advance toward fooling people that you have intelligence.” (Oremus) A sentiment that many share, and worry over.

Figure 7:

(Puig)

No longer do attackers have to resort to pre-planned conversations and canned responses (see Figure 7) when they want to automate/scale their activities. Instead, a fleet of AI-powered social media accounts could autonomously prime targets and execute scams. Meanwhile, another bot could be acting as the "IT Support Desk" for a scam site typosquatting a trusted organization.

The level to which AI can imitate sentience and personhood, however, has the potential to do harm far past the intentional misuse by attackers. Even legitimate company support bots are beginning to convince users that there is a human on the other end of the line.

Some believe that the language we use surrounding AI, primes users to believe that these models are more human-like than perhaps deserved. "We now have machines that can mindlessly generate words, but we haven't learned how to stop imagining a mind behind them," stated Emily M. Bender, a University of Washington professor of linguistics, "The terminology used with large language models, like "learning" or even "neural nets," creates a false analogy to the human brain." (Tiku)

The quickest way to help prevent these kinds of scams is a greater societal understanding of these terms and AI concepts. We can no longer get by on black-box thinking and allowing mysticism to surround this subject. The prevalence of deepfakes and AI chatbots in online fraud is just one of many reasons for increased awareness and education around the use of AI.

Conclusion

The COVID-19 pandemic has forever changed the landscape of social engineering tactics, with AI advancements not far behind in enabling more sophisticated attacks. Pre-Covid, social engineering attacks were primarily limited to traditional methods, like phone calls and emails. However, the online migration caused by the pandemic has opened up many new frontiers for attackers to exploit, such as social media platforms. Target profiles have also been shifting, with younger people being increasingly targeted due to their larger online presence. This is in stark opposition to Pre-Covid patterns where the primary target was those without internet experience, typically the elderly.

Auto-flagging software, virtual meetings with two-factor authentication, and simulated phishing attacks are some of the most common approaches to prevention that have emerged. Many organizations are still working to find more effective security measures, while others lag behind to the detriment of their users. Individuals and organizations must remain aware and

willing to adapt to evolving social engineering attacks, as AI will only continue to play a significant role in shaping the future of security.

References

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. SA Journal of Information Management, 23(1). https://doi.org/10.4102/sajim.v23i1.1277

Griffith, C. (2023, April 6). The latest phishing statistics (updated April 2023). Retrieved April 14, 2023, from https://aag-it.com/the-latest-phishing-statistics/#:~:text=Phishing%20is%20the%20most%20common,sent%20in%202022%20were%20spam.

Hardin, D. (2023, March). Security - KnowBe4 Phishing and Training Campaign - March 2023. Samtec, Inc. Retrieved April 5, 2023, from https://samtec.sharepoint.com/sites/ITNewsHub/SitePages/Security–KnowBe4-Phishing-and-Training-Campaign–March-2023

Harwell, D. (2022, November 14). A fake tweet sparked panic at Eli Lilly and may have cost Twitter Millions. The Washington Post. Retrieved April 9, 2023, from https://www.washingtonpost.com/technology/2022/11/14/twitter-fake-eli-lilly/

Hernandez, J. (2023, March 22). Scammers are using AI-generated voice clones, the FTC warns. *NPR*. Retrieved April 3, 2023, from https://www.npr.org/2023/03/22/1165448073/voice-clones-ai-scams-ftc

Jones, K. S., Armstrong, M. E., Tornblad, M. K. K., & Siami Namin, A. (2021). How social engineers use persuasion principles during vishing attacks. *Information & Computer Security*, *29*(2), 314–331. https://doi.org/10.1108/ICS-07-2020-0113

Mata, C. (2022, November 30). What the healthcare? how one fake tweet sparked an assessment of U.S. Healthcare System. The Spectator. Retrieved April 7, 2023, from https://seattlespectator.com/2022/11/30/what-the-healthcare-how-one-fake-tweet-sparked-an-assessment-of-u-s-healthcare-system/#

Microsoft. (n.d.). *How different technologies effect Microsoft teams sign-on, including restricting sign-on, and sign-in behaviors. - microsoft teams*. How different technologies effect Microsoft Teams sign-on, including restricting sign-on, and sign-in behaviors. - Microsoft Teams | Microsoft Learn. Retrieved April 17, 2023, from https://learn.microsoft.com/en-us/microsoftteams/sign-in-teams

"Microsoft." *Microsoft Support*, https://support.microsoft.com/en-us/office/phishing-and-suspicious-behaviour-0d882ea5-eedc-4bed-aebc-079ffa1105a3?redirectSourcePath=%252farticle%252f3d44102b-6ce3-4f7c-a359-b623bec82206.

Okereafor, K., & Adelaiye, O. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. International Journal of Recent Engineering Research and Development (IJRERD), 5(7), 61–72. https://doi.org/https://www.researchgate.net/publication/343318105_Randomized_Cyber_Attack_Simulation_Model_A_Cybersecurity_Mitigation_Proposal_for_Post_COVID-19_Digital_Era

Oremus, W. (2022, June 17). *Analysis | Google's AI passed a famous test — and showed how the test is broken*. The Washington Post. Retrieved April 13, 2023, from https://www.washingtonpost.com/technology/2022/06/17/google-ai-lamda-turing-test/

Puig, A. (2023, March 20). *Scammers use AI to enhance their family emergency schemes*. Federal Trade Commission. Retrieved April 3, 2023, from https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes

Ranger, Taran. "The Most Effective Phishing Phrases." *Cynation*, 24 Nov. 2017, https://www.cynation.com/the-most-effective-phishing-phrases/.

Threatcop. (2022, October 28). *Zoom phishing attacks: A method for scammers*. Threatcop. Retrieved April 3, 2023, from https://threatcop.com/blog/zoom-phishing-attacks/#:~:text=Zoom%20Phishing%20Attacks%20Use%20its,receiving%20calls

%20through%20this%20app.&text=The%20display%20name%20in%20the,us%E2%80%9D.

Tiku, N. (2022, June 11). *The Google engineer who thinks the company's AI has come to life*. The Washington Post. Retrieved April 13, 2023, from https://www.washingtonpost.com/technology/2022/06/11/google-ai-lamda-blake-lemoine/

Unlikely targets: More young Canadians report being a victim of financial fraud than older Canadians. (2023, February 15). CPA Canada. Retrieved April 3, 2023, from https://www.cpacanada.ca/en/the-cpa-profession/about-cpa-canada/media-centre/2023/february/cpa-canada-fraud-survey-2023

Vedova, H. (2023, February 23). *New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022*. Federal Trade Commission. Retrieved April 13, 2023, from https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social engineering attacks during the COVID-19 pandemic. SN Computer Science, 2(2), 77–77. https://doi.org/10.1007/s42979-020-00443-1

Whiteman,Jack R., I.,II. (2017). Social Engneering: Humans are the Prominent Reason for the Continuance of These Types of Attacks (Order No. 10684196). Available from ProQuest Dissertations & Theses Global. (2007620740). Retrieved from: http://echo.louisville.edu/login?url=https://www.proquest.com/dissertations-theses/social-engneering-humans-are-prominent-reason/docview/2007620740/se-2

YouGov. (2018). The economist/YouGov poll August 17 - 20, 2019 - 1500 US adult citizens. Retrieved April 15, 2023, from

https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/u4gcv1suy6/econTabReport.pdf

Zoom. (n.d.). *Managing Two-factor authentication (2FA) – zoom support*. Managing two-factor authentication (2FA). Retrieved April 17, 2023, from https://support.zoom.us/hc/en-us/articles/360038247071-Managing-two-factor-authentication-2FA-