Lab 4

Influence, Vectors and Techniques

Group 2

, Abdul-Ramon Adeyemi Folarin, &

, , , &

School of Information Technology Administration & Security, Seneca Polytechnic

DPI914NIA: Social Engineering

Professors Chris Robertson & Suranjit Paul

June 3, 2026

Student Integrity Statement: I/we declare that the attached assignment is my/our own work in accordance with the Seneca Academic Policy. No part of this assignment has been copied manually or electronically from any other source (including web sites) or distributed to other students

Table of Contents

Table of Figures 5
1. Introduction 6
2. Research 7
3. Definitions 8
Original Attack 8
Complex Attack 8
Principles of Influence 8
4. Ranked Attacks 9
Rank 1: Arup Deepfake Video Call Fraud, Reported January 29, 2024 9
Summary 9
Diagram 9
Explanation 10
Influence 10
Vector 10
Technique 10
Rank 2: MGM Resorts Scattered Spider Vishing Attack, September 11, 2023 12
Summary 12
Diagram 12
Explanation 13
Influence 13
Vector 13
Technique 13
Rank 3: Caesars Entertainment Scattered Spider Attack, September 7, 2023 14
Summary 14
Diagram 14
Explanation 15
Influence 15
Vector 15
Technique 15
Rank 4: Coinbase Insider Bribery and Targeted Social Engineering, Disclosed May 15, 2025 17
Summary 17
Diagram 17
Explanation 18
Influence 18

Vector 18
Technique 18
Rank 5: ClickFix SEO Poisoning and Fake Browser Update Campaign (2024-2025) 20
Summary 20
Diagram 20
Explanation 21
Influence 21
Vector 21
Technique 21
Rank 6: WPP CEO Deepfake WhatsApp Scam, May 10, 2024 23
Summary 23
Diagram 23
Explanation 24
Influence 24
Vector 24
Technique 24
Rank 7: CoGUI Mass Phishing Campaign Targeting Japan, January to April 2025, Reported May 6, 2025 26
Summary 26
Diagram 26
Explanation 27
Influence 27
Vector 27
Technique 27
Rank 8: Marks and Spencer Coordinated Retail Phishing and Credential Attack, April 22, 2025 29
Summary 29
Diagram 29
Explanation 30
Influence 30
Vector 30
Technique 30
Rank 9: Change Healthcare Credential-Based Network Intrusion, Initial Access February 12, 2024 and Ransomware February 21, 2024 31
Summary 31
Diagram 31

Explanation 32
Influence 32
Vector 32
Technique 32
Rank 10: Fake Road Toll Smishing Surge, FBI Alert April 12, 2024 34
Summary 34
Diagram 34
Explanation 35
Influence 35
Vector 35
Technique 35
5. Conclusion 36
6. References 37
7. Bibliography 40

Table of Figures

Figure 1 Arup Deepfake Video Call Fraud Diagram....9
Figure 2 MGM Resorts Scattered Spider Vishing Attack Diagram....12
Figure 3 Caesars Entertainment Scattered Spider Attack Diagram....14
Figure 4 Coinbase Insider Bribery and Targeted Social Engineering Diagram....17
Figure 5 ClickFix SEO Poisoning and Fake Browser Update Campaign diagram....20
Figure 6 WPP CEO Deepfake WhatsApp Scam diagram....23
Figure 7 CoGUI Mass Phishing Campaign Targeting Japan Diagram....26
Figure 8 Marks and Spencer Coordinated Retail Phishing and Credential Attack diagram....29
Figure 9 Change Healthcare Credential-Based Network Intrusion diagram....31
Figure 10 Fake Road Toll Smishing Surge (E-ZPass and Similar Agencies) diagram....34

1. Introduction

In this lab, we researched recent real-world social engineering attacks (from lab 2) to better understand how attackers are using human trust, business processes, and communication channels to compromise organizations and individuals. As a group, we focused on attacks from 2023 to 2025 that showed different levels of originality and complexity, including deepfake impersonation, vishing, insider bribery, phishing kits, SEO poisoning, SMS phishing, and credential-based intrusions [1], [4], [7], [9], [10]. We chose these cases because they show that social engineering is not limited to simple phishing emails; attackers are now combining technical tools with psychological pressure, trusted brands, executive authority, and weak verification processes to make their attacks more convincing [5], [6], [12]. The purpose of this report is to identify ten recent social engineering attacks, explain how each attack worked, and rank them from most original and complex to least original and complex. Each ranked section includes a summary, a diagram showing the attack flow, an explanation of why the attack received its ranking, an analysis of which principles of influence were applied, the attack vectors used, and the specific techniques employed.

2. Research

We identified the ten attacks below by surveying incidents from 2023 to 2025 across institutional reports, industry research, cybersecurity vendor reports, and news coverage. The most substantive sourcing came from the FBI IC3 2024 Annual Report, Verizon's 2025 Data Breach Investigations Report, and Palo Alto Networks Unit 42's 2025 Global Incident Response Report [7], [9], [10]. The Unit 42 report was particularly useful because it identified social engineering techniques such as ClickFix as confirmed initial access vectors in enterprise incident response cases [7]. Cybersecurity outlets and industry sources including ZeroFox, Secureframe, Mitnick Security, and Communications of the ACM were used to add broader context on recent social engineering trends and attack methods [4], [5], [6], [12]. CNN and the World Economic Forum were used for post-incident reporting on the Arup deepfake fraud case [1], [2]. Additional reporting was used to confirm exact dates and operational details for incidents such as WPP, CoGUI, Coinbase, Change Healthcare, and the FBI toll smishing alert [13], [14], [15], [16], [17]. We required at least two independent sources to confirm the core facts of each attack before including it. The final selection was deliberately varied across different techniques, sectors, and levels of sophistication to avoid a list that only reflected whichever attack type happened to dominate headlines in a given month.

The following ten social engineering attacks were identified:

- Arup Deepfake Video Call Fraud (reported January 29, 2024)
- MGM Resorts Scattered Spider Vishing Attack (September 11, 2023)
- Caesars Entertainment Scattered Spider Attack (September 7, 2023)
- Coinbase Insider Bribery and Targeted Social Engineering (disclosed May 15, 2025)
- ClickFix SEO Poisoning and Fake Browser Update Campaign (2024 to 2025)
- WPP CEO Deepfake WhatsApp Scam (May 10, 2024)
- CoGUI Mass Phishing Campaign Targeting Japan (January to April 2025, reported May 6, 2025)
- Marks and Spencer Coordinated Retail Phishing and Credential Attack (April 22, 2025)
- Change Healthcare Credential-Based Network Intrusion (initial access February 12, 2024; ransomware deployment February 21, 2024)
- Fake Road Toll Smishing Surge (FBI alert April 12, 2024)

3. Definitions

Original Attack

We consider an original attack is one that forces defenders to revise their assumptions about what can be weaponized. The key question is whether the technique was genuinely new at the time of execution, not just well-executed, but unexpected in some meaningful way. That newness can show up in the attack vector, the delivery medium, how trust is established, or how a familiar workflow is turned against its intended purpose. A flawlessly executed spear-phishing email against a standard corporate inbox scores low on originality regardless of how convincing it is. An attack that exploits a system or behaviour nobody had thought to exploit before scores high.

Complex Attack

Whereas we consider a complex attack requires sustained effort across multiple stages before the final objective is reached. Complexity is measured by how much had to go right for the attack to work: the depth of pre-attack reconnaissance, how many independent components had to operate in sequence, how tightly the attacker had to adapt to the specific target, and how difficult the chain would have been to detect or interrupt at any point. Sending a bulk phishing email is not complex; it requires almost nothing to go right individually. An attack that required custom AI model training, live multi-person coordination, and pre-positioned financial accounts across five banks before a single dollar moved is.

Principles of Influence

For this lab, we use Cialdini's six principles of influence to analyze how each attack psychologically manipulated its targets:

- **Reciprocity:** The target feels obligated to return a favour or exchange.
- **Commitment and Consistency:** Once a person starts a course of action, they feel pressure to continue it.
- **Social Proof:** People follow the lead of others or defer to signals of group validation.
- **Authority:** People comply with those who appear to be legitimate figures of authority.
- **Liking:** People are more easily influenced by those they know, like, or find familiar.
- **Scarcity:** Urgency or limited availability pressures people into acting quickly without full verification.

4. Ranked Attacks

Rank 1: Arup Deepfake Video Call Fraud, Reported January 29, 2024

Rank: 1 of 10

Title: Arup Deepfake Video Call Fraud

Summary

On January 29, 2024, Hong Kong police received a report involving a deepfake video conference fraud later publicly identified as involving Arup, a multinational engineering firm based in the United Kingdom [1], [2]. A finance employee was tricked into transferring approximately USD 25.6 million after receiving a phishing email impersonating the company's CFO and then joining a video conference containing AI-generated deepfakes of senior executives [1], [3]. The employee initially suspected the email was suspicious, but the realistic video call convinced him that the request was legitimate [1]. He authorized 15 wire transfers totaling approximately USD 25.6 million across five attacker-controlled bank accounts [1], [8]. The fraud was discovered only after the employee contacted Arup headquarters in London and learned that no such meeting or transfer request had been authorized [1], [2].

Diagram

The diagram below shows the steps and flow of this attack:

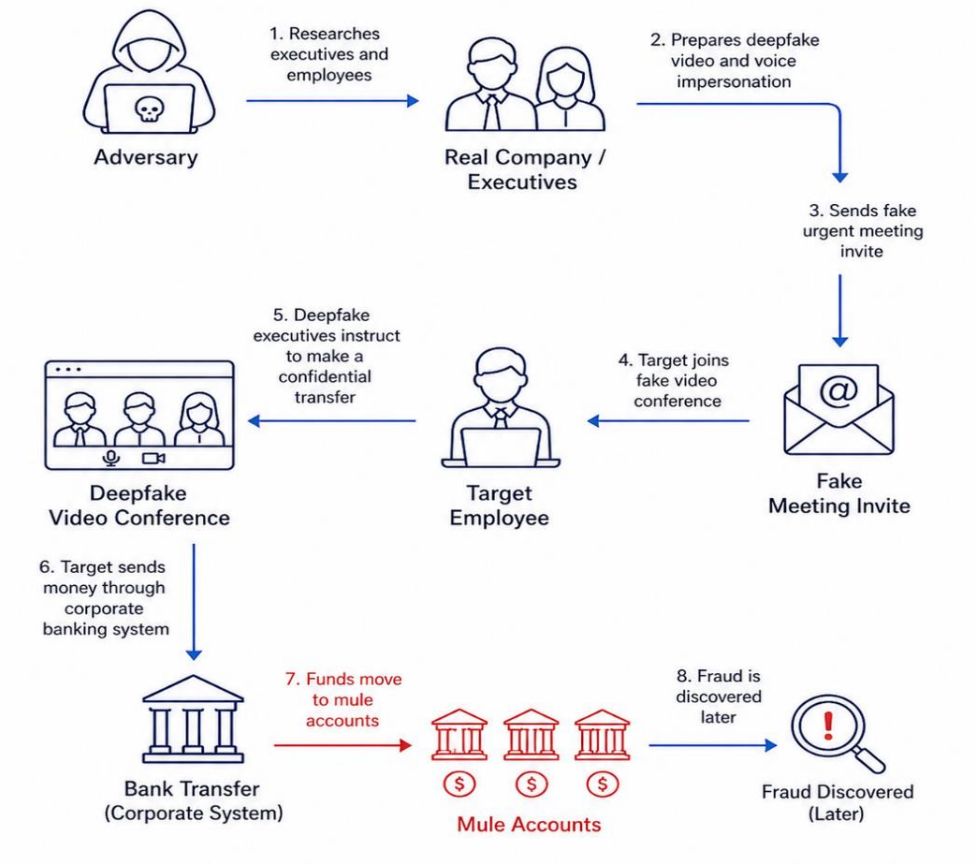


Figure 1 Arup Deepfake Video Call Fraud Diagram

Figure 1 shows how the attacker researched company executives, prepared deepfake video and voice impersonation, and used a fake meeting invite to convince the target employee to join a fraudulent video conference [1], [2]. During the call, the deepfake executives instructed the employee to make a confidential transfer, causing funds to move through the corporate banking system into mule accounts before the fraud was later discovered [1], [8].

Explanation

What puts this attack above everything else on this list is that the employee did everything right and still lost. He was suspicious of the phishing email, but the attackers anticipated that doubt and used a live video call with deepfake versions of multiple senior executives to override it [1], [2]. The attack did not exploit a misconfigured system or an untrained user; it exploited trust in visual proof during a business meeting [1], [3]. The operational requirements were substantial: convincing AI-generated impersonation, real-time meeting coordination, and multiple bank accounts ready to receive the transfers [1], [8]. Any one of those components failing could have broken the chain, which is why this attack ranks first for both originality and complexity.

Influence

- **Authority:** The attackers impersonated the CFO and multiple senior executives. The target employee complied because the video call appeared to show people with legitimate financial authority over him, making the wire transfer request feel like a directive from leadership rather than a suspicious demand [1], [2].
- **Social Proof:** Multiple deepfake executives were present on the call at the same time. Seeing several senior colleagues apparently validate the same instruction reinforced the target's belief that the request was legitimate and collectively approved [1], [3].
- **Scarcity:** The transfer was framed as confidential and time-sensitive, encouraging the employee to act quickly and quietly without seeking additional verification or involving colleagues who might have raised concerns [1], [8].

Vector

- **Phishing:** The initial point of contact was a phishing email impersonating the CFO. The email was used to create the pretext for the video call and to invite the finance employee into the fraudulent meeting [1], [2].
- **Deepfake video call impersonation:** The primary delivery vehicle was a video conference in which AI-generated deepfakes of multiple senior executives were used in real time to convince the employee that the transfer request was legitimate [1], [3].

Technique

- **CEO/CFO fraud (Business Email Compromise):** The attack used the CFO's identity as the initial hook, which is a defining feature of BEC fraud. The goal was to manipulate a finance employee into authorizing large wire transfers by impersonating executive authority [1], [8].
- **Deepfake multi-person impersonation:** Rather than impersonating one executive, the attackers deployed deepfake versions of several senior employees simultaneously. This multi-person approach was intended to overwhelm any single point of doubt the target might have had [1], [2].

- **Pretexting:** A false scenario was constructed around a confidential executive meeting requiring urgent financial action. The pretext gave the employee a believable business reason to bypass standard authorization procedures [1], [3].
- **Wire fraud:** The ultimate goal was financial theft through 15 wire transfers sent across five separate attacker-controlled bank accounts, designed to complicate tracing and recovery [1], [8].

Rank 2: MGM Resorts Scattered Spider Vishing Attack, September 11, 2023

Rank: 2 of 10

Title: MGM Resorts Scattered Spider Vishing Attack

Summary

On September 11, 2023, MGM Resorts International publicly disclosed that it had identified a cybersecurity issue affecting several company systems [18]. Reporting later linked the attack to Scattered Spider and ALPHV/BlackCat activity [18], [19]. The attackers used social engineering rather than a traditional software exploit, researching an MGM employee and contacting the IT helpdesk while impersonating that employee [4], [6]. The helpdesk reset the credentials, which gave the attackers authenticated access to MGM's network [4], [6]. After gaining access, the attackers moved laterally and ransomware activity disrupted casino floors, digital room keys, reservation systems, and ATM infrastructure across multiple properties [6], [19]. MGM later reported major financial and operational losses from the incident [4], [19].

Diagram

The diagram below shows the steps and flow of this attack:

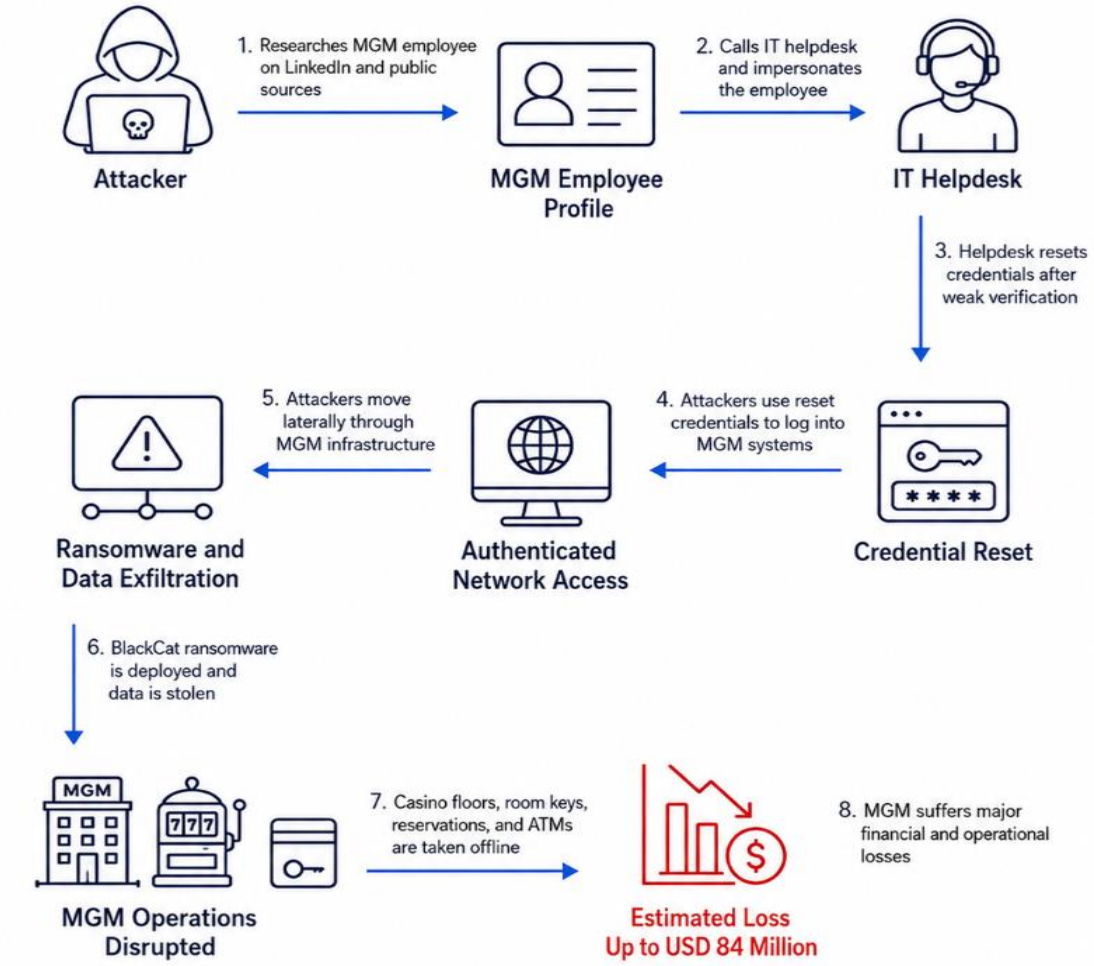


Figure 2 MGM Resorts Scattered Spider Vishing Attack Diagram

Figure 2 shows how the attackers researched an MGM employee, impersonated them in a call to the IT helpdesk, and convinced the helpdesk to reset the employee's credentials [4], [6]. The attackers then used the reset credentials to access MGM systems, move laterally, deploy ransomware, steal data, and disrupt casino operations, leading to major financial and operational losses [4], [19].

Explanation

The IT helpdesk is designed to be helpful, and Scattered Spider exploited that exact business function [4], [6]. The originality comes from turning a normal credential reset process into an initial access path, while the complexity comes from combining public employee research, vishing, credential reset abuse, lateral movement, and ransomware deployment [4], [6]. The attack is ranked second because it showed how a short social engineering call could bypass technical perimeter controls and lead to enterprise-wide disruption [18], [19].

Influence

- **Authority:** The attacker impersonated a real MGM employee, drawing on that employee's organizational identity and legitimate authority within the company. IT helpdesk staff are trained to assist employees, and impersonating one created an immediate entitlement to helpdesk services [4], [6].
- **Liking:** The attacker adopted a cooperative, friendly tone consistent with how a genuine employee would approach the helpdesk. By presenting as an approachable colleague in need of assistance, the attacker reduced the helpdesk agent's suspicion [4], [6].
- **Commitment and Consistency:** Once the helpdesk agent began the credential reset process, completing the request was consistent with standard IT procedure. Stopping partway through would have required the agent to actively break from established workflow, which creates psychological friction [4], [6].

Vector

- **Vishing:** The attacker called the MGM IT helpdesk by phone, using voice communication to impersonate an employee and request a credential reset without any in-person or document-based verification [4], [6].
- **Impersonation:** The attacker posed as a specific, real MGM employee whose identity had been researched in advance using LinkedIn or similar public sources. This gave the impersonation credibility beyond a generic social engineering attempt [4], [6].

Technique

- **Helpdesk impersonation:** The attacker called the IT helpdesk and posed as an employee who was locked out or needed a credential reset. Helpdesks are designed to recover access for employees, making them a structural weak point when identity verification is inadequate [4], [6].
- **Pretexting:** A believable scenario was constructed in which an employee appeared to have a legitimate access problem requiring helpdesk intervention. The pretext enabled the attacker to request credential changes without triggering additional scrutiny [4], [6].
- **Credential reset abuse:** The helpdesk's credential reset function was used as the actual initial access mechanism. Once the password was reset, the attacker had authenticated access to MGM systems without needing to exploit any technical vulnerability [4], [6].

Rank 3: Caesars Entertainment Scattered Spider Attack, September 7, 2023

Rank: 3 of 10

Title: Caesars Entertainment Scattered Spider Attack

Summary

On September 7, 2023, Caesars Entertainment determined that an unauthorized actor had acquired a copy of its loyalty program database, including driver's license numbers and Social Security numbers for a significant number of members [20]. Reporting linked the incident to Scattered Spider-style social engineering involving a third-party IT support vendor [4], [6]. Attackers impersonated a Caesars employee and convinced the vendor to reset credentials or provide access, giving the attackers a path into Caesars systems [4], [6]. The attackers exfiltrated loyalty program member data and threatened to publish it unless a ransom was paid [6], [20]. Caesars later disclosed the incident in a September 14, 2023 SEC filing, and reporting stated that the company paid approximately USD 15 million in ransom [20], [21].

Diagram

The diagram below shows the steps and flow of this attack:

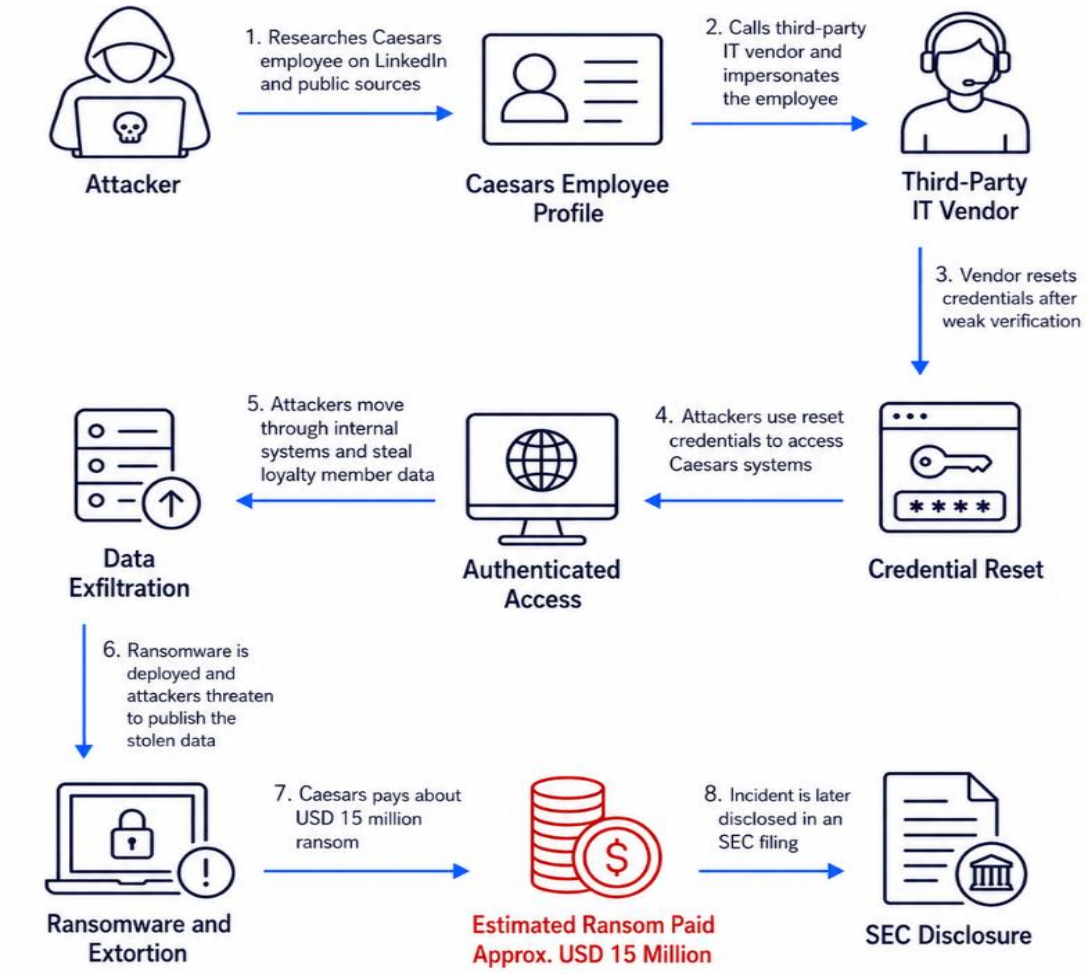


Figure 3 Caesars Entertainment Scattered Spider Attack Diagram

Figure 3 shows how the attackers researched a Caesars employee, impersonated them through a third-party IT vendor, and convinced the vendor to reset the employee's credentials [4], [6]. The attackers then used the reset credentials to access Caesars systems, steal loyalty member data, deploy ransomware, and pressure the company into paying an estimated USD 15 million ransom before the incident was later disclosed in an SEC filing [20], [21].

Explanation

This attack is ranked below MGM because it used a very similar Scattered Spider style of helpdesk or vendor-focused social engineering [4], [6]. However, the third-party IT vendor angle makes the Caesars case important because it shows how attackers can exploit trusted supplier relationships instead of attacking the organization directly [6], [20]. The attack was complex enough to include impersonation, vendor compromise, data theft, and extortion, but it was less original than the higher-ranked attacks because the overall method closely matched other Scattered Spider incidents [4], [6].

Influence

- **Authority:** By impersonating a Caesars employee, the attacker drew on the perceived authority of someone who already had a legitimate relationship with the vendor. The vendor's role was to support Caesars staff, so an apparent employee request carried built-in authority [4], [6].
- **Liking:** The vendor likely operated on a cooperative service model with Caesars employees. The attacker exploited the friendly, service-oriented relationship that third-party IT vendors typically maintain with their clients [4], [6].
- **Commitment and Consistency:** The vendor was operating within its normal service agreement by fulfilling what appeared to be a standard employee support request. Following through with credential assistance was consistent with the vendor's contractual and operational role [4], [6].

Vector

- **Vishing or impersonation through vendor channel:** The attacker contacted a third-party IT support vendor rather than Caesars directly, using impersonation to pose as a Caesars employee and obtain credential access through the vendor's support process [4], [6].
- **Supply chain / third-party targeting:** Rather than attacking Caesars head-on, the attacker targeted a trusted vendor with lower verification standards. This third-party pathway bypassed controls that might have existed if the request had been made directly to an internal Caesars helpdesk [6], [20].

Technique

- **Third-party vendor impersonation:** The attacker used the vendor relationship as an attack surface, knowing that the vendor was obligated to assist Caesars employees and likely had less rigorous identity verification than an internal helpdesk [4], [6].
- **Pretexting:** A false scenario was used to justify why a Caesars employee needed the vendor's help with credential access, consistent with the kind of routine requests the vendor would have handled regularly [4], [6].

- **Supply chain social engineering:** Targeting a supplier rather than the primary organization is a technique designed to exploit trust relationships and potentially weaker security controls in the vendor's environment [6], [20].
- **Extortion:** After exfiltrating the loyalty program database, the attackers threatened to publish the stolen data unless Caesars paid a ransom. This data extortion component was used as leverage to extract approximately USD 15 million [20], [21].

Rank 4: Coinbase Insider Bribery and Targeted Social Engineering, Disclosed May 15, 2025

Rank: 4 of 10

Title: Coinbase Insider Bribery and Targeted Social Engineering

Summary

On May 15, 2025, Coinbase disclosed that cybercriminals had bribed and recruited overseas customer support agents to steal sensitive customer data from internal systems [15]. The stolen information included personal customer details that could be used to make later impersonation attempts more convincing [15], [22]. The attackers then used the data to conduct targeted social engineering against Coinbase customers by impersonating Coinbase support staff [15], [22]. Coinbase stated that no passwords, private keys, or customer funds were directly exposed through the insider access, but some customers were tricked into sending funds to attackers [15]. Coinbase rejected a USD 20 million extortion demand and began remediation and reimbursement efforts, with estimated costs reaching hundreds of millions of dollars [15], [22].

Diagram

The diagram below shows the steps and flow of this attack:

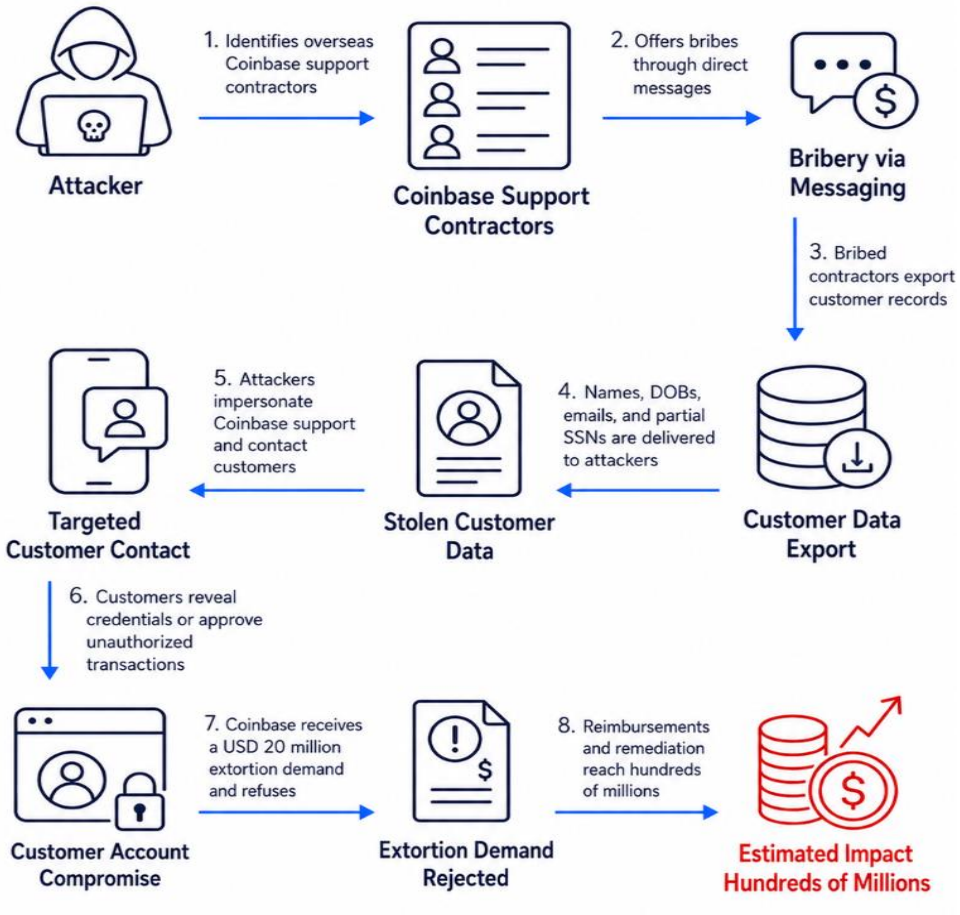


Figure 4 Coinbase Insider Bribery and Targeted Social Engineering Diagram

Figure 4 shows how attackers targeted overseas Coinbase support contractors, bribed them through direct messages, and used their access to export sensitive customer records [15], [22]. The stolen data was then used to impersonate Coinbase support, contact customers, compromise accounts through social engineering, and create a major financial impact after Coinbase rejected the extortion demand [15], [22].

Explanation

The most important part of this attack is that the first social engineering target was not the customer; it was the contractor with legitimate access [15], [22]. Recruiting insiders bypasses many technical controls because the data leaves through accounts that are supposed to have access to it [15]. The downstream customer impersonation was more conventional, but it became more convincing because the attackers had accurate personal data [15], [22]. This combination of insider recruitment and customer-targeted social engineering is why the attack ranks fourth.

Influence

- **Reciprocity:** The attackers offered financial bribes to overseas contractors in exchange for data access. By offering money first, the attackers created a sense of obligation and mutual exchange that encouraged contractors to act on their behalf [15], [22].
- **Authority:** When targeting Coinbase customers downstream, the attackers impersonated Coinbase's own support team, leveraging the brand's authority over its users. Customers were more likely to comply with requests that appeared to come from the platform they trusted [15], [22].
- **Liking:** Attackers likely used a low-pressure, friendly approach when recruiting contractors, making the initial bribe offer feel less like coercion and more like an informal opportunity. This reduced resistance before the contractor made a decision [15], [22].

Vector

- **Insider threat:** The primary vector was the direct recruitment and bribery of overseas Coinbase support contractors who already had legitimate access to customer data. The attack entered through trusted internal accounts rather than an external breach [15], [22].
- **Customer impersonation (support fraud):** Once data was collected, the attacker impersonated Coinbase customer support to contact real customers. This outbound impersonation was enabled entirely by the accuracy of the stolen customer records [15], [22].

Technique

- **Insider recruitment and bribery:** The attackers directly approached contractors with financial offers, bypassing technical defenses entirely by converting a legitimate insider into a threat actor. This technique is effective against organizations that rely on third-party or overseas support staff [15], [22].
- **Data-driven support impersonation:** Using the stolen customer data, the attackers could contact customers with accurate personal details, making impersonation of Coinbase support much more convincing than a generic phishing attempt [15], [22].

- **Extortion:** After obtaining the data and exfiltrating it, the attackers demanded USD 20 million from Coinbase to prevent publication. Coinbase refused and began remediation instead [15], [22].

Rank 5: ClickFix SEO Poisoning and Fake Browser Update Campaign (2024-2025)

Rank: 5 of 10

Title: ClickFix SEO Poisoning and Fake Browser Update Campaign

Summary

From 2024 into 2025, ClickFix became a major social engineering technique used for initial access in enterprise incidents [7]. Attackers used SEO poisoning and malvertising to push malicious pages into search results, making the pages appear trustworthy to users searching for software or troubleshooting help [7], [12]. When targets visited the spoofed page, they were shown a fake browser error, CAPTCHA, or update prompt [7], [12]. The page instructed the user to open the Windows Run dialog and paste a PowerShell command, causing the user to execute the malicious payload themselves [7], [12]. Palo Alto Networks Unit 42 identified ClickFix as a confirmed initial access vector in multiple enterprise cases [7].

Diagram

The diagram below shows the steps and flow of this attack:

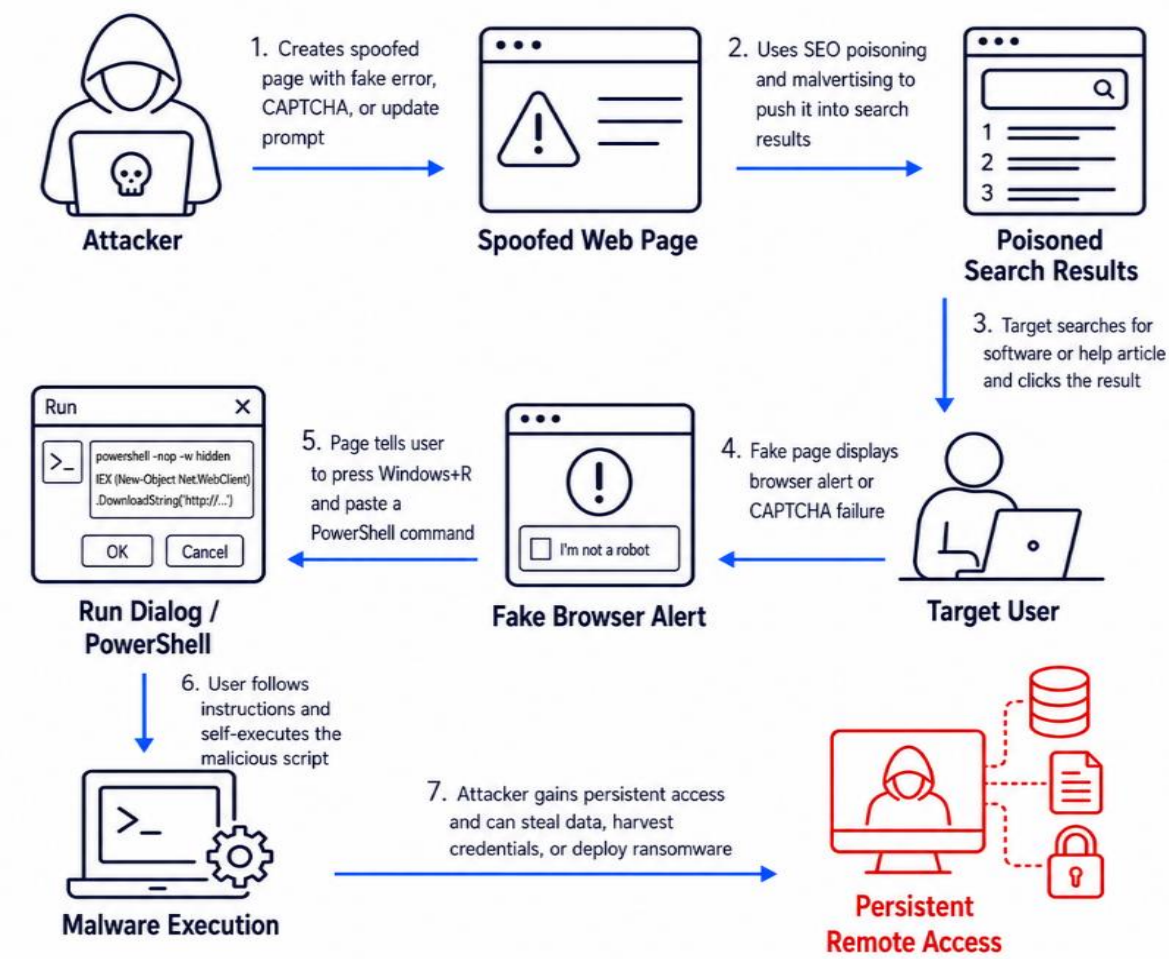


Figure 5 ClickFix SEO Poisoning and Fake Browser Update Campaign diagram

Figure 5 shows how the attacker created a spoofed webpage with a fake browser error, CAPTCHA, or update prompt, then used SEO poisoning and malvertising to push the page into search results [7], [12]. The target followed the fake instructions, pasted a PowerShell command into the Run dialog, and unknowingly executed malware, giving the attacker persistent remote access [7].

Explanation

ClickFix works because it turns the victim into the delivery mechanism [7], [12]. Instead of sending a traditional malicious attachment, the attacker convinces the user to manually run the command, which can make the activity look like normal troubleshooting [7]. The SEO poisoning layer also matters because the target arrives at the page through a search they initiated, not through a random phishing email [7], [12]. This gives the attack moderate originality and complexity, especially because it combines search engine trust, fake browser messaging, and user-driven script execution [7].

Influence

- **Authority:** The fake browser error or CAPTCHA prompt appears to originate from the operating system or the browser itself, which users inherently trust as authoritative software. This makes the instruction to run a command feel like a system-generated requirement rather than an attacker's request [7], [12].
- **Social Proof:** SEO poisoning ensures the malicious page appears prominently in legitimate search results. Appearing at the top of a search result implies that many users have visited the page, lending it implied credibility through placement [7], [12].
- **Scarcity:** Fake browser errors and update prompts create urgency by implying that the user's browser is broken, outdated, or unable to proceed until the fix is applied. This time pressure discourages users from stopping to question whether the instruction is legitimate [7], [12].

Vector

- **SEO poisoning:** Search engine results were manipulated to position malicious pages prominently for queries related to software downloads or technical troubleshooting. Users arrived at the page through a search they initiated themselves, which reduced suspicion [7], [12].
- **Malvertising:** Malicious advertisements were used to drive additional traffic to the spoofed pages, appearing alongside or above legitimate search results [7].
- **Self-execution payload delivery:** The user was instructed to open the Windows Run dialog and paste a PowerShell command manually. This technique transfers the execution step to the victim, bypassing some endpoint security controls that focus on file-based or email-based delivery [7], [12].

Technique

- **ClickFix:** The core technique involves presenting a fake browser error, CAPTCHA, or update prompt that instructs the user to copy and paste a PowerShell command into the Windows Run dialog. The user unknowingly executes the malicious payload [7], [12].

- **Living-off-the-land (LoTL**): The payload was delivered and executed using native Windows tools, specifically PowerShell and the Run dialog. Using built-in system utilities reduces the likelihood of triggering signature-based detection [7].
- **Fake browser update or error prompt**: The spoofed page displayed a fake system message to create urgency and provide a plausible reason for the user to run the command [7], [12].

Rank 6: WPP CEO Deepfake WhatsApp Scam, May 10, 2024

Rank: 6 of 10

Title: WPP CEO Deepfake WhatsApp Scam

Summary

On May 10, 2024, WPP CEO Mark Read was reported as the target of a deepfake social engineering scam [13], [23]. Cybercriminals created a fraudulent WhatsApp account using a publicly available image of Read and used it to invite a senior WPP executive to a virtual meeting [13]. During the meeting, the attackers used AI-generated voice cloning and video-related impersonation elements to support the deception [13], [23]. The attacker attempted to convince the executive to establish a new business venture involving corporate fund transfers and personal information disclosure [13]. The executive became suspicious and refused to comply, preventing financial loss [13], [23].

Diagram

The diagram below shows the steps and flow of this attack.

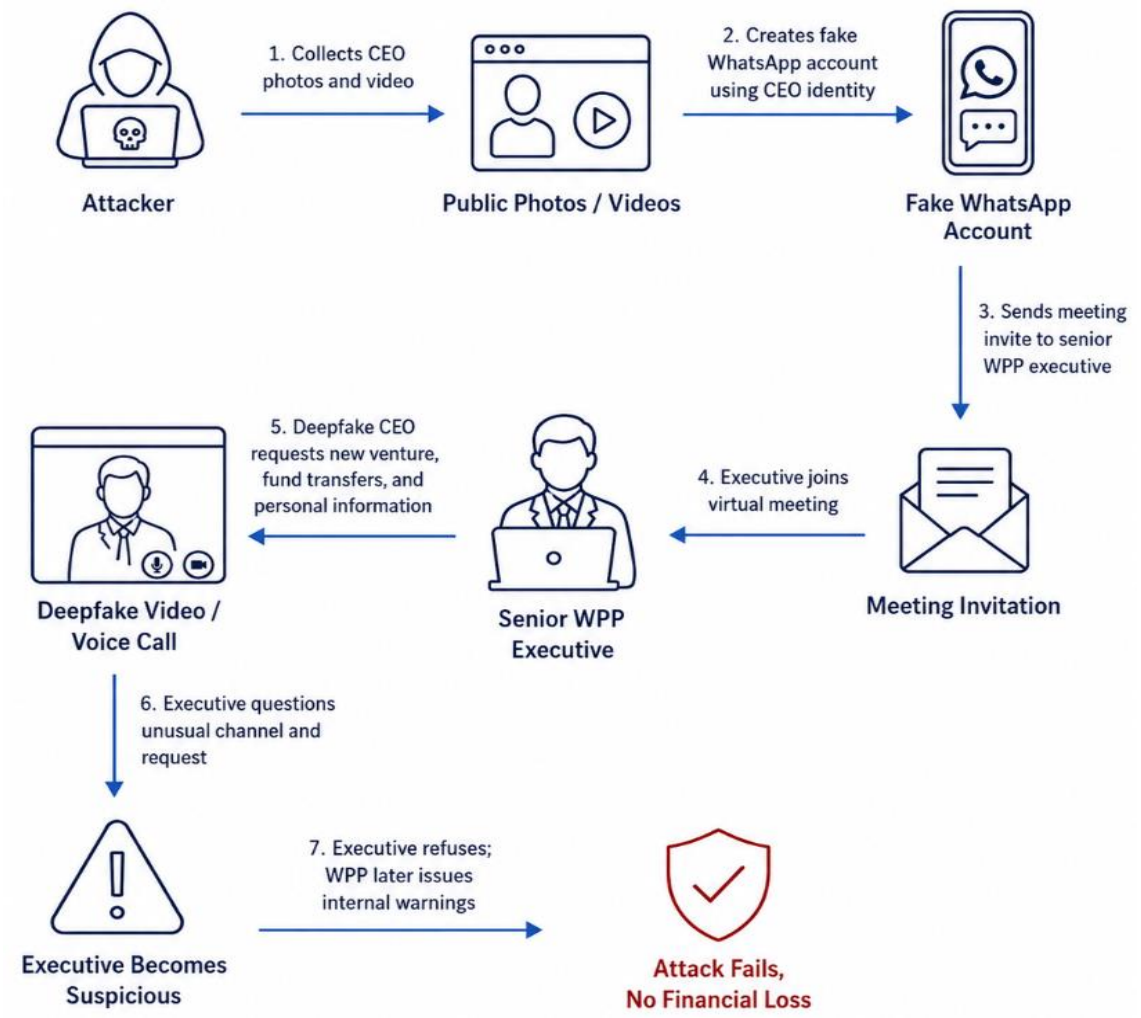


Figure 6 WPP CEO Deepfake WhatsApp Scam diagram

Figure 6 shows how the attacker collected public CEO photos and videos, created a fake WhatsApp account, and used it to send a meeting invitation to a senior WPP executive [13], [23]. During the virtual meeting, the attacker used deepfake video and voice impersonation to request a new venture, fund transfers, and personal information, but the executive became suspicious and refused, causing the attack to fail without financial loss [13].

Explanation

This attack is useful to study because it failed despite using deepfake technology [13], [23]. The CEO impersonation was novel, but the WhatsApp channel and unusual business request did not match normal corporate decision-making processes [13]. Compared with the Arup case, this attack had less operational depth because it did not involve a multi-person executive meeting, pre-positioned transfer accounts, or a completed financial loss [1], [13]. That is why it ranks below Arup even though both attacks involved AI-generated executive impersonation.

Influence

- **Authority:** The attacker impersonated the CEO of one of the world's largest advertising companies. A message or meeting request appearing to come from the most senior executive in the organization carries significant weight for any employee receiving it [13], [23].
- **Liking:** Using a real publicly available photo of Mark Read made the fake WhatsApp account feel familiar to the executive who received the invitation. Familiarity with a person's face creates a baseline level of comfort and reduced suspicion [13], [23].
- **Scarcity:** The framing of a new confidential business venture implied urgency and exclusivity, suggesting that the executive was being approached for a special opportunity that required prompt engagement [13].

Vector

- **Messaging platform impersonation:** The attacker created a fraudulent WhatsApp account using a photo of the CEO, then used it to initiate contact with a senior executive. Consumer messaging platforms like WhatsApp are not standard channels for high-value corporate decisions, which contributed to the executive's eventual suspicion [13], [23].
- **Deepfake voice and video impersonation:** During the virtual meeting, the attacker used AI-generated voice cloning and visual impersonation to support the deception. The goal was to make the request appear as though it came directly from Mark Read in real time [13], [23].

Technique

- **CEO fraud:** The attack used the CEO's identity to request a financial commitment and personal information from a senior subordinate. CEO fraud relies on executive authority to suppress a target's instinct to question or verify [13], [23].
- **Deepfake voice cloning:** AI-generated audio was used to impersonate the CEO's voice during the virtual meeting. Voice cloning makes impersonation more convincing than text alone and is harder to immediately dismiss as fake [13], [23].
- **Fake social account:** A WhatsApp account was created using publicly available images of the CEO. Creating a fake social profile is a common reconnaissance and impersonation

technique that requires minimal technical sophistication but leverages public trust in familiar faces [13].

- **Pretexting:** The attacker fabricated a story about a new business venture to justify the meeting and the requests for funds and personal information [13].

Rank 7: CoGUI Mass Phishing Campaign Targeting Japan, January to April 2025, Reported May 6, 2025

Rank: 7 of 10

Title: CoGUI Mass Phishing Campaign Targeting Japan

Summary

Between January and April 2025, a phishing campaign using the CoGUI phishing kit delivered more than 580 million phishing emails, primarily targeting users in Japan [14], [24]. Proofpoint reported the campaign on May 6, 2025, identifying CoGUI as a high-volume phishing kit used to impersonate consumer and finance brands [14]. The emails impersonated organizations such as Amazon, PayPal, Apple, and Japanese tax-related entities [14], [24]. Recipients were sent to credential-harvesting pages designed to imitate the impersonated services [14]. Victims who entered login credentials or payment information had that data collected for account takeover or resale [14], [24].

Diagram

The diagram below shows the steps and flow of this attack:

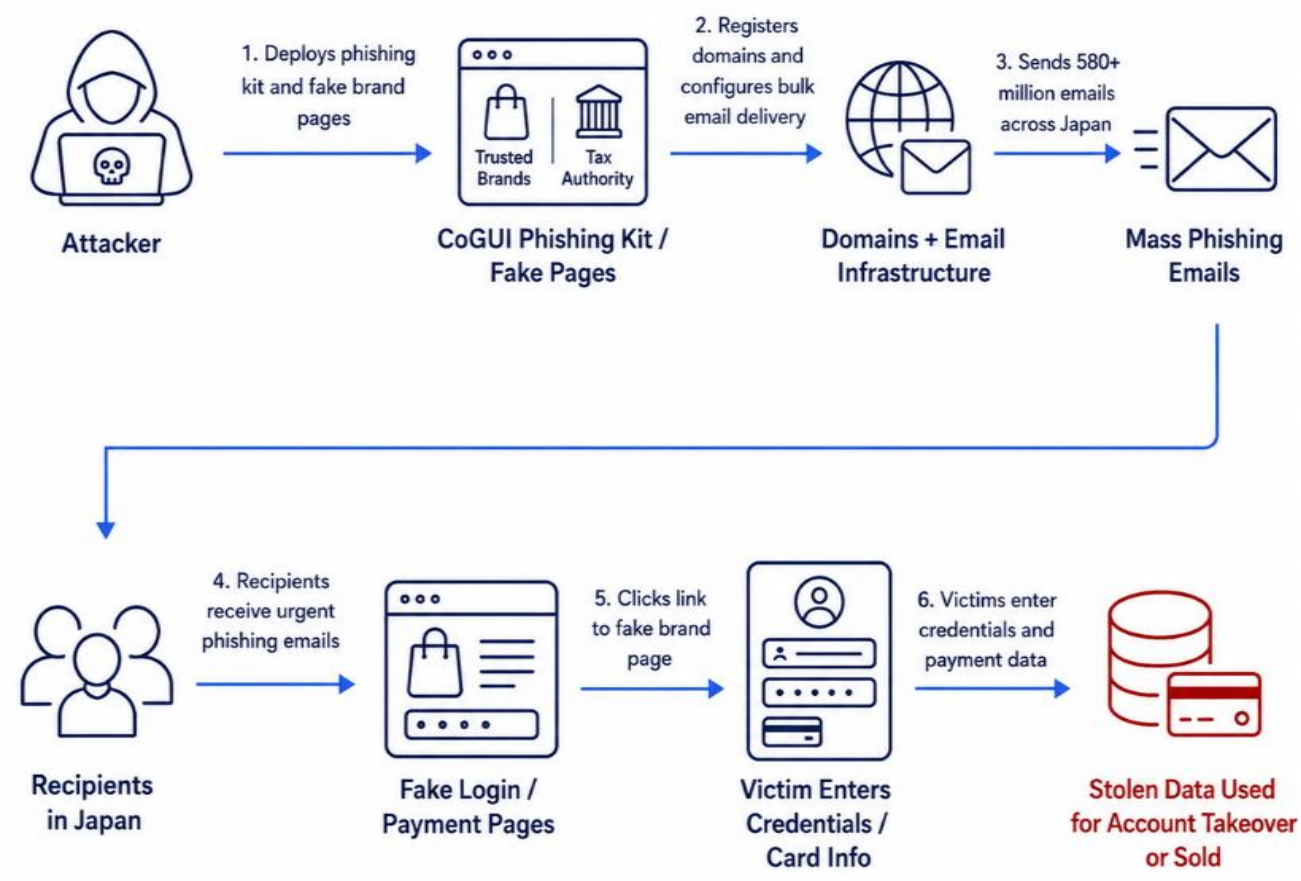


Figure 7 CoGUI Mass Phishing Campaign Targeting Japan Diagram

Figure 7 shows how attackers used the CoGUI phishing kit to create fake brand and payment pages, register supporting domains, and send more than 580 million phishing emails across Japan [14], [24]. Recipients were directed to fake login or payment pages where their credentials and card information were captured for account takeover or resale [14].

Explanation

The scale of this campaign is impressive, but the technique itself is not especially original [14], [24]. Brand impersonation phishing and credential-harvesting pages are well-known social engineering methods [5], [11]. The complexity comes mainly from the infrastructure required to send hundreds of millions of emails and maintain phishing pages at scale [14]. Since the campaign relied on a phishing kit rather than a highly customized attack chain, it ranks below the more targeted and adaptive attacks [14], [24].

Influence

- **Authority:** The campaign impersonated globally trusted brands including Amazon, PayPal, Apple, and official Japanese tax entities. Recipients were more likely to respond to messages appearing to come from organizations they regularly interact with and trust [14], [24].
- **Scarcity:** Phishing messages in campaigns of this type typically claim account suspension, pending payment failures, or overdue tax obligations, creating urgency that pressures recipients to act before they take time to verify the message [14], [24].
- **Social Proof:** Impersonating well-known global brands implies widespread legitimacy. Receiving a message that appears to come from a company with hundreds of millions of users creates an implicit assumption that the communication is routine and credible [14].

Vector

- **Phishing (email):** More than 580 million phishing emails were delivered across Japan using the CoGUI phishing kit infrastructure. Email was the primary delivery channel, relying on volume to ensure a percentage of recipients would engage [14], [24].
- **Fake login and payment page infrastructure**: Victims who clicked links in the phishing emails were redirected to spoofed pages hosted on attacker-controlled domains. These pages were designed to visually replicate the login and checkout flows of the impersonated services, functioning as the landing infrastructure for the campaign [14], [24].

Technique

- **Brand impersonation:** The CoGUI kit was used to replicate the visual design and sender identity of Amazon, PayPal, Apple, and Japanese tax authorities. Impersonating recognizable brands lowers the victim's defenses because the communication looks routine [14], [24].
- **Phishing kit deployment:** The CoGUI phishing kit automated large portions of the campaign, including email delivery, domain registration, and page hosting. Using a kit reduces the technical expertise required to run a campaign at scale [14], [24].
- **Credential and payment data collection:** Once victims submitted information on the fake pages, the CoGUI kit captured and stored the login credentials and payment card

details server-side. The collected data was then used for account takeover or sold to other threat actors through underground markets [14], [24].

Rank 8: Marks and Spencer Coordinated Retail Phishing and Credential Attack, April 22, 2025

Rank: 8 of 10

Title: Marks and Spencer Coordinated Retail Phishing and Credential Attack

Summary

On April 22, 2025, Marks and Spencer publicly confirmed a cyber incident that disrupted customer-facing services, including contactless payments and online order functions [16]. Reporting later connected the broader incident to social engineering methods used against retail organizations, including phishing, credential abuse, and helpdesk-style manipulation [4], [6]. Attackers targeted customers and employees through convincing messages and fake login pages designed to capture credentials [4]. Stolen credentials could then be used for account takeover or attempted access into internal systems [4]. M&S responded by investigating the incident, notifying relevant authorities, warning customers, and strengthening verification procedures [4], [16].

Diagram

The diagram below shows the steps and flow of this attack:

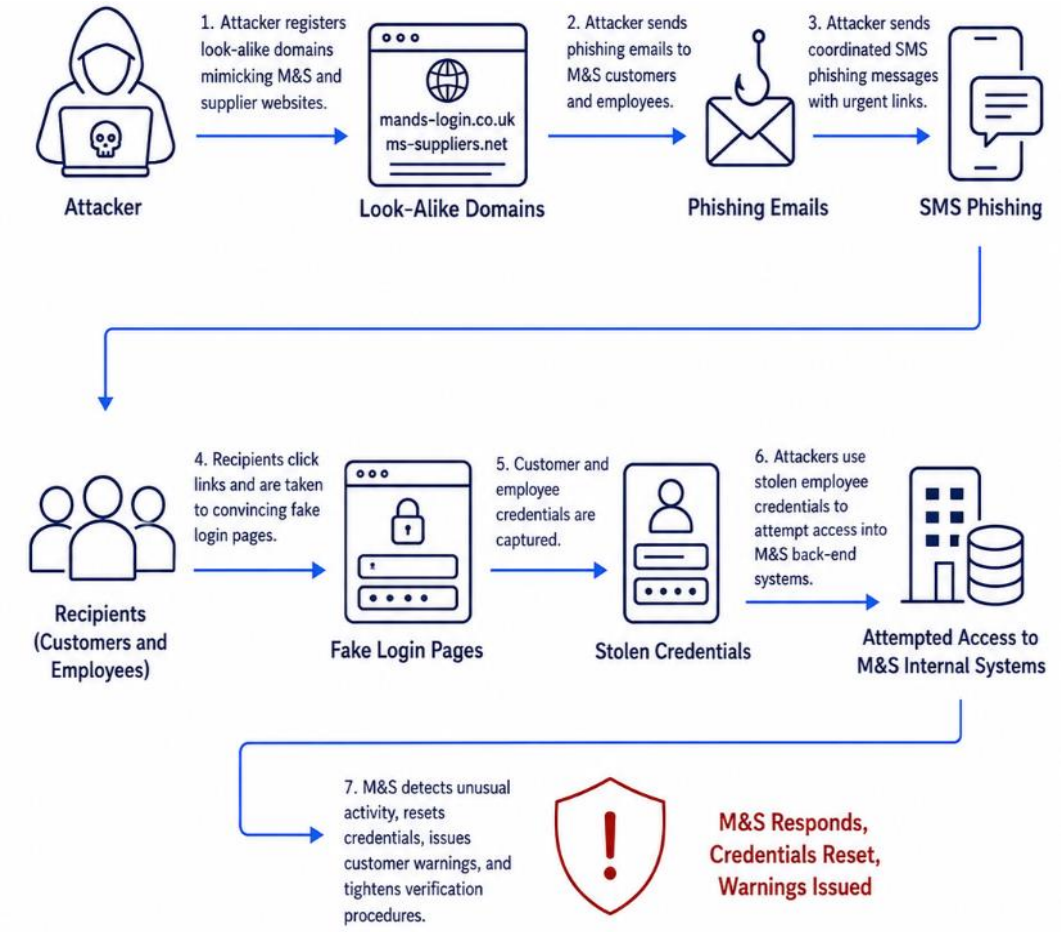


Figure 8 Marks and Spencer Coordinated Retail Phishing and Credential Attack diagram

Figure 8 shows how attackers registered look-alike domains, sent phishing emails and SMS messages, and directed M&S customers and employees to fake login pages [4]. The stolen credentials were then used to attempt access into M&S internal systems, leading the company to reset credentials, warn customers, and strengthen verification procedures [4].

Explanation

The M&S attack ranks eighth because it used multiple social engineering channels, but the individual techniques were familiar [4]. Email phishing, SMS phishing, fake login pages, and look-alike domains are established attack methods [5], [11]. The attack is more complex than a single phishing email because it combined several delivery methods and affected both customers and staff [4], [16]. However, it does not rank higher because it lacked the originality of deepfake impersonation, insider bribery, or search-engine-based payload delivery.

Influence

- **Authority:** Attackers impersonated M&S, a well-established and trusted retail brand with a large loyal customer base. Emails and SMS messages appearing to come from M&S carried the brand's authority, making recipients more likely to act on the instructions [4].
- **Scarcity:** Phishing messages in retail campaigns of this type typically warn of account issues, suspicious activity, or payment problems requiring immediate resolution. This urgency discourages recipients from pausing to verify whether the message is legitimate [5], [11].
- **Social Proof:** M&S is a widely recognized brand with tens of millions of customers. A message appearing to come from a retailer that most recipients have interacted with creates an assumption of normalcy and legitimacy [4], [16].

Vector

- **Phishing (email):** Fake M&S branded emails were sent to customers and employees, directing them to credential-harvesting pages that mimicked the M&S login portal [4].
- **Smishing (SMS phishing):** SMS messages were also used to reach customers through mobile devices. Smishing is effective because SMS notifications have a high open rate and are often perceived as more personal and urgent than emails [4], [11].

Technique

- **Brand impersonation:** The M&S brand identity was spoofed across email, SMS, and fake web pages. Consistent use of M&S logos, colors, and language across multiple channels increased the overall believability of the campaign [4].
- **Multi-channel delivery:** Combining email and SMS delivery expanded the attack surface and increased the probability that some recipients would engage through whichever channel they found more familiar or trustworthy [4].
- **Credential harvesting:** Fake login pages were used to capture customer and employee credentials, which were then available for account takeover or further access attempts into M&S internal systems [4].
- **Look-alike domain spoofing:** Registered domains that closely resembled official M&S domains were used to host fake pages. This technique reduces the likelihood of recipients noticing an incorrect URL without careful inspection [4].

Rank 9: Change Healthcare Credential-Based Network Intrusion, Initial Access February 12, 2024 and Ransomware February 21, 2024

Rank: 9 of 10

Title: Change Healthcare Credential-Based Network Intrusion

Summary

On February 12, 2024, BlackCat/ALPHV affiliates gained access to Change Healthcare by using stolen credentials against a Citrix remote access portal that did not enforce multi-factor authentication [17], [25]. On February 21, 2024, ransomware was deployed across Change Healthcare systems, causing major service disruption [17], [25]. No zero-day exploit was required for initial access because the attackers used valid credentials [17]. Once inside, the attackers moved laterally, exfiltrated protected health information, and encrypted systems [17], [25]. The outage disrupted prescription processing and claims services across the United States, and UnitedHealth later reported major financial impact from the incident [17], [25].

Diagram

The diagram below shows the steps and flow of this attack:

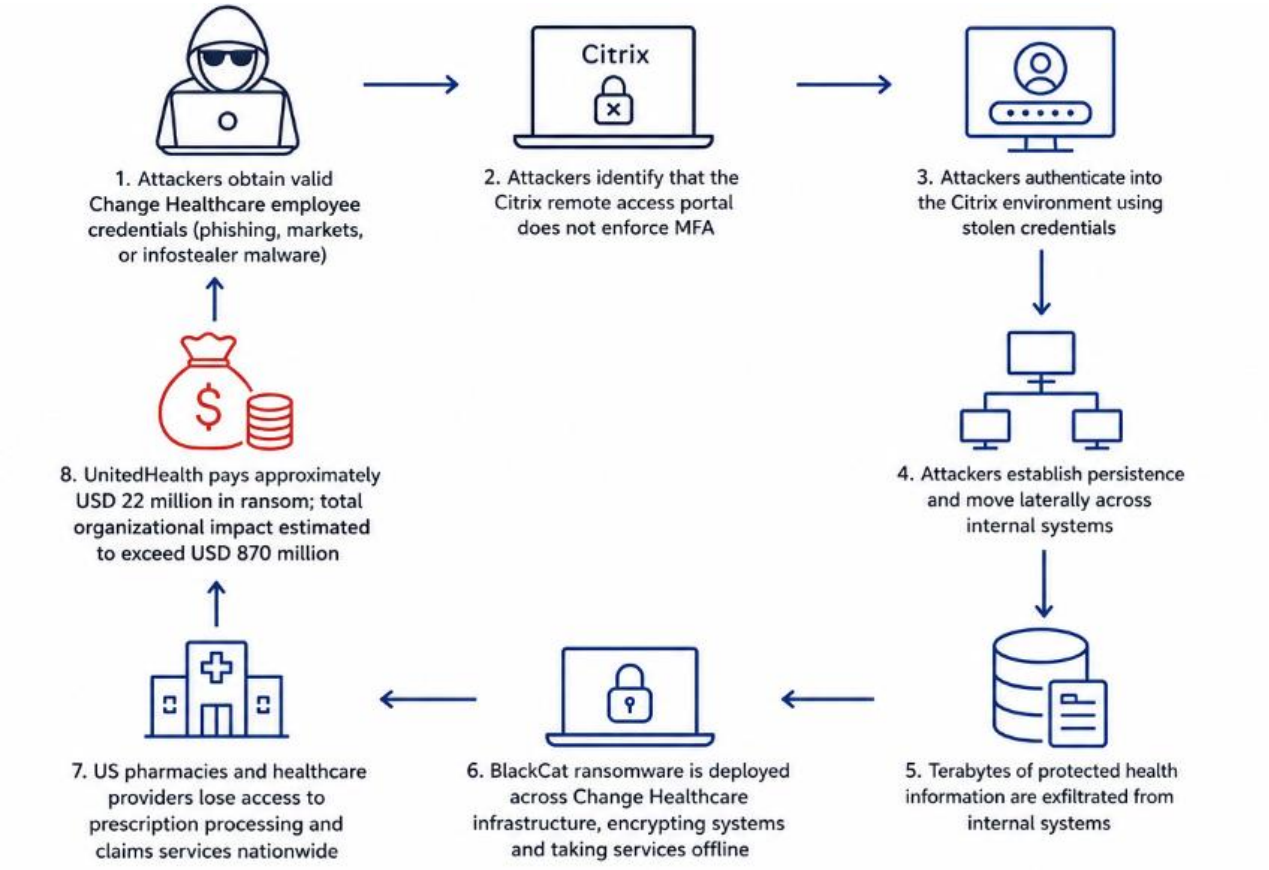


Figure 9 Change Healthcare Credential-Based Network Intrusion diagram

Figure 9 shows how attackers used stolen Change Healthcare employee credentials to access a Citrix remote access portal that did not enforce MFA [17], [25]. After gaining access, the attackers moved laterally, stole protected health information, deployed BlackCat ransomware, disrupted healthcare and pharmacy services nationwide, and pressured UnitedHealth into paying an estimated USD 22 million ransom [17], [25].

Explanation

The Change Healthcare attack had enormous real-world impact, but the social engineering component was not the most original part of the incident [17], [25]. The defining weakness was that stolen credentials could be used against a Citrix remote access portal without MFA [17], [25]. The lateral movement, data theft, and ransomware deployment were serious, but those stages followed after access was already obtained [17], [25]. This is why the attack ranks ninth for originality even though its operational impact was extremely high.

Influence

- **Authority:** The phishing or credential-theft method used to obtain the employee's login details most likely involved impersonating a trusted source, such as an IT security alert, a system notification, or a known internal service. Employees are conditioned to respond to messages that appear to come from authoritative systems or departments within their organization [9], [17].
- **Scarcity:** Credential-harvesting campaigns typically create urgency by claiming an account will be locked, access will expire, or a security issue requires immediate action. This pressure shortens the window in which a target might stop and verify whether the request is legitimate [9], [17].
- **Commitment and Consistency:** Once an employee begins engaging with what appears to be a routine IT or security notification, they tend to complete the process, including entering credentials, because stopping partway through feels inconsistent with how they normally respond to system prompts [9], [17].

Note: The exact method used to steal the credentials has not been fully confirmed in public reporting. The influence analysis above reflects the most probable upstream scenario based on available sources and is presented as inferred rather than confirmed.

Vector

- **Stolen credential use:** The attacker used previously compromised Change Healthcare employee credentials to authenticate against the Citrix remote access portal. No phishing or direct interaction with a target was required at the point of access [17], [25].
- **Remote access portal abuse:** The Citrix portal was the specific entry point. Because it did not enforce MFA, valid credentials alone were sufficient to gain authenticated remote access to Change Healthcare's internal environment [17], [25].

Technique

- **Credential stuffing or stolen credential use:** Attackers used credentials that had been obtained through prior compromise. The credentials were tested against the Citrix portal and were found to be valid and active, giving immediate access without requiring any further social engineering at the point of entry [17], [25].

- **MFA bypass through absence:** The Citrix portal did not enforce MFA, meaning the attacker did not need to bypass a second factor; the control simply did not exist. This is a configuration gap rather than a technical exploit, and it enabled full access through credentials alone [17], [25].
- **Lateral movement:** After gaining initial access, the attackers moved through Change Healthcare systems to reach high-value targets including protected health information and systems critical to pharmacy and claims processing [9], [17].
- **Ransomware deployment:** BlackCat/ALPHV ransomware was deployed on February 21, 2024, encrypting systems and causing widespread disruption to prescription processing and claims services across the United States [17], [25].

Rank 10: Fake Road Toll Smishing Surge, FBI Alert April 12, 2024

Rank: 10 of 10

Title: Fake Road Toll Smishing Surge (E-ZPass and Similar Agencies)

Summary

On April 12, 2024, the FBI IC3 issued a public alert about smishing messages impersonating road toll collection services [26]. The FBI stated that since early March 2024, IC3 had received more than 2,000 complaints involving these toll-related scam texts [26]. Victims received SMS messages claiming they had unpaid toll balances and were directed to fake payment pages [26]. These pages were designed to collect credit card, banking, or personal information [26]. The campaign exploited urgency, small payment amounts, and familiarity with legitimate toll notifications to pressure recipients into paying quickly [9], [26].

Diagram

The diagram below shows the steps and flow of this attack:

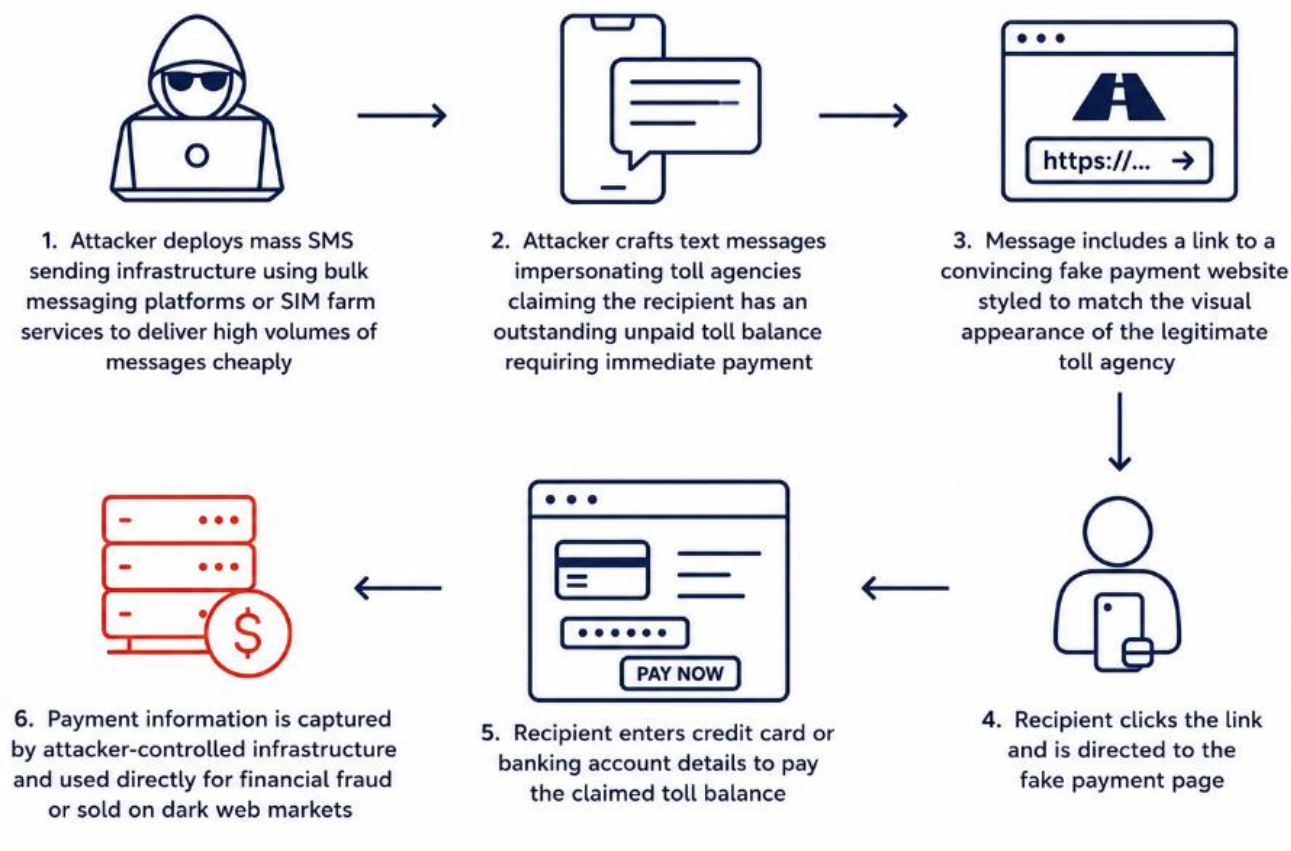


Figure 10 Fake Road Toll Smishing Surge (E-ZPass and Similar Agencies) diagram

Figure 10 shows how attackers used mass SMS infrastructure to send fake toll payment messages that impersonated agencies such as E-ZPass and similar services [26]. The messages directed recipients to a fake payment website where they entered credit card or banking details, allowing attackers to capture the information for fraud or resale [26].

Explanation

This attack ranks tenth because it uses one of the most common social engineering patterns: bulk SMS phishing with a fake payment page [9], [26]. The toll theme is believable because many people may not know their exact toll balance, but the attack chain itself is simple [26]. There is little evidence of target-specific reconnaissance, advanced tooling, or multi-stage adaptation [26]. The campaign is still important because of its volume and public impact, but it is the least original and least complex attack in this ranked list.

Influence

- **Authority:** The messages impersonated official government-linked toll agencies such as E-ZPass, which have the authority to require payment and issue penalties. Recipients are conditioned to treat toll notifications from these agencies as legitimate obligations [9], [26].
- **Scarcity:** Messages claimed that an unpaid balance was overdue and that failure to pay promptly would result in additional fees or penalties. This urgency was designed to push recipients into paying before questioning the message's authenticity [26].
- **Commitment and Consistency:** Many recipients are actual road toll users who are accustomed to occasional balance notifications. Receiving a message about an unpaid toll is consistent with their existing experience, making it harder to immediately recognize the message as fraudulent [9], [26].

Vector

- **Smishing (SMS phishing):** All contact with victims was made through SMS text messages. Smishing reaches people on personal devices, where they may be less guarded than on a work computer, and toll-related notifications are a familiar format for many recipients [9], [26].

Technique

- **Government brand impersonation:** Messages impersonated E-ZPass and similar toll agencies, which are government-linked services with authority over drivers who use toll roads. Using a government-adjacent brand increases the perceived legitimacy of the payment demand [26].
- **Fake payment page:** Recipients were directed to spoofed payment sites that collected credit card numbers, banking details, and personal information. The pages were designed to resemble legitimate toll payment portals [26].
- **Urgency-based pressure:** The small dollar amounts claimed as outstanding balances made the demand seem routine and not worth questioning, while the threat of penalties added pressure to pay without verification [26].

5. Conclusion

In conclusion, this lab showed that recent social engineering attacks vary widely in originality, complexity, and the psychological mechanisms they exploit. The highest-ranked attacks, such as the Arup deepfake fraud and MGM vishing attack, were not just successful because of technical skill; they succeeded because they exploited trusted business processes, executive authority, and assumptions about identity verification [1], [4], [19]. In both cases, the principle of authority was central: the targets complied because the request appeared to come from people with legitimate power over them. Mid-ranked cases such as Coinbase, ClickFix, WPP, and CoGUI show how attackers combine insider access, AI impersonation, search-engine trust, and phishing infrastructure to make deception more convincing at scale [7], [13], [14], [15]. These attacks layered multiple principles, including authority, scarcity, and social proof, to reduce the window in which a target might pause and question what they were being asked to do. Lower-ranked cases such as Change Healthcare and road toll smishing still caused serious harm, but their social engineering methods were less original and relied more on stolen credentials or basic phishing templates [17], [26]. Overall, the ranking shows that effective defence requires more than user awareness training; organizations also need strong verification procedures, MFA, monitoring for lateral movement, and controls that assume trusted communication channels can be abused.

6. References

[1] CNN, "British engineering giant Arup revealed as $25 million deepfake scam victim," May 2024. [Online]. Available: https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk

[2] R. Greig, "This engineering firm was hit by a deepfake fraud. Here's what it learned," World Economic Forum, Feb. 2025. [Online]. Available: https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

[3] PurpleSec, "Arup Deepfake: How An AI-Generated Video Stole $25 Million," Jan. 2026. [Online]. Available: https://purplesec.us/breach-report/arup-deepfake/

[4] ZeroFox, "Inside the Criminal Mind: How Social Engineering Attacks Really Work in the Age of AI," Dec. 2025. [Online]. Available: https://www.zerofox.com/blog/how-social-engineering-attacks-work/

[5] Secureframe, "The 13 Most Common Types of Social Engineering Attacks in 2025," Jul. 2025. [Online]. Available: https://secureframe.com/blog/most-common-social-engineering-attacks

[6] Mitnick Security, "5 Examples of Top Social Engineering Attacks in 2025," Sep. 2025. [Online]. Available: https://www.mitnicksecurity.com/blog/top-social-engineering-attacks

[7] Palo Alto Networks Unit 42, "2025 Unit 42 Global Incident Response Report: Social Engineering Edition," Aug. 2025. [Online]. Available: https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/

[8] CoverLink Insurance, "Cyber Case Study: $25 Million Deepfake Scam," Aug. 2025. [Online]. Available: https://coverlink.com/case-study/case-study-25-million-deepfake-scam/

[9] FBI Internet Crime Complaint Center (IC3), "2024 Internet Crime Report," Apr. 2025. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf

[10] Verizon, "2025 Data Breach Investigations Report," 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[11] Secureframe, "85+ Social Engineering Statistics to Know for 2026," Oct. 2025. [Online]. Available: https://secureframe.com/blog/social-engineering-statistics

[12] Communications of the ACM, "Social Engineering 2.0," Sep. 2025. [Online]. Available: https://cacm.acm.org/blogcacm/social-engineering-2-0/

[13] The Guardian, “CEO of world’s biggest ad firm targeted by deepfake scam,” May 10, 2024. [Online]. Available: https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam

[14] Proofpoint, “CoGUI Phish Kit Targets Japan with Millions of Messages,” May 6, 2025. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/cogui-phish-kit-targets-japan-millions-messages

[15] Coinbase, “Protecting Our Customers, Standing Up to Extortionists,” May 15, 2025. [Online]. Available: https://www.coinbase.com/en-ca/blog/protecting-our-customers-standing-up-to-extortionists

[16] The Guardian, “M&S apologises after ‘cyber incident’ hits contactless payments and online orders,” Apr. 22, 2025. [Online]. Available: https://www.theguardian.com/business/2025/apr/22/marks-and-spencer-apologises-cyber-incident-contactless-payments-online-orders

[17] Kaspersky, “UnitedHealth ransomware attack,” Feb. 20, 2025. [Online]. Available: https://www.kaspersky.com/blog/unitedhealth-ransomware-attack/53065/

[18] Reuters, “MGM Resorts breached by ‘Scattered Spider’ hackers,” Sep. 13, 2023. [Online]. Available: https://www.reuters.com/technology/moodys-says-breach-mgm-is-credit-negative-disruption-lingers-2023-09-13/

[19] University of Hawai‘i West O‘ahu, “ALPHV: Hackers Reveal Details of MGM Cyber Attack,” Oct. 24, 2023. [Online]. Available: https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/

[20] Caesars Entertainment, “Form 8-K,” U.S. Securities and Exchange Commission, Sep. 14, 2023. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1590895/000119312523235015/d537840d8k.htm

[21] Cybernews, “Caesars SEC breach report: $15m ransom paid,” Sep. 15, 2023. [Online]. Available: https://cybernews.com/news/caesars-15m-ransom-sec-breach-report-6t-stolen-data/

[22] Associated Press, “Coinbase said cyber crooks stole customer information and demanded $20 million ransom payment,” May 15, 2025. [Online]. Available: https://apnews.com/article/e3ef5297dfea296eb7b7320d8c58647e

[23] Financial Times, “WPP boss targeted by deepfake scammers using voice clone,” May 10, 2024. [Online]. Available: https://www.ft.com/content/308c42af-2bf8-47e4-a360-517d5391b0b0

[24] BleepingComputer, “CoGUI phishing platform sent 580 million emails to steal credentials,” May 7, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/cogui-phishing-platform-sent-580-million-emails-to-steal-credentials/

[25] IBM, “Change Healthcare discloses USD 22M ransomware payment,” May 2024. [Online]. Available: https://www.ibm.com/think/news/change-healthcare-22-million-ransomware-payment

[26] FBI Internet Crime Complaint Center, “Smishing Scam Regarding Road Toll Collection Service,” Apr. 12, 2024. [Online]. Available: https://www.ic3.gov/PSA/2024/PSA240412

7. Bibliography

[27] CISA, "Recognize and Report Phishing," Cybersecurity and Infrastructure Security Agency. [Online]. Available: https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

[28] CISA, "Avoiding Social Engineering and Phishing Attacks," Cybersecurity and Infrastructure Security Agency, Feb. 1, 2021. [Online]. Available: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

[29] NSA, CISA, FBI, and MS-ISAC, "Phishing Guidance: Stopping the Attack Cycle at Phase One," Oct. 2023. [Online]. Available: https://media.defense.gov/2023/Oct/18/2003322402/-1/-1/1/CSI-PHISHING-GUIDANCE.PDF

[30] OWASP Foundation, "Content Spoofing," OWASP Community Pages. [Online]. Available: https://owasp.org/www-community/attacks/Content_Spoofing

[31] OWASP Foundation, "Credential Stuffing," OWASP Community Pages. [Online]. Available: https://owasp.org/www-community/attacks/Credential_stuffing

[32] Canadian Centre for Cyber Security, "Strategies for Protecting Web Application Systems Against Credential Stuffing Attacks," Feb. 3, 2022. [Online]. Available: https://www.cyber.gc.ca/en/guidance/strategies-protecting-web-application-systems-against-credential-stuffing-attacks