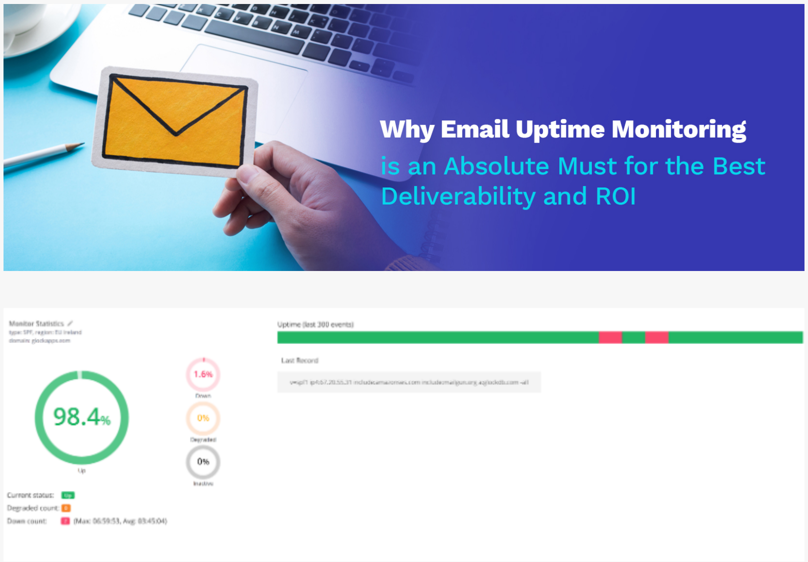
EINPRESSWIRE

Why Email Uptime Monitoring is an Absolute Must for the Best Deliverability and ROI

It is not enough to just implement SPF, DKIM, and DMARC. But how to keep their health and configuration under control at every given moment?

PINEDALE, WYOMING, UNITED STATES, January 13, 2021 /EINPresswire.com/ -- There are many variables involved when we talk about email deliverability. Today we will concentrate on email authentication, because it has its influence on whether your email gets blocked, will land in a spam folder or an inbox. How? It proves you are a trustworthy and legitimate sender, or otherwise.



Monitor Statistics
type: SPF, region: EU Ireland
domain: glockapps.com

Current status: Up
Degraded count: 0
Down count: 7 (Max: 06:59:53, Avg: 03:45:04)

Last Record
v=spf1 ip4:67.20.55.31 include:amazonses.com include:mailgun.org a:glockdb.com -all

GlockApps SPF Uptime Monitor

You should remember that it is not enough to just implement SPF, DKIM, and DMARC. It is also important to make sure they are healthy and correctly configured at any given moment.

Here’s a brief detour for those of you who are not familiar with email authentication methods. And if you are – just scroll to the next section.

What is Email Authentication?
Email authentication is a number of procedures that are used to validate emails and prove the identity of the email sender. Basically, these techniques help mailbox providers see if the email that claims it was sent by you, was in fact, from you.

Today we have three commonly used authentication protocols – SPF, DKIM, and DMARC. Each of them has its pros and cons and each of them should be configured properly. What happens if it’s not? We’ll see in a minute.

What is Uptime Monitoring for Email Authentication Record?
If you are familiar with website uptime monitoring – here we have the same concept. If you are

not – authentication record uptime – is the amount of time that the record is correctly configured and up to date. Depending on a record (SPF, DKIM, or DMARC) it can also have a degraded status and a down status, which means that it is broken, misconfigured, or even missing.

The uptime monitor reaches to email authentication records and checks if there is an issue with any of them. And if there is – it sends instant notifications so that you could start the recovery process immediately. Try how it works.

What Happens If You Don't Monitor Authentication Records?

Decreased Inbox Placement

First and foremost, lacking authentication records, or having misconfigured ones, will lead to a lower inbox placement rate. The moment your email can no longer be proven to be sent by you – mailbox providers will stop trusting you. As a result, your emails will start landing in spam.

Note, that offers, newsletters, and other advertising emails generally have lower inbox placement than transactional emails. In this situation, we're talking about all of your emails, including high-priority and urgent ones.

Disgruntled Clients

When the latter starts happening, unhappy clients become an unavoidable consequence. Who would like to pay for the product and not receive a shopping receipt or register for an event and not receive a confirmation email?

This situation can snowball into calling and writing your support team, and trying to get hold of you everywhere, including social networks, like Twitter. Now, we all know what social networks can do to a brand's reputation, so the last thing you want is somebody tweeting and complaining about your company.

Increased Vulnerability to Cyber-Criminals

Missing or misconfigured authentication records can lead to sensitive information compromise, spoofing attacks, and the loss of brand reputation and money. If you are the one who has authentication records in place, you probably do not worry about one of them going missing, correct?

Turns out, a common problem is people changing their DNS hosting service provider without adding authentication records to a new one. Emails can go to spam for a month, and the domain will be vulnerable to spoofing but the owner can stay oblivious to this fact. With the Uptime Monitoring, they would receive timely notification about a missing SPF record.

The research made by Detectify showed that over 50% of the 500 top-ranking domains on Alexa were vulnerable due to not having an SPF record or because of it being misconfigured. Yes, unfortunately, it is quite simple to misconfigure the SPF record, and time may pass before anyone notices. With Uptime Monitoring, a misconfiguration will be immediately noticed and the owner will receive an alarm.

When it comes to DKIM, this protocol has keys that can expire and have to be changed. Again, it is easy to forget to change the keys, which will lead to a validation error. In this case, the Uptime Monitor is a great reminder.

How Does Uptime Monitor Help?

Uptime Monitor checks your authentication records' uptime at 1-minute intervals 24/7 and sends immediate alerts if any issue happens to minimize the consequences and keep your inbox placement high, customers satisfied and domain – protected.

Narrow the problem search

Uptime Monitor shows three types of authentication record statuses: up – when the record is healthy, down – when it is broken/missing, or degraded – a sign of a misconfigured record. These statuses help understand what kind of problem you are dealing with and eliminate it faster.

Be in control 24/7

With Uptime Monitoring, everything happens automatically. You don't have to perform checks yourself, yet you keep your authentication records under full control every minute of every day, so you have one less thing to worry about. Moreover, in the Uptime Monitor, you have a timeline to easily see all your previous records.

Reduce financial and reputation losses

Authentication record's status can be checked as often as every minute. It eliminates the chance of missing the moment when something goes wrong. Solving an issue on time spares you a lot of long-term consequences, including financial losses, unsatisfied customers, and damaged reputation.

Overall, knowing that your systems are under control reduces everyday anxiety and helps you sleep better. We believe it's very much worth it!

With GlockApps Uptime Monitor free trial, you get:

– 20 Monitors;
– 1-minute monitoring intervals;
– HTTP/TCP/TLS Monitors;
– SPF/DKIM/DMARC Monitors;
– IP Reputation Monitor;
– Instant notifications.
Start a free trial now.

Alex Markov

GlockApps
+1 205-736-9794
email us here