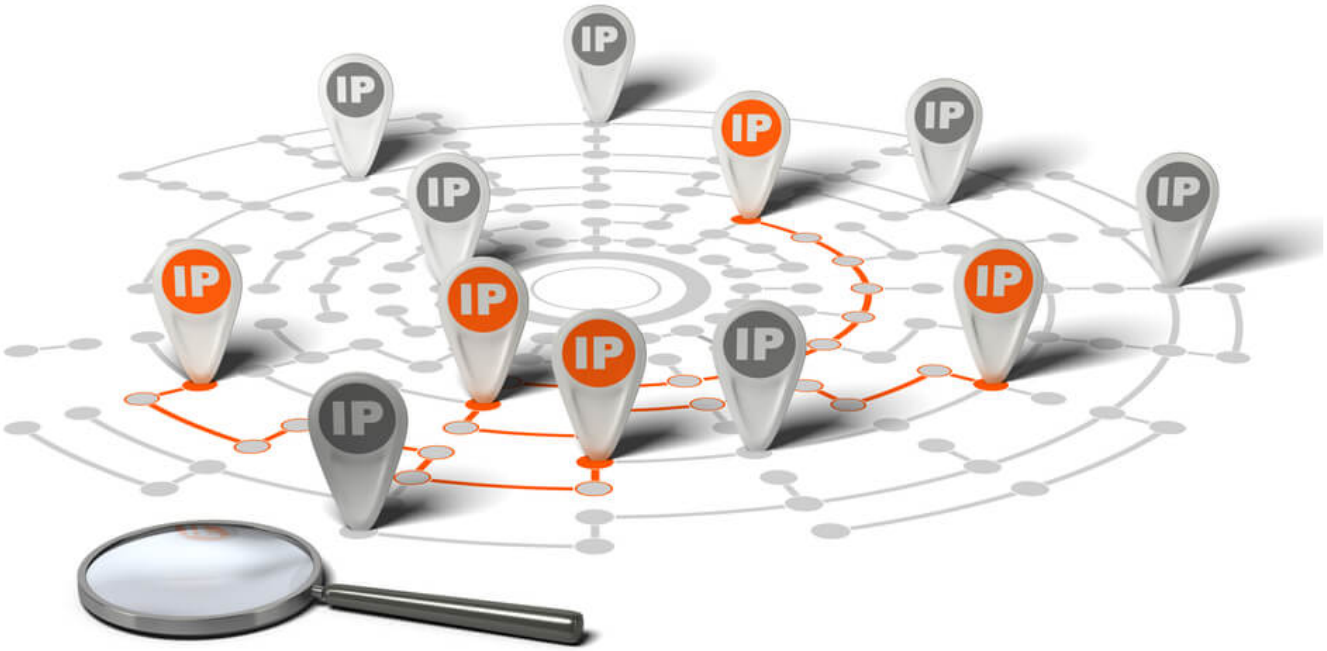
# How to Improve Multifactor Authentication with Reverse IP Address Lookup

Posted on December 9, 2019



Nowadays, cybersecurity is becoming increasingly important for both online users and website owners. Cybercrime has extended an arm that reaches almost everyone who accesses the Internet, and people need to adopt full security measures in place to mitigate threats.

While threat identification is essential, prevention has its own perks, and one effective way to prevent threats from entering a network and keeping users safe is by improving multifactor authentication (MFA), notably with Reverse IP API.

## What Is Multifactor Authentication?

MFA is an identification method that validates two or more user credentials from separate factors (in most cases via different devices) before granting access. Factors can include knowledge, possession, and inherence.

### The Evolution of Multifactor Authentication

In the past, MFA was primarily used by corporations. However, the increasing number of stolen credentials has forced more and more users to rely on MFA to protect their networks and personal accounts.

Authentication and user access management (UAM) evolved from merely providing passwords to also giving out a personal identification number (PIN) code. Even the use of questions and answers to authenticate users is no longer reliable. Easy-to-recall answers translate into easy discovery by hackers. Users, however, cannot recall complicated answers, hence the rise of two-factor authentication (2FA).

As more and more people realized that they needed better security to protect their confidential data, a second factor came into existence — one that users can carry away from their computers

(considered the first factor). This second factor came in the form of a USB token, a public key infrastructure (PKI) smart card, or a one-time password (OTP) keyed into a smartphone.

But, after some time, even 2FA became unsafe. Cybercriminals learned how to bypass 2FA by using phishing and other techniques meant to disarm each factor one after the other. This development led to the addition of yet at least another factor, and MFA was born.

## Why Is Improving Multifactor Authentication Important?

First off, like any digital solution, MFA is not immune to cyber attacks. Just last month, the Federal Bureau of Investigation (FBI) released a security advisory warning industry partners about the growing threat of attacks that can bypass MFA solutions. In a Private Industry Notification issued September 17, 2019, the FBI warned that some threat actors could thwart MFA via social engineering and certain sophisticated technical tactics.

While the FBI cited several attacks, it also maintained that MFA continues to be a reliable and effective security measure to protect online accounts, as long as users take precautions to ensure they do not fall for scams. As such, website owners are advised to implement MFA so they can:

- Make sure that their websites and other online services are safe from unauthorized access
- Protect users from unauthorized payment transactions
- Prevent data breaches
- Ensure compliance with regulatory requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the General Data Protection Regulation (GDPR), the Control Objectives for Information and Related Technology (COBIT), and the Sarbanes-Oxley Act (SOX)

# How Reverse IP Lookup Can Enhance Multifactor Authentication

IP addresses can be an additional factor in determining the validity of access and transactions on websites. For instance, if a user is trying to access a website from China when his/her last access point three hours ago was from California, the website owner can investigate its cause. It could turn out that a cyber attacker instigated one of the transactions. IP geolocation enabled by a **reverse IP address lookup** tool can flag suspicious log-ins.

## Detecting Access from Malicious Domains

A **reverse IP lookup** tool can give website owners a comprehensive list of all the domains with the same IP address. They can include all IP addresses related to a fraudulent domain on their blacklist so that unauthorized users cannot bypass their network security.

## Improving Client Authentication

If authentication systems keep track of IP addresses, website owners can verify if these are the usual ones that users employ when they connect to a network. The systems can be configured to give out alerts if that is not the case, allowing security specialists to take action on a questionable IP address. Using Reverse IP API, they can check if the IP address has ties to domains known for malicious activity. Should the results show such a connection, the IP address can be blocked from accessing the network.

## Restricting Access Based on Geolocation

Should website owners get wind of reports of increased malicious activity coming from specific geolocations, they can use a **reverse IP lookup** tool to block all connections from IP addresses coming from the identified locations temporarily. They can then subject the domains the IP addresses are tied to closer scrutiny before restoring their access to the network.

---

MFA is a relatively effective method of protecting your websites and users from threats. There are many ways to improve it though, and one of them is by integrating a reverse IP address lookup tool into already existing MFA solutions.