6 Δεκεμβρίου 2022

Εντοπισμός του πραγματικού αποστολέα στο Gmail

/ Επιστήμες, Τέχνες & Πολιτισμός

Δείτε πως μπορείτε να εντοπίσετε τον πραγματικό αποστολέα ενός ηλεκτρονικού ταχυδρομείου του Gmail καθώς και αν αυτό μπορεί να είναι επικίνδυνο.

Το πρώτο πράγμα που κάνετε όταν δείτε ότι έχετε νέο μήνυμα στο Gmail σας είναι να ελέγξετε τον αποστολέα, σωστά; Είναι ο πιο γρήγορος τρόπος για να καταλάβετε από ποιον προέρχεται το email, καθώς και το αν έχει έρθει κάτι ενδιαφέρον ή όχι.

Όμως κάθε email συνοδεύεται από πολύ περισσότερες πληροφορίες από αυτές που εμφανίζονται στα περισσότερα προγράμματα παραλαβής και αποστολής email. Υπάρχει πλήθος πληροφοριών σχετικά με τον αποστολέα που περιλαμβάνονται στην κεφαλίδα του email. Πληροφορίες που μπορείτε να χρησιμοποιήσετε για να εντοπίσετε την πραγματική πηγή και άλλες λεπτομέρειες.

Δείτε πώς μπορείτε να εντοπίσετε από που προήρθε πραγματικά ένα μήνυμα ηλεκτρονικού ταχυδρομείου και γιατί πρέπει να το κάνετε.

Γιατί να εντοπίσετε μια διεύθυνση email;
Η απάντηση είναι προφανής. Στην εποχή μας, τα κακόβουλα email είναι πάρα πολλά. Οι απάτες, τα ανεπιθύμητα μηνύματα, τα κακόβουλα προγράμματα και τα μηνύματα ηλεκτρονικού ψαρέματος είναι ένα κοινό φαινόμενο στα εισερχόμενα κάθε προγράμματος διαχείρισης ηλεκτρονικού ταχυδρομείου.

Εάν εντοπίσετε ένα email πίσω στην πηγή του, έχετε μια καλή πιθανότητα να ανακαλύψετε από ποιον (ή από πού) προέρχεται το email και αν αυτό είναι

επικίνδυνο.

Σε άλλες περιπτώσεις, μπορείτε να εντοπίσετε την προέλευση ενός μηνύματος ηλεκτρονικού ταχυδρομείου για να αποκλείσετε μια επίμονη πηγή ανεπιθύμητου ή καταχρηστικού περιεχομένου, αφαιρώντας το οριστικά από τα εισερχόμενά σας. Οι διαχειριστές διακομιστών εντοπίζουν μηνύματα ηλεκτρονικού ταχυδρομείου για τον ίδιο λόγο.

Πώς να δείτε τις πλήρης λεπτομέρειες ενός email

Μπορείτε να εντοπίσετε την διεύθυνση email του αποστολέα κοιτάζοντας την πλήρη κεφαλίδα του email. Η κεφαλίδα email (header) περιέχει πληροφορίες δρομολόγησης και μεταδεδομένα email, πληροφορίες που συνήθως δεν σας ενδιαφέρουν. Αλλά αυτές οι πληροφορίες είναι ζωτικής σημασίας για τον εντοπισμό της πηγής του μηνύματος του ηλεκτρονικού ταχυδρομείου.

Τα περισσότερα προγράμματα ηλεκτρονικού ταχυδρομείου δεν εμφανίζουν άμεσα την πλήρη κεφαλίδα του email, επειδή είναι γεμάτη τεχνικά δεδομένα και κάπως άχρηστη για ένα μη εκπαιδευμένο μάτι. Ωστόσο, τα περισσότερα προγράμματα email προσφέρουν έναν τρόπο ελέγχου της πλήρους κεφαλίδας αυτών. Απλά πρέπει να ξέρετε πού να κοιτάξετε, καθώς και τι κοιτάτε.

Για τα πιο κοινά προγράμματα ο τρόπος για να εισέλθετε σε αυτές τις πληροφορίες είναι:

Gmail: Ανοίξτε τον λογαριασμό σας στο Gmail και, στη συνέχεια, ανοίξτε το email που θέλετε να ανιχνεύσετε. Επιλέξτε το αναπτυσσόμενο μενού στην επάνω δεξιά γωνία και, στη συνέχεια, “Προβολή Αρχικού” από το μενού.
Outlook : Κάντε διπλό κλικ στο email που θέλετε να ανιχνεύσετε, μεταβείτε στο Αρχείο > Ιδιότητες. Οι πληροφορίες εμφανίζονται στις κεφαλίδες του διαδικτύου.
Apple Mail: Ανοίξτε το email που θέλετε να ανιχνεύσετε και, στη συνέχεια, μεταβείτε στο View > Message > Raw Source.
Φυσικά, υπάρχουν και άλλα αμέτρητα προγράμματα διαχείρισης email. Μια γρήγορη αναζήτηση στο διαδίκτυο θα αποκαλύψει πώς να βρείτε την πλήρη κεφαλίδα email στο πρόγραμμα της επιλογής σας. Μόλις ανοίξετε την κεφαλίδα του email, θα καταλάβετε τι εννοούσαμε με τον όρο “γεμάτη τεχνικά δεδομένα”.

Κατανόηση των δεδομένων σε μια πλήρη κεφαλίδα email
Αυτό που θα δείτε σε μία πλήρη κεφαλίδα email έχει πολλές πληροφορίες. Ωστόσο, λάβετε υπόψη τα εξής: διαβάζετε την κεφαλίδα του email χρονολογικά, από κάτω προς τα πάνω (δηλαδή, οι παλαιότερες πληροφορίες στο κάτω μέρος) και ότι κάθε νέος διακομιστής μέσω του οποίου ταξιδεύει το email προσθέτει και την δικιά του

κεφαλίδα Received (Λήφθηκε).

Δείτε αυτό το δείγμα κεφαλίδας ηλεκτρονικού ταχυδρομείου από το λογαριασμό μας στο iGuru Gmail:

Υπάρχουν πολλές πληροφορίες. Ας τις αναλύσουμε. Αρχικά, κατανοήστε τι σημαίνει κάθε γραμμή (διαβάζοντας από κάτω προς τα πάνω).

♦ DATE (Ημερομηνία): Η ημερομηνία που στάλθηκε το email

♦ Το (Προς): Τους προβλεπόμενους παραλήπτες του μηνύματος ηλεκτρονικού ταχυδρομείου. Μπορεί να εμφανίζει πολλές διευθύνσεις.

♦ Content-type (Τύπος περιεχομένου): Λέει στο πρόγραμμα περιήγησής σας ή στο πρόγραμμα του ηλεκτρονικού ταχυδρομείου πώς να ερμηνεύσει το περιεχόμενο

του μηνύματος ηλεκτρονικού ταχυδρομείου.

♦ MIME-Version: Δηλώνει το πρότυπο μορφής email σε χρήση. Η έκδοση MIME είναι συνήθως “1.0.”

♦ Subject (Θέμα): Το θέμα του περιεχομένου του email.

♦ Message-ID: Η ταυτότητα του email. Είναι σαν ένα ψηφιακό δακτυλικό αποτύπωμα ενός μηνύματος και συνήθως προστίθεται από τον διακομιστή αλληλογραφίας που στέλνει το μήνυμά σας για λογαριασμό του προγράμματος-πελάτη της αλληλογραφίας σας.

♦ From (Από): Εμφανίζει τον αποστολέα του μηνύματος. Είναι εύκολο να παραποιηθεί.

♦ DKIM-Signature (DKIM-Υπογραφή): Domain Keys Identified Mail. Ελέγχει την ταυτότητα του domain από τον οποίο στάλθηκε το email και προστατεύει από πλαστογράφηση και απάτη του αποστολέα.

♦ Received-SPF: Το Send Policy Framework (SPF) αποτελεί μέρος της διαδικασίας ελέγχου ταυτότητας email που σταματά την πλαστογράφηση της διεύθυνσης αποστολέα.

♦ Received (Λήφθηκε): Η γραμμή “Received” παραθέτει κάθε server (διακομιστή) από τον οποίο ταξιδεύει το email πριν φτάσει στα εισερχόμενά σας. Διαβάζετε τις γραμμές “Received” από κάτω προς τα πάνω. Το κατώτατο Received είναι και ο δημιουργός του email.

♦ Return-Path (Διαδρομή επιστροφής): Η τοποθεσία όπου καταλήγουν τα μηνύματα που δεν αποστέλλονται ή αναπηδούν.

♦ ARC-Authentication-Results (ARC-Έλεγχος ταυτότητας-Αποτελέσματα): Το Authenticated Receive Chain είναι ένα άλλο πρότυπο ελέγχου ταυτότητας. Το ARC επαληθεύει τις ταυτότητες των διαμεσολαβητών email και των διακομιστών που προωθούν το μήνυμά σας στον τελικό προορισμό του.

♦ ARC-Message-Signature (ARC-Μήνυμα-Υπογραφή): Η υπογραφή λαμβάνει ένα στιγμιότυπο των πληροφοριών της κεφαλίδας του μηνύματος για επικύρωση. Παρόμοιο με το DKIM.

♦ ARC-Seal (ARC-σφράγιση): “Σφραγίζει” τα αποτελέσματα ελέγχου ταυτότητας ARC και την υπογραφή του μηνύματος, επαληθεύοντας το περιεχόμενό τους. Παρόμοιο με το DKIM.

♦ X-Received: Διαφέρει από το “Received” στο ότι θεωρείται μη τυπικό. Δηλαδή, μπορεί να μην είναι μόνιμη διεύθυνση, όπως ένας παράγοντας μεταφοράς αλληλογραφίας ή διακομιστής SMTP Gmail.

♦ X-Google-Smtp-Source: Εμφανίζει τη μεταφορά email χρησιμοποιώντας έναν διακομιστή SMTP Gmail.

♦ Received (Λήφθηκε): Δεύτερος σταθμός “Received” πριν το email φτάσει σε εσάς. Είναι ο No2 server (διακομιστή) από τον οποίο ταξιδεύει το email. Σας θυμίζουμε ότι πρέπει να διαβάζετε τις γραμμές “Received” από κάτω προς τα πάνω. Το κατώτατο Received είναι και ο δημιουργός του email.

♦ Delivered-To (Παραδόθηκε σε): Ο τελικός παραλήπτης του μηνύματος ηλεκτρονικού ταχυδρομείου.

♦ X-Forwarded-For: Υποδεικνύει ότι ένα μήνυμα email προωθήθηκε από έναν ή περισσότερους άλλους λογαριασμούς (πιθανώς αυτόματα). Αν τα email είναι ενοχλητικά στείλτε email στη πρώτη διεύθυνση στο τμήμα X-Forwarded-For και πείτε τους να σταματήσουν την αυτόματη προώθηση των email τους.

♦ X-Forwarded-To: Υποδεικνύει ότι ένα μήνυμα email προωθήθηκε από έναν ή περισσότερους άλλους λογαριασμούς (πιθανώς αυτόματα).

Πέραν των παραπάνω, πιθανά θα συναντήσετε και τα (που δεν τα χωράει στην φωτογραφία του παραδείγματός μας):

♦ Authentication-Results (Έλεγχος ταυτότητας-Αποτελέσματα): Περιέχει ένα αρχείο των ελέγχων ελέγχου ταυτότητας που πραγματοποιήθηκαν. Μπορεί να περιέχει περισσότερες από μία μεθόδους ελέγχου ταυτότητας.

♦ Replay-To (Απάντηση σε): Η διεύθυνση email στην οποία στέλνετε την απάντησή σας.

Το βασικό είναι ότι δεν χρειάζεται να καταλάβετε τι σημαίνουν όλα αυτά για να εντοπίσετε ένα email. Αλλά αν μάθετε που να κοιτάτε μέσα στην κεφαλίδα του email, μπορείτε γρήγορα να αρχίσετε να εντοπίζετε τον αποστολέα του email.

Ανίχνευση του αρχικού αποστολέα ενός email

Για να εντοπίσετε τη διεύθυνση IP του αρχικού αποστολέα email , κατευθυνθείτε στο πρώτο Received (Λήφθηκε) στην κεφαλίδα του email. Δίπλα στην πρώτη γραμμή Received βρίσκεται η διεύθυνση IP του διακομιστή (server) που έστειλε το email.

Μερικές φορές, αυτό εμφανίζεται ως X-Originating-IP ή Original-IP. Μπορεί να μην δείτε IP αλλά το domain του server.

Αντιγράψτε τη διεύθυνση IP και, στη συνέχεια, κατευθυνθείτε στο MX Toolbox . Εισαγάγετε τη διεύθυνση IP στο πλαίσιο, αλλάξτε τον τύπο αναζήτησης σε Reverse Lookup (Αντίστροφη αναζήτηση) χρησιμοποιώντας το αναπτυσσόμενο μενού και, στη συνέχεια, πατήστε Enter.

Τα αποτελέσματα αναζήτησης θα εμφανίσουν μια ποικιλία πληροφοριών που σχετίζονται με τον διακομιστή αποστολής.

Αν η αρχική διεύθυνση IP είναι μία από τις εκατομμύρια ιδιωτικές διευθύνσεις IP, σε αυτή την περίπτωση, θα εμφανιστεί το μήνυμα ότι είναι ιδιωτική και δεν θα επιστρέψει κάποιο αποτέλεσμα.

Στο δικό μας το παράδειγμα δεν χρειάστηκε αντίστροφη αναζήτηση καθώς το header του email μας έδωσε σαν πρώτο αποστολέα το mailb-dc.linkedin.com και έτσι γνωρίζουμε ότι είναι από το Linkedin.

Δωρεάν εργαλεία για τον εντοπισμό email και διευθύνσεων IP

Φυσικά, υπάρχουν στο διαδίκτυο μερικά εύχρηστα εργαλεία που αυτοματοποιούν αυτή τη διαδικασία για εσάς. Είναι ορθότερο να γνωρίζετε για τα header των emails και τις πληροφορίες που μεταφέρουν, αλλά μερικές φορές χρειάζεστε γρήγορες πληροφορίες.

Επιπλέον, θέλετε να ανιχνεύσετε τα μηνύματα ηλεκτρονικού ταχυδρομείου δωρεάν, χωρίς συνδρομή ή εγγραφή. Γιαυτό δείτε τους παρακάτω αναλυτές header:

GSuite Toolbox Messageheader (της ίδιας της Goolge)
MX Toolbox Email Header Analyzer
IP-Address Email Header Trace (αναλυτής κεφαλίδας email + ιχνηλάτης διεύθυνσης IP)

Μπορείτε πραγματικά να εντοπίσετε μια διεύθυνση IP από ένα email;

Υπάρχουν περιπτώσεις όπου ο εντοπισμός μιας διεύθυνσης IP μέσω της κεφαλίδας του email είναι χρήσιμος. Ιδιαίτερα σε ενοχλητικούς αποστολείς που στέλνουν διαφημιστικά μηνύματα, ή ανεπιθύμητη αλληλογραφία, αλλά και για να βρείτε την πηγή μηνυμάτων ηλεκτρονικού ψαρέματος.

Λάβετε υπόψη ότι ορισμένα μηνύματα ηλεκτρονικού ταχυδρομείου θα προέρχονται μόνο από συγκεκριμένες τοποθεσίες. Για παράδειγμα, τα email σας στο PayPal δεν θα προέρχονται από την Κίνα ! Αν δείτε κάτι τέτοιο προφανώς και είναι ψεύτικο email.

Όμως ο ακριβής εντοπισμός της προέλευσης ενός email δεν είναι πάντα εύκολος. Καθώς ένας τεράστιος αριθμός ανθρώπων χρησιμοποιεί δωρεάν υπηρεσίες email όπως το Gmail, το Outlook και το Yahoo, η ανίχνευση ενός email που αποστέλλεται από αυτές τις υπηρεσίες ώστε να βρείτε την πραγματική διεύθυνση IP που σχετίζεται με τον αποστολέα παραμένει εξαιρετικά δύσκολη.

Πηγή: iguru.gr