

"Digital black hole" – A study on the experience design of telecommunications network fraud

Yunjing Shi

Sydney School of Architecture, Design and Planning, University of Sydney, Sydney, Australia

yunjing20021108@163.com

Abstract. As telecom network fraud gradually infiltrates daily scenarios such as social interactions, consumption, part-time work, and online payments, traditional anti-fraud publicity, which primarily relies on text, posters, and case studies, still has room for improvement in terms of engagement and memorability. This article uses the concept of a "digital black hole" as its core, comparing the stages of attraction, belief, and gradual entrapment in the fraud process to the attractive properties of a black hole, and transforming this concept into an experiential design. The work consists of three parts: a black hole magnetic interaction device, a visual illusion science popularization wall, and a fortune-telling card game. These components present the risks of fraud from the perspectives of physical sensation, visual judgment, and interactive cognition, respectively. Through specially designed magnetic shoes, eight categories of common fraud science popularization content, and 104 interactive cards, the work attempts to transform the relatively abstract process of fraud into a more intuitive experience. Participants can recognize the inducement methods and risk characteristics of fraudulent information through observation and interaction, and further reflect on the application value of experiential design in the dissemination of anti-fraud knowledge.

Keywords: telecommunications network fraud, digital black hole, experience design, metaphorical design, interactive design

1. Introduction

Today, telecommunications and internet fraud has become one of the more common risks in daily life. Fraudsters approach victims by exploiting personal information, impersonating identities, leveraging authority relationships, or manipulating emotional trust, and then continuously exerting psychological pressure to gradually impair the victim's judgment. According to data released by the Ministry of Public Security, in 2023, among victims of telecom network fraud, individuals aged 18 to 40 accounted for 62.1%¹. Ten common types of fraud, including order brushing and rebate scams, false online investment and financial management, fake shopping services, impersonation of e-commerce and logistics customer service, and false credit information,

¹ Ministry of Public Security. (2024, June 25). Ministry of Public Security announces the top 10 most prevalent types of telecom network fraud.

made up nearly 88.4% of the total cases. Among the victims of order brushing and rebate scams, there were a significant number of students. This indicates that fraud is increasingly infiltrating young people's online lives. College students frequently use social media and are often exposed to information related to part-time jobs, online shopping, loans, and social interactions, making them prone to encountering a mixture of true and false information. Traditional anti-fraud publicity primarily relies on text, posters, and case studies. While these methods can convey basic knowledge, they often fail to leave a lasting impression. Compared to simply telling people "don't be fooled," if it can truly make individuals experience the allure of being deceived and the loss of judgment, it may be more effective in creating a lasting impression.

Based on this idea, this article summarizes the "attract-approach-fall" stages in the process of fraud as a "digital black hole." The characteristic of a black hole continuously attracting surrounding objects bears a certain resemblance to how fraud gradually draws people closer to risks. Centered around this concept, the work primarily consists of three parts: a black hole magnetic interaction device, a visual illusion science popularization wall, and a fortune-telling card game. These three parts explore the anti-fraud knowledge from the perspectives of physical sensation, visual judgment, and interactive learning, respectively, aiming to move beyond mere textual understanding.

2. The concept of "digital black holes" and design ideas

2.1. The concept of "digital black hole"

"Digital black holes" originally came from an intuitive understanding of the fraud process. Many scams don't appear dangerous in the first place, but rather attract attention first with an interest, a relationship, an opportunity, or an authority. After constant contact, victims will gradually invest time, emotions and even money. When aware of the problem, it is often very difficult to exit. The process is like falling into a bottomless hole. The more you go inside, the harder it is to turn back. Thus, "black holes" are not a simple visual representation here, but rather a central metaphor for the entire work. It represents both the attraction generated by fraud and the gradual loss of initiative in the process of continuous belief and action.

Lakoff and Johnson argue in metaphor research that people often use familiar physical and life experiences to understand more abstract concepts [1]. From this perspective, the "black hole" gives a more understandable picture of the fraud process, which was previously invisible. The focus of this article can be summarized in one sentence: A scam isn't about trapping people all at once, but about getting people to take the initiative step by step.

2.2. Visual metaphor

The scam itself has no fixed form and is difficult to be directly "drawn," so the work chooses to express it using visual metaphor. In visual design, whirlpools, concentric circles, black-and-white contrast, and visual illusions make up the main language. The whirlpool represents a state of gathering at the center, the contrast between black and white creates a sense of instability, and the visual illusion corresponds to the "difficulty in distinguishing between real and fake" in fraud. Real-life scams are often disguised as ordinary everyday information. It could be a seemingly normal customer service message, a familiar platform page, or it could use the faces and personal information of acquaintances to add credibility.

Experimental research on phishing sites by Dhamija, Tygar, and Hearst found that even people with some web experience can be tricked by fake sites with high visual authenticity [2]. This shows that when people judge whether information is real or fake, they are easily influenced by visual form and familiarity. So visual illusion isn't just meant to make the picture more impactful, it's also a reminder to the viewer that what appears

to be real information is not necessarily reliable. The popularization wall also includes eight categories of video content for common scams, combining visual effects with practical knowledge to avoid the work remaining only formal.

2.3. From visual to bodily experience

Physical experiences are often more direct than reading text. Norman's research on interaction design emphasizes that users need to be able to understand the connection between their actions and results, and clear feedback can help people build this understanding [3]. Therefore, the work does not simply represent "being attracted" with images, but uses magnetic devices that allow the experimenter to really feel this power. Participants need to wear special magnetic shoes to approach the device. The closer you get to the center of the black hole, the more noticeable the magnetic force on the soles of your feet. In this process, it is not the model representing money or information that is sucked away, but the experimenter himself. This approach is closer to what the work is really trying to say - the victim is not standing by and watching the scam happen, but is getting into it themselves.

Kolb's experiential learning theory holds that learning not only comes from the direct input of knowledge, but also develops in the process of concrete experience, reflection and practice [4]. From this perspective, physical interactions are not meant to increase entertainment, but rather to use real feelings to help participants understand an abstract concept.

3. Types and causes of telecommunications network fraud

3.1. Common types of fraud

The forms of telecommunications scams are constantly changing, but the basic logic used by many scams is actually very similar. Among the high-frequency scam types announced by the Ministry of Public Security, they include order-brushing rebate scams, fake online investment and wealth management, fake shopping services, impersonating e-commerce and logistics customer service staff, false credit claims, fake loans, and impersonating leaders' acquaintances². Fraudulent investment scams usually build trust through small profits or false profit information before tempting victims to invest more. Among the typical cases published by the Supreme People's Court, there have also been cases in which fraud gangs used social platforms, so-called "investment mentors" and fake profit screenshots to guide victims into fake investment platforms³. Order-brushing rebate fraud often uses part-time jobs and commissions as bait. Initially, a small amount of money may be returned, making the platform seem reliable, and then asking for further payments on the grounds of a failed task, a linked order, a transaction error, or an account exception⁴.

Loan and credit frauds take more advantage of people's anxiety about credit history, loan eligibility, and funding needs, and require victims to pay a deposit, service fee, or so-called account-unfreezing fee. Identity impersonation is also a common method, including impersonating an acquaintance, a leader, a customer service officer, a banker, or a public prosecutor or a law officer. Such scams do not necessarily exploit the lure of money and sometimes rely more on people's trust in relationships, institutions and authority. Online

² See note 1 above.

³ Supreme People's Court. (2026, February 26). Typical cases of punishing property-related crimes such as telecommunications network fraud by people's courts according to law.

⁴ See note 1 above.

romance scams are similar processes. Whitty and Buchanan point out that some emotional scammers build online relationships and trust before making further demands for money [5]. As we can see from these cases, although the forms of fraud are different, they all generally go through a similar process: Make people believe first, then make people act. So rather than remembering a large number of scam names that are constantly being updated, it's more important to recognize the recurring signals within them, such as unusually high yields, the sudden creation of urgency, asking for a verification code, turning on screen sharing, or constantly urging an immediate transfer.

3.2. Why people get deceived

Being deceived does not simply mean "lack of common sense." Fraud is successful because it often happens when someone is in a state of tension, anxiety, excitement or anticipation. The temptation to profit, fear, empathy, wishful thinking, and trust in authority can all affect normal judgment. Norris, Brookes and Dowell summarized the research on victimization of online fraud and pointed out that the success of fraud is related to information characteristics, personal experience and individual psychological characteristics. Some fraudulent information takes advantage of time pressure, making people think less deeply and make decisions more quickly [6]. This also explains why scammers often use tactics such as "deal with it now," "don't tell anyone else," and "it will have serious consequences if you don't act now." In such a situation, people are easily focused on solving immediate problems and thus neglect to verify the source of information.

In addition, if a portion of the money has already been invested, some victims may also continue to invest because they are unwilling to accept previous losses in the hope of getting the money back. Therefore, what needs to be developed most about fraud knowledge is not "how many cases to remember," but a simple response habit: Stop, confirm, and act. Research on cybersecurity warnings has also found that warnings that truly attract attention and appear at critical operational stages are more likely to influence users' subsequent choices than passive prompts that are easily ignored [7]. This has also become an important idea in the design of "digital black holes": instead of repeatedly telling people "danger," try to make the danger really noticeable during the experience.

4. "Digital black hole" experience design

4.1. Overall design

The entire work consists of a black hole magnetic device, a visual illusion educational wall, and a fortune-telling card game. There are no fixed visiting sequences set for the three sections, and viewers are free to experience them according to their interests. But in terms of content, they correspond to three levels of physical feeling, information judgment, and interactive learning. The magnetic device emphasizes the feeling of "being attracted," the visual illusion wall discusses authenticity judgment, and the card section further turns the knowledge of fraud into information that participants actively seek and match. These three approaches are not simply to repeat the same content, but to explain from different perspectives why fraud can gradually affect people's judgment.

4.2. Black hole magnetic interaction device

The magnetic device is the most central part of the entire work. Participants need to wear specially designed magnetic shoes to enter the interactive area. As the position gets closer to the center of the black hole, the magnetic pull on the soles of the feet becomes more and more evident. This change corresponds to the process

by which fraud gradually escalates. In the beginning, the person may be exposed to a simple piece of information and the risks are not obvious. But as we continue to communicate, trust and invest, exit may become increasingly difficult. Instead of using objects such as money or mobile phones as symbols of being "sucked into a black hole," the device allows the experiencer to enter the device himself. This is also an important choice in the overall design. Because people, not money, are really caught up in scams. If you only see an object being sucked away, the viewer is still on the sidelines; When one's feet begin to feel resistance noticeably, what was once an abstract "attraction" turns into a personal experience.

There were also practical problems during the production of the installation. The initial use of a small number of magnets could have a noticeable effect on ordinary objects, but was almost imperceptible when placed in a human experience. This question also leads to a very straightforward understanding: a sound concept does not necessarily produce an effective experience. If the experiencer does not feel the magnetic changes themselves, then the "black hole" metaphor is difficult to really understand, even if it is complete. As a result, the number of magnets was subsequently increased, making the resistance to the soles of the feet more noticeable. After the adjustment, the magnetic device also left a stronger impression on participants. The results also further suggest that direct feedback from the body may be more likely to form memories than simply looking at an image.

4.3. Visual illusion science popularization wall

The visual illusion wall mainly represents the confusing information in fraud and the difficulty of distinguishing between true and false. This section uses black-and-white graphics, whirlpools and visual illusions, while adding eight popular science videos about common scams. When viewing illusory images, people usually believe the results at first glance, but after closer inspection, they may find that their judgment is not accurate.

This is similar to fraudulent information. A scam doesn't directly tell the victim "this is a scam," instead it often tries to make its content seem real and reasonable. So what this area is trying to convey is not just that "vision can deceive," but a much simpler problem: Are "looking real" and "really real" the same thing in a digital environment? The visual illusion is responsible for asking questions, and a later popular science video provides specific content. This preserves both the visual experience and avoids the work relying solely on formal expression.

4.4. Fortune card interaction

The card section contains 104 cards. Participants need to find the corresponding content based on the subject text on the card. The same subject represents a successful pairing. The reason why the forms of "fortune-telling" and "card matching" were chosen is because there is a process related to "believing in speech" between fortune-telling and fraud. People may begin to believe in a certain outcome because of an explanation, a hint, or a promise. Fraud also uses language to create a seemingly complete situation and then pushes the victim to continue to act in accordance with that situation. This is not to equate fortune-telling directly with fraud, but to borrow this process of "accepting information - generating confidence - continuing to judge" and to make a connection between the interaction itself and the subject of fraud. Rather than displaying large amounts of educational text directly, cards at least require participants to actively search for, read, and judge information.

Plass, Homer, and Kinzer argue that the focus of gamified learning is not simply adding game elements, but making connections between learning objectives, participation, challenge, and feedback [8]. Therefore, the

card section does not emphasize winning or losing, but rather uses accessible activities to make fraud knowledge easier to understand.

5. Conclusions

"Digital black holes" attempt to explain telecommunications network fraud in a more intuitive way. One of the biggest characteristics of fraud is that it often starts not with an obvious danger but with a common message, a chat or a seemingly reasonable request. The meaning of black holes is also here. People don't suddenly appear at the center of a black hole, but only after getting closer and closer until they realize they're already affected. Magnetic devices turn this "closeness" into resistance that the body can feel; Visual illusions make people rethink the authenticity of information; Cards turn fraud tactics and prevention knowledge into processes that require active judgment. The three parts, while different in form, ultimately point to the same question: whether a person can realize that he or she is beginning to approach risk when a message is constantly driving people to continue to believe and act.

Rather than making the viewer remember the type of scam, this work wanted to make a simple impression: When you encounter unfamiliar, unusual, or overly urgent information, stop first. At present, the work is still dominated by design practices and has not been fully tested by users. Subsequently, participants' memories of fraud signals and prevention knowledge could be observed through questionnaires, interviews or simple identification tasks before and after the experience. From the current experience, the magnetic device is the most memorable of the three parts. This also shows that anti-fraud communication can think further than telling people "what is fraud": How to make risks really felt.

References

- [1] Lakoff, G., & Johnson, M. (1980). *Metaphors we live by*. University of Chicago Press.
- [2] Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–590. <https://doi.org/10.1145/1124772.1124861>
- [3] Norman, D. A. (2013). *The design of everyday things: Revised and expanded edition*. Basic Books.
- [4] Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice-Hall.
- [5] Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 181–183. <https://doi.org/10.1089/cyber.2011.0352>
- [6] Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34(3), 231–245. <https://doi.org/10.1007/s11896-019-09334-5>
- [7] Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1065–1074. <https://doi.org/10.1145/1357054.1357219>
- [8] Plass, J. L., Homer, B. D., & Kinzer, C. K. (2015). Foundations of game-based learning. *Educational Psychologist*, 50(4), 258–283. <https://doi.org/10.1080/00461520.2015.1122533>