



Κυβερνοασφάλεια

Θέματα ασφάλειας Ηλεκτρονικών Υπηρεσιών

Παναγιώτης Βαβίλης
ΕΤΕΠ Τμ. Επιστήμης Υπολογιστών
ΥΑΣΠΕ Πανεπιστημίου Κρήτης



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

digiGOV
innoHUB



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE



Ασφαλής πλοήγηση & χρήση ψηφιακών υπηρεσιών



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

 **digiGOV**
innoHUB



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Προσωπική συσκευή

Προσωπική συσκευή είναι κάθε ηλεκτρονική συσκευή που ανήκει ή χρησιμοποιείται κυρίως από ένα άτομο—π.χ. κινητό, tablet, φορητός υπολογιστής, έξυπνο ρολόι. Περιέχει προσωπικά δεδομένα (φωτογραφίες, μηνύματα, λογαριασμούς) και συχνά πρόσβαση σε υπηρεσίες/εργασία.



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

digiGOV
innoHUB



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Γιατί οι προσωπικές συσκευές είναι κρίσιμες για την ασφάλεια

- Είναι ο πιο συχνός στόχος (phishing, malware, SIM-swap, κλοπή)
- Ένα παραβιασμένο κινητό/laptop = γέφυρα προς εταιρικά συστήματα
- Κινούνται παντού → έκθεση σε δημόσια Wi-Fi, απώλεια/κλοπή
- Ένας οικιακός υπολογιστής ή κινητό μπορεί να χρησιμοποιηθεί από παιδιά

Γιατί να ενημερώνω τις συσκευές μου

- Τα updates κλείνουν «τρύπες» ασφαλείας που εκμεταλλεύονται οι επιτιθέμενοι
- Βελτιώνουν την προστασία (antimalware, firewall, secure boot)
- Διορθώνουν σφάλματα που μπορεί να οδηγήσουν σε διαρροή δεδομένων
- Αναβαθμίζουν εφαρμογές & προγράμματα οδήγησης (drivers) που είναι στόχοι
- Συχνά ενεργοποιούν αυτόματα νεότερα επίπεδα κρυπτογράφησης/ιδιωτικότητας
- **Μη ενημερωμένη συσκευή = εύκολος στόχος** για phishing, ransomware, account takeovers



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Τι να κάνω στην πράξη (κινητό, laptop, κ.λπ.)

- Ενεργοποιώ **Auto-Update** για λειτουργικό & εφαρμογές
- Εφαρμόζω κρίσιμες ενημερώσεις άμεσα· προγραμματίζω τις υπόλοιπες εκτός ωραρίου
- Κατεβάζω **apps** μόνο από επίσημα stores/ιστότοπους· αποφεύγω “σπασμένες” εκδόσεις
- Στην περίπτωση δικής μου συσκευής δημιουργώ διαφορετικό λογαριασμό χρήστη για τα υπόλοιπα μέλη της οικογένειας ή γενικά σε τρίτους που έχουν πρόσβαση σε αυτή

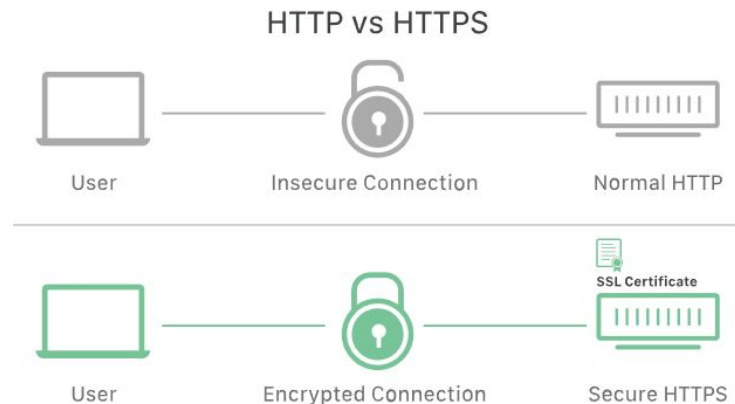
Ασφαλής χρήση browser (φυλλομετρητή)

- Σύγχρονες συσκευές με ενημερωμένο λειτουργικό σύστημα
- Επιλογή σύγχρονου browser (Chrome, Firefox, Edge)
- Αποφυγή επίσκεψης σε ύποπτους/μη ασφαείς ιστότοπους
- Μη εγκατάσταση ανεξέλεγκτων extensions



HTTPS vs HTTP – γιατί έχει σημασία

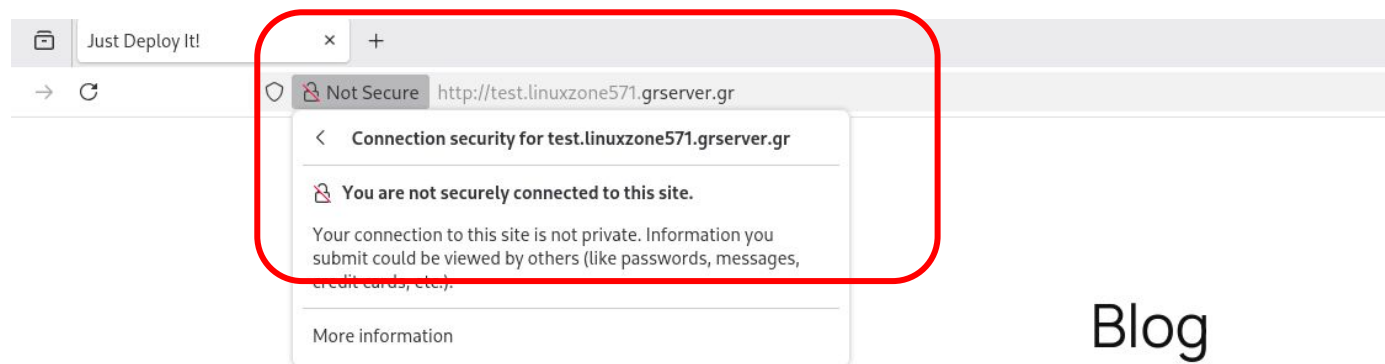
- **Κρυπτογράφηση:** Το HTTPS κρυπτογραφεί τα δεδομένα· στο HTTP περνούν “plain text” (όποιος είναι στο ίδιο δίκτυο μπορεί να τα δει/κλέψει)
- **Ακεραιότητα:** Με HTTPS ο ενδιαμέσος δεν μπορεί να αλλάξει περιεχόμενο (injection διαφημίσεων/κακόβουλου κώδικα).
- **Γνησιότητα:** Τα πιστοποιητικά TLS αποδεικνύουν ότι μιλάς με τον σωστό server
- **Απόρρητο & Συμμόρφωση:** Μειώνει νομικό/κανονιστικό ρίσκο



HTTPS vs HTTP



VS



Blog

Αποφεύγουμε αποδοχή



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **test.linuxzone571.grserver.gr**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

test.linuxzone571.grserver.gr uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

[View Certificate](#)

[Go Back \(Recommended\)](#)

[Accept the Risk and Continue](#)



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

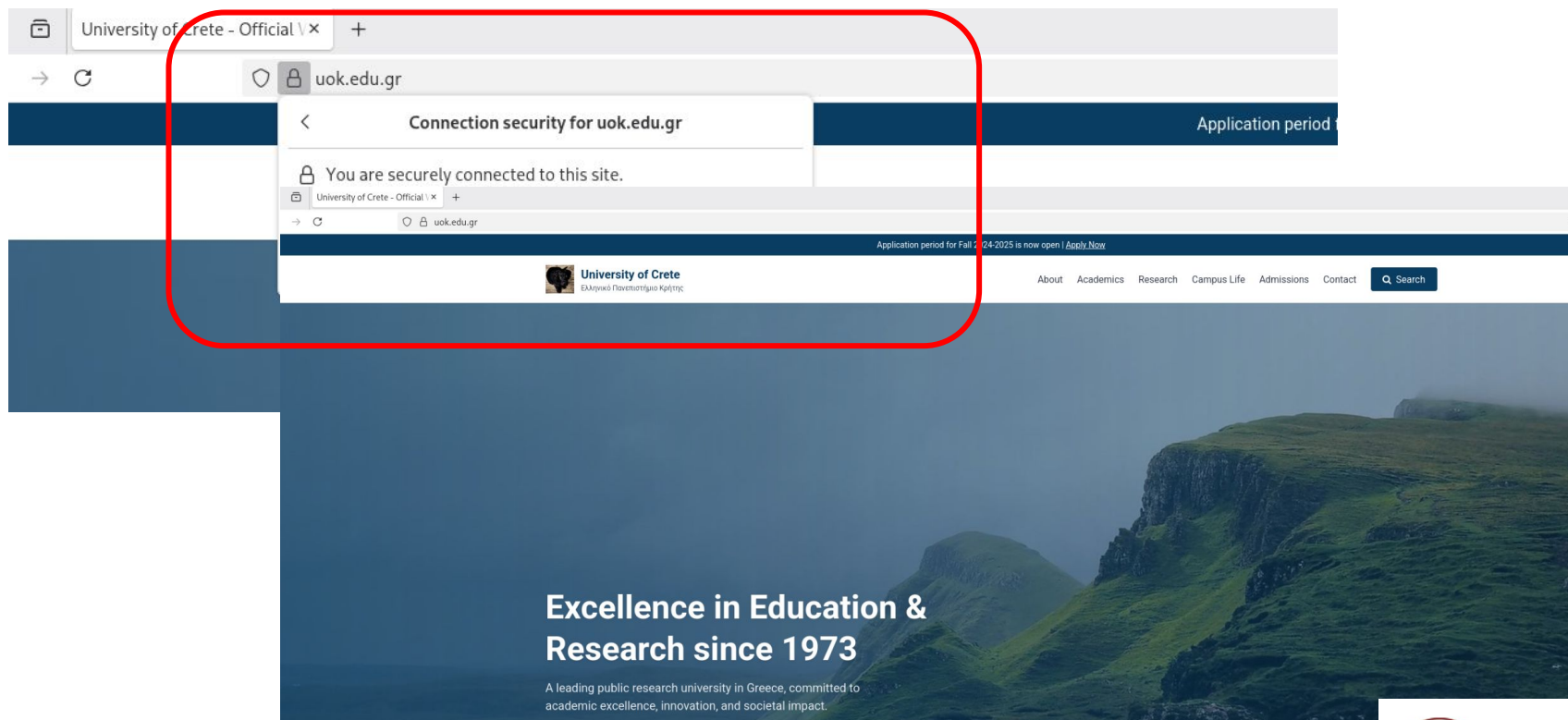
 **digiGOV**
innoHUB



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Συχνά λάθη

- “Έχει λουκετάκι άρα είναι ασφαλές site” → Το HTTPS δεν εγγυάται αξιοπιστία περιεχομένου.



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Cookies, pop-ups & extensions – τι να προσέχω

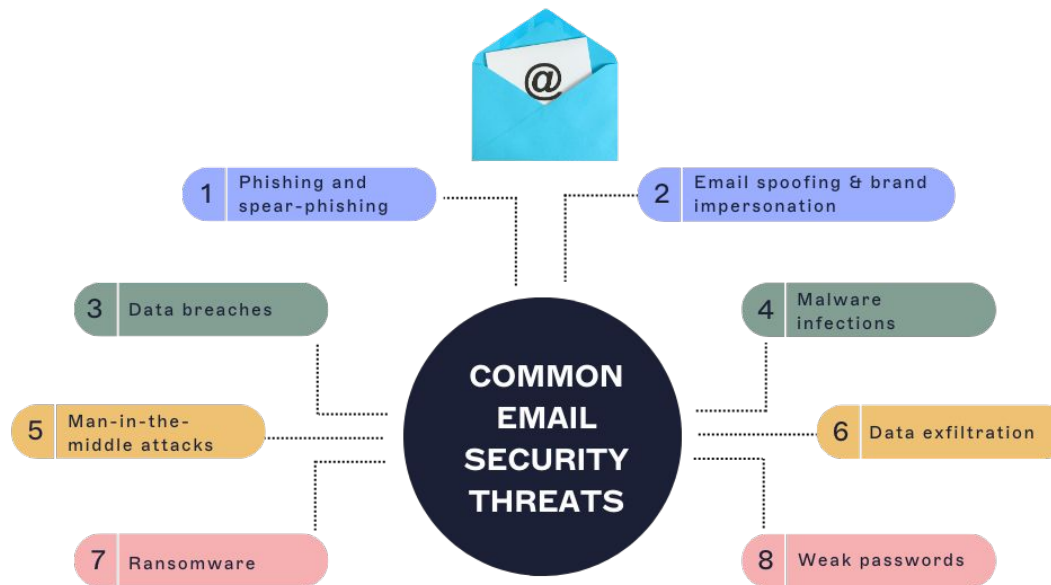
- **Cookies:** επιτρέπουν την αποθήκευση πληροφοριών → χρήσιμα αλλά και πιθανώς καταχρηστικά
 - Session vs persistent cookies
- **Pop-ups:** συχνά μέσο εξαπάτησης – να μπλοκάρονται
 - Malvertising μέσω pop-ups
- **Extensions:** να εγκαθίστανται μόνο από έγκυρες πηγές
 - Έλεγχος δικαιωμάτων και χρήσης πριν από εγκατάσταση

Ηλεκτρονικό ταχυδρομείο (email)

- **Τι είναι:** Ηλεκτρονικά μηνύματα που στέλνονται μέσω δικτύου μεταξύ μοναδικών διευθύνσεων (π.χ. onoma@uoc.gr)
- **Γιατί είναι σημαντικό:** Γρήγορη, παγκόσμια επικοινωνία με χαμηλό κόστος και αποδεικτικό ιστορικό
- **Χρήσεις:** Επαγγελματική επικοινωνία, προσωπική επικοινωνία, εξυπηρέτηση πελατών, επιβεβαιώσεις/ειδοποιήσεις, εγγραφές σε υπηρεσίες, ενημερώσεις



Κίνδυνοι μέσω email

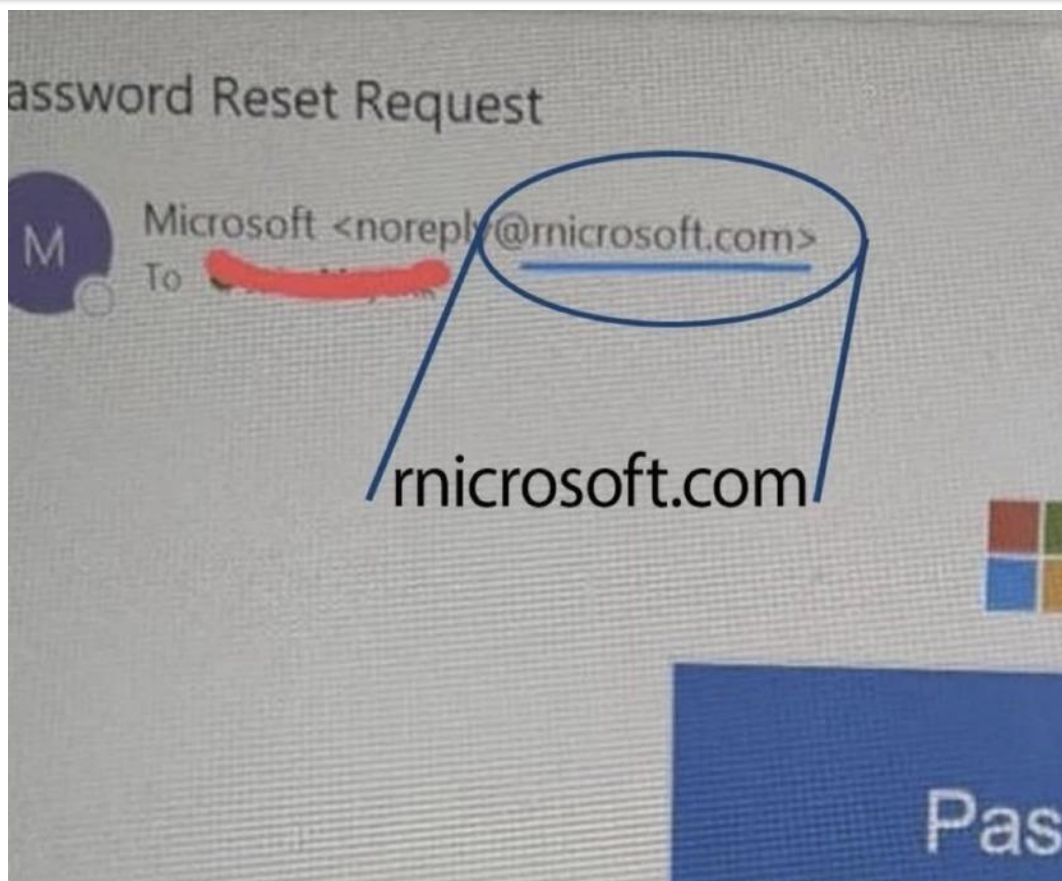


Αναγνώριση phishing

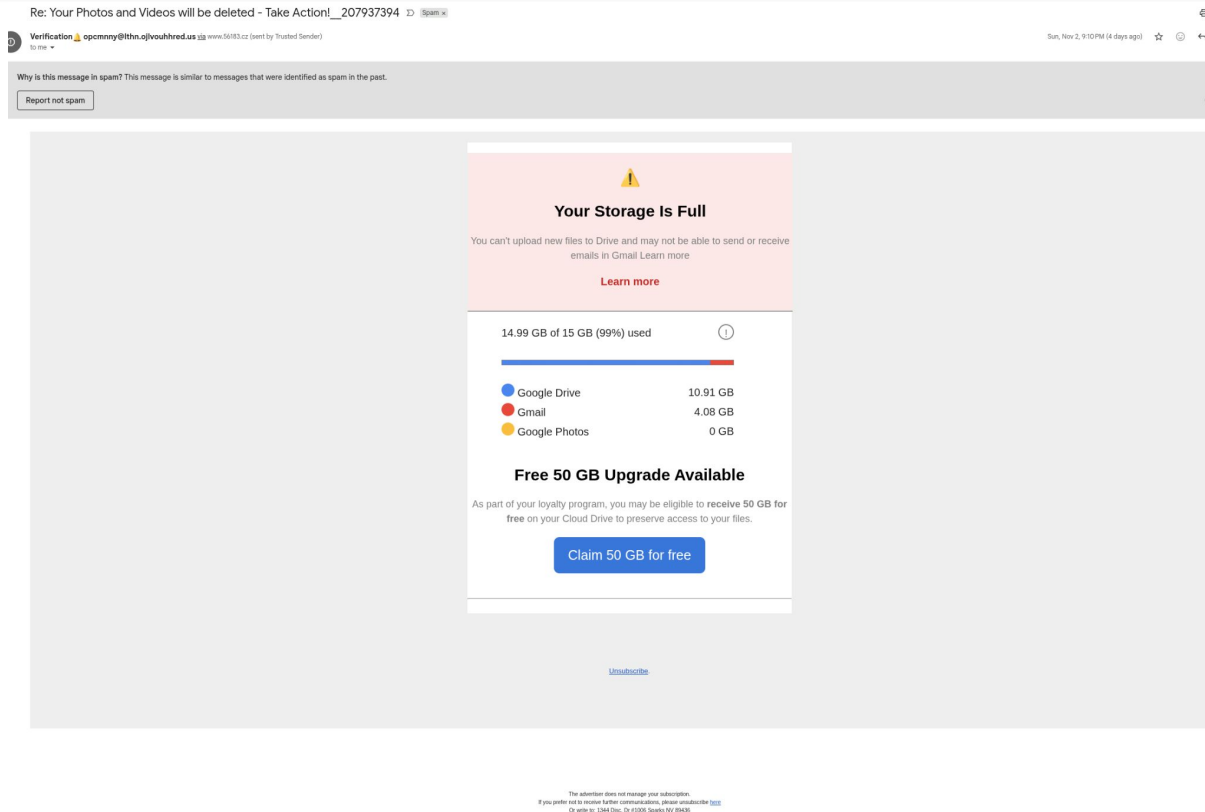
- Προσοχή σε:
 - Αποστολέα που δε γνωρίζετε
 - Ορθογραφικά λάθη
 - Συνδέσμους με ύποπτο URL
 - Επισυναπτόμενα αρχεία
 - Αίσθηση "επείγοντος"
- **ΜΗΝ** πατάτε αμέσως – ελέγξτε πρώτα



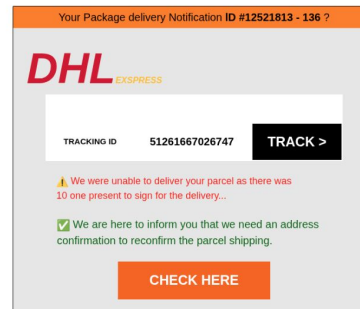
Πραγματικά παραδείγματα κακόβουλων email



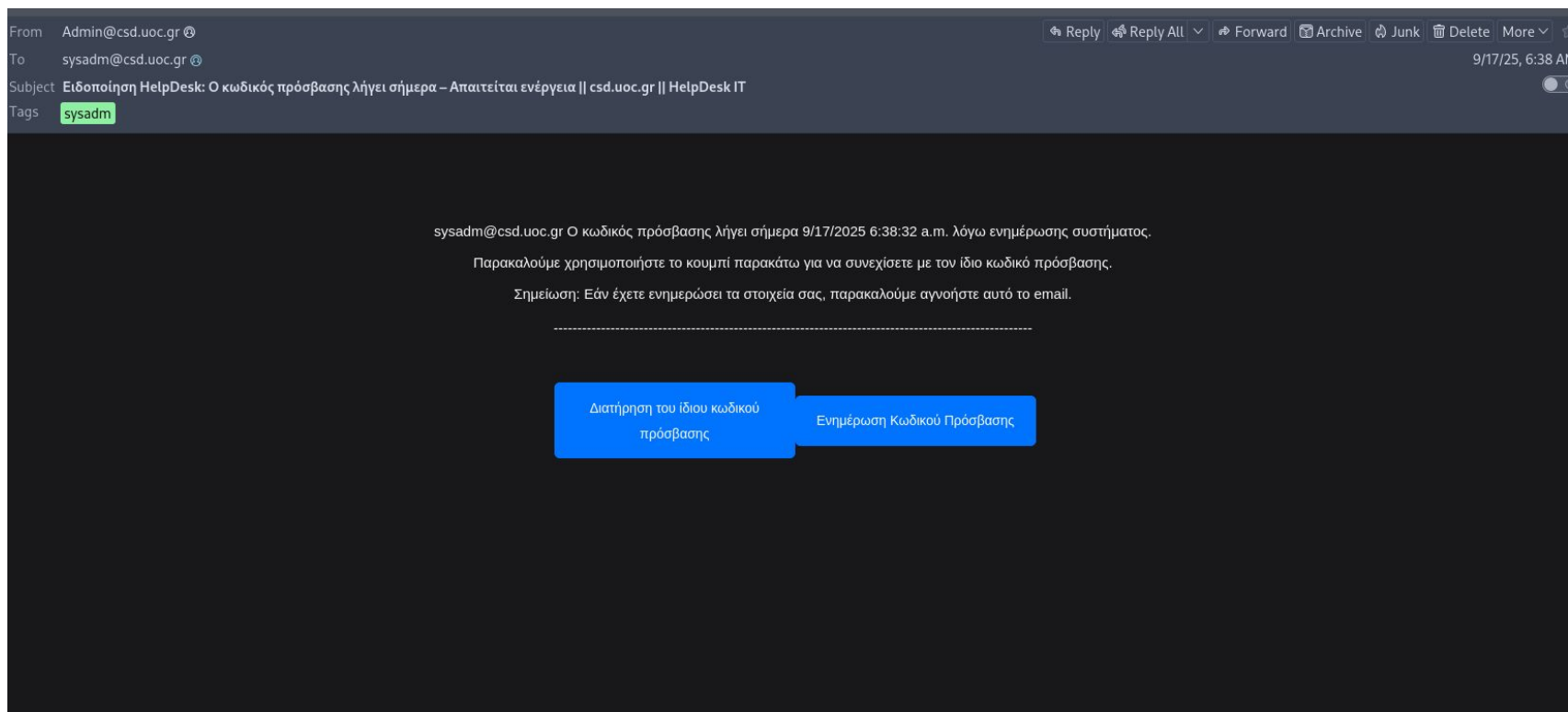
Πραγματικά παραδείγματα κακόβουλων email



Πραγματικά παραδείγματα κακόβουλων email



Πραγματικά παραδείγματα κακόβουλων email



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

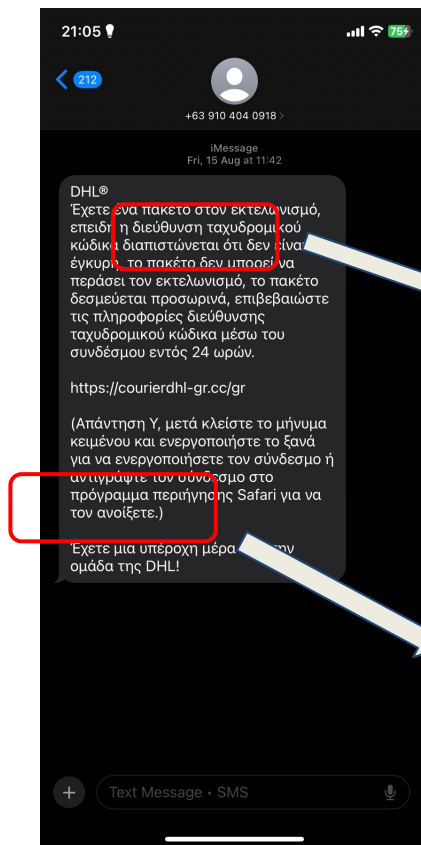


ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Πραγματικά παραδείγματα κακόβουλων sms



+63: Φιλιππίνες

<https://courierdhl-gr.cc/gr>

Δημόσια δίκτυα Wi-Fi



Δημόσια δίκτυα Wi-Fi – τι να προσέχουμε



Κοινωνικά δίκτυα

- Τα μέσα κοινωνικής δικτύωσης (social media) είναι διαδικτυακές πλατφόρμες όπου οι χρήστες δημιουργούν προφίλ, συνδέονται με άλλους και μοιράζονται περιεχόμενο (κείμενο, εικόνες, βίντεο, ζωντανές μεταδόσεις).
- Η μετάβαση σε smartphones και δεδομένα κινητής εκτόξευσε τη χρήση, ενώ σήμερα τα social αποτελούν βασικές υποδομές επικοινωνίας, ενημέρωσης, ψυχαγωγίας και εμπορίου—με σημαντικές ευκαιρίες αλλά και ζητήματα ιδιωτικότητας



Κοινωνικά δίκτυα και κίνδυνοι

1	Identity theft Stealing personal information for fraudulent activities	
2	Cyberbullying Harassment or bullying through online platforms	
3	Fake giveaways Fraudulent offers that lure users into scams	
4	Likejacking Gaining unauthorized access by tricking users into liking	
5	Phishing scams Deceptive messages to steal personal information	

6	Data breaches Unauthorized access to sensitive data	
7	Malware Malicious software spread through social media	
8	Brand impersonation Faking a company's profile to deceive users	
9	Affiliate scams Misleading promotions to earn commissions illegally	
10	Social engineering Manipulating individuals into revealing confidential info	



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

 **digiGOV**
innoHUB



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Σας ευχαριστώ!