**Scams: What They Are, Different Types, Their Relationship with Computers**

Alrica Avila

04/09/2025

CSIT100\_12

Montclair State University

“Click here for a chance to win a spin the wheel!” “Your car payment is due; click this link to pay now!” Do these emails, texts, or calls sound familiar? These messages are examples of scams or fraud. Everywhere people turn, there is a scam around the corner. A scam is committed by a person known as a fraudster, a con(confident) artist, or a scammer. Scammers commit any action meant to fool their victim, the mark, and acquire illicit profit. A mark could be a singular individual or an entire organization. Presently, scams are dreadful encounters because an individual’s credentials can be stolen and a deceitful stranger broke their heart; even worse, a whole company’s database could be jeopardized and lead to bankruptcy, ruining multiple individuals’ lives at once. Scamming has changed throughout time; individuals deceived others with alterations of policies or identities to earn more than losses; thanks to the internet and fast-acting computers, there are more opportunities for these money-hungry tricksters to con. Aside from knowing how scams came to be, it is essential to know about the common types of scams, the role of computers and their relationship with scams, and how to protect family and friends from scams. (Fraud.com, 2022)

Before the calls, texts, and emails, con artists had been causing people distress for a couple of thousand years. Two merchants from Greece forced people to give up their belongings if they forgot to settle their obligations with interest behind the sales they acquired as part of their insurance method. (Fraud.com, 2022) Then, they “decided to sink the ship so they could pocket all the loaned money. However, they were caught in the act” (Fraud.com, 2022). This deception was the first recorded scheme approximately 400 years ago. Fraud evolved with the times, making it either harder to catch the scammers or more effortless for them to catch marks; however, insurance scams modeled by these two men still occur constantly. Correspondingly, almost 5 centuries forward, the guard who slew the Roman monarch sold an empire that was not theirs, destroying peace but creating the first financial fraud. Gregor MacGregor fooled individuals by advertising an imaginary ground, the 1821 example of property fraud. The 1920s were not safe either; a noteworthy example is that the Ponzi scheme peaked cheque and identity fraud. Charles Ponzi, a bank employee, utilized his position to execute illicit efforts; in the famous scheme, Ponzi settled the obligation to previous lenders with a new individual’s profit. (Fraud.com, 2022)

As technological advances arose, con artists’ opportunities expanded to reach even more individuals in a condensed amount of time; however, the script or formula of what scammers do and why they do what they do remains consistent. Beforehand, tricksters would seemingly appear out of the blue and try to offer their false services or products. With advanced technology, like printers, these criminals could publish their sham and reach more victims or print to forge a bogus identity. Then, when computers came, hackers would pop up advertisements, emails, and websites to hook their marks into surrendering their information without ever meeting in person, and it is quicker than the newspaper or snail mail; this process went rapidly when internet speeds and social media were developed. Finally, the creation of phones produces more effortless routines for talking to people via calls or texts, which instantly accomplishes a hoax. (Mineo, 2024)

Considering the several ways an individual could get hacked or hoaxed, fraudsters choose numerous methods to conduct their craft. The most common scams nowadays are phishing, tech support scams, online shopping scams, investment scams, ransomware or malware scams, and romance scams (Scamwatch, 2024).

Firstly, phishing scams are fraudulence committed by impersonating a business or a person, sending emails or messages to their mark to permit authority they do not have. For example, the con corresponds to their target organization’s behavior in requesting to “review” the mark’s confidential details via a link or website to accomplish crimes. The email is so effective that the mark tumbles into the snare, surrendering their username, passcode, or banking information. Phishing is often accompanied by spoofing; a scammer makes a website identical to the original legitimate site at face value but unexpectedly modifies a letter or two. Specific types of phishing are vishing (voice interactions), smishing (text messages), and pharming (code that leads users to spoofed sites). (FBI, n.d.)

Secondly, tech support scams are similar to phishing; instead of an email, the prey would receive a pop-up on their device or an unanticipated call from the perpetrator, who feigns to be part of organizations that provide official assistance. The reality is that once the mark gives consent by transmitting their information to the hacker, they have the capability to embezzle private files or download malware. (Scamwatch, 2024)

As e-commerce or electronic commercial trade develops, online shopping has skyrocketed, and so has the possibility of online shopping scams (Scamwatch, 2024). Another use of spoofing is advertising a product that either does not exist, is a knockoff, or is not theirs to trade (FBI, n.d.). Online shoppers unknowingly get scammed until their information has been misappropriated, or they acquire no product.

Additionally, e-commerce swayed cryptocurrency creation and investment prospect expansion. Essentially, con artists use the same methods of scamming mentioned previously, but more specifically, they target legal subsidizing schemes as lies. (Mineo, 2024) For example, frauds like Ponzi invite investors to fund a profit that does not exist and use the earnings for the fraud’s benefit (Fraud.com, 2022).

Next, ransomware and malware ensnare users by persuading them to visit or download destructive software. It is a parallel concept to tech support or investment scams but more stealing users’ data and hacking their systems by plausible threats like deleting all personal files and, in turn, users downloading an application of some sort; however, this leads to their files being in possession of the hacker instead.

Lastly, romance scams are arguably the worst to fall for because they affect the victim financially and emotionally. Not only will the thief get away with stealing an individual’s information, but they will also get away with stealing that individual’s heart. The scammers would make or steal other people’s identities to create a relationship with a mark. There are levels of how severe the romance scam can proceed. First, the fraud could simply be a pop-up ad leading to a spoofed site of “Single Hot Moms”; then, increasing the risk, scammers could create fake profiles of people on dating websites or social media to lure their prey, talking and texting them and asking them for “favors.” These schemes could last from a few seconds on a screen to months- or worse, years. The poor user has been robbed of personal information, time, money, and effort and has had his feelings involved with a heartless criminal. (Scamwatch, 2024)

In addition to the variety of ways con artists cheat people, modern hoaxes are hosted via computers and the internet, and how victims prevent losses. The computer era’s evolution and the internet’s development have immensely modified how scams are executed. Preceding scams require in-person interaction or a cellular device, which is easier to avoid due to the awareness spread about the subject and is easier to detect and report. Now, with computers, criminals can avoid detection when being anonymous and carried out by more people at a faster rate (Mineo, 2024). The fraudster could disguise behind several false characters or profiles and create a new identity to replace the one discovered by authorities. The scammers can exploit the psychology of their targets, using their emotions when typing messages mentioning ethos (creditable source), pathos (something emotionally initiating), or altered logos (logical statements backed up by facts). As mentioned before, these bogus criminals can abuse the identity of their victim’s boss or create panic by saying, “your account has been compromised.” Even if there are not multiple people on the job, hackers can code bots or programs to scam them, automating the operation and dispatching thousands of emails or messages within the blink of an eye. Scammers could also work together and send each other information gathered in secret parts of the internet like the black market or the dark web (LII, n.d.)

Circling back to the days prior to computers, the worst thing that could happen is being in debt or losing much money when it comes to fraudulent crimes; however, nowadays, not only do they worry about what is in their banks and if their numbers drop, they also have to worry about their devices and data. Humanity leans more on the value and benefits of technology maturation, especially when simplifying and compacting behaviors. For example, people rely on storing a computer’s input, storing all kinds of files on their computers. This way, they do not have to worry about physically losing the file. However, easier things come with a price; not only does the computer have use in storage, but advancements such as storing things in a cloud could jeopardize the information safety as well as the device safety being a gateway for hackers to steal the privatized documents if not protected or not careful about who and how it can get accessed. (Adorjan & Colaguori, 2023)

As previously mentioned, scams are not solely defined as financial drain. Victims lose their livelihoods, personal data (and not bound to passwords, but even more private matters such as when they eat or where they live, comprising privacy and safety), jobs, or businesses. According to the book Crime, Deviance, and Social Control in the 21st Century: A Justice and Rights Perspective, “Cybercrime… costs passing $1 trillion since 2018. This includes both the financial losses from cybercrime, estimated at $945 billion, and the $145 billion spent on cybersecurity annually.” (Adorjan & Colaguori, 2023). The operations that lead to these losses affect a single individual and their families, employees, and even larger corporations.

Furthermore, expanding the topic about specific scams and their effect on victims, romance scams, individuals who go under these schemes fear judgment, emotional trauma, and strings attached. Ransomware jeopardizes businesses that sell products, hospitals, and patient welfare and safety. People put much faith in the safety of their devices, and scams ruin or break the bond between users and their machines even though they were designed to be utilized for the betterment of the future and ease in day-to-day life.

Awareness is key to prevention, but just because a potential victim does not fall for the trap one day does not mean they will never be a victim. Sometimes, the moment or opportunity strikes the scammers, and no matter how high a person’s IQ is, the possibility of being caught off guard can occur. (Mineo, 2024) According to the FBI, here are a few good practices to protect people from these frauds:

“...companies … don’t contact you…for your username or password. Don’t click on anything in an unsolicited email or text message. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing), and call the company to ask if the request is legitimate. Be careful what you download…Set up two-factor (or multi-factor) authentication…Be careful with what information you share online or on social media.” (The FBI, n.d.)

As humanity develops, technology will follow, further connecting our bonds through vast distances and communication almost as fast as sound; however, with the rise of good comes the riot of evildoers such as scammers. From the prehistoric methodology of deceit to modernized technological exploitation, fraud destroys trust and unawareness. Whether it is phishing, romance hoax, or a ransomware attack, the effects of scams cause ruin on a personal, emotional, and financial level. The relationship between scams and computers is not just one of convenience for scammers—it reflects how much society now relies on digital platforms for everyday life. As much as innovation makes life easier, it also increases the need for caution. The best defense lies in awareness, skepticism, and proactive digital hygiene. Like any other weakness or ailment, staying informed and thinking critically before clicking may be the strongest shield against becoming the next mark.

**Work Cited**

1. Adorjan, M., & Colaguori, C. (2023). Scams, fraud, and cybercrime in a globalized society. Crime, Deviance, and Social Control in the 21st Century: A Justice and Rights Perspective, 407, 407-437.
2. Federal Bureau of Investigation. (n.d.). *Spoofing and phishing*. FBI.<https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing>
3. International, Fraud. com. (2022, July 30). *The history and evolution of fraud*. <https://www.fraud.com/post/the-history-and-evolution-of-fraud>
4. Legal Information Institute. (n.d.). *Computer and internet fraud*. Cornell Law School.<https://www.law.cornell.edu/wex/computer_and_internet_fraud>
5. Mineo, L. (2024, September 27). *You’d never fall for an online scam, right?* Harvard Gazette. <https://news.harvard.edu/gazette/story/2024/09/youd-never-fall-for-an-online-scam-right/>
6. Scamwatch. (2024, August 16). *Types of scams*. <https://www.scamwatch.gov.au/types-of-scams>