UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff,* v. DOES 1–25, *Defendants.*	Civil Action No.:

DECLARATION OF [redacted] IN SUPPORT OF PLAINTIFF'S MOTION FOR AN *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

I, [redacted], declare as follows:

1. My name is [redacted] I am over eighteen years of age and competent to testify to the matters set forth herein.

2. I am a member of NAXO Labs LLC ("NAXO"), a company that conducts blockchain and cyber investigations in connection with civil and criminal litigation. At NAXO, I manage and oversee crypto asset, cyber, dark web, and related investigations. Before joining NAXO, [redacted] I used my technical expertise in blockchain and the dark web to investigate a wide range of cyber and crypto-related crime, including crimes against children, financial crimes, and network intrusions. I also led investigations identifying, locating, and apprehending criminals who used decentralized networks to obfuscate their identities. Among other matters, I led a multi-year investigation that resulted in the identification, apprehension, and conviction of two individuals who operated one of the most heavily trafficked criminal sites on the dark web. After apprehending the site's

administrators, I led the effort to use their accounts to identify and arrest a large network of offenders operating on the dark web.

3. Prior to my time at [redacted]. There, I was responsible for investigating financial crimes and cybercrimes and recovering electronic evidence from seized devices. I also served as a [redacted], where I used data analysis to investigate complex federal contract fraud.

4. I hold a [redacted]

5. Over the course of my career, I have testified as an expert in the areas of access device fraud, financial crimes, digital forensics, and cybercrime investigations in legal proceedings on several occasions, including testimony at trials, before grand juries, and in hearings at both the federal and state levels.

6. In support of the accompanying Complaint, I conducted an investigation of phishing software known as "Outsider" developed by one or more persons or entities using the Telegram handles @chenlun and @sinkinto01, and others. The software enables criminal actors to steal personal information and financial data from victims by creating fake websites that closely resemble legitimate websites. When victims enter their personal and/or financial data into the fraudulent websites, that data is funneled to the users of Outsider. The Outsider users then appropriate the stolen information for personal financial gain, either by exploiting victims' financial accounts themselves or selling bulk collections of stolen data to other criminals. The user(s) of the Telegram handle @sinkinto01 work with a network of cybercriminals to perpetrate

phishing schemes. For example, the user(s) of the Telegram handles @bailiworking and @adc88adc provide infrastructure to send bulk text messages to victims by the thousands through iMessage, Short Message Service ("SMS"), and Rich Communication Services ("RCS"), and the user(s) of the Telegram handle @yy0205 sell products to help monetize stolen credit card information and launder stolen funds. The Outsider software and its predecessor software created by @chenlun have been used to create tens of thousands of phishing websites, leading to the theft of financial information from over 100,000 victims, and losses of millions of dollars. My investigation involved researching public information, entering online chat forums and communicating with threat actors, reviewing phishing websites created using Outsider, and purchasing, installing, and using Outsider myself.

7. I have been retained by Google LLC to conduct the investigation described herein. I am being compensated at a rate of $625 per hour. The opinions I am providing are my own and are not contingent on my compensation or the outcome of this matter.

I. Background Terminology

8. Phishing is a cybercrime in which attackers impersonate legitimate entities to trick people into clicking on a link or navigating to a website built to steal sensitive personal information. Phishing messages are typically delivered through email, text message, or targeted online advertising. Commonly impersonated entities include financial institutions, postal and shipping companies, telecommunications companies, government agencies, and cryptocurrency exchanges. Phishing attacks target personal data, usernames and passwords, and banking and credit card information.

9. Phishing-as-a-service is a term that describes the business model that sells software and support services to facilitate phishing, making it relatively easy for those without technical

expertise to create a phishing campaign. This software, also sometimes referred to as a "phish kit" or "phishing kit," provides the infrastructure necessary to create a fake website (or other platform), send bulk text messages and emails to victims, and collect and store stolen personal and/or financial information. For example, phishing software may contain ready-made website templates that closely resemble legitimate websites.

10. SMS phishing scams refer to phishing attempts sent through text message (or other telephone messaging services like RCS and iMessage). These messages target thousands of phone numbers at a time and often encourage recipients to click on a malicious link that leads to a fraudulent phishing website. The fake websites used in these scams often mimic those of toll enforcement agencies, postal and shipping companies, or financial institutions. This is sometimes referred to as "smishing."

11. Telegram is a free messaging service with over one billion monthly active users.[1] Users typically create Telegram accounts with a phone number and can set a unique Telegram username.[2] Telegram allows users to directly message each other and join conversational groups with up to 200,000 members.[3] Typically, any member of a group can post in that group. Users can also join Telegram channels, which are designed for one-way information sharing. Usually, only channel administrators ("admins") can post in a channel.[4] Any user can create new Telegram groups and channels.

---

[1] *See* Katherine Li, *Telegram Hits 1 Billion Active Users as CEO Pavel Durov Takes Swipe at Meta-Owned Rival WhatsApp*, Business Insider (Mar. 19, 2025), https://tinyurl.com/pz7ac7ax.
[2] *See No-SIM Signup, Auto-Delete All Chats, Topics 2.0 and More*, Telegram Blog (Dec. 6, 2022), https://tinyurl.com/3akd4xdm.
[3] *See Group Chats on Telegram,* Telegram Blog, https://tinyurl.com/vppe886w (last visited May 5, 2026).
[4] *See Telegram Channels*, Telegram Blog, https://tinyurl.com/8aajwsk9 (last visited May 5, 2026).

12. Multi-factor authentication ("MFA") is an account security measure that requires enhanced verification to access an account in addition to a username and password. Most commonly, this is a one-time passcode sent to an account holder's email or phone.

13. 3-D Secure refers to a security technology implemented by many credit card issuers that aims to reduce online fraud. When a user attempts certain actions with the credit card, like making an online payment or adding a credit card to a mobile wallet, the card issuer can request additional authentication (MFA) from the user. Brand names of this technology include Visa Secure,[5] Mastercard Identity Check,[6] American Express SafeKey,[7] Discover ProtectBuy,[8] and Google Secure Payment Authentication.[9]

14. An Internet Protocol ("IP") address is a unique set of numbers and sometimes letters assigned to devices connected to the internet, allowing connected devices to communicate with each other.

15. Domains or domain names are human-readable addresses for websites that replace numerical or alphanumerical IP addresses, such as www.google.com.

16. Crypto assets (sometimes called "cryptocurrency") are digital assets that exist only in electronic form and rely on cryptography to facilitate and validate transfers of value from one party to another. Bitcoin, first introduced in a 2008 whitepaper, is generally considered to be the

---

[5] *See Visa Secure with EMV 3-D Secure Authentication*, Visa Online Payment Fraud, Emerging Threats, Segment Analysis Market Forecasts 2018-2023 (Nov. 2018), https://tinyurl.com/bde43zrb.

[6] *See Identity Authentication, Ensure Your Customers Are Real*, Mastercard Cybersecurity and fraud prevention, Identity, https://tinyurl.com/2wdzhxz9 (last visited May 5, 2026).

[7] *See American Express SafeKey & Online Safety*, American Express.com, https://tinyurl.com/257r5nfv/, (last visited May 5, 2026).

[8] *See 3DS ProtectBuy, Reduce the Growing Threat of Card-Not-Present Fraud*, DiscoverGlobalNetwork.com, https://tinyurl.com/3yywej6j, (last visited May 5, 2026).

[9] *See* Jose Ugia, *What's New in Google Play*, Google for Developers (May 23, 2023), https://tinyurl.com/4hypr6s4.

first widely adopted crypto asset.[10] Users of crypto assets are represented by "addresses," virtual locations from which crypto assets are sent and received.

17. USDT is a crypto asset that is available on multiple blockchains. It is issued by Tether and is a "stablecoin," meaning that it aims to be priced at or near one U.S. dollar.[11]

II. Overview of the Outsider Phishing-as-a-Service Software

18. People who use mobile phones or the internet are regularly targeted by scammers attempting to steal their account logins or financial information. Potential victims receive text messages directing them to click on a link, open emails pretending to be from real businesses or contacts, or accidentally navigate to websites that look almost identical to those of legitimate companies. If internet users are not careful, these text messages, emails, or even their own browsing can lead them to malicious websites. These websites "spoof" those of legitimate companies and are built to look and function the same as the trusted websites people visit daily. When scam victims are fooled by one of these spoofed websites, they will often input their personal and/or financial information, like a credit card or bank account number, which is directly funneled to a criminal actor who uses it to steal their money. Phishing is by far the most frequent internet crime reported to the FBI, with over 193,000 complaints received in 2024 and over $70 million in reported losses in the United States.[12]

19. Despite the scope and reach of this crime, it is relatively easy to commit, thanks in large part to phishing software like Outsider. This type of software provides someone who wants to run a phishing scam with many of the tools they need to do so: ready-made templates for popular

[10] Satoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, Bitcoin.org (Oct. 31, 2008), https://tinyurl.com/2vyrxxby.
[11] *See Transparency*, Tether.com (Oct. 7, 2025), https://tinyurl.com/2vabzysu.
[12] *See* FBI Internet Crime Complaint Center, Federal Bureau of Investigation Internet Crime Annual Report 2024, 9, 10 (2024), https://tinyurl.com/55pwfp6a.

phishing scams, the ability to make a fake version of almost any website, and a platform to collect and organize stolen personal financial information. The recent use of artificial intelligence ("AI") tools to create and customize these websites has only increased the ease and efficacy of the scams.[13] For a weekly licensing fee of approximately $88, a scammer can create hundreds of websites that could reach thousands of victims, within hours of purchasing a license. Telegram communities created and used by the software developers connect scammers with co-conspirators providing other necessary resources: data brokers who supply lists of potential victims' contact information;[14] "spammers" who specialize in sending out text messages in bulk, often operating farms of multiple cell phones or SIM cards;[15] and other specialists to help launder stolen funds once scammers acquire phished credentials.[16]

20. Once scammers use the Outsider software to steal data, they profit from it in various ways. One common trend supported by the Outsider software is to load numerous stolen credit cards onto Apple or Android mobile devices, which can be sold in bulk to criminal networks to

[13] In late-2025, AI-generated phishing attacks generated using artificial intelligence increased more than fourteenfold and now account for over half of all reported phishing incidents. Eliot Baker & Maxime Cartier, *Phishing Trends Report 2026*, Hoxhunt (2026), https://tinyurl.com/3c485zwv.

[14] Data brokers collect bulk sets of contact information from various sources including public records, social media, and data breaches. *See What to Do If a Scammer Has Your Phone Number*, Identity Guard (Feb. 14, 2024), https://tinyurl.com/2bynehp2. For example, in 2021, hackers claimed to have stolen the data of 100 million T-Mobile customers, which they sold on the dark web. Breached data is often available for sale in dark web forums relatively inexpensively. *See, e.g.*, Brian Barnett, *The T-Mobile Data Breach Is One You Can't Ignore*, WIRED (Aug. 16, 2021), https://tinyurl.com/23xwyb3p.

[15] Telegram forums sell both the hardware necessary to send these messages in bulk and access to service providers who operate the hardware on behalf of scammers. One piece of hardware used to do this is an SMS modem pool that can operate over 500 SIM cards, allowing messages to be sent in bulk from telephone numbers that appear to be coming from the United States. *See* Gary Warner, *SMS Pools and what the US Secret Service Really Found Around New York*, Security Boulevard Blog (Sept. 29, 2025), https://tinyurl.com/yta29z8e.

[16] *See* Mnemonic Security Podcast, *The Economy for Phish* (Buzzsprout, Aug. 18, 2025), https://tinyurl.com/4dr3h52v.

make purchases or launder money.[17] Scam groups also have the ability to relay new stolen card information in real time to devices used by co-conspirators who use them to make in-person purchases, a practice known as "ghost tapping."[18] Some recent law enforcement actions have identified networks of Chinese nationals in the United States who take advantage of tap-to-pay functionality to use phones loaded with stolen credit card information to purchase gift cards in bulk.[19] Individuals associated with Outsider including @yy0205 purchase their own tap-to-pay machines and use stolen credit cards to make payments directly to themselves.[20] Additionally, phishing attacks were reported as the leading entry point for ransomware delivery in 2025

[17] *See* Brian Krebs, *How Phished Data Turns into Apple & Google Wallets*, Krebs on Security (Feb. 18, 2025), https://tinyurl.com/wpazfcdv.

[18] *See Ghost-Tapping and the Chinese Cybercriminal Retail Fraud Ecosystem*, Recorded Future (Aug. 14, 2025), https://tinyurl.com/wy5yza4c ("We believe that established, Southeast Asia-based criminal groups that have been involved in scamming activities (romance, investment scam, and cryptomining, among others) since 2020 have begun and will continue to incorporate ghost-tapping campaigns into their activities for financial gains.").

[19] *See* Brian Krebs, *Arrests in Tap-to-Pay Scheme Powered by Phishing*, Krebs on Security (Mar. 21, 2025), https://tinyurl.com/hps3pr3m; Josh Jarnagin, *Knox County Detectives Investigating 'Ghost Tap' Credit Card Fraud,* WVLT8 (May 31, 2025), https://tinyurl.com/y2t7tvzv/; Media Release*, Joint Advisory on Unauthorised Card Transactions Made Using Contactless Payment Methods in Singapore*, Monetary Auth. of Singapore (Feb. 17, 2025), https://tinyurl.com/3uabmj63 ("This modus operandi starts with the scammer . . . obtaining the victim's card credentials through e-commerce related phishing websites, including social media advertisements. The scammer then adds the card details onto the Apple wallet of his own device. An SMS One-Time Password (OTP) would be sent to the victim, who is then tricked to enter the OTP into the phishing website operated by the scammer, thereby giving the scammer access to their card. After successfully taking over the victim's card, the scam syndicate will conspire with a money mule to make unauthorised transactions by connecting the mule's mobile device to the scammer's Apple wallet. The money mule would then be able to make in-person purchases using the contactless payment method . . . to buy goods in-store, for example, high value electronic items or luxury goods.").

[20] *See* @yy0205, Post in the @sinkintojl channel, Telegram (Oct. 17, 2025), https://t[.]me/sinkintojl/562706 (translated), *infra* ¶ 133. *See also* Brian Krebs, *How Phished Data Turns into Apple & Google Wallets*, Krebs on Security (Feb. 18, 2025), https://tinyurl.com/wpazfcdv.

(involved in 35% of all attacks, an increase from 25% in 2024), meaning that data collected through phishing of individuals is often then used to conduct ransomware attacks on organizations.[21]

21. The Outsider software in particular has been used to facilitate a trend in which scammers use stolen brokerage firm credentials to perpetrate a new version of a "pump and dump" scheme. In this version of the scheme, scammers pre-purchase a certain stock, and then use compromised brokerage accounts to purchase large volumes of the stock, inflating the price. Once it reaches a certain price, they liquidate their original holdings.[22] @sinkinto01 has posted a tutorial video showcasing Outsider's ability to create a fraudulent version of a major United States-based brokerage firm's website and the software offers pre-made templates spoofing the websites of 31 financial and brokerage firms.

III. @chenlun, @sinkinto01, and the History of Outsider

22. The developer(s) behind Outsider were one of the first major purveyors of sophisticated phishing-as-a-service software. In October 2022, the user(s) using the Telegram handle @chenlun released an early version of the phishing kit.[23] At the time, the platform offered templates focused on spoofing postal and shipping companies like the United States Postal Service ("USPS") and its international counterparts. The Telegram profile @chenlun posted openly about the phishing kit and operated various Telegram channels dedicated to the marketing and operation of the software. In the fall of 2023, a blogger and a security researcher independently published content linking the Telegram user @chenlun to various postal phishing scams, which caused the

[21] *2025 SpyCloud Identity Threat Report: Trends, Benchmarks, and Strategies to Strengthen Identity Threat Protection*, SpyCloud.com (Sept. 23, 2025), https://tinyurl.com/yv9krpx3.
[22] *See* Brian Krebs, *Mobile Phishers Target Brokerage Accounts in 'Ramp and Dump' Cashout Scheme*, Krebs on Security (Aug. 15, 2025), https://tinyurl.com/6z23acbu.
[23] g0njxa, *Chenlun aka Sinkinto01: A worldwide phishing & carding campaigns provider*, Medium (Aug. 21, 2023), https://tinyurl.com/kb3bzsym.

@chenlun account to be spammed.[24] Shortly thereafter, @chenlun deleted much of their Telegram presence and activity slowed for some time.

23. In the spring of 2025, the former user of @chenlun reappeared using the Telegram handle @sinkinto01. I note that the Chinese characters that make up "chenlun" translate to "Sinkinto" or "Sinking." On May 29, 2025, the user of @sinkinto01 posted on a known phishing forum, CoSmileOnly. In two lengthy posts, the user described their journey into the "C Circle," a term I know to refer to "carding," or phishing leading to credit card theft, in 2021 and 2022. They described how, after being targeted by foreign bloggers, they changed their username from @chenlun and gave up on the industry. The post, however, served as an announcement that they would be coming out of retirement. A second post included links to the @sinkinto01 username and Telegram channels that later sold the Outsider software.

24. Days later, on June 1, 2025, Telegram user @sinkinto01 posted a message in a new Telegram channel, @sinkintopd, announcing that source code would be released in approximately one month. The user then indicated that the software required a "complete redevelopment" due to "recent risk control measures." This Telegram channel was thereafter devoted completely to discussions of the Outsider phishing software.

[24] *See* Brian Krebs, *Phishers Spoof USPS, 12 Other Natl' Postal Services*, Krebs on Security (Oct. 9, 2023), https://tinyurl.com/37nf7eyd.

Figure 1. @sinkinto01, Post in the @sinkintopd channel announcing the development of Outsider software, Telegram (June 1, 2025), https://t[.]me/sinkintopd (translated).[25]

25. In June and July of 2025, @sinkinto01 posted updates on the software development and even showed demos of early versions of the software. On July 29, 2025, @sinkinto01 posted four tutorial videos, making clear that by this date, the software was operational and ready for purchase. The tutorial videos, among other things, detailed instructions for purchasing the software using a self-service order bot (@OutsiderCodeBot), installing the software, activating the software, and utilizing different features of the software to make phishing pages. Whereas the previous version of @chenlun's software relied mostly on pre-made templates, Outsider featured additional functionality including the ability to use AI to target any brand with a phishing page, new customization options, and more templates targeting additional industries. It also claimed to feature "anti-blocking" capabilities, which I understand to mean the ability to subvert attempts by browsers like Google Chrome to block or mark certain websites as malicious.

[25] Figures that include "(translated)" in the description have been translated from Chinese to English. At the time of my review, I used Google Translate or Telegram's translation feature. I have since had all such figures translated by a court-certified service. **Exhibit 1** includes true and correct copies of the original screenshots I took of the software, Telegram channels, or tutorial videos and the respective English translations and certificates. Ex. 1 at 4.

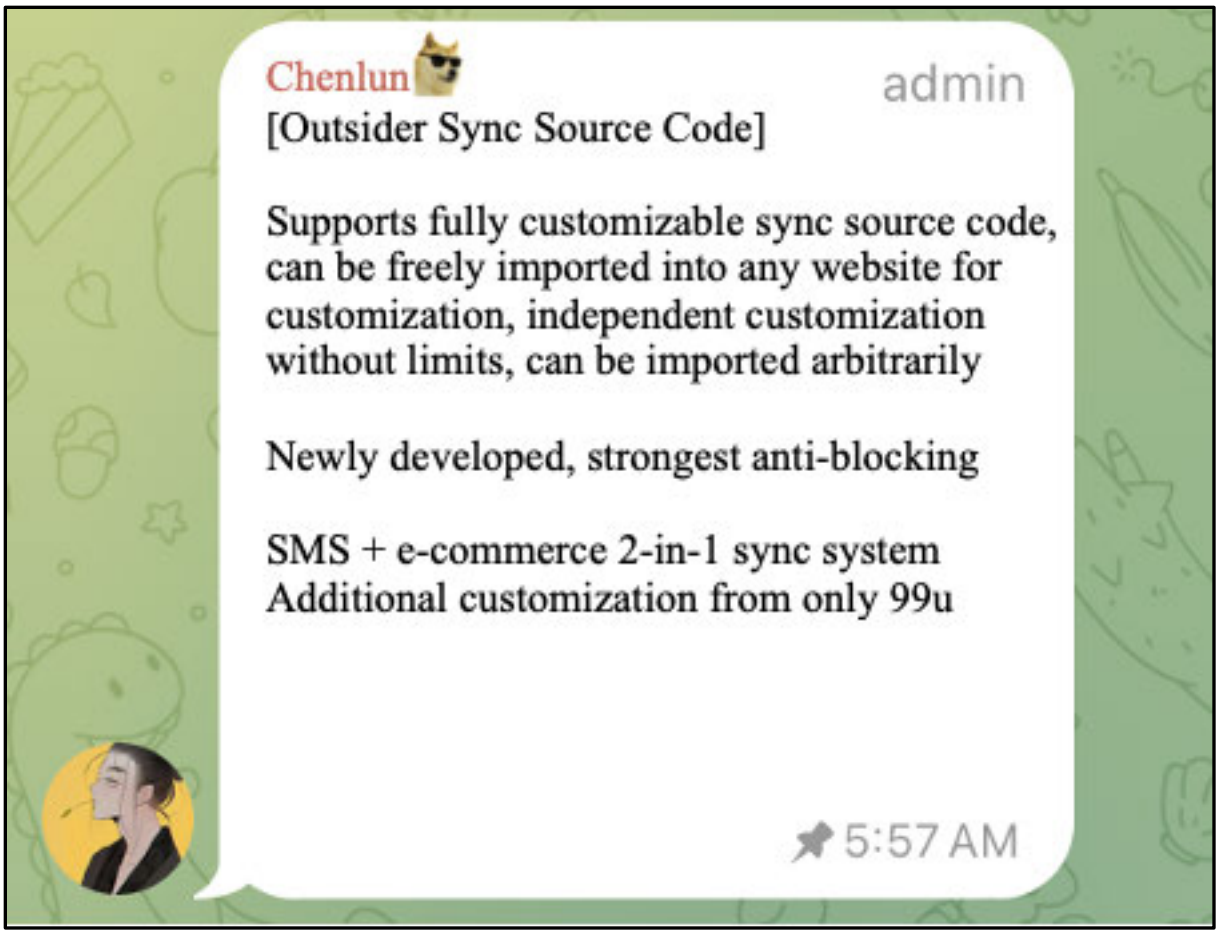


Figure 2. @sinkinto01, Post in phishing-related channel @Shiqi0205 advertising Outsider source code features, Telegram (Sept. 29, 2025), https://t[.]me/Shiqi0205/3986 (translated).[26]

26. Over the next few days, @sinkinto01 posted additional tutorial videos. These discussed features like the ability of Outsider to link directly to Google Drive, allowing users to automatically upload their stolen financial data to Google's cloud storage.[27] Another tutorial video showed how users could incorporate code generated by Google Gemini into Outsider phishing pages. Yet another tutorial video advertised a service in which Outsider personnel would purchase a Google Cloud server on which scammers could host phishing pages created with Outsider. Since the relaunch, the software has been updated by @sinkinto01 at least 53 times.

[26] Ex. 1 at 8.
[27] Based on a review of Outsider's features, this feature was disabled in early 2026.

27. While the exact scope of the fraud connected to Outsider is not easily quantifiable, it is one of the most pervasive phishing software products available today. One security research firm estimated that as of November 2023, the prior version of the software released by @chenlun was responsible for the theft of at least 36,000 payment cards issued from financial institutions in 95 countries.[28] As will be discussed in further detail herein, NAXO identified approximately 31,391 websites created with the original version of the Chenlun software and approximately 9,354 domains created using Outsider.

IV. Examples of Phishing Schemes Facilitated by Outsider

28. Outsider offers the ability to turn any website into a phishing website and can thereby support virtually any type of phishing scheme. As certain schemes lost their efficacy due to growing public awareness, the Enterprise shifted to different schemes. One of the most common phishing schemes manufactured by Outsider software targets customers of financial institutions. In these types of scams, victims receive text messages purporting to be from their bank or brokerage firm. The texts say things like, "Did you authorize this transaction?" or "Prevent your account from being frozen" or even, "You have a message," and include a link that purports to take them to the website of their financial institution. The victim clicks the link in the text message and navigates to the website that appears to be a login page for their financial institution. Although the victim thinks they are logging in to their financial account, they are in reality funneling their account login information directly to the scammers through the spoofed website.[29]

[28] *See As Black Friday Approaches, 3 Key Trends Offer Insights for Mitigating Online Shopping Scams*, Gemini Advisory Blog (Nov. 22, 2023), https://tinyurl.com/5v9df9re.
[29] *Stay Vigilant Against Text Scams*, Fidelity Investments Learning Center, Customer Service (Aug. 7, 2025), https://tinyurl.com/mpad6cw6.

29. A July 29, 2025, tutorial video posted by @sinkinto01 demonstrates the use of a phishing template targeting a United States-based brokerage firm. In the phishing page displayed in the video, a victim is presented with a webpage that claims that their account has been restricted. It then prompts the user to "verify their account," through one of various methods, each requiring them to input personal information.

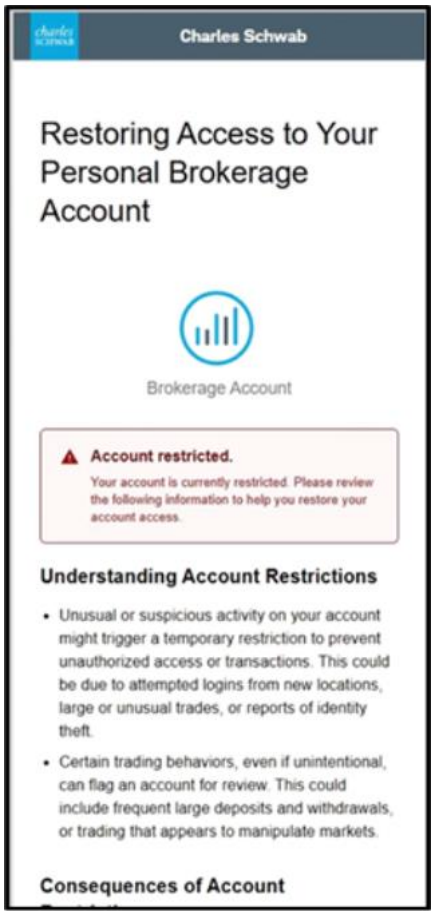
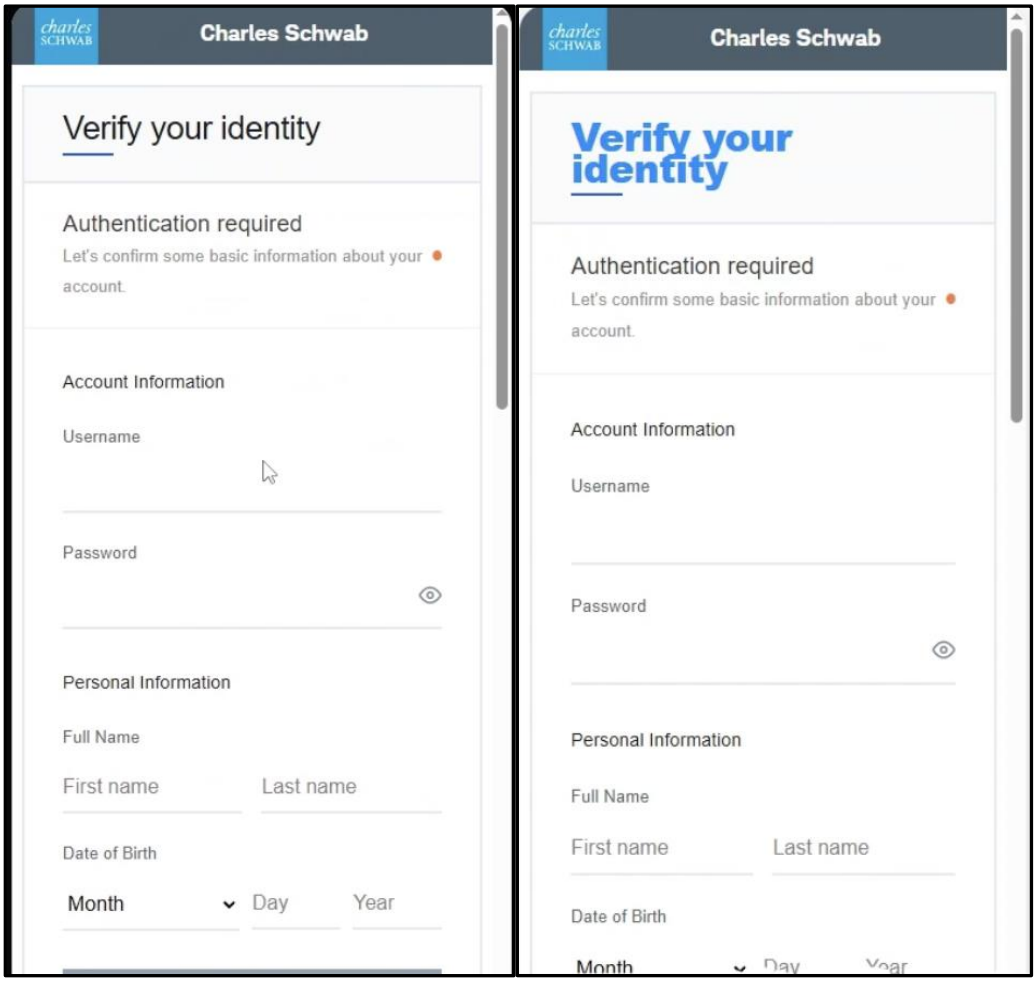


Figure 3. Screenshot from Outsider tutorial video, Telegram (July 29, 2025), https://t[.]me/sinkintopd/12.

30. As the tutorial video continues, it highlights features of the Outsider software that allow scammers to customize the brokerage company phishing pages in various ways. Scammers can configure the phishing pages to ask for different types of information from victims. For example, the scammer can choose to require a victim to "verify their account" by providing personal information, setting up MFA, or answering security questions, all of which allow

scammers to collect information that would let them take over not only the brokerage account, but possibly other accounts as well. Scammers can also use the software to alter the text, font, and appearance of the page.



Figures 4, 5. Screenshots from Outsider tutorial video showing the ability to customize font and color on the phishing website, Telegram (July 29, 2025), https://t[.]me/sinkintopd/12.

31. Many financial institutions implement MFA technologies to combat fraud, including by sending numerical codes via SMS or through a dedicated mobile application. Certain features of Outsider also enable the fraudsters to acquire these codes. According to the brokerage company tutorial video, and my own familiarity with the software, I believe that Outsider subverts MFA protections in the following way. Once a victim attempts to access their account on the pages

pictured above, they are directed to a fictitious MFA phishing page, prompting them to enter a code to verify their purchase.

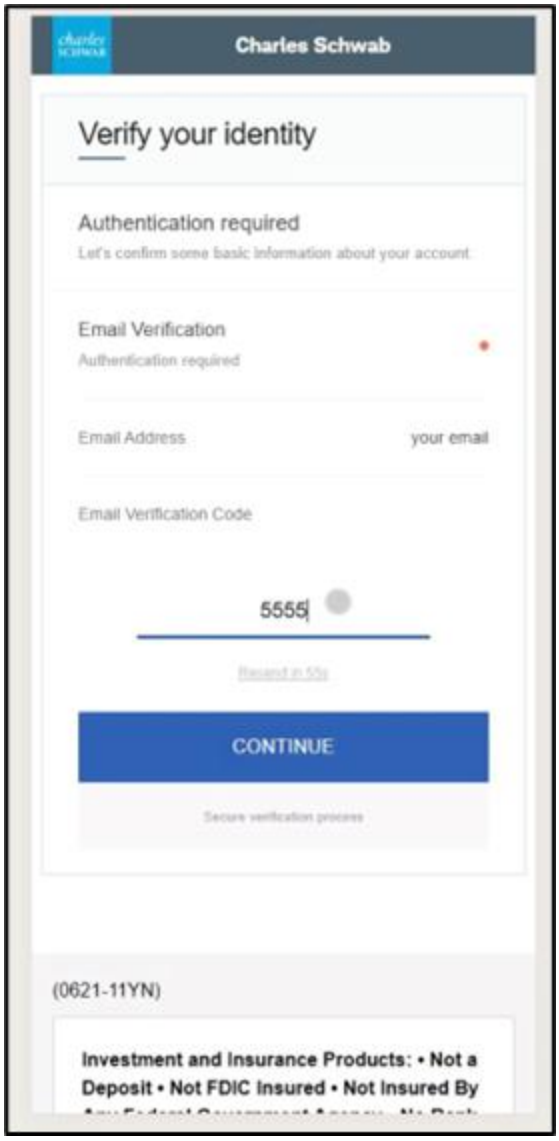
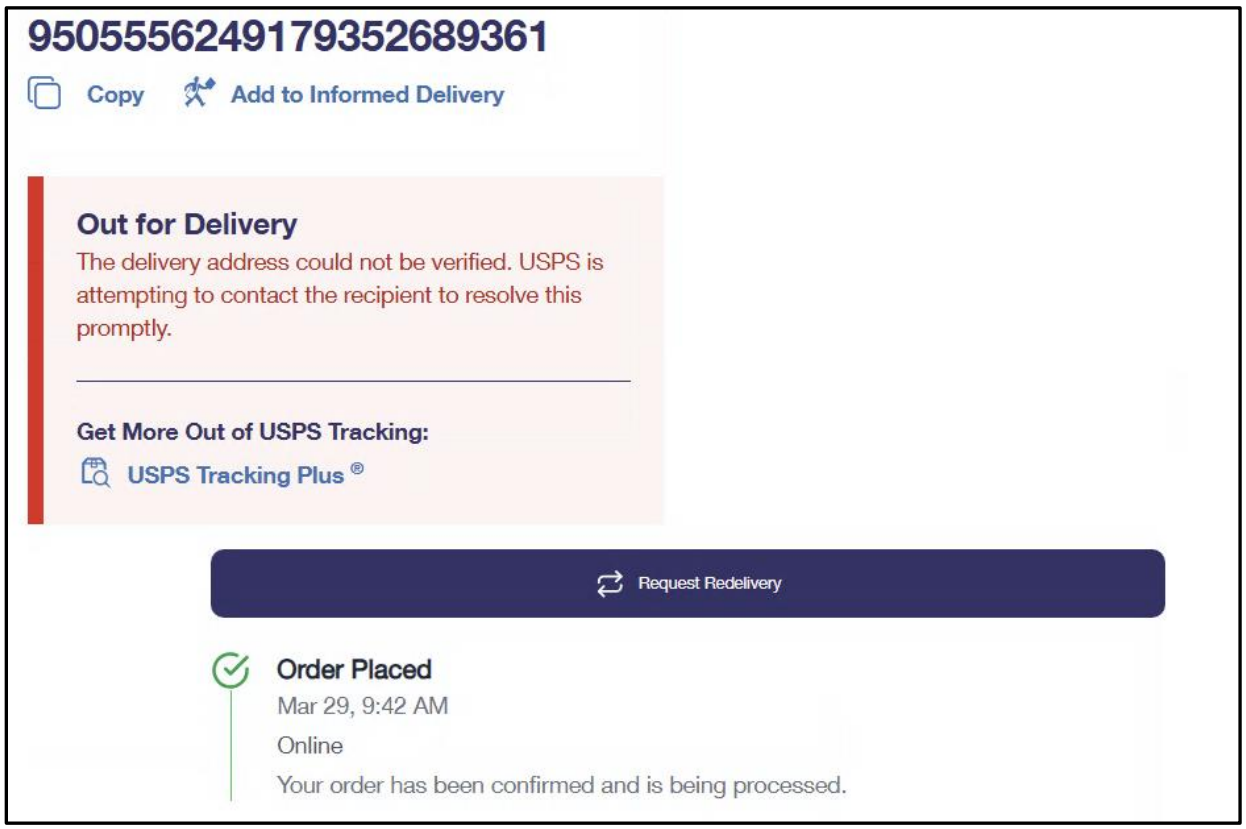


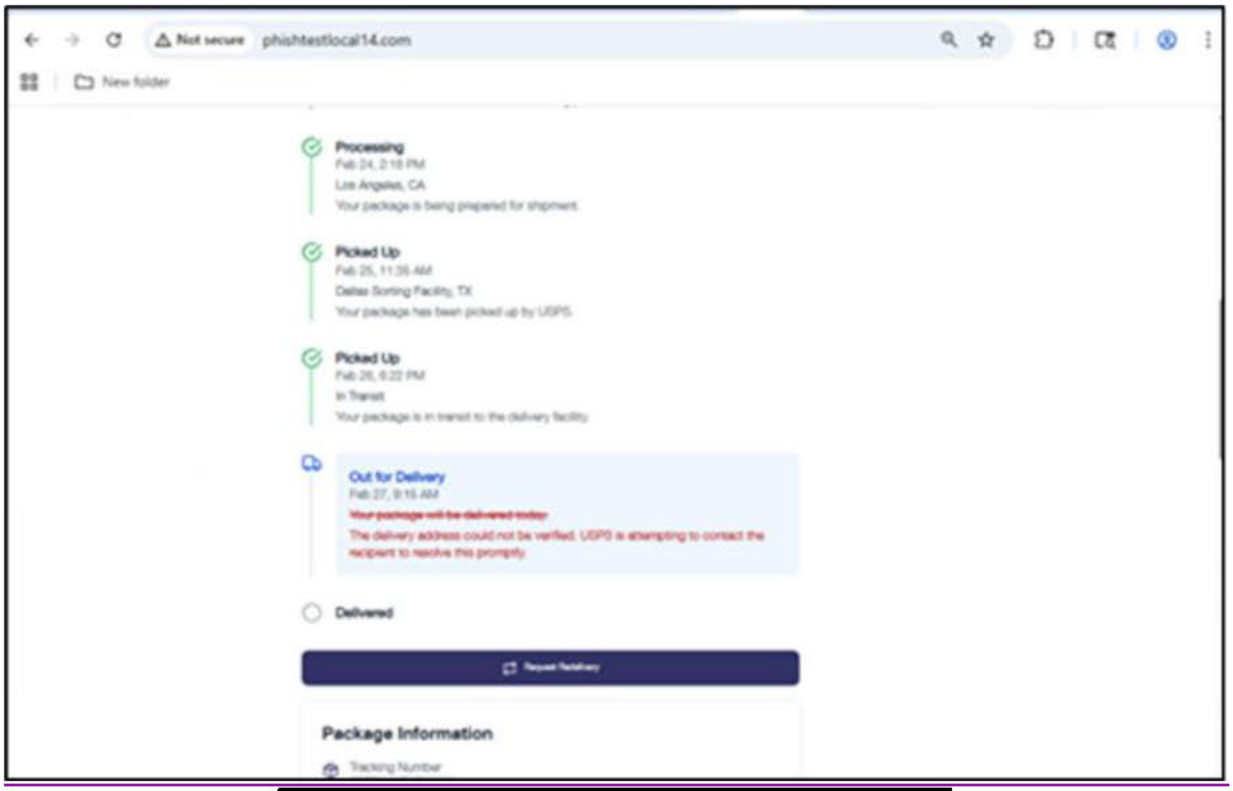
Figure 6. Screenshot from Outsider tutorial video, Telegram (July 29, 2025), https://t[.]me/sinkintopd/12.

32. At the same time, the scammer uses the account login information that the victim previously provided to navigate to the real brokerage website and attempt to log in as the victim. This prompts the brokerage firm to send an MFA code to the victim, who then types it into the phishing page pictured above. This allows the scammer to input the code in the real brokerage website and access the account from their own device. This can then allow the scammer to make

their device a trusted device, negating the need for MFA codes when they access the account in the future.

33. The Outsider phishing kit also includes templates for the original @chenlun scam targeting USPS and other national and international shipping companies. From the victim's perspective, the USPS scam begins with a fake USPS text message purporting to notify a victim of an issue with a package delivery, such as that the target missed a package delivery. The message includes a link (to the website created using Outsider) for the victim to reschedule their delivery. If the victim clicks the link, they are directed to the fake USPS website that requires payment of a small redelivery fee. Of course, the original text message was a ruse, and there was no package to deliver. The scammers simply collect any payment information that the victim types into the website.





Figures 7, 8, 9. Screenshots of USPS phishing page template included in Outsider software (emphasis added). I note that the YouTube logo is included in the bottom of the page.

34. Additionally, on January 21, 2026, @sinkinto01 advertised a "brand new US traffic ticket" source code with "significantly improved visuals compared to ordinary traffic ticket

information." I understand this to mean that @sinkinto01 updated the Outsider software to include improved templates that look more like real government websites that collect payments for traffic tickets. In this scheme, victims receive a text message indicating that they owe money to a local municipality for a traffic or parking ticket. The text message usually includes a link to a website that mimics that of a real collection website. When a user attempts to pay their outstanding ticket, they are prompted to input payment data, which is funneled to the scammers.

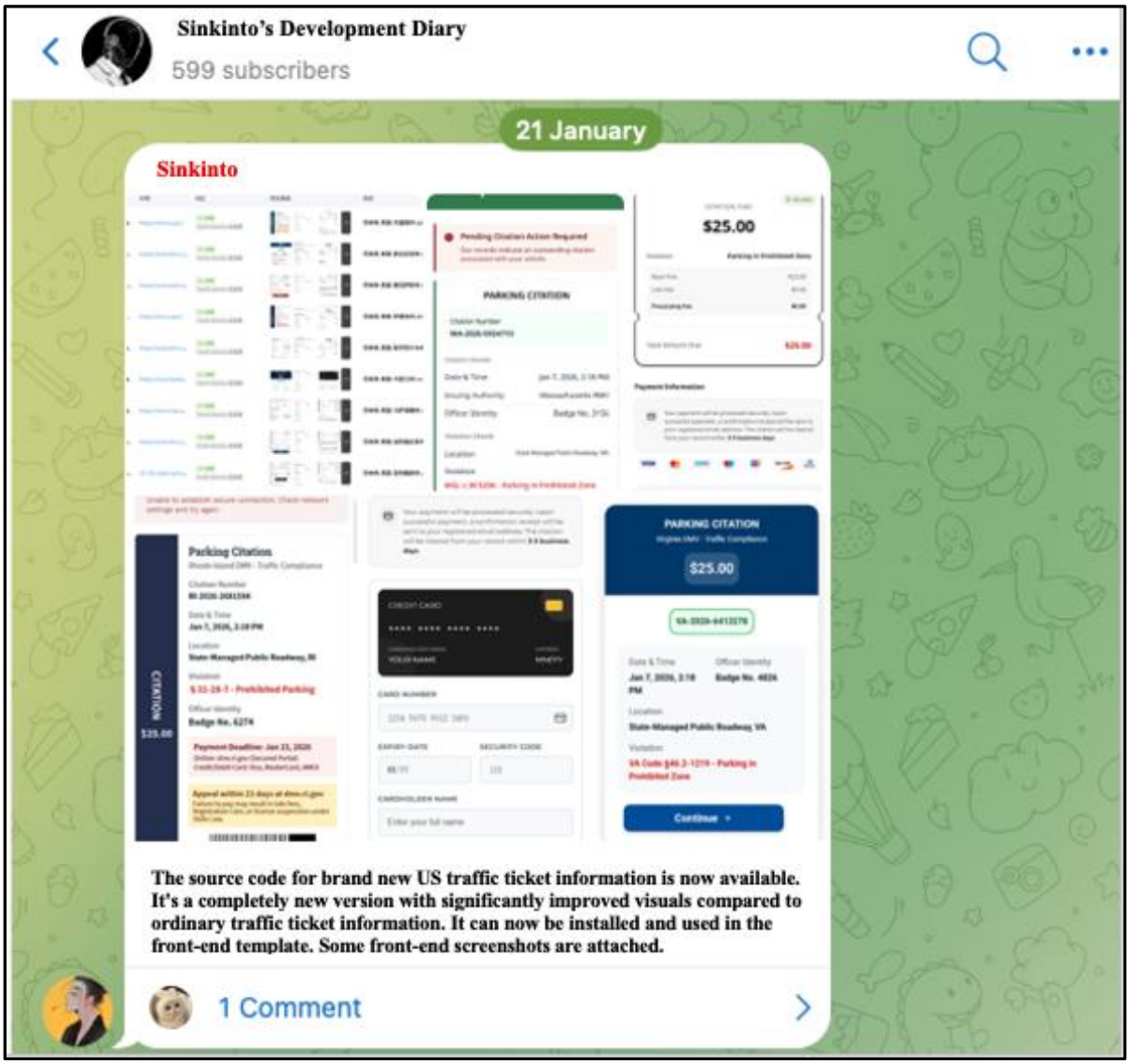
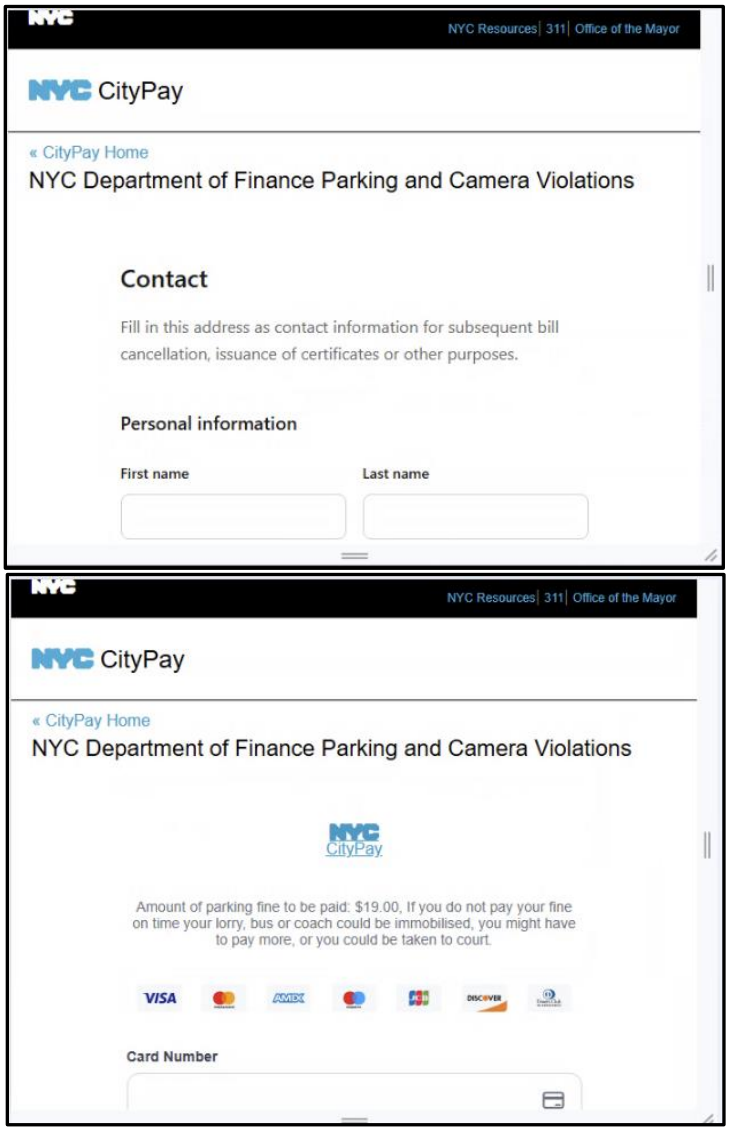


Figure 10. @sinkintopd, Post showing templates for traffic ticket phishing pages, Telegram (Jan. 21, 2026), https://t[.]me/sinkintopd (translated).[30]

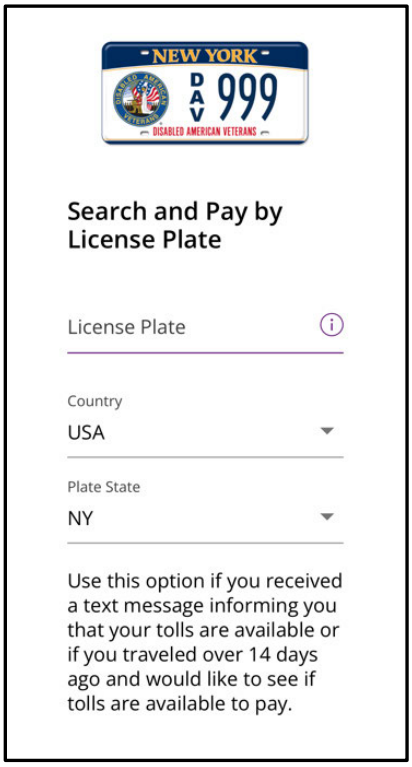
[30] Ex. 1 at 12.

35. For example, the Outsider software has a template for a phishing scam impersonating NYC.Gov, which appears to collect a fine for "parking and camera violations." The website prompts users to input their payment information, which is of course funneled to the scammers.



Figures 11, 12. Screenshots from NYC CityPay phishing page template included with Outsider software.

36. Outsider also supports a very similar scam in which phishing pages impersonate toll collection agencies. One template impersonates E-ZPass New York, targeting New York residents with purported overdue toll violations.



Figures 13, 14. Screenshot from E-ZPass NY phishing page template included with Outsider software (l) and screenshot of the E-ZPassny.com website as it appeared on or around March 10, 2026 (r). Wayback Mach. Internet Archive, E-ZPass New York Service Center, https://tinyurl.com/23tasnt6 (mobile version).

37. A scheme which appears to have gained popularity in early 2026 targets victims by mimicking telecommunications companies. In this scam, victims receive a text message notifying them of available points for redemption in a rewards program offered by their service provider. The Outsider platform includes a variety of templates that can be used to create phishing websites for this scheme. An example of one template that contains Google logos is shown below in Figure 15.

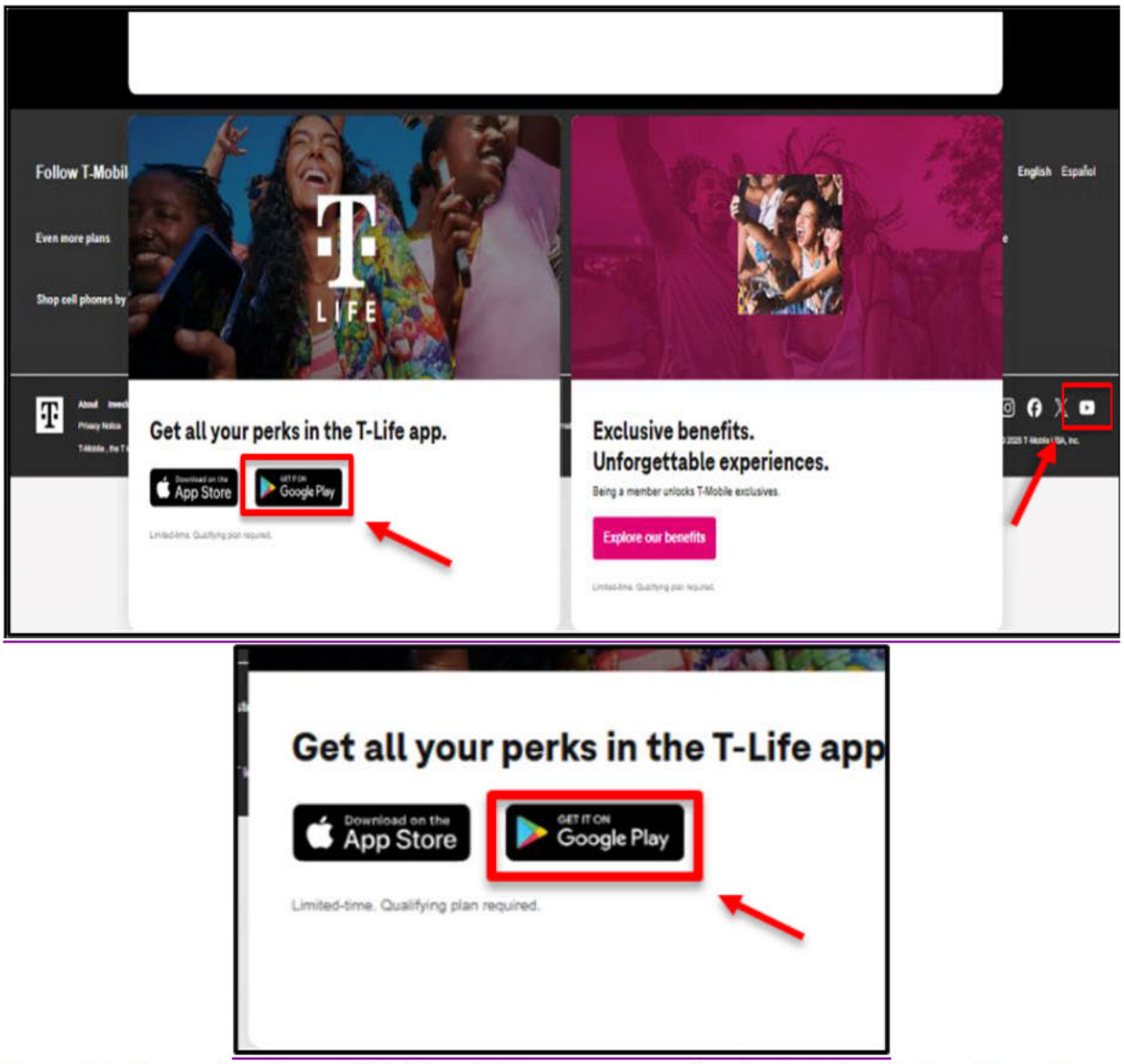


Figure 15. Screenshot from T-Mobile phishing page template included with Outsider software (emphasis added). I note that this template includes the Google Play and YouTube logos; zoomed in Google Play logo.

38. To assess how the telecommunications scams work, I downloaded a template for a phishing website from the Outsider platform that replicated a T-Mobile rewards webpage. The template included several different parts, which each provided a template for a different webpage that a scammer can use to generate each of the subdomains needed to compile an interactive phishing site. Based on my review of the different parts of the template, I believe that the telecommunications scheme works as described below.

39. A victim that clicks the link in a bait message is directed to a website that mimics a rewards program through the recipient's wireless carrier. Using the T-Mobile program template, for example, the victim is directed to a fake "Rewards Portal" that prompts the victim to enter their phone number, as shown in Figure 16 below.

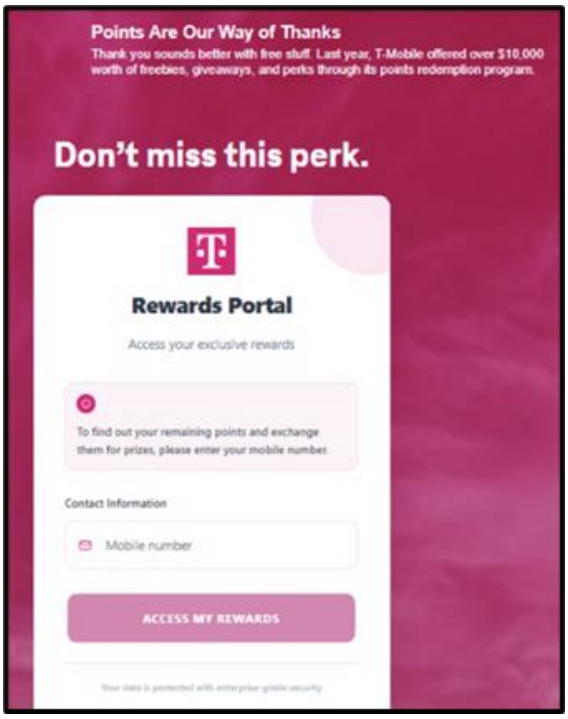


Figure 16. Screenshot from T-Mobile phishing page template included with Outsider software.

40. After entering a phone number and "logging in" to the fake portal, the victim is taken to a fake rewards page that prominently creates a sense of urgency by warning that the victim's accumulated (fictitious) points are about to expire, typically showing that nearly all of the points will expire in the near term, as shown in Figure 17 below. This encourages the victim to redeem expiring points for various products.

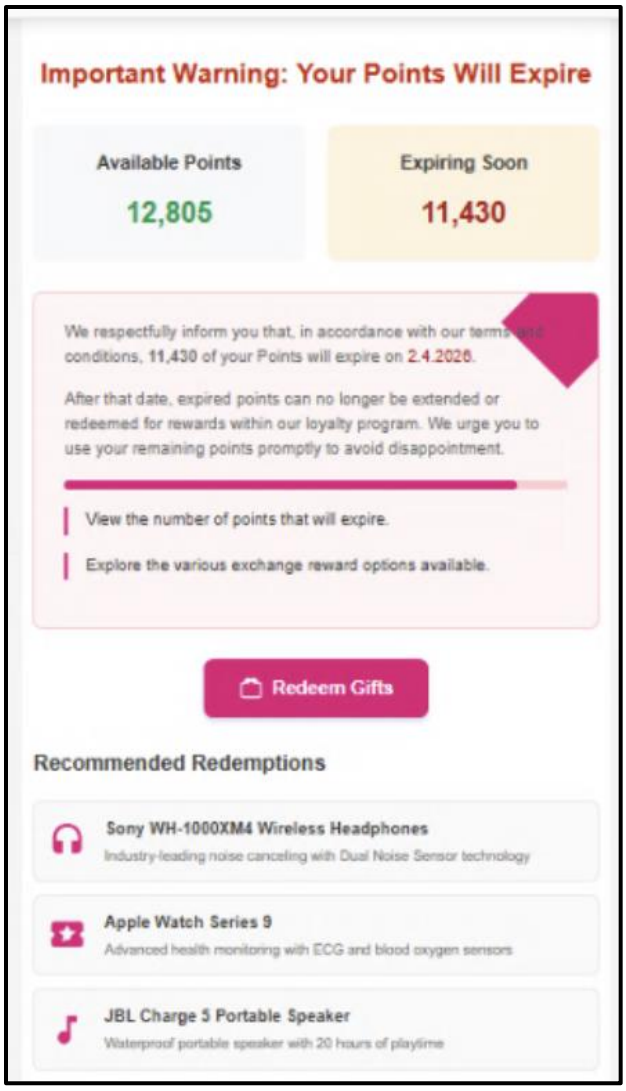


Figure 17. Screenshot from T-Mobile phishing page template included with Outsider software.

41. The rewards page in this template also includes a "Redeem Gifts" option together with a "Recommended Redemptions" section designed to entice the victim with high-value items, such as Bluetooth headphones, a late-model Apple Watch, or a portable speaker.

42. Once a victim clicks "Redeem Gifts," the victim is taken to a page that allows the victim to choose from various high-end products. An example is shown in Figure 18 below.

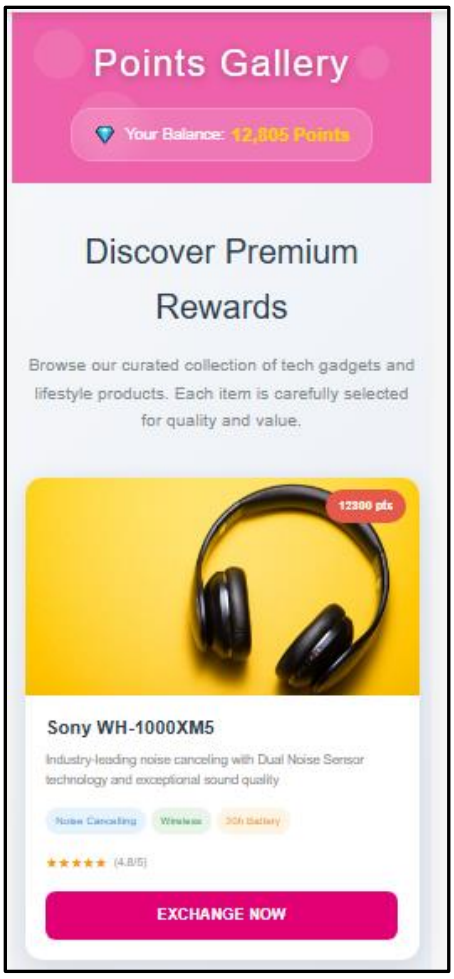
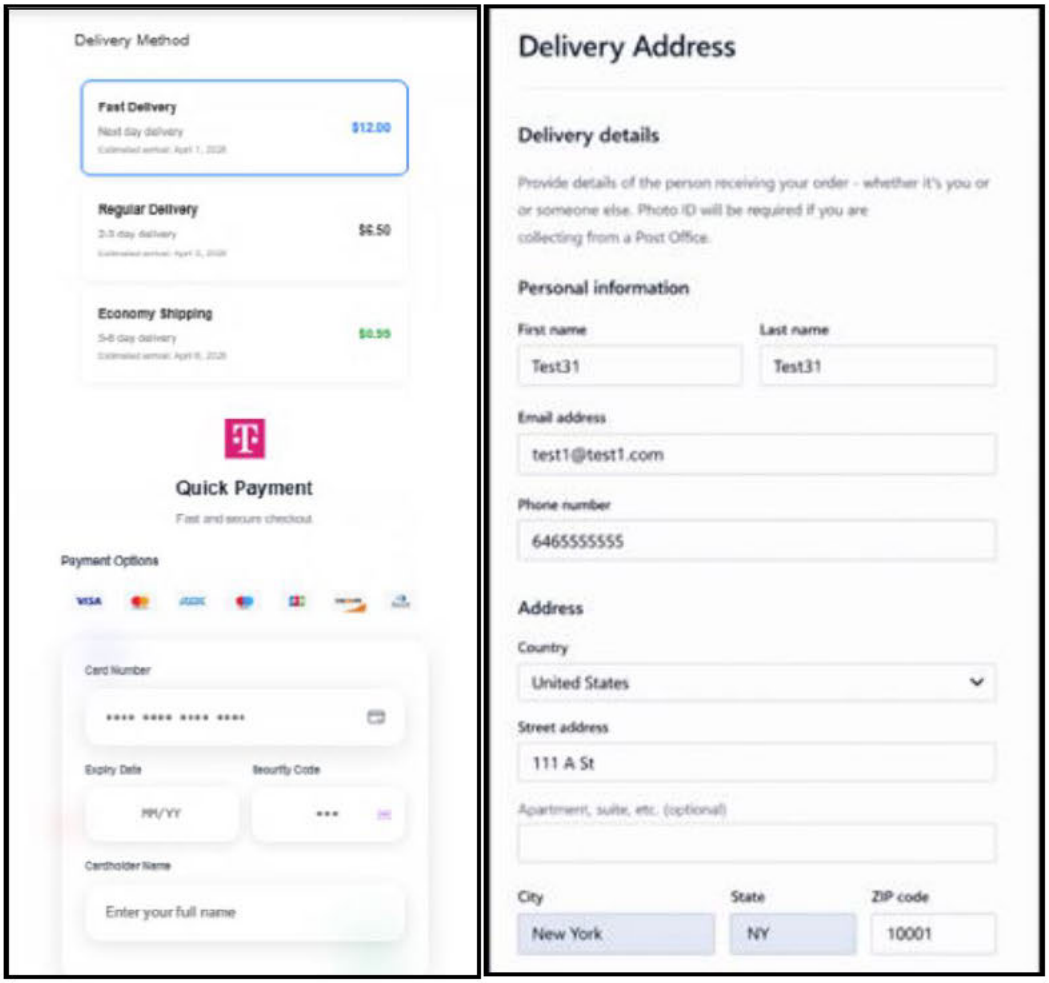


Figure 18. Screenshot from T-Mobile phishing page template in Outsider platform.

43. When the victim selects an item and clicks "Exchange Now," the victim is asked to provide payment information to pay for some portion of the cost of the products or to cover a shipping fee. The victim is led to believe that the listed item will be provided in exchange only for a small shipping fee, in a range of approximately $0.99 to $12.00, as shown in Figure 19 below. The site's portal for entering financial information to pay the "shipping" fee is where the victim's information is stolen.



Figures 19, 20. Screenshots from T-Mobile phishing page template in Outsider platform.

44. As the victim enters his or her information into the shipping and payment pages, the Outsider platform captures it in real time and it is immediately visible to the scammer through the Outsider dashboard. This allows the scammers operating Outsider to compile a profile of the victim's personal information including name, email address, shipping address, and financial information. Information obtained from victims is monetized, as described in areas of this declaration referring to the activities of @yy0205.

45. The USPS/shipping company, telecom company, parking/traffic ticket, and financial institution scams are examples of SMS scams, scams which typically begin with text messages directing victims to fake websites. Outsider includes over 290 templates for fake

websites that can be used in SMS scams. **Appendix B** is a true and correct list of a representative sample of Outsider templates with screenshots of each template.

46. Outsider also offers tools to create "e-commerce" phishing scams—one that can be used with a content management system ("CMS") platform, and another tailored to a United States-based e-commerce platform—both of which allow a user to create their own fake online store, the only purpose of which is to steal victims' payment information.

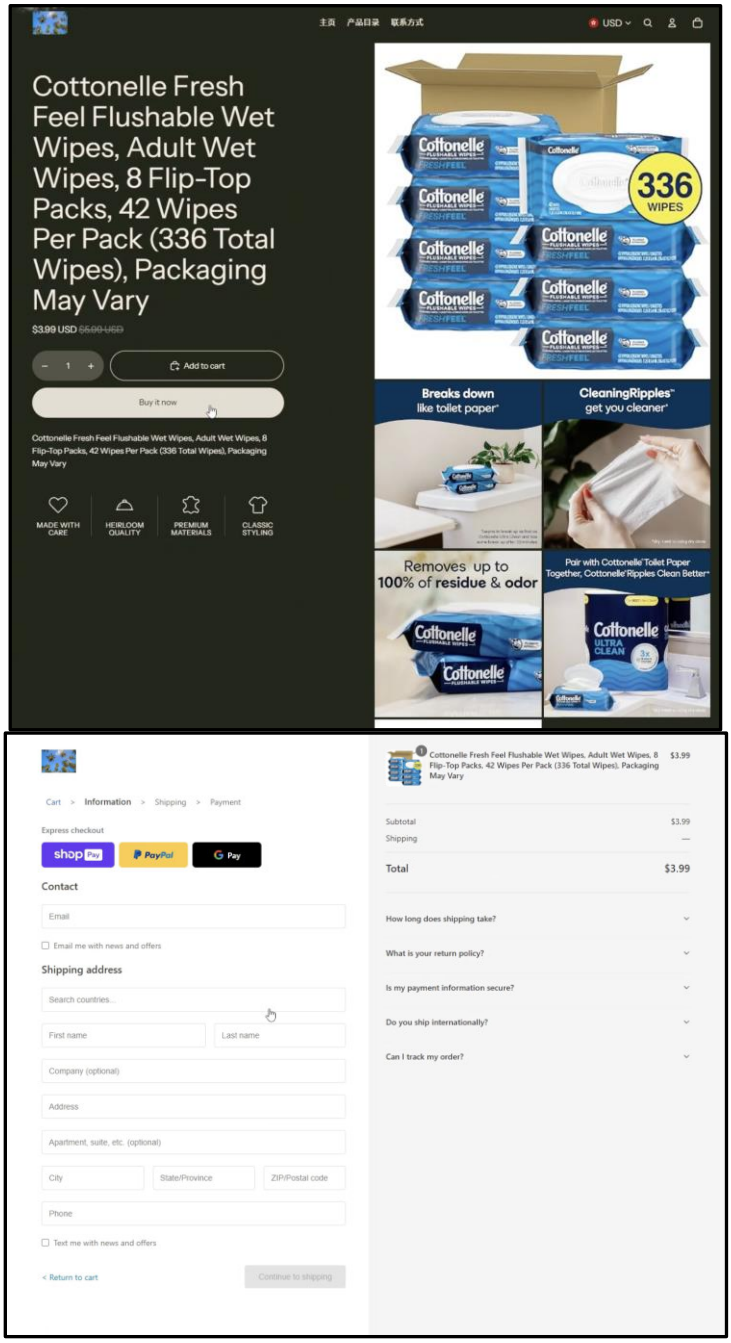
47. The CMS version of the tool provides scammers with the ability to create a fraudulent website from scratch and integrate payment options that funnel user data to Outsider.[31] These pages often spoof legitimate retail websites.

48. The e-commerce platform version of the tool supports developing a fake store on a legitimate e-commerce platform. Unlike the CMS version of the software, which allows users to completely customize their website, the e-commerce platform already provides some infrastructure for an online store, and users simply add photographs and descriptions of whatever products they want to sell (or, in the case of the scammers, pretend to sell). Outsider can manipulate the payment functionality on the e-commerce platform to directly funnel any payment information to Outsider.

49. In either type of e-commerce scam, when victims input personal details and payment information to purchase products on these fake websites, the information is funneled to Outsider and victims never receive their purchases. I believe that victims are directed to these websites through online advertisements or search results.

[31] The CMS version of the tool references a software-as-a-service company that offers tools and features that, among other things, help create websites to sell products to customers online. Its users access settings and options for their websites through a web-based dashboard that adds various functionalities and configures the user experience.

50. For example, @sinkinto01 posted a tutorial video for creating one such website on the e-commerce platform. The video shows that when a user attempts to purchase a listed product (in this case flushable wet wipes), they are directed to a page that prompts them to input various payment methods and a shipping address.



Figures 21, 22. Screenshots from e-commerce tutorial video, Telegram (Aug. 23, 2025), https://t[.]me/sinkintopd/34.

51. The page allows three options for "express checkout" including Shop Pay, PayPal, and Google Pay. In this tutorial video, the "phishing victim" clicks on PayPal and is directed to a box prompting them to input their phone number and password.

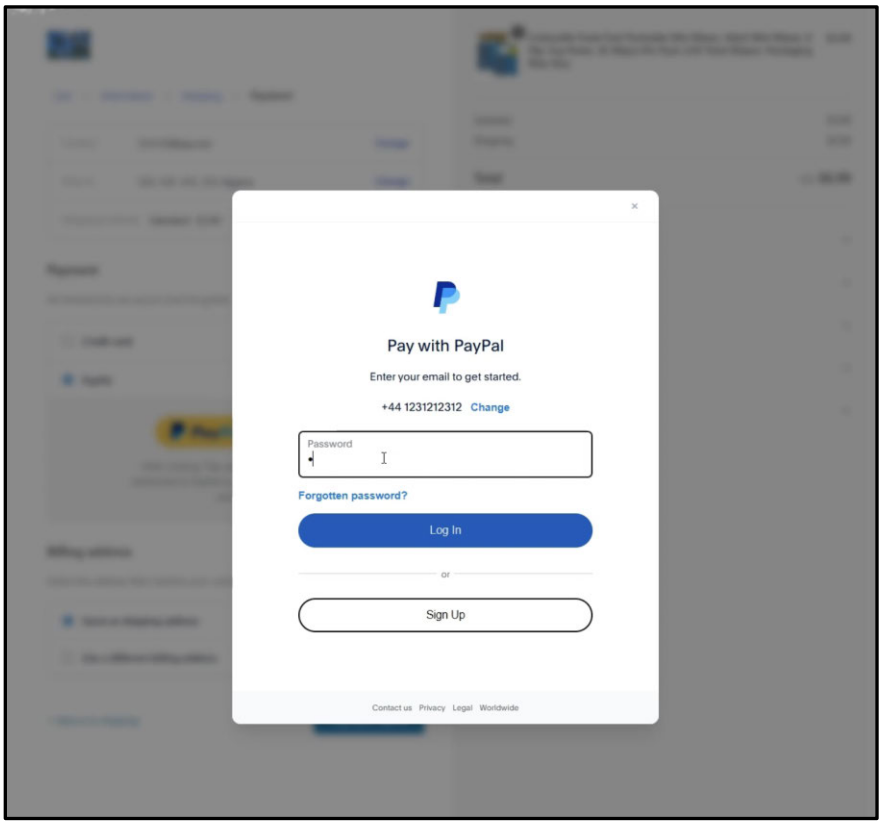


Figure 23. Screenshot from e-commerce tutorial video, Telegram (Aug. 23, 2025), https://t[.]me/sinkintopd/34.

52. In the video, when the phishing victim enters an email address and password, both entries immediately appear in the Outsider software. The scammer selects from a list of options in the software, and causes the victim to receive a pop-up that reads "Add Credit or Debit Card." It is accompanied by an error message reading, "Due to updates in the bank's security policies, our system has undergone an upgrade. As a result, we kindly ask you to reverify or update your bank card information." I understand this to be the scammer's attempt to steal not only the PayPal login, but a credit card number as well. I notice that this page includes the logos for various credit card

companies purportedly "accepted" by the payment platform Outsider is spoofing: Mastercard, Discover, Diners Club, Visa, American Express, and JCB.

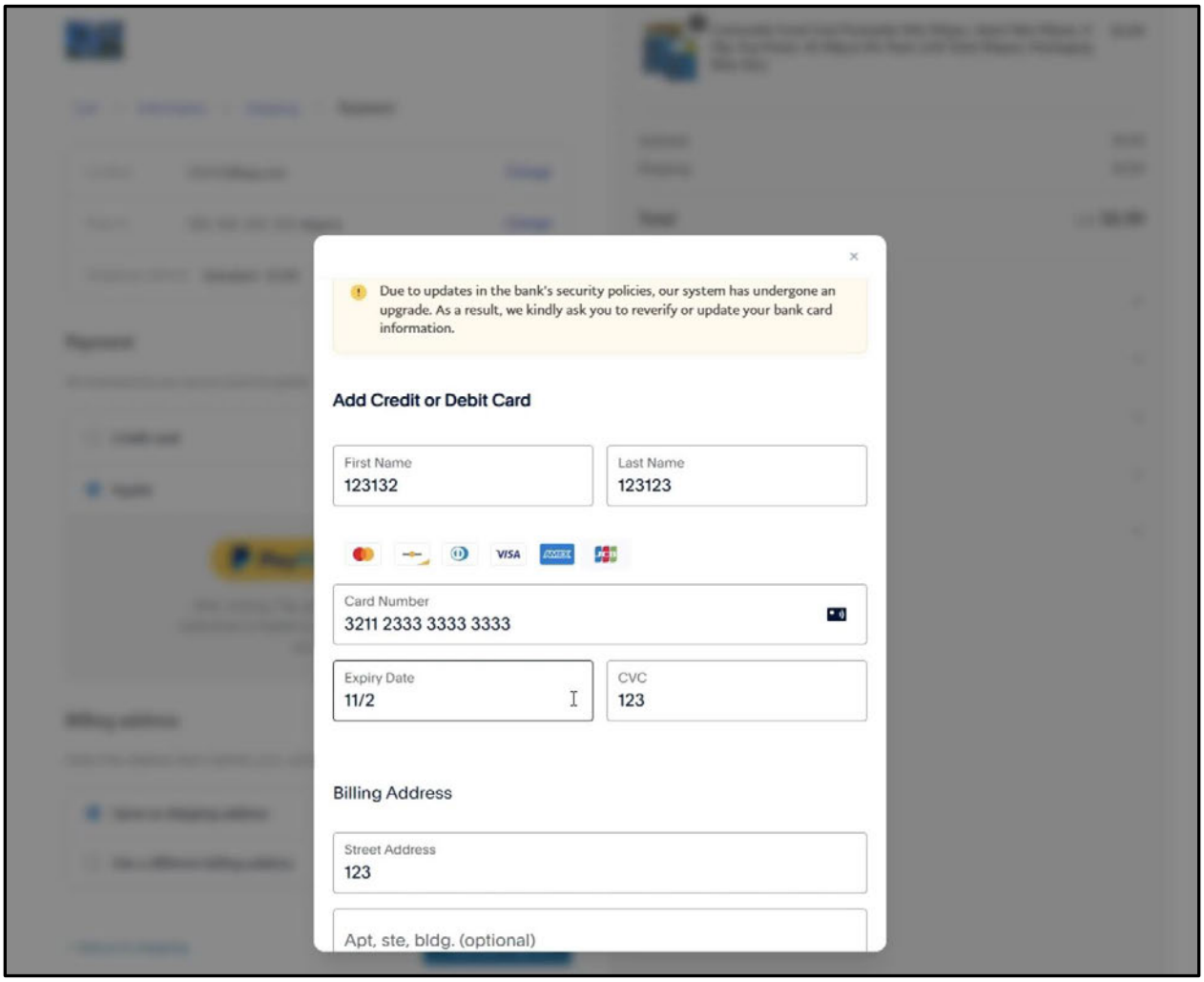


Figure 24. Screenshot from e-commerce tutorial video, Telegram (Aug. 23, 2025), https://t[.]me/sinkintopd/34.

53. After the "victim" inputs their credit card information and submits it, they are directed back to a PayPal screen which prompts them to enter a security code. Although not visible in the video, I believe that, at this point in the scam, the fraudster attempts to log in to the victim's PayPal account (with the login and password the victim previously entered into the phishing website), prompting an MFA code to be sent to the victim's phone. The phishing victim receives

a verification code from PayPal which they enter into the phishing website, allowing the fraudster to successfully access the victim's PayPal account.

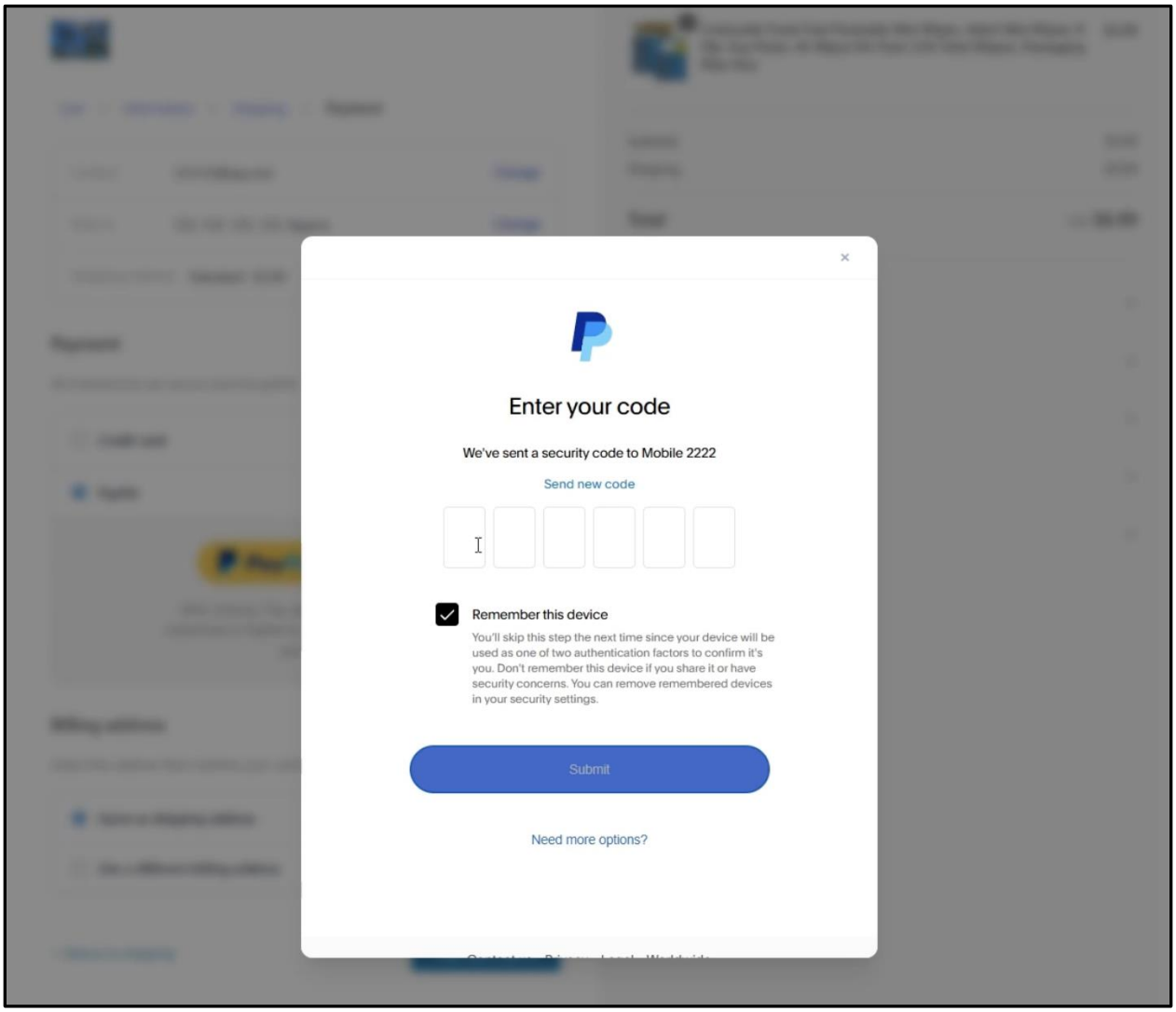


Figure 25. Screenshot from e-commerce tutorial video, Telegram (Aug. 23, 2025), https://t[.]me/sinkintopd/34.

54. Once the scammer is satisfied that they have collected sufficient data about the phishing victim, they can send the victim to a page indicating that their purchase was complete.

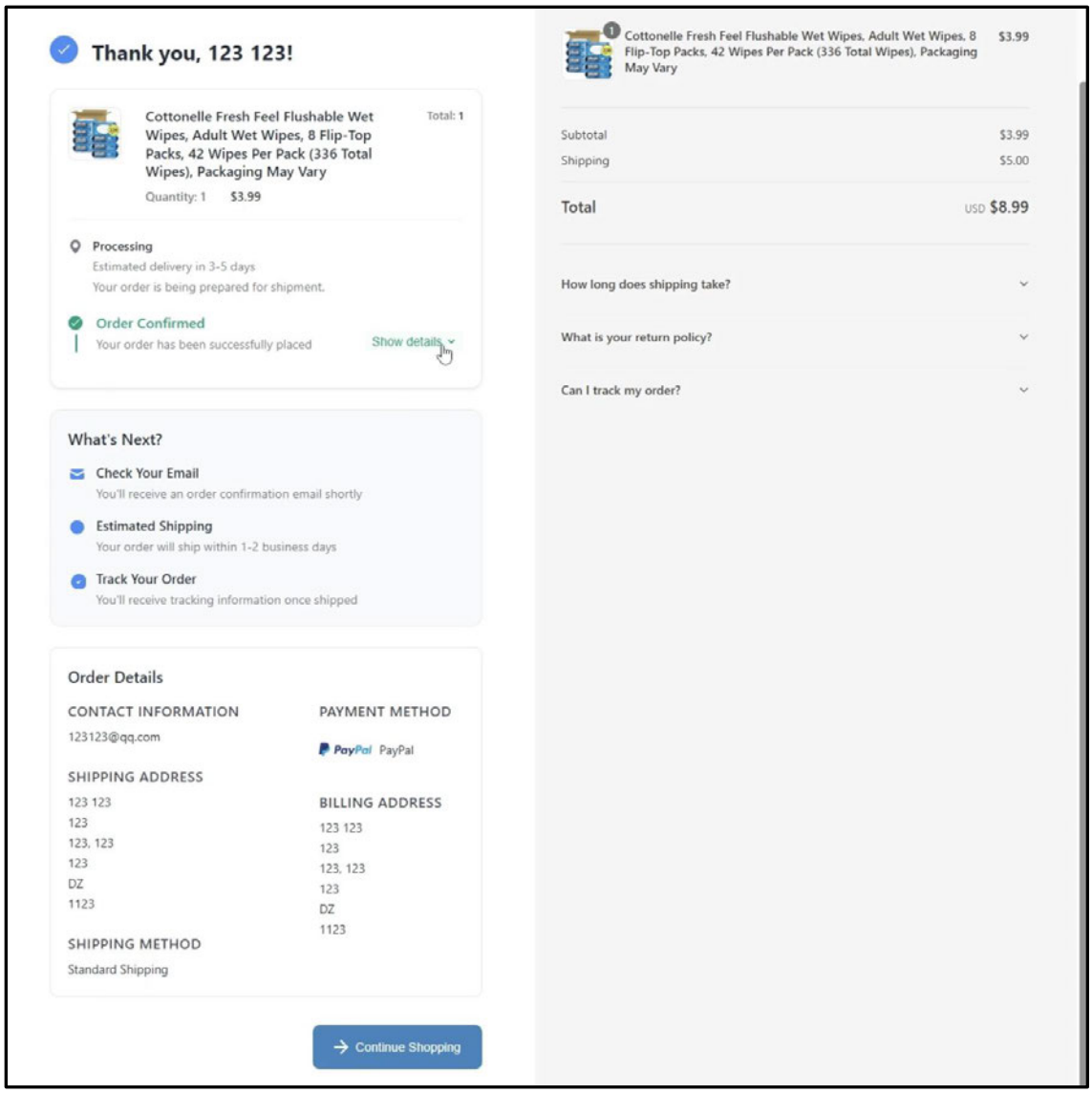


Figure 26. Screenshot from e-commerce tutorial video, Telegram (Aug. 23, 2025), https://t[.]me/sinkintopd/34.

55. The payment portions of these websites are designed to funnel credit card information directly to the user of Outsider. When I navigated to the custom template page of Outsider, I noticed that they specifically feature the ability to include Google Pay in the custom templates. I understand this to mean that when a scammer created a phishing page spoofing whatever brand or company they wanted, they could input the below functionality to steal a victim's Google Pay credentials. I understand that if the victim were to choose to pay with Google Pay, it would function similarly.

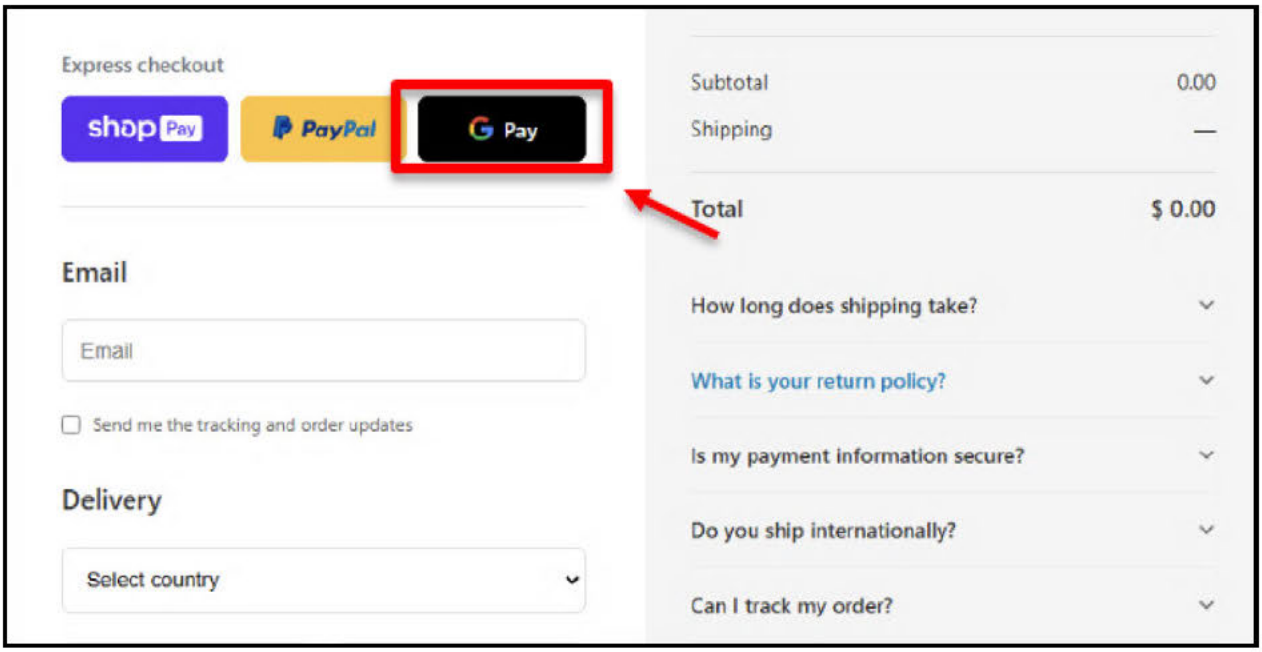


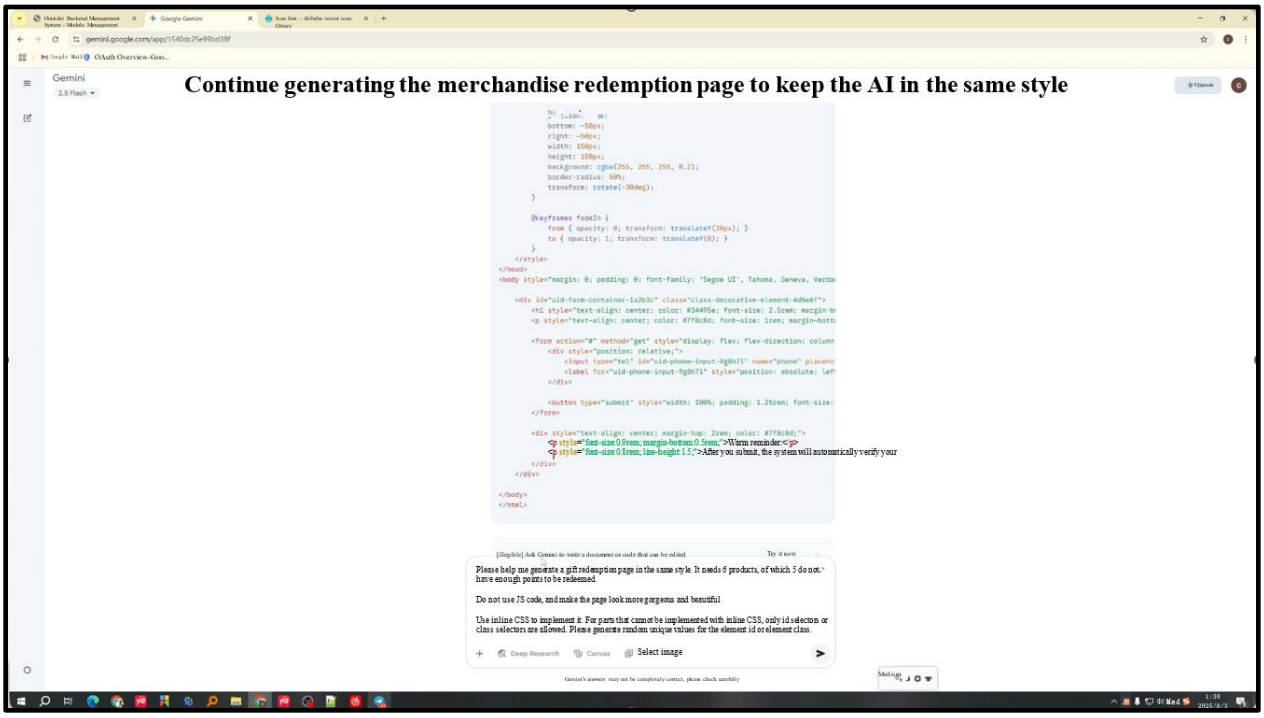
Figure 27. Screenshot from Outsider "custom template" page of software (emphasis added).

56. Outsider also supports the creation of custom phishing campaigns, in which users can use AI platforms (@sinkinto01 recommends Google Gemini and ChatGPT) to write customized code to create phishing websites spoofing any company they choose.

57. A tutorial video, posted August 2, 2025, specifically explains how Outsider customers can use Google Gemini in order to create custom website shells that Outsider can turn into phishing sites. In the video, a user appears to be using Outsider's "custom template" feature to modify a phishing page spoofing the Los Angeles Department of Transportation Parking Violations Bureau. The video shows the Outsider user navigating to the "gemini.google[.]com/app" URL which shows a webpage with "Gemini 2.5 Flash," a large language model. It is clear that the user is logged in to the Gemini account as the page reads, "Hello, Chen!" which I understand to refer to "chenlun." The user then enters the following prompt in the entry field: "Please help me generate a New York ticket and use inline CSS to implement it

. . . ."[32] I understand that CSS stands for cascading style sheets, a visual presentation language often used on the Web, and that "inline CSS" refers to a specific way of using CSS to visually design a webpage using HTML code.

58. Gemini returns a section of HTML code that appears to conform to the user's request. The user then enters a new prompt, requesting that Gemini create a gift redemption page. The user specifies that "it needs 6 products, of which 5 do not have enough points to be redeemed." It includes specific requests about the type of code and also instructs Gemini to "make the page look more gorgeous and beautiful." Once again, the user submits the prompt and Gemini creates HTML code that appears to conform to the user's request while leaving placeholders for images.



[32] *See* screenshot from tutorial video showing use of Google Gemini to create custom HTML code for use in Outsider platform, Telegram (Aug. 2, 2025), https://t[.]me/sinkintopd (translated), Ex. 1 at 16, 20. I note that despite the template being focused on LA, the Gemini prompt discusses New York. I think that the video creator was simply trying to show off examples of the types of prompts that people using the software might input. They never went so far as to paste any New York-focused code into the platform during the video.

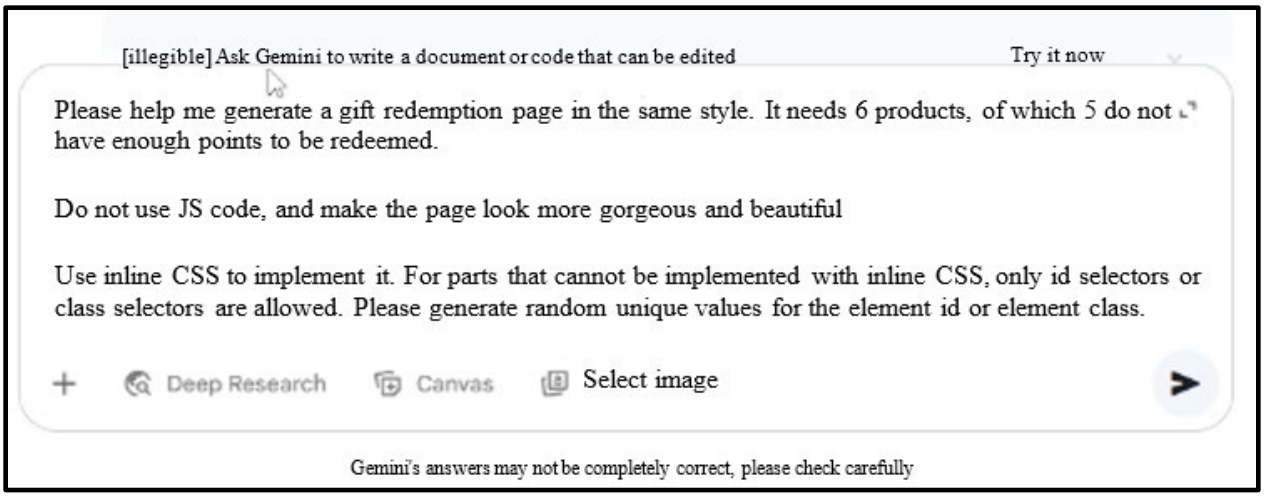


Figure 28. Screenshot from tutorial video showing the use of Google Gemini to create custom HTML code for use in Outsider platform, Telegram (Aug. 2, 2025), https://t[.]me/sinkintopd (translated); zoomed in version of prompt.[33]

59. The user copies the HTML code from the Gemini window and returns to the Outsider phishing platform, where they subsequently paste the code into the editor window. In the center, the preview of the phishing page template changes to display the instructions found in the new Gemini-created HTML code.

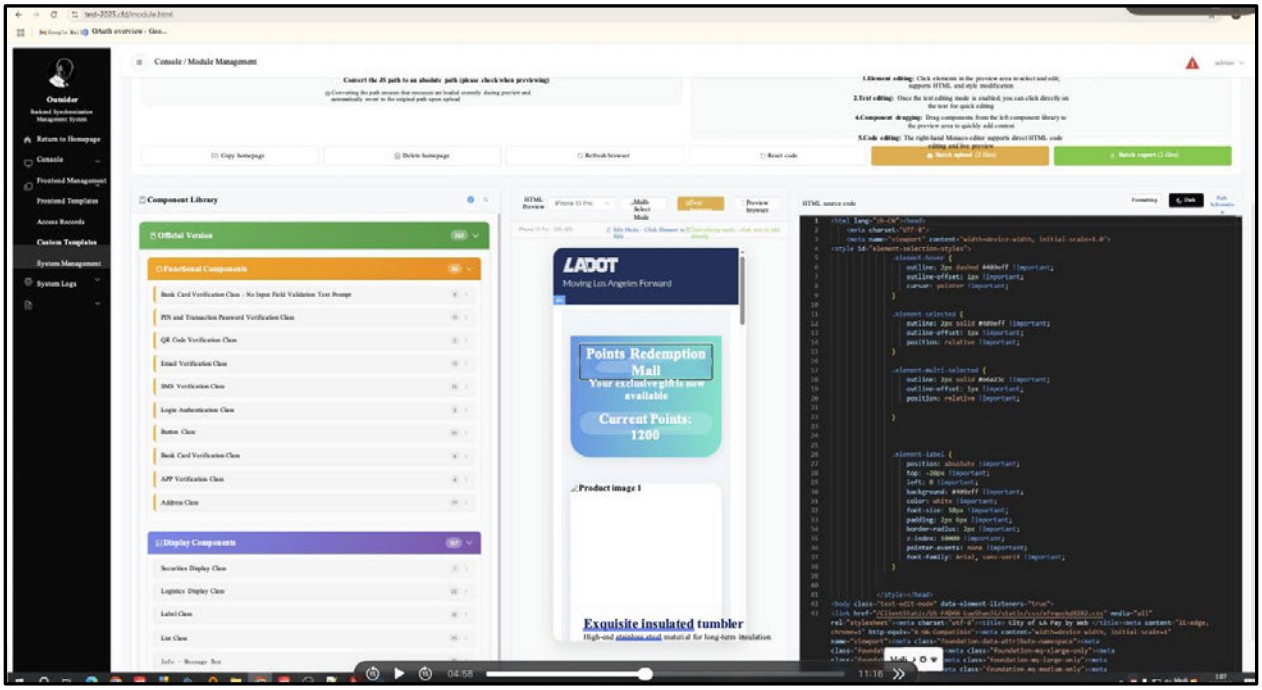
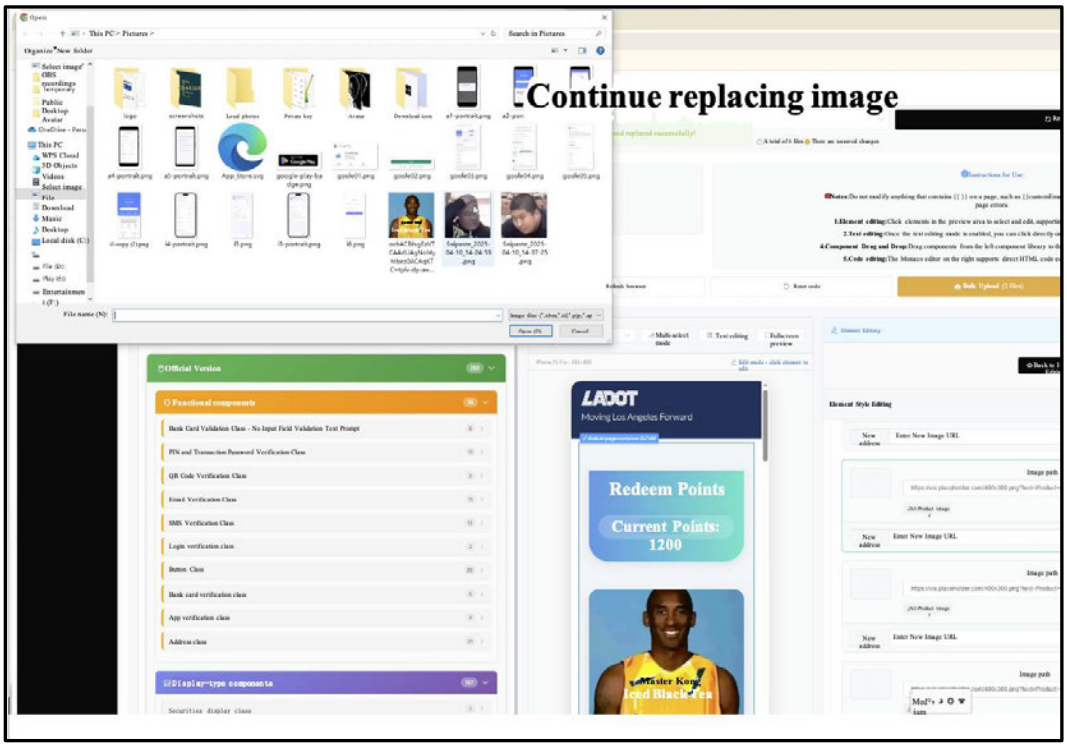


Figure 29. Screenshot from tutorial video showing Gemini code after being pasted into Outsider

[33] Ex. 1 at 20.

custom template part of platform showing gift redemption page, Telegram (Aug. 2, 2025), https://t[.]me/sinkintopd (translated).[34]

60. The tutorial video then showcases other features of the custom template. At one point, the user displays how to manually insert separately-downloaded images into the phishing pages. At that point in the video we can see the user's computer screen with a Windows Explorer folder containing several images of known logos and images belonging to well-known brands. For example, file names were visible including: "google-play-badge.png" depicting the Google Play symbol visible on pages that indicate the presence of an app in the Google Play store, and files named goole01.png through goole05.png [sic] which appear to be screenshots of a particular app. This indicates that the creator of the tutorial video (@sinkinto01) likely used these Google logos in this or other phishing templates.



[34] Ex. 1 at 24.

Figure 30. Screenshot from custom template tutorial video where threat actor has saved Google logos, Telegram (Aug. 2, 2025), https://t[.]me/sinkintopd (translated); zoomed in Google logos.[35]

61. Although the tutorial video focused on the SMS scams, I understand that the e-commerce phishing pages can be modified using Gemini-created code as well.

V. Review of the Outsider Software

62. In order to research the Outsider software, I purchased a license for the software and installed it in a controlled network environment. This controlled network environment allowed me to use Outsider as if I were an actual scammer by downloading templates, configuring settings, and setting up phishing domains. However, I blocked access to the phishing websites I created by any computer outside of my controlled network environment. In other words, I could create phishing websites that were accessible only by my NAXO computers. This type of analysis was necessary in order to fully analyze the software and to identify infrastructure supporting it and phishing websites created with it. My research of @sinkinto01 led me to the Telegram channel @OutsiderCodeBot which was advertised as a "bot" for the sale of Outsider licenses. On January 13, 2026, I navigated to the bot, and a "Menu" button brought me to a 10-button option menu.

[35] Ex. 1 at 28.

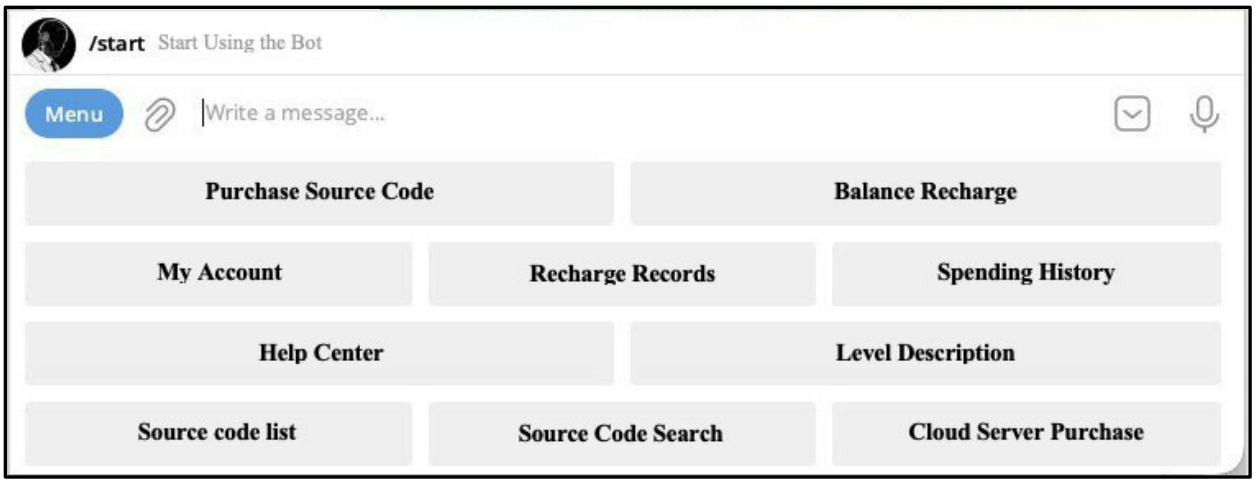


Figure 31. Screenshot of @OutsiderCodeBot menu page (translated).[36]

63. The top left button in the menu was labeled, "Purchase Source Code." Clicking this link displayed a message in the chat screen showing my membership level, any discounts available, and my account balance. The last line of the message read, "available products," followed by three buttons. The first button was labeled, "SMS + E-commerce Synchronization System Weekly Card" with a price of 88 USDT. The two other buttons allowed me to choose longer license terms (monthly for 200 USDT and annual for 1688 USDT).

[36] Ex. 1 at 32.

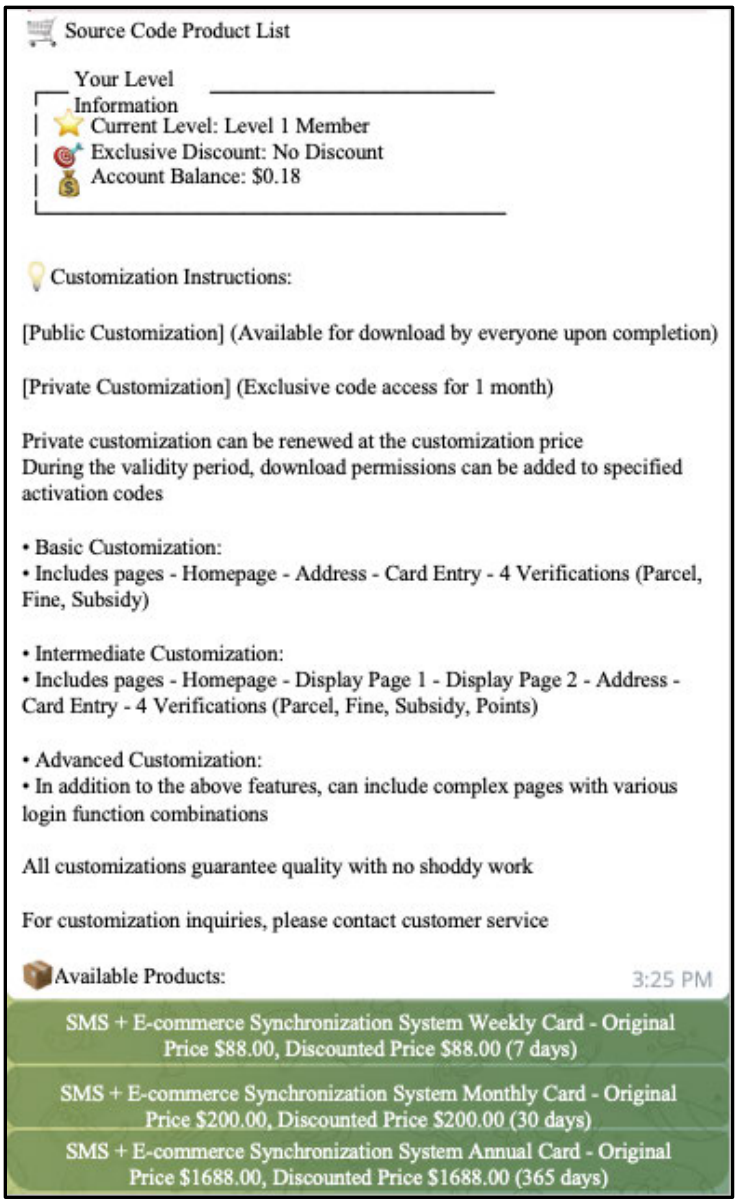
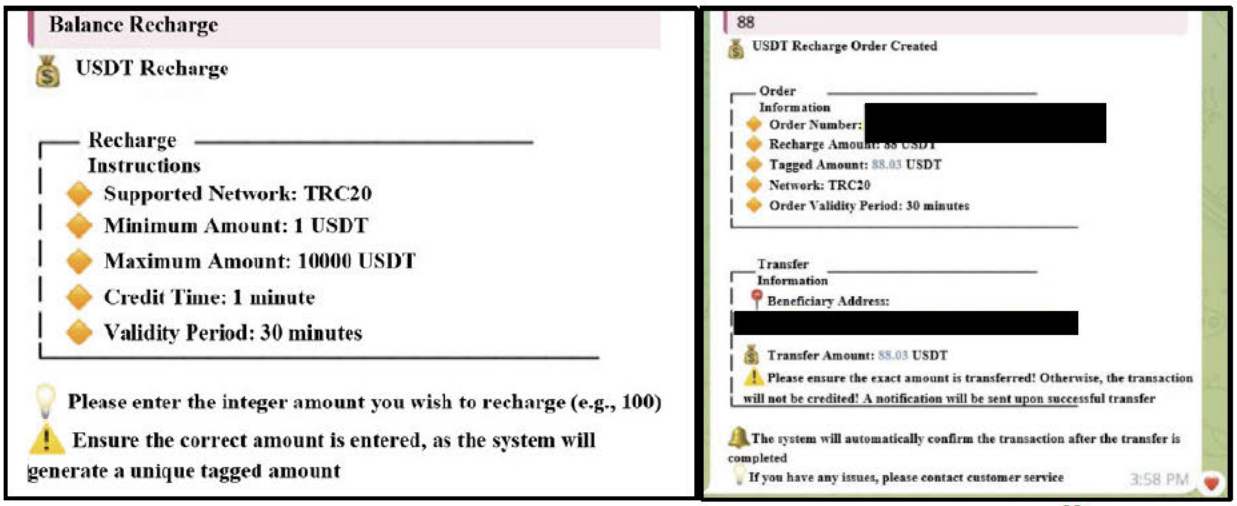


Figure 32. Screenshot of @OutsiderCodeBot source code purchase page (translated).[37]

64. I chose the weekly option which displayed a pop-up message stating that my balance was insufficient and that 88 USDT was required. I returned to the main menu and selected the button reading, "balance recharge." A message displayed in the chat window detailed instructions for how to deposit USDT and then instructed me to enter the amount of USDT to be

[37] Ex. 1 at 36.

deposited. I transferred USDT from a crypto asset wallet controlled by NAXO to the wallet displayed in the instructions sent by the bot.



Figures 33, 34. Screenshots of @OutsiderCodeBot deposit instructions (translated).[38]

65. Less than a minute after paying for the license with USDT sent to the cryptocurrency address, a message displayed in the chat window stating that the funds had been received. It included an order number along with a confirmation that my account had been credited with the correct amount of USDT. I then returned to the @OutsiderCodeBot main menu and selected the "Purchase Source Code" option. I clicked the one-week authorization code which displayed a message stating that the product I had selected was the SMS and E-commerce Synchronization System Weekly Card and that it was valid for seven days after the software had been activated. The message also stated that the weekly pass includes five template downloads (any of which can be used to create multiple phishing pages).[39] After confirming my purchase, I received an activation code. The message also included [redacted]

[38] Ex. 1 at 40, 44.

[39] I renewed the weekly license on January 22, 2026, using the same process described herein, which allowed me to download another five templates. On February 26, 2026, I activated a monthly license using the same process but paying $200.01 USDT (which unlocked additional features of the software, including more customization options). The monthly license allowed me to download an additional ten templates.

[redacted] Lastly, the message invited me to join a private chat group, the Outsiders Member Group, on Telegram.

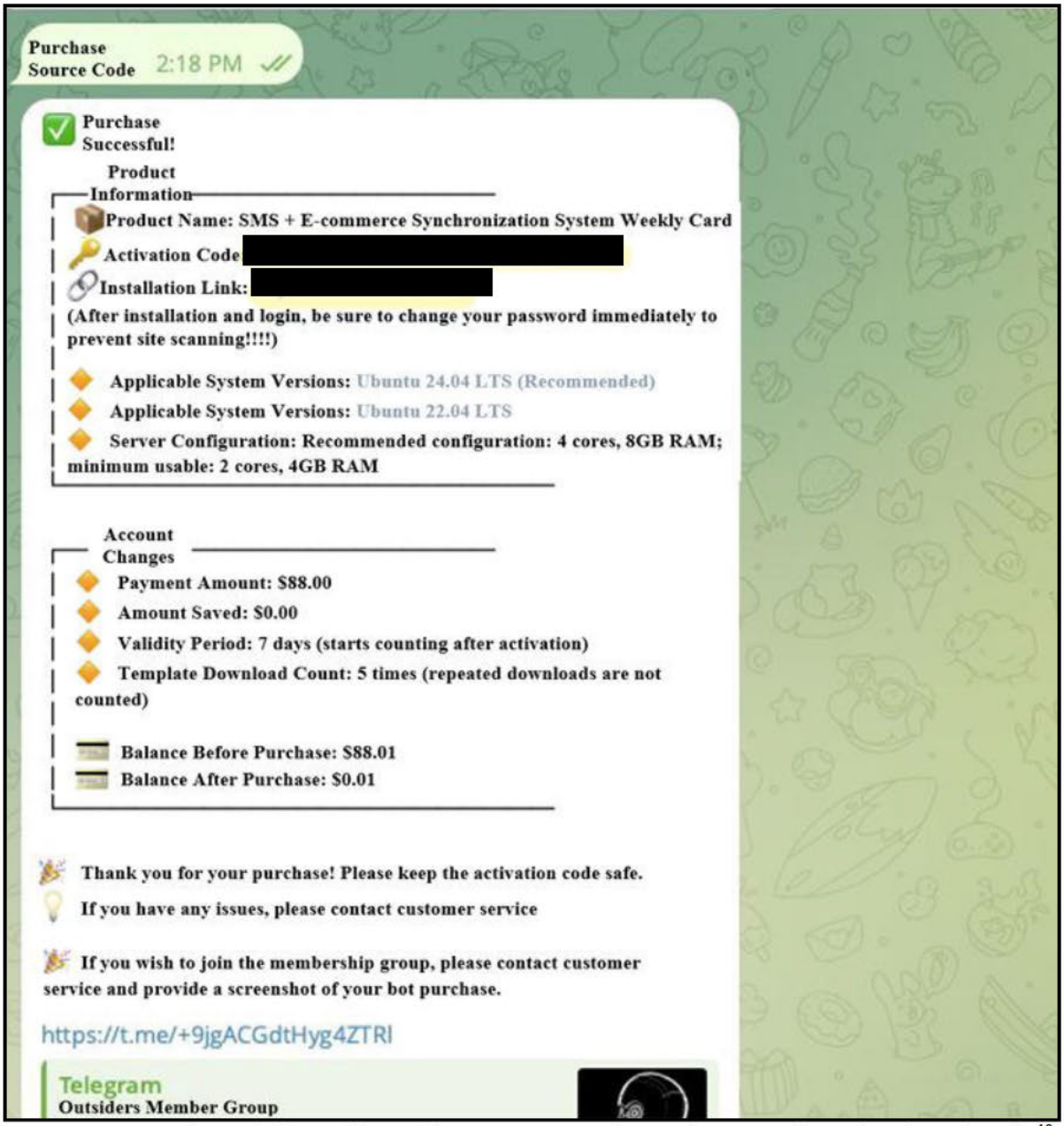


Figure 35. Screenshot of @OutsiderCodeBot source code purchase confirmation (translated).[40]

[40] Ex. 1 at 48.

66. Using open-source information, I identified that the domain [redacted] was registered on July 26, 2025, to an anonymous individual or entity using the "Super Privacy Service" provided by Dynadot, LLC, an internet service provider located in San Mateo, California. [redacted] both of which are registered to Cloudflare, an internet service provider located in San Francisco, California. This indicates to me that Outsider's providers take steps to route the internet traffic that facilitates the download of the software through intermediate service providers in the United States in order to provide increased anonymity and the ability to evade detection by anti-phishing services and law enforcement.

67. Using the Google Chrome browser, I visited the [redacted] website. The site is flagged as "dangerous." I acknowledged the warning and continued on to the [redacted] website.

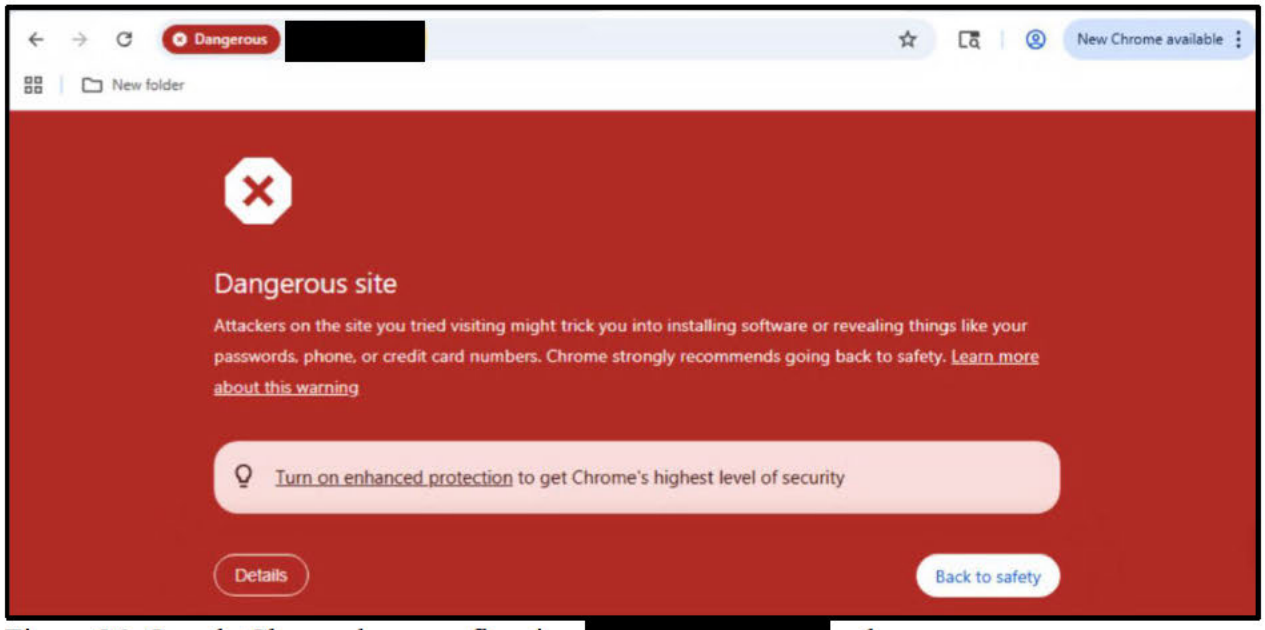


Figure 36. Google Chrome browser flagging [redacted] s dangerous.

68. I recalled reading a post from September 10, 2025, in which Telegram user @sinkinto01 posted an update to the channel when Google flagged the [redacted] website as unsafe.

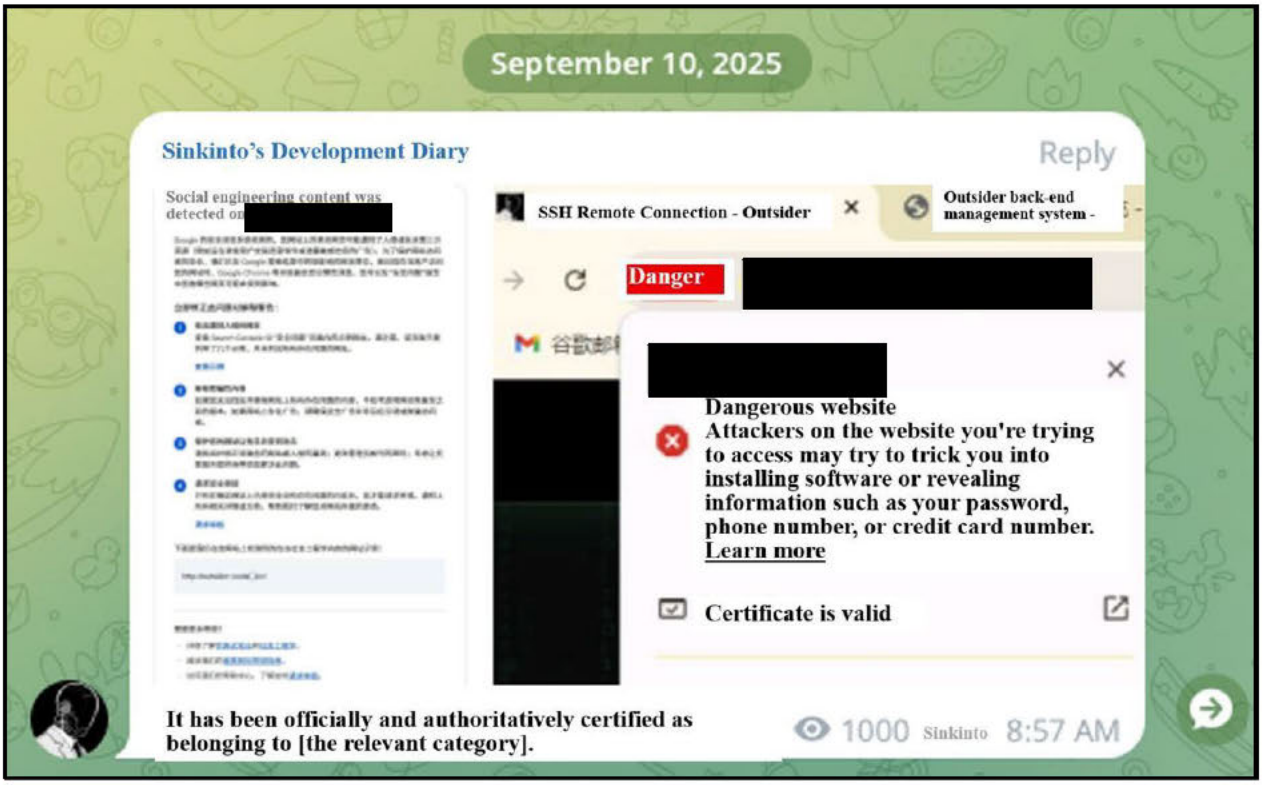


Figure 37. @sinkinto01, Post indicating that Google Chrome had flagged the website as malicious, Telegram (Sept. 10, 2025), t[.]me/sinkintopd (translated).[41]

69. The [redacted] website natively displays in Chinese. At the top of the page are four options: "Homepage," "SSH terminal," "One-Click Deployment," and "Learn More," not all of which were functional. After navigating to the home page, I was taken to a webpage that describes Outsider as "a revolutionary synchronization management platform that combines high customization to help your team achieve a leap in sales performance." The page apparently highlighted various features of Outsider including "[c]ustom synchronization pages, cloud backup,

[41] Ex. 1 at 52.

and data security."[42] It also listed statistics such as "156+ Enterprise Users" and "89.2% Sales Conversion Rate Improvement."[43] The bottom of the page reads, "© 2024 Outsider. All rights reserved."[44]

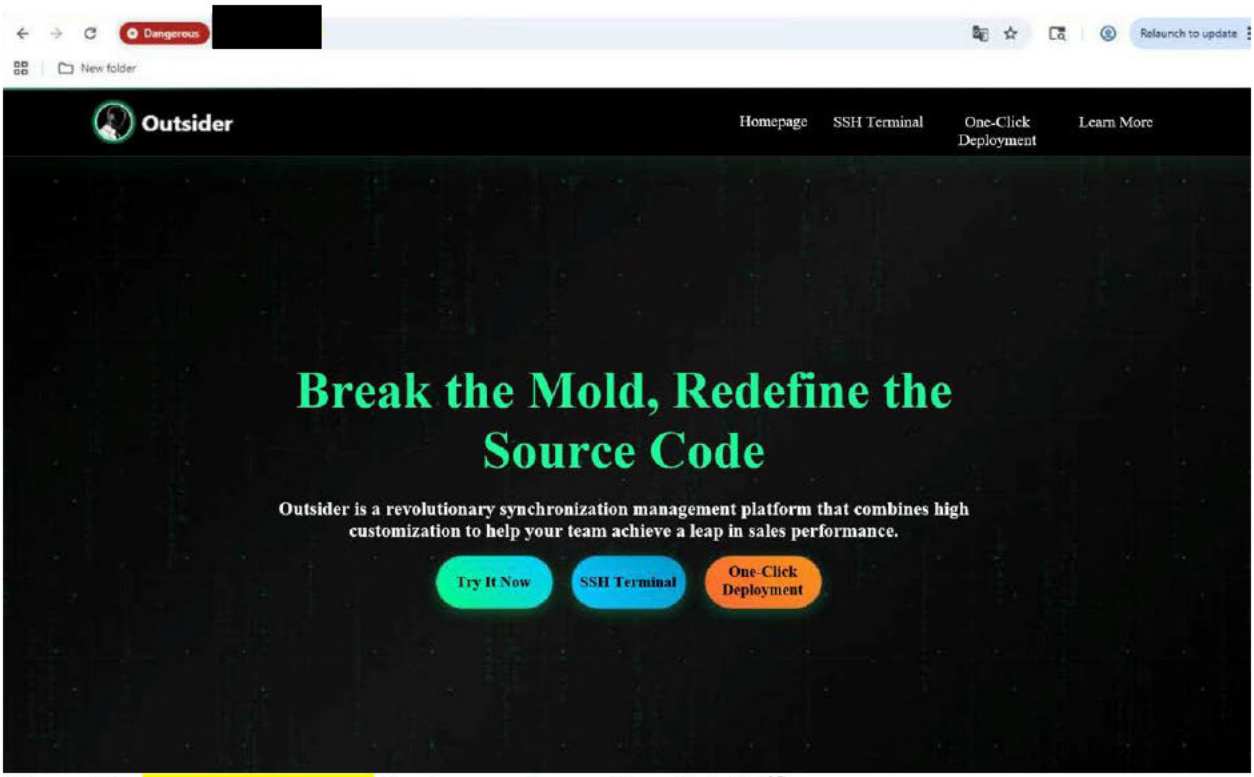


Figure 38. [redacted] deployment page (translated).[45]

70. I then navigated to the "One-Click Deployment" link at the top of the page. The page prompted me to input my "Server Address," "Port Number," "Password," and "Authorization Code." I noticed a button prompting me to connect to an SSH terminal.[46] Based on my experience and from information obtained in the Outsider Telegram channels, I know that the information being requested in these fields refers to the fact that users must connect Outsider to a server on

[42] Ex. 1 at 56.
[43] Ex. 1 at 60.
[44] Ex. 1 at 64.
[45] Ex. 1 at 68.
[46] Ex. 1 at 72.

which the Outsider source code will be deployed. In order to create phishing pages using Outsider, scammers need to have a server from which to host both the software and the phishing pages.[47]

71. In preparation for downloading the software, I created a virtual private server ("VPS") at a public internet hosting provider for the purposes of installing and analyzing the Outsider software and hosting test phishing pages. A VPS is an isolated, virtualized computer server that allows multiple other virtualized servers to share the same underlying physical computer hardware without interfering with each other. In my experience, the developers and operators of phishing kits typically install and operate phishing software using a VPS.

72. I created an exact "bit-for-bit" copy (sometimes called a "forensic image") of the VPS's virtual hard disk prior to installing the Outsider software, and then I compared it to a second copy created after installing the Outsider software to identify any changes made during installation. To prevent other users and computers on the internet from inadvertently accessing the Outsider server and example phishing websites I created while conducting the analysis described in my report, the VPS operating the Outsider software and phishing websites was isolated from public internet traffic and accessible only by certain members of the NAXO team from a separate VPS created for this analysis.

73. On the Outsider website, I entered my server IP address, port number, username, and password as well as the authorization code generated by the @OutsiderCodeBot. I then clicked the "connect to SSH terminal" button. A box on the right side of the page began displaying the Outsider software installation information, including providing real-time updates, such as that the process was beginning, the time zone was set to Asia/Shanghai, and the file size was approximately 70.3 megabytes. The Outsider installation deployment continued for about two minutes. One

[47] A server is a computer that provides data or services to other computers on a network.

interesting log entry indicated that the network connection was checked using Google DNS. I understand that Outsider likely uses Google's domain name server records to query whether domain names are associated with IP addresses downloading the software. The installation process concluded with a URL address to access the installed software on the server along with a username and password. As soon as the installation of Outsider concluded, the VPS was locked down to any other traffic.

74. Using the URL address provided during the installation process ([NAXO Server IP address]/7vuph/login[.]html), I accessed the login page of the Outsider software. A message at the top of the page read, "Outsider Backend Management System" with a sub-headline of "Efficient Development, Detailed Templates, Intelligent Backend, Real-time Synchronization." It prompted me to enter a username and password to log in. After entering the information received during the installation process, I was redirected to a new URL address and asked to enter my authorization code. I did so and clicked a button prompting me to activate the account.

Figure 39. Outsider login page (translated).[48]

75. At this point, I was given access to the software. On the left side of the page, I noticed an avatar which was the same avatar from the @OutsiderCodeBot, @sinkintojl, and

[48] Ex. 1 at 76.

@sinkintopd Telegram channels. I noted that the page included an expiration date in a week, tracking when my license would expire. I navigated to the home page, a dashboard containing statistics in six different widgets titled "today's visits," "today's card entries," "today's user count," "number of cards bound," "today's login count," and "data with captcha." I understand these widgets to keep updated statistics on phishing pages deployed by the user of the Outsider software like the number of credit cards collected each day. Below the widgets is a world map which is used to display the location of visitors to the phishing pages deployed by the Outsider software.

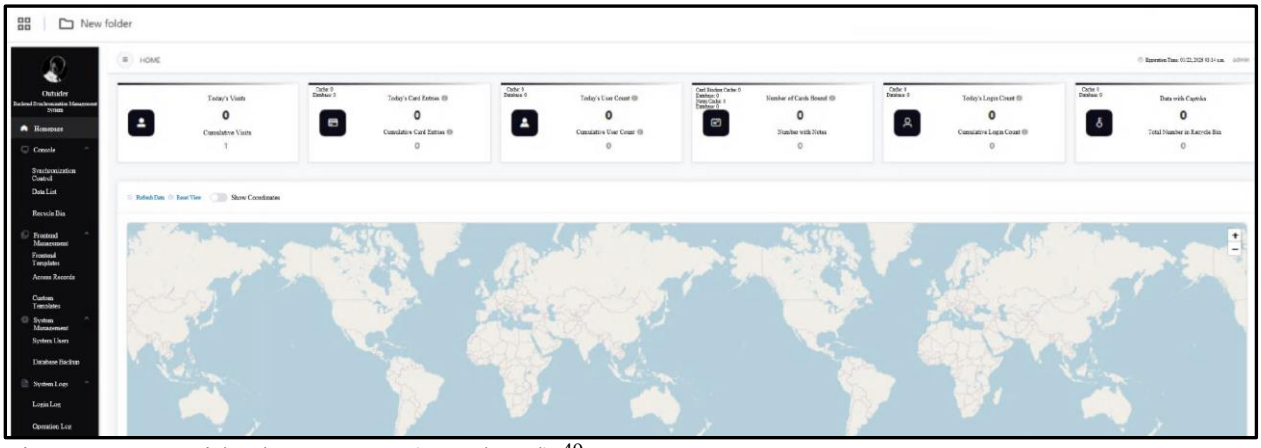


Figure 40. Outsider home page (translated).[49]

76. I then navigated to the "frontend" management menu item in the left column which I believed would allow me to create the phishing pages. I was asked to choose between three sub-menu options: "frontend templates," "access records," and "custom templates."[50] I selected the "frontend templates" sub-menu and navigated to a list of phishing page templates for download, categorized using five columns, including template, official website, region, preview template, and description.

[49] Ex. 1 at 80.

[50] The "front end" in tech parlance refers to the user-facing features of a product or tool. For example, the "Send" button in Gmail is a part of Gmail's "front end," while the code that translates a click of that button into the transmission of a message is a part of Gmail's "back end."

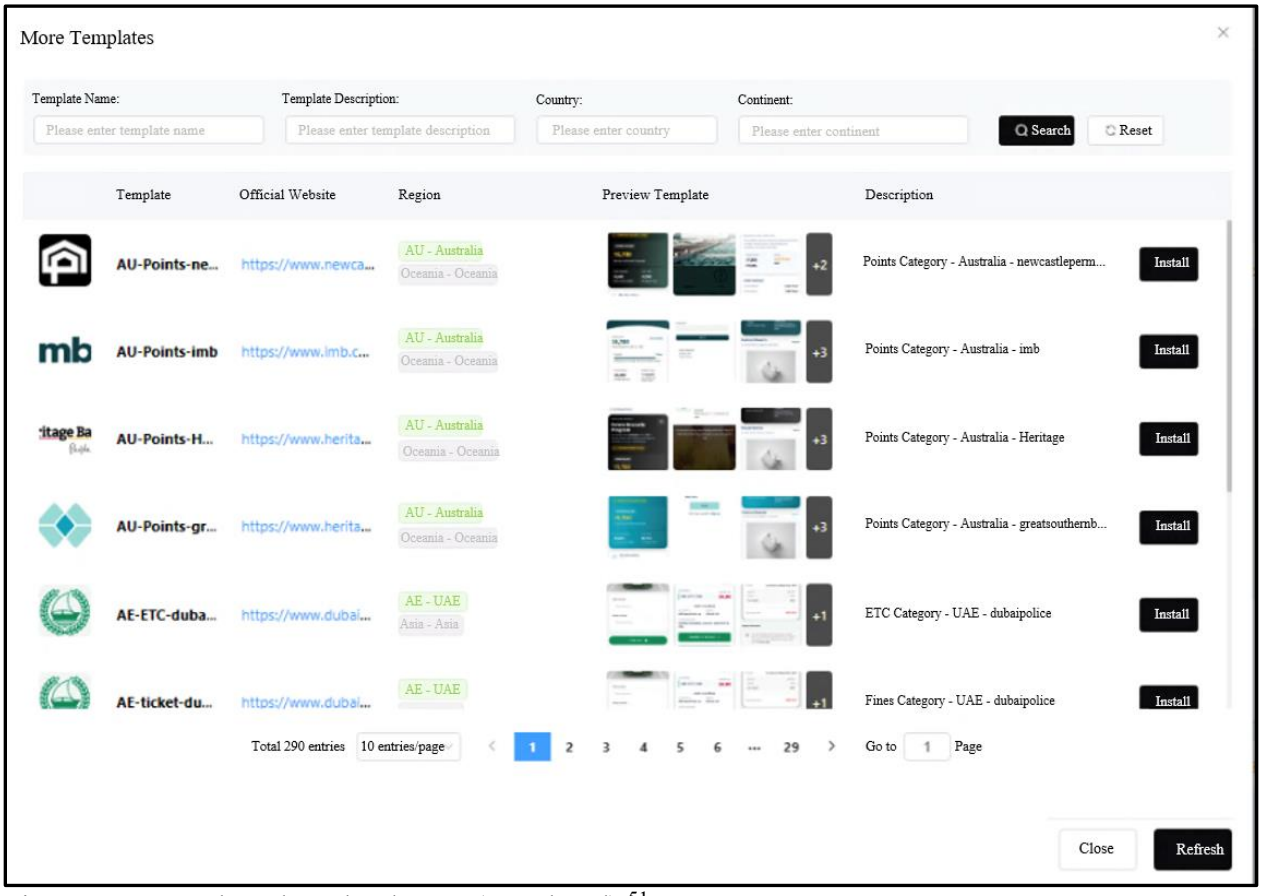
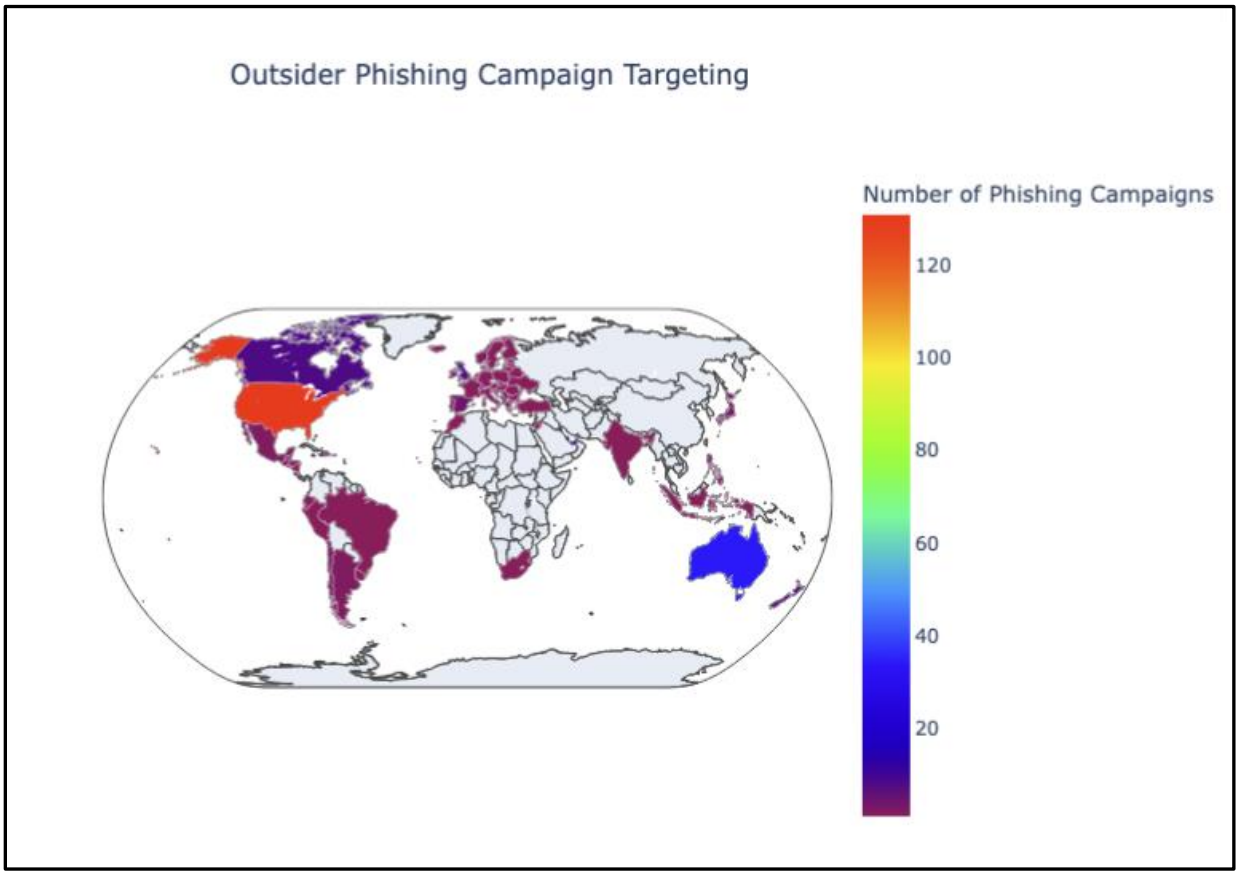


Figure 41. Template download page (translated).[51]

77. NAXO team members reviewed all of the template entries on the list. The templates spoof over 290 distinct entities. Of those, 131 were categorized by Outsider as targeting the United States—the largest number targeting any single country, as reflected in the graphic below. Of the phishing templates categorized in the software as targeting U.S. victims, 102 were government websites (typically supporting the parking ticket scams), ten were financial institution websites, nine were toll collection websites, three were shipping company websites (including USPS), three were telecommunications company websites, and three were online retail websites. Four of the templates spoofed nyc.gov, ny.gov, and e-zpassny.com, specifically targeting victims in New

[51] Ex. 1 at 84.

York. The software included templates targeting over 50 other countries. At least 14 of the templates contain Google logos.[52]



78. Some of the templates listed are the e-commerce websites and the CMS discussed previously, which do not specifically target a certain country, but I have included them in the "online retail" category above. I understand that these templates could be downloaded to create e-commerce scams.

79. Using my first weekly license, I installed five "US" templates. I later installed an additional 20 templates. After clicking "install" and then closing the available templates pop-up window, the main "frontend templates" page was now populated with the US templates I had

[52] I note that as I was only able to download a relatively small number of templates, and I think it is likely that additional templates contain Google logos.

installed from the previous step. The templates include a link to the legitimate website that the phishing page is attempting to emulate, one or more thumbnail photos previewing the site, a status update to indicate whether a page is currently active, and "installation time" that displays the date and time a template was installed on the Outsider platform.

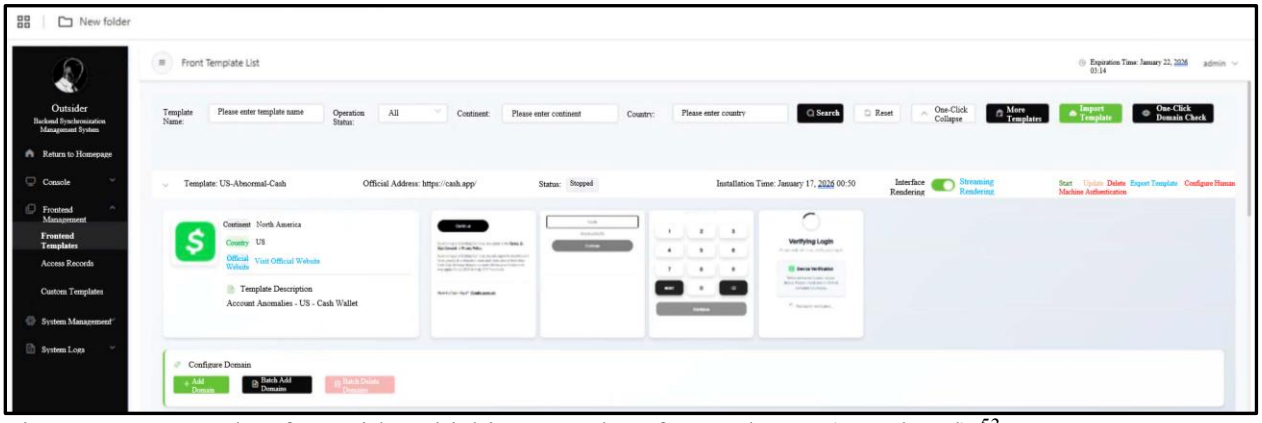


Figure 42. Example of Outsider phishing template for CashApp (translated).[53]

80. Below each template entry is a bar containing three buttons: "add domains," "batch add domains," and "batch delete domains." When attempting to add a domain, I was brought to a page that prompted me to input a domain name ("please enter the domain e.g.: shop.example.com"). This is the field where the Outsider platform user would enter the phishing domain they had previously registered with a domain registration service, linking the phishing page created in Outsider with a website accessible by victims.

81. This part of Outsider also has a feature allowing users to add a separate suffix to inputted phishing domains. This allows for multiple phishing pages to be used across a single domain by adding a unique suffix for each one (e.g., phishingpage.com; phishingpage.com/1). The platform also allows users to request, configure, or upload a certificate. I understand this to refer

[53] Ex. 1 at 88.

to an SSL certificate to allow for secure (https) connections between the phishing page and the phishing victim, which helps to make the site look more legitimate.[54]

82. In preparation for deploying test phishing pages that could only be accessed on my internal local network, I edited the Microsoft Windows "hosts" file found in the "etc" directory within the operating system. I created domains that were iterations of "phishtestlocalX.com" where "X" was a numeral ranging between one and nine.

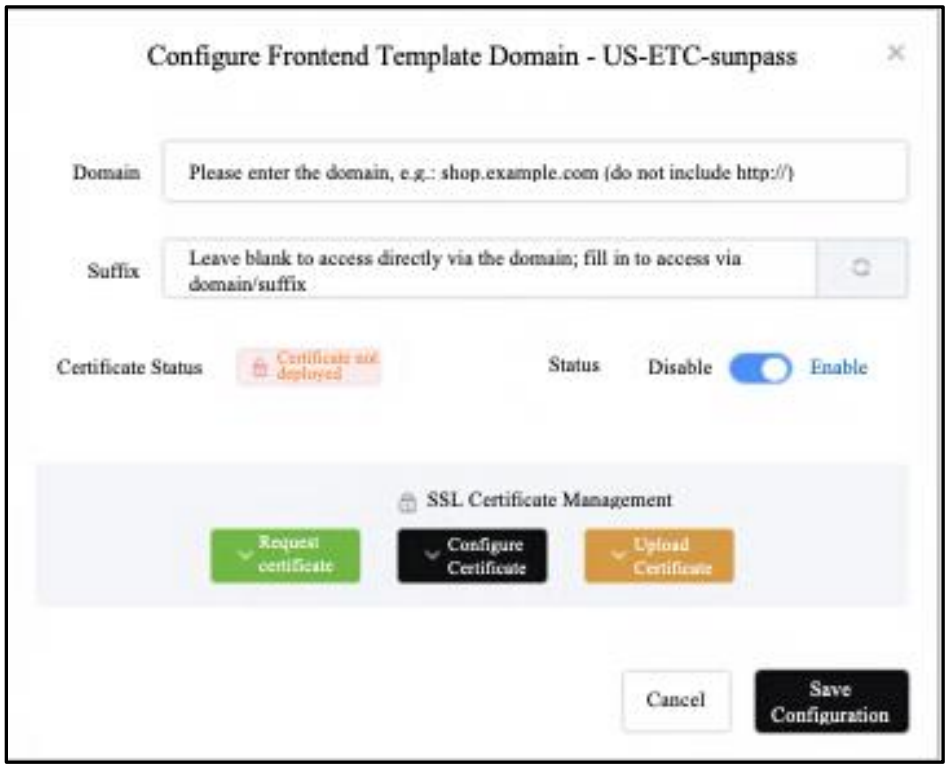


Figure 43. Screenshot depicting addition of domains to a phishing template (translated).[55]

83. I then used the "add domain" feature to assign my "phishtestlocal" domains to the templates I had downloaded. I used the Chrome browser to navigate to the "phishtestlocal3[.]com"

[54] SSL stands for secure sockets layer, a "protocol used for protecting private information during transmission via the internet." National Institute of Standards and Technology, Computer Security Resource Center Glossary, https://tinyurl.com/mr3cz3pc (last visited Apr. 5, 2026). SSL encrypts data sent over the SSL session. "[M]any web sites use the protocol to obtain confidential user information, such as credit card numbers." *Id.*

[55] Ex. 1 at 92.

domain that I had assigned to the "DC.gov Department of Motor Vehicles Failure to Pay a Ticket" phishing template. I enabled the developer tools option within the Chrome browser, which allows for the inspection of website resources and other information that occurs behind the scenes when a user visits a website. This allowed me to view the files used to build the phishing website as well as other attributes that are unique to the Outsider software.

84. I then activated the phishing website on my local network. The initial page I viewed had a DC.gov logo and "Mayor Muriel Bowser" appearing below. The page then appears to include information about a parking citation. I note that the phishing website also includes four social media logos including one for YouTube, which links to the actual DC DMV YouTube channel.

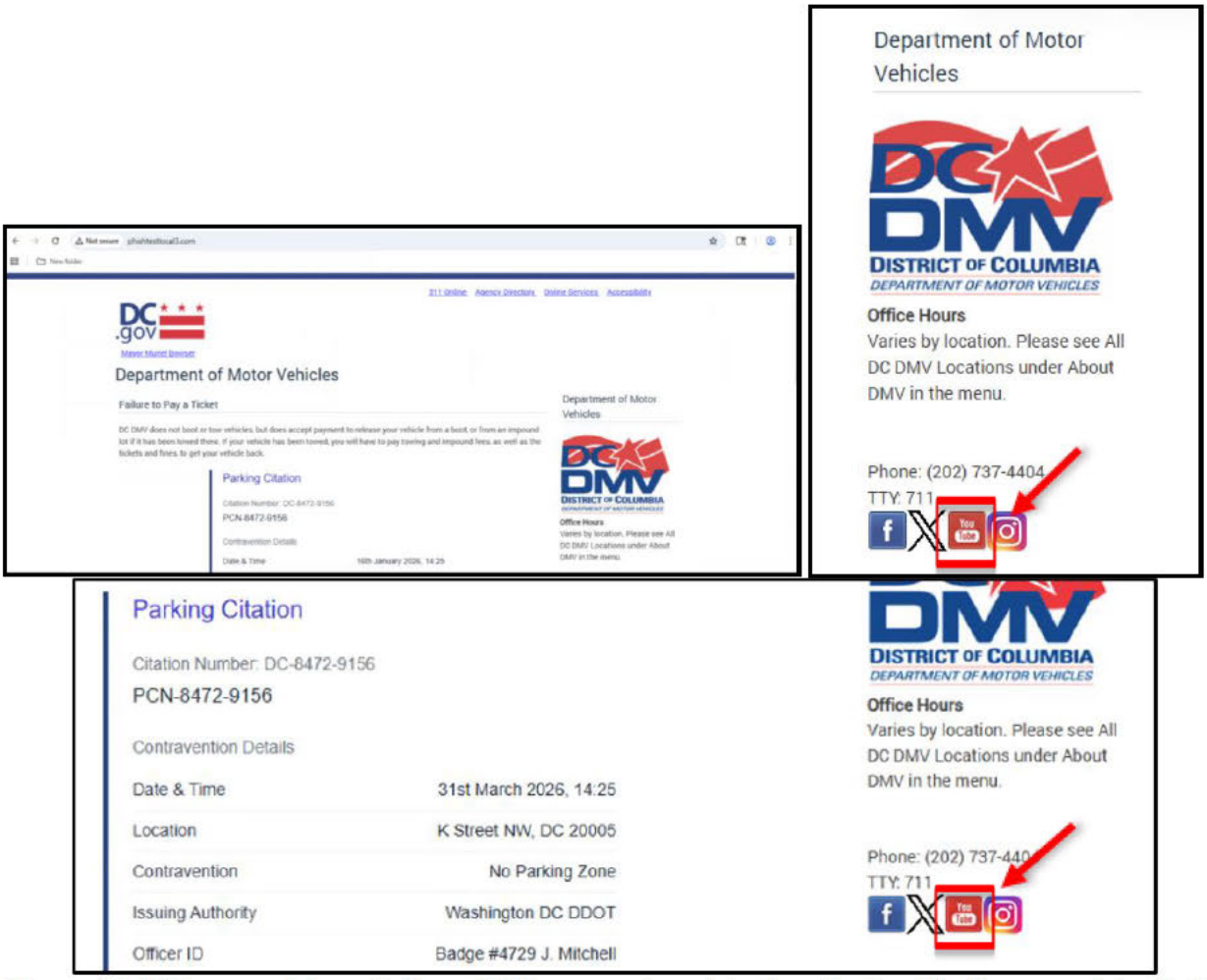


Figure 44. DC.gov parking citation phishing page template (emphasis added); zoomed in photos of DC DMV logo with YouTube icon.

85. I navigated to the next page, which prompted victims to input their personal information. As I navigated the "DC DMV" phishing page, the Developer Tools window in the Chrome browser displayed the files used to create the information that appears on the webpage, as well as network connection information relayed between the phishing page and the Outsider platform server. [redacted] I also noticed there was a WebSocket connection to Outsider, which provides a persistent connection for allowing real-time data transfer between the website and the server. This is what allows for the live collection of data as a victim types it into the phishing website.

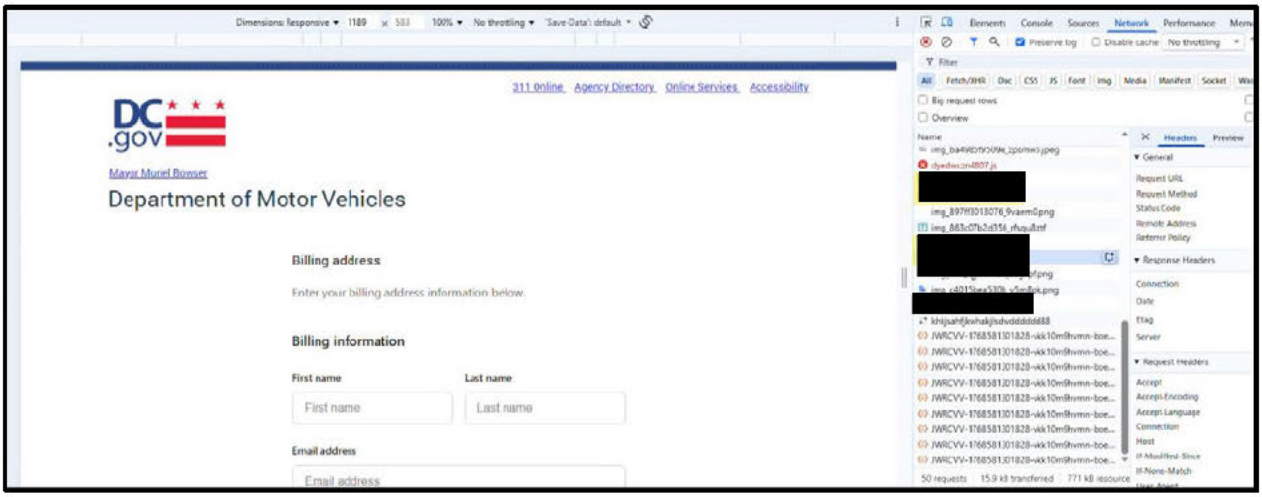
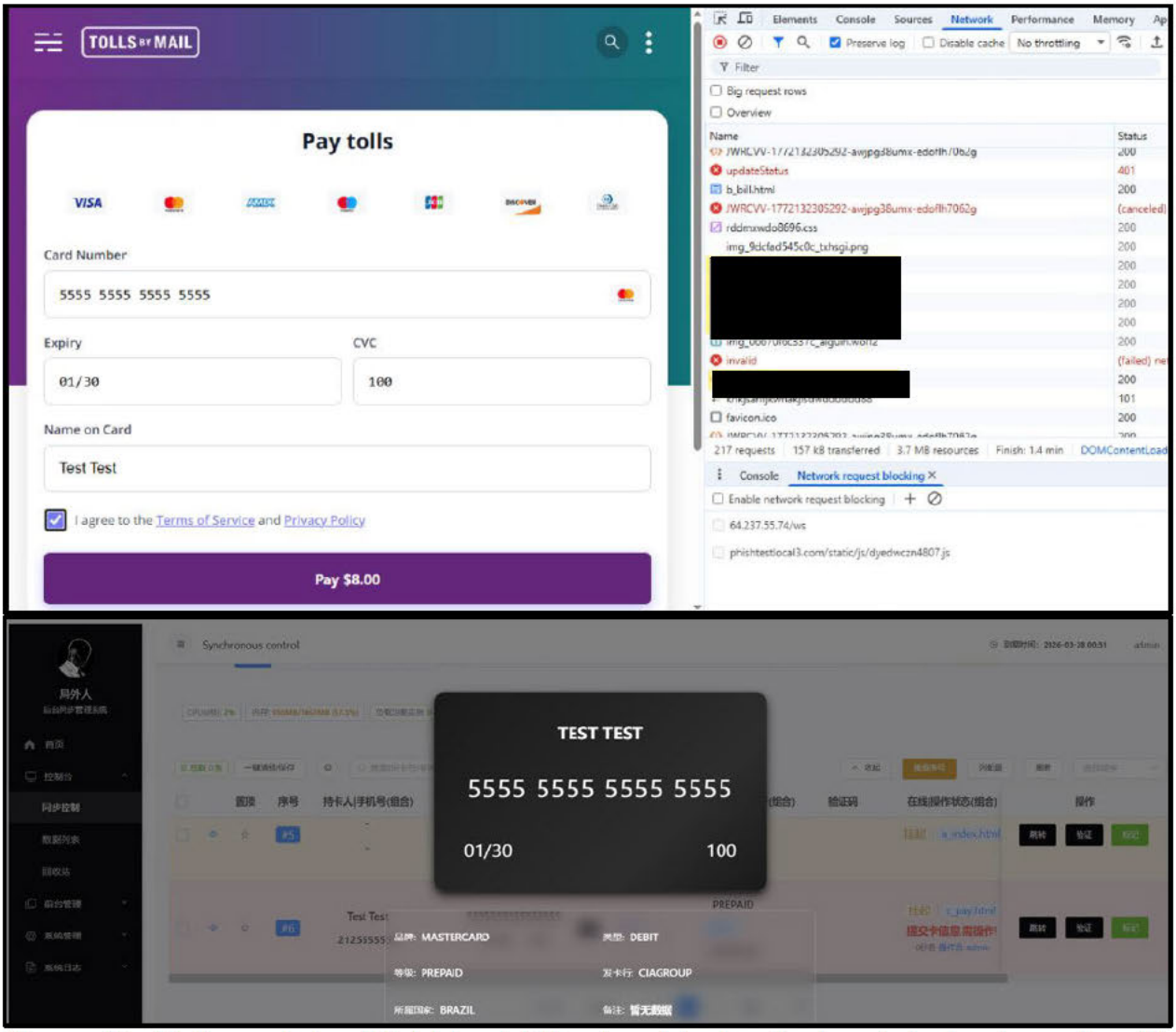


Figure 45. DC.gov phishing page viewed through Developer Tools.

86. Once I created the phishing page, I also tested how it works when a potential victim inputs their data. I noticed that as a potential victim types data into the phishing page, the information appears in real time inside the Outsider interface. In other words, even before a victim "submits" their information, the software automatically collects their keystrokes the moment information is typed into the website. In the example below, I typed card number 5555555555555555 into a phishing page spoofing New York EZ-Pass. As I typed it in, I viewed

it being entered into the Outsider software. The software also has a feature that puts the card information into the format of an actual credit card as it is typed in, depicted in the screenshot below.



Figures 46, 47. Screenshots of Outsider phishing template showing keystroke logging and credit card display.

87. I know that the reason the software depicts the card number on a digital credit card in this manner is that it allows the card to be added to mobile devices. Mobile wallets like Google Wallet use a mobile device's camera to take photos of credit cards to add to the wallets. I believe that these card images generated by the software allow scammers to load cell phones with stolen

credit card information, for use with tap-to-pay machines. I also noticed that Outsider automatically detects the credit card provider based on the numbers submitted by the victim.

Figure 48. Screenshot of Outsider phishing template showing credit card provider (translated).[56]

88. Additionally, once a victim inputs certain data, the software allows an option for the scammer operating the page to send them requests for additional information including: SMS verification, PIN verification, email verification, and app verification. I also noticed that the platform updated the home page statistics in real time with the numbers of visitors to the website and number of cards entered.

89. I used Outsider to create several SMS phishing websites that I tested on my internal network. I did not create any e-commerce websites as they required connecting to legitimate services in order to test those websites. My review of Outsider made clear, however, that e-commerce websites interacted with the platform similarly to SMS phishing websites, with all of the features discussed herein (e.g., the way the platform collects user data, the ability to create card images for use of tap-to-pay, etc.).

90. Under the "System Management" menu on the left-hand column of the Outsider platform is a link labeled "Database Backup." After I clicked on it, I was directed to a database backup management page which allows a user to export the Outsider platform database to a local storage destination, or to upload it to a cloud data storage service. The first option on the page is "Cloud Backup" with a button labeled "Connect Google Drive to enable cloud backup." I

[56] Ex. 1 at 96.

understand that Google offers cloud storage through Google Drive for those with Google accounts to store data.

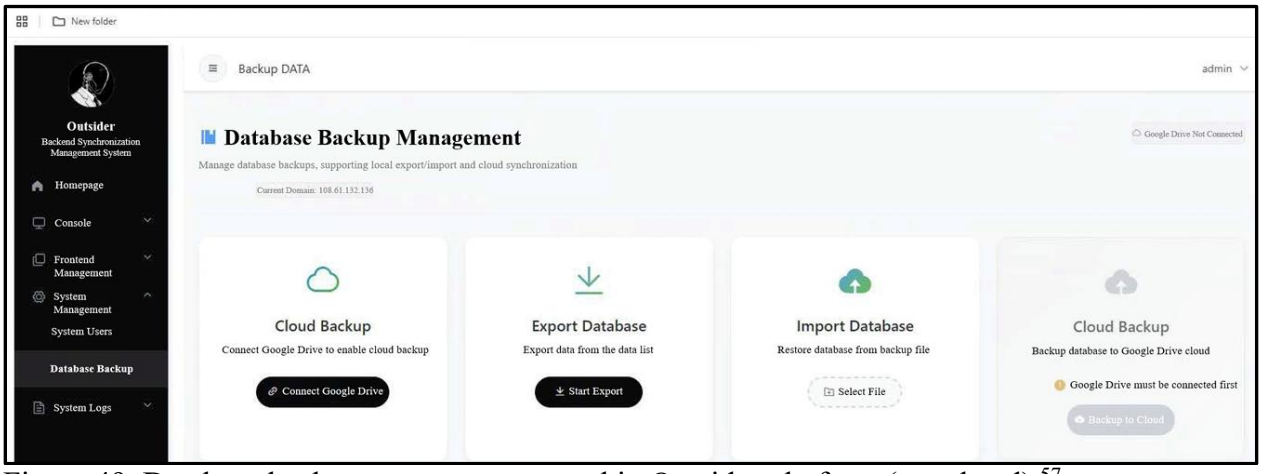


Figure 49. Database backup management panel in Outsider platform (translated).[57]

91. Clicking the "Connect Google Drive" button connects to a Google-operated webpage (accounts.google[.]com) containing a warning banner that states that access to Google Drive by the Outsider platform has been disabled.

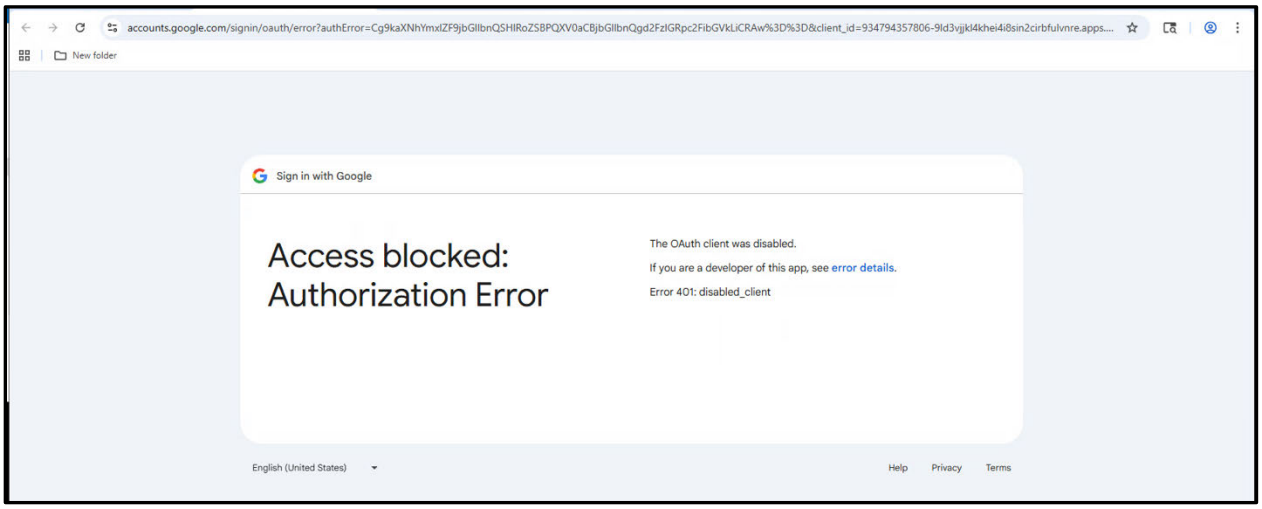


Figure 50. Screenshot of blocked link to Google Drive.

92. I reviewed an August 2, 2025, tutorial video posted by @sinkinto01 which showcased this feature when it was previously functional. In that video, the user clicked on the

[57] Ex. 1 at 100.

"Connect Google Drive" button on the cloud backup page in Outsider. This action opened a new web browser window using an "accounts.google[.]com" URL, displaying a Google account page with the Outsider logo, the name "chen lun," and the email address [redacted]." This indicated that the email address was logged into a Google account on the computer. A subsequent page was then displayed with the Outsider logo and the [redacted]" email address and a message that indicated that the Outsider Backup System was requesting access to the user's Google account.

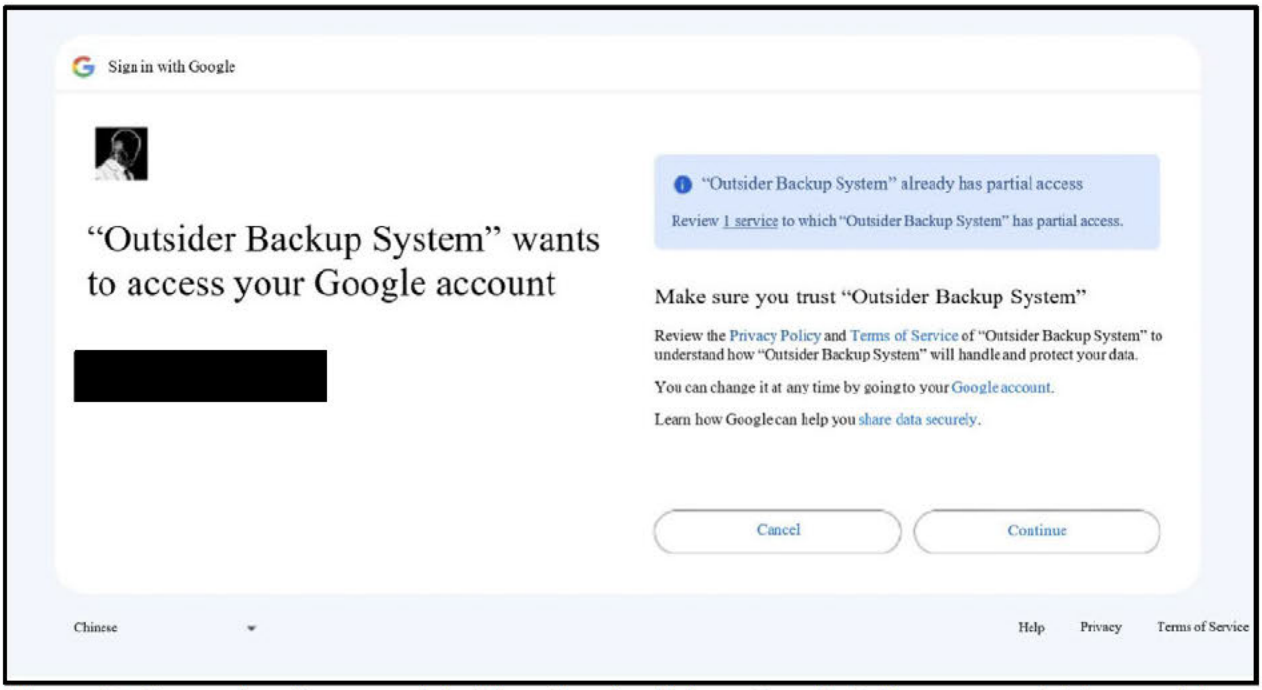


Figure 51. Screenshot from tutorial video showing link to Google Drive account, Telegram (Aug. 2, 2025), https://t[.]me/sinkintopd (translated).[58]

93. After approving access, the user was taken to the Outsider web page using the [redacted] [sic] URL with a message noting that the user should click the button to connect their Google Drive account.

[58] Ex. 1 at 104.

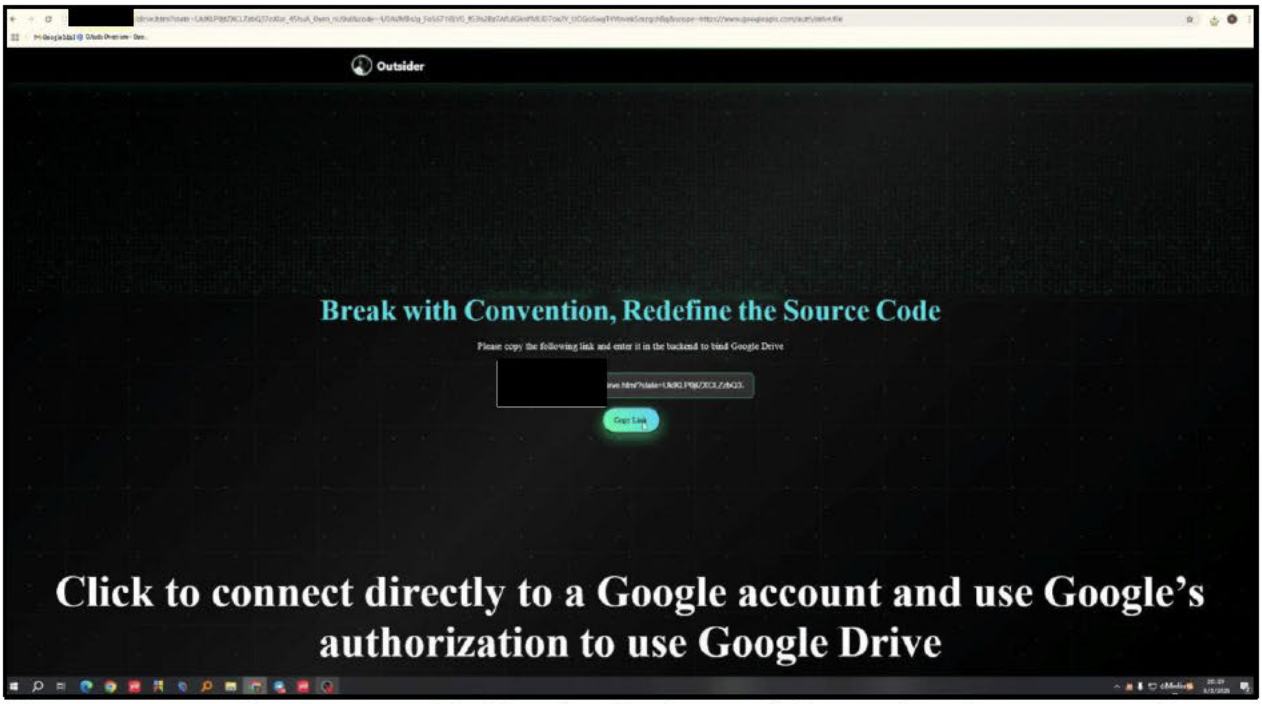


Figure 52. Screenshot from tutorial video showing how to link Google Drive account, Telegram (Aug. 2, 2025), https://t[.]me/sinkintopd (translated).[59]

94. After returning to the Outsider Platform, the option all the way to the right of the screen in Figure 49 now appeared activated since the Google Drive account had been linked. The user in the tutorial video pressed that button and navigated to "drive.google[.]com." The window displayed a single file named "admin_manual_backup_20250802_203010.sql." The user clicked on the database file, opening a preview window displaying text that includes "table structure for table 'cvvs'" and other data consistent with the collection of credit card and personal information. The Outsider platform had directly linked to Google Drive, a cloud storage platform, where the Outsider user could upload a file containing stolen credit card information.

95. After I determined that this feature was currently blocked by Google, I returned to the Outsider database backup page and used the export database function to export a copy of the database to my local downloads directory instead of to cloud storage. The process produced a

[59] Ex. 1 at 108.

Structured Query Language ("SQL") database file "admin_backup_20260124_000145.sql." I note that this is consistent with the naming convention of the file in the tutorial video. Based on these results, I am reasonably confident that, if access to Google Drive was not blocked, the Outsider software would have exported an Outsider SQL database file to a Google Drive account as depicted in the tutorial video.

96. Although the Google Drive functionality appears to be non-functional, I noticed that the @OutsiderCodeBot still displayed a message with information on how to purchase cloud-based servers for the Outsider software using an @OutsiderServerBot Telegram channel. I understand this service to allow users to request that @sinkinto01's bot purchase Google Cloud space that would allow for the storage of servers hosting phishing websites deployed with the Outsider software. While the Google Drive service used to backup stolen data was embedded in the Outsider platform, Google Cloud servers would be purchased separately to host Outsider as well as the phishing websites created with the software.

97. Using the @OutsiderServerBot channel, I navigated through the menu and clicked the account application button. The menu displayed options for four different cloud server providers, one of which is Google Cloud. I selected the Google Cloud option which displayed a pricing menu of $500 to $5,000 to add to my account. I selected the $500 option which then displayed a message instructing me to enter a Gmail address into the chat message window to bind my email address to my server purchase. The next message displayed instructions on making the $500 payment using USDT on the Tron network along with an address to send the funds. The message also indicated that this is a "unique" address, such that USDT payments would not be linked to the server purchase. I understand that a scammer would use this service in order to more

anonymously host their phishing websites and to avoid detection by Google security teams that attempt to prevent fraud on their platform.

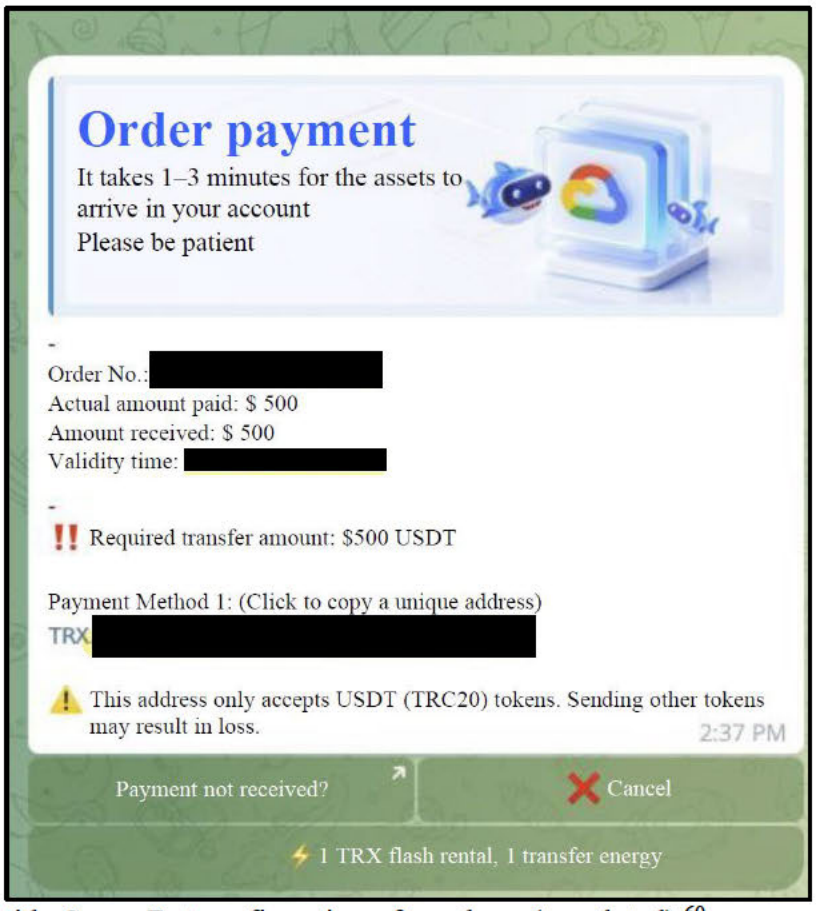


Figure 53. @OutsiderServerBot confirmation of purchase (translated).[60]

98. After a few minutes, the @OutsiderServerBot Telegram window displayed a confirmation that my payment was received, along with a link to my Google Cloud console account (https://console.cloud.google.com/welcome?project=[redacted] the associated email address, and a project ID [redacted]. I copied the link and used the Google Chrome browser to access the provided Google console account. I was required to authenticate my account using my Gmail email address and password, which opened up a Google Cloud welcome screen and a Terms of Service agreement. The information included a message that states, "create and manage

[60] Ex. 1 at 112.

your Google Cloud instances, disks, networks, and other resources in one place." I note that the URL of the webpage used the "console.cloud.google.com" domain, indicating that I was accessing the official Google Cloud resources and services. I agreed to the Google Cloud Platform Terms of Service which opened up a management dashboard, displaying various options to administer the Google Cloud account. I clicked on the option to access the Google Cloud Shell which allows command line access to Google project resources on the cloud platform. The displayed username was the Gmail address I submitted to the @OutsiderServerBot during the purchase process, along with a message stating "your Cloud Platform project in this session is set to [redacted]." I note that the displayed Cloud Platform project number matches the Project ID number provided with the @OutsiderServerBot payment and order confirmation message.

99. I returned to the @OutsiderServerBot Telegram channel and selected the option to manage my account which opened a pop-up window labeled as "Outsider International." I selected the Google Cloud option which displayed my account information, including the project ID and an account balance of 500 USDT. A second tab displayed the Google Cloud logo along with my order number and the 500 USDT deposit for the Google Cloud services. My understanding of the Google Cloud deployment process using the @OutsiderServerBot is that as I deploy servers and utilize network bandwidth using the Google console, the 500 USDT deposit will be incrementally debited for payments on my Google account. I note that I tried to do more to engage with the platform, but I received various error messages saying that I needed "admin permissions." When I tried to engage with @sinkinto01 about this issue, the account was unresponsive.

VI. Identifying Outsider-Created Phishing Domains

100. To identify active domains hosting phishing websites created with Outsider, I used two methods. Both are reliable, but they work differently and are therefore able to identify more domains that one or the other method might miss.

101. First, I used my analysis of the software and the websites I created with it to pinpoint unique "fingerprints" of the Outsider sites. As will be discussed more herein, I identified files that, due to the presence within them of the fingerprints, I believe to be unique to SMS sites created with Outsider. I then searched active domains that contained these specific files.

102. I note that my searches almost certainly returned only a subset of Outsider-created phishing websites. I used URLScan.io, a repository of publicly submitted websites, the contents of which have been scanned and preserved, to search for websites with files containing the Outsider fingerprints. When a website is submitted to URLScan.io, URLScan.io automatically browses to it and records activity including "the domains and IPs contacted, the resources (JavaScript, CSS, etc.) requested from those domains, ... cookies created by the page," and more. It will also take a screenshot of the page.[61] If a website is offline when it is submitted to URLScan.io, URLScan.io cannot scan it. In addition, if a website has a captcha or other mechanism in place to prevent access by websites like URLScan.io, URLScan.io might only be able to scan the captcha or other landing page and not the entire website that might contain the fingerprints. Websites that were not affirmatively submitted by internet users to URLScan.io, were offline when a user submitted them, or otherwise were not scanned, would therefore not have been identified in my search.

103. I identified the Outsider fingerprints used to search URLScan.io in the following manner. After using Outsider to create phishing pages using several of the downloaded template

[61] *See About*, URLScan.io, https://tinyurl.com/44zh8ypp (last visited June 1, 2026).

files and assigning them unique URLs, I used the Chrome browser to access and review each page. [redacted] The details of these files revealed that they were identical to the file paths that I had previously identified in the Outsider software. [redacted] noting that they were identical to the hash values I had calculated for the files from the Outsider server.

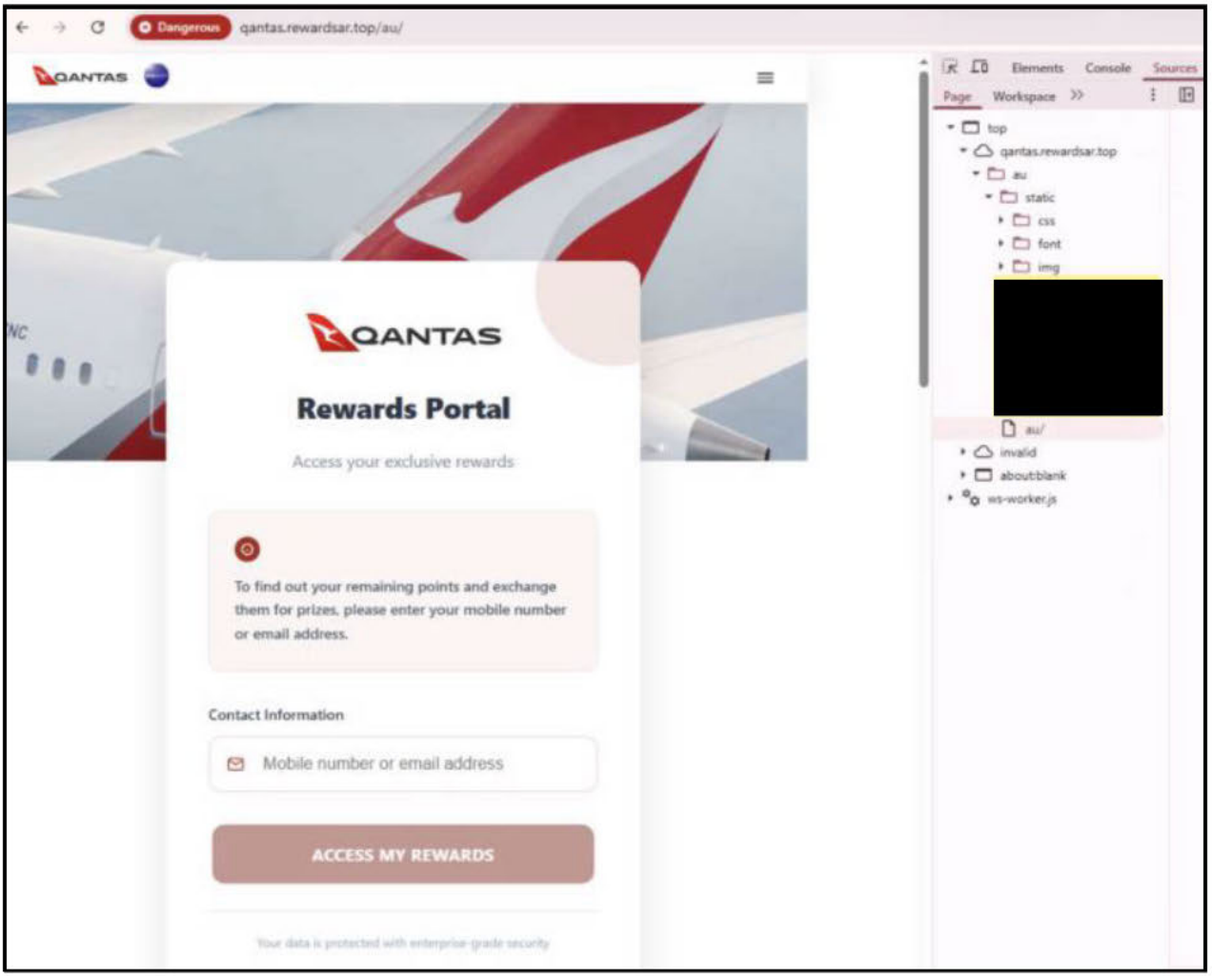
104. [redacted] and other phishing pages I created using the Outsider software, [redacted] All three of these files provide distinct functionality to the Outsider software, facilitating the theft of victims' sensitive information. Additionally, by analyzing the phishing sites created with the Outsider software, [redacted].[62] These four content storage names only appear on Outsider phishing pages and have not been attributed to any legitimate website functionality.

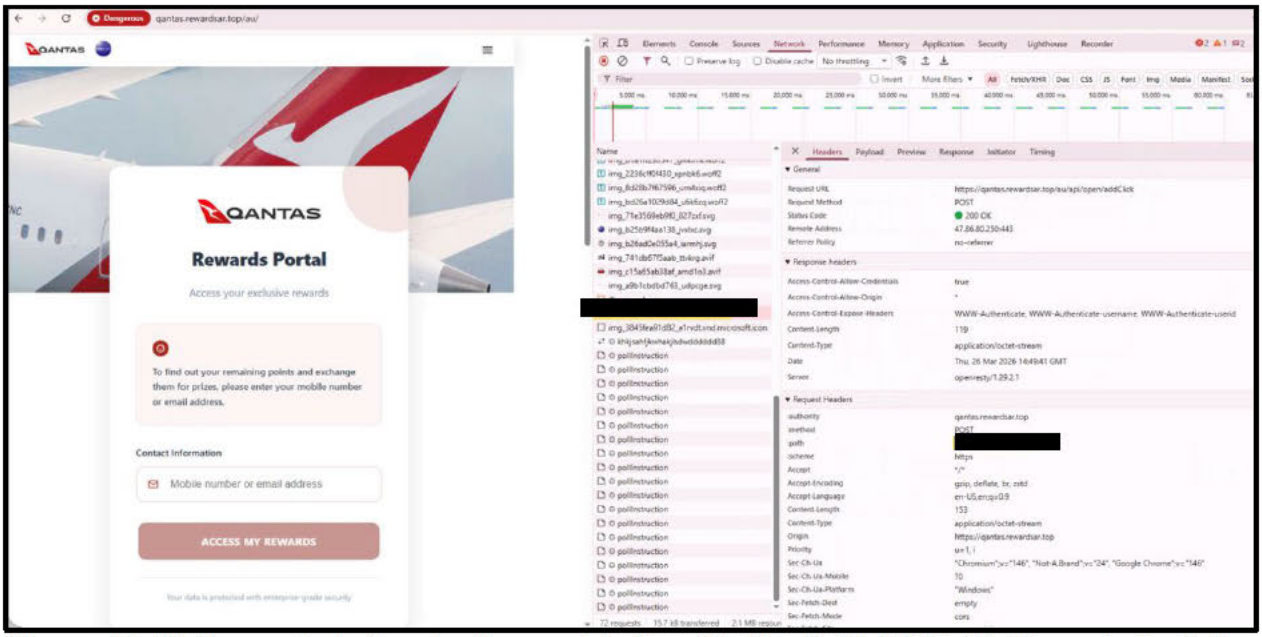
[62] Content storage refers to local and session storage, which are similar to cookies, used by web browsers to temporarily store data when a user visits a website. *Are Local Storage and Session Storage Compliant with Privacy Laws?*, Cookie Script (Apr. 19, 2025), https://tinyurl.com/yxdk6huv.

105. Based on my review of the Outsider software and by creating phishing sites using the provided Outsider templates, as well as an analysis of actual phishing sites identified by using tools such as URLScan.io, [redacted]

106. Using the above fingerprints, I searched URLScan.io for all scans that contained any of the files. The resulting list of URLs from the scan was consistent with phishing pages. I reviewed the search results for any indicators of legitimate websites. Based on my experience, each of the reviewed domains and their corresponding files and screenshots were consistent with phishing scams. In addition to our review of the list of websites, other NAXO team members or I manually reviewed over 100 of the websites, all of which appeared to be fraudulent. For example, on March 26, 2026, the most recent search result was for qantas.rewardsar[.]top/au/. I immediately recognized this as being consistent with a phishing domain, as the brand name "qantas" was listed as a subdomain, with the apex domain being "rewards" with extra letters "ar." This is consistent with how fraudsters try to make their domains appear legitimate. A review of information related to the apex domain "rewardsar[.]top" identified that it was created on March 25, 2026 and the registrant is located in Germany, whereas the legitimate Qantas[.]com domain was created in 1996 and the registrant is located in Australia. To my knowledge, Qantas Airlines, an Australian airline, uses the apex domain of "Qantas." Of course, established brands have held their domains for many years.

107. I accessed the qantas.rewardsar[.]top/au/ website using the Chrome web browser, and I was presented with a website with the Qantas logo, apparently spoofing the Qantas rewards portal. I believe this scam is similar to the telecommunications scams discussed herein, where users are tricked into sending information to pay for products or services on a fraudulent rewards website. Using the Chrome developer tools, I reviewed the network requests for this website. I observed network requests for my identified fingerprints.





Figures 54, 55. Screenshots showing fingerprints found in March 26, 2026 phishing website. I also note that the website contained the YouTube logo.

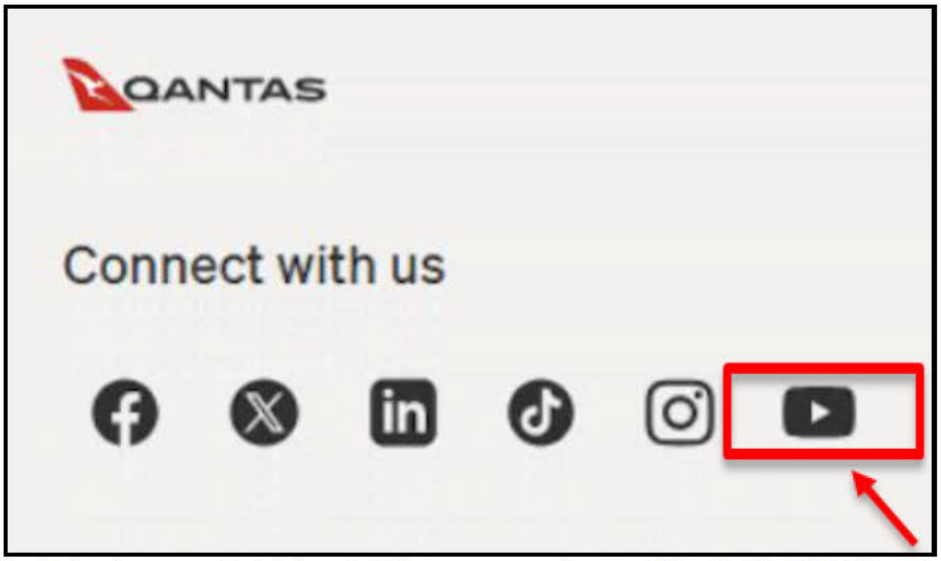


Figure 56. YouTube logo on Outsider phishing page, active on March 26, 2026 (emphasis added).

108. My search results included only phishing websites created on or after July 22, 2025. This is consistent with the timing of the release of Outsider and helps support my theory that the fingerprint I identified is unique to Outsider phishing pages.

109. Second, to identify additional domains, I coordinated with Google investigators. I understand that Google used the same fingerprints that I used to identify domains containing the

Outsider fingerprints noted above, but Google reviewed a repository distinct from URLScan.io. Google sent me a list of the domains in which it identified an Outsider fingerprint and asked me to verify their findings.

110. Google's results overlapped largely but not entirely with the domains I had identified through URLScan.io using my first method. I believe this is because of the previously-discussed limitations of URLScan.io, including that it can only scan active websites—such that if a website is inactive when URLScan.io's analysis is attempted, URLScan.io cannot scan the domain, even if the domain remains viable and even if the fingerprint was previously present on the site. I understand from Google's investigators that they were, using a distinct repository from URLScan.io, able to review websites that URLScan.io did not detect by virtue of their being unavailable to scan.

111. As to the domains that were not visible on URLScan.io, I took additional steps to verify that the domains are malicious. I reviewed the domains for additional markers of cybercrime. I also manually reviewed each of the domains and assessed whether they exhibited patterns consistent with the other phishing domains I identified. A common pattern for phishing websites (observed with the Qantas example herein) is that the subdomain spoofs a legitimate company and the apex domain is often an odd, unrecognizable, or apparently random combination of letters. I also know that scammers commonly use certain less common top-level domains (instead of .com) like .top or .shop. In my experience, these factors indicate that a domain is a phishing website. For example, one of the domains that Google identified that was not on my original list was [redacted]. Combined with Google's findings that the fingerprints I identified were found on that website, my knowledge that T-Mobile is a company often targeted by Outsider, and the recognizable pattern of the domain, I was able to confirm that

this domain is a malicious phishing website. I conducted a manual analysis of each domain identified by Google that was not on my original list and based on that analysis, I believe that all of the domains identified using both methods and listed in Appendix A are malicious phishing sites.

112. In total, I identified approximately 9,354 domains that I verified are malicious phishing sites using the methods described above. I confirmed that Outsider fingerprints were present on the sites identified by URLScan.io, and I confirmed that indicia of maliciousness were present on sites on which Google identified the presence of Outsider fingerprints. The domains and a list of registrars hosting those domain names are attached as Appendix A.

113. In order to attempt to identify a broader set of fingerprints that would include domains created using the older version of the Chenlun software, [redacted] Searching all of these files led me to a list of 31,391 phishing pages which I think were likely created with Outsider and its predecessor software created by @chenlun. Members of the NAXO team created a graphical representation of the industries targeted by phishing scams over time, which is also consistent with my research.

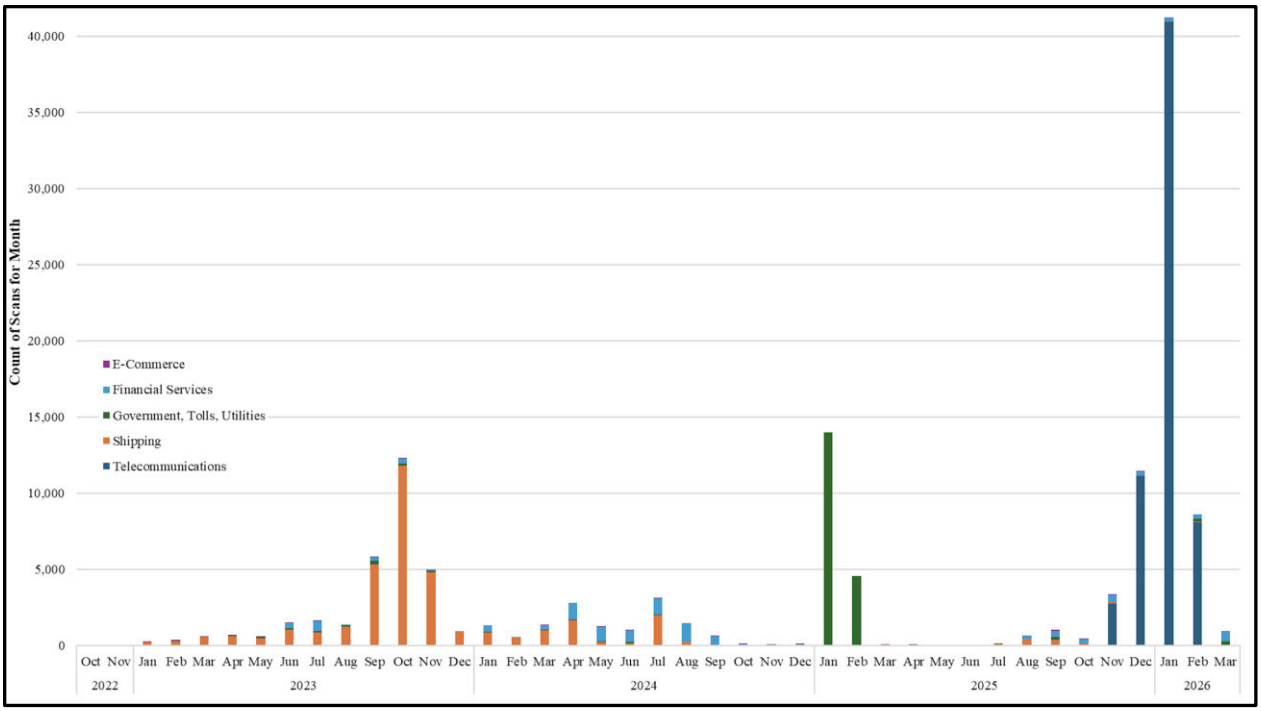


Figure 57. Trends in @chenlun/@sinkinto01 phishing scam targeting over time.

114. This graph indicates that the first Chenlun phishing websites I identified with these fingerprints began to appear in January of 2023. At that time, and through the spring of 2024, shipping scams (including USPS) were the most popular phishing scams. In 2024, a larger percentage of scams focused on financial institutions. I notice that in January and February of 2025, there was a spike in toll/parking ticket scams. Subsequently, as public awareness of those schemes has grown, the graph indicates that there was then a substantial drop in phishing websites with these fingerprints until the re-release of Outsider in July of 2025. Most recently, there has been a substantial spike in scams targeting telecommunications companies, which is consistent with what industry experts and law enforcement have observed in terms of shifting trends.[63] **Appendix C** is a representative sample of phishing websites that contain Outsider fingerprints.

[63] *See* Brian Krebs, *SMS Phishers Pivot to Points, Taxes, Fake Retailers*, Krebs on Security (Dec. 4, 2025), https://tinyurl.com/3dc7r54y; Fraud Alert: Telecommunications Scam, Middlesex County, NJ (Jan. 30, 2026), https://tinyurl.com/3suk4kf6.

VII. @sinkinto01/@chenlun and the Distribution of Outsider

115. The person or persons using Telegram handles @chenlun and @sinkinto01 identify as the developers of the Outsider software.

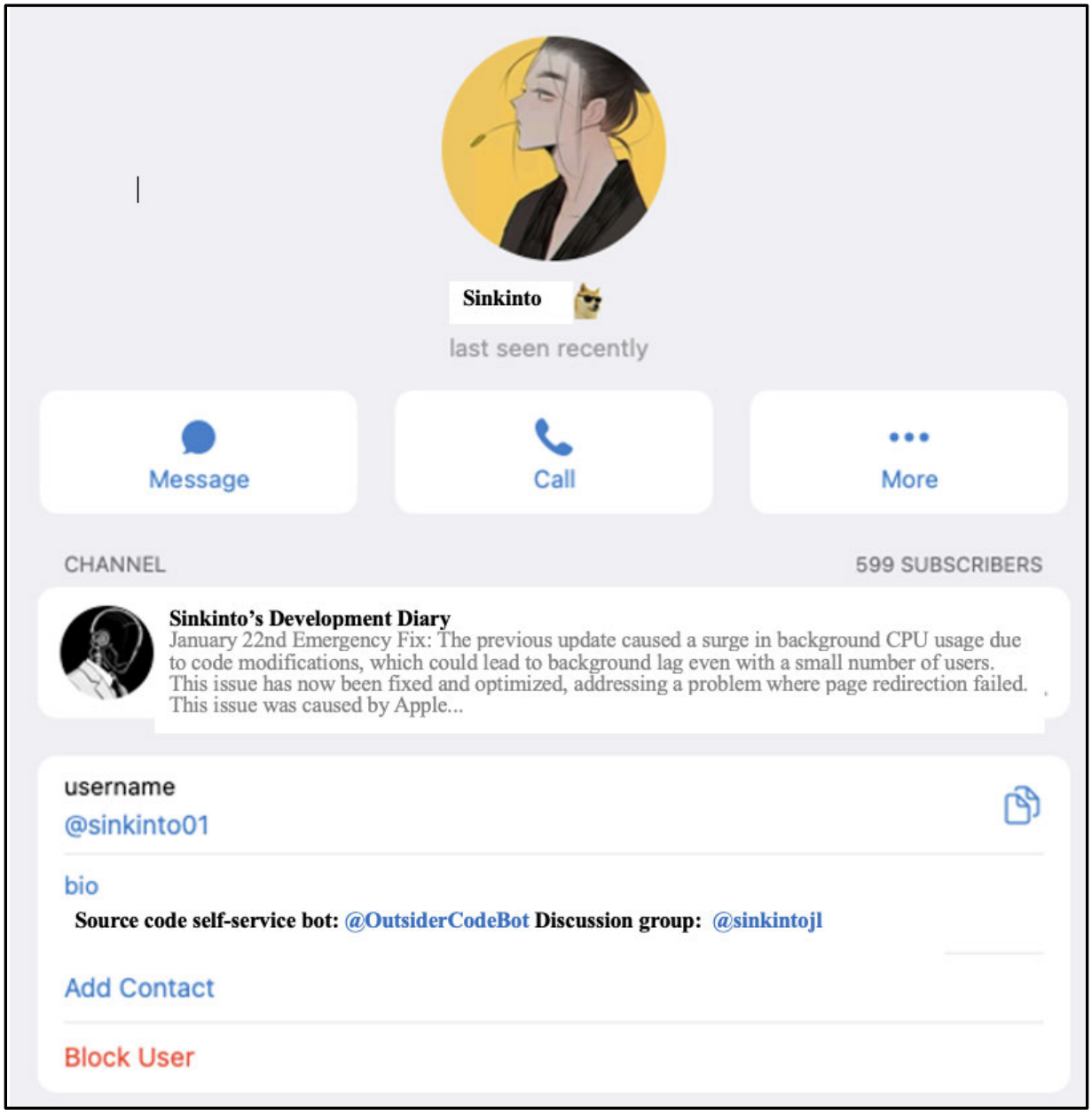


Figure 58. Screenshot of the Telegram profile for @sinkinto01 as of January 2026, https://t[.]me/sinkinto01 (translated).[64]

[64] Ex. 1 at 116.

116. As discussed previously, @sinkinto01 authored a post on cosmileonly[.]com in May 2025 in which they claimed to have developed both the original Chenlun source code and Outsider. The post was titled, "Chenlun's journey from a poor kid to a successful celebrity in three years."[65] Specifically, they told the story about how upon graduation after studying IT in 2022, they had trouble finding internships so they "took out an online loan of 20,000 and began [their] C-circle journey." They described meeting an "older brother" in an online community who encouraged them to use their IT background to create source code for him. @sinkinto01 did so, creating source code which they boasted, featured improved anti-blocking capabilities allowing "a domain name [to] be used for more than a month on average" before being flagged as malicious.[66] According to @sinkinto01, the source code became very popular. @sinkinto01 described how around that time, they also began phishing themselves. In a lengthy narrative excerpted below, they described initial success which led to the previously discussed media attention and retirement of the Chenlun name.

> Before this, I had never done phishing myself; I learned about it through communication with group members, because at that time, just by selling source code I could sell nearly 200,000 per month. For someone like me who until recently had been an ordinary worker, what more could I ask for? Later, I . . . began to try phishing, and from then on I was hooked. That period was really a carnival for the C-circle. It was also the first time I experienced what it was like to make 200,000 a day lying down doing nothing, but the good times didn't last long. . . . At that time, I was sending out hundreds of thousands of messages every day and was also targeted by some foreign bloggers. In order to avoid the limelight, I cleared all the content and tutorials from the channel. . . The former TG name @chenlun was also changed. Coupled with the rise of various peers, I felt the source code industry was just too competitive so I completely gave up the source code industry from then on.[67]

[65] @sinkinto01, Chenlun's journey from a poor kid to a successful celebrity in three years, (May 29, 2025), cosmileonly[.]com (translated), Ex. 1 at 123–27.
[66] *Id.*
[67] *Id.*

117. @sinkinto01 described taking time away from the industry but the post concluded with their recent decision to work on a new product. A second post that same day provided more information on their process for creating and testing new source code. It also included a link to the @sinkintopd Telegram channel with a note reading, "if I continue the source code business in the future, it will be published here."[68] Just a few months later, Outsider was in fact published on that Telegram channel.

118. Over the course of my investigation, I directly messaged @sinkinto01 to ask questions about the software and always received prompt responses. For example, on January 13, 2026, I sent a screenshot of an error message I received in the software and @sinkinto01 responded that my server was not supported. When I explained that I had used that type of server for outside deployment, they responded, "[d]on't worry, this third-party deployment platform was developed by me personally and will not leak any of your server information."[69] I understood this to be an assurance that using the Outsider infrastructure would protect my personal server information from exposure to third parties. I later asked @sinkinto01 why I could only download five templates. They asked for my authorization code, which I sent, and then responded, "[t]he weekly plan allows downloading up to 5 different templates, while the monthly plan allows 10."[70]

119. The @sinkinto01 Telegram profile links to various channels devoted to the sale of Outsider: @OutsiderCodeBot, the Telegram robot used to purchase Outsider licenses; @sinkintopd, the "development diary" channel in which @sinkinto01 posts updates and tutorials about the Outsider software; and @sinkintojl, the Outsider-related community discussion group in

[68] @sinkinto01, Post describing the creation and testing of new source code, (May 29, 2025), cosmileonly[.]com (translated), Ex. 1 at 132–34.
[69] Ex. 1 at 138.
[70] Ex. 1 at 142.

which various people post about phishing-related issues and services. These groups also link to the channel @OutsiderServerBot, the bot that facilitates the purchase of cloud servers. Additionally, after I purchased the monthly license, I was invited to a closed, customers-only "Outsiders Member Group" which includes 211 members as of April 2026.

120. As discussed previously, I purchased my Outsider license on @OutsiderCodeBot. In order to do so I paid a fee in USDT through a Telegram bot. I later conducted an analysis of the cryptocurrency address to which I (and presumably other customers) paid the fee. Transactions on the Tron blockchain are represented as a public ledger, which allows anyone to review deposit and withdrawal information for specific addresses. Using the prices advertised on the bot for the weekly and monthly license, members of the NAXO team analyzed how many corresponding payments the address had received over time. The chart below depicts the estimate of the number of weekly and monthly phishing licenses purchased from @sinkinto01 each month since the release of the Outsider software.

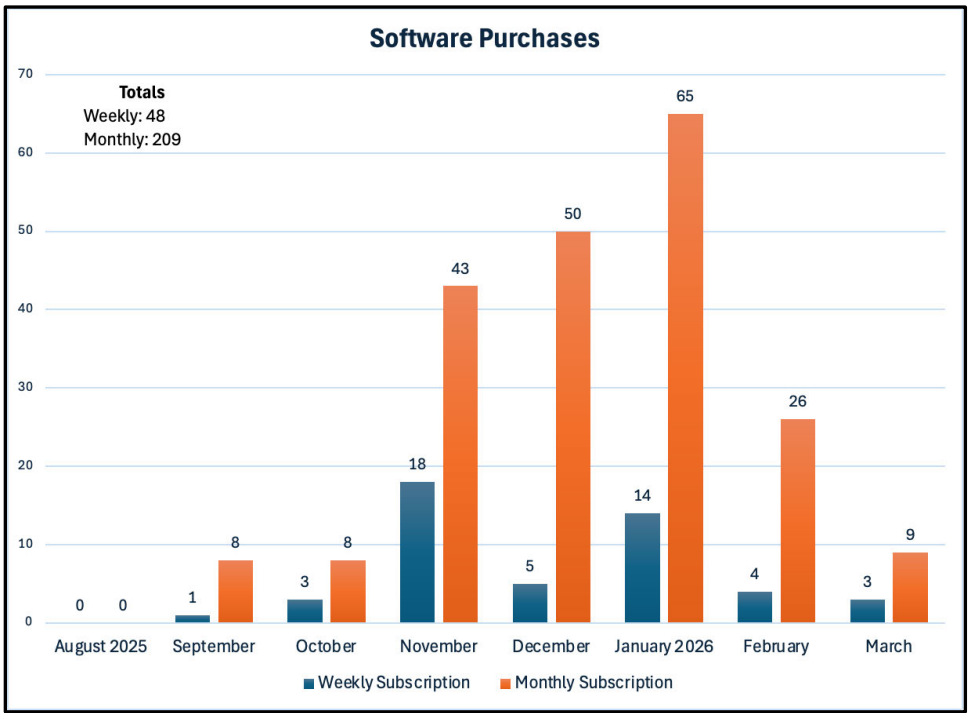


Figure 59. Payments to the Outsider USDT address from August 2025 through March 2026.

121. This chart indicates that in January 2026, for example, over 65 people purchased monthly Outsider licenses. One license could allow a person to create hundreds of websites that could steal hundreds or thousands of credit cards each day.

122. The "development diary" @sinkintopd is a Telegram group that was initiated on June 1, 2025. @sinkinto01 is the only administrator and the only user that can post in the group. On the date it was created, @sinkinto01 posted a message announcing a new version of the Outsider software. The channel has since posted at least 175 messages and 13 tutorial videos explaining different features of the Outsider software. @sinkinto01 posts regular instructions and notes about updates to the software. For example, on February 9, 2026, @sinkinto01 posted an update that stated among other things, "[t]he anti-blocking system has been completely redesigned" and described specific features designed to overcome security protocols meant to block malicious websites.[71]

123. The community discussion group, @sinkintojl includes posts from various individuals advertising and requesting services related to phishing. For example, on November 10, 2025, users made posts offering to sell global SMS data, credit card data, and personal information like passports and other identification documents. Another user offered to sell stolen Gmail account information.

[71] Ex. 1 at 146.

Figure 60. Examples of posts made in the @sinkintojl community discussion group, Telegram (Nov. 10, 2025), https://t[.]me/sinkintojl/581580 (translated).[72]

[72] Ex. 1 at 150.

124. This is a representative sample of the types of posts that occur in this group daily. I note for example that "Nan'an Overseas Data" appears to be a data broker providing global contact information for potential victims. Another user was "[u]rgently" in need of "SMS routes for Colombia, Mexico, Chile," which I understand to mean that they were looking for access to delivery channels, vendors, or infrastructure capable of sending phishing SMS messages to people in those countries.

125. The @sinkintojl discussion group has one owner, @sinkinto01, and five administrators: @sinkinto02, @fangzhangBot, @Zhyuebot, @bailiworking, and @yy0205.[73] Admins all have authority to invite, ban, or remove members or moderate content by deleting messages, "pinning" important messages, and controlling other chat settings. The group admins all apparently provide different services to support the Outsider phishing operation.

126. One group admin is @bailiworking, a "spammer" who offers services sending SMS/RCS messages. The user of the Telegram handle's profile reads, "RCS IM one-stop shop with good performance, professionally selling base station data source code." It links to an affiliated channel which frequently discusses SMS support services for phishing.

[73] @fangzhangBot and @Zhyuebot are robots, and @sinkinto02 is a backup account for @sinkinto01.

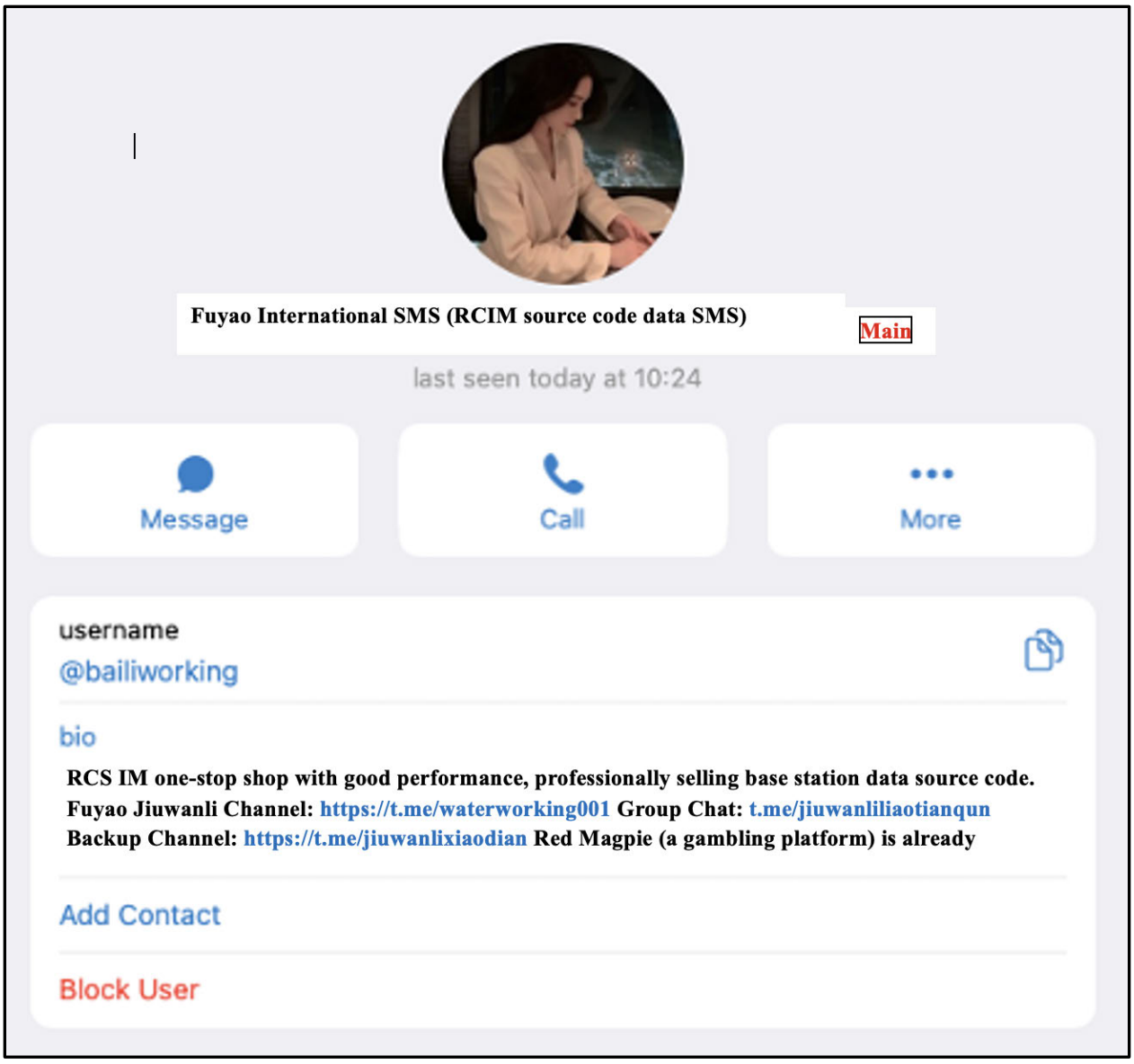
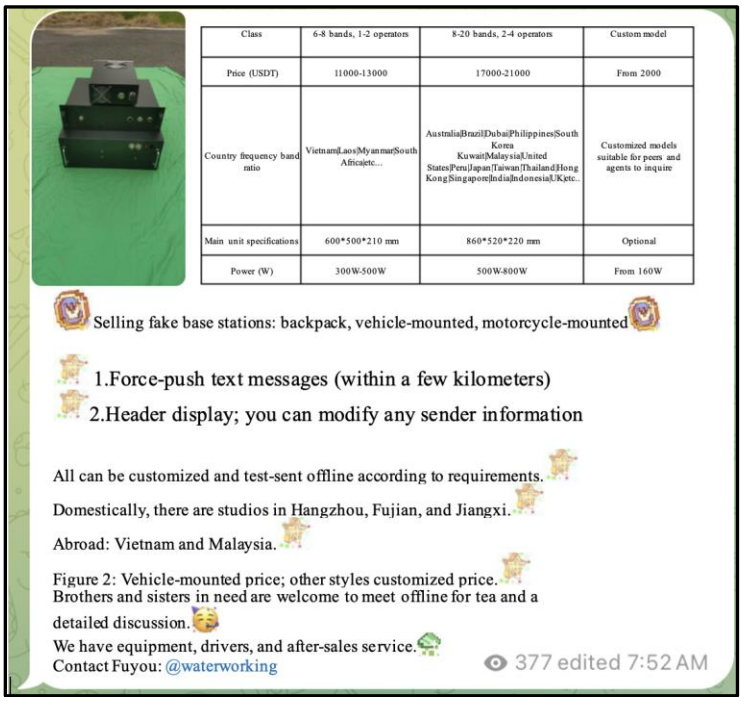


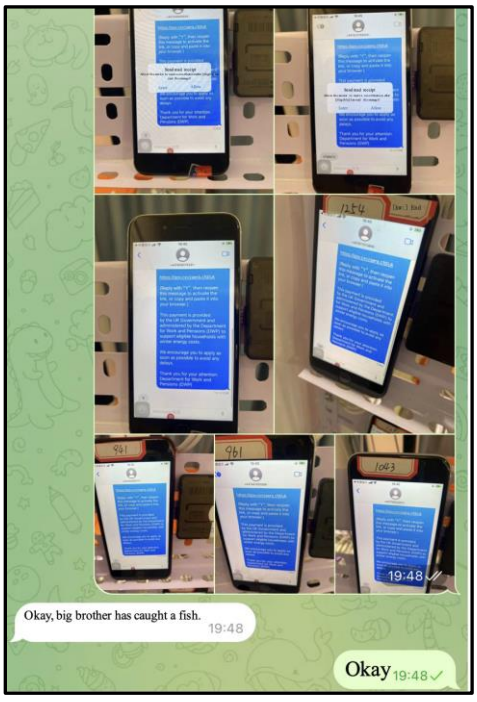
Figure 61. Screenshot of the Telegram profile for @bailiworking as of February 10, 2026, https://t[.]me/bailiworking (translated).[74]

127. On January 10, 2025, for example, @bailiworking posted an advertisement for "fake base stations" with "force-push text messages (within a few kilometers)" highlighting that they "can modify any sender information." I understand this to be a machine used to generate phone numbers from which text messages can be sent out to users within a certain distance of the station, allowing a sender to control or modify the originating number associated with the messages

[74] Ex. 1 at 154.

sent from the base stations. The Telegram user also claimed to operate studios in China, Vietnam, and Malaysia. I know that high-volume spamming organizations often set up call centers filled with banks of cell phones used for sending bulk SMS messages. In fact, on October 21, 2025, @bailiworking posted a photograph depicting various cell phones sending what appears to be a phishing text message captioned with the words "Okay, big brother has caught a fish." These appear to be set up in a large data center.





Figures 62, 63. @bailiworking, Posts advertising SMS/RCS services (Jan. 10, 2025) (l), and showcasing the ability to send multiple text messages (Oct. 21, 2025) (r), https://t[.]me/waterworking001/271, 833 (translated).[75]

128. On August 23, 2025, @bailiworking announced in his/her own Telegram channel that, "[t]he source code for Sinkinto is back!" They offered a discount, and stated, "contact me to purchase." A screenshot of the Outsider software was included with the post.

[75] Ex. 1 at 158, 162.

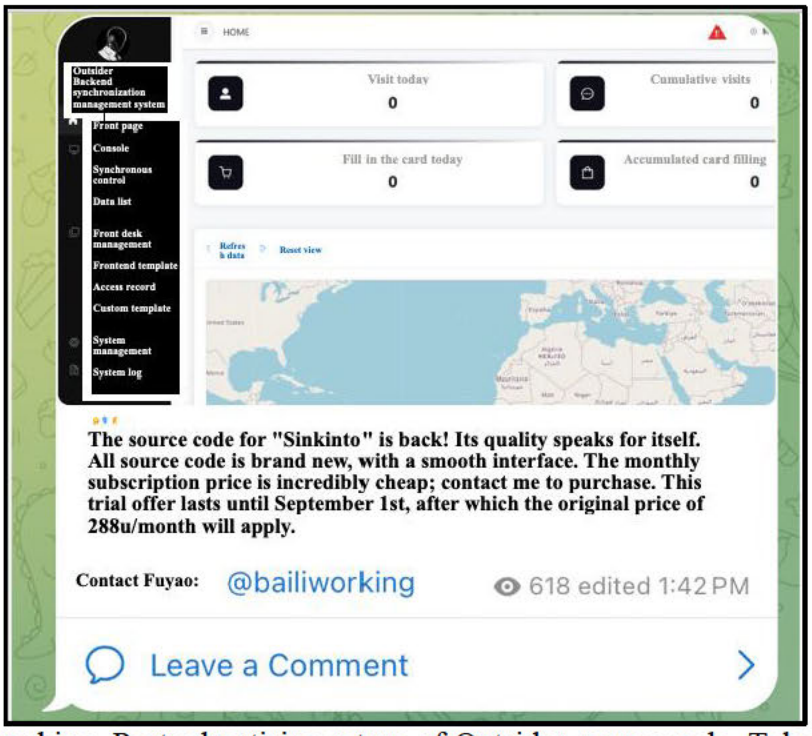


Figure 64. @bailiworking, Post advertising return of Outsider source code, Telegram (Aug. 23, 2025), https://t[.]me/waterworking001/723 (translated).[76]

129. On January 22, 2026, I initiated a conversation with @bailiworking. I inquired about whether he or she offered SMS services to use with Outsider by sending a screenshot of the Outsider platform. When I asked if @bailiworking works with Chenlun, @bailiworking described them as a friend and sent me a screenshot of a conversation between them that occurred in December of 2025. An excerpt of our conversation is included here:[77]

[redacted]: Can RCS instant messaging functionality be used by external users?

@bailiworking: can send rcs

[redacted]: With outsider source code?

[76] Ex. 1 at 166.

[77] *See* **Exhibit 2**, which is a true and correct copy of a certified translation of my conversation with @bailiworking on Telegram. I communicated using a Telegram username that I have omitted from the declaration. I initially used Google Translate to communicate in Chinese. Page 4 does not have a translation because those messages were all in English.

@bailiworking: Which country do you need to send to?

[redacted]: US

@bailiworking: Poor feedback from the US

@bailiworking: Only a few out of ten thousand text messages

[redacted]: Even with the new parking citation templates?

@bailiworking: I don't know about that, you can try it and see.

[redacted]: How much for 1,000?

@bailiworking: 23.2u

[redacted]: What address do I use?

@bailiworking: trc20

[redacted]: Do you work with Chenlun? I am using the Outsider Sync. I want to make sure this works.

130. In response, @bailiworking responded simply, "friend," and sent me a screenshot of a conversation they had with @sinkinto01 as evidence. I believe that @bailiworking was telling me that he or she was a friend of @sinkinto01. They later confirmed, "I have sms rcs im."[78] I believe that @bailiworking is a data broker who not only maintains lists of contact information for potential victims but sends out text messages on behalf of scammers.

131. The Telegram user @yy0205 is another admin of the @sinkintojl Outsider discussion channel. Their telegram profile reads "(Outsider Source Code) Seventeen."

[78] Ex. 2 at 3, 5, 7.

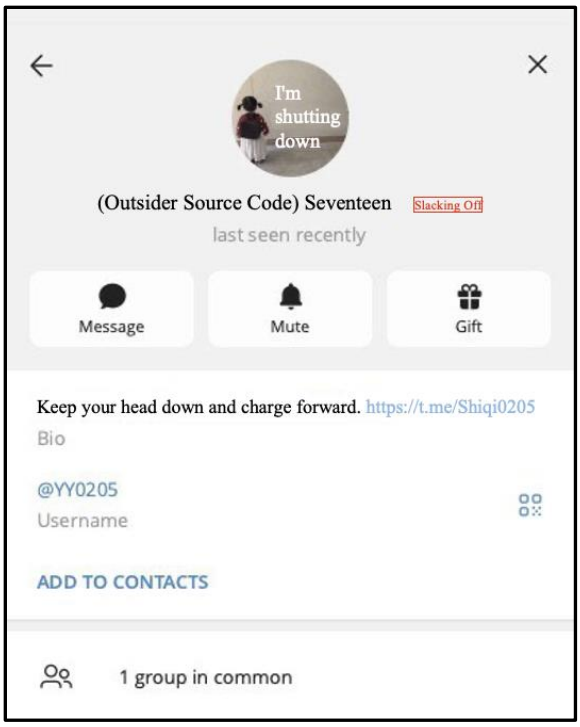


Figure 65. Screenshot of the Telegram profile for @yy0205 as of February 10, 2026, https://t[.]me/yy0205 (translated).[79]

132. In a January 22, 2025 post, @yy0205 described themselves as "the strongest intermediary on the entire internet," encouraging potential customers to contact them and adding that "[n]othing is impossible; everything is readily available."[80] On October 17, 2025, @yy0205 posted a photograph of what appears to be a point of sale machine that takes credit card payments to the @sinkintojl channel stating, "[b]rand-new equipment sold in bulk." I know that scammers use these machines to launder funds from stolen credit cards. Specifically, after credit cards are loaded onto cell phones, scammers can use the phones' tap to pay functionality to make "payments" to themselves using these machines.

[79] Ex. 1 at 170.
[80] Ex. 1 at 174.

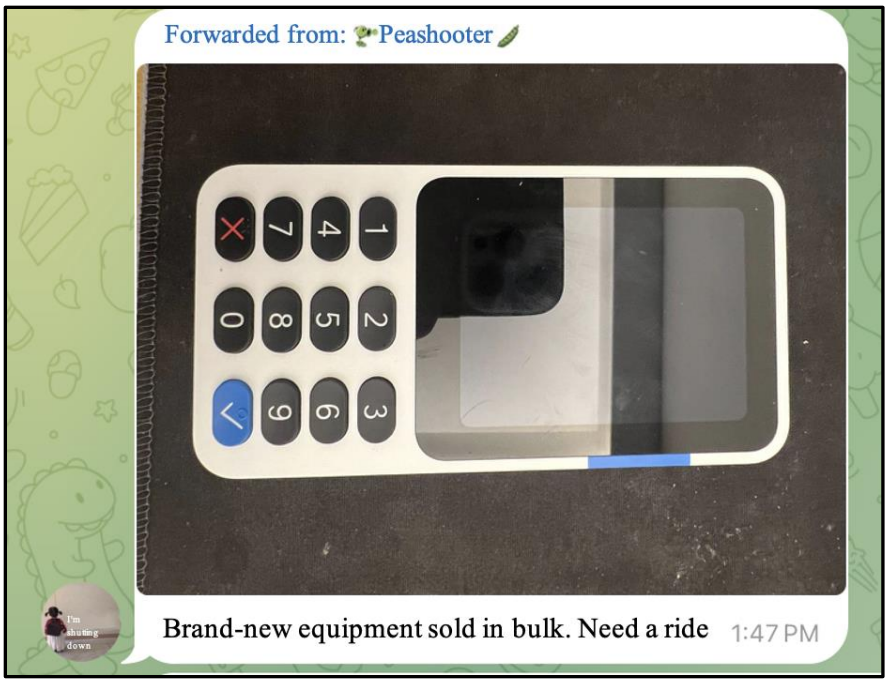


Figure 66. @yy0205, Post in the @sinkintojl channel, Telegram (Oct. 17, 2025), https://t[.]me/sinkintojl/562706 (translated).[81]

133. @yy0205 is also the creator of the Telegram channel @shiqi0205, of which @sinkinto01 and @bailiworking are also admins. This channel also includes discussions about phishing and related services. For example, @sinkinto01 advertised Outsider there and on October 14, 2025, @yy0205 posted the following photographs of cell phones loaded with apparently phished credit cards reading, "[h]elping a friend sell cards again." They then included a picture of a British flag and wrote, "[a]ll the big cards are here."

[81] Ex. 1 at 178.

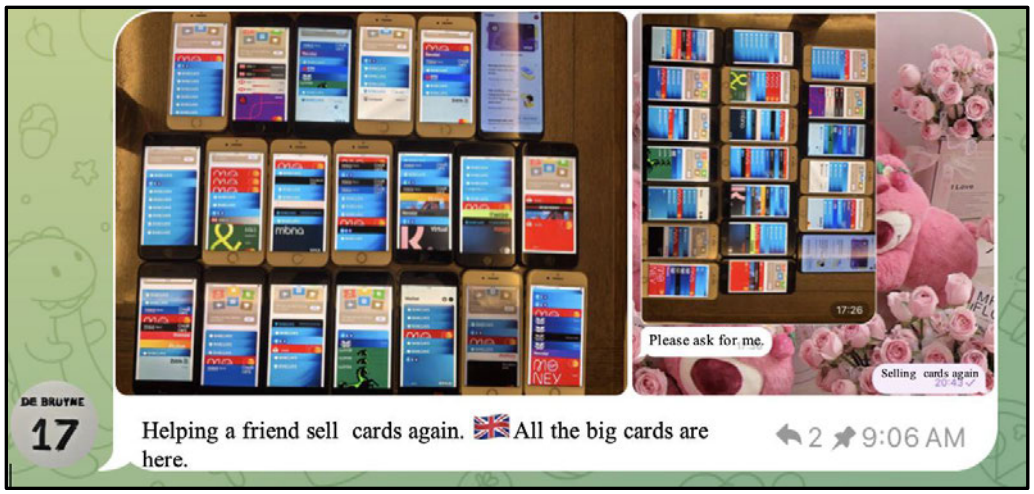


Figure 67. @yy0205, Post in @shiqi0205 channel, Telegram (Oct. 14, 2025), https://t[.]me/Shiqi0205/4307 (translated).[82]

134. Finally, the third admin of the @sinkintojl channel, @FHER777, appears to provide stolen account credentials and to operate a cryptocurrency exchange service. @FHER777 operates several channels, including @zhuoyue_logs which appears to offer access to stolen accounts from popular retail stores and online services including Uber, DoorDash, and Walmart. These accounts may be obtained by phishing campaigns using software such as the Outsider platform. @FHER777 also operates the @Zhyuebot channel which is an automated bot system that offers crypto asset exchange services. Customers who wish to purchase the Outsider software are required to use USDT through the @OutsiderCodeBot channel. These customers can use the @Zhyuebot to swap other types of crypto for USDT without having to use an exchange which may collect identifying information.

[82] Ex. 1 at 182.

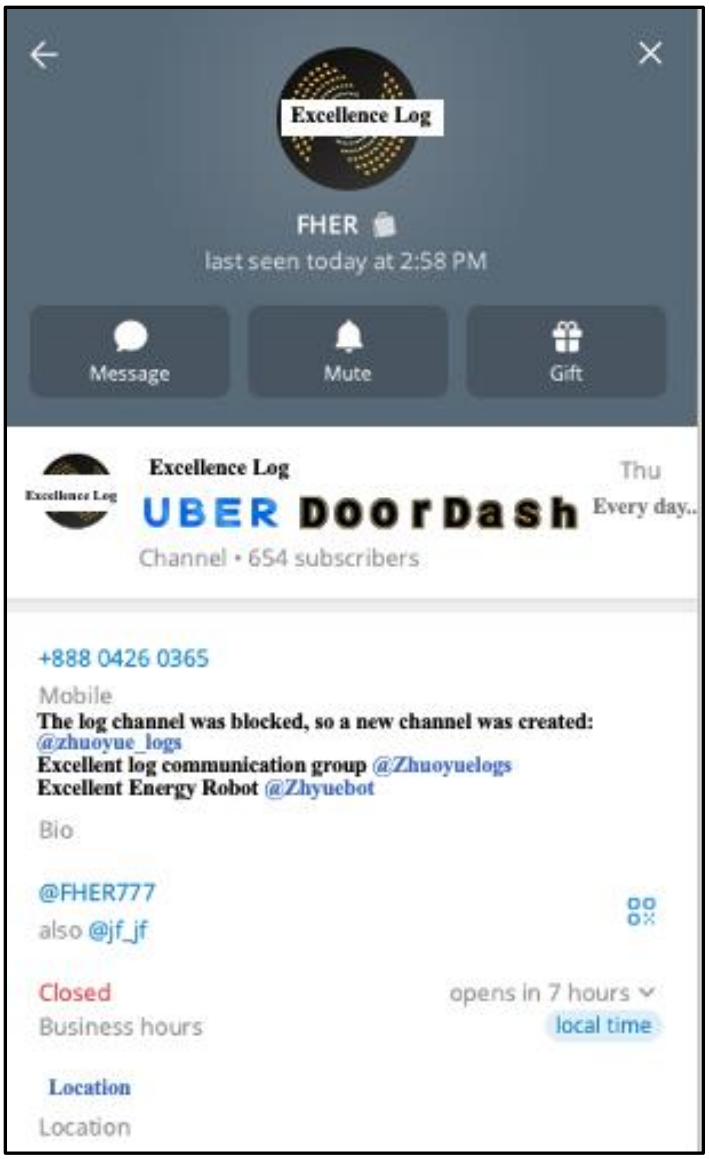


Figure 68. Telegram profile of @FHER777 as of February 2026 (translated).[83]

135. I have identified other Telegram accounts that appear to work with @sinkinto01 as well. As discussed previously, I used @OutsiderCodeBot to purchase a license for the Outsider software. Up until early 2026, @OutsiderCodeBot had a menu option that was entitled "Strategic Partners." This menu option linked to two "partners," apparent associates of @sinkinto01, one of

[83] Ex. 1 at 186.

whom offered SMS services (represented by an emoji of a cell phone) and one of whom appeared to offer credit card verification services (represented by an emoji of a credit card).

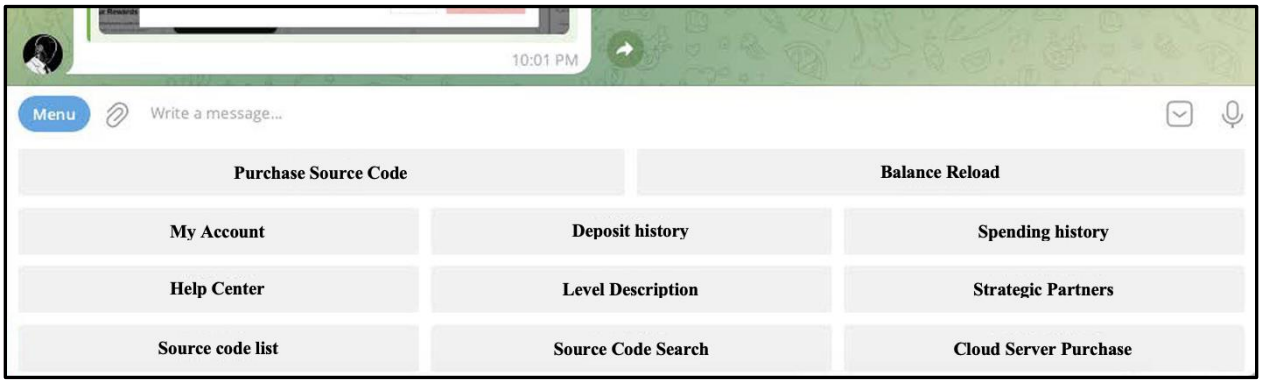


Figure 69. Screenshot of @OutsiderCodebot main menu, as of December 2025 (translated).[84]

136. Choosing the first option (with the phone emoji) brought me to a page linking me to Telegram user @adc88adc, a user who was clearly selling SMS/RCS services.

Figure 70. Screenshot of @OutsiderCodebot Strategic Partner, December 2025 (translated).[85]

[84] Ex. 1 at 190.
[85] Ex. 1 at 194.

137. I accessed the "official website" for adc888[.]com and noted that it listed prices per message sent over various platforms including WhatsApp, Google Chat, and "RCS-iOS Devices," the last of which I understand would be a message to an Apple device like an iPhone.

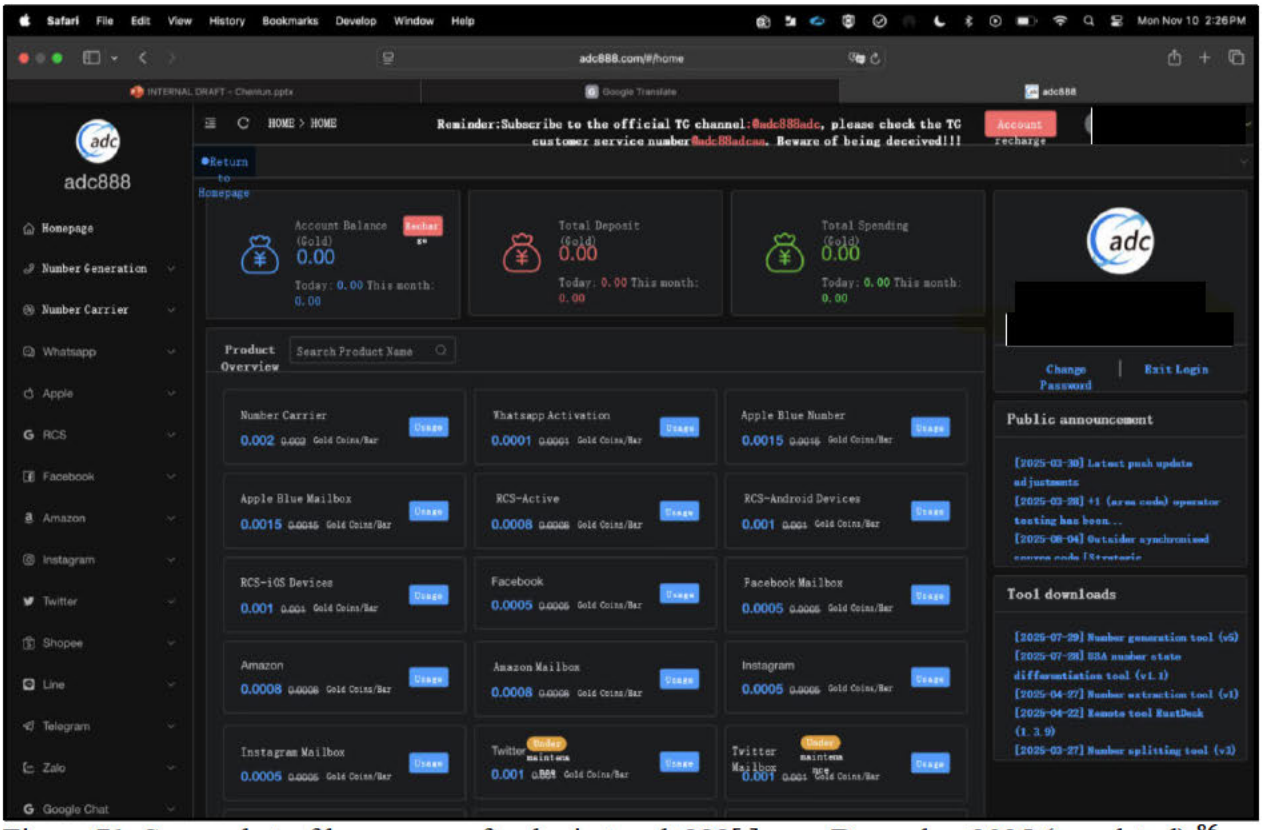


Figure 71. Screenshot of homepage after login to adc888[.]com, December 2025 (translated).[86]

138. The @bailiworking conversation, interaction with the @OutsiderCodeBot, and the adc888[.]com pricing menu (which lists per-message prices for WhatsApp, Google Chat, and "RCS-iOS Devices") I accessed are all consistent with my understanding that Outsider users can send messages through Apple iMessage, RCS, and SMS.

139. I also noted that the website listed a "public announcement" section and on August 4, 2025, it linked to the following advertisement for "Outsider Synchronized Source Code."

[86] Ex. 1 at 198.

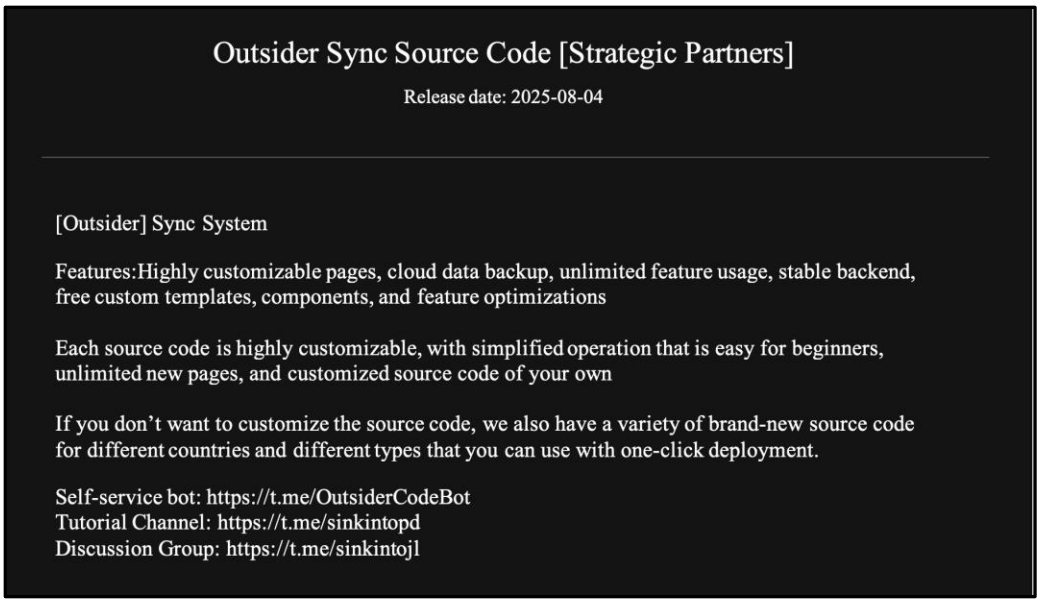


Figure 72. Screenshot of "announcement" posted on August 4, 2025, adc888[.]com, December 2025 (translated).[87]

140. As of January 2026, the website was no longer functioning.

141. The second "strategic partner" from the menu, accessed by clicking on the link with a picture of a credit card that read "activated or not," linked me to @alicehuocc and channel admin @caozei. The @alicehuoccpd Telegram channel provides a service in which people can verify whether credit card numbers are legitimate. For a fee paid in USDT, scammers can check the validity of their stolen credit card information before making a purchase. On October 8, 2025, @alicehuocc posted a Telegram conversation with someone interested in the services they provide. The @alicehuoccpd account replied in English explaining, "Our website is a check cc website, I don't sell CC."[88] On November 23, 2025, the @alicehuoccpd channel posted a link to the kami.alicehuo[.]cc website.[89] This website appears to be a storefront

[87] Ex. 1 at 202.
[88] *See* Post of screenshot of conversation, Telegram (Oct. 8, 2025), t[.]me/alicehuoccpd, Ex. 1 at 206.
[89] *See* Post of kami.alicehuo[.]cc website, Telegram (Nov. 23, 2025), t[.]me/alicehuoccpd, Ex. 1 at 210.

where customers can purchase credits with USDT that will allow them to check a certain number of cards based on their number of credits.

142. Finally, I reviewed the conversations in the Outsiders Member Group channel, which was an invite-only channel for purchasers of Outsider licenses. @sinkinto01, @yy0205, @bailiworking, and @FHER777 are members of this group along with over 150 other purchasers of Outsider. The group includes conversations between Outsider users about strategies for optimizing their phishing campaigns. @sinkinto01 often chimes in to answer questions, but various members of the group also chime in with tips and tricks. For example, a conversation from November of 2025 discusses ways to make e-commerce websites most appealing to targets in Canada. The conversation also implies that the e-commerce websites are advertised to users on TikTok ("TK") in the chat.

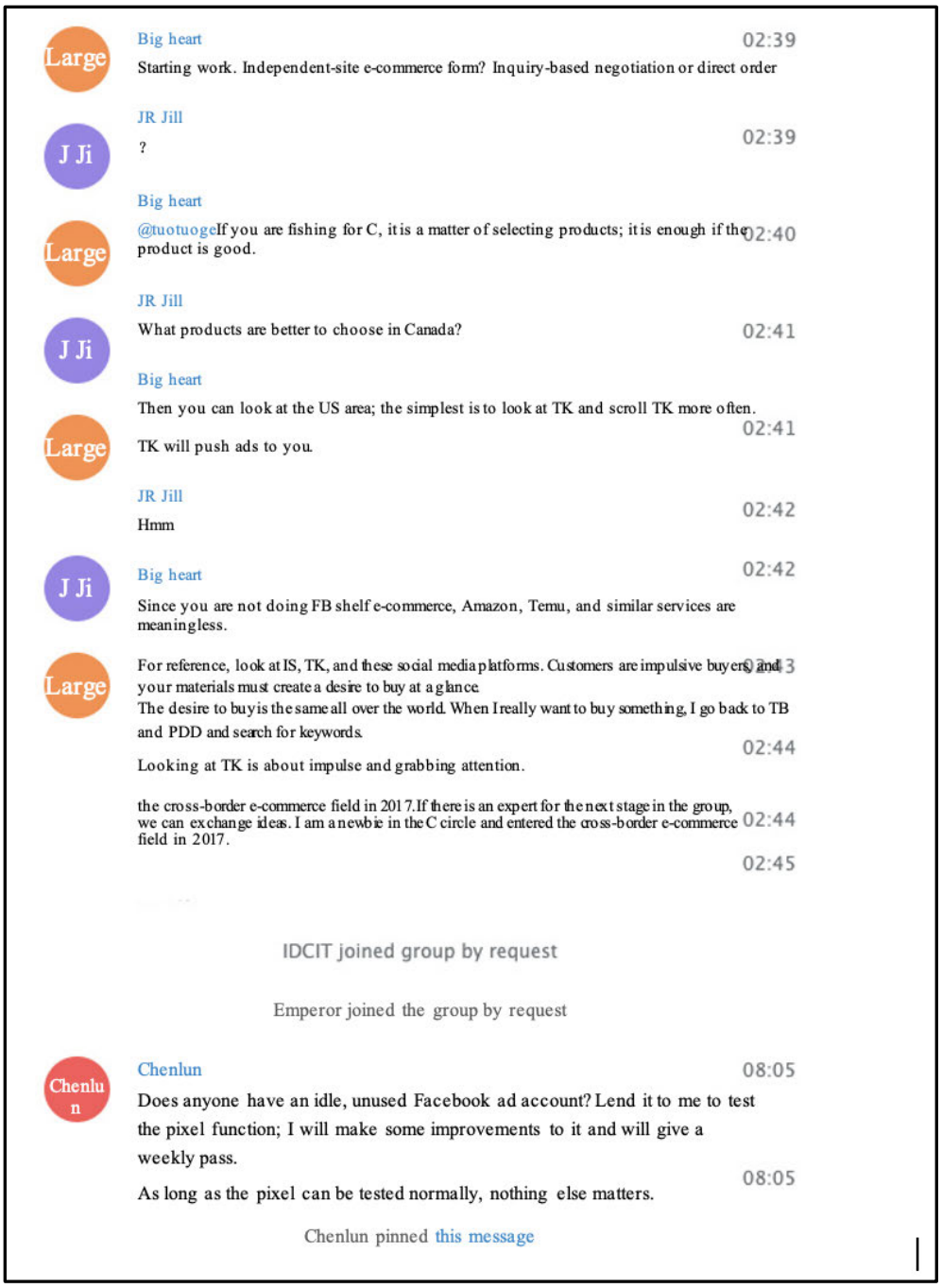


Figure 73. Sample of discussions from Outsiders Member Group, Telegram (Nov. 2025) (translated).[90]

143. On December 5, 2025, one user asked whether anyone had a "Middle East link that supports Google Pay" and another user chimed in that they were accepting Apple Pay and Google

[90] Ex. 1 at 214.

Pay in Germany.[91] As the conversation in the group frequently included discussions of different financial institutions across countries with varying levels of security, I believe that these users were talking about how easy it was to phish Google Pay credentials in different countries.

144. Additionally, on February 26, 2026, a user advertised, "Work has started! E-commerce fish for CA and US, contact me if you need a fish package." I believe they may have been selling contact information for U.S.-based victims. That same day, another user asked, "[w]ho has Chilean fish?" looking for potential victims in Chile.[92]

VIII. Conclusion

145. The Outsider software is pervasive and sophisticated. It allows for the creation of essentially any kind of phishing website, with a vast array of pre-made templates, and the ability to custom create fraudulent websites through the misuse of Google Gemini. @sinkinto01, @bailiworking, and others distribute the phishing software through an organized communication and payment platform that provides updates and customer service. The network provides scammers with all the tools and resources necessary to conduct a widespread operation, from sending SMS messages, to laundering stolen funds through tap-to-pay machines and phones loaded with stolen credit card information.

146. By impersonating government agencies and trusted companies to steal from victims, these fraudsters erode the trust everyday users place in these institutions and the internet. Given the software's customization features, no company is safe from potential impersonation, and no internet user is safe from being targeted.

[91] Ex. 1 at 218.
[92] Ex. 1 at 222.

In accordance with 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed on June 9, 2026, in [redacted], [redacted].

[redacted]