SEON

seon.io

Digital Footprint Analysis: What is It & How It Works

Contents

Digital footprint analysis can help fight fraud, identify loan applicants who are likely to default, and more. All while keeping business operations efficient and customer onboarding friction to a minimum.

Find out what digital footprint analysis is, why you need it, and how to implement it below.

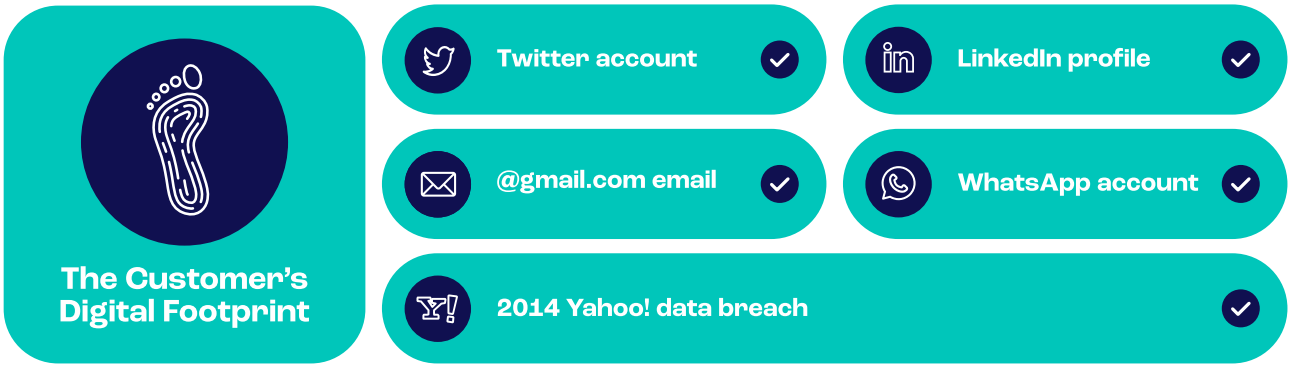
What Is a Digital Footprint?

The term refers to the information – the "footprint" – we each leave behind as we spend time on the internet. This is sometimes thought of as, and called, a "digital shadow" that a user casts, knowingly or not.

This ranges from registered accounts on various websites and services to our social media accounts and public posts, to upvotes or downvotes on reviews, and so on – including content on all sorts of digital platforms, from ads to forum comments.

One thing to keep in mind is that digital footprints are not linked directly to individuals in the sense of a real person or a full name, but to an aspect of their online identities. For example, there is a digital footprint associated with your current IP address. There is a digital footprint associated with your email handle. These often overlap and, in as much detail as possible, allow someone to know as much about whether we are a legitimate person as possible.

A digital footprint is a valuable source of information for background checks, as it can tell us a lot about a person without having to speak to them, giving us an idea of who they are and whether they are trustworthy.



Types of Digital Footprint

In general terms, there are various types of digital footprint, which depend on what aspect of it we're focusing on and how the footprint is left behind – such as passive, active and private footprint. Let's take a closer look.

- **Active digital footprint:** The primary distinction between active vs passive digital footprint. An active digital footprint comprise all the actions they intentionally make online – e.g. a tweet, a comment on Facebook, or a review on Tripadvisor
- **Passive digital footprint:** Everything else – everything not created by a user's actions and/or not intentionally shared with the organization doing the footprinting. For example, the pages you visit more often on a eshop, or whether you've been to a website before.
- **Anonymous:** Data left behind by anonymous users are sometimes called anonymous digital footprints. This is still valuable to several stakeholders – for example, information on a website visitor's cursor movements can show a company which parts of their home page are more appealing.
- **Eponymous/personally identifiable:** If, for any reason, you use your full name online, part of your digital footprint can be eponymous – linked to your real, full name. This is, for example, generated when you are signed in online accounts which use this name. For example, when you use LinkedIn logins to access third-party websites.
- **User input**: All data originating from the user's own input, including clicks, forms filled and other deliberate actions. There is a lot of overlap with an active digital footprint, but they are not identical.
- **Sensor data footprint:** When they use mobile devices, which come with accelerator sensors, GPS, etc, a user's digital footprint includes data from these sensors.

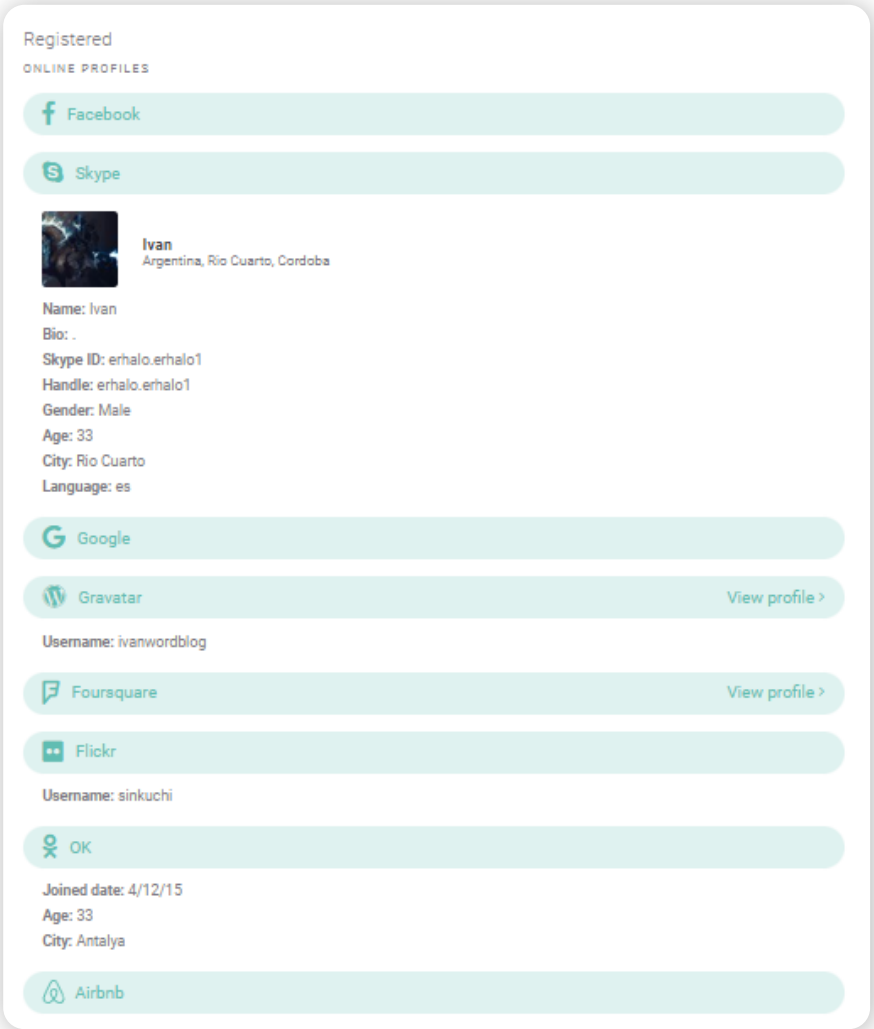
Digital Footprint Examples

Examples of what makes up a digital footprint include things like public comments on forums, their social media posts and uploads, any places where their email ad-

dress has shown up inadvertedly or not (e.g. on mailing lists, if made public), etc. Here is an example of the digital footprint linked to an email address:

- Facebook profile registered with address
- Skype profile registered with address & public name, handle, shared information (see image below)
- Google profile exists
- Gravatar profile exists, and its username
- OK.ru profile exists, and date registered.
- and so on.

As we'll see below, for purposes of fraud prevention, the absence of a digital footprint is as important as its existence, as it isn't easy for a fraudster to mimic a real, good customer in this way.



How Does Digital Footprinting Work?

Digital footprinting takes one or more datapoints and gathers the user's related online activity through a reverse lookup. Starting with an email address or phone number (for example), the process will find things like:

- whether any social media accounts are associated with that datapoint
- whether the datapoint is linked to any data breaches
- what the user's IP address is and which country they are usually based in
- how long a phone number or email address has been active
- whether a phone number or email address is a disposable one
- which network a phone number is on

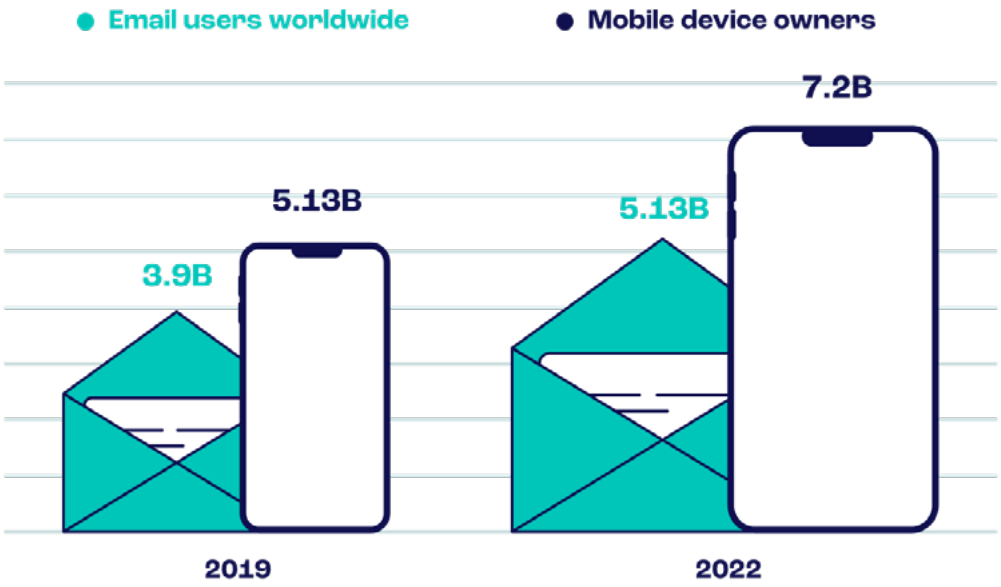
The digital footprint is built up of all these pieces of information, which combine to create a unique profile – a footprint – of the individual. It uses open data to do this, i.e. data that the user has opted to share publicly. A business can analyze the resulting footprint to inform their decisions relating to the user, including whether they may be a fraudster or likely to default on a loan.

Why Is Digital Footprint Analysis Important?

Fraud detection and prevention is an industry as old as ecommerce itself, going as far back as 1984 – the dawn of online commerce. The battle between cybercriminals and fraud prevention is ever-evolving, with innovation on one side driving the other.

In the past decade, cybercrime has exploded with the help of darknet markets, cryptocurrencies and specialist groups offering everything needed to commit fraud to would-be criminals.

Estimates put global losses to fraud at $5.38 trillion a year today.



Digital footprinting is important to businesses because it can help them fight fraud, determine how likely a customer is to default on a payment, and assess a range of other risks. It enables businesses to make informed, data-driven choices about who they deal with and on what terms. All without increasing friction for the customer, meaning organizations can use it without impacting customer satisfaction levels.

This has a knock-on effect for businesses. A reduced risk of fraud generally means a healthier bottom line and happier regulators. It can also help a business maintain a good reputation in the general public's eye, which can support higher customer numbers, further contributing to higher profits.

Digital footprinting is also important to individuals, as employers, colleges, banks, and other businesses may use digital footprint analysis when engaging with them. This places an onus on individuals to maintain a good digital reputation.

How to Catch Fraud Using Digital Footprint Analysis

Digital footprint analysis can help businesses spot fraudsters by identifying common red flags. Together, these red flags enable organizations to identify users with digital footprints that look suspicious, and thus are likely to belong to fraudsters.

Examples of suspicious behaviour include use of:

- a VPN
- a temporary email address or phone number
- an email address or phone number with no associated social media or other accounts
- an email address that has never been in a data breachLeading digital footprint analysis tools carry out this process in real-time, then assign a risk score to each user. Organizations can set their own weighting for these risk scores, to finetune the analysis to meet their own needs. In this way, businesses can use digital footprint analysis to catch likely instances of fraud *before* the event, rather than *after*.

Leading digital footprint analysis tools carry out this process in real-time, then assign a risk score to each user. Organizations can set their own weighting for these risk scores, to finetune the analysis to meet their own needs. In this way, businesses can use digital footprint analysis to catch likely instances of fraud before the event, rather than *after*.

Digital Footprinting: Key Findings from SEON's Internal Data

At SEON, we have loads of data that can help us discern what fraudsters are doing to try to trick organizations in 2022, because this insight is such a key part of how we stop them in their tracks.

For this guide, we looked at our internal transactional data in three different sectors – ecommerce, online lending and iGaming – representing SEON's defense systems in live environments.

What we found is telling...

1. IP Addresses Are Linked to the Most Triggered Rules

Across different sectors, the majority of rule triggers are related to IP addresses with high risk scores. Why? Fraudsters use proxies and VPNs for two purposes:

- **Operational security:** They don't want to get traced and caught.
- **To mimic their victims:** To match the online presence of their victims, who are often in other, sometimes richer, countries.

Accordingly, our statistics show that 52% of rule triggers in iGaming and 65% in ecommerce were related to IP addresses. This means that transactions and user actions were flagged because the IP they were using was considered high risk – showing the popularity of VPNs and proxies among cybercriminals as their weapon of choice.

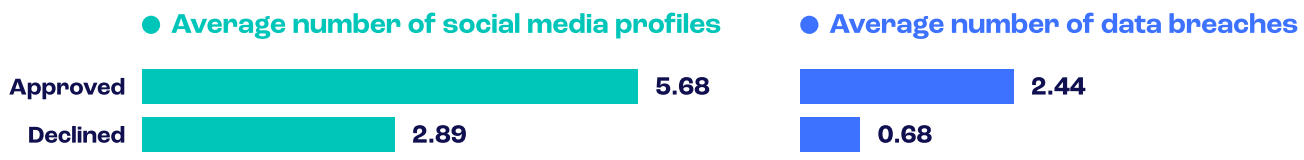
This is why it's key to have good device fingerprinting and proxy detection in place. It acts as your first line of defense against fraud.

2. More Accounts = Safer to Approve

Next, we looked at transactions that were approved, declined or flagged for manual review. How many profiles can we find for each email address, and how many data breaches was that address involved in?

For example, in ecommerce, approvals are certainly linked to a wider presence online. These legitimate users have 5.68 social media/online platform accounts on average.

Digital Footprint via Email in Ecommerce Transactions



Source: SEON

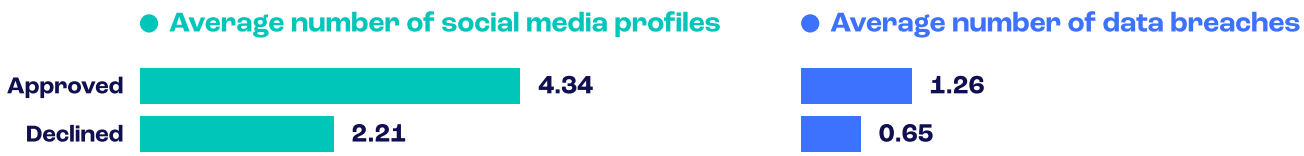
On the contrary, declined transactions only had 2.89 of these accounts on average. As for those sent for manual review, they are in between these, at 3.37 social accounts.

The iGaming industry and online lending sector demonstrate a similar trend, with 4.34 vs 1.26 average profiles for the former and 5.45 vs 1.02 for the latter.

In simple terms, this means that in online lending, the average applicant who gets approved has an online presence that spans between 5 and 6 online profiles (social media, review websites, crowdsourcing platforms, messaging apps, etc.).

On the other hand, the people who were rejected only had 1 or 2 digital profiles on average. Considering how some free email providers auto-populate certain social profiles with your address as soon as you sign up, this number is very small – and suspicious.

Digital Footprint via Email in iGaming Transactions



Source: SEON

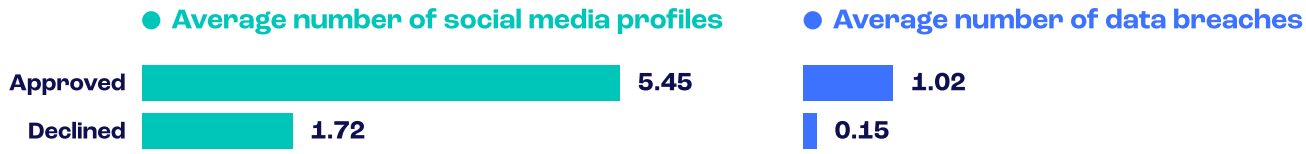
3. More Data Breaches = Safer to Approve

The digital footprinting picture is similar when we look at the number of data breaches in which the email address was involved.

This is done through the lookup module, which will search known lists of leaked emails, using the haveibeenpwned data breach API. We also take into account when the breach is from, because this is evidence the email account existed at the time.

The results once again show how potent digital footprinting is in assessing user intent.

Digital Footprint via Email in Loan Applications



Source: SEON

In ecommerce, "good" users who were approved automatically had been involved in 2.44 data breaches on average. Fraudster addresses were only at 0.68 on average.

In iGaming, the average legitimate account had been involved in 1.26 data breaches in the past. Suspicious accounts were similar to ecommerce, at 0.65.

As for loan applications, the difference is also impressive: 1.02 vs 0.15 breaches.

Considering how the biggest data breaches in history were massive, it goes without saying that most people's email addresses will have appeared in some. For the record, Yahoo's in 2014 exposed 3 billion accounts, and the 2020 incident at Marriott leaked the data of 505 million guests.

Digital Footprinting for Fraud: Key Takeaways

SEON's research has shown that fraudsters are relatively lazy, settling for throwaway email addresses and disposable phone numbers with virtually no related online presence. This means that digital footprinting can be effective in helping spot and block fraudsters. As digital footprinting is frictionless for customers, businesses can do so efficiently.

Our experience also shows that businesses increasingly rely on digital footprint signals over time. This increased trust results from organizations seeing their fraud metrics improve when they introduce digital footprint analysis.To read more about how we fight fraud at SEON, head to our products page or choose your industry from our use cases.

Frequently Asked Questions

What's the difference between active and passive digital footprint?

An active digital footprint is based on a user's active participation online, such as posting on social media or a review site. A passive digital footprint is based on the way the user behaves online, such as which websites they visit, and which pages they navigate to within those sites.

How to get someone's digital footprint

Digital footprint tools work by taking one or more datapoints – an email address, phone number or photograph, for example – and looking online to see where else that same data appears. You can do this using specialist websites and applications, including digital footprint analysis tools.

Can digital footprints become a problem?

Colleges, employers, banks, online lenders, and various other businesses may look up an individual's digital footprint. This means that digital footprints can become a problem for people who have visited websites that they would rather keep private. Digital footprint analysis can also be a problem in the wrong hands – for example, when a fraudster undertakes it as part of stealing someone's identity.

Sources

Datareportal: Global Social Media Stats
Crowe: The financial cost of fraud 2021
Tech Jury: 27+ Biggest Data Breaches In History
Internal SEON data

SEON

Easy fraud detection
for every business

Try for free

seon.io info@seon.io +44 20 8089 2900 SEON Technologies Ltd.