SOCIAL MEDIA IMPERSONATION AS A CYBERSECURITY THREAT[1]

Radoslav BALTEZAREVIĆ
Senior Research Fellow, Institute of International Politics and Economics, Belgrade, Republic of Serbia
ORCID ID: https://orcid.org/0000-0001-7162-3510
Ivana BALTEZAREVIĆ
Associate Professor, Faculty of Law, Megatrend University, Belgrade, Republic of Serbia
ORCID ID: https://orcid.org/0000-0003-4605-1420

Abstract
Social media platforms function as a virtual environment where billions of people communicate, exchange knowledge, and develop relationships. Because of the enormous amount of personal information that is shared on these platforms, hackers find them to be appealing targets. The act of making fictitious social media pages, accounts, or identities that closely resemble real ones is known as social media impersonation. These accounts are meant to trick people into thinking they are communicating with a reliable person or entity, which greatly undermines their cybersecurity. Social engineering is a broader term for a set of techniques that include psychological manipulation, including the act of impersonating genuine individuals on social media. The goal is to deceive victims into divulging private information or into acting against their better judgment. Social media impersonation may involve credit card, computer, and financial fraud, harassment, and other crimes that are covered by this Act, depending on the seriousness of the conduct and their outcomes. Although security precautions are put in place by social media sites to safeguard user data, they are not infallible. Cybercriminals take advantage of platform security flaws, frequently using creative methods, to obtain unauthorized access to user accounts and compromise personal data. The battle against impersonation on social media is not one that belongs to one person. It necessitates a coordinated, societal approach based on knowledge and instruction.
Keywords: Social Media Impersonation, Cybersecurity, Cybercriminals, Virtual Environment.

Introduction

Digital technology has evolved into an essential part of modern life. On the other hand, there is a flip side to this narrative, which suggests that cyberspace serves as a favourable setting for a variety of illicit activities. Cybercriminals have the potential to seriously hurt digital users financially and emotionally. These actions turn into a significant issue that affects not just the states but also the general public and small and large business systems (Baltezarevic & Baltezarevic, 2021a). When users of social media pretend to be someone else, it's a frequent phenomenon known as impersonation. By comparing the impersonator's profile page details with those of the victim, it is possible to perpetrate impersonation. The goal of impersonators is to harm, harass, intimidate, and deceive another individual (Page, 2014).

Cybercriminals use impersonation attacks, in which they assume the identity of a well-known individual or group in order to steal money or sensitive information. Attackers persuade

[1] The paper presents findings of a study developed as a part of the research project "Serbia and challenges in international relations in 2024", financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade during year 2024.

gullible victims to perform common acts like sharing a file, opening a link, or paying an invoice by using social engineering techniques to assume an identity, either by breaking into an account or fabricating a lookalike (Abnormalsecurity, 2024). Imitating someone on social media can have detrimental effects for both the individual doing the impersonation and the people they deceive. It may result in the dissemination of misleading information, scams, harassment, cyberbullying, and digital identity theft. Reputational harm can also occur to people and companies when their name or brand is utilized maliciously. It is critical that people and businesses understand social media impersonation and take preventative action to safeguard themselves against this type of online fraud. This can involve keeping a close eye on their online presence, alerting the appropriate social media platforms to phony identities, warning staff members about the dangers, and enforcing stringent privacy settings on social media accounts (Bolster AI, 2024).

Impersonations can take many different forms, such as using a false account, social media account hijacking, executive impersonation, personal account impersonation, and brand impersonation. Credential stuffing is one of the most common techniques used to expose social network accounts. Passwords and usernames are among the details exposed by data breaches; with these credentials, hackers can try to access various services. Cybercriminals can locate a matched identity on a social network that accepts those credentials and take over the account if users have reused the disclosed passwords. From there, it only takes an attacker a few clicks to trick someone into downloading malware, making a donation, or engaging in other privacy-invading activities (Weber, 2023). According to estimates from the U.S. Federal Bureau of Investigation (FBI), impersonation assaults have cost more than $5.3 billion in losses worldwide. Therefore, we all need to develop strong digital threat awareness abilities because so much of our lives now takes place online. These skills include recognizing the warning signals of digital impersonation and comprehending its nature (Marr, 2023).

Literature review

A frequent occurrence on almost all social media sites is impersonation. It is essential to the creation and distribution of content on online social networks (Zarei et al., 2019). By identifying the impersonated user through their profile, a social media user can take on their true identity. Because impersonators frequently attempt to conceal real accounts on social media by creating similar profiles and disseminating authentic information, it can be challenging to tell authentic postings apart from fraudulent ones (Zarei et al., 2020).

The phony social media profile may include details that are wholly made up or belong to someone else. The flexibility in adopting a virtual persona stem from the seclusion afforded by social media platforms. The primary challenge in fighting and detecting crimes related to social media platforms is the lack of appropriate detection mechanisms for internet users (Hoffmeister, 2014). For instance, accounts that pretend to be well-known individuals or representatives of prominent businesses, etc. are examples of impersonators or imposters. Such impersonators are available on all major social media platforms. Celebrities, influencers, companies, and public figures of various levels of notoriety use Instagram extensively. While many impersonators are probably harmless, there are also accounts that are maliciously fake. These frequently have predetermined strategies that include making accounts seem more popular than they actually are, creating deceptive engagements, abusing brands, and producing pre-planned, unreliable content (Zarei et al., 2020).

There are two primary categories of impersonators: bot impersonators and fan impersonators. Bot accounts are publicly available fraudulent accounts or social bots that mimic real people and usually generate simple content. Usually, these bots are just basic Instagram accounts with the default settings, which don't include a biography, full name, or occasionally even any profile photos. These bots have a small number of followers, yet they follow a lot of other accounts. A fan-created and -maintained account regarding a celebrity, object, or specific

phenomenon is known as a fan impersonator. These accounts are run by fans and have a human operator. Fans are more popular than bots when it comes to following, having a biography, being fully public, and typically using a URL on their profiles (Ferrara et al., 2016). Identity theft is not the same as impersonation, despite their similarities. A person who impersonates a police officer, a doctor, or a solicitor is not breaking the law in and of itself when they do so. On the other hand, when it comes to brand impersonation, the steps involved in carrying out the crime are illegal, including financial fraud, privacy violations, and trademark infringement (Porta, 2023).

Sharing anything on social media in someone else's identity might result in criminal charges and other severe legal repercussions. Legality varies by jurisdiction, with many laws prohibiting impersonation when it is done deliberately to cause injury, fraud, harassment, or other bad effects on others. While parody and satire accounts are usually protected as long as they make it obvious that they are humorous in order to prevent deceiving the public, not all forms of impersonation are prohibited. Depending on the seriousness of the conduct and its consequences, several states have passed laws prohibiting social media impersonation, with fines to jail time as possible punishments (Horsey, 2024). Phishing schemes, counterfeiting, fake news, and scanning or frauds are only a few examples of the various forms of impersonation. Scammers use phishing to get hold of private information from customers, like bank account details, passwords, and social security numbers. These behaviours have the greatest impact on the financial sector. Fraudsters attempt to trick clients by offering them fake goods. In order to divert users to a website that is not part of the social network where the transaction is being completed, they frequently ran aggressive advertising efforts. In the luxury and fashion sectors, this approach is very pertinent. In order to spread misleading information and news, fake news accounts pose as prominent figures, and celebrities (Weber, 2023).

The following are some typical instances of impersonation attacks: a) CEO fraud: Also referred to as executive impersonation or whaling, this type of fraud involves an attacker pretending to be an executive. Then, they make contact with gullible workers to demand private information or invoice payment. b) Supply chain compromise: Phishing attacks are used by attackers to specifically target the supply chain of a company. If they are successful, they will pretend to be the seller and ask for invoice payment using their actual account. c) Account takeover: An employee's account gets compromised by an attacker who then uses it to impersonate a colleague. Account takeover assaults have comparable demands for data sharing and invoice payment as other impersonation schemes (Abnormalsecurity, 2024). In a sort of impersonation attack known as "domain spoofing," a cybercriminal buys a domain name that sounds similar to the target's and uses it to host a copy of the target's website. Cybercriminals can fake the domain name using a variety of methods, such as typo squatting, domain masking, establishing lookalike domains, or using a URL shortener tool to conceal the true domain name. When victims of the fraud engage with a spoof domain that mimics the target organization's website, they are actually providing cybercriminals with their personal information. Customers primarily engage with brands through mobile applications, particularly those that demand particular login credentials (such as banks). The absence of regulation, or the delayed regulation of internet app stores, is what bad actors rely on, and they frequently make similar programs to trick people. Digital enemies, for instance, frequently target the financial services sector by making phony mobile applications that mimic the real apps of well-known financial services firms. Usually, these apps are promoted in unregulated app shops. When a target downloads the fake software and attempts to log in using their safe access credentials, they are actually giving those details to online thieves who will exploit them to defraud the gullible victim of their money (Zerofox, 2022).

Brand impersonation is a type of phishing cyberattack in which the attacker pretends to be a reputable company in order to obtain sensitive information from its targets. Every brand,

regardless of size, is vulnerable to impersonation techniques. However, because these companies have a vast user base, attackers frequently pose as well-known companies like Google, Microsoft, Facebook, and Amazon. In this case, a brand imposter would craft a false message to ask a client or user of these brands for personal information. The loss of credibility and reputation that impersonated brands experience makes brand imitation costly as well (Darktrace, 2024). Cybercriminals eroded the trust of customers who fulfilled their needs and desires through digital purchasing by exploiting data and engaging in actions that may harm Internet users both mentally and physically (Baltezarević & Baltezarević, 2021b). In November 2022, CNN reported that an avalanche of phony accounts impersonating celebrities and companies was observed on Twitter following the platform's transition to a paid verification scheme (Astound, 2024). Someone pretending to be the massive pharmaceutical company (Eli Lilly & Co) claimed to tweet that insulin would be free. The phony tweet was live for hours after Eli Lilly denied it on their account. At the end, Eli Lilly's stock ultimately fell 4.37%, resulting in a loss of more than $15 billion (Rylah, 2022).

In order to identify fake accounts and efforts at impersonation, artificial intelligence (AI) and machine learning technologies are getting more advanced. These tools make it easier to spot and delete these accounts by analysing patterns of behaviour that point to fraudulent activity. More stringent verification procedures for account creation and recovery are probably going to be implemented by social media networks. To make it more difficult for impersonators to create fake accounts, this may entail needing extra forms of identification, biometric data, or other verification techniques (Singh, 2024). It is indisputable that human-machine collaboration still results in the greatest performance gains, even if artificial intelligence technology has shown to be incredibly successful in low-level, repetitive jobs (Baltezarević, 2023). Although social network moderation teams say they try their hardest to delete fake accounts, many go undetected or uninstalled until it's too late. There are still a ton of fake accounts on social media sites, despite their efforts as well as those of private citizens and security organizations. Facebook has successfully eliminated billions of fraudulent profiles, but the company projects that approximately 90 million accounts, or 5% of its total user base, are fraudulent. Similarly, Instagram estimates that approximately 95 million identities on its platform are fraudulent (Chiavetta, 2024). By enhancing online privacy, informing users about potential risks, and putting platform-level solutions into place, impersonation schemes can be avoided and protected against. It could significantly lower risk of being a victim of social media impersonation by implementing these precautions (Astound, 2024).

Conclusion

In the modern digital environment, impersonation attacks are becoming a bigger worry, particularly with the rise in the usage of social media for both personal and professional reasons. These assaults have serious dangers and repercussions for both persons and organizations. Cyber criminals can obtain sensitive data using a range of methods, including malware, social engineering, and phishing scams. Upon gaining access to accounts, they can utilize personal data to perpetrate identity fraud, initiate social engineering schemes against acquaintances, and disseminate inaccurate information about users or their companies. Malicious actors have the ability to damage the reputation of their target by acting inauthentically and carrying out immoral or unlawful actions in their name.

Sharing anything on social media in someone else's identity might result in criminal charges and other serious legal consequences. Legality varies by jurisdiction, with many laws prohibiting impersonation when it is done deliberately to cause injury, fraud, harassment, or other bad effects on others. Internet users and their businesses can be better protected from danger by having a greater awareness of the many forms of impersonation, their motivations, and the potential outcomes. Maintaining security, credibility, and trust in the online

environment can be facilitated by putting best practices for prevention into effect and having a well-thought-out plan for handling impersonation attacks.

References

Abnormalsecurity (2024). What Is an Impersonation Attack? How Attackers Trick Victims Into Paying Invoices or Sharing Private Data. Retrieved from: https://abnormalsecurity.com/glossary/impersonation-attacks (Accessed: 27.08.2024.)

Astound (2024). Social media impersonation: How to identify, prevent and respond. Retrieved from: https://www.astound.com/learn/internet/social-media-impersonation/(Accessed: 26.08.2024.)

Baltezarevic, R. & Baltezarevic, I. (2021a). The Dangers and Threats that Digital Users Face in Cyberspace. IPSI Transactions on Internet Research, Vol. 17, No. 1, January 2021, pp. 46-52.

Baltezarević, I. & Baltezarević, R. (2021b). Sajber bezbednost: izgradnja digitalnog poverenja, *Megatrend Revija*, Vol. 18 (4). pp. 269-280. DOI: 10.5937/MegRev2104269B

Baltezarević, R. (2023). Uticaj veštačke inteligencije na globalnu ekonomiju. *Megatrend revija,* Vol. 20, № 3, 2023: 13–24. DOI: 10.5937/MegRev2303013B

Bolster AI (2024). Social Media Impersonation: Understanding the Dangers. Retrieved from: https://bolster.ai/glossary/social-media-impersonation (Accessed: 29.08.2024.)

Chiavetta, R. (2024). How to Prevent and Respond to Social Media Impersonations. Retrieved from: https://blackcloak.io/how-to-prevent-and-respond-to-social-media-impersonations/ (Accessed: 29.08.2024.)

Darktrace (2024). What is Brand Impersonation? Retrieved from: https://darktrace.com/cyber-ai-glossary/brand-impersonation (Accessed: 26.08.2024.)

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96-104.

Hoffmeister, T. (2014). The challenges of preventing and prosecuting social media crimes. Pace L. Rev., 35, 115.

Horsey, D. (2024). How to Deal With Social Media Impersonation. Retrieved from: https://www.minclaw.com/social-media-impersonation/ (Accessed: 28.08.2024.)

Marr, B. (2023). The Dark Side Of Technology: Navigating The Threat Of Digital Impersonation. Retrieved from: https://www.forbes.com/sites/bernardmarr/2023/04/07/the-dark-side-of-technology-navigating-the-threat-of-digital-impersonation/ (Accessed: 27.08.2024.)

Page, R. (2014). Hoaxes, hacking and humour: analysing impersonated identity on social network sites. In The language of social media (pp. 46-64): Springer.

Porta, J. (2023). Social media impersonation: What is it? How to stop it. Retrieved from: https://www.redpoints.com/blog/social-media-impersonation-what-is-it-how-to-stop-it/ (Accessed: 28.08.2024.)

Rylah, J. B. (2022). One fake Tweet may have cost Twitter a lot. Retrieved from: https://thehustle.co/11152022-eli-lilly (Accessed: 27.08.2024.)

Singh, U. (2024). Social Media Impersonation: A Comprehensive Guide (2024). Retrieved from: https://www.tikaj.com/blog/social-media-impersonation/ (Accessed: 28.08.2024.)

Weber, T. (2023). What to do if you are being impersonated on social media. Retrieved from: https://repweber.com/2023/11/01/what-to-do-if-you-are-being-impersonated-on-social-media/ (Accessed: 27.08.2024.)

Zarei, K., Farahbakhsh, R., & Crespi, N. (2019). Typification of impersonated accounts on instagram. Paper presented at the 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC).

Zarei, K., Farahbakhsh, R., Crespi, N., & Tyson, G. (2020). Impersonation on Social Media: A Deep Neural Approach to Identify Ingenuine Content. arXiv preprint arXiv:2010.08438.
Zerofox (2022). 3 Impersonation Attack Examples You Should Know (And How to Prevent Them). Retrieved from: https://www.zerofox.com/blog/3-impersonation-attack-examples-you-should-know-and-how-to-prevent-them/ (Accessed: 26.08.2024.)