

## My emails go directly to spam when I send them to Yahoo/Hotmail/Gmail. What can I do to prevent that from happening?

- 2023-04-04 - Spam

Υπάρχει περίπτωση να στέλνετε email από τον email λογαριασμό του hosting σας σε Yahoo, Hotmail, Gmail και αυτό να παραδίδεται σαν ανεπιθύμητη αλληλογραφία. Συνήθως, αυτό προκαλείται γιατί υπάρχουν πολύπλοκα antispam φίλτρα στον απομακρυσμένο διακομιστή που λανθασμένα θεωρούν τα μηνύματά σας ως spam. Οι απομακρυσμένοι email servers έχουν διαφορετικούς τύπους κανόνων προστασίας για την ανίχνευση των email που είναι Spam και ποιων δεν είναι. Ακριβής λύση σε αυτό το πρόβλημα δεν μπορεί να δοθεί. Στην Top.Host και συγκεκριμένα σε όλους τους Linux server μας, έχουμε εγκατεστημένο ήδη το SPF record.

Ένα πράγμα που μπορείτε να κάνετε είναι να ζητήσετε από τους παραλήπτες το μηνύματός σας, να προσθέσουν στην email διεύθυνσή σας στον διευθυνσιογράφο τους. Αυτή η διαδικασία πολλές φορές λύνει το πρόβλημα, αλλά είναι δύσκολο να υλοποιηθεί.

Επίσης παρακάτω μπορείτε να βρείτε κάποιες ενέργειες για την αύξηση της αξιοπιστίας της εξερχόμενης αλληλογραφίας σας ώστε να μην καταλήγει σε spam:

### 1. Ενεργοποίηση της DKIM εγγραφής στη DNS υπηρεσία του domain σας

Αφού συνδεθείτε στο Plesk σας, ακολουθήστε την διαδρομή **Websites & Domains** >> **Email Addresses** (κάτω από το domain που σας ενδιαφέρει) >> **Mail Settings** και τσεκάρετε το κουτάκι **Use DKIM spam protection system to sign outgoing email messages**. Σχετικές οδηγίες θα βρείτε [εδώ](#).

### 2. Προσθήκη SPF record αν δεν χρησιμοποιείτε ήδη.

Η συγκεκριμένη εγγραφή διασφαλίζει πως οι απομακρυσμένοι mail servers που διαθέτουν φίλτρα για έλεγχο SPF, θα δέχονται πάντα email από το domain σας αν χρησιμοποιείτε τον ίδιο server. Η παραπάνω διαδικασία, θεωρείται πολύ

αποτελεσματική στην καταπολέμηση της ανεπιθύμητης αλληλογραφίας αλλά και της πλαστογραφίας. Μπορείτε να προσθέσετε ή να τροποποιήσετε ένα SPF record μέσα από το DNS Settings στο Plesk σας.

Στους περισσότερους server μας είναι by default ενεργό αλλά θα πρέπει να ελέγξετε αν χρησιμοποιείτε κάποια εξωτερική mail υπηρεσία ώστε να τροποποιήσετε κατάλληλα το σχετικό record. Οδηγίες για αυτό θα βρείτε [εδώ](#).

### **3. Ενεργοποίηση DMARC εγγραφής στη DNS ζώνη του domain σας**

Ιδιαίτερα η Google, το τελευταίο διάστημα κάνει πολύ συχνά χρήση του DMARC μηχανισμού για τη διασφάλιση της εισερχόμενης προς αυτή αλληλογραφίας και επισημαίνει σαν spam μηνύματα που δεν τον χρησιμοποιούν. Οδηγίες για την προσθήκη DMARC θα βρείτε [εδώ](#).

### **4. Ενεργοποίηση SMTP authentication σε περίπτωση που χρησιμοποιείτε mail client για την διαχείριση της αλληλογραφίας σας authentication**

Αν χρησιμοποιείτε Outlook για την αποστολή των μηνυμάτων σας βεβαιωθείτε ότι είναι ενεργή η επιλογή "My outgoing server (SMTP) requires authentication". Οδηγίες για αυτό θα βρείτε [εδώ](#).

### **5. Έλεγχος αξιοπιστίας της εξερχόμενης αλληλογραφίας**

Μετά την πραγματοποίηση των παραπάνω ενεργειών από τη μεριά σας, ένα πολύ αξιόπιστο εργαλείο που μπορείτε να χρησιμοποιήσετε για τον έλεγχο της αξιοπιστίας της εξερχόμενης αλληλογραφίας σας είναι το [παρακάτω](#).