10-2-2024

Pig Butchering in Cybersecurity: A Modern Social Engineering Threat

Sharon L. Burton
Embry-Riddle Aeronautical University, SharonL.Burton@erau.edu

Pamela D. Moore
Columbia Southern University

Scholarly Commons Citation

Burton, S. L., & Moore, P. D. (2024). Pig Butchering in Cybersecurity: A Modern Social Engineering Threat. *SocioEconomic Challenges, 8*(3). https://doi.org/10.61093/sec.8(3).46-60.2024

AR&P

Pig Butchering in Cybersecurity: A Modern Social Engineering Threat

Dr. Sharon L. Burton, **ORCID:** https://orcid.org/0000-0003-1653-9783
PhD, Professor of the Practice, Department of Applied Aerospace Science, College of Aviation, Embry-Riddle Aeronautical University, USA

Dr. Pamela D. (Vickerson) Moore, **ORCID:** https://orcid.org/ 0009-0005-8907-3672
Doctorate of Business Administration, Global Business and Leadership, Federal Emergency Management Agency (FEMA), Branch Manager/Assistant Director of Curriculum Development and Evaluations Department, Columbia Southern University, USA

Corresponding author: Sharon L. Burton, SharonL.Burton@erau.edu

Type of manuscript: review paper

Abstract: *Pig butchering is an escalating cybersecurity threat that exploits social engineering to build trust and execute financial fraud. The relevance of this research problem lies in the growing incidence and sophistication of these scams, which have severe financial and psychological impacts on victims. The main purpose of this research is to uncover the methods used in pig butchering scams and their impact on individuals and businesses. The research focuses on digital platforms such as social media, dating apps, and professional networking sites, chosen for their wide user bases and the ease of establishing personal connections. The study period encompasses recent developments from the past five years to capture the evolving nature of these scams. The research utilizes a qualitative literature review as its primary method, drawing on academic articles, industry reports, and case studies. The study's statistical basis includes data from law enforcement agencies, cybersecurity firms, and victim reports. Key findings confirm the effectiveness of proactive cybersecurity measures, such as continuous education and specialized services, in mitigating pig butchering scams. The research hypothesis, stating that these measures can significantly reduce scam success rates, is supported by the data. Results indicate that enhancing cybersecurity protocols and training programs is crucial for protecting against such threats. Future research should focus on developing predictive models and integrating AI and machine learning for better detection and prevention. This study provides valuable insights for policymakers, cybersecurity professionals, and educators, highlighting the need for international cooperation and advanced technological defenses to combat this pervasive threat.*

Keywords: cybersecurity, pig butchering scam, social engineering, financial, fraud, trust, manipulation, proactive defense, risk aware.
JEL Classification: A14, F01, K24, P37, K14.

Received: 03.06.2024 **Accepted:** 23.08.2024 **Published:** 02.10.2024

Funding: There is no funding for this research.
Publisher: Academic Research and Publishing UG (i.G.) (Germany).
Founder: Academic Research and Publishing UG (i.G.) (Germany).

Cite as: Burton, S. L., & Moore, P. D. V. M. (2024). Pig Butchering in Cybersecurity: A Modern Social Engineering Threat. *SocioEconomic Challenges*, *8*(3), 46-60. https://doi.org/10.61093/sec.8(3).46-60.2024.

INTRODUCTION

The rise of social engineering scams in cybersecurity, particularly the pig butchering scam tactic, poses significant threats to individuals and businesses. Also known as Sha Zhu Pan in Chinese, or in certain cases romance scams, pig butchering scams are a sophisticated form of online fraud where cybercriminals meticulously build trust with their targets over extended periods, ultimately manipulating them into financial ruin through fake investment platforms and romantic persuasion (United States Attorney's Office Central District of California, 2024; U. S. Immigration and Customs Enforcement, 2023; Wang, 2024; Whittaker et al., 2024). This United States Secret Service (2024) offered that there are cases regarding pig butchering scams connected to false work from home schemes. Pig butchering scams are primarily executed by criminal syndicates located in Mekong region of Southeast Asia, employing victims of labor trafficking to reach out to millions of people globally (State of Michigan Consumer Protection, 2024), and primarily out of Cambodia, Myanmar, and Laos (Jackson, 2024), Thailand (Marsanic, 2023). After victims place their initial "investment," the platforms sometime display significant returns to enrich the scam. The United States Secret Service (2024), stated that even though pig butchering scammers characteristically pursue the most vulnerable, even wealthy and highly educated individuals have been tricked by these schemes.

As given by the U.S. Department of the Treasury's Financial Crimes Enforcement Network (U. S. Treasury FinCEN, 2023), these scams are known as pig butchering because they mirror the process of feeding a pig to increase its weight before it is slaughtered. Also, in these scams, the victims are metaphorically called "pigs" by the fraudsters, who create false identities (Button & Cross, 2017) and use the promise of potential relationships along with intricate narratives to build trust (United States Secret Service, 2024; U. S. Treasury FinCEN, 2023); this part of the metaphorical relation is in the initial contact (British Chamber of Commerce Dubai, 2024). Further, this deceit serves to "fatten" the victims' belief in a genuine connection, over weeks or months (U. S. Treasury FinCEN, 2023) is referred to as grooming and bonding (British Chamber of Commerce Dubai, 2024). The term "butchering" or "slaughtering" is used by scammers when they finally strip the victims of their assets, resulting in financial and emotional damage to the individuals targeted (U. S. Treasury FinCEN, 2023) and is referred to as the the financial hook (British Chamber of Commerce Dubai, 2024).

Pig butchering scams leverage social engineering tactics to manipulate victims through various channels, including social media, dating apps, professional networking sites (Sarkar & Shukla, 2024), and use messaging service such as WhatsApp or WeChat (Finra, 2022) to pretend they have inadvertently use a "wrong number" (Podkul, 2022). Victim loss from pig butchering totaled $75.3 billion (Griffen and Mei, 2024), $3.3 billion in 2022 (U. S. Immigration and Customs Enforcement, 2023). These crimes are renowned for their innovative techniques, yet there is still much to be understood about the scammers' methods and the psychological manipulation involved (Sarkar & Shukla, 2024). This research aims to comprehensively understand the tactics used in pig butchering scams, focusing on the strategies employed by scammers to exploit their victims' trust and vulnerabilities. Criminal Investigation agents have alerted that pig butchering scams are predominantly targeting U.S. taxpayers (The Criminal Investigation U. S. Internal Revenue Service, 2023). Also, the largest recorded single loss in such scams is $2 million, although the typical financial damage amounts to several hundred thousand dollars per victim (The Criminal Investigation U. S. Internal Revenue Service, 2023). In 2022, the FBI's Internet Crimes Complaint Center (IC3) recorded that investment fraud led to the most significant financial damages among all reported scams, amounting to $3.31 billion (United States Attorney's General Central District of California; 2023). Also, the majority of these fraudulent activities were related to cryptocurrency schemes, such as pig butchering, which saw a staggering 183% rise in reported losses, reaching $2.57 billion compared to the previous year (Gore, 2024).

Further, the FBI noted that the largest group of complainants were individuals aged between 30 and 49 (Gore, 2024; United States Attorney's General Central District of California, 2023).

The evolving landscape of pig butchering scams demonstrates an alarming increase in sophistication and occurrence. Cybercriminals dedicate substantial time and resources to crafting these schemes, complicating detection and prevention efforts.

A vital aspect of these scams involves using blockchain addresses to track cryptocurrency flows. Scammers often use these addresses to receive and mask illicit funds. Techniques used to obscure these transactions include conducting multiple transfers, swapping different types of cryptocurrencies via decentralized finance (DeFi) intelligent contracts, and bridging—moving assets across different blockchain platforms to complicate further the traceability of funds (Chaudhry, 2021).

Swapping between cryptocurrencies through DeFi involves automated contracts that exchange one digital currency for another without an intermediary, which can often bypass traditional monitoring systems. Bridging across blockchains refers to transferring assets from one blockchain to another, which can involve wrapping a cryptocurrency into another compatible format on a different blockchain, further obscuring the origin of funds (Lee et al., 2023).

A blockchain is a digital ledger that records data across multiple computers in a decentralized manner (Lafourcade & Lombard-Platet, 2020). Unlike traditional databases managed from a single location, a blockchain is maintained across numerous nodes, or computers, connected in a network. This setup ensures that the data, ranging from cryptocurrency transactions to ownership details of NFTs and DeFi smart contracts, is duplicated and synchronized in real-time across all nodes (Lafourcade & Lombard-Platet, 2020). Each piece of data is stored in blocks, which are linked in a sequential chain (Lafourcade & Lombard-Platet, 2020). New blocks are added through a consensus mechanism, where a majority of nodes validate the data's authenticity before it is appended to the chain, making blockchain technology secure and resistant to fraudulent alterations.

Blockchain addresses are specific identifiers within the blockchain network (Caldeira & Correia, 2021). They are analogous to bank account numbers in traditional finance, serving as unique destinations where cryptocurrency can be sent or received. According to this research team, each address is associated with a pair of cryptographic keys: a public key, which is openly shared and akin to an account number, and a private key, which remains confidential and acts like a password. When a transaction is conducted, the blockchain records it by noting the transfer of digital assets from one address to another, thus maintaining a transparent and secure history of all transactions associated with that address (Caldeira & Correia, 2021). These addresses ensure that the interaction on the blockchain is secure, trackable, and tied to specific nodes or users, reinforcing the blockchain's integrity and decentralized nature (Caldeira & Correia, 2021).

The orchestrators of these scams often engage with prominent cryptocurrency exchanges, executing over 104,000 small transactions, potentially as a ploy to build trust with victims. Ultimately, substantial amounts, often in the form of Tether, a type of cryptocurrency known as a stablecoin (Osman et al., 2024), exit the cryptocurrency network through less transparent but significant exchanges like Binance, one of the largest and most well-known cryptocurrency exchanges globally (Guo et al., 2024), Huobi, a global cryptocurrency exchange (Chiu, 2024), and OKX formerly known as OKEx, is a prominent cryptocurrency exchange that provides a platform for trading various digital assets (Chiu, 2024). These revelations underscore the role of the ostensibly reputable crypto industry in enabling significant criminal capital flows, acting as th gateways and exit points for these illicit funds (Johnson & Roberts, 2020).

The general problem addressed in this study is the increasing prevalence and sophistication of pig butchering scams, which have transcended beyond personal fraud to target businesses, magnifying their impact on organizations financial and operational integrity of organizations (Ogundiran et al., 2023). The essence of this study lies in addressing the gap in current cybersecurity practices by focusing on the social engineering aspect of pig butchering scams. Three main research questions guide this study include:

- RSQ1: How do pig butchering scams exploit psychological manipulation to achieve their goals?
- RSQ2: What are the primary channels through which these scams are perpetrated?
- RSQ3: What proactive cybersecurity measures can be implemented to prevent these scams?

This study is scientifically significant as it combines psychological analysis with cybersecurity strategies, offering a multifaceted approach to comprehending and combating these threats (Iftikhar, 2024). The outcomes shed light on a significant criminogenic aspect within the pig butchering scam, an area that has received limited attention thus far. This knowledge is crucial for a comprehensive understanding of the factors contributing to the transformation of trafficked individuals into scammers, thereby offering valuable insights for preemptive prevention and rehabilitation initiatives (Wang, 2024).

From a practical perspective, the findings of this study are crucial for decision-makers in private and public sectors. Implementing the recommended cybersecurity measures can significantly reduce the risk of financial fraud, thereby preserving the integrity of financial and digital assets (Jones, 2021). Moreover, the study's insights into the psychological manipulation techniques used in pig butchering scams can inform the development of more effective training programs for employees, enhancing their ability to recognize and respond to potential threats (Wang, 2024). The study underscores the necessity for proactive measures and continuous education to counteract the sophisticated threats posed by pig butchering scams effectively. These findings guide the development of cybersecurity policies and practices, aiming to create a safer digital environment for all users. Moreover, they emphasize the significance of international collaboration to address the transnational nature of these scams, ensuring that cybersecurity measures and regulations are harmonized across borders to prevent safe havens for cybercriminals.

ANALYTICS, THEORETICAL AND CONCEPTUAL FRAMEWORK

Apprehending the psychological manipulation tactics and impacts of sophisticated scams like pig butchering is critical for developing effective countermeasures as cyber threats evolve (U. S. Department of Justice, 2024). The rise in social media technology has enabled a single perpetrator to target a larger number of victims (Walls, 2017). Also, the costs and expertise needed to carry out cybercrimes have diminished (Sood & Enbody, 2013). This literature review aims to consolidate current research on the psychological effects and operational methods of pig butchering scams, providing a comprehensive overview that informs cybersecurity practices and victim support mechanisms. Additionally, it seeks to bridge gaps in knowledge and foster a deeper understanding of the strategies employed by perpetrators, enhancing our ability to protect potential targets.

Emotional Manipulation and Trust Exploitation

Social engineering cyberattacks pose a significant risk as they frequently precede more complex and damaging cyber incidents (Montañez et al., 2020). It ranks among the top threats to information security. This issue is growing more complex and common, affecting individuals and organizations. Deep emotional manipulation is used to exploit victims' trust, often through building sophisticated and intensely personal relationships over extended periods, leading to significant emotional investment from the victims (Whittaker et al., 2024). The scammers' ability to establish seemingly genuine connections makes the eventual financial betrayal profoundly impactful, causing severe emotional distress.

Emotional manipulation begins with scammers crafting believable and appealing personas (Button & Cross, 2017), often aligning with the victim's interests and emotional needs. By mirroring the victim's desires and behaviors, scammers create an illusion of a deep connection. This process exploits fundamental psychological principles of trust and reciprocity, making victims more susceptible to manipulation (Rotenberg, 2021).

Psychological Trauma Stress, and Support for Victims

The emotional manipulation involved in pig butchering scams results in significant psychological trauma (Montañez et al., 2020). Victims often experience intense feelings of stress, anxiety, and depression. These psychological effects are exacerbated by the realization that their trust has been exploited, which can lead to feelings of humiliation and guilt (Whittaker et al., 2024).

The financial losses further compound these emotional wounds, creating a cycle of stress and anxiety that can be difficult to break. Research has shown that victims of such scams often suffer from long-term psychological effects, including chronic stress and the potential development of mental health disorders like post-traumatic stress disorder, PTSD (Curtis & Oxburgh, 2022).

The betrayal of trust and significant financial loss can alter a victim's perception of safety and trust in others, leading to long-term psychological distress (Curtis & Oxburgh, 2022; Wang, 2024).

Providing psychological support to victims of pig butchering scams is essential for their recovery. Counseling and mental health services can help victims process their experiences and rebuild their lives. Support groups and peer networks can also provide a sense of community and shared understanding, helping victims feel less isolated in their experiences (Sarkar & Shukla, 2024).

Mental Health Interventions and Support Networks

Mental health professionals can play a crucial role in helping victims address the emotional and psychological impact of the scams. Cognitive-behavioral therapy (CBT) and other therapeutic approaches can help victims manage their stress and anxiety, rebuild their self-esteem, and develop coping strategies for moving forward (Whittaker et al., 2024). These interventions can be tailored to address scam victims' specific needs, focusing on immediate relief and long-term recovery. Building a support network for scam victims is also crucial. Support groups, whether in-person or online, can provide a platform for victims to share their experiences, offer mutual support, and learn from each other's coping strategies. Peer support can be particularly effective in helping victims feel understood and less alone in their experiences (Wang, 2024).

Behavioral Changes and Longterm Impacts

The long-term psychological impact of pig butchering scams can be profound, often resulting in severe financial stress due to the significant amounts of money lost. This financial strain can affect the overall quality of life, leading to continued mental health challenges such as chronic stress and anxiety, which may manifest in physical health problems like hypertension and cardiovascular issues (Whittaker et al., 2024). Furthermore, the psychological trauma can lead to a persistent sense of vulnerability and a decreased sense of self-worth. The betrayal experienced in these scams can erode victims' confidence and self-esteem, making it challenging for them to rebuild their lives and trust in others (Wang, 2024). Additionally, the psychological impact leads to notable behavioral changes in victims; post-scam, they may exhibit heightened distrust and suspicion towards new relationships, whether online or offline. This mistrust can severely impact their social interactions, leading to social withdrawal and isolation, and the constant state of vigilance can contribute to ongoing mental health issues such as anxiety and depression (Iftikhar, 2024). Studies suggest that victims might also develop risk-averse behaviors such as avoiding online interactions and financial transactions out of fear of being scammed again, affecting their ability to engage fully in digital environments (Sarkar & Shukla, 2024).

Financial Impacts of Pig Butchering Scams

As victims continue to invest, the scammer may create fake documents such as the 24 fake pig butchering documents revealed in the research by Maras and Ives (2024) or use other methods to convince the victim of the legitimacy of the investments. Eventually, when the victim attempts to withdraw their funds, they are either denied access or asked to pay exorbitant fees to release the money. At this point, the scammer disappears, leaving the victim with significant financial losses (Maras & Ives, 2024). According to the FBI's Internet Crime Complaint Center, losses from pig butchering scams have been rising dramatically. In 2022, reported losses from these types of scams exceeded $3 billion, highlighting the significant financial damage they can cause (Iftikhar, 2024). The financial impact of pig butchering scams remains substantial, with victims often losing significant sums of money, $22,000 USD (United Stated dollars) to 9.6 million USD (Maras & Ives, 2024). The financial strain from these scams can have a ripple effect, impacting victims' ability to meet daily expenses, pay off debts, and maintain their standard of living. For many victims, the financial losses represent not just money but also the loss of financial security and peace of mind (Blitz et al., 2023).

Case Studies and Statistics

In 2024, the U.S. Attorney's Office, District of Massachusetts, initiated a civil forfeiture action to reclaim cryptocurrencies linked to a "pig butchering" romance scam that defrauded a resident of Massachusetts (United States Attorney's Office District of Massachusetts, 2024). The action targets various cryptocurrencies totaling approximately $2,300,000, stored in two Binance accounts. This move comes after an investigation that started in spring 2023, where fraudsters developed trust with victims online, coaxing them into a deceptive cryptocurrency investment, leading to substantial financial and emotional losses. The victim involved was deceived into transferring over $400,000 to a cryptocurrency wallet, which was then moved across different wallets, including those at Binance. The seized funds were connected to monetary losses of 36 other victims across the U.S. The U.S. Attorney's Office District of Massachusetts (2024) alleged these funds are proceeds from wire fraud and money laundering, necessitating forfeiture. This case highlights the significant legal implications of using digital platforms for fraudulent schemes and underscores the ongoing efforts by law enforcement to trace and recover such illicitly obtained assets.

Han's 2023 study investigates the prevalence and impact of Telecommunication Network Fraud (TNF) and pig butchering scams in China, areas previously underexplored in English-language research. Employing a mixed-methods approach, the study analyzed 1144 survey responses and conducts 25 interviews with stakeholders including fraud victims, law enforcement officers, and a bank employee. The findings revealed a significant increase in victims of remote online scams, affecting their economic and psychological health. TNF is identified as the most common scam, often linked to organized crime and grey market activities such as data leaks and money laundering. These scams frequently present as lucrative opportunities, exploiting trust through schemes that may involve romantic deception leading to fraudulent gambling or investment traps (State of Michigan Consumer Protection (2024). Despite robust legal reforms and anti-fraud initiatives enhancing public awareness and prevention, challenges persist in tackling international fraud due to border constraints and resource limitations within Chinese law enforcement. The study underscores the complexity of fraud in China, particularly, pig butchering, highlighting the intricate roles of law enforcement, societal support, and grey market industries in combating these crimes. According to Farivar (2022), a 52-year-old Bay Area resident named Cy fell victim to an Internet scam orchestrated by an individual named Jessica. In October 2021, Cy confided in Jessica about his hardships, including financial pressures and the emotional burden of placing his father in hospice care. The deceptive scheme utilized platforms engineered to appear legitimate, convincing victims of substantial, although fictitious, investment returns. By December, Cy had lost over one million dollars, a significant portion of which was borrowed, leaving his financial situation devastated (Farivar, 2022). Statistics reveal the growing prevalence and impact of pig butchering scams. For instance, the FBI reported over 4,325 complaints related to pig butchering scams in 2021, with losses exceeding $429 million (FBI Internet Crime Complaint Center, 2021). By 2022, these numbers had surged, with total losses from investment fraud, including pig butchering, reaching $3.31 billion (FBI Internet Crime Complaint Center, 2022). This significant increase underscores the effectiveness of these scams and the substantial financial impact on victims.

Proactive Cybersecurity Measures

Cybersecurity measures are essential to combat pig butchering scams (Yu, 2023; Han, 2023). These measures include technological defenses (Han, 2023), educational initiatives (Ratiu, 2024), sociological implications (Levi & Smith, 2022), and regulatory and legal responses (Khan et al., 2022) to raise awareness about the tactics used in these scams. Effective enforcement of these measures requires coordination across various sectors, ensuring that technological solutions, legal frameworks, and educational efforts are aligned and responsive to the evolving nature of cyber fraud. Additionally, international cooperation is crucial, as many cyber scams operate across borders, making it essential for global security protocols and legal agreements to adapt and tackle these sophisticated threats effectively.

Technological Defenses

Cyber-enabled fraud has evolved, increasing in complexity and making detection by targets and law enforcement more challenging (Maras & Ives, 2024). Technological defenses against pig butchering scams incorporate various advanced methods to improve security and mitigate fraud. Financial institutions and online platforms can adopt AI algorithms and machine learning models to detect anomalous activities and potential fraud (Alt, 2021). Robust spam filters can intercept scam-related emails, while enhanced authentication processes, such as multi-factor authentication and biometric verification, ensure secure system access (Sultana, 2020. The integration of blockchain technology aids in tracing the complete supply chain of transactions, which enhances transparency and reduces the chance of fraudulent activities. Continuous education on cybersecurity practices (Burton, 2022), alongside technological advancements (Maras & Ives, 2024), plays a crucial role in defending against these sophisticated social engineering scams (Ratiu, 2024).

Comprehending the evolution and complexity of cyber-enabled fraud is crucial for several reasons. First, as scams like pig butchering become more sophisticated, traditional detection methods by targets and law enforcement may be insufficient, underscoring the need for continuous updates and advancements in fraud detection technologies (Maras & Ives, 2024). Second, integrating advanced technologies such as AI, machine learning, and blockchain into the security infrastructure of financial institutions and online platforms enhances their ability to detect and prevent fraudulent activities, providing a more robust defense against cyber fraud (Alt, 2024; Sultana, 2020). Last, ongoing education about cybersecurity practices is vital, as it not only keeps individuals and organizations informed about the latest threats and preventive technologies but also cultivates a culture of security awareness that is essential in mitigating the impact of these scams (Burton, 2022; Ratiu, 2024). These combined efforts contribute significantly to the resilience against increasingly complex social engineering tactics.

Educational Initiatives

Education plays a pivotal role in combating cyber-enabled fraud (Ene & Imo, 2024), especially in raising awareness about pig butchering scams (Efijemue et al., 2023). The expansion of social media has opened up numerous avenues for augmented professional development beyond traditional settings, involving academics, healthcare providers, business professionals, and others (Kanchan & Gaidhane, 2023). Informative public awareness campaigns utilizing diverse media platforms, including social media (Kanchan & Gaidhane, 2023), are crucial for spreading knowledge about these scams. These campaigns effectively share real-life victim stories, warn about common red flags, and outline preventive strategies to empower individuals to act prudently during online interactions. Moreover, specialized training programs targeted at employees, especially those in financial services and customer-facing roles, further bolster defenses by equipping workers with the necessary tools and knowledge to identify and prevent these scams (Whittaker et al., 2024). Futher, the U. S. Department of Justice’s Office of Justice Programs (2020) offer fraud awareness programs to educate the public about diverse types of fraud (U. S. Department of Justice, 2020).

Grasping the role of education in combating cyber-enabled fraud is essential (Ene & Imo, 2024). First, it empowers individuals by equipping them with knowledge about the tactics used in pig butchering scams, thus enabling them to recognize and avoid these threats more effectively. Second, using social media as a platform for professional development and public awareness campaigns broadens the reach of educational efforts, ensuring that valuable information about fraud prevention reaches a diverse audience quickly and efficiently (Kanchan & Gaidhane, 2023). Last, specialized training programs for employees in sensitive sectors like financial services can fortify institutional defenses against fraud, creating a more secure and informed workforce that can act as the first line of defense against scammers (Whittaker et al., 2024). This holistic approach to education and awareness is crucial for minimizing the impact of cyber fraud on individuals and organizations.

Sociological Implications

The sociological implications of pig butchering scams extend beyond individual financial loss, affecting broader social structures and community trust dynamics. These scams, which exploit social engineering techniques to build trust before financially exploiting victims, deeply impact interpersonal trust within communities, particularly in online environments (Wang, 2024). Vulnerable groups, including the elderly and those less digitally literate, are often disproportionately targeted by these scams, leading to social isolation and a diminished sense of security (Pérez-Escolar & Canet, 2023). Additionally, these scams can foster a culture of skepticism that affects genuine digital and interpersonal communications, complicating legitimate online business and social interactions (U. S. Immigration and Customs Enforcement, 2023; Wang, 2024; Whittaker et al., 2024. Community awareness programs are essential to guard against the sociological impacts of pig butchering (Australian Federal Police, 2024). These programs should focus on educating the public about the nature of these scams, the signs to watch for, and the significance of verifying digital identities. Furthermore, fostering environments that encourage reporting and discussing scam experiences can help build community resilience against such threats, ensuring a collective protective measure that reinforces trust and support among community members (Ratiu, 2024; Rotenberg, 2021).

Ascertaining the sociological implications of pig butchering scams is essential for several reasons. First, these scams erode trust within communities, specifically online, where interpersonal relationships and business interactions are increasingly conducted, thus threatening the overall integrity of digital communication (Wang, 2024). Second, they disproportionately affect vulnerable populations such as the elderly and the digitally unsophisticated, leading to increased social isolation and decreased security, which necessitates targeted interventions to protect these groups (Pérez-Escolar & Canet, 2023). Finally, fostering a culture where scam experiences are openly discussed and reported can strengthen community resilience, encouraging preventive behaviors and mutual support, which are critical in combatting the pervasive effects of such scams and rebuilding trust (Ratiu, 2024; Rotenberg, 2021). These points help to maintain the fabric of community interactions and safeguard against the disruptive impact of sophisticated fraud schemes.

Regulatory and Legal Responses

Regulatory bodies and law enforcement agencies are increasingly recognizing the threat posed by pig butchering scams and are taking steps to combat them (AFP, 2024; State of Michigan Consumer Protection, 2024; United States Attorney’s Office District of Massachusetts, 2024). FinCEN issued advisories to financial institutions to help identify and report suspicious activities related to pig butchering scams (U.S. Treasury FinCEN, 2022). These advisories highlight common red flags, such as unusual patterns of cryptocurrency transactions and sudden large withdrawals from personal accounts. Legal responses have also included efforts to shut down scam operations and prosecute those involved. International cooperation is crucial in these efforts, as many pig butchering operations are based overseas, making it challenging to track and apprehend the perpetrators (Wang, 2024).

Legislation and Policy

Various countries have enacted specific legislation to combat cybercrime and protect victims of financial fraud. Here are four countries with notable legal frameworks: The United States enacted the Computer Fraud and Abuse Act (CFAA), a civil and criminal cybersecurity law (Congressional Research Service, 2020). The report states that this legislation was enacted in 1986 and amended several times (1984, 1994, 1996, 2001, 2002, and 2008) to address evolving cyber threats.

The national connection is that the CFAA is a cornerstone of U.S. federal cybercrime law prohibiting unauthorized access or damage to computer systems and has been used to prosecute various offenses, including financial fraud (Congressional Research Service, 2020). The impact on cybercrime and financial fraud is that the Act allows for the prosecution of nearly all types of cyber criminal activities and mandates cooperation between various sectors, enhancing protections against financial fraud and cyber-attacks (Congressional Research Service, 2020, 2023). Next is the United Kingdom.

The United Kingdom enacted the Computer Misuse Act in 1990 (CMA, 1990). The national connection is that the Act makes unauthorized access to computer materials a criminal offense and has been amended to include the making, supplying, or obtaining of articles likely to be used in computer misuse offenses (Moreno et al., 2023).

The impact on cyber crime and financial fraud is that it offers a framework for prosecuting cybercrimes and mandates that financial institutions and other entities report cyber incidents, which helps curtail activities like financial fraud (Moreno et al., 2023). Next is Australia.

Australia enacted the Cybercrime Act of 2001 (Bansal, 2023). The national connection is that this legislation aligns with international efforts to combat cybercrime and includes provisions for protecting personal and financial data (Baansal, 2023). The impact on cyber crime and financial fraud is that it introduced obligations for businesses to secure their electronic systems and report breaches, which directly supports the prevention of financial fraud and enhances the security of online transactions. Last is India.

India enacted the Information Technology Act of 2000 (Rattan & Rattan, 2022).

The Act was amended in 2008 to address specific cybersecurity concerns (Pandey, 2023).

The national connection is that this Act provides a legal framework for electronic governance by recognizing electronic records and digital signatures (Guha & Matilal, 2023).

The Impact on Cybercrime and Financial Fraud includes stringent provisions against identity theft and unauthorized access to computer resources, focusing on preventing financial fraud through increased regulation of digital transactions and mandatory cybersecurity practices for corporations (Guha & Matilal, 2023; Pandey, 2023).

These laws are integral to national strategies against cybercrime, often involving collaborative efforts across government, law enforcement, and private sectors to enhance cyber resilience and protect citizens from emerging threats such as financial fraud. The continuous updating of the CFAA demonstrates a commitment to adapting to the technological advancements and changing tactics of cybercriminals, ensuring the law remains effective in the digital age. Furthermore, these amendments facilitate the development of more sophisticated cybersecurity measures and promote a proactive approach to identifying and mitigating cyber threats before they can cause widespread harm. Policies that promote information sharing between financial institutions, law enforcement, and cybersecurity firms can also enhance the collective response to pig butchering scams (Sarkar & Shukla, 2024).

Financial Fraud and Regional Trends

Fraudulent activities continue to evolve and expand globally, with each continent displaying unique trends and challenges in cybercrime (U. S. Department of Treasury FinCEN, 2023). While the Business Email Compromise remains prevalent in Africa, there is a noticeable rise in pig butchering frauds, particularly in West and Southern Africa.

Meanwhile, in the Americas, the spectrum of fraud ranges from impersonation and tech support scams to more severe crimes tied to human trafficking, exacerbated by operations such as INTERPOL's Operation Turquesa V. In Asia, the inception of pig butchering frauds during the COVID-19 pandemic has positioned the region as a pivotal center for such scams, with criminals employing sophisticated corporate-like structures to execute their plans.

Also, Europe is not spared, as it witnesses a surge in online investment frauds and phishing attacks, where criminals increasingly target mobile phone apps and use complex fraud combinations to maximize their illicit gains.

These developments across continents illustrate the dynamic and pervasive nature of global financial fraud, demanding vigilant and coordinated international responses.

Africa: Business Email Compromise continues to be widespread in Africa, but there is a growing incidence of pig butchering fraud, particularly in West and Southern Africa, targeting victims outside the continent. The Black Axe, Airlords, and Supreme Eiye, criminal groups based in West Africa, are expanding their operations transnationally. These groups are adept at online financial scams such as romance, investment, advance fees, and cryptocurrency fraud (INTREPOL, 2024).

Americas: Impersonation, romance, tech support, advance payment, and telecom fraud are the most prevalent types across the Americas. Human trafficking-related fraud is on the rise, as demonstrated by INTERPOL's Operation Turquesa V, which uncovered that hundreds were trafficked from the region after being deceived through messaging apps and social media into committing crimes like investment fraud and pig butchering. Additionally, there is growing evidence that Latin American criminal organizations, including Commando Vermelho, Primeiro Comando da Capital (PCC), and Cartel Jalisco New Generation (CJNG), are engaging in financial fraud (INTREPOL, 2024).

Asia: Pig butchering fraud originated in Asia in 2019 and proliferated during the COVID-19 pandemic, establishing the region as a central hub for these schemes, where criminal organizations adopt corporate-like frameworks. In addition, Asia has seen a significant increase in specific telecommunication fraud, where criminals pose as law enforcement or bank officials to deceive victims into revealing sensitive financial information or transferring large sums of money. This type of fraud has become particularly rampant across economically disadvantaged areas within Asia (INTREPOL, 2024).

Europe: In Europe, online investment frauds, phishing, and other financial schemes have intensified, targeting specific victims for maximum profit. Mobile phone apps are increasingly becoming a focus for cybercriminals. The criminal networks behind these operations exhibit sophisticated and intricate methods, often blending various types of fraud. Additionally, pig butchering scams, primarily operated from call centers in Southeast Asia, are experiencing a surge (INTREPOL, 2024).

International cooperation and robust cybersecurity measures become imperative as cybercriminals continue to harness more sophisticated techniques and broaden their geographic targets.

The diversity of fraud types—from high-tech scams in Europe and Asia to complex, transnational operations in Africa and the Americas—highlights the necessity for adaptive and proactive approaches to law enforcement and prevention strategies.

Ultimately, enhancing global vigilance and strengthening legal frameworks will be crucial in curtailing the escalation of these pervasive financial crimes (U. S. Department of Treasury FinCEN, 2023).

International Cooperation

Given the global nature of pig butchering scams, international cooperation is essential for effective enforcement. The Criminal Investigation U. S. Internal Revenue Service (IRS; 2023) warned tax payers at the International Fraud Awareness Week, which took place Nov. 12 – 18, not to get scammed by pig butchers. Collaborative efforts between countries can facilitate the tracking and prosecuting of cybercriminals, even when they operate across borders. Organizations like INTERPOL and Europol are vital in coordinating these efforts and supporting national law enforcement agencies (Whittaker et al., 2024).

In this qualitative study, the methodology for collecting and analyzing existing literature involved a systematic review of scholarly articles, as recommended by Zhang et al. (2024). Tiwari (2024) asserts that conducting a literature review is crucial for comprehensively synthesizing previous research findings. The primary purpose of employing a literature review approach in this study was to identify gaps in the existing research, thus strengthening the foundation for further investigation. Zhang et al. (2024) stated that literature reviews are critical for evaluating the current state of research, including its strengths, weaknesses, and unaddressed areas. Nursansiwi (2024) also notes that literature reviews play a significant role in delineating the connections between various academic works and their collective contributions to the subject matter and related fields. Through this literature review, the researcher skillfully navigated the complexities of various academic material (Nursansiwi, 2024). The execution of this comprehensive literature review entailed examining publications up to the year 2024. The research utilized a variety of search terms relevant to risk management in the fields of project management and cybersecurity. The literature search, conducted from November 2023 to July 2024, methodically used targeted keywords such as *cybersecurity*, *financial fraud*, *pig butchring*, *proactive defense*, *riskaware*, *social engineering*, and *trust manipulation* with a focus on fraud.

This precise use of keywords was crucial for getting articles pertinent to the research themes. The search strategy included specialized academic databases and publicly accessible web resources, such as EBSCO's databases, IEEE Xplore, the Homeland Security Digital Library, the ProQuest Dissertation Database, and ABI Inform Complete, as well as Google Scholar for the latest peer-reviewed publications. This diligent approach facilitated the organization of the literature in a way that underscored its significance to the research.

This research is guided by a well-defined theoretical framework and conceptual framework that provides a structured approach to comprehending and analyzing the complexities of pig butchering scams. Based on the Social Engineering Threats Theory, the theoretical framework delves into the psychological manipulation tactics scammers use to exploit victims effectively (Montañez et al., 2020). Concurrently, the conceptual framework, the Cybersecurity Measures Framework, focuses on evaluating the efficacy of various proactive cybersecurity measures designed to mitigate such scams. Together, these frameworks form the backbone of this research, enhancing the analysis of these sophisticated human and technical dimensions of fraud, thereby enabling a comprehensive exploration of preventative strategies.

Social Engineering Threats Theory

The social engineering threats theory exploits human vulnerabilities within information system security (Aijaz & Nazir, 2024). This theory is the optimal theoretical framework for studying pig butchering scams, as these scams are fundamentally about manipulating human behavior and decision-making. Further, this framework emphasizes understanding scammers' psychological techniques to exploit trust and induce victims to part with their money (Montañez et al., 2020). The research is grounded in analyzing these interpersonal tactics, making this theory highly relevant (Aijaz & Nazir, 2024). The framework's connection to this research is its focus on the psychological manipulation inherent in pig butchering scams, aiming to dissect the social engineering tactics employed. This theory helps unpack how scammers build trust and deceive their targets, directly connecting to the research study's goal of understanding and mitigating such frauds. The social engineering threats theory is not without critique.

As given by Washo (2021), focusing exclusively on individual psychology may only fully safeguard an organization if the systems and the broader company culture are noticed. Similarly, emphasizing only the technological systems neglects the crucial role of the employees who manage them and disregards the collective strength of the workforce. In other words, critics of social engineering theory might argue that it overemphasizes individual responsibility and underplays the role of systemic vulnerabilities in technology and regulation that enable such scams (Washo, 2021). Critics suggest that focusing solely on individual interactions may overlook broader preventive strategies.

Conceptual Framework

The Cybersecurity Measures Framework is an ideal conceptual framework for this research because it provides a structured approach to analyzing the effectiveness of different security measures in preventing pig butchering scams (Melaku, 2023). It integrates technological, educational, and regulatory dimensions, offering a comprehensive view of potential defenses (Melaku, 2023).

This holistic perspective ensures that the analysis addresses the technological vulnerabilities and encompasses the human and organizational factors critical to enhancing overall security resilience. The connection of this framework to this research is that the cybersecurity measures framework, a practical and comprehensive approach, is applied to evaluate the proactive cybersecurity measures (Melaku, 2023) that can be implemented to thwart pig butchering scams. It provides a basis for assessing how different strategies — from technological solutions to educational programs — can shield individuals and businesses from these frauds, making it a crucial tool in our research (Melaku, 2023). This framework is not without critiques.

A noted critique of the cybersecurity measures framework is its potential over-reliance on technological solutions, which may not fully address the human factors involved in social engine A noted critique of the cybersecurity measures framework is its potential overreliance on technological solutions, which may not fully address the human factors involved in social engineering scams. Additionally, critics argue that the framework might need to capture cyber threats' dynamic and evolving nature adequately, necessitating continuous updates to remain effective (Safitra et al., 2023).

Both frameworks are not only crucial for a comprehensive understanding of pig butchering scams but also have significant practical implications. While the Social Engineering Theory provides deep insights into the human aspects of these frauds, the Cybersecurity Measures Framework offers a practical approach to developing and implementing effective countermeasures. Combining insights from both frameworks could lead to more robust and adaptive strategies to combat these sophisticated cyber threats. This integrated approach enables a dual focus on both preventing initial exploitation and mitigating potential damages, thereby enhancing both preemptive and reactive capabilities. Furthermore, it encourages a dynamic feedback loop where lessons learned from addressing these scams are continuously integrated into security practices.

CONCLUSIONS

The phenomenon of pig butchering scams represents a significant and evolving challenge in the field of cybercrime. This research aimed to dissect the methods of psychological manipulation, explore the digital platforms that facilitate such scams, and propose effective cybersecurity measures to counter them.

The research's examination of psychological manipulation techniques exposed that scammers are skilled at creating scenarios that echo directly with their targets. The emotional complexity of these relations often induces victims to obligate sizable sums of money, blinded by the trust and emotional bond the victims think they share with the fraudsters. Cybersecurity training programs should integrate modules on the psychological maneuvers utilized by fraudsters, assisting people to distinguish and challenge exploitation to apply these findings in practical settings. Also, ascertaining psychological support systems for victims, comprising counseling services and peer support groups, can support in the recovery progression and diminish long-term psychological impacts.

The utilization of digital platforms is the battleground on which these scams unfold. Through detailed analysis, this study identified that platforms like dating apps, social media sites, and even professional networking sites are manipulated by scammers. These platforms are chosen for their broad user bases and the ease with which personal connections can be made and nurtured. Enhanced privacy features, while beneficial for legitimate users, also allow scammers to operate anonymously, making them difficult to trace.

Addressing the second aim, this study considered different cybersecurity measures that could be realized to lessen the threat from these scams. It became apparent that while technical defenses are vital, they must be united with robust educational programs to be effective. Cybersecurity software that flags possible scam actions can only succeed if consumers are educated on distinguishing and responding to these warnings. Also, regulatory strategies need strengthening, particularly regarding cryptocurrencies, which scammers have exploited due to their anonymity and ease of transacting across borders. Explicit examples of actionable moves for policymakers comprise the formation of international task forces to facilitate cross-border examinations and the conception of unified regulatory standards for cryptocurrency transactions.

The implications of these findings for policy and practice are manifold. At the policy level, there is a distinct directive toward the need for international cooperation, these scams are not narrowed to geographic boundaries. Explicit examples of actionable steps for policymakers comprise creating international task forces to facilitate cross-border investigations and forming unified regulatory standards for cryptocurrency transactions. Policies must progress to maintain pace with the changing technologies that these scams misuse, for instance incorporating innovative machine learning algorithms for real-time fraud detection and augmenting data-sharing protocols amongst financial institutions and law enforcement agencies.

Scientific and Practical academic discourses exist for this work. Scientifically, this research adds meaningfully to the academic body of knowledge by plotting the operations of pig butchering scams within the broader range of financial fraud. It lengthens the comprehension of the manner that cybercriminals familiarize with and ill-use new technological environments, offering a foundation for future studies on cyber fraud and social engineering schemes.

Practically, this study offers actionable insights that can guide the development of more effective cybersecurity strategies and regulatory policies. For example, the results can inform the design of public awareness campaigns to educate people regarding collective scam practices. The study also advocates the application of augmented cybersecurity measures like multi-factor authentication and blockchain analysis tools to footprint illegal transactions. These practical applications are vital for lessening the effect of pig butchering scams on people and organizations."

Notwithstanding the given insights, this study recognizes evident limitations, such as the potential underreporting of these scams, which could tilt the comprehension of their true scope and impact. Moreover, the precipitous progression of scamming techniques continuously challenge researchers and practitioners. Also, the geographical and cultural diversity of victims adds another layer of involvedness, affecting the generalizability of prevention and intervention strategies across different regions.

Future research should focus on developing predictive models to anticipate new scamming trends and conducting longitudinal studies to assess the long-term psychological impacts on victims. In addition exploring the integration of artificial intelligence and machine learning could refine detection capabilities and automate responses to emerging threats. Research could lead to more effective prevention strategies and support systems, ultimately enhancing the resilience of individuals and communities against these complex cyber threats.

In conclusion, while this research has significantly advanced the understanding of pig butchering scams, the dynamic nature of cyber threats demands continual vigilance and adaptation. Building on this study's findings and recommendations, future research can continue to uncover and counteract cybercriminals' evolving tactics globally. Collective works between researchers, policymakers, and practitioners are vital to emerging far-reaching strategies that can endure complex threats.

Author Contributions: Conceptualisation: S. L. B.; Data curation: P. D. V. M.; Formal analysis: S. L. B.; Investigation: S. L. B. and P. D. V. M.; Methodology: S. L. B.; Project administration: P. D. V. M.; Supervision: S. L. B.; Visualisation: P. D. V. M.; Writing – original draft: S. L. B.; Writing – review & editing: P. D. V. M.

Acknowledgements

Not applicable.

Conflicts of Interest

The author declares no conflict of interest.

Data Availability Statement

Not applicable.

Informed Consent Statement

Not applicable.

References

1. Aijaz, M., & Nazir, M. (2024). Modelling and analysis of social engineering threats using the attack tree and the Markov model. International *Journal of Information Technology*, 16, 1231–1238. [CrossRef]
2. Alt, R. (2021). Electronic markets on digital platforms and AI. *Electronic Markets*, 31, 233-241. [CrossRef]
3. Australian Federal Police (2024, January 21). *Pig Butchering Scam Targeting Australians as AFP Warns Lonely Hearts to Be Wary this Valentine's Day*. [Link]
4. Bansal, T. (2023). Regulation of Cybercrimes and Penalties: A Comparative Analysis. *Jus Corpus Law Journal*, 4, 95. [Link]
5. Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). *Tainted love: a systematic literature review of online romance scam research.* Interacting with Computers. [CrossRef]
6. British Chamber of Commerce Dubai (2024, May 15). *Protect yourself from pig butchering scams.* [Link]
7. Burton, S. L. (2022).*Cybersecurity leadership from a Telemedicine/Telehealth knowledge and organizational development examination* (Order No. 29066056). Available from ProQuest Central; ProQuest Dissertations & Theses Global. (2662752457). [Link]
8. Button, M. & Cross, C. (2017). *Cyber frauds, scams and their victims*. (1st. ed.). Routledge. [CrossRef]
9. Caldeira, M. & Correia, M. (2021). Blockchain address transparency with DNS," *In the 2021 IEEE Symposium on Computers and Communications (ISCC)*, Athens, Greece, pp. 1-7. [CrossRef]
10. Chiu, I. H. Y. (2024). Prudential Regulation Policy Responses to Financial Technological Innovations: The Future for Banks and Crypto-Finance? In: Bodellini, M., Gimigliano, G., Singh, D. (eds). *Commercial Banking in Transition. Palgrave Macmillan Studies in Banking and Financial Institutions*. Palgrave Macmillan, Cham. [CrossRef]
11. Congressional Research Service (2023, May 16). *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes*. [Link]
12. Congressional Research Service. (2020, September 21). *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*. [Link]
13. Criminal Investigation U. S. Internal Revenue Service (2023). *CI Issues Red Flags, Tips To Avoid Falling Victim To Pig Butchering Schemes During International Fraud Awareness Week*. [Link]
14. Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*. [CrossRef]
15. Efijemue, O., Obunadike, C., Olisah, S., Taiwo, E., Kizor, S., Odooh, C., & Ejimofor, I. (2023). *Cybersecurity Strategies for Safeguarding Customers Data and Preventing Financial Fraud in The United States Financial Sectors*. [Link]
16. Ene, W. R., & Imo, A. S. (2024). Cybercrime and its implications for human capital development: A study of Otuoke Community, Fuo Students. *Fuoye Journal Of Criminology And Security Studies, 3*(2). [Link]

17. Farivar, C. (2022, October 25). How one man lost $1 million to a crypto 'Super Scam' called pig butchering. *Forbes*. [Link]
18. Federal Bureau of Investigation and Internet Crime and Complaint Center (2023). *The FBI Warns Of False Job Advertisements Linked To Labor Trafficking At Scam Compounds*. Alert Number I-052223-PSA. [Link]
19. Federal Bureau of Investigation Internet Crime Complaint Center (2021). *Federal Bureau of Investigation Internet Crime Report 2022: Business email compromise*. [Link]
20. Federal Bureau of Investigation Internet Crime Complaint Center (2021). *Federal Bureau of Investigation Internet Crime Report 2021: Confidence fraud / romance scams*. [Link]
21. Finra. (2022, December 13*). Pig butchering scams: What they are and how to avoid them*. [Link]
22. Gore, L. (2024, February 6). *FBI Issues warning about 'pig butchering' online scam*. Government Technology. [Link]
23. Griffin, J. M., & Mei, K. (2024, February 24). *How Do Crypto Flows Finance Slavery? The Economics Of Pig Butchering*. SSRN, Elsevier. [Link]
24. Guha, S., & Matilal, S. (2023). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021-A Reassessment of the Contours and Limits. *National University for Juridical Science (NUJS) Journal of Regulatory Studies*, 8, 32. [Link]
25. Guo, L., Sang, B., Tu, J., & Wang, Y. (2024). Cross-cryptocurrency return predictability. *Journal of Economic Dynamics and Control*, 163, 104863. [CrossRef]
26. Han, B. (2023). *Individual frauds in China: exploring the impact and response to telecommunication network fraud and pig butchering scams* (Doctoral dissertation, Ph. D. University of Portsmouth). [Link]
27. Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science*, 10. [CrossRef]
28. Internal Revenue Service (2023). *CI issues red flags, tips to avoid falling victim to pig butchering schemes during International Fraud Awareness Week.* [Link]
29. INTREPOL (2024, March 11). INTERPOL financial fraud assessment: A global threat boosted by technology. [Link]
30. Jackson, W. (2024, May 15*). How South-East Asia's pig butchering scammers are using artificial intelligence technology*. ABC News. [Link]
31. Jones, L. A. (2021). A content analysis review of literature to create a useable framework for reputation risk management. *Handbook of Research on Multidisciplinary Perspectives on Managerial and Leadership Psychology*, 91-133. [CrossRef]
32. Kanchan, S., & Gaidhane, A. (2023). Social media role and its impact on public health: A narrative review. *Cureus, 15*(1). [CrossRef]
33. Khan, A., Krishnan, S., & Arayankalam, J. (2022). The Role of ICT Laws and national culture in determining ict diffusion and well-being: A cross-country examination. *Informations System Frontier*, 24, 415–440. [CrossRef]
34. Lafourcade, P., & Lombard-Platet, M. (2020). About blockchain interoperability. *Information Processing Letters*, 161, 105976. [CrossRef]
35. Lee, S. S., Murashkin, A., Derka, M., & Gorzny, J. (2023, May). Sok: Not quite water under the bridge: Review of cross-chain bridge hacks. *In 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-14). IEEE. [CrossRef]
36. Levi, M., & Smith, R. G. (2022). *Fraud and pandemics. Journal of Financial Crime, 29*(2), 413-432. [CrossRef]
37. Maras, M., & Ives, E. R. (2024). Deconstructing a Form of Hybrid Investment Fraud: Examining 'Pig Butchering' in the United States. *Journal of Economic Criminology*, 100066. [Crossref]
38. Marsanic, D. (2023, October 3). *Decoding Thailand's $277M 'pig butchering' crypto scam*. Dailycoin. [Link]
39. Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327-350. [CrossRef]
40. Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, 11. [CrossRef]
41. Moreno, F. R., Barker, K., Griffin, J. G. H., & Collingwood, L. (2023). *BILETA Response to Review of the Computer Misuse Act 1990*. BILETA. [Link]

42. Nursansiwi, D. A. (2024). The role of forensic accounting in detecting financial frauds. *Accounting Studies and Tax Journal (COUNT)*, *1*(1), 111-116. [CrossRef]
43. Ogundiran, A., Chi, H., Yan, J., & Miller, J. (2024). Forensic analysis of Social Media Android Apps via Timelines. *In:* Arai, K. (eds.). *Advances in Information and Communication. FICC 2024. Lecture Notes in Networks and Systems*, 921. Springer, Cham. [CrossRef]
44. Osman, M. B., Urom, C., Guesmi, K., & Benkraiem, R. (2024). Economic sentiment and the cryptocurrency market in the post-COVID-19 era. *International Review of Financial Analysis*, 91, 102962. [CrossRef]
45. Pandey, V. (2023). Measures and emerging difficulties in information technology act. *International Journal of Criminal, Common, and Statutory Law*, *3*(1), 20-24. [Link]
46. Pérez-Escolar, M., & Canet, F. (2023). Research on vulnerable people and digital inclusion: toward a consolidated taxonomical framework. *Univ Access Inf Soc* 22, 1059–1072. [CrossRef]
47. Podkul, C. (2022). *What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One?* Pro Publica Inc. [Link]
48. Ratiu, R. (2024, February 12). *Securing the Future: Enhancing Cybersecurity in 2024 and beyond*. ISACA. [Link]
49. Rattan, J., & Rattan, V. (2022). Role of Information and Communication Technologies in the Metamorphosis of Justice Administration in India: A Legal Study. *Indian Journal of Public Administration*. [CrossRef]
50. Rotenberg, K. J. (2021). *The psychology of interpersonal trust: Theory and research* (1st ed.). Routledge. [CrossRef]
51. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369. [CrossRef]
52. Sarkar, G., & Shukla, S. K. (2024). Bi-Directional Exploitation of Human Trafficking Victims: Both Targets and Perpetrators in Cybercrime. *Journal of Human Trafficking*, 1-22. [CrossRef]
53. Sultana, T. (2020). Email based spam detection. *International Journal of Engineering Research*, *9*(6). [CrossRef]
54. Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28-38. [CrossRef]
55. State of Michigan Consumer Protection (2024). *Cryptocurrency scam: Pig Butchering*. [Link]
56. Tiwari, M., Ferrill, J. & Allan, D. M. C. (2024). Trade-based money laundering: a systematic literature review. *Journal of Accounting Literature*. [CrossRef]
57. U. S. Department of Justice (2024, May 17). *Two foreign nationals arrested for laundering at least $73M through shell companies tied to cryptocurrency investment scams*. [Link]
58. U. S. Department of Justice's Office of Justice Programs (2020, August 14). *Fraud awareness: Special feature*. [Link]
59. U. S. Immigration and Customs Enforcement (2023, April 28). *HSI, ACAMS issue guidance on combating financial fraud, other crypto scams*. [Link]
60. U. S. Treasury FinCEN (2023, September 8). *FinCEN Alert on prevalent virtual currency investment scam commonly known as "Pig Butchering."* [Link]
61. United States Attorney's Office Central District of California. (2024, April 3). *Justice Dept. seizes over $112M in funds linked to cryptocurrency investment schemes, with over half seized in Los Angeles case*. [Link]
62. United States Attorney's Office District of Massachusetts. (2024, March 13). *United States Files Forfeiture Action to Recover Cryptocurrency Traceable to Pig Butchering Romance Scam*. [Link]
63. United States Secret Service. (2024). *Stay safe online: Avoid romance scams*. [Link]
64. Wall, D. S. (2017). *Policing identity crimes. In Policing cybercrime* (pp. 29-52). Routledge. [Link]
65. Wang, F. (2024). Victim-offender overlap: the identity transformations experienced by trafficked Chinese workers escaping from pig-butchering scam syndicate. *Trends in Organized Crime*, 1-32. [CrossRef]
66. Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, 4, 100126. [CrossRef]

67. Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of “pig butchering” (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, 3, 100052. [CrossRef]
68. Yu, L. W. (2023). The Crime of of "Pig-butchering Scams" in the Securities Market and Legal Regulation *Science of Law Journal*, *2*(1), 41-52. [CrossRef]
69. Zhang, L., Carter Jr., R. A., Greene, J. A., & Bernacki, M. L. (2024). Unraveling challenges with the implementation of universal design for learning: A systematic literature review. *Educational Psychology Review*, *36*(1), 35. [CrossRef]