# RABBIT HOLE: A NEW MULTI-STAGE FRAUD SCHEME

*"Same as with Alice following the white rabbit in Lewis Carroll's fairy tale, attackers lead their victims from one website to another, stealing personal data, bank card information, or money."*

***Group-IB experts***

Traditional phishing has become less effective lately. Users no longer trust out-of-the-blue notifications of winnings or rewards. True, some are still poorly informed or careless enough to fall for it, but by and large people don't find straightforward phishing surprising anymore. The adverse effect of this is that individual users and brands have somewhat relaxed their vigilance, thinking that they can always recognize the threat. This, in turn, has encouraged scammers to come up with a new phishing scheme. The situation follows the familiar pattern of pandemic thrillers: the virus mutates and grows more resistant, so that the existent methods of treatment become ineffective.

The new scheme derives its provisional name from Alice's Adventures in Wonderland, since it begins with harmless actions the user takes while trusting the "white rabbit". Eventually the user lets their guard down and falls down the "rabbit hole".

The new scheme is especially dangerous because each step in the scheme looks safe even to IT security services, attacks are tailored to the victim's individual characteristics, and users tend to follow the "white rabbit" along the entire course of the scheme on their own initiative.

Potential victims are mostly gullible teenagers who use their parents' bank cards. Also, attackers may use the false pretext of social experiments, crowdfunding, or charity in social networks, easily gaining the trust of those users who frequently participate in such actions.

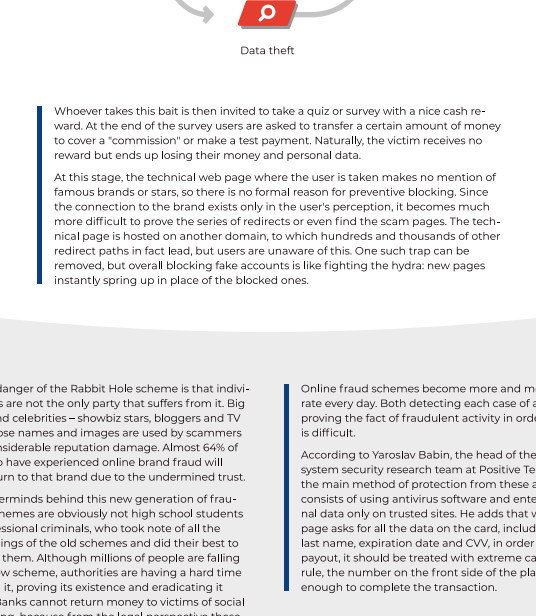
**Group-IB experts divide the entire fraudulent scheme into two large stages:**

## Stage 1. Follow the white rabbit
or the traffic acquisition stage

*Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it... Suddenly a White Rabbit with pink eyes ran close by...*

*She had never before seen a rabbit with either a waistcoat-pocket, or a watch to take out of it.*

**Traffic acquisition**




During the first stage of the Rabbit scheme, scammers use fake accounts of celebrities and well-known brands, on whose behalf they announce giveaway contests, special deals or surveys with decent prizes and gifts – smartphones, headphones, show tickets, etc.

When the user clicks on a banner, contextual ad or a malicious link, they do not immediately end up on a static website but are instead taken first to a so-called redirect path, where web page code collects all kinds of the user's information, including identity, geolocation, language, browser, provider's name, and so on.

Note that banners and contextual ads using images of celebrities in social networks are often targeted based on the specific user's interests and other previously gathered information. In the next step, malicious code automatically creates a personal phishing link to the redirect path[1] complete with a timestamp[2]. As a result, the link is followed only once and only by this specific user. This is important because when the company that owns the brand complains to the provider, the link either won't work or there will be something totally innocent in its place: no threat to eliminate.

*...Burning with curiosity, she ran across the field after it, and fortunately was just in time to see it pop down a large rabbit-hole under the hedge. In another moment down went Alice after it, never once considering how in the world she was to get out again.*

After clicking on the link, the victim is taken to an application form and asked to answer simple questions[3] as well as to "share" their "luck" with friends on WhatsApp or in social networks. This starts off a chain-reaction mailing with the unsuspecting, legitimate user at the beginning and their trusted circle of friends, who, in turn, fail to detect the danger and make their own steps down the "white rabbit" maze.

This mechanism ensures the viral spread of the scheme and drives traffic to the attackers' fraudulent websites. At the same time, each victim is asked for their email address, which can be later used for phishing or malware mailings. Once these preparations are complete, the scammers move on to the next stage.

## Stage 2. The rabbit hole
or the attack stage, where the user's money or bank card data is stolen.



*The rabbit-hole went straight on like a tunnel for some way, and then dipped suddenly down, so suddenly that*

*Alice had not a moment to think about stopping herself before she found herself falling down a very deep well.*

**Attack**




Whoever takes this bait is then invited to take a quiz or survey with a nice cash reward. At the end of the survey users are asked to transfer a certain amount of money to cover a "commission" or make a test payment. Naturally, the victim receives no reward but ends up losing their money and personal data.

At this stage, the technical web page where the user is taken makes no mention of famous brands or stars, so there is no formal reason for preventive blocking. Since the connection to the brand exists only in the user's perception, it becomes much more difficult to prove the series of redirects or even find the scam pages. The technical page is hosted on another domain, to which hundreds and thousands of other redirect paths in fact lead, but users are unaware of this. One such trap can be removed, but overall blocking fake accounts is like fighting the hydra: new pages instantly spring up in place of the blocked ones.

Another danger of the Rabbit Hole scheme is that individual users are not the only party that suffers from it. Big brands and celebrities – showbiz stars, bloggers and TV hosts whose names and images are used by scammers – take considerable reputation damage. Almost 64% of users who have experienced online brand fraud will never return to that brand due to the undermined trust.

The masterminds behind this new generation of fraudulent schemes are obviously not high school students but professional criminals, who took note of all the shortcomings of the old schemes and did their best to eliminate them. Although millions of people are falling for the new scheme, authorities are having a hard time detecting it, proving its existence and eradicating it entirely. Banks cannot return money to victims of social engineering, because from the legal perspective these users willingly transferred their funds to the fraudsters' accounts or shared their card information.

Online fraud schemes become more and more elaborate every day. Both detecting each case of attack and proving the fact of fraudulent activity in order to stop it is difficult.

According to Yaroslav Babin, the head of the banking system security research team at Positive Technologies, the main method of protection from these attacks consists of using antivirus software and entering personal data only on trusted sites. He adds that when a web page asks for all the data on the card, including first and last name, expiration date and CVV, in order to process a payout, it should be treated with extreme caution. As a rule, the number on the front side of the plastic card is enough to complete the transaction.

***Be alert!***
***Our security starts with our own vigilance!***

***1*** *– The custom link is generated for the specific user, based on their location, IP address, device configuration, user agent, etc. According to Group-IB experts, scammers gather preliminary information about the victim from social networks, increasing the chance of successful attack*

***2*** *– Exact time and date of the event*

***3*** *– This psychological trick is used to gain the victim's trust*