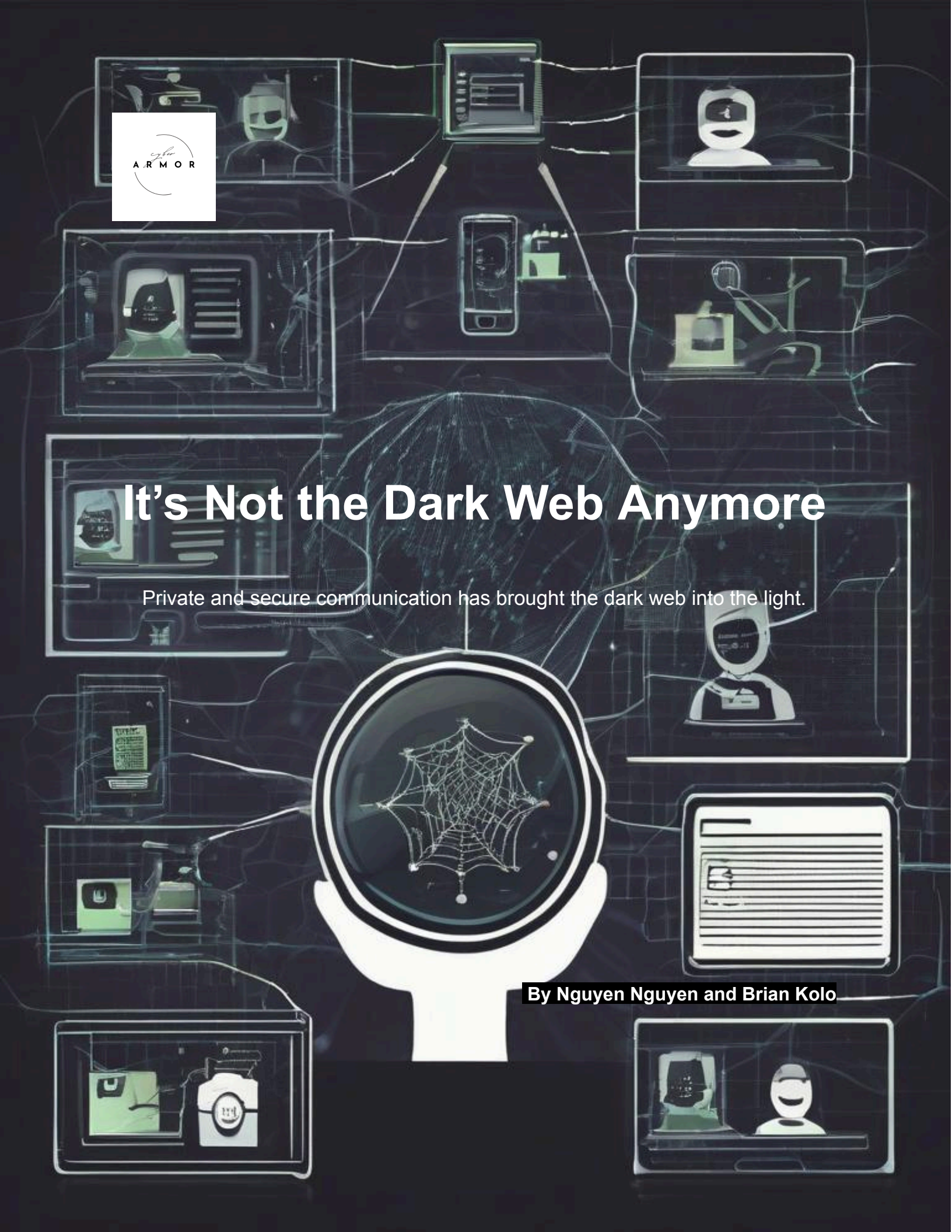


# It’s Not the Dark Web Anymore

Private and secure communication has brought the dark web into the light.

**By Nguyen Nguyen and Brian Kolo**

## 1 Introduction

Online criminal activity has evolved significantly over the past forty years and now includes an international group of criminal actors, some working alone, others in groups, but most connected only through online activity. These loosely coupled groups are difficult to trace to specific people, and even more difficult to stop through international law.

The original cyber criminals were individual actors or small groups with personal connections, and the criminal activity began and ended with them. Stealing from a bank meant these individuals would identify vulnerabilities, exploit the vulnerabilities, and execute a means to leverage the exploits into financial gain.

All of this was done by a lone individual or small group. Both the risk and reward were placed on this group, and all criminal activity was tied together.

Times have changed. Modern financial cybercrime involves many actors across multiple countries, where the various actors only know each other through online handles, and criminal activity cannot be traced to a single person. A fraudulent bank transfer ends with someone using hacked credentials to move money from one account to another, but it begins on another continent with no criminal intent. One hypothetical: A software company offers a bounty program that pays researchers who find security issues with their products. A college student in America discovers a bug in one product and reports this to claim the bounty. The company validates the issue, publishes a fix, and reports the vulnerability to the Mitre CVE database.

Earlier, unpatched versions of the software are still vulnerable. A programmer in Thailand builds an exploit kit that uses the vulnerability to gain access to an unpatched

system and deploys a payload containing a keylogger to monitors logins. However, this programmer doesn't launch the exploit kit. Instead, they post on Telegram offering to sell the kit and eventually sell it to a small hacker group in Germany. This group launches the kit against many targets and collects credentials for many systems including banks. But they don't access anyone's bank account, that's too risky. Rather, they sell these credentials by posting to a forum on Discord. The credentials are purchased by someone in Brazil who verifies access to the bank accounts and the amounts available in the accounts. Fraudulent bank transfers are very risky, and our Brazilians don't want that kind of heat. Again, back to Telegram where they message a connection in Russia who is happy to pay for the verified credentials through Zelle. And here we reach the tip of the cyber spear with a transfer of funds.

This is just one possible path through the cyber-criminal landscape. There are many niche players specializing in identification of vulnerabilities, development of exploit kits, deployment of kits, credential identification, credential validation, fund transfer, brute force attacks, phishkit, phishing campaigns, and malware development. Some of these players have no criminal intent, some are for hire, some sell their criminal product, and others want a percent of the take.

Most importantly, the risk and reward are spread over many people. This means in countries where the risk of cybercrime is high, people can engage in less risky activities not directly connected to transfer of funds. In regions where cybercrime is less prosecuted, criminals may engage in higher-risk activities involving hacking into systems or fund transfers.

The criminal forums have changed as well. Early on, cybercriminals operated on

the fringe, anonymously accessing private forums via Tor with a specific onion address. Access was by invite only and often required a personal connection to vouch for a new member.

Today cybercrime operates openly on the web surface, leveraging technologies accessible to anyone with an internet connection. They use Telegram, Facebook, and Discord to offer their product and services alongside legitimate activities.

There is little attempt to hide or obfuscate their illicit nature. Groups and forums are created as quickly as these services identify them and shut them down, and news of new groups are rapidly posted on other platforms.

When platform administrators find an illicit channel and shut it down, a new channel is created and posted across many other venues. Old players migrate their offers to the new forum until it shuts down and the process repeats.

## 2 Landscape of Dark Web Cybercrime

Cybercrime is no longer relegated to the deep recesses of the internet on invite-only forums. Cybercriminals leverage large tech platforms to advertise, recruit, and promote their brand. Overt promotion of the brand is a key aspect for advertising cyber-capabilities. Sellers explicitly state the illicit nature of their business while distinguishing their tools and techniques from competitors. The illicit nature of the offers are on full display, not obfuscated with code-words or hinted at indirectly. Sellers want to convey their unique abilities to attract buyers and distinguish themselves from competitors. Modern tech platforms are the technology of choice. Different platforms target different aspects of the criminal tool chain.

**Telegram** - General ads, products, solutions, tutorials, and promotions, highly active,

open discussions on criminal activity. Commercial hub of activity where buyers and sellers come together.

**Discord** - General ads, moderately active, limited discussions. Generally felt as less secure than Telegram but still somewhere buyers and sellers can meet.

**WhatsApp -** General meeting place with ads, moderately active, limited discussions. Similar to Discord, less secure than Telegram.

**TikTok -** General ads, low activity, no discussions.

**Instagram -** General ads, low activity, no discussions.

**Twitter -** General ads, moderate discussion. Advertisements directed to followers and redirects to Telegram.

**Facebook -** Leverage personal network to recruit assistance with criminal activity. Posts looking for friends with accounts at specific banks to help transfer illicit funds(mule account).

**LinkedIn -** Activity is private, not openly discussed. Identify insiders to assist in infiltrating specific organizations. LinkedIn can locate everyone in the IT department at the target, and profiles help narrow down candidates.

These forums also provide access to niche skill sets. For example, coupling LinkedIn with Facebook, insider candidates may be privately approached or manipulated into service. LinkedIn provides a list of insiders while Facebook provides a means to privately connect and assess personal motivations.

Telegram is another place where buyers and sellers come together. Advertising is pushed across many platforms including Discord, WhatsApp, TikTok, Instagram, Twitter, and Facebook. These ads are blatantly for illicit activity, and advertisers

promote the effectiveness of their illicit wares.

### 2.1 Dark Commerce

The dark web sellers are indistinguishable from legitimate businesses. These are NOT hidden, they flagrantly advertise and brand their wares with their handles.

They have logos, slick marketing pages, even hosted websites. Sellers offer volume discounts, recurring subscription fees, and even promotional codes.

#### 2.1.1 New Dark Commerce Channels

**Telegram** - Telegram is a free, secure, and encrypted messaging platform. Secure, encrypted messaging has made Telegram the platform of choice for cybercrime advertising. Buyer and seller are able to communicate securely and the buyer is able to provide better real time services. Often when the buyer is unable to log into the purchased accounts, they can call the seller and the seller would guide them through the process.

**Discord -** Similar to Telegram, Discord provided a free, secure, and encrypted message platform. And the buyer can purchase directly from the seller. The seller is able to interact with the buyer and provide a greater customer experience.

#### 2.1.2 Dark Sales

Every aspect of cyber crime is for sale: malware[23], ransomware[22], webpage/script developers[7], credentials[22], credit cards[3], email accounts[6], etc.

Many sellers offer methods to bypass One-Time-Passwords[1][2][3], two-factor authentication[3][7], and 3D Secure[3].

Custom coders are available to develop scampages for phishing campaigns[6][7]. Credit cards are available from American Express[3], Discover[3],

Chase[3][21], as well as every major credit card vendor.

Online payment providers are no exception with accounts available from PayPal[3][6][11], Apple Pay[6][11], and Google Pay[6][11].

Sellers offer bank account credentials[11] across the board from Bank of America[3], Wells Fargo[3][21], and Navy Federal[21].

There are online websites to confirm Personal Identifiable Information (PII)[PII Verification] and credit card CVVs[6].

There is software available for ransomware, malware, password capture, screen capture, and webcam takeover[22].

### 2.1.3 Advertising

Advertising is open and explicit in Telegram. Sellers tout the features of their product in an attempt to solicit buyers. Some examples of the advertisement statements:

- Vouchers References to establish the credibility of the seller[7].
- Credit Card drops sellers post a list of credit cards to establish their credibility[17].
- Superior Superlatives of sellers features over competitors[7].
- Demos See the product before you buy[7].
- Want-To-Buy Requests for purchasing spammers and mail access[14].
- Fast Delivery Buyers get the product immediately after payment is complete[7].
- Ease of Use Product is easy to use, gets into everything[5].
- Customizations Custom scripts and voices to better suit the product to the buyer[2].

- Scripts pre-made scripts for specific financial institutions to quick-start buyers[3].
- Many Users and Components 2600+ Users, 40+ modules[2].
- No Limits Unlimited calls[1].
- Example of Product OTP Bypass Example[8] and repeated requests[9].

### 2.1.4 Features

Sellers promote the features of their products and services to attract buyers and brand their goods, ads and services with their unique trademarks[22][23]. Sellers promote fast availability of their products[7][9][9]. Products provide customization abilities using custom scripts[12] and voices[2]. Sellers guarantee that customizations will not be sold to other customers reassuring buyers that their individualized customizations will not be made available to others[7].

Bypassing authentication schemes is very popular, including bots to bypass OTPs[1][2][3], two factor authentication[3], and 3D Secure[3].

Sellers have pre-made scripts for accessing accounts at American Express, Discover, Bank of America, Chase, PayPal, Apple Pay, and more[3].

### 2.1.5 Countermeasures

As cybersecurity professionals develop counter measures against cybercrime, the cybercrime industry is developing counter-countermeasures. Scampages have countermeasures to block fake login attempts, prevent red-paging, and avoid bots[7]. Malware developers deploy countermeasures to anti-viral software[22].

### 2.1.6 Automation

Sellers use automation to increase their ability to service their clients[1][2][3]. Similar to cyber security professionals, automation decreases response time, increases

reliability, and reduces the staff required. Sellers use bots to automate One-Time Password requests[11], Credit Card Verification Values (CVVs)[6].

### 2.1.7 Online Marketplace

Sellers have established an online presence to advertise their products and sell services. There are online markets to lookup credentials matching buyers criteria, allowing buyers to identify credentials for specific account types[24].

Websites are available to verify PII allowing buyers to obtain information on specific individuals[18]. This provides buyers the potential to pose as the victim and answer security questions or create new accounts with the victim's identity.

Phishing attacks are automated as well. Attackers send a list of email addresses to a bot that automatically sends a phishing email to the targets. Attackers previously setup scampages linked in the email campaign that collect credential information from victims. The scam page automatically sends the captured credentials to a Telegram channel using the Telegram BOT API. The attacker determines when to use the captured credentials, and uses an OTP bot to automate the bypass of a One-Time-Password, leading to an account takeover.

### 2.1.8 Subscriptions

Sellers offer subscriptions to products, no different from legitimate businesses[1]. Subscriptions provide an annuity stream for the seller while providing a means for the buyer to pay over time.

Sellers offer a variety of subscription models including Service Level Agreements[2] and discounts for long-term paid-up-front[3].

### 2.1.9 Payment Options

Sellers typically prefer payment via digital coin. Whereas credit card transactions may be reversed, digital coins are lost once transferred. Digital coins may be quickly distributed internationally across multiple accounts. Most digital coins are accepted including Bitcoin, Ethereum, Lite Coin, Dai, Tether, Matic, USD Coin, and Bitcoin Cash[4].

Sellers also use middlemen to facilitate transactions[7][10]. These middlemen effectively operate as an escrow service where payment is made by buyers to the middlemen and only released to sellers once the product or service is delivered.

#### 2.1.10 Franchise and Pyramid Schemes

Criminal franchises are offered as well. BOT sellers offer to sell their BOTs for others to resell to other buyers. Organizations that use credentials offer to sell and extra credentials they are not planning to use[15].

#### 2.1.11 Discount Pricing

Sellers offer discounts for volume purchases and long-term subscriptions[3]. Lifetime subscriptions are also available[4] as well as low vs. high end packages for standard/VIP members[20].

#### 2.1.12 Help and Support

Sellers offer a variety of support options for their products to help customers take full advantage of the products they are purchasing:

- Community Support Chat with a large user community[2].
- FAQs explain the product and answer common questions[10].
- Custom Support Seller will review and make changes to products that do not perform as expected[10].

- Command Help List of commands for software[12].
- Private Chat Private chat training[20].
- Tutorials are available for credit card theft, how to prevent canceling, direct deposits, bank log, Tax Returns, bill pay, wire transfer, Robinhood[16]
- Online Learning Hacking, antivirus prevention, traffic leakage[20]

**2.2 Dark Recruiting**

Social media is proving an effective means to recruit help with illicit activities. Friends connected on Facebook and LinkedIn provide a trusted source of accomplices. When a friend asks to deposit money into your account if you simply transfer it out (minus a fee of course), what could go wrong? The intimate nature of the request provides a false sense of security. My friend wouldn't be involved in some major criminal activity, nobody is getting hurt, this seems like an easy way to make a little money.

Communities like Facebook provide a means for people to send out requests to friends, directly or in groups, to recruit accomplices. Interactions with friends help identify people who are more likely to engage in these activities, and also provides a forum to normalize the activity leading to future accomplices. Criminals can post how well they are doing and how easy it is to make money, even posting pictures of large amounts of cash. This generates envy with friends who want to be a part of the easy money.

Employment based sites such as LinkedIn may provide an appearance of legitimacy to the offer. Criminals can create fake companies that appear legitimate and post adverts as job opportunities. These jobs are actually for illicit activity such as mule

accounts or launching phishing and/or malware campaigns.

### 2.2.1 Mules

Criminals use Facebook communications to solicit account-holders at specific financial institutions[25]. Money is transferred into these accounts, then transferred out, and pays a fee for the access[26][27].

### 2.3 Dark Automation

Dark crime leverages sophisticated software and cloud platforms. Software agents are deployed in cloud-based infrastructure providing customers a means to quickly access these services using standard software interfaces.

Telegram is a favorite of dark automation. BOTs are deployed using sophisticated organized activity a) Ransomware SEC b) Automation OTP. Hackers steal checks, steal USPS keys, steal mail, distributed across the country.

## 3 Questions

***Why are cyber crimes moving from the dark web to open discussions***?

Security Platforms like Telegram provide a secure means to discuss criminal activity without revealing the identities of the actors. This feeling of security is leading to more open and explicit discussions.

**Privacy -** Telegram also assures individual privacy. Telegram saves only the information required to provide their service. They don’t need your actual name, address, or any other identifying information. Even if law enforcement gets a warrant for Telegram's data, there is nothing saved to lead them to the perpetrator.

***Is it really a crime****?*

Mule accounts or simply allowing someone to run a program on your computer

may not feel like a major criminal activity. Simply having money deposited into your account then transferring it to another account, why would that be illegal? This leads to normalizing the activity and feeling that simply doing things that are otherwise legal isn't really a crime.

**Safety in Numbers -** Open communications about criminal activity makes it seem that it is no big deal. When these open discussions are not shut down and nothing bad seems to happen, people may feel that this is criminal. There is a sense of safety when many people are openly engaged in something leading to others joining as they feel this is safe.

***Why aren't these criminals prosecuted?***

**Jurisdiction -** Police are less likely to investigate outside their jurisdiction. Illicit activity leveraging social media isn't located in a single jurisdiction. These activities are often spread over a wide geographic region, potentially across multiple continents.

**Small/Non-Violent Crime -** Investigative resources are focused on criminal activity that immediately impacts the community. Scam based crimes may be prioritized lower because the amount stolen is often low ($500 or less) and does not include a threat of force or violence.

**Unclear Laws -** Some countries don't have laws covering cybercrime, while others have laws that are little testes and unclear. Investigators may be reluctant to spend a time investigating activity where they are unsure if it is actually illegal or if it would be prosecuted.

**Bribes and Organized Crime -** Bribes and threats from organized crime is another reason criminal cyber activity is not prosecuted. Especially when the victims

are in another country, investigators may feel that these crimes don't actually hurt their community and should remain someone else's problem.

**State Sponsored** - Some cybercriminals are working for their governments and have no fear of prosecution. State-sponsored cyber-activity is thus not actually illegal and there is no fear of prosecution for these actors.

**Anonymous** - Determining who the actors actually are is difficult and likely requires court ordered warrants against social media companies to release the identities of the perpetrators. However, even if law enforcement were to obtain a warrant, the account information is likely fraudulent and may not significantly aid an investigation.

## 4 Conclusion

It's no longer the dark web. Cybercrime is no longer relegated to unsearchable private forums hosted in lawless countries. Cybercrime is taking place in the open, leveraging websites with billions of traffic hits, and easily accessible to anyone with internet access.

Secure online communication has brought the dark web into the light. The increase in demand for privacy has created an opportunity for cyber criminals to exploit secure private channels to conduct illicit activity with little fear of repercussions. Criminals not only openly discuss their activities, they sell their services and are able to advertise to a worldwide audience. There is no need to obfuscate the talk: Criminals explicitly state what they offer, how much they charge, and deliver their services on the same computer infrastructures that millions of people use every day.

The criminals also flaunt their success. They post pictures with loads of cash

obtained from illicit activity, which creates jealousy and envy with the audience. Some are interested in joining the criminal commerce, and there are many ways to engage. A simple way to engage is to offer access to their bank account for loading and transferring money. Once complete, they report their account as hijacked and collect their fee with little risk.

On the other extreme, they may purchase a scam page and launch a phishing campaign to collect credentials from unsuspecting victims. They can use these credentials to take over an account and drain the funds.

In between these extremes are many options with a wide variety of risk and reward. There are programmers looking for new software vulnerabilities, hackers creating exploits, software developers creating BOTs, phishers/smishers selling credentials, money launderers buying account access, account-holders selling account access, and many many more.

Flaunting success draws more people toward criminal activity, and open discussions normalizes it. It looks easy, profitable, and risk-free.

More and more people join the online community every year. More and more countries are bringing inexpensive internet access to an ever growing audience. And more and more people will be drawn into criminal commerce. Things are going to be different. We need to adapt to a changing world of cybercrime.

## 5. Appendix

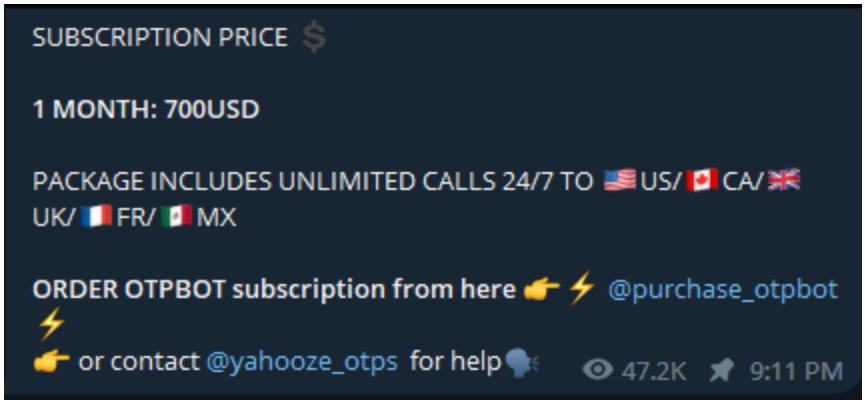


**Figure 1: Subscription tool used to bypass OTP.**

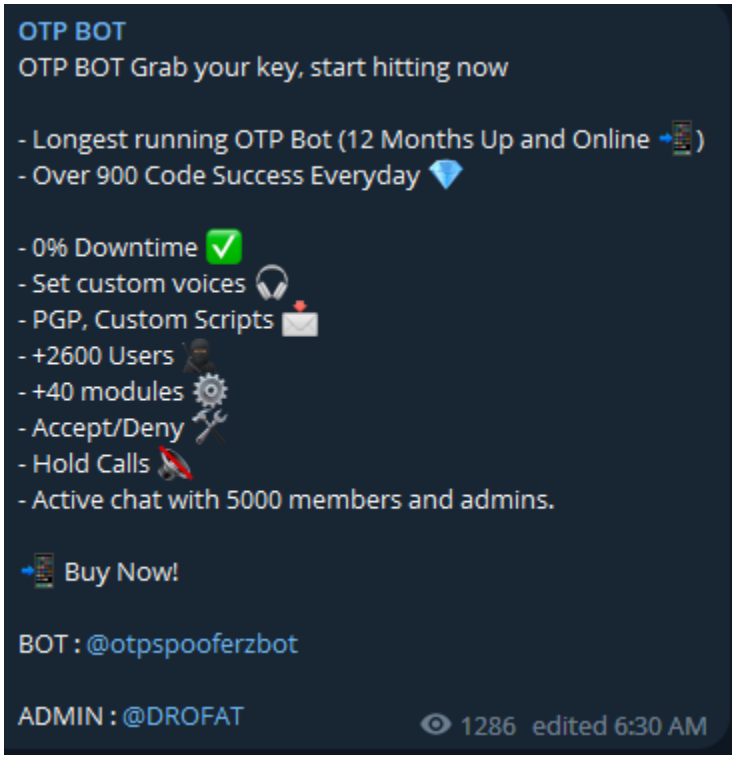


**Figure 2: Advertising chat support with other subscribers, customizations, and large user base.**

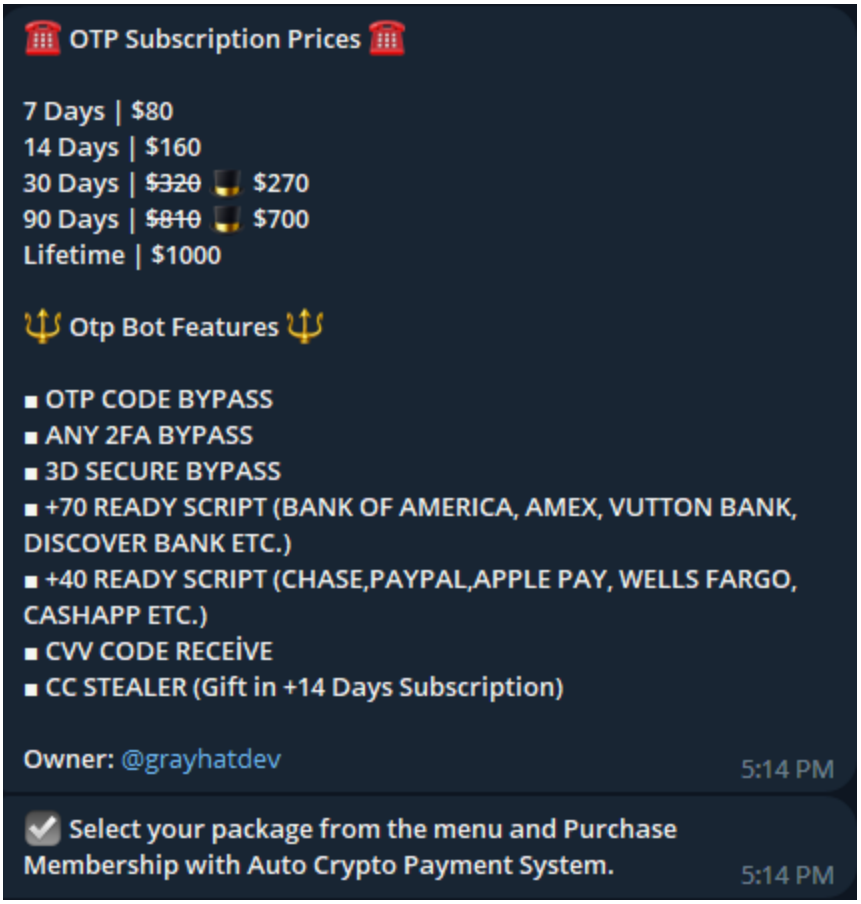


Figure 3: Advertising subscriptions to OTP bypass service.

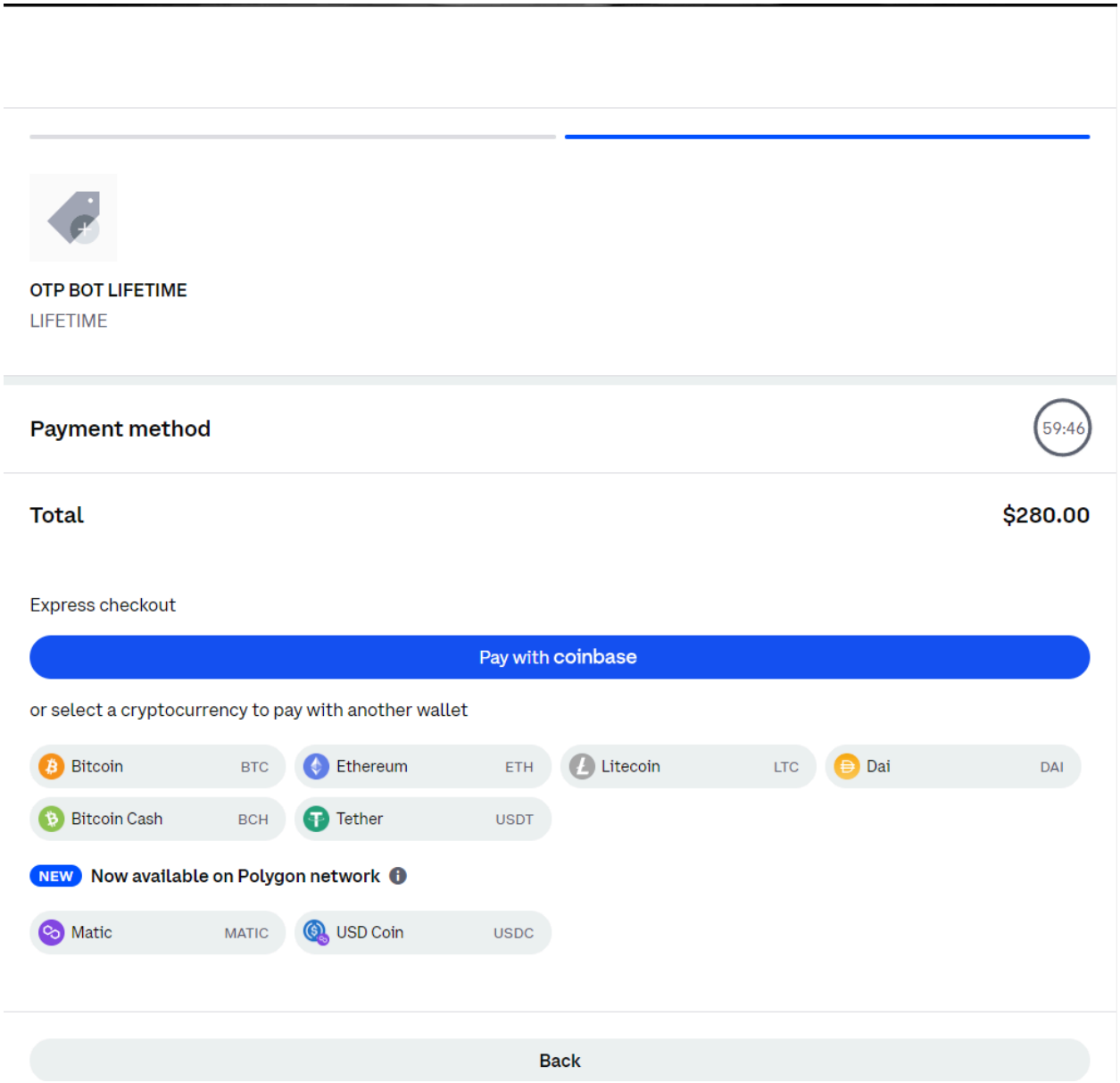


Figure 4: Several coin payment options.

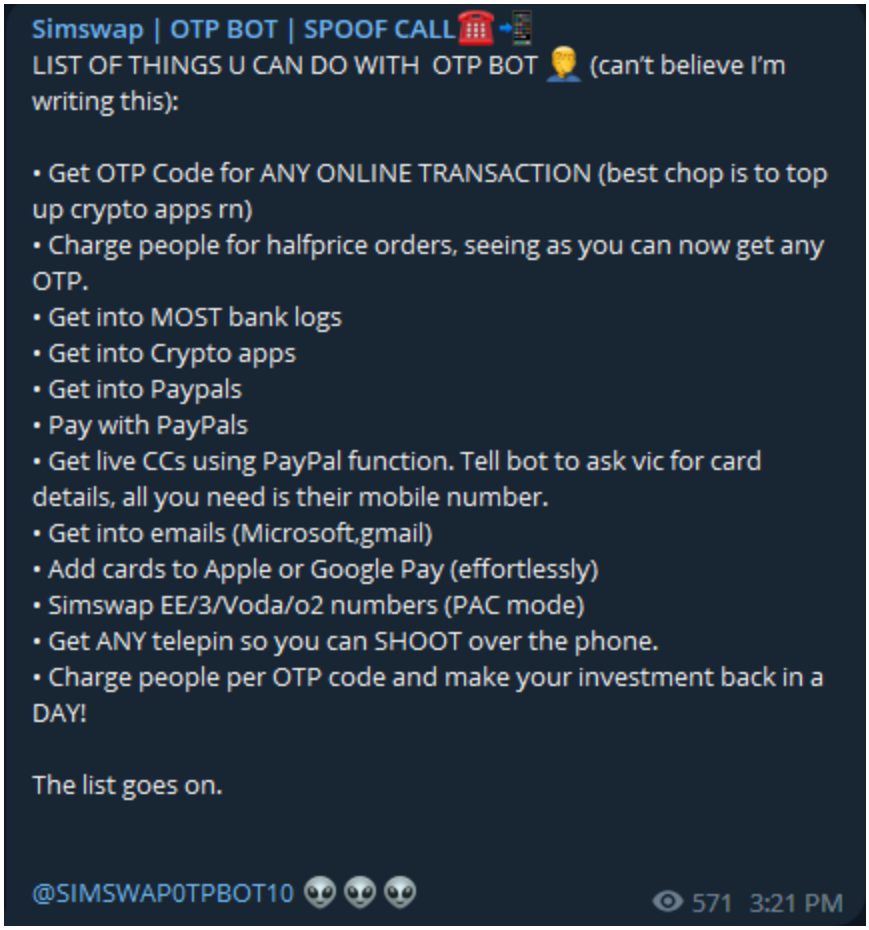


Figure 5: List of features for using this tool over competitor tools.

☠ Death OTP ☠
SCAMPAGE CODING SERVICE

1)Regular SCAMPAGE
2)Live Panel (Command/OTP SCAMPAGE)
3)True login/cookies (SCAMPAGE)

=> REGULAR PAGE GOOD SIDE :

-Normal login/otp/card etc page
-Send data to mail/telegram
-Regular hosting can use cpanel
-Best for big amount bulk spam

=> BAD SIDE OF REGULAR PAGE :

-Can't bypass 2fa
-Invalid login issues
-Can't get correct security question
-Can't get cookies

=> Live panel GOOD SIDE :

-Bypass 2fa/security question
-Valid login/Mail access only
-Can be use for cashout
-Can block fake login/info
-Can get cookies also
-It's can bypass any hard big security

=> Bad SIDE OF Live Panel PAGE:

-Can't handel too much victim same time
-U need stay online during your job

=> True login/cookies PAGE GOOD SIDE :

-Its full auto (don't need stay online )
-Its work same as original site/bank
-Bypass OTP
-Capture Valid login Only
-Capture Log balance and send to telegram
-Bypass mail access
-Victim can't submit any wrong info
-Auto Cashout/Auto Bypass wire otp

Note: For true login page you need to provide your drop access
We make all country's page

Ok, for see the demo come inbox
Price depend on the page u want and the site security

@pagescript 316 4:24 PM

Figure 6: Scampage Coding Service

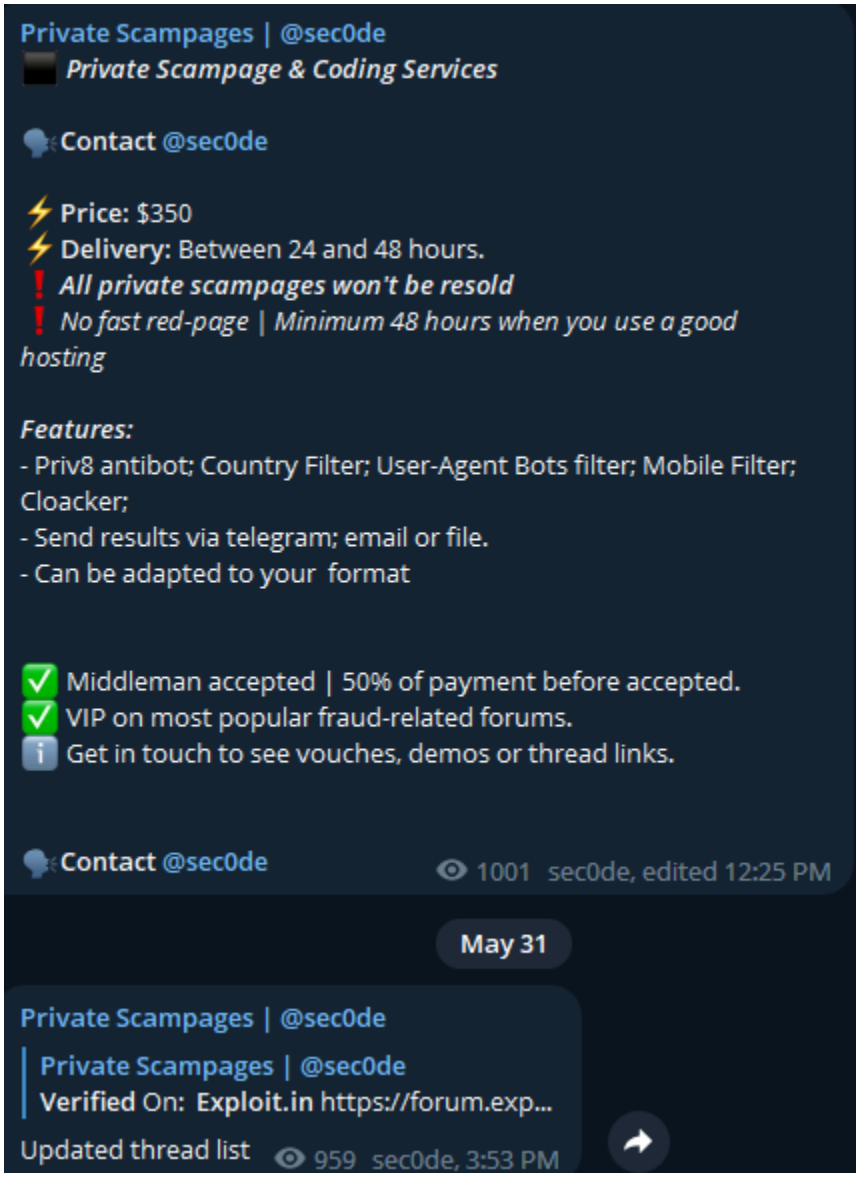


Figure 7: Website to receive credentials from a phishing email.

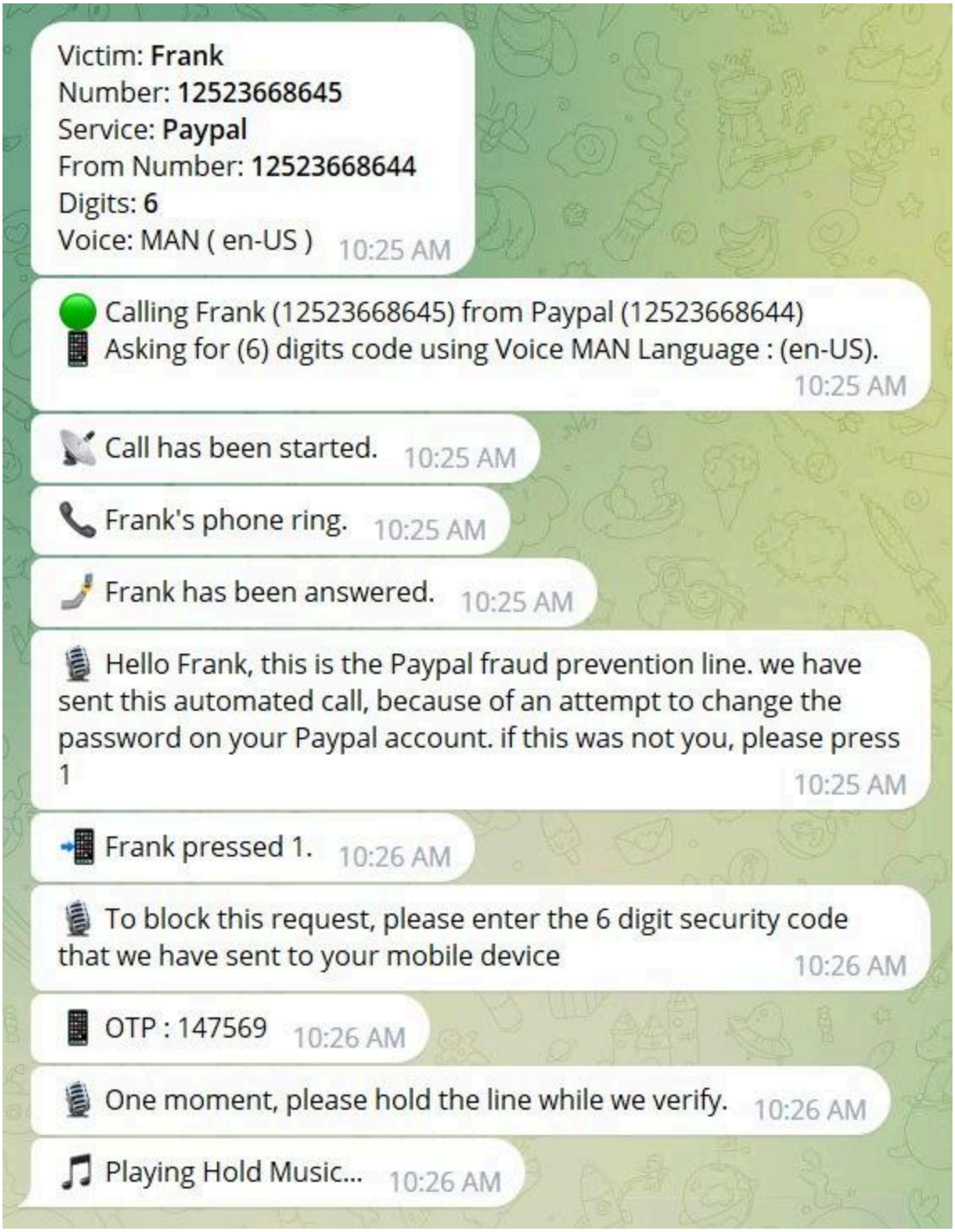


Figure 8: Sample showing the steps in obtaining an OTP code.

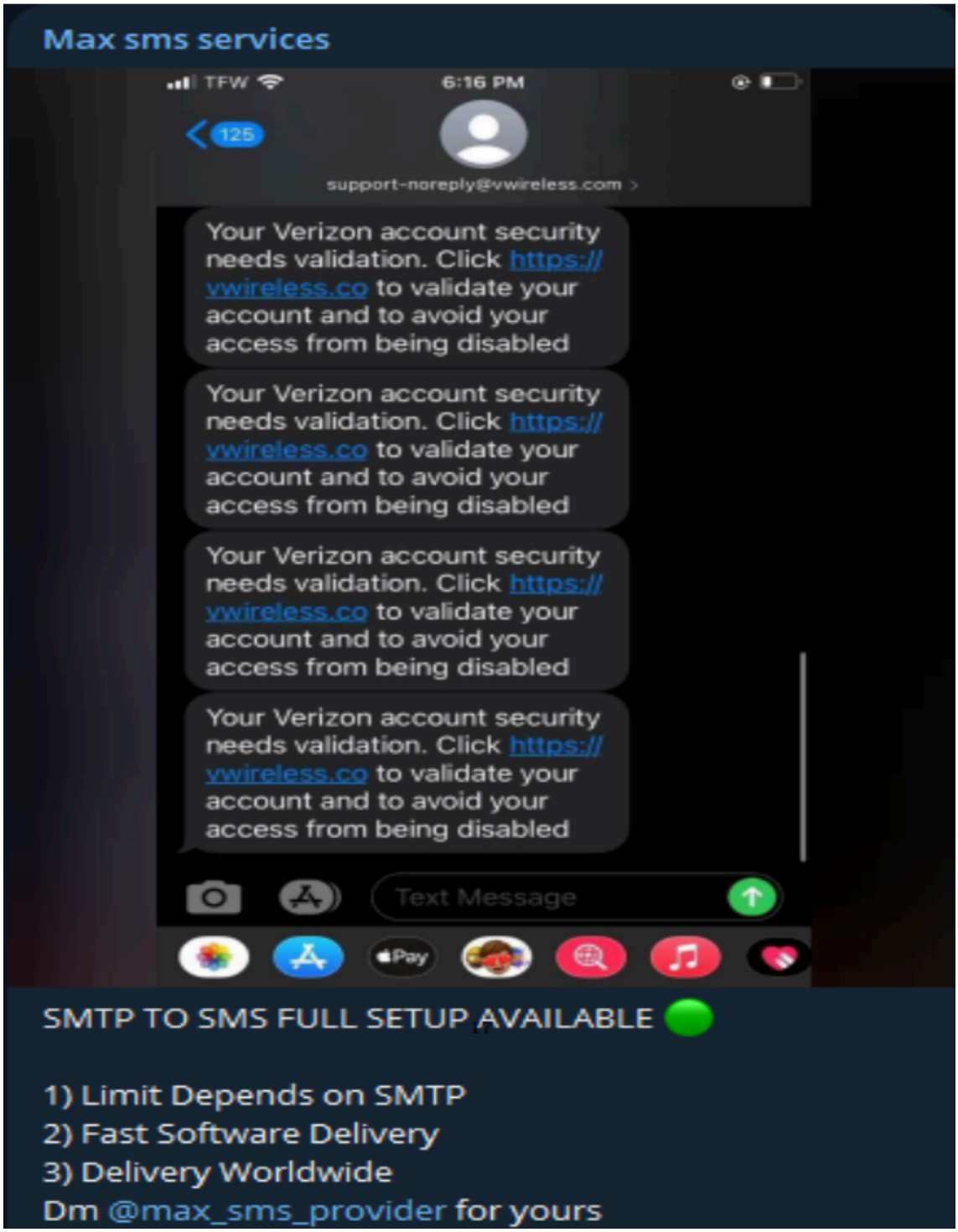


Figure 9: SMS Phishing Setup

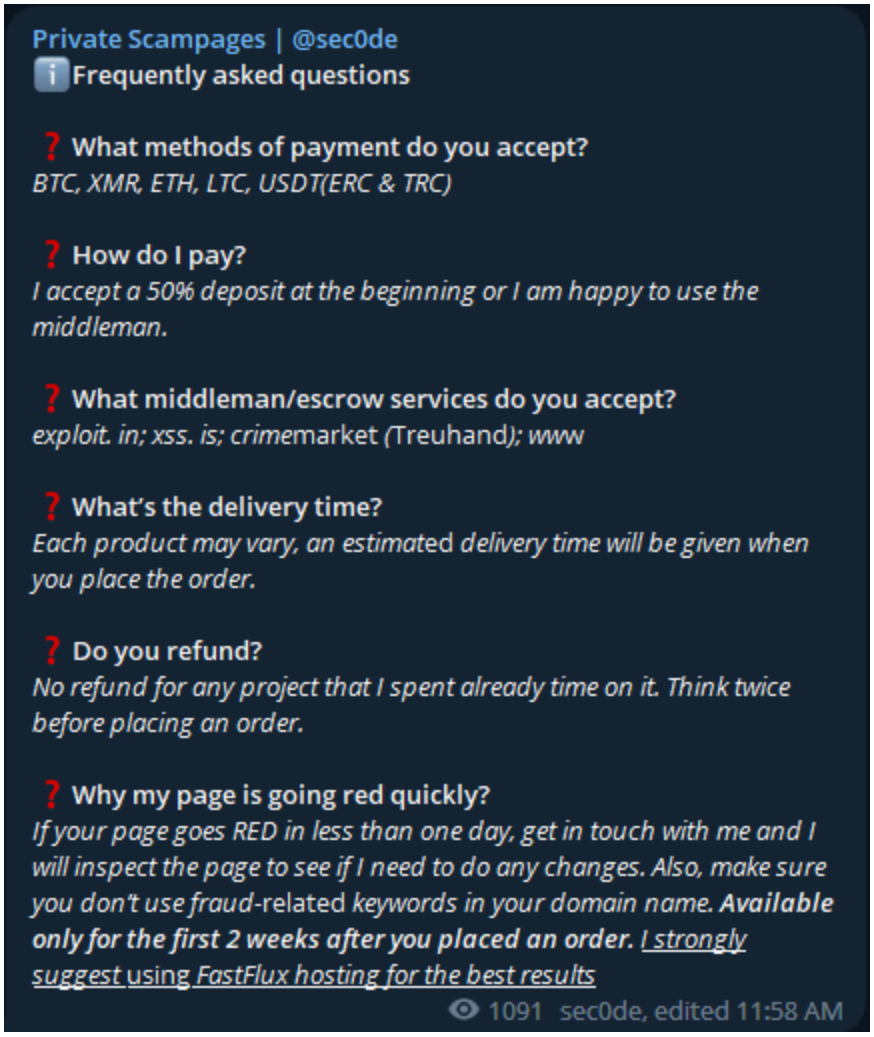


Figure 10: Support FAQ

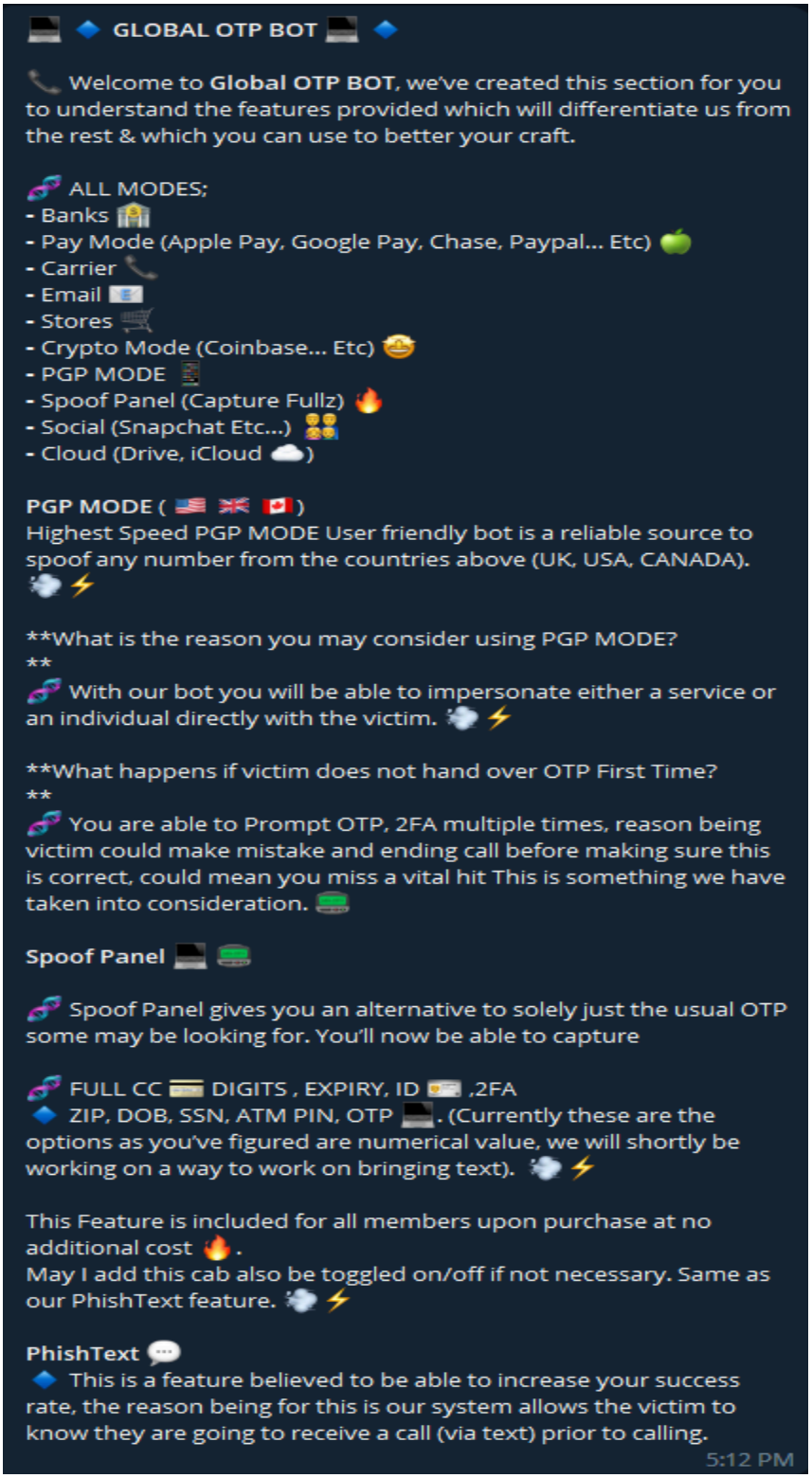


Figure 11: Global OTP Service Advertisement

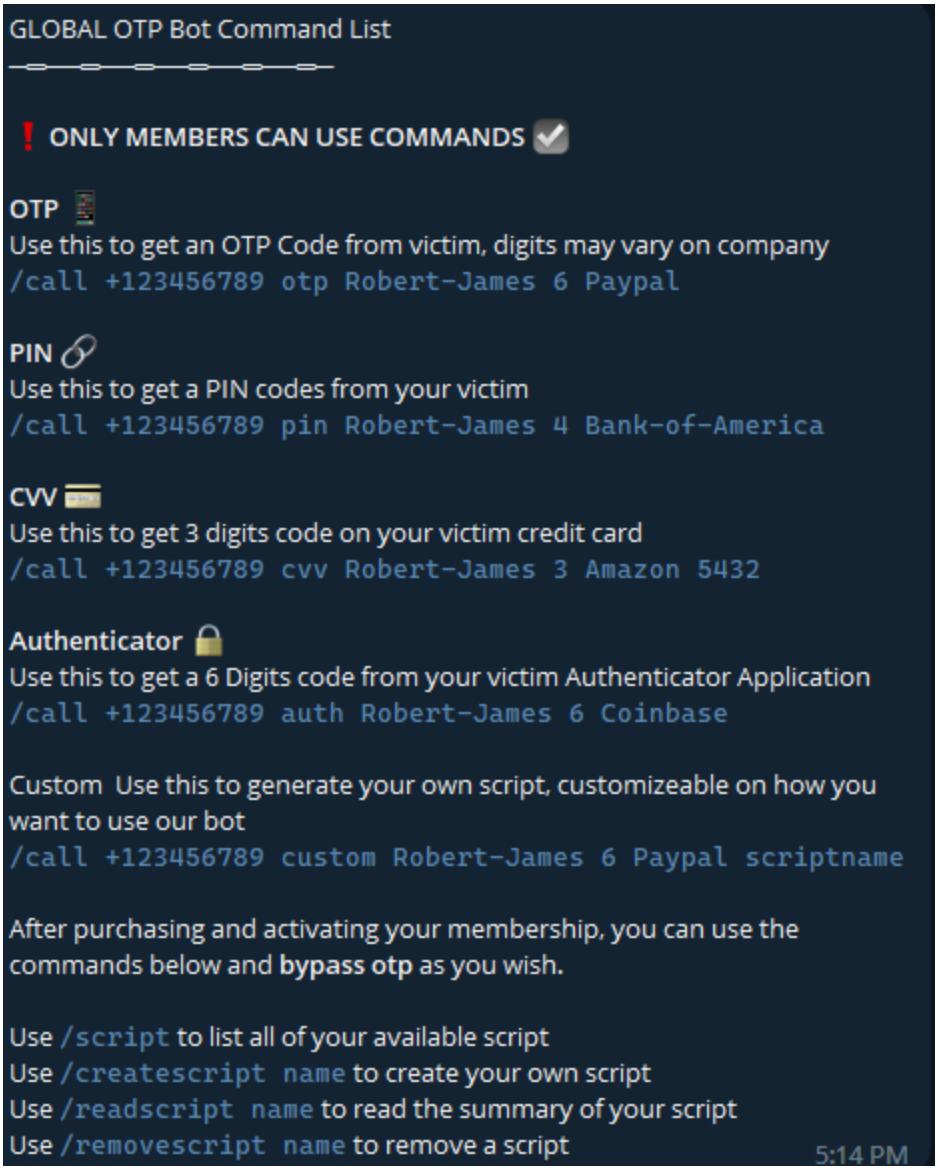


Figure 12: Support document with list of available commands.

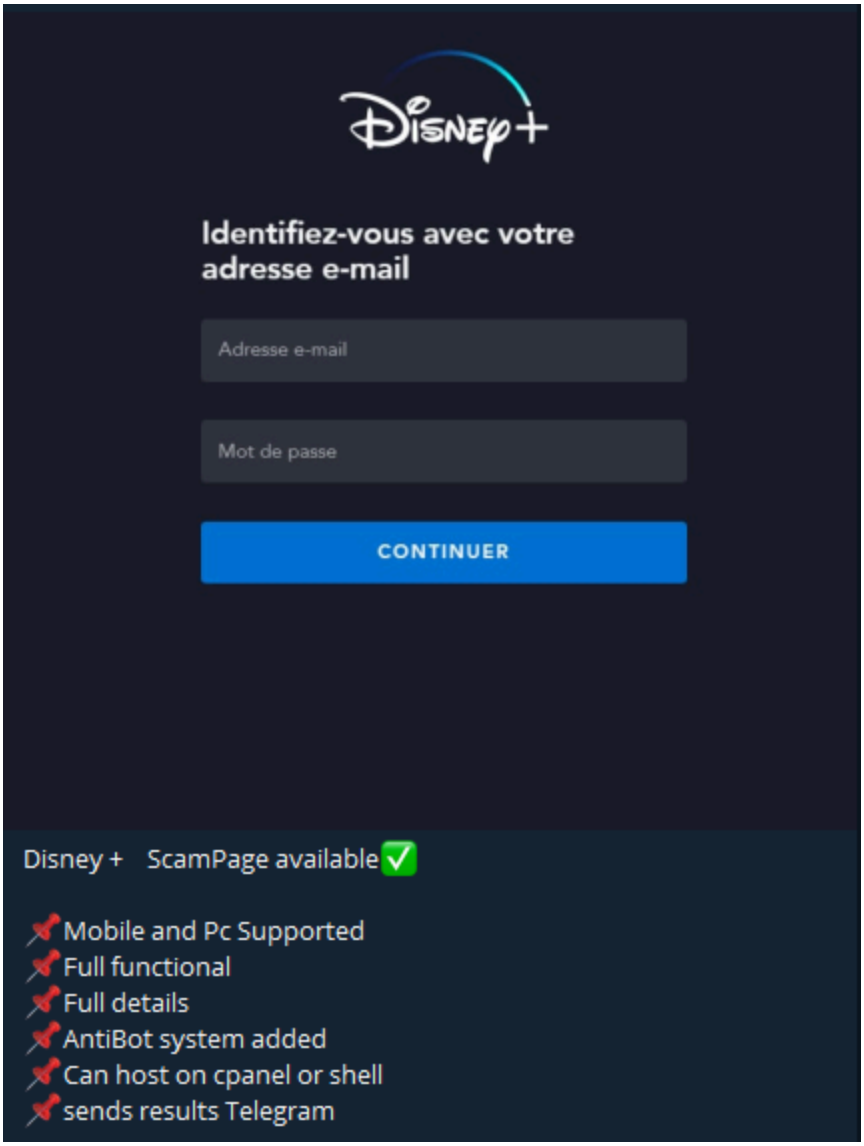


Figure 13: Example of a scampage used in phishing.

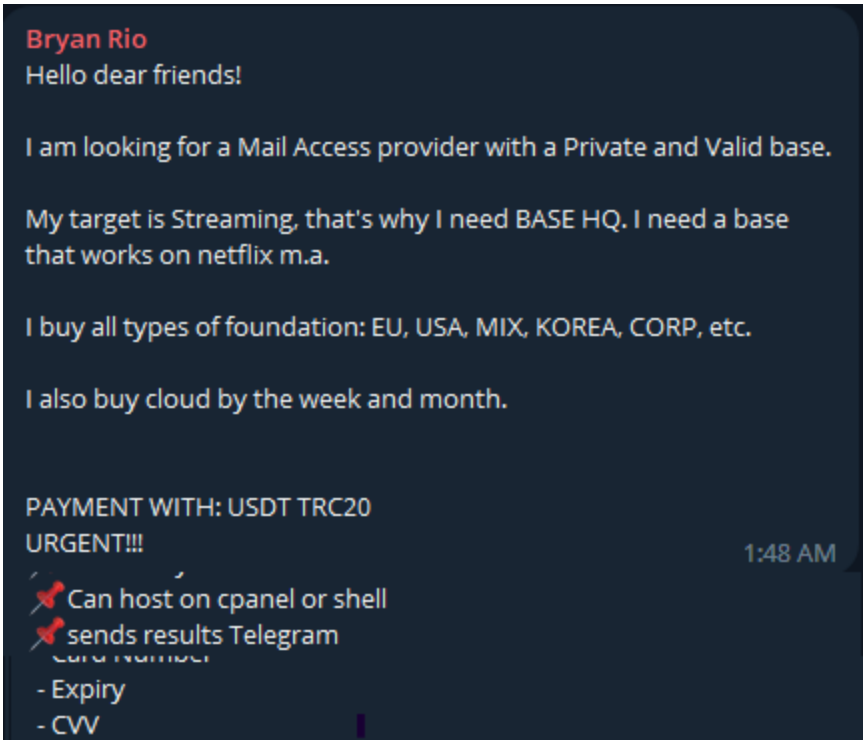


Figure 14: Buyer looking to connect with a seller.

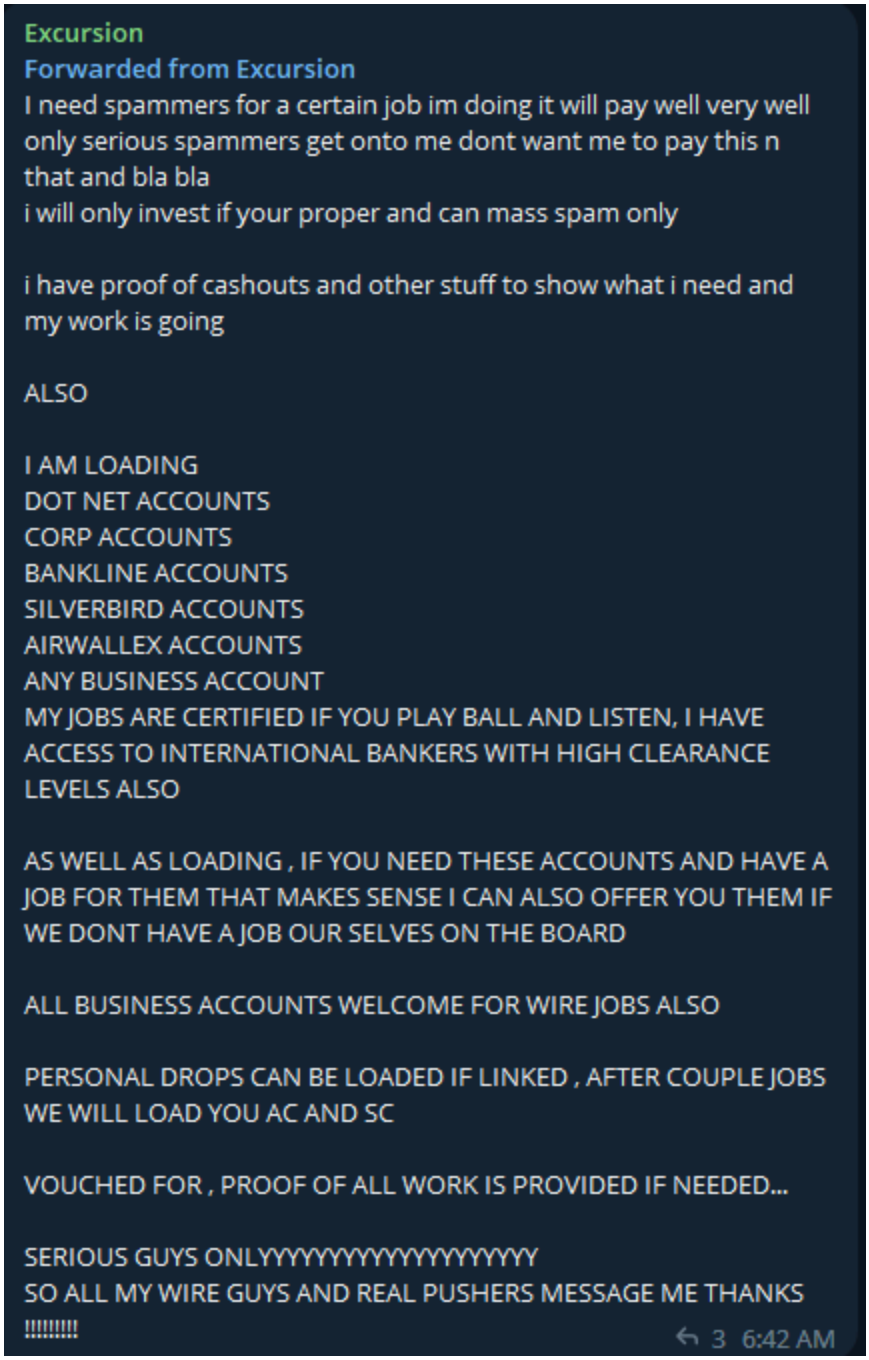


Figure 15: Buyer looking for a spammer seller.


Figure 16: Fraud Tutorial/Methods

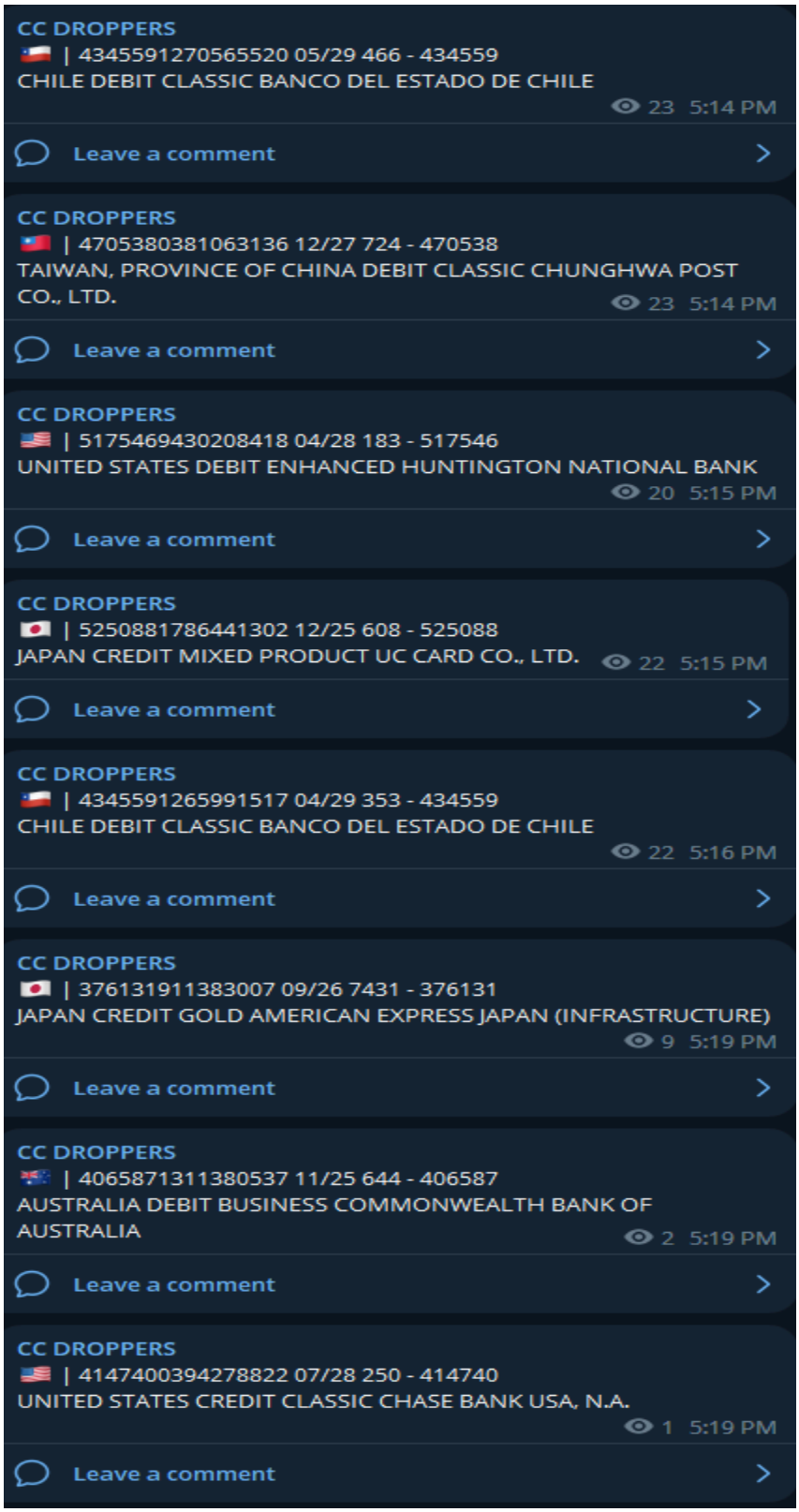


Figure 17: Free Credit/Debit Cards

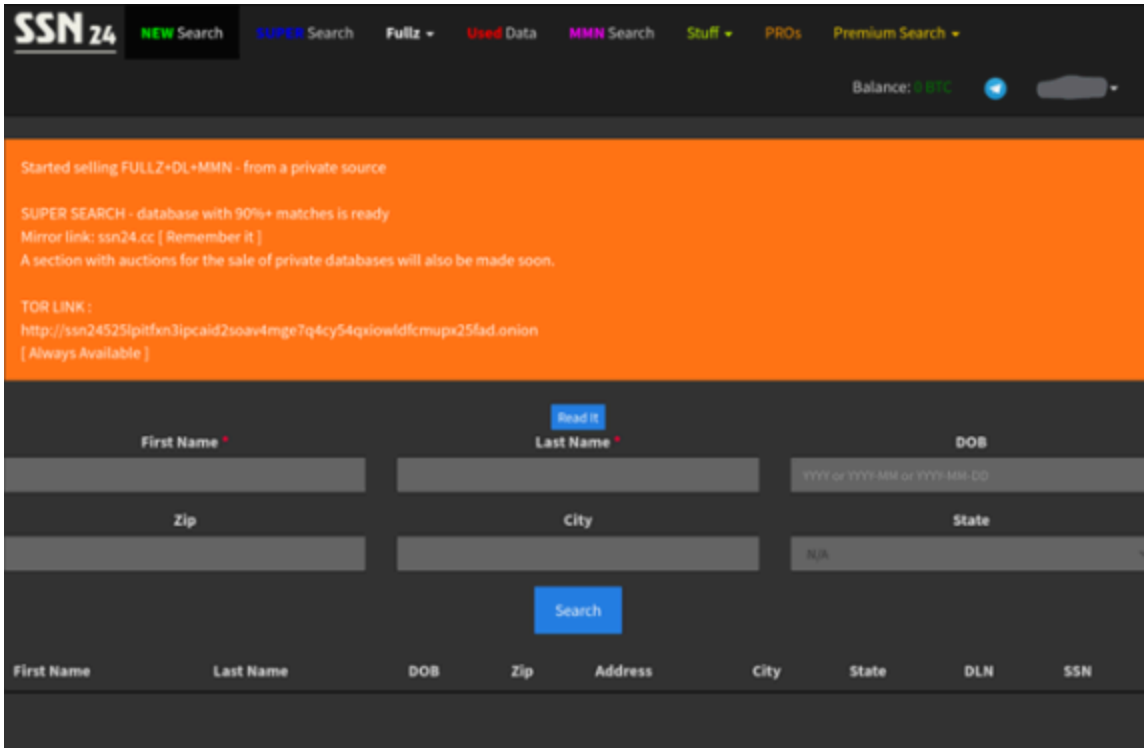


Figure 18: Website that allows lookup of PII.

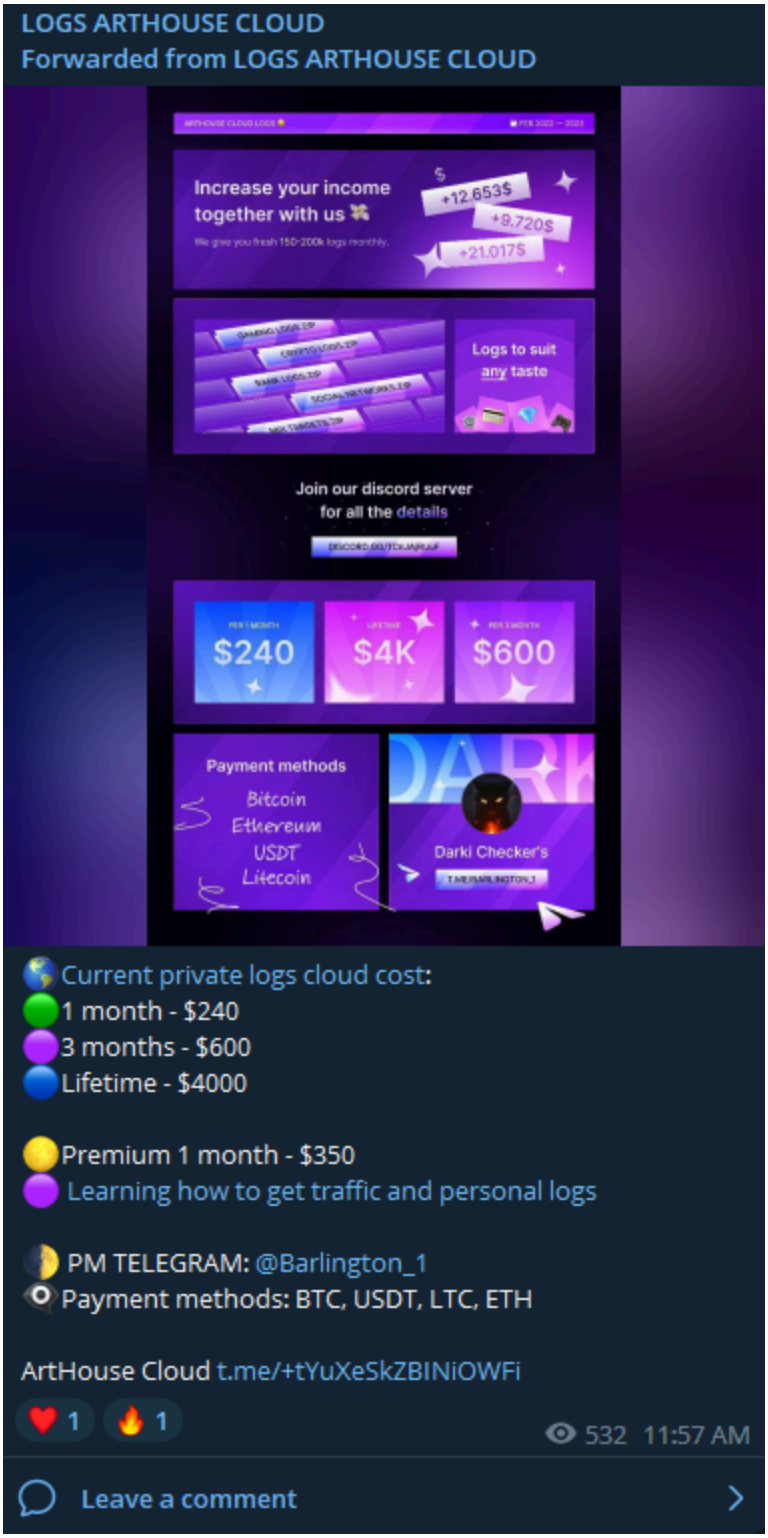


Figure 19: Subscription Model for Personal Logs

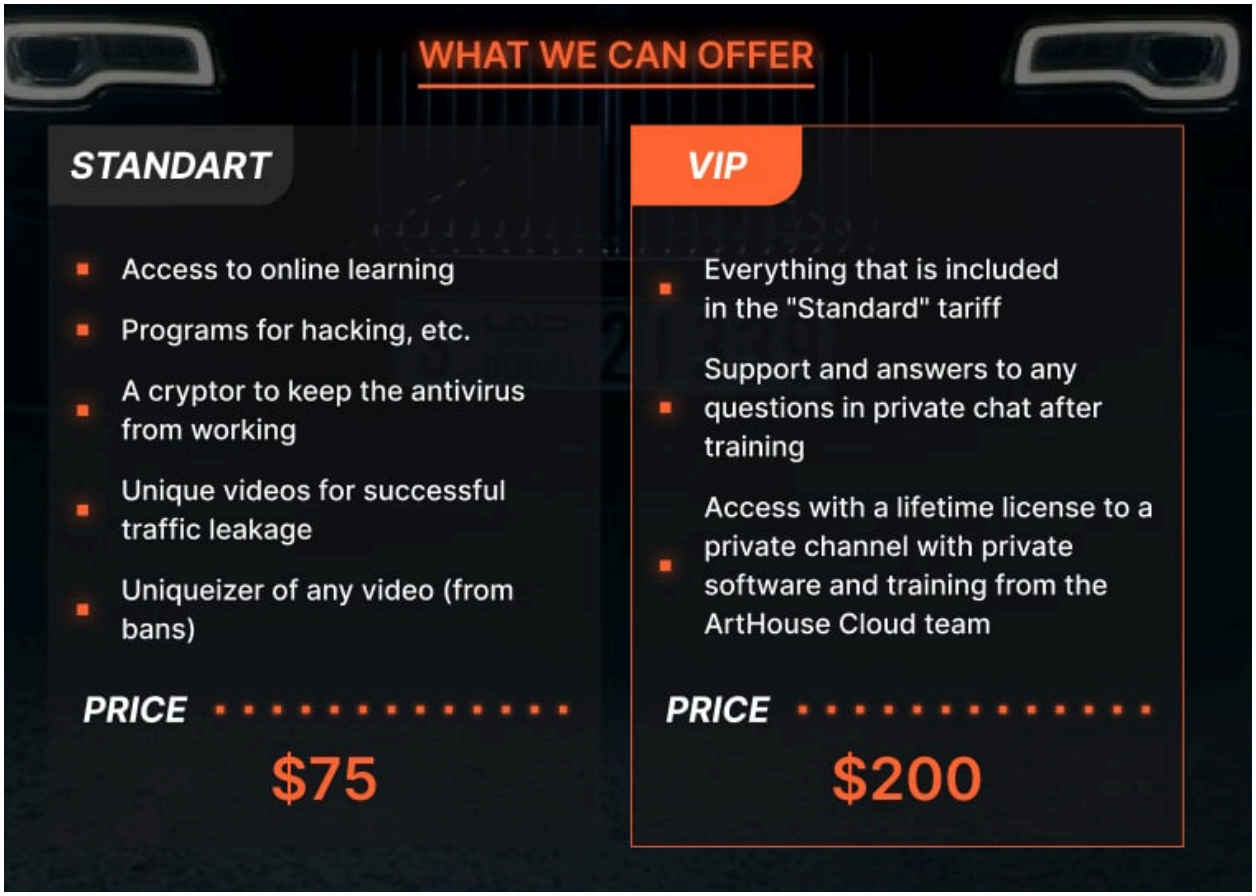


Figure 20: Two-tiered pricing.

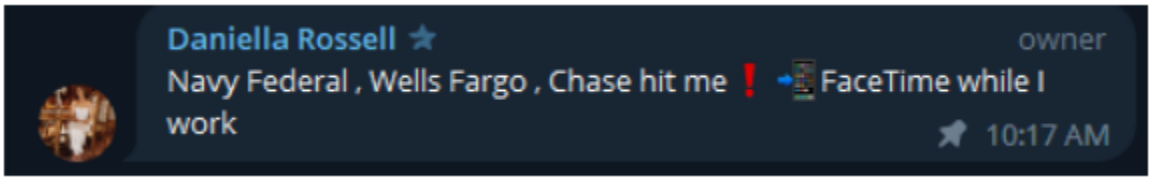


Figure 21: Specialization focusing on specific banks.

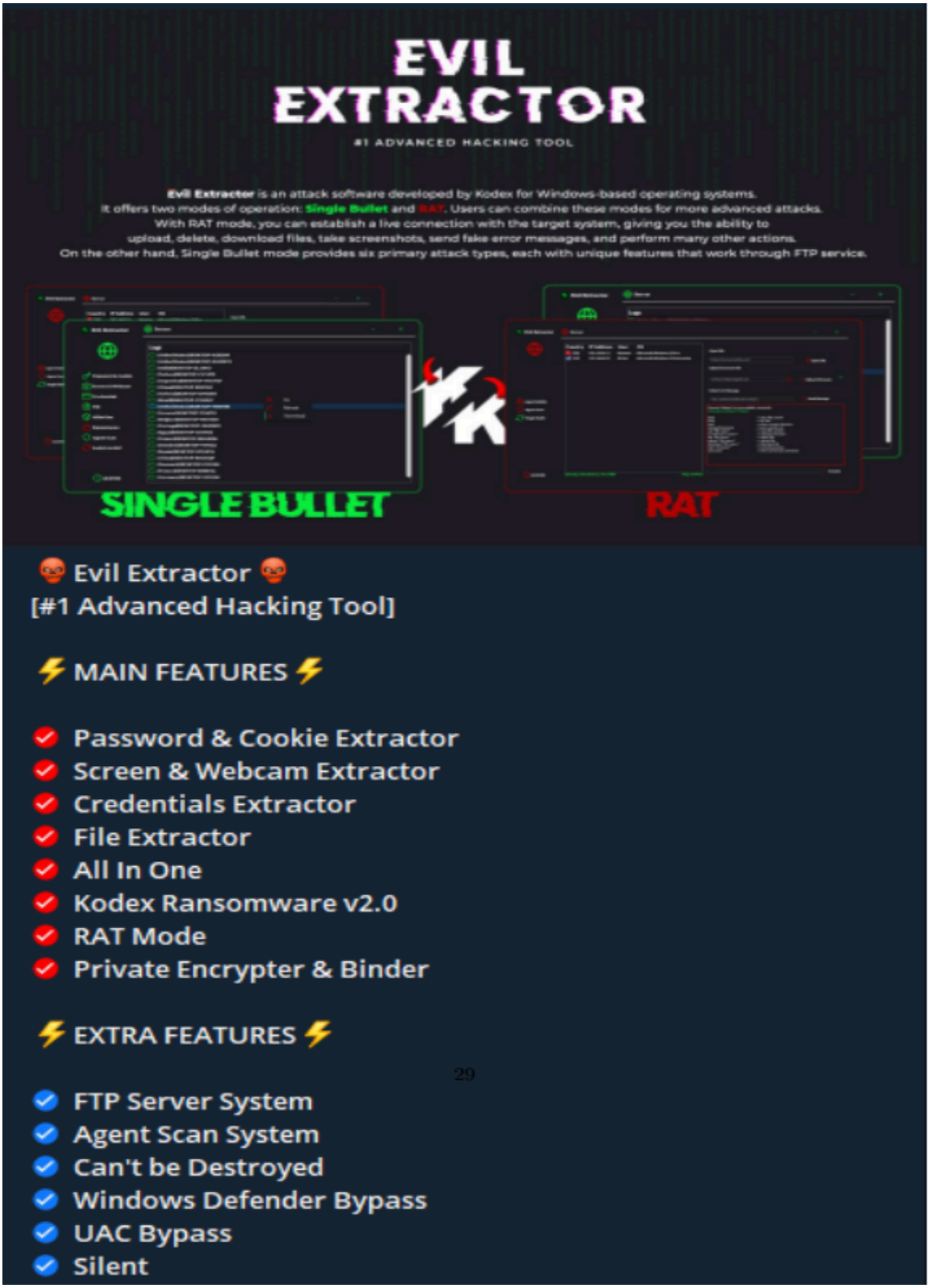


Figure 22: Rat & Ransomware Tools For Sale

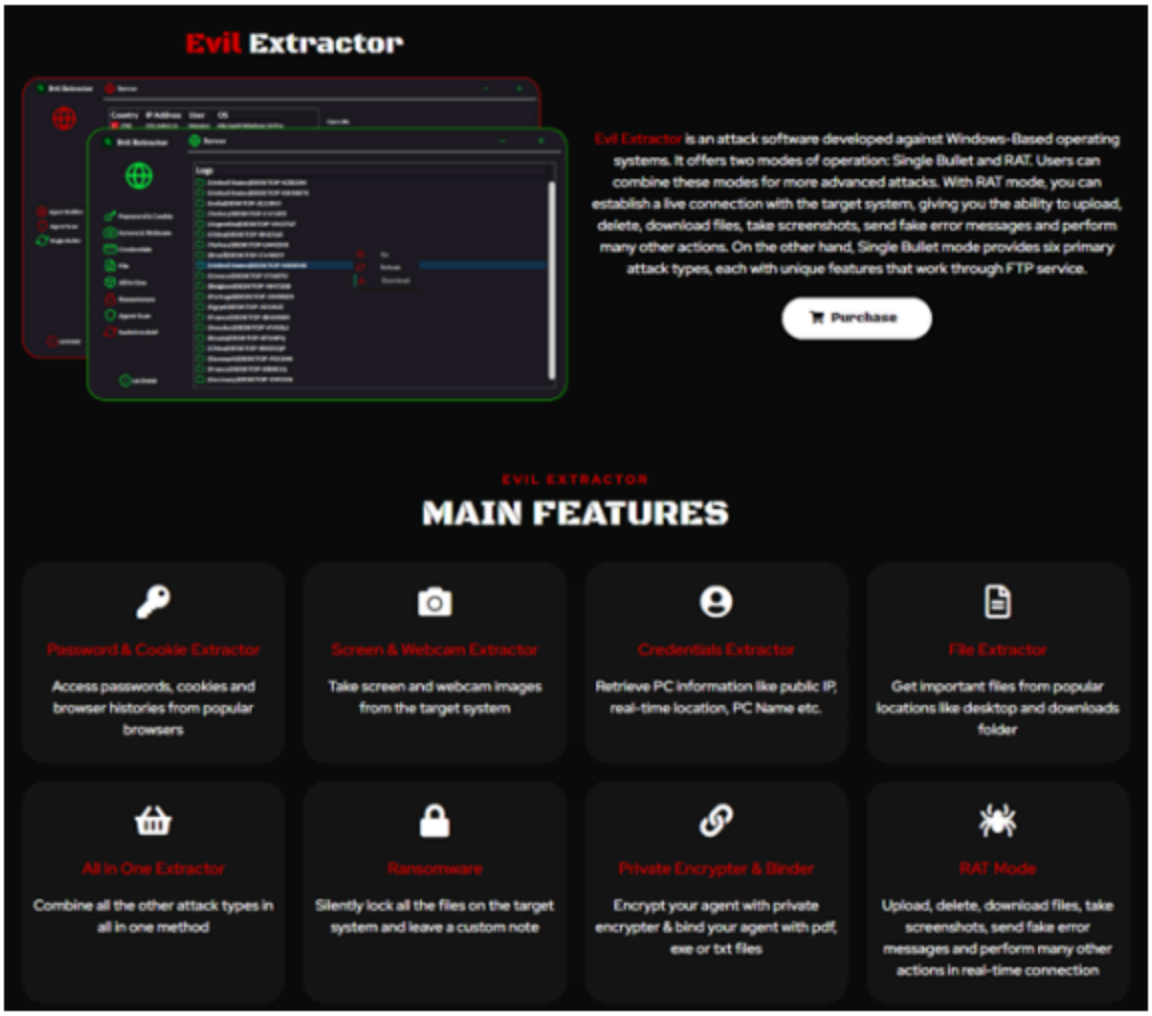


Figure 23: One-pager marketing with branding and logos.


Figure 24: Online market for credentials.

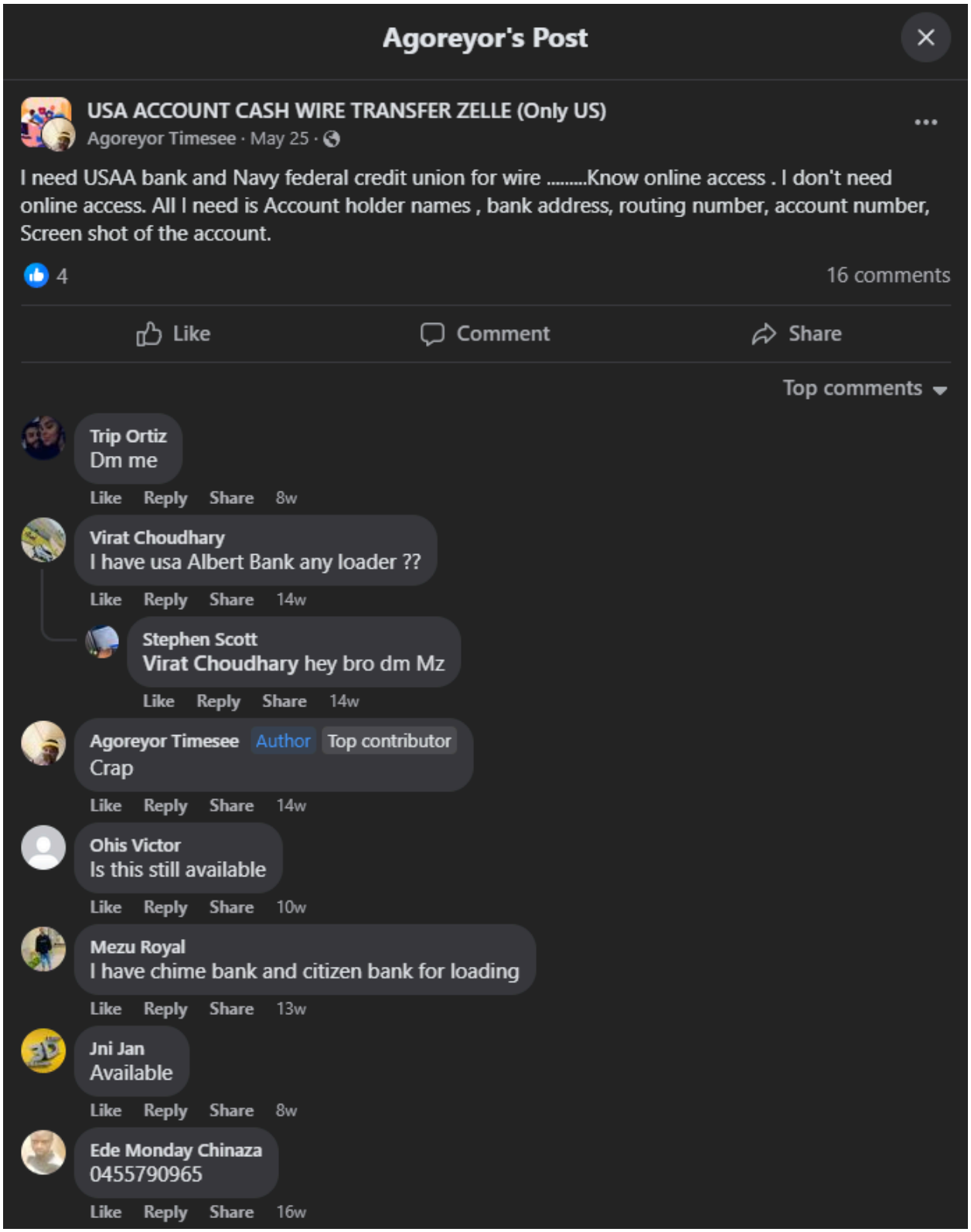


Figure 25: Recruit account-holder for wire transfer.

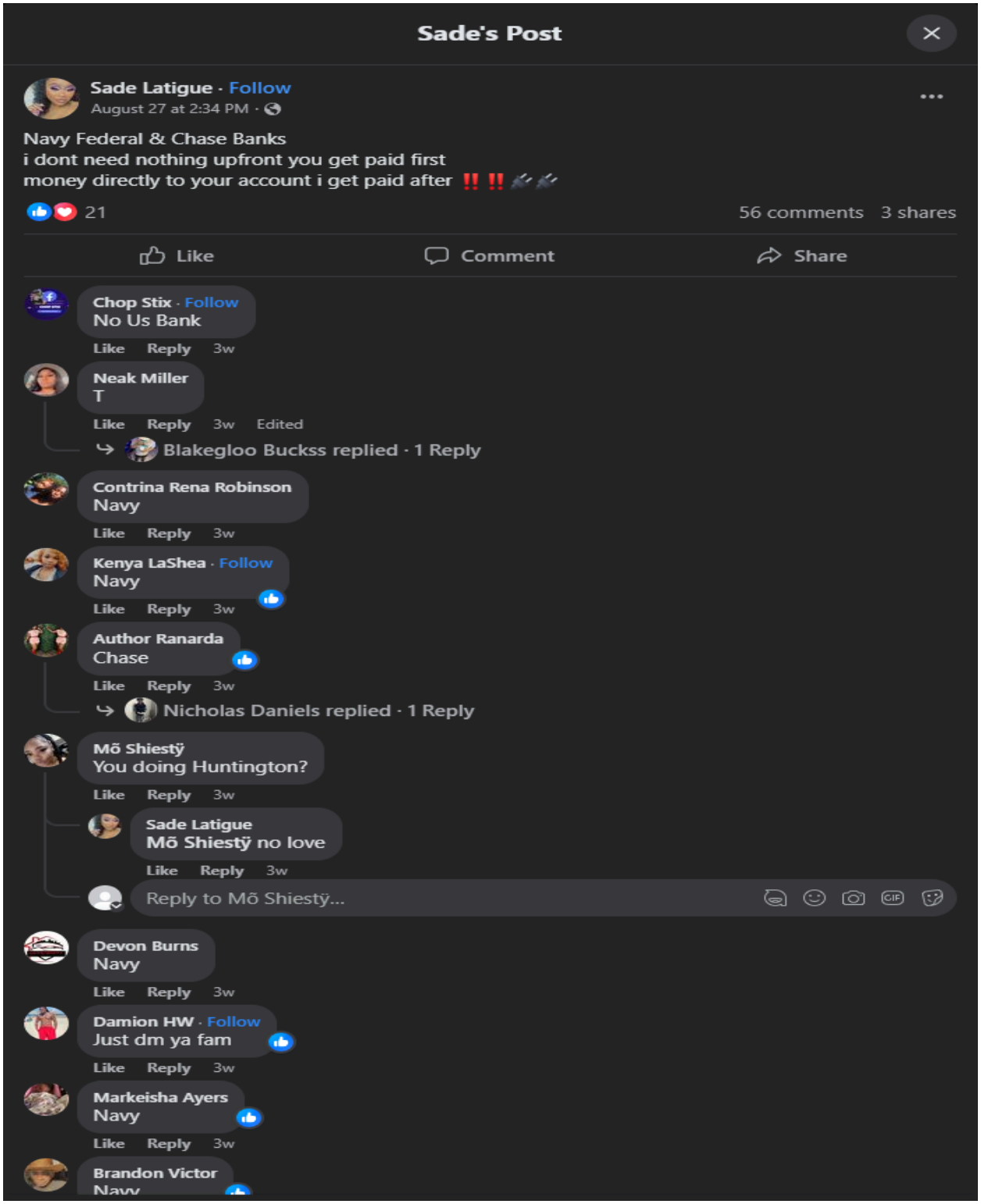


Figure 26: Mule Recruiting on Facebook

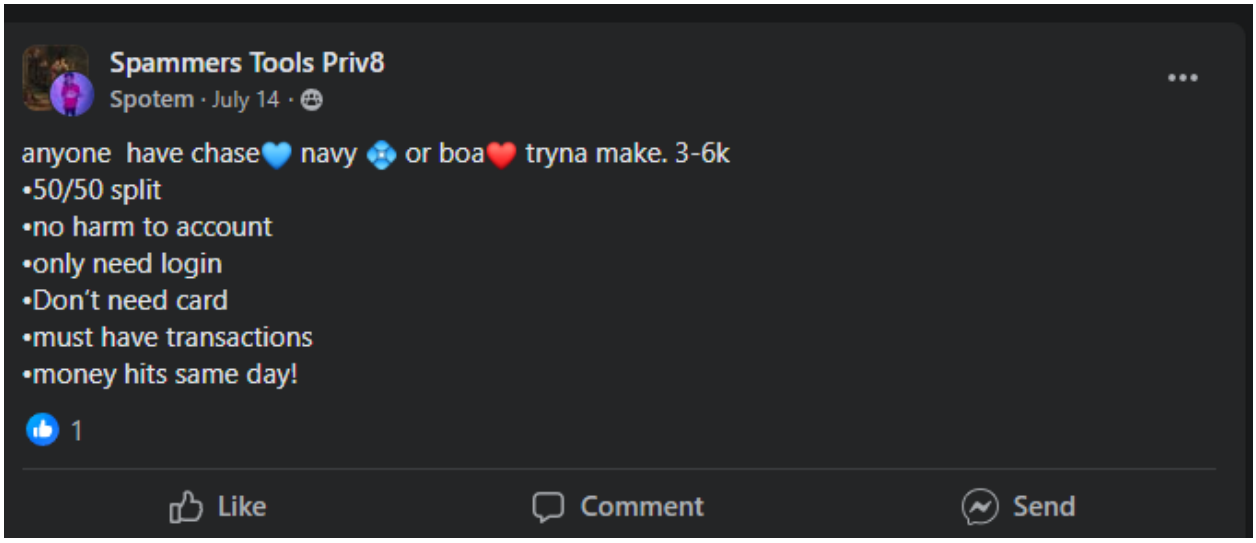


Figure 27: Recruit account-holder for wire transfer.

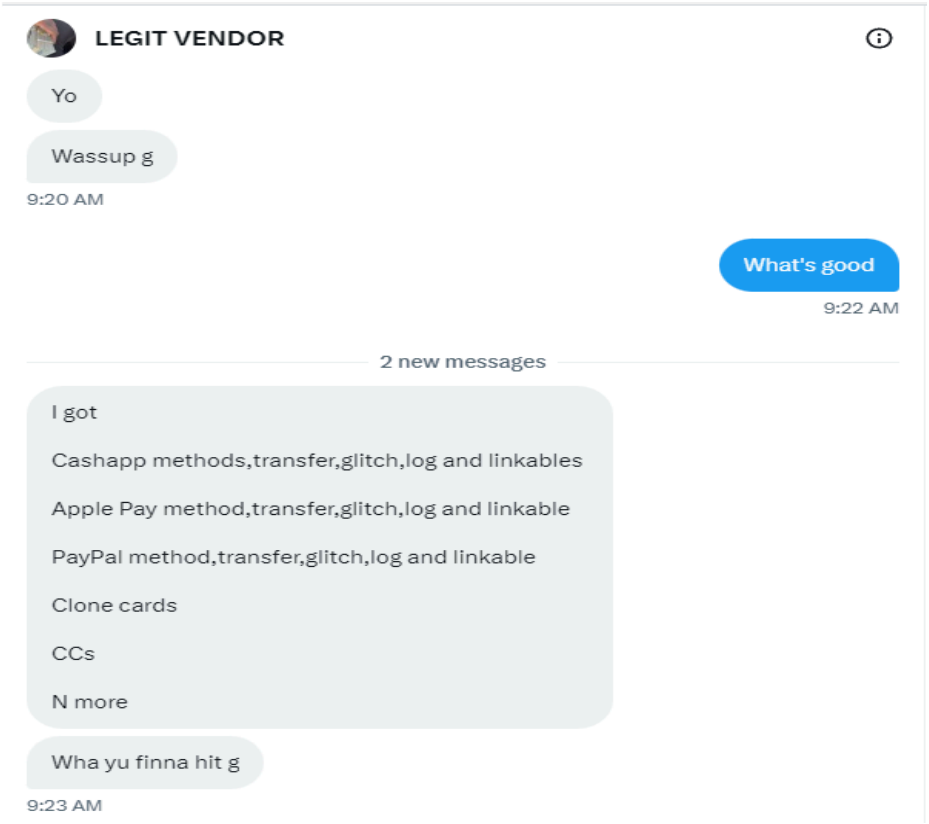


Figure 28: Sell to follower on Twitter

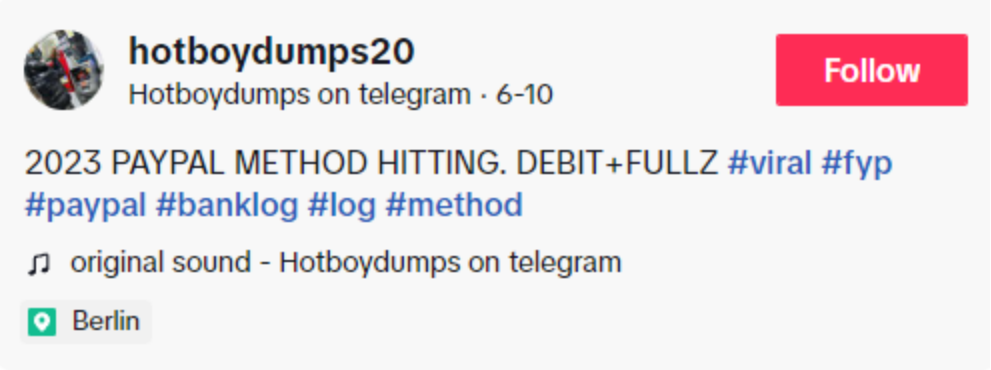


Figure 29: Advertising on TikTok

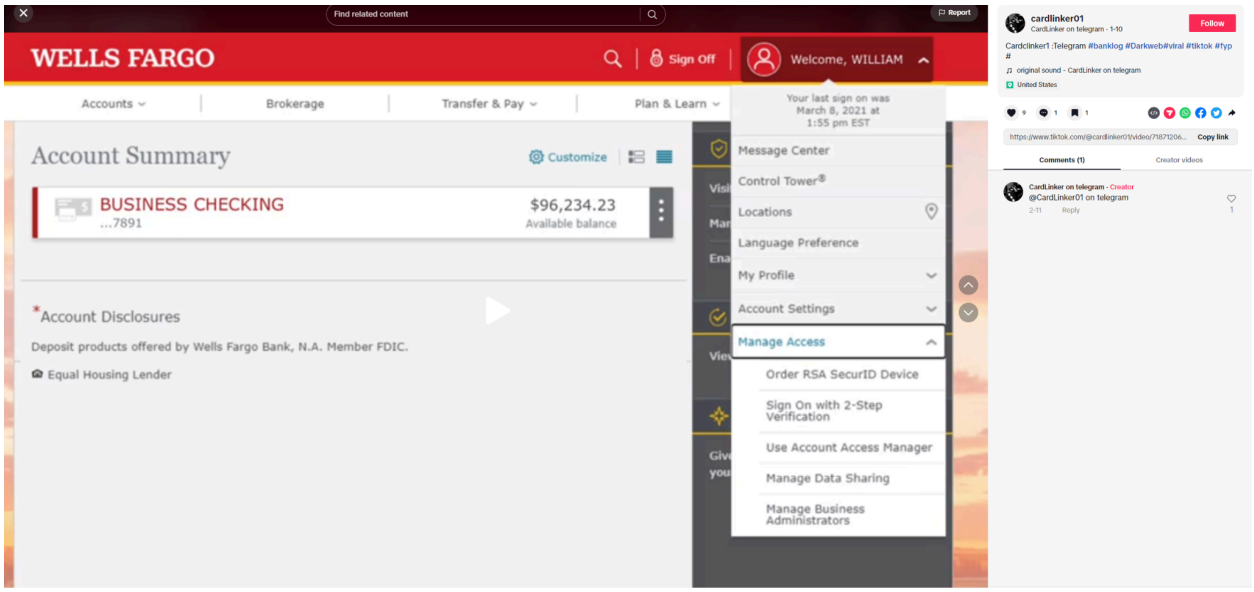


Figure 30: Advertising Access on TikTok