Exploring the most common use cases for industries that suffer from bonus abuse, loyalty fraud, new account fraud and account takeover

Fraud in retail & e-commerce

Based on data gathered by

Kaspersky®
Fraud Prevention

kaspersky

Learn more on kaspersky.com

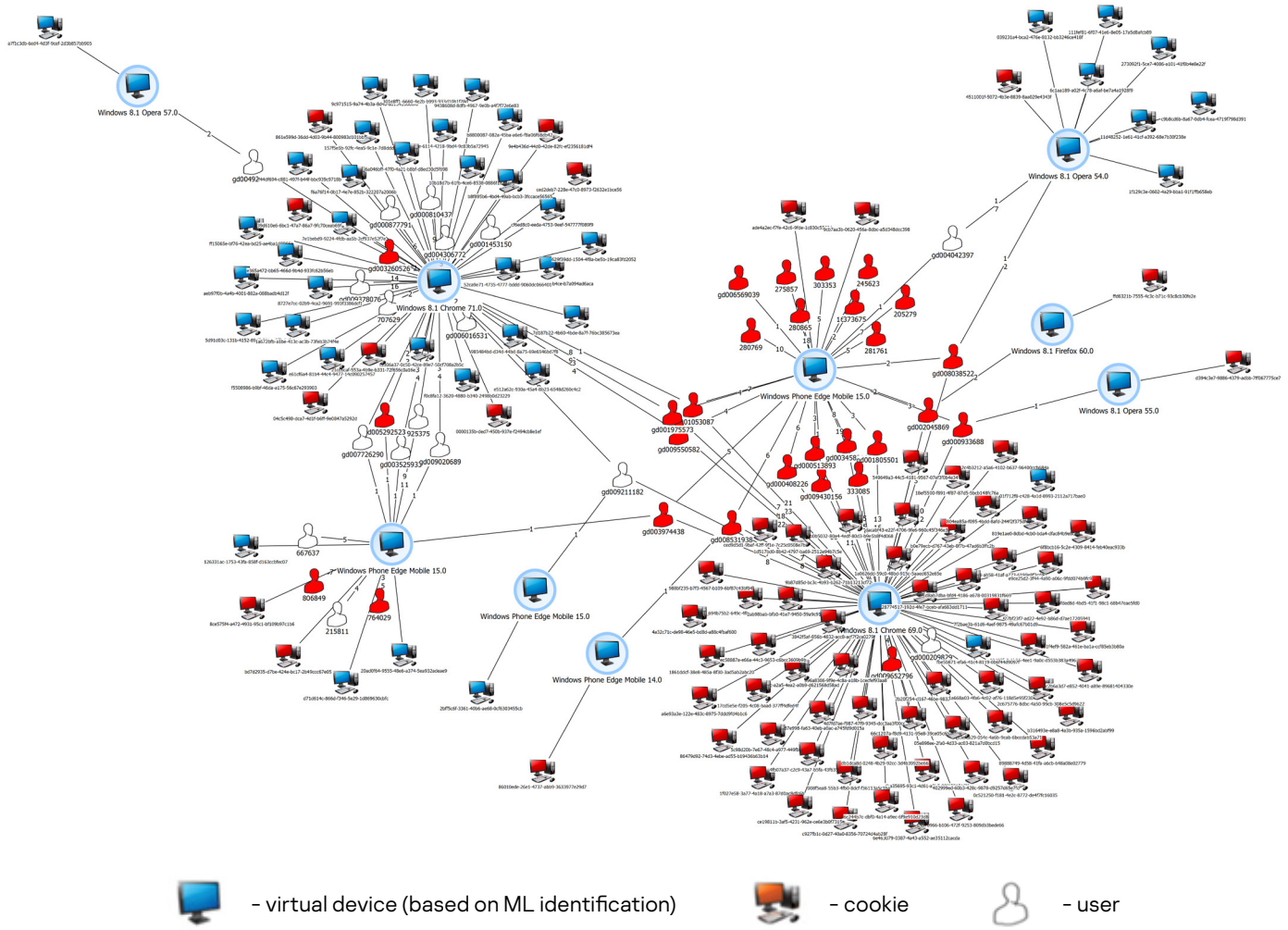
How do fraudsters attack online retailers and digital e-commerce services?

Account takeover →	Taking over accounts to pay with bonuses
New Account Fraud →	Registration of multiple accounts for bonus abuse

Let's take a look at some specific cases of new account fraud that affect the services of online retailers and e-commerce vendors:

In this first case, the account takeover is centered around the loyalty points that some organizations grant customers within their loyalty programs. There are two ways for fraudsters to exploit this. They can find buyers, purchase the product for them and keep the bonus points for themselves to resell on the DarkNet. Alternatively, they can take advantage of welcome bonuses by registering multiple new accounts to gain bonuses and then sell them online.

When fraudsters create multiple accounts to abuse loyalty programs they tend to do it from limited devices (clearing cookies) that form clusters:



As can be seen from the illustration, one device can be used to control hundreds of fake accounts. By implementing global device reputation and global entity linking methods, Kaspersky Fraud Prevention was able to uncover large abnormal clusters of devices and accounts.

Fraudsters treat bonus abuse like fraud as a service and interact with legitimate users online

The correlation between bonus points and new account fraud is key to understanding the motives of fraudsters in the industry of e-commerce and retail.

One way cybercriminals exploit loyalty programs is by acquiring as many bonus points as they can by creating multiple fake accounts. They then offer the additional discounts online, granting the buyer some bonus points, but on the condition that they make the purchase themselves (with the buyer's money) and receive the additional benefits that come with the purchase (e.g. gift scratch cards). This way the criminals can turn their accumulated points into cashback.

A fraudster can accumulate enough bonus points using this scheme to cover the full cost of a product. This allows the criminal to make a purchase, either for himself or to resell afterwards.

Meanwhile, the methods and means used by fraudsters are constantly evolving. For example, fraudsters are now utilizing a sophisticated scheme known as triangulation fraud:

The 3-step plan

1. Offer low-priced products that are in high demand through a fake e-commerce store, where payments can only be made with credit cards. This enables fraudsters to collect data.
2. Fraudsters are then able to purchase the requested product from a legitimate store and deliver it to the victim as promised.
3. The fraudster is then able to use the stolen credit card data for their own purposes.

What do the numbers show?

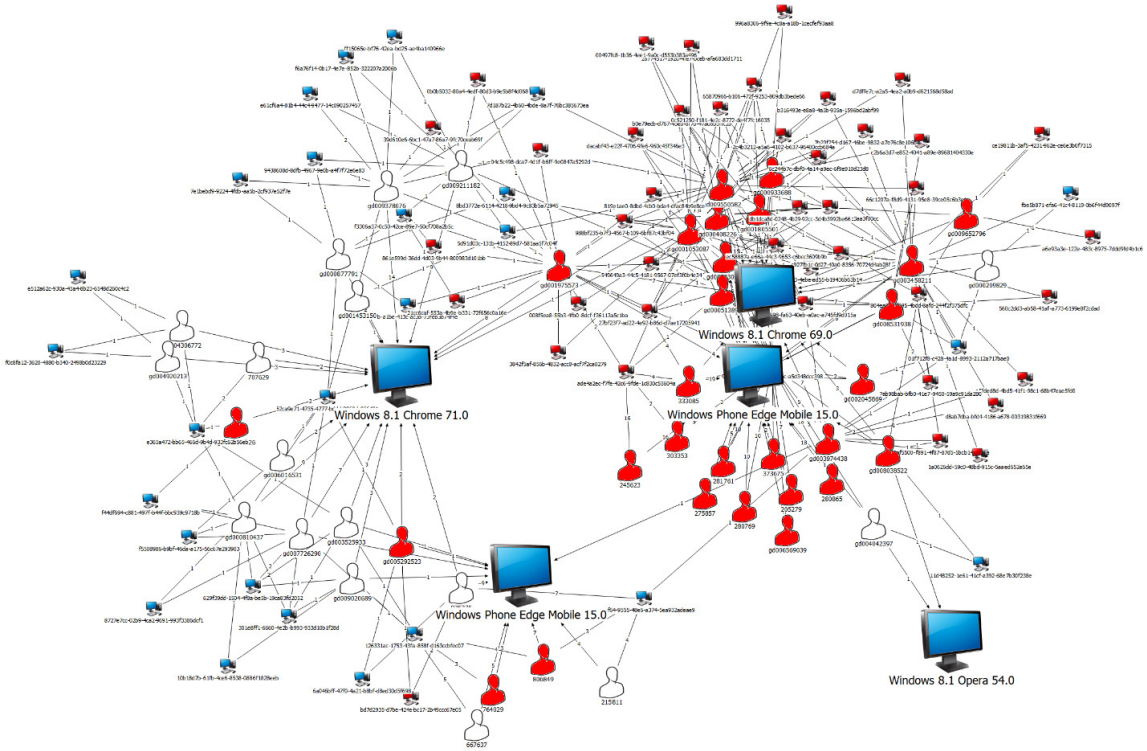
The Kaspersky Fraud Prevention team recently discovered over 3,000 fake accounts in the loyalty program of just one major retailer. The accounts were used to acquire welcome bonuses for newly registered users, and were then sold on the dark web at a reduced fee.

Statistics show that a physical bank robbery may result in average gains of around $5,000-$7,000, while selling 100-150 gift cards at $50 each brings the same rewards but a much reduced risk of being caught.

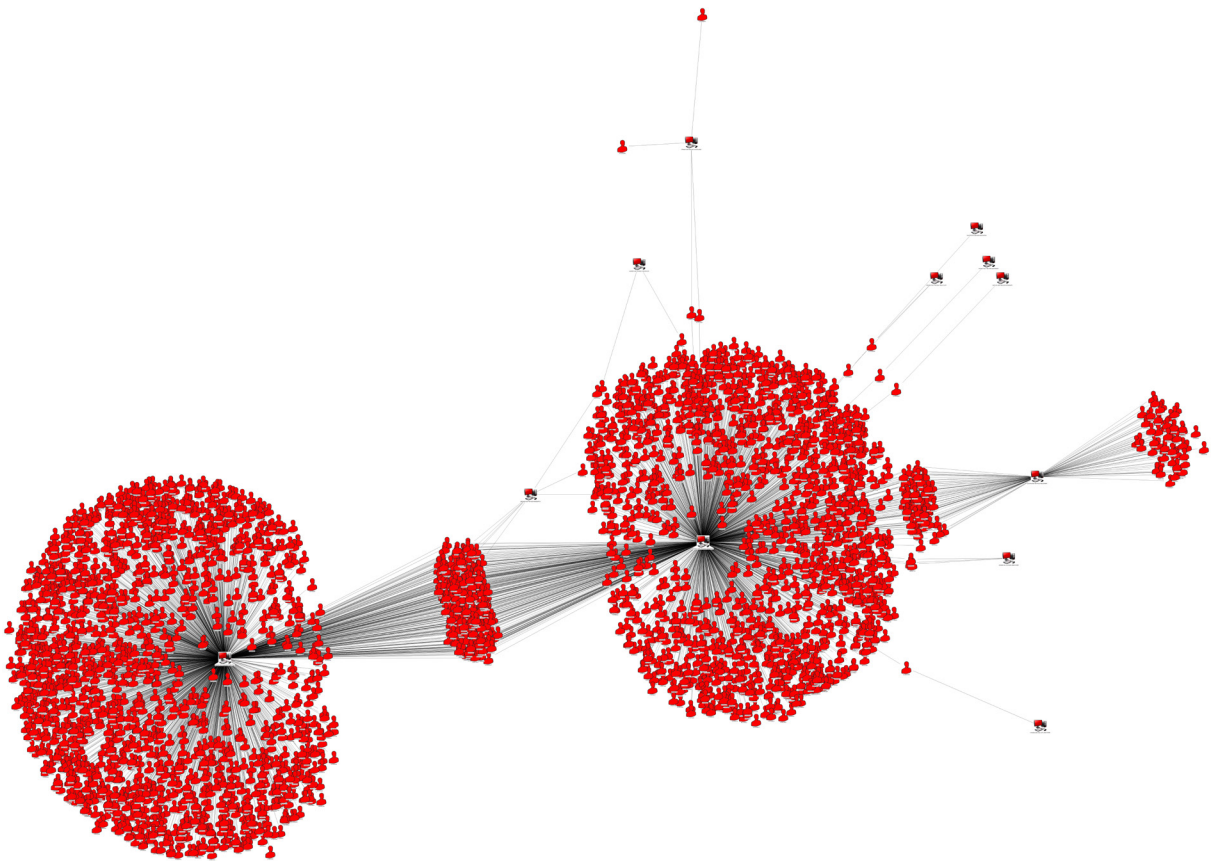
In the past year, almost 7% of digital service users were subject to various kinds of identity fraud, while account takeover losses tripled and reached more than $5 billion globally.

Why fighting fraud is neccessary?

At this point it is quite clear that monitoring user activity and detecting correlations between devices and customers is essential for preventing fraudulent activity and making sure bonus points and loyalty programs are safe. But just how important is it for fraud prevention to take action? Let's analyze two examples:

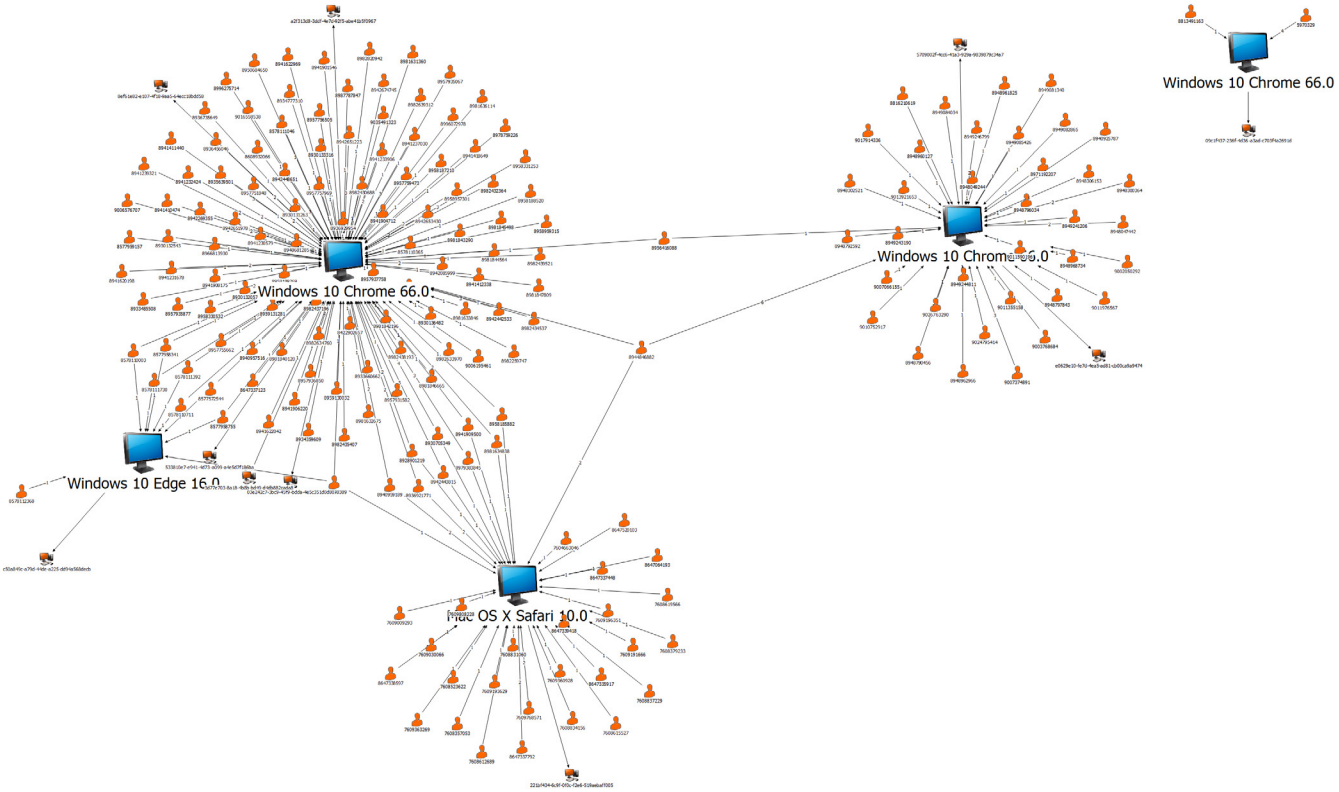


In this instance the client is actually combating fraud, so the fraudsters delete all their cookies and use new devices for new sessions to ensure they are under the radar. View the illustration below to see what happens when they don't remove cookies:

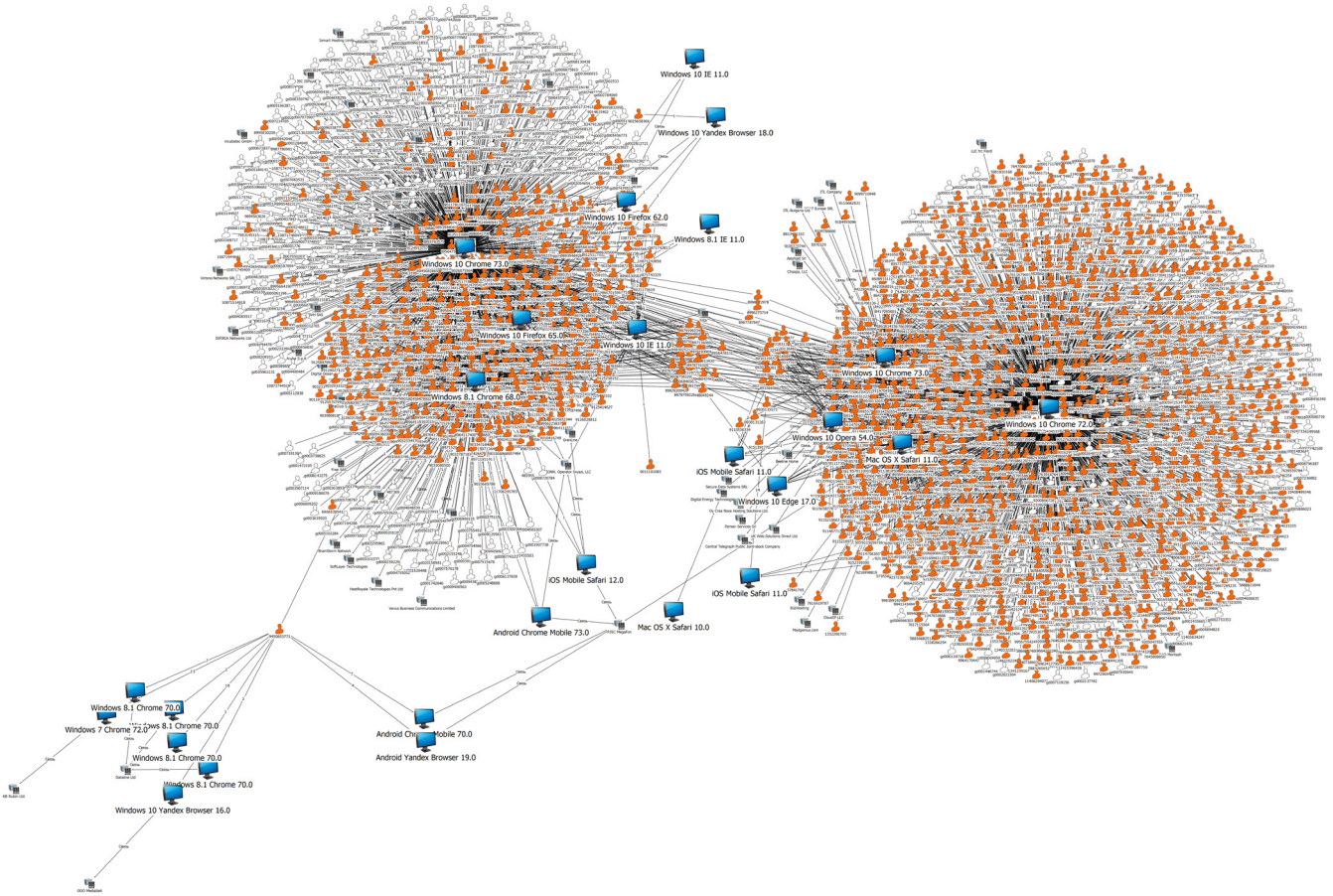


As can be seen from the illustration above, if the fraudsters don't delete their cookies before entering the session, the cluster grows exponentially. The ring of three devices contains 2,650 users, while a ring of 10 devices can support up to 65,000 users:

Now let's look at how global reputation operates when it comes to detecting fraudsters' circles on an example of a major e-commerce vendor:



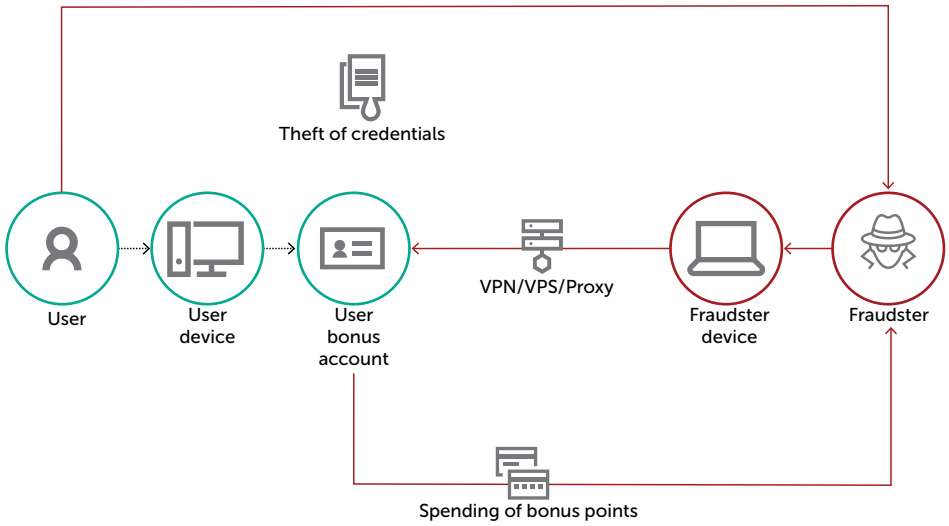
The fraud network above was formed in 2018 and was subject to massive expansion that culminated in thousands of synthetic accounts:



Account takeover among other threats to loyalty program accounts

Compromise of a loyalty program account

The compromise of a bonus system account usually occurs in three ways: a targeted attack on a personal account (brute force, collateral compromise via other services (email account, or with the help of Trojan stealers. The attacker then enters the personal account, preventing the owner from restoring access by changing the contact information, and subsequently manages the bonus account.

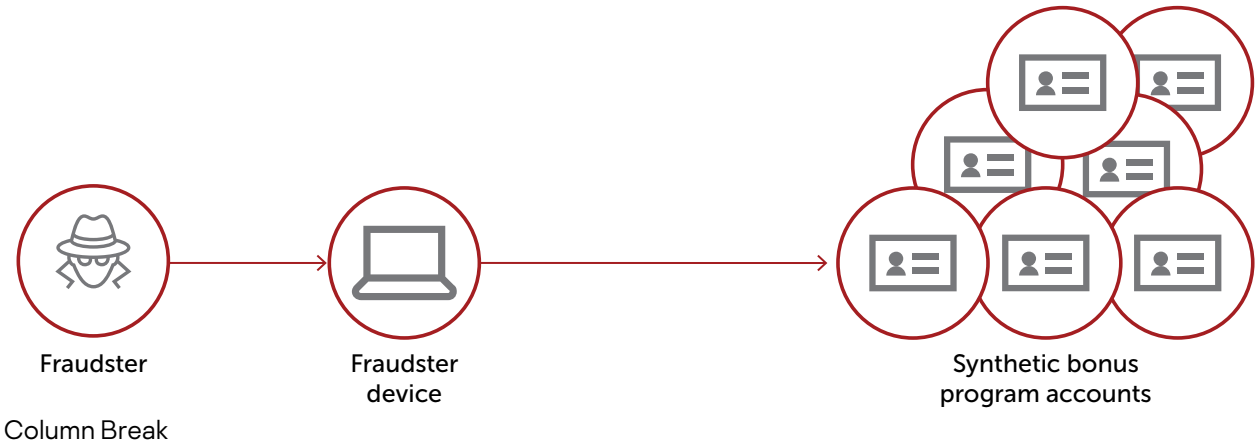


- Bonus points stolen by transferring them to other accounts (if the bonus program allows transfers).
- Bonus points spent on purchases/orders issued to other accounts, addresses, etc.
- Use of various privileges available to the compromised account (discounts, gifts, etc.).
- Sale of a compromised account to other interested parties on sites with a related theme.

'Synthetic' loyalty program accounts

The creation of 'synthetic' (fake) accounts is relatively easy for scammers and at the same time provides lots of opportunities to commit fraud. Fraudsters can use or resell 'welcome' bonuses, promo codes or other gifts received upon registration or they can boost their chances of winning a prize in promos by participating from multiple accounts.

If a bonus program participant only uses a physical bonus card, the fraudster (armed with the bonus card data) can create a new, fake account, attach it to the card and steal the user's accumulated bonus points.



Column Break

Sometimes synthetic accounts can be used with various partner programs for fraudulent schemes involving advertising traffic.

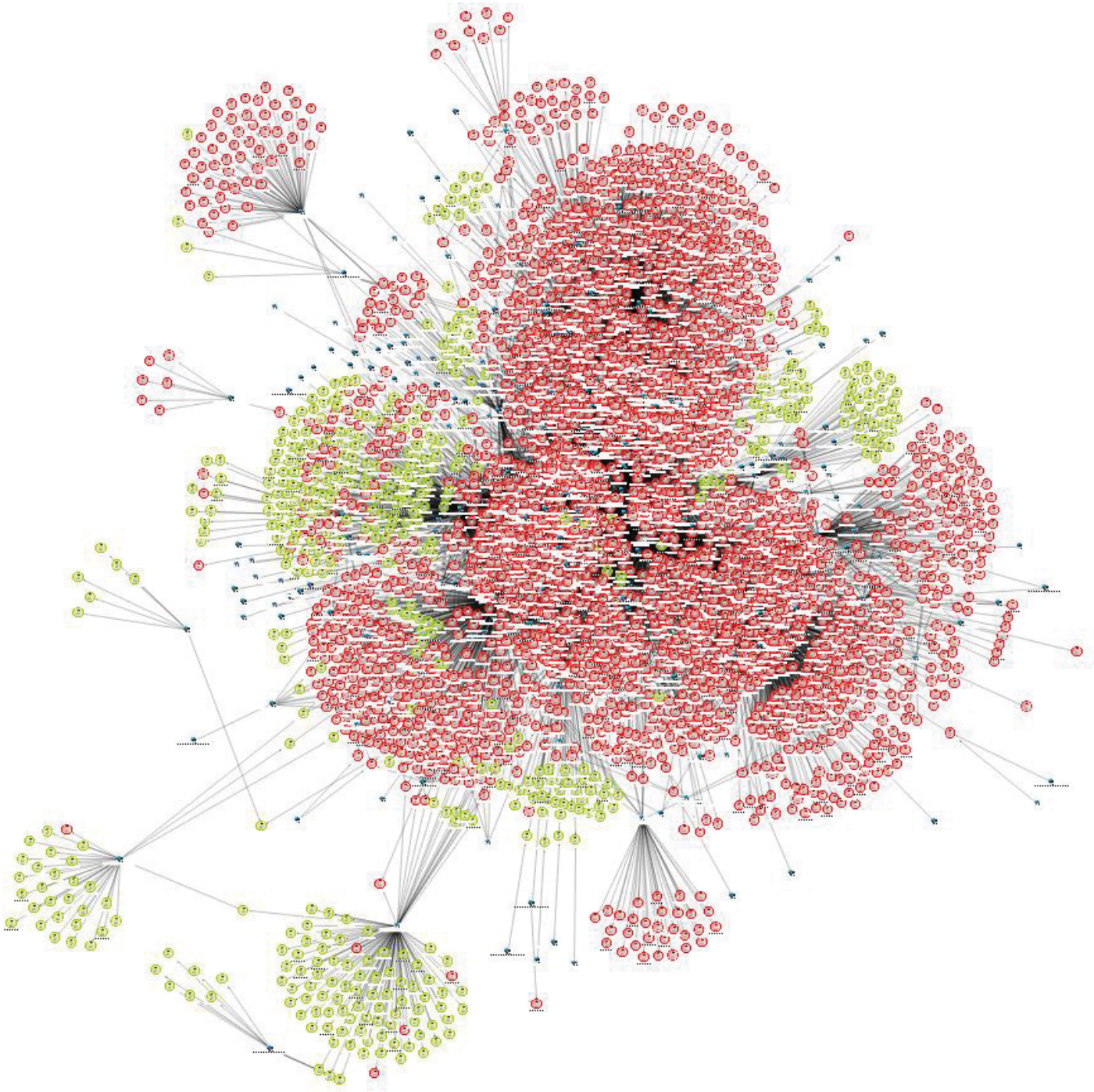
Then there is the creation of synthetic accounts by 'resellers' of goods that are bought using a 'welcome' bonus and then resold on other sites; this also comes with the added benefit of more loyalty program bonus points and, for example, cashback to the bank card used to make the purchase.Account takeover among other threats to loyalty program accounts.

Creation of synthetic accounts to obtain promotional codes for a loyalty program

At the end of 2017, a group of almost 3,000 synthetic accounts was discovered among the accounts of a loyalty program. They were used to receive 'welcome' bonuses for registering new accounts, with a view to reselling them on related internet sites. A distinctive feature of this group was the use of a single email box to manage the entire group. This was made possible due to a feature of the Gmail service that does not take into account the dot symbol in an alias, allowing all accounts in the incident to become modified versions of the main primary address with the addition of a dot.

After Kaspersky Fraud Prevention was connected to another major marketplace bonus program it was found that the same scammer had begun creating synthetic accounts to receive welcome bonuses for this service as well, using the same devices and the same trick with the email addresses on Gmail. The attacker managed to create a total of 542 synthetic accounts in the bonus program.

Below is an illustration of the compromised account links for two different loyalty programs via the fraudster's devices:

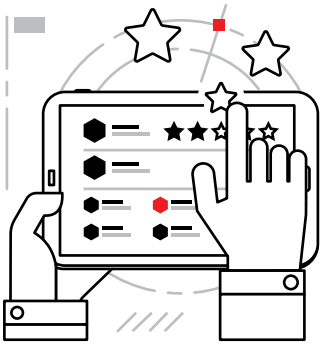


Customers have high expectations of such service:

- seamless access to the digital account;
- high level of personal data protection;
- ability to access accounts from multiple devices anywhere anytime.

Organizations with loyalty programs face tough consequences when they encounter fraud:

- restoring stolen points and loyalty program benefits to victims;
- recovering their brand reputation;
- keeping the consumer within the loyalty program.



Key use cases for retail and e-commerce:

- Immediate recognition of synthetic accounts
- Detection of new unknown device
- Spotting signs of ATO at the login
- stage and throughout a session
- Detecting anomalies and suspicious behavior in real-time
- Accuracy and speed of detection

To conclude...

Moving to the digital world means elevating cybersecurity for e-commerce and retail enterprises. It is essential to provide security for consumers during the entire session, including registration, login and transactions, but not just limited to this.

Timing is a major factor for retailers when interacting with their customers via digital channels. It is no surprise that buyers expect the service to be instant: fast payment for a fast order that will be delivered fast. This leaves the merchant no room for error. Fraud rates are soaring and it is impossible for any fraud specialist to keep up with all the threats.

Criminals are exploiting these vulnerabilities: they are aware that no human analyst is capable of tracking ever emerging attacks at the pace required to keep customers satisfied and secure.

Making sure that an organization does not suffer financial and reputational consequences requires strong yet seamless authentication and analysis of both identities and session data. Striking a balance between protecting customers from new account fraud and account takeover and ensuring the user experience is seamless and smooth remains a difficult task.
Data gathered by Kaspersky Fraud Prevention presents the big picture when it comes to a correlation between suspicious user activity and actual fraud taking place within the network of a retail or e-commerce provider. Taking into account the possible negative outcomes and damage that they might bring, the decision to protect your business with the help of a proven cybersecurity provider should be seriously considered.
Prevention is definitely better than cure when it comes to fraud scenarios.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.