User Susceptibility to Social Engineering in AR Environments

The cutting-edge technology augmented reality (AR), an interactive experience of a real-world environment enhanced by computer-generated perceptual information, is increasingly used in many fields, and market growth projections are in the US billions through 2025.[1] But the potential cybersecurity risk facing users of this technology remains a point of concern.[2]

AR faces common cybersecurity threats such as denial of service (DoS), malware, man-in-the-middle (MitM) and social engineering attacks.[3] However, the partially virtual interface of AR poses a distraction to users that could interfere with the ability to recognize an attack attempt, such as text messages masquerading as legitimate home screen notifications. Due to the ease of sending text messages from an external source as opposed to having to gain system access to carry out many other attack methods, attackers most often appeal to the human user through social engineering.[4] As the adoption of AR applications on a variety of devices—especially mobile phones—continues to grow, understanding user susceptibility to social engineering, the most common cyberattack, becomes increasingly important.

Attackers often adopt methods that take advantage of familiarity and urgency to trick users into interacting with malicious attachments and links through phishing campaigns.

The Distraction of the Simulation

Given the distractive nature of immersive environments, users face a higher risk of deception when using AR.[5] Moreover, the common use of text messaging on mobile devices provides ample opportunities for threat actors to send malicious links through native mobile application messaging to targets utilizing AR applications on mobile interfaces. With the user distracted by the AR simulative environment, an attacker could seize the opportunity to send a message with a malicious link posing as a routine notification for a message from a contact or a software update. Since attackers often adopt methods that take advantage of familiarity and urgency to trick users into interacting with malicious attachments and links through phishing campaigns, an independent study[6] examined whether AR users appear more susceptible to personalized messaging scams that impersonate someone the user knows (familiarity) or send fraudulent software update notifications (urgency).

SARAH KATZ

Is a cybersecurity technical writer at Microsoft with seven years of experience in the information security industry, including roles at NASA and Facebook. Her book *Digital Earth: Cyber Threats, Privacy and Ethics in an Age of Paranoia* was published in early 2022. She has also published articles in *Cyber Defense Magazine, Dark Reading* and *Infosecurity Magazine*.

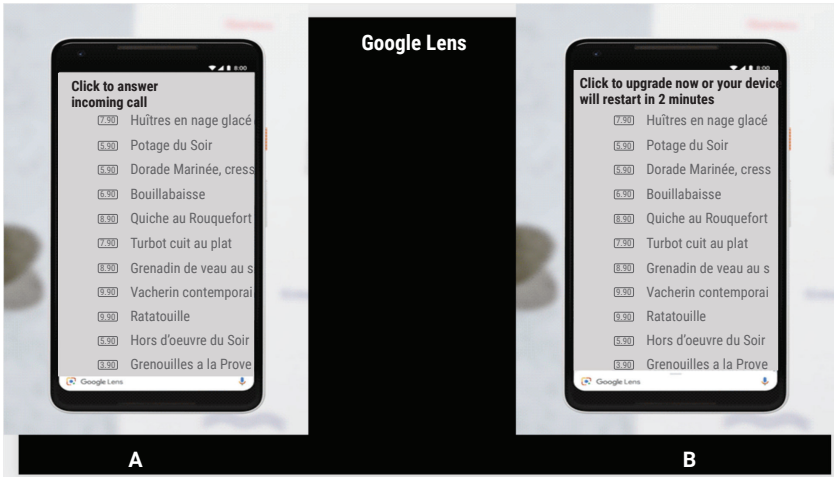
Applications of Social Engineering

Although the tactics of familiarity and urgency have been explored in the context of desktop and mobile phishing, they have not yet been examined for digital immersive environments.[7] AR is increasingly used in fields such as medicine[8] and education,[9] and in popular mobile games such as Pokémon GO and everyday applications such as Google Lens. A better understanding of a user's risk of falling for attacker tactics should help developers design these technologies for a safer user experience.[10] As familiarity[11] and urgency[12] have been identified in the literature as psychological ploys often used by attackers, the qualitative study mentioned explored which of these tactics tends to most successfully deceive users immersed in the environments of four popular AR applications: Google Lens, Google Maps, Google Translate and Instagram. Understanding the most successful social engineering tactics used by attackers in AR could help mobile application developers better determine which types of onscreen notifications can be safely sent to the user. Although familiarity and urgency remain primary tactics used for onscreen messaging in social engineering attacks, identifying whether the same tactics prove as successful when the user is more distracted can be helpful for assessing any heightened risk to users of more immersive environments.

For the study, a focus group was formed consisting of 20 regular leisure users of AR applications that were selected at random from the AR-specific platforms AVForums and ar-eye.com and social media platforms Facebook and Reddit. Each participant was shown a Microsoft PowerPoint presentation simulating the environments of the four aforementioned AR applications. Participants were questioned about their likelihood of clicking on an onscreen text box presented within the simulated environment. The first text showed an incoming message from a contact to denote familiarity. The second text instructed the user to click on a link that would upgrade system software or risk device restart to denote urgency. The resulting responses were analyzed and expanded on to determine the reasons the individuals engaged with messages denoting familiarity vs. urgency while immersed in an AR environment (**figure 1**).

FIGURE 1

Familiarity vs. Urgency in Social Engineering Within AR Mobile Applications



Attention to social norms suggests that users in a partially immersive environment such as AR may value social pressures over personal digital security.

In the focus group, 15 of 20 subjects reported between 75 percent and 100 percent prioritization of Option A (familiarity), while three respondents prioritized Option B by 75 percent to 100 percent (urgency). The remaining two subjects selected 50 percent for each option.

When questioned about the motivation behind their choices, respondents who focused on familiarity reported:

- I would rather answer a call than trust an upgrade.
- I always ignore updates anyway.
- I associate application user interfaces with social interaction.
- I instinctively prioritize incoming calls because updates will automatically occur.
- I associate these applications more with calls.
- I do not trust cryptic upgrade messages.
- I would not expect updates, so such pop-ups would be suspicious.
- The short timeframe for the upgrade feels like a threat.

- I would expect more calls than updates.
- Calls are more important to me.
- I feel more socially obligated to answer calls than upgrade my device.
- The pop-up seems like a scam.
- The pop-up seems like spyware.

Interestingly, although some of the aforementioned users reported prioritizing familiarity out of a sense of suspicion about the urgency-based message, the majority appeared to consider social expectations as the most important reason for foregoing an upgrade to take an incoming call. When it comes to the assessment of sudden visual stimuli during a distractive experience, such attention to social norms suggests that users in a partially immersive environment such as AR may value social pressures over personal digital security.

On the other hand, respondents who prioritized urgency noted:

- I do not tend to answer calls, but do not want my device to turn off on me.
- I was actively engaging in the application rather than a call and wanted to prevent the application from turning off.
- I felt a greater sense of obligation to upgrade than answer the call.
- The upgrade message seemed more intrusive on screen than the call notification.

While respondents who prioritized familiarity exhibited social pressure concern, those who focused on urgency appeared more likely to cite the brief time sensitivity factor as a primary motivator for choosing the upgrade option. This willingness to comply to avoid a perceived threat—even one as potentially minor as one's device turning off during leisure use of social applications—could suggest susceptibility to another kind of pressure often used by cyberattackers.

However, these results might not necessarily reflect data that could have been collected from a larger focus group with additional simulation methods employed.

This study reflects only a small sample of the responses that may be seen in future studies of this nature. Still, the implied effects of distraction within an immersive environment combined with psychological persuasion and intimidation tactics employed by attackers indicate the need for further experiments on how an increasing number of AR users might respond to the threat of social engineering when using everyday applications.

> The human element remains the weakest aspect of cybersecurity, but it has the potential to become the strongest.

Conclusion

At the end of the day, the human element remains the weakest aspect of cybersecurity, but it has the potential to become the strongest. When it comes to social engineering, users of any computing device have the power to thwart cyberattacks simply by knowing how to recognize and refuse messages they were not anticipating. To address the particular case of text message pop-ups appearing while users are partially immersed in AR, application developers can more effectively inhibit those messages by vetting text messages with links before they can present within the simulated environment.

Endnotes

1 Kohnke, A.; "The Risk and Rewards of Enterprise Use of Augmented Reality and Virtual Reality," *ISACA® Journal*, vol. 1, 2020, *https://www.isaca.org/archives*

2 Kalpokas, I.; "Problematising Reality: The Promises and Perils of Synthetic Media," *SN Social Sciences*, vol. 1, iss. 1, 9 November 2020, *https://doi.org/10.1007/s43545-020-00010-8*

3 Kaspersky, "What Are the Security and Privacy Risks of VR and AR," *https://www.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr*

4 Klimburg-Witjes, N.; A. Wentland; "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses," *Science, Technology, and Human Values*, vol. 46, iss. 6, 10 February 2021, *https://doi.org/10.1177/0162243921992844*

5 Ferreira, A.; S. Teles; "Persuasion: How Phishing Emails Can Influence Users and Bypass Security Measures," *International Journal of Human-Computer Studies*, vol. 125, May 2019, *https://doi.org/10.1016/j.ijhcs.2018.12.004*

ENJOYING THIS ARTICLE?

- Learn more about, discuss and collaborate on risk manangement in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

6 *Ibid.*

7 de Guzman, J. A.; K. Thilakarathna; A. Seneviratne; "Security and Privacy Approaches in Mixed Reality: A Literature Survey," *ACM Computing Surveys*, vol. 52, iss. 6, November 2020, *https://dl.acm.org/doi/10.1145/3359626*

8 Eckert, M.; J. S. Volmerg; C. M. Friedrich; "Augmented Reality in Medicine: Systematic and Bibliographic Review," *JMIR MHealth UHealth*, vol. 7, iss. 4, 2019, *https://doi.org/10.2196/10967*

9 Huang, K.T.; C. Ball; J. Francis; R. Ratan; J. Boumis; J. Fordham; "Augmented Versus Virtual Reality in Education: An Exploratory Study Examining Science Knowledge Retention When Using Augmented Reality/Virtual Reality Mobile Applications," *Cyberpsychology, Behavior, and Social Networking*, vol. 22, iss. 2, 2019, *https://doi.org/10.1089/cyber.2018.0150*

10 Moustafa, A. A.; A. Bello; A. Maurushat; "The Role of User Behaviour in Improving Cyber Security Management," *Frontiers in Psychology*, vol. 12, 2021, *https://doi.org/10.3389/fpsyg.2021.561011*

11 Chen, R.; J. Gaia; H. Raghav Rao; "An Examination of the Effect of Recent Phishing Encounters on Phishing Susceptibility," *Decision Support Systems*, vol. 133, June 2020, *https://doi.org/10.1016/j.dss.2020.113287*

12 Washo, A. H.; "An Interdisciplinary View of Social Engineering: A Call to Action for Research," *Computers in Human Behavior Reports*, vol. 4, 2021, *https://doi.org/10.1016/j.chbr.2021.100126*