# 2 Very Common Reasons Applicants Are Not Receiving Your Emails

## WHERE ARE MY EMAILS?

Applicant communications are an essential part of the hiring process. But have you received calls from applicants telling you they never received your emails? Missed communications can have a chilling effect on your applicant's journey.

Missing emails have many causes. In this article, we look at two of the most common reasons our clients experience undelivered emails. Both are related to email security, and we show you how to fix them.

Cyber threats are real. Criminals often use email attacks to compromise businesses. Did you know that there are at least 3.4 billion fake emails sent out as part of a phishing scam every day? (techradar.com). By using basic email protections, businesses can prevent many of these security threats.

### Reason 1: Transport Layer Security

The most common reason your email does not reach an applicant is due to security or rather a lack of security. Emails are one of the most common forms of communication. Unfortunately, email messaging was not invented with security or privacy in mind. It can be comprised on your device, on networks, on servers – you get the picture.

Businesses use a standard protocol called **Transport Layer Security** (TLS) to make email and other online communications and transactions more secure. While your IT department is very familiar with this term, you are likely not.

#### What is Transport Layer Security (TLS)?

**TLS** is a cryptographic protocol designed to provide secure communications over a computer network. So, what is **cryptography**? It's the process of changing your ordinary plain text into something unintelligible and then back to plain text once it reaches its destination. Cryptographic protocols allow only the sender and intended recipient of a message to view its contents. It keeps other people from reading your communications!

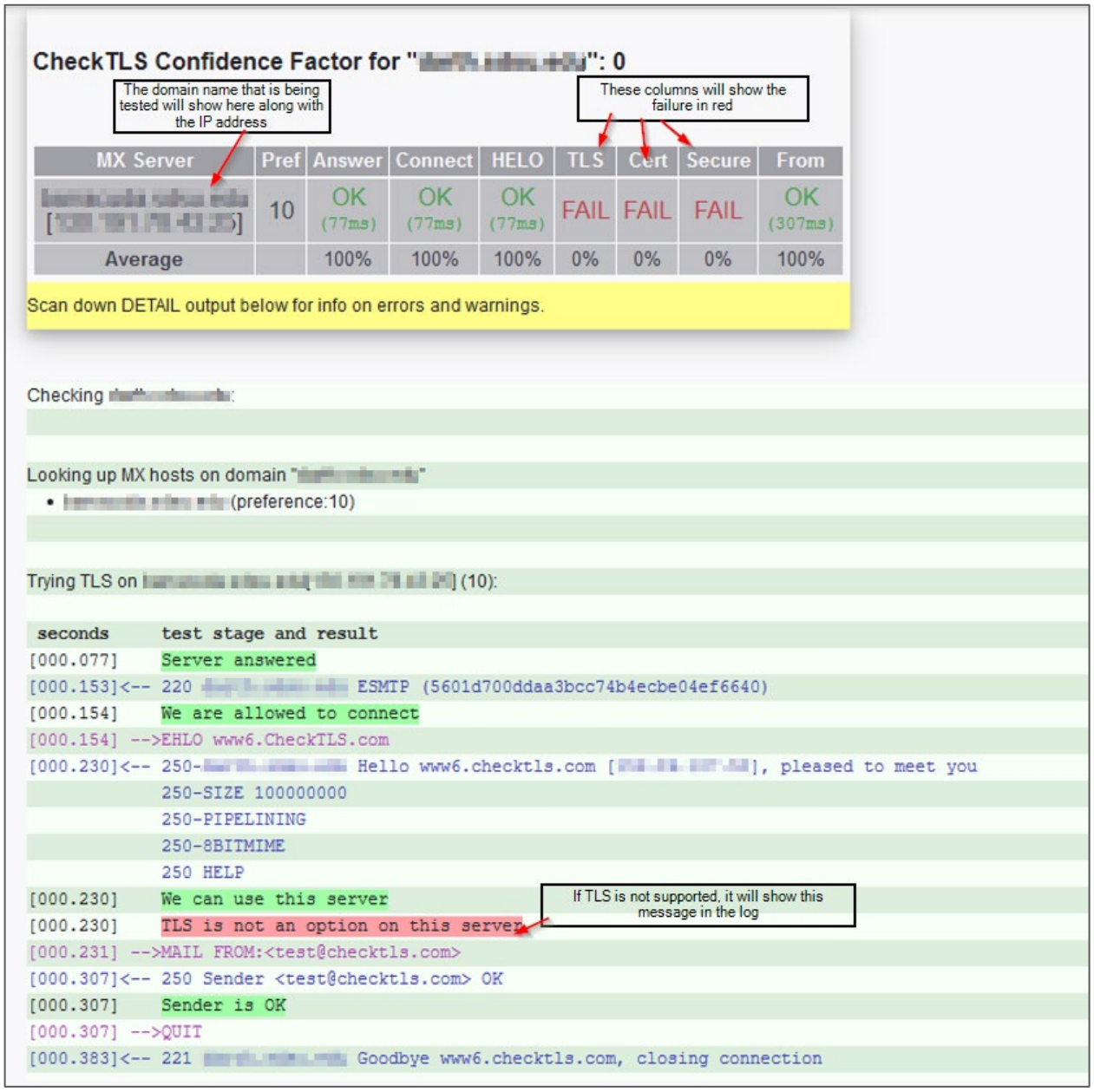
Your applicant will not receive your email if they use a domain name (i.e., Gmail, Hotmail, Outlook) that doesn't support **TLS**. You can perform a quick test to see if this is the problem.

Click on the link below to check your candidate's email domain for TLS support.

https://www.checktls.com/TestReceiver

Once you access the website, you will see the "TestReceiver parameter entry" box at the top left side. In the "eMail Target field," type the email domain of your candidate (i.e., gmail.com, Hotmail.com). Be sure to include the .com. Then click "Run Test."

The test will take several seconds.  Once completed, the page will present the diagnostics for that particular domain:




## The Fix

If your candidate's email domain fails this test, it means their email address is not secure.  To correct this problem and receive your emails, they will need to give you a different and secure email address to use.

## Reason 2: Email Spoofing

Another common reason your applicants are not receiving your emails is spoofing.

### What is Email Spoofing?

**Email spoofing** is the creation of email messages with a forged sender address, making the email appear to come from a legitimate source. Often someone you know and trust. Criminals use email spoofing to carry out phishing attacks, one of the most common security challenges facing companies today.

Typical email security protocols don't have a way to verify the email sender. So, the email will end up in your inbox, where it is likely you will mistake it for a legitimate email.

For more detailed information on email spoofing, reference this link:

https://en.wikipedia.org/wiki/Email_spoofing

If your company uses the **Domain Name System (DNS)**, your email system will reject the spoofed email. The Domain Name System (DNS) is the phonebook of the Internet. The emails get rejected because they are not on your list of authorized senders on the DNS.

Your IT team can fix this by updating the Sender Policy Framework **(SPF)** settings.

### What is Sender Policy Framework (SPF)?

SPF is a simple email validation system that helps protect email senders and recipients from spam, phishing, and spoofing. SPF checks to see that the mail server sending the email in question is authorized to send an email for that specific domain. The list of authorized sending hosts for domains is published in the Domain Name System (DNS).

For more detailed information on SPF, reference this link:

https://en.wikipedia.org/wiki/Sender_Policy_Framework

## The Fix

Your IT team can add the domain name of the email address or the IP address of the mail server to the SPF record. This action will ensure that emails from specific domains (i.e., CadientTalent.com) will be recognized, accepted, and delivered.

Example to include the domain name:

v=spf1 mx include:<clientname>.org include:mydomain.com –all

Example to include the mail server IP addresses:

v=spf1 mx include:<clientname>.org ip4:66.179.50.77 ip4:66.179.50.78 ip4:66.179.50.72 ip4:66.179.50.69 -all

Below is a tool to check an SPF record by entering the domain name :

http://mxtoolbox.com/SuperTool.aspx?action=mx:&run=toolpage#