Proxy/VPN Detection

Your IP address reveals the identity and location of your network or device when you browse the internet. We all have one. *But* – cybercriminals that are up to no good can use a proxy or VPN to hide this address to get past security checks. And worst of all for you, this means they can attack your business while going completely undetected!

Don't despair – you can stop them in their tracks and protect yourself with the IP reputation and Proxy Detection API from IPQS. This lets you check any IP address online in real-time to uncover threats, bots, and fraudulent connections that are using a proxy or VPN. By analysing advanced location data, device details, and connection information, as well as sweeping for recent abusive activity, this API will flag if a user, link, or transaction online is malicious and help you secure your network in time.

Device Fingerprint

Sometimes it feels like cyber threats are hiding around every corner; that your business is just a sitting duck online. But cybercriminals aren't as sneaky as you might think. Every device on the internet leaves behind a trace – a fingerprint. And it's thanks to this that you can stop suspicious behaviour right in its tracks. Whether it's a risky user or transaction; whether it's a bot or a full-blown cybercriminal trying to gain access, you can use the IPQS Device Fingerprint Tracking API to stamp out malicious activity. It doesn't matter if a user is trying to hide by changing their device, identity, browser, or location – this API uses over 300 data points to lock onto their every movement. From monitoring the devices, payments, and transactions your business deals with and detecting fraud, to fishing out spam bots and users abusing a free trial, the Device Fingerprint Tracking API is ideal for helping protect your critical registration, login, and checkout or payment pages.

Email Validation

Did you know that most cyberattacks start by email? All it takes is one click to let a hacker into your company system and they can take it over. This is what's known as a phishing attack and it's why it's so important to verify the addresses you're getting emails from. With the IPQS Email Verification API, you can do just this. The API performs hundreds of continuously updated checks to work out whether an email address exists and if it has been involved in abusive or fraudulent activities, helping you safeguard your inbox and the reputation of your email campaigns. It can spot and remove spam accounts and leaked emails, and even help you monetise your data and catch out frequent complainers. Thanks to direct relationships with mail service providers, this API lets you verify email addresses in ways that other services just can't do, with the most accurate results in the industry.

Phone Number Validation

Getting calls from a suspicious number? Want to know who's on the other end? If you're not careful, fraudulent numbers can wreak havoc on your business. Take back control with the IPQS Phone Number Validation API by quickly and confidently finding out if a phone number is suspicious. This API provides a real-time and easy-to-read Fraud Score of 0-100 based on information such as a phone number's carrier, line type, and country, as well as if it has been involved in fraudulent behaviour or abusive activity, to help you safeguard your users, marketing lists, and quality control processes. The Phone Number Validation API can also be combined with the IPQS IP Reputation and Email Validation APIs for even greater security.

Malicious URL Scanner

By the time you've clicked on a malicious link, it's probably too late. You might have already released a virus into your system, allowed a cybercriminal to take over your account, or put your business at risk of a ransom attack.

Detect dangerous links before it's too late with the IPQS Malicious URL Scanner API. This API scans content in real-time using highly accurate, deep machine learning analysis to reveal phishing scams, spam emails, malware, viruses, reputation issues, and more. Have you been sent a suspicious email or webpage? This API can sift through the content and work out whether it's malicious without you having to click on anything yourself and putting your business at risk.

Dark Web Data Leak

The Dark Web is home to the internet's most dangerous fraudsters and criminals. You can't get there using normal search engines or internet connections, and it's so well hidden for a reason – many people use it for buying and selling illegal content. At any moment, your personal data could end up here too. It happens more often than you think, especially after major data breaches on popular websites, and if someone in your business falls victim to this, it might not be long until cyber attackers try to extort you or bring down your operations.

With the IPQS Dark Web Data Leak API, you can protect yourself. This API sweeps the Dark Web for stolen email addresses, phone numbers, usernames, and passwords, trawling through a wide collection of leaked databases from popular websites to see if your information is at risk. It also features complete protection for fraud prevention and risk scoring, helping you stay one step ahead of attackers.

Malware Scanner

Have you ever come across something online that just looks – *wrong* – somehow? Are you wondering what's hiding behind that file? Well, clicking on it is the worst way to find out. Once a file is open, whatever an attacker might have stashed inside will be set loose within your network. Instead, be confident that links and files are safe to open first with the IPQS Malware Scanner API. This tool scans files in real-time to detect malware like ransomware, trojan horses, keyloggers, and all sorts of unwanted and dangerous software that cybercriminals try and use to take over your business network, giving you total peace of mind that you're dealing with safe and reliable content.