FRAUDHUNT

ACCOUNT FRAUD PREVENTION

Introduction

The report is based on the assessment of data about bot threats and account takeover / fake account creation in the digital ecosystem and investigates the possibility of creating the system perfectly balanced between user satisfaction and account takeover / fake account creation protection.

Problem magnitude

The digital commerce ecosystem has been a leading field of human economic activity for quite some time now with a staggering number of new businesses appearing every day.

Whereas the potential benefits of online business are evident, the problems of security and customer satisfaction are creating a state in which digital fraud has more ways to thrive than we can possibly imagine.

The economic incentives of fraudulent activity are a topic of another discussion, but it is safe to say that we now find ourselves in an environment infested with fraudsters on a truly terrifying scale. Reports show that around 90% of websites with login pages suffered attacks connected with credential cracking and staffing and 80% of websites were victims of activities aimed at the creation of new fake accounts.

Importance of account protection

Digital ecosystem trends clearly show a shift in the attitude of most businesses with 72% of companies indicating the improvement of customer satisfaction as their top priority. Companies that fail to deliver satisfactory user experience disappear and those that successfully cope with the task spend billions to improve the user experience.

With new ways to create customer value and satisfaction comes an increase in digital fraud and types of abuse, among which fake account creation and account takeover are, without a doubt, taking leading positions.

These types of fraud are especially dangerous because they significantly damage the user experience. No one is too keen to get locked out of their account or receive tons of spam messages. These are the most obvious examples of how account fraud ruins UX and eventually businesses, but there is a myriad more ways it can harm you.

The password as a way to protect your account has long ceased to be a reliable security measure with reports indicating around 80% people reusing their passwords among different profiles and recent credential spill reports indicating 3B credentials being stolen in 2016 alone. This has led companies to come up with various additional fraud prevention techniques.

Fraud Prevention Techniques

Modern fraud prevention techniques provide a staggering number of methods to fight digital account fraud, varying all the way from blocking users after unsuccessful password entry to using authentication methods like captchas, security questions, etc.

90%

of websites with login pages suffered from hacking attempts

80%

of websites were victims of fake account creation

72%

of companies claim customer satisfaction to be their top priority

Most common fraud-signup prevention techniques include:

1. Captcha;
2. Mobile Number verification;
3. Social Login;
4. Honey Pot;

Most common account-takeover prevention techniques include:

1. Account block after a certain number of failed login attempts;
2. IP address block after a certain number of failed attempts;
3. Cookies and browser fingerprinting;
4. Step up authentication, secret questions, captchas, and added time delays;

While most of the techniques described above show great results with specific types of fraud, they all show weaknesses to specific fraud types or create difficulties for legitimate quality users.

User Experience vs Security

The main issue that any business faces in the era of customer centricity is maintaining excellent user experience while providing the highest possible level of security. Opening new digital channels and simplifying necessary procedures have created a state in which users do not have to waste time on lengthy purchases or subscriptions. On the other end, however, companies find themselves vulnerable to the ever-increasing fraud threat.

Most fraud prevention techniques are treated as a necessary evil rather than a remedy for the fraud problem. CAPTCHAS are used by companies whose websites are constantly targeted by scrapers and other bot types, although it can cost them up to 3% decrease in conversions due to captchas being burdensome for many users.

The solution we at FraudHunt are working on is aimed at creating a state in which every individual user will be evaluated and additional checks and verifications will be established for potentially dangerous users only. This will ensure as small an impact of security measures on quality customers as possible, increasing trust in the product at the same time providing security measures that will effectively battle a majority of fraud threats before they actually reach your user zone.

FraudHunt Solution

FraudHunt is best described as multifunctional user evaluation system. Our scripts gather massive amounts of information about every user and enable a deep control over the quality of your traffic. Complex analytics and machine learning modules allow precise scoring and detection of all modern fraud techniques. In addition to providing a quality score for each user, FraudHunt enables detailed reporting on each individual case that allows not only effective fraud prevention but also a possibility to really know each of your visitors.

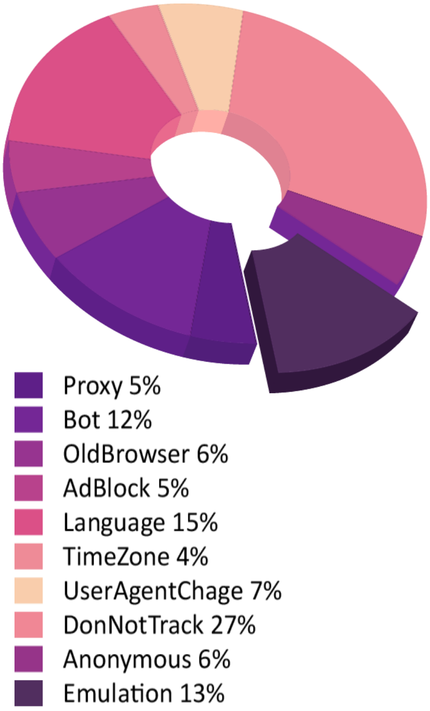
Each user is assigned a unique resistant key:

BBBW507B2B6F83A88E5EC4BD0B9F37F7

It ensures that even if a certain user changes device parameters, we will still know to whom the device belongs.

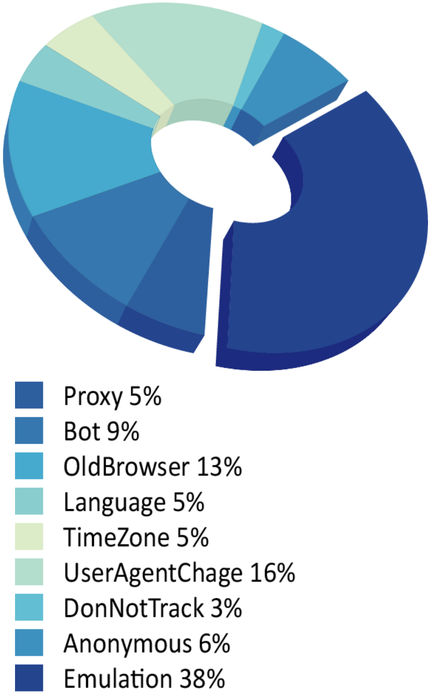
We segment traffic based on a number of triggers. The triggers themselves are designed to detect potentially dangerous users in all digital ecosystem. The combination of triggers in any specific field, however, may vary, so it is up to every individual case to determine the sequence of triggers topical for the case.

Here you can see a ratio diagram for the most common triggers for all users across all of our websites. Some of the triggers are considered to be always fraudulent, like emulation presented on the diagram, users with it are in most cases fraudsters or bot systems. Other triggers, like do not track or adblock are actually more common with the quality users than fraudsters and are used for the traffic analysis and other analytics tasks.



The trigger ratio for specifically fraudulent traffic reflects the change in ratio between the triggers, with the most dangerous triggers taking the lead.

Bot, User Agent Change, and Emulation are, by far, the most dangerous triggers. In most cases, each one of them constitutes a malicious bot, an automated system or a fraudster. Any combination of these plus a number of other triggers is a 100% fraudster.



FraudHunt Value

The main value in the proposed solution lies in the ability to deeply segment your website users and block bots and fraudsters without burdening your quality users with unnecessary security checks.

Our API allows you to store information about every user. Saving an email + FPkey combination for every user or FPkey + any identifier you use will ensure you have a database of FPkeys for every user stored on your server. This will enable detection of the same user across all platforms he or she uses.

FraudHunt Script Integration

The core of the system itself is comprised of a single line JS, that is integrated on your website.

```
<script src="https://p8h7t6p2.map2.ssl.hwcdn.net/fp/Scripts/ffp.js" data-cid="111111111" />
```

The time the scripts needs depends on such factors like user location, user device, user agent, etc. In around 3 seconds after a user visits your page all necessary information about him or her will be present in our database and

ready for the API call.

The script is to be integrated on the following pages:

- The landing page (optional);
- The registration page;
- The welcome page;

Triple layer integration ensures that the script will extract all the necessary information irrespective of the time user spends on any given page and will ensure that any potential fraudster will be checked even in case of successfully bypassing the initial block page.

FraudHunt API integration

There are two types of API available with FraudHunt

Public API integration

Public API is perfect for small websites who need a basic filtering service and is based solely on user score.

The access to the Public API is given to any user upon approve from FraudHunt team. The API call uses a security check via a token added at the end of the request.

The API call is initiated the moment any given user clicks on the Register button on your website.

The response contains a score of the user and basic information about their location.

You set up a score that will trigger the captcha, plus you can set up your server to initiate additional verification steps for users with high scores or block them from registering or logging in altogether.

Public API stores:
FPkey:
httpInfo:
refererUrl:
originUrl:
publicIp:
location:
fraudScore:

Custom API integration

Custom API is designed for companies with high traffic volumes and those who need advanced analytics and blocking features. The API database is stored on your server, which provides such useful features as unlimited storage time, custom format, and the ability to do whatever you desire with your information.

The Custom API is to be deployed on a server of your choosing with Linux CentOS and a number of parameters provided by the FraudHunt Team.

The API call is initiated the moment any given user clicks on the Register button.

The API response, in this case, depends solely on your preferences and is based on the triggers described above, plus all the information about user’s device:

The main difference here is the ability to pinpoint exact triggers you are looking to block or to send for additional verification.

Using this model enables a flexible authentication procedure. For example, you can initiate different additional checks for different types of triggers (captchas for bots, user agent changes, and emulations, phone number verification for proxy services, etc.) as well as send users for manual reviews depending on any given factors.

Custom API stores all of the above, list of triggers, plus:
userAgent:
language:
cookies:
timeZone:
plugins:
browser:
browserVersion:
OS:
deviceModel:
screenInfo:

Conclusion

Every website owner faces a challenge of maintaining excellent customer relations while keeping fraudsters at bay. FraudHunt Account Fraud Prevention offers a holistic approach in the field of fraud elimination. Our solution allows deep analysis of every visitor and gives you the power to make life easier for quality user and unbearable for fraudsters and malicious bots.