ΠΡΟΣΟΧΗ ΣΤΑ ΥΠΟΠΤΑ EMAIL

Πρακτικός οδηγός αναγνώρισης phishing

ΣΤΑΜΑΤΩ • ΕΛΕΓΧΩ • ΕΠΙΒΕΒΑΙΩΝΩ • ΑΝΑΦΕΡΩ

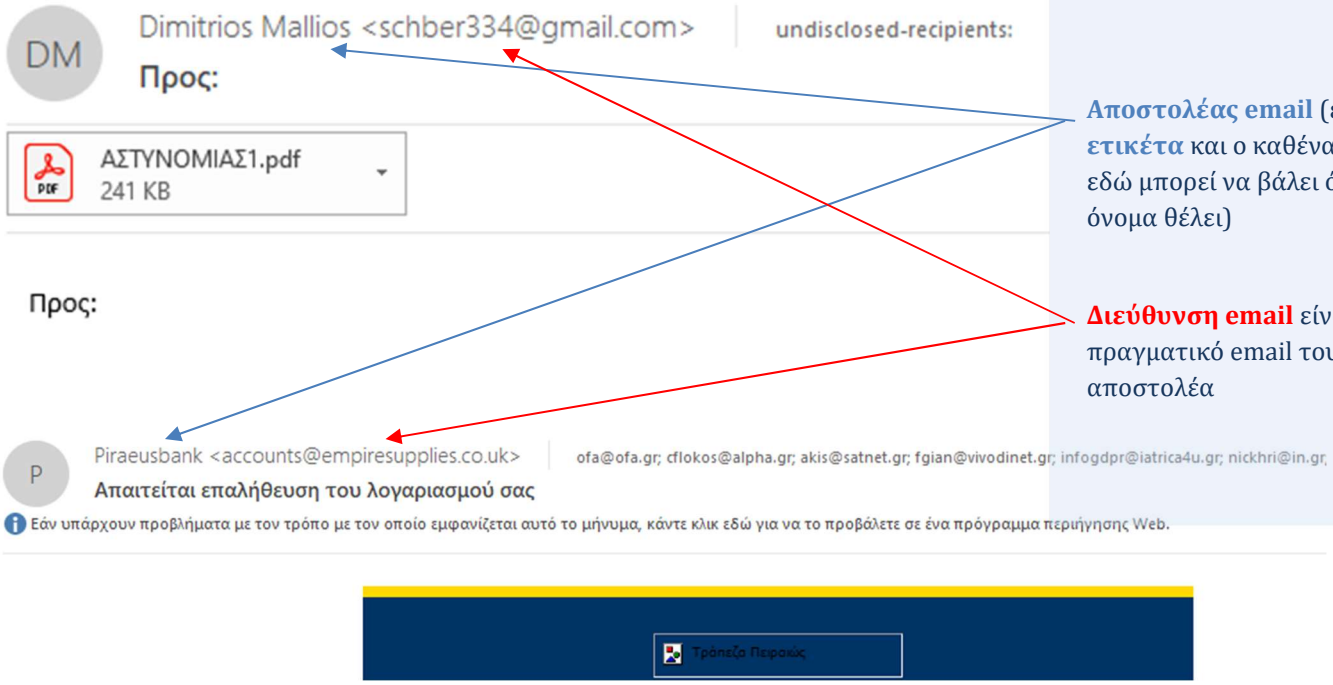
Αν το μήνυμα φαίνεται επείγον, απειλητικό ή υπερβολικά καλό για να είναι αληθινό, δεν πατάμε σύνδεσμο και δεν ανοίγουμε συνημμένο πριν επαληθεύσουμε τη γνησιότητά του.

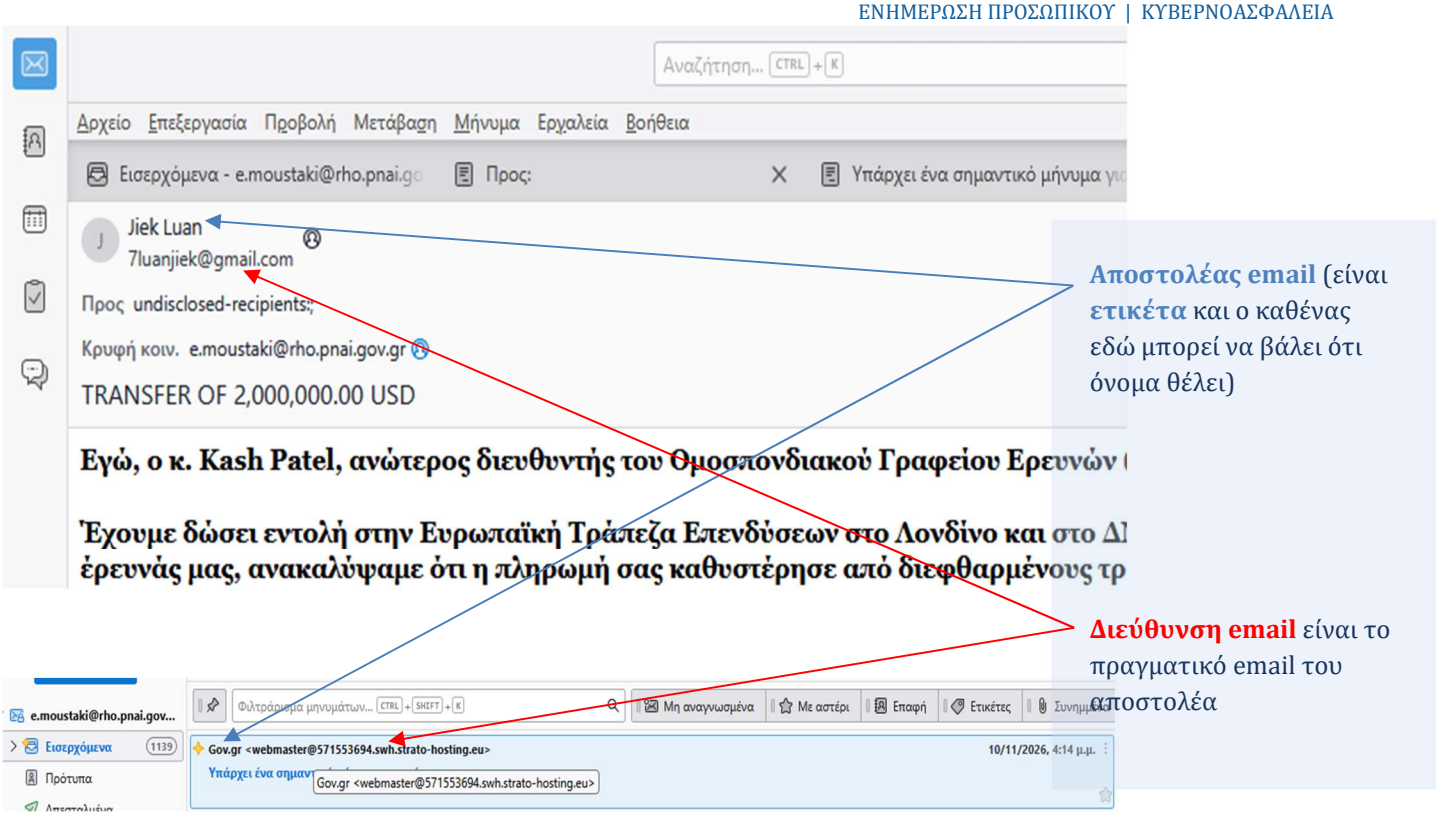
Γιατί μας αφορά

Ένα μόνο παραπλανητικό μήνυμα μπορεί να οδηγήσει σε υποκλοπή κωδικών, παραβίαση υπηρεσιακού λογαριασμού, διαρροή προσωπικών δεδομένων πολιτών ή μόλυνση υπολογιστή. Τα μηνύματα συχνά χρησιμοποιούν ονόματα δημόσιων αρχών, τραπεζών και γνωστών οργανισμών.

Βήμα 1 — Ελέγχουμε τον πραγματικό αποστολέα

- Στον Thunderbird, τοποθετούμε τον κέρσορα του ποντικιού πάνω από τον αποστολέα του email για να εμφανιστεί ένα αναδυόμενο παράθυρο με περισσότερα στοιχεία προκειμένου να ελέγξουμε τον λογαριασμό του email.
  Προσοχή μας ενδιαφέρει η διεύθυνση του email (πχ: schber334@gmail.com ή accounts@empiresupplies.co.uk ή webmaster@571553694.swh.strato-hosting.eu και όχι το όνομα/η ετικέτα του (π.χ. «Dimitrios Mallios", ή «Piraeusbank» ή «Gov.gr»).
- Ένα όνομα φορέα ή λογότυπο μπορεί εύκολα να αντιγραφεί.
- **ΟΜΩΣ:** Ακόμη και μια φαινομενικά κανονική διεύθυνση δεν αποδεικνύει ασφάλεια: ένας πραγματικός λογαριασμός μπορεί να έχει παραβιαστεί ή η διεύθυνση να έχει πλαστογραφηθεί.





Βήμα 2 — Διαβάζουμε προσεκτικά το αίτημα

- Προσοχή σε απειλές με δικαστικές ενέργειες, χρονικές προθεσμίες («εντός 48 ωρών»), μεγάλα χρηματικά ποσά και αιτήματα άμεσης επαλήθευσης.
- Δεν δίνουμε ποτέ κωδικούς, κωδικούς μιας χρήσης (OTP), στοιχεία ταυτότητας ή τραπεζικά δεδομένα ως απάντηση σε ανεπιβεβαίωτο email.

Βήμα 3 — Ελέγχουμε τους συνδέσμους χωρίς να τους ανοίγουμε

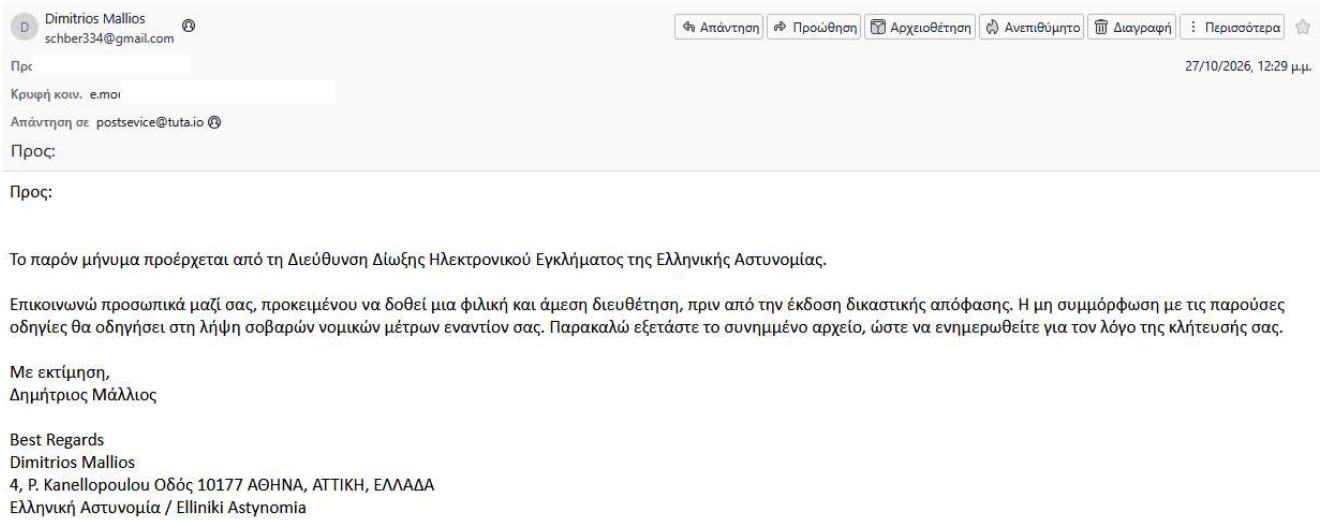
- Σε υπολογιστή, αφήνουμε το ποντίκι πάνω από το κουμπί ή τον σύνδεσμο, χωρίς κλικ, και διαβάζουμε τον πραγματικό προορισμό. Αν δεν φαίνεται καθαρά, δεν τον ανοίγουμε.
- Δεν εμπιστευόμαστε σύντομους, περίεργους ή άσχετους συνδέσμους. Επισκεπτόμαστε την υπηρεσία από δικό μας σελιδοδείκτη ή πληκτρολογώντας την επίσημη διεύθυνση.

ΣΗΜΑΝΤΙΚΟ

Το HTTPS και το εικονίδιο λουκέτου δείχνουν κρυπτογραφημένη σύνδεση· δεν πιστοποιούν ότι ο ιστότοπος είναι ο πραγματικός φορέας. Η σωστή ορθογραφία και η επαγγελματική εμφάνιση δεν αρκούν.

Πραγματικά περιστατικά που έφτασαν στην υπηρεσία τις τελευταίες μέρες.

Παράδειγμα 1 — Ψευδής Ελληνική Αστυνομία / Δίωξη Ηλεκτρονικού Εγκλήματος



Dimitrios Mallios
schber334@gmail.com

Απάντηση | Προώθηση | Αρχειοθέτηση | Ανεπιθύμητο | Διαγραφή | Περισσότερα

Πρς

27/10/2026, 12:29 μ.μ.

Κρυφή κοιν. e.mo

Απάντηση σε postsevice@tuta.io

Προς:

Προς:

Το παρόν μήνυμα προέρχεται από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας.

Επικοινωνώ προσωπικά μαζί σας, προκειμένου να δοθεί μια φιλική και άμεση διευθέτηση, πριν από την έκδοση δικαστικής απόφασης. Η μη συμμόρφωση με τις παρούσες οδηγίες θα οδηγήσει στη λήψη σοβαρών νομικών μέτρων εναντίον σας. Παρακαλώ εξετάστε το συνημμένο αρχείο, ώστε να ενημερωθείτε για τον λόγο της κλήτευσής σας.

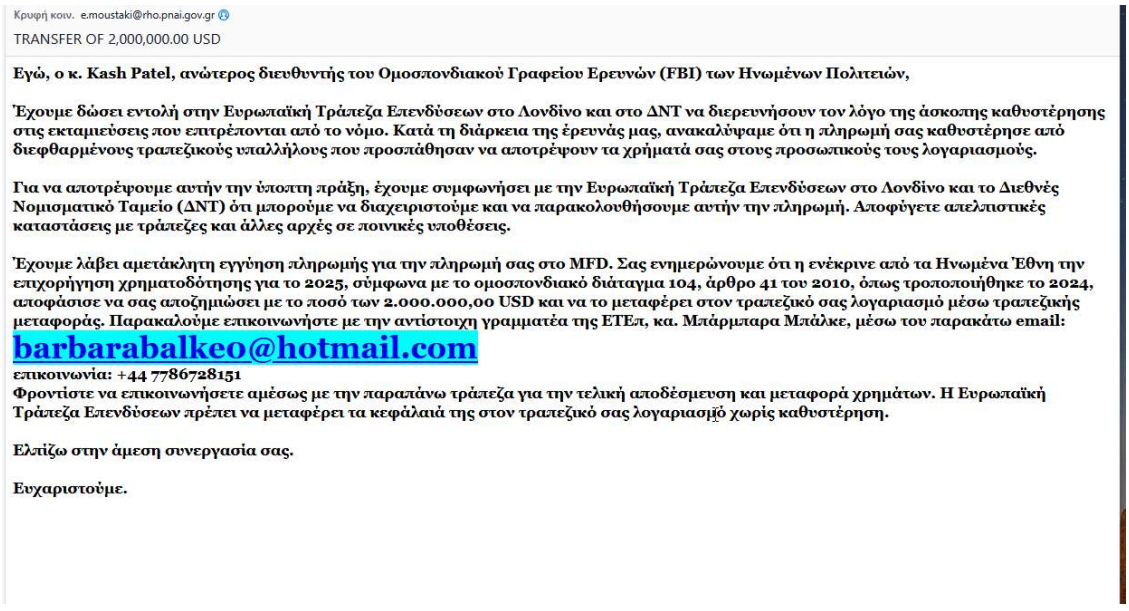
Με εκτίμηση,
Δημήτριος Μάλλιος

Best Regards
Dimitrios Mallios
4, P. Kanellopoulou Οδός 10177 ΑΘΗΝΑ, ΑΤΤΙΚΗ, ΕΛΛΑΔΑ
Ελληνική Αστυνομία / Elliniki Astynomia

Εικόνα 1. Επίκληση δημόσιας αρχής και απειλή για νομικές συνέπειες.

Τι παρατηρούμε: προσωπική διεύθυνση Gmail αντί για επαληθευμένη υπηρεσιακή επικοινωνία, εκφοβιστικό ύφος και παρότρυνση να εξεταστεί συνημμένο αρχείο. Δεν ανοίγουμε συνημμένο.

Παράδειγμα 2 — «FBI» και μεταφορά 2.000.000 USD



Κρυφή κοιν. e.moustaki@rho.pnai.gov.gr

TRANSFER OF 2,000,000.00 USD

Εγώ, ο κ. Kash Patel, ανώτερος διευθυντής του Ομοσπονδιακού Γραφείου Ερευνών (FBI) των Ηνωμένων Πολιτειών,

Έχουμε δώσει εντολή στην Ευρωπαϊκή Τράπεζα Επενδύσεων στο Λονδίνο και στο ΔΝΤ να διερευνήσουν τον λόγο της άσκοπης καθυστέρησης στις εκταμιεύσεις που επιτρέπονται από το νόμο. Κατά τη διάρκεια της έρευνάς μας, ανακαλύψαμε ότι η πληρωμή σας καθυστέρησε από διεφθαρμένους τραπεζικούς υπαλλήλους που προσπάθησαν να αποτρέψουν τα χρήματά σας στους προσωπικούς τους λογαριασμούς.

Για να αποτρέψουμε αυτήν την ύποπτη πράξη, έχουμε συμφωνήσει με την Ευρωπαϊκή Τράπεζα Επενδύσεων στο Λονδίνο και το Διεθνές Νομισματικό Ταμείο (ΔΝΤ) ότι μπορούμε να διαχειριστούμε και να παρακολουθήσουμε αυτήν την πληρωμή. Αποφύγετε απελπιστικές καταστάσεις με τράπεζες και άλλες αρχές σε ποινικές υποθέσεις.

Έχουμε λάβει αμετάκλητη εγγύηση πληρωμής για την πληρωμή σας στο MFD. Σας ενημερώνουμε ότι η ενέκρινε από τα Ηνωμένα Έθνη την επιχορήγηση χρηματοδότησης για το 2025, σύμφωνα με το ομοσπονδιακό διάταγμα 104, άρθρο 41 του 2010, όπως τροποποιήθηκε το 2024, αποφάσισε να σας αποζημιώσει με το ποσό των 2.000.000,00 USD και να το μεταφέρει στον τραπεζικό σας λογαριασμό μέσω τραπεζικής μεταφοράς. Παρακαλούμε επικοινωνήστε με την αντίστοιχη γραμματέα της ΕΤΕπ, κα. Μπάρμπαρα Μπάλκε, μέσω του παρακάτω email:

barbarabalkeo@hotmail.com

επικοινωνία: +44 7786728151

Φροντίστε να επικοινωνήσετε αμέσως με την παραπάνω τράπεζα για την τελική αποδέσμευση και μεταφορά χρημάτων. Η Ευρωπαϊκή Τράπεζα Επενδύσεων πρέπει να μεταφέρει τα κεφάλαιά της στον τραπεζικό σας λογαριασμό χωρίς καθυστέρηση.

Ελπίζω στην άμεση συνεργασία σας.

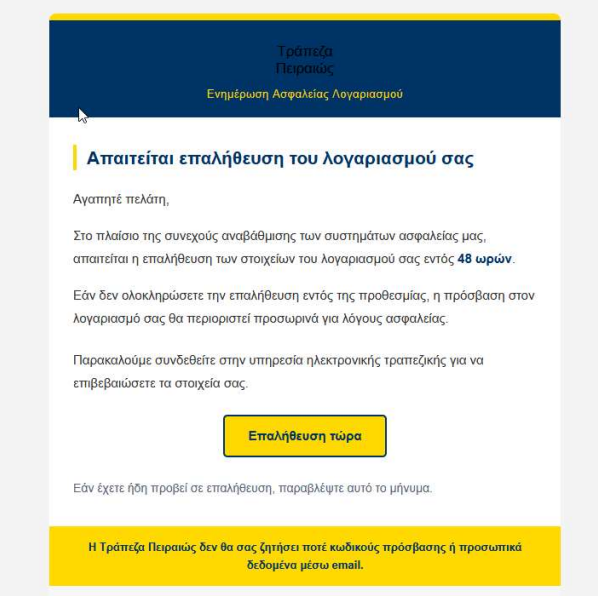
Ευχαριστούμε.

Εικόνα 2. Υπόσχεση χρημάτων και επικοινωνία μέσω προσωπικής διεύθυνσης Hotmail.

Τι παρατηρούμε: απίθανη οικονομική υπόσχεση, αυθαίρετη επίκληση διεθνών αρχών και οδηγία επικοινωνίας σε προσωπικό email. Δεν απαντάμε και δεν αποστέλλουμε προσωπικά ή τραπεζικά στοιχεία.

Πραγματικά περιστατικά — συνέχεια

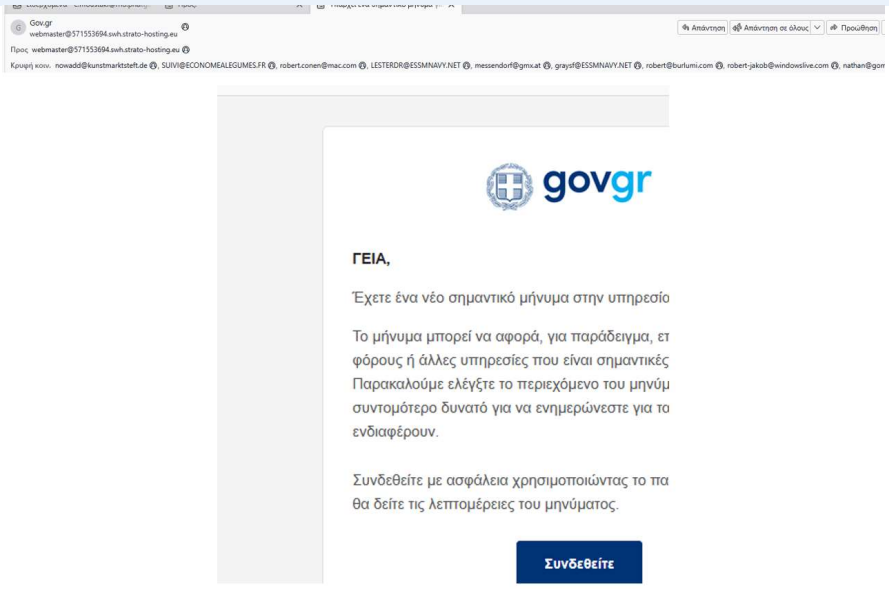
Παράδειγμα 3 — Υποτιθέμενη ειδοποίηση Τράπεζας Πειραιώς



Εικόνα 3. Προειδοποίηση για περιορισμό πρόσβασης και κουμπί «Επαλήθευση τώρα».

Τι παρατηρούμε: προθεσμία 48 ωρών, φόβο απώλειας πρόσβασης και κουμπί επαλήθευσης. Τα εταιρικά χρώματα δεν αποδεικνύουν γνησιότητα. Ελέγχουμε τυχόν ειδοποιήσεις μόνο από την επίσημη εφαρμογή ή από ιστότοπο που ανοίγουμε μόνοι μας.

Παράδειγμα 4 — Υποτιθέμενο μήνυμα «Gov.gr» (11/11/2026)



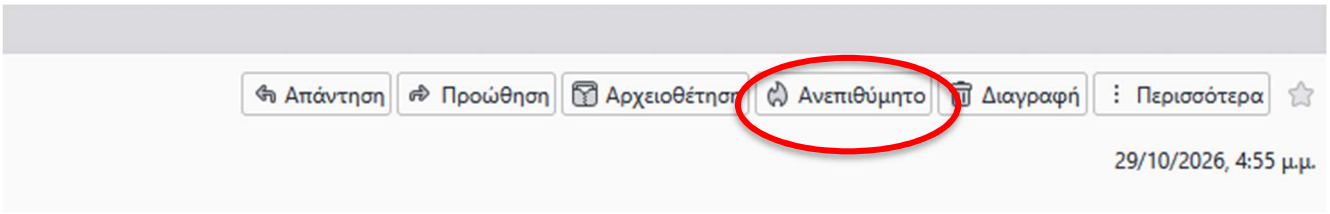
Εικόνα 4. Το όνομα «Gov.gr» δεν συμφωνεί με το domain της διεύθυνσης αποστολέα.

Τι παρατηρούμε: εμφανιζόμενο όνομα «Gov.gr» αλλά πραγματική διεύθυνση webmaster@571553694.swh.strato-hosting.eu, γενικόλογο «σημαντικό μήνυμα», κουμπί «Συνδεθείτε» και ασυνήθιστα πολλούς παραλήπτες σε κρυφή κοινοποίηση. Δεν πατάμε το κουμπί.

Τι κάνουμε στην πράξη

Αν λάβουμε ύποπτο email

- Δεν ανοίγουμε συνημμένα και δεν πατάμε κουμπιά ή συνδέσμους.
- Δεν απαντάμε, δεν καλούμε αριθμούς που αναφέρονται μέσα στο μήνυμα και δεν το προωθούμε μαζικά σε συναδέλφους.
- Επικοινωνούμε με τον φερόμενο αποστολέα από ανεξάρτητο, επίσημο κανάλι, αν χρειάζεται να επαληθεύσουμε το αίτημα.
- Το επισημαίνουμε ως ανεπιθύμητο.
- Το διαγράφουμε.



Αν έχουμε ήδη πατήσει σύνδεσμο ή ανοίξει συνημμένο

- Σταματάμε αμέσως την αλληλεπίδραση και ενημερώνουμε χωρίς καθυστέρηση την ΓΔΨΛ, ακόμη κι αν δεν υπάρχει ορατό πρόβλημα.
- Αναφέρουμε το μήνυμα στη Γενική Διεύθυνση Ψηφιακής Λειτουργίας (ΓΔΨΛ).
- Περιγράφουμε τι κάναμε και πότε (κλικ, λήψη αρχείου, εκτέλεση, πληκτρολόγηση δεδομένων).
- Αν δώσαμε κωδικό ή OTP, ζητάμε άμεση αντιμετώπιση λογαριασμού: αλλαγή κωδικού από την πραγματική υπηρεσία με ασφαλή τρόπο, ανάκληση ενεργών συνεδριών και έλεγχο για μη εξουσιοδοτημένη πρόσβαση.
- Αν εκτελέσαμε αρχείο ή παρατηρούμε ύποπτη συμπεριφορά, ακολουθούμε τις οδηγίες της ΓΔΨΛ για απομόνωση και έλεγχο του υπολογιστή. Δεν επιχειρούμε μόνοι μας «καθαρισμό».