Διαδικτυακοί κίνδυνοι & πως να προστατευτείτε

Γεώργιος Αθ. Γέρμανος

Ειδικός στην πρόληψη & στη διερεύνηση κυβερνοεγκλημάτων

Υποψ. Διδάκτορας Τμήματος Πληροφορικής & Τηλεπικοινωνιών Πανεπιστημίου Πελοποννήσου

Διαδίκτυο

slido.com

#3414 553

Περιστατικά & εγκλήματα

Κατά ανηλίκων

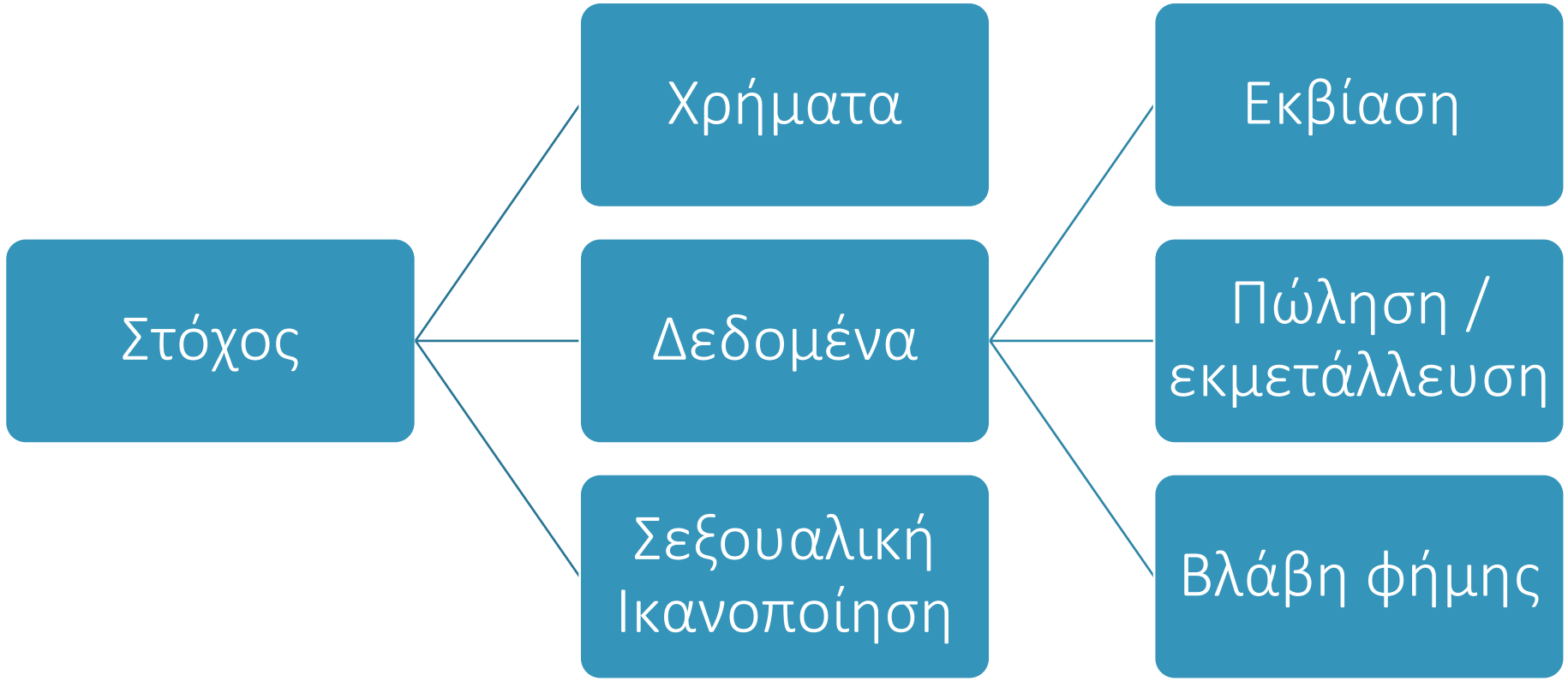
Κυβερνοεπιθέσεις (cyber attacks)

Οικονομικής φύσης

Προσωπικά δεδομένα

…

Εγκληματίες
στον κυβερνοχώρο



Προσωπικά δεδομένα

Social media

- Χρήση δεδομένων (ιδίως φωτογραφιών) για τη δημιουργία ψεύτικων προφίλ
- Ανάρτηση, σε κοινή θέα, υλικού που αποτελεί προσωπικό δεδομένο

Εγκλήματα κατά ανηλίκων

Απαίτηση για συνάντηση

Βιντεοκλήση

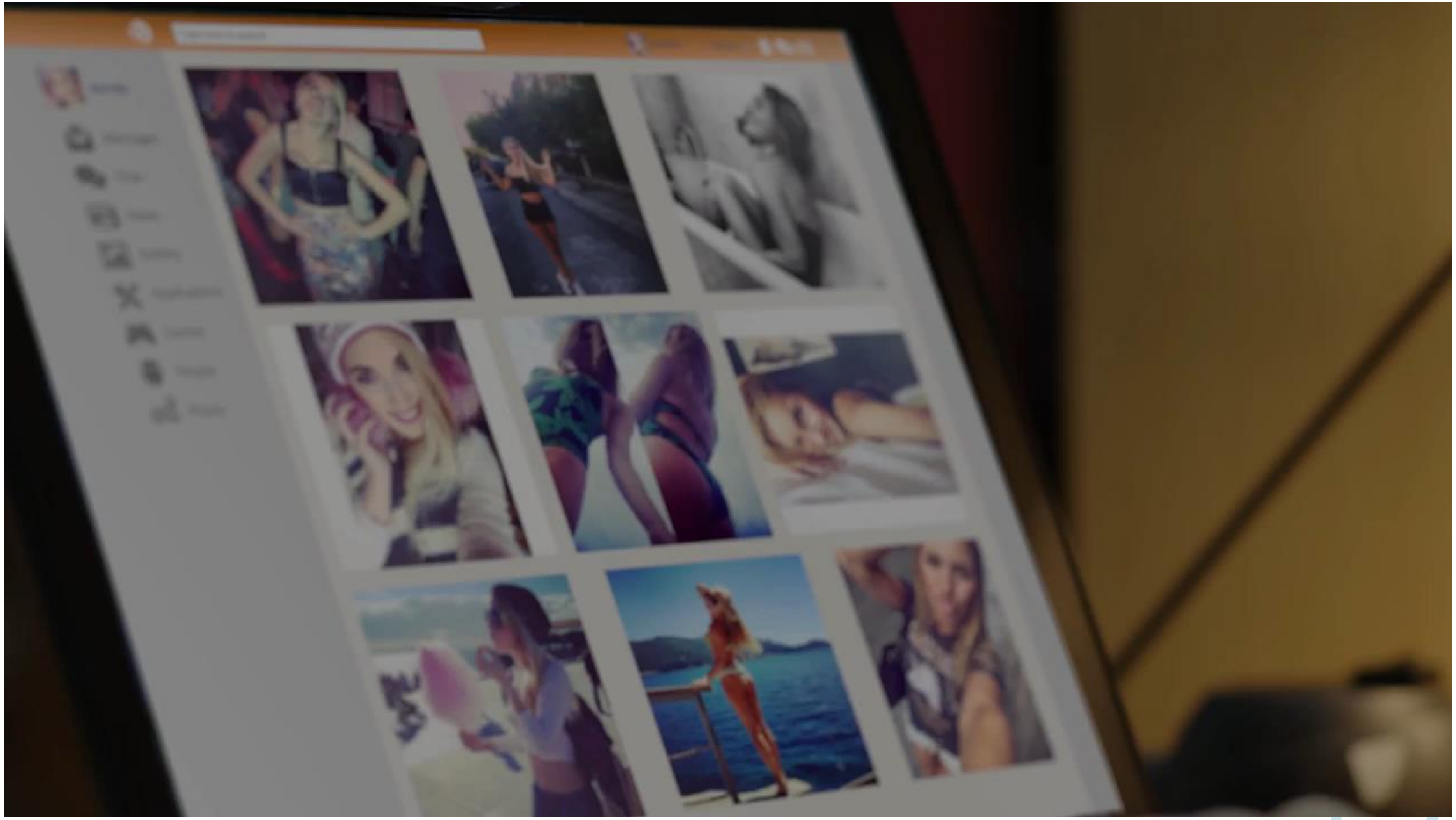
Ανταλλαγή αρχείων σεξουαλικού περιεχομένου

18

Ανταλλαγή μηνυμάτων με άσεμνο περιεχόμενο

Διαδικτυακή επικοινωνία

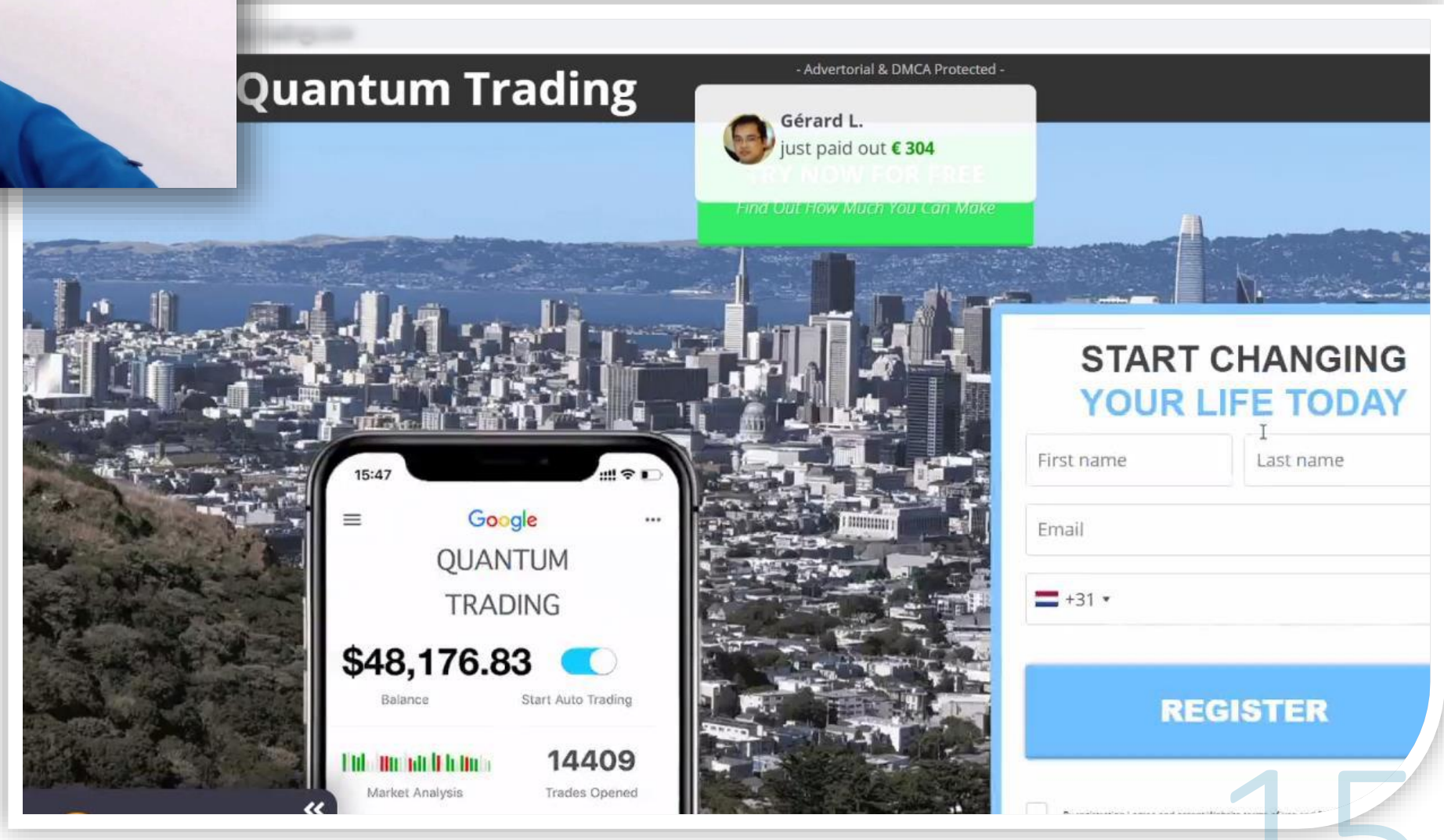
Απώλεια χρημάτων
στον κυβερνοχώρο



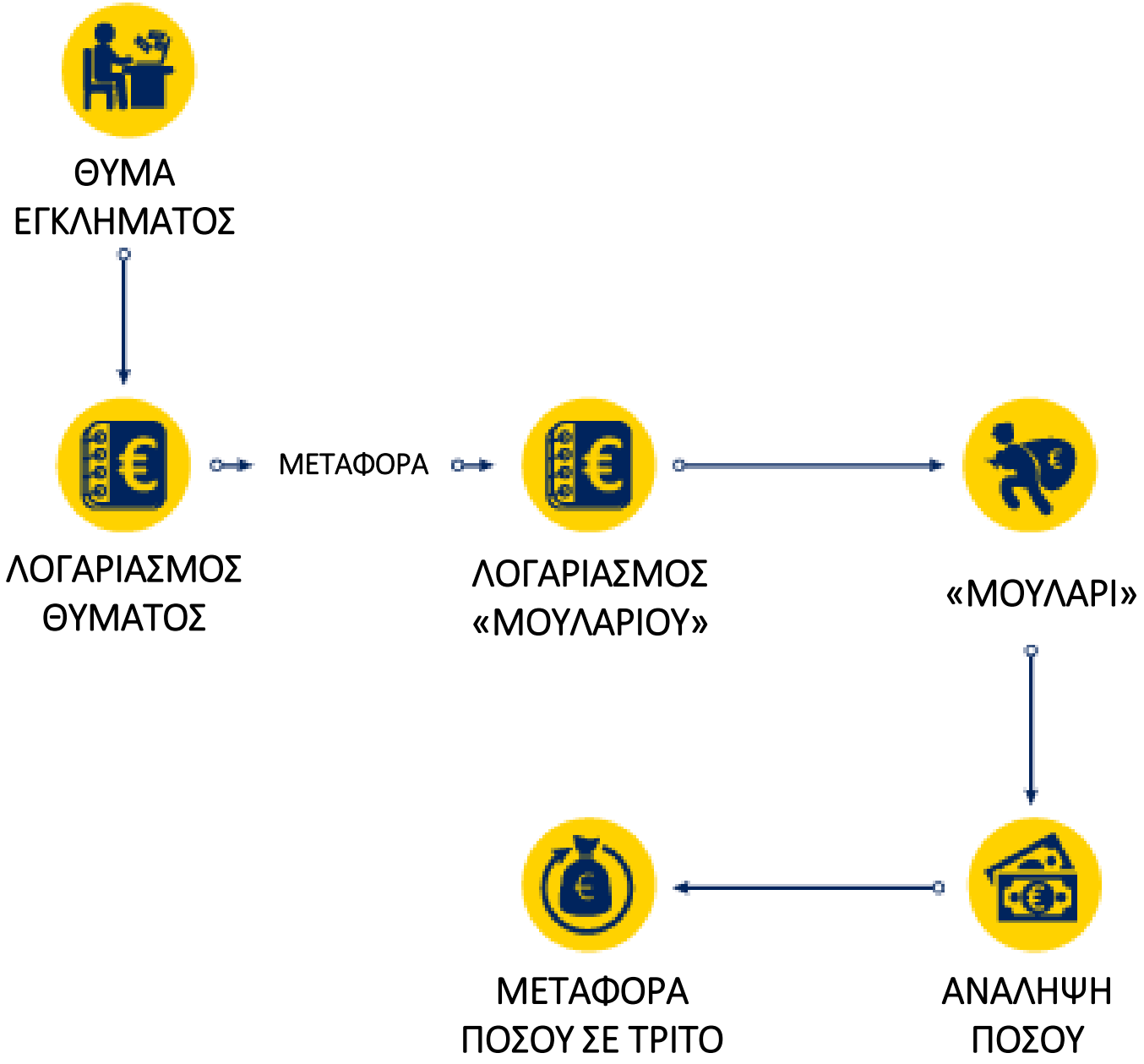

SCAM


ROYAL BANK
of
NIGERIA
I have emailed everyone I can possibly find, my Prince, but no-one wants to help you move your money.


GREAT INVESTMENT!
TALK
END

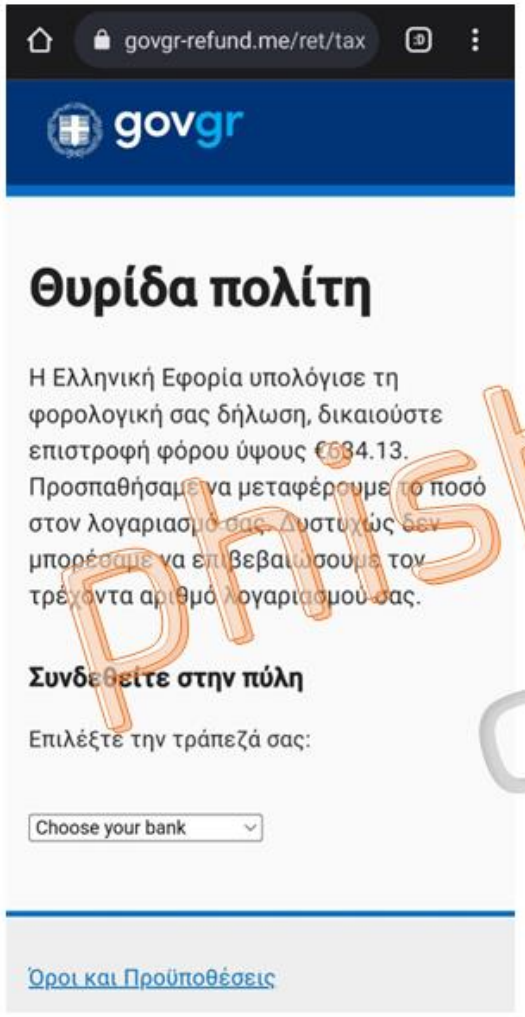

Quantum Trading
- Advertorial & DMCA Protected -
Gérard L.
just paid out € 304
TRY NOW FOR FREE
Find Out How Much You Can Make
15:47
Google
QUANTUM
TRADING
$48,176.83
Balance
Start Auto Trading
14409
Market Analysis
Trades Opened
START CHANGING
YOUR LIFE TODAY
First name
Last name
Email
+31
REGISTER

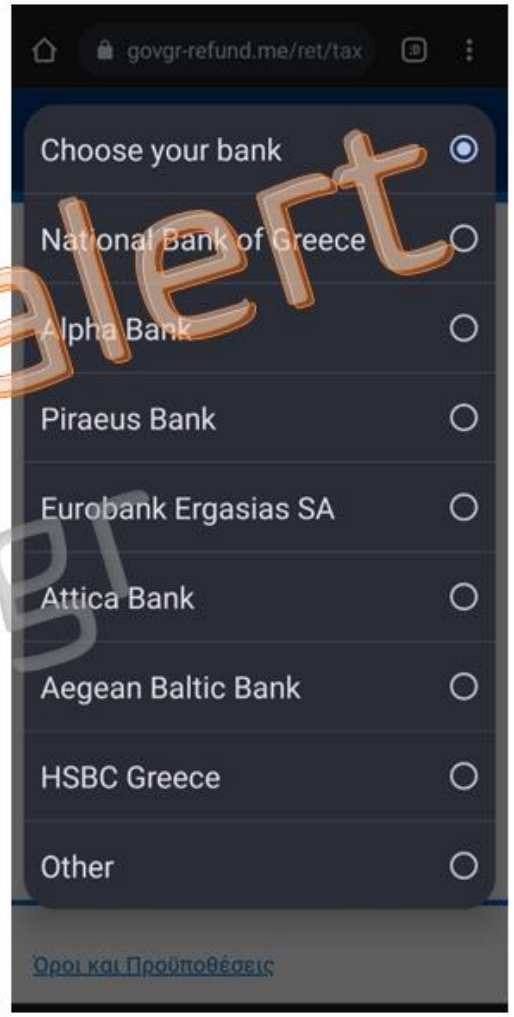
Γ. ΓΕΡΜΑΝΟΣ


ΘΥΜΑ
ΕΓΚΛΗΜΑΤΟΣ
ΛΟΓΑΡΙΑΣΜΟΣ
ΘΥΜΑΤΟΣ
ΜΕΤΑΦΟΡΑ
ΛΟΓΑΡΙΑΣΜΟΣ
«ΜΟΥΛΑΡΙΟΥ»
«ΜΟΥΛΑΡΙ»
ΑΝΑΛΗΨΗ
ΠΟΣΟΥ
ΜΕΤΑΦΟΡΑ
ΠΟΣΟΥ ΣΕ ΤΡΙΤΟ

Αλίευση δεδομένων - phishing

Υποκλοπή στοιχείων πρόσβασης σε web banking και λοιπούς online λογαριασμούς






NETFLIX
Your account is on hold.
Please update your payment details
Hi Dear,
We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.
UPDATE ACCOUNT NOW
Need help? We're here if you need it. Visit the Help Centre or contact us now.
- Your friends at Netflix
Questions? Call

Τι είναι το phishing;

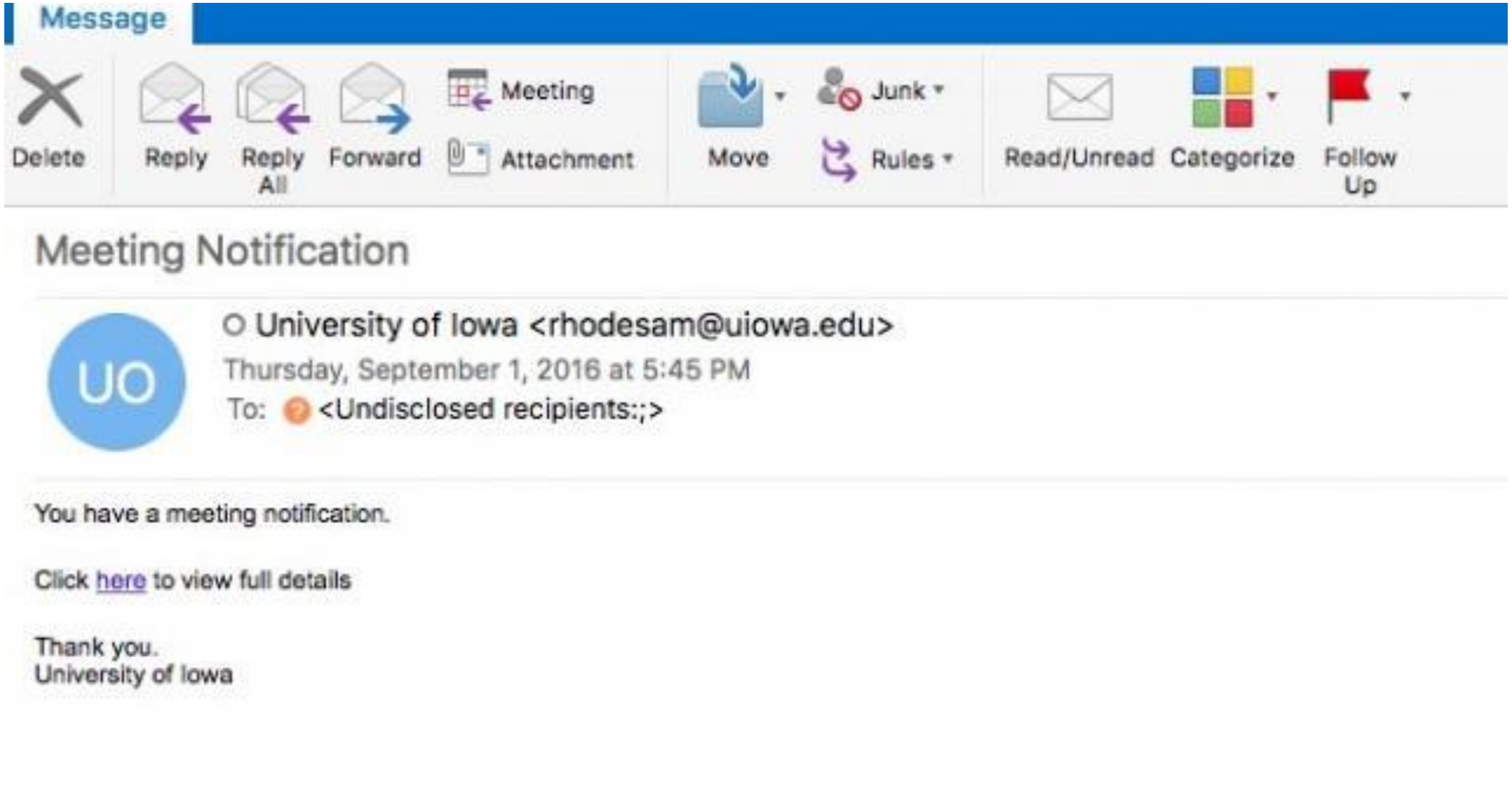
Κάποιος προσπαθεί να μας πείσει να εισάγουμε τα credentials μας σε μια φόρμα, που είναι όμοια με την αληθινή.

Προσέγγιση μέσω:

- Email
- SMS
- Τηλεφωνικής κλήσης

Στόχος η αποκάλυψη:

- Username
- Password
- Αριθμό κινητού τηλεφώνου
- One Time Password (OTP)


Message
Delete
Reply
Reply All
Forward
Meeting
Attachment
Move
Junk
Rules
Read/Unread
Categorize
Follow Up
Meeting Notification
UO
University of Iowa <rhodesam@uiowa.edu>
Thursday, September 1, 2016 at 5:45 PM
To: <Undisclosed recipients:;>
You have a meeting notification.
Click here to view full details
Thank you.
University of Iowa

From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ

Αγαπητέ πελάτη,

Αυτή είναι μια τρίτη ειδοποίηση, η Εθνική Τράπεζα έχει βελτιώσει τα μέτρα ασφαλείας για διαδικτυακές συναλλαγές και απαιτεί υποχρεωτική επιβεβαίωση εκ μέρους σας.

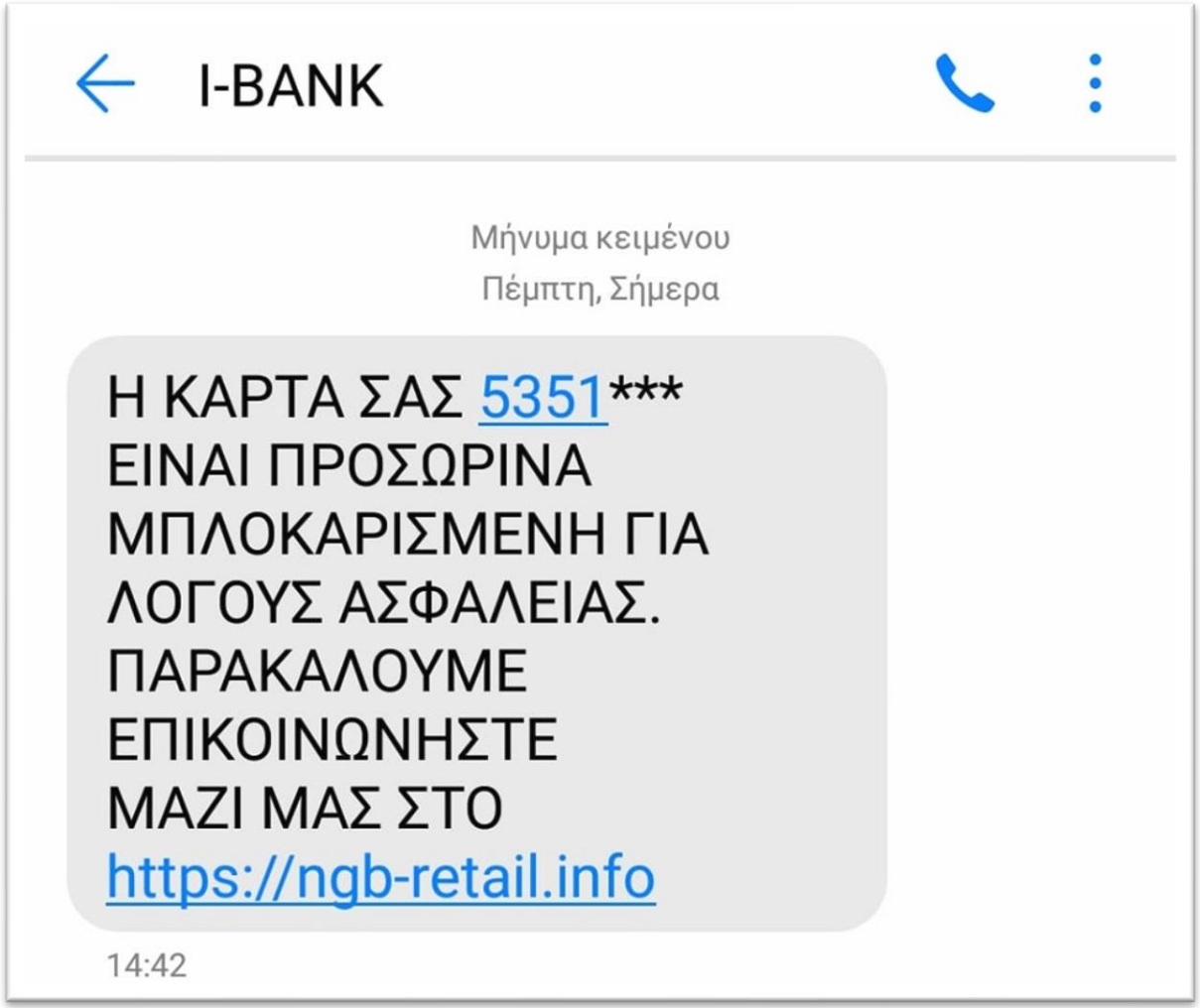
Ακολουθήστε αυτά τα βήματα για να ενεργοποιήσετε ξανά τις διαδικτυακές δυνατότητες:

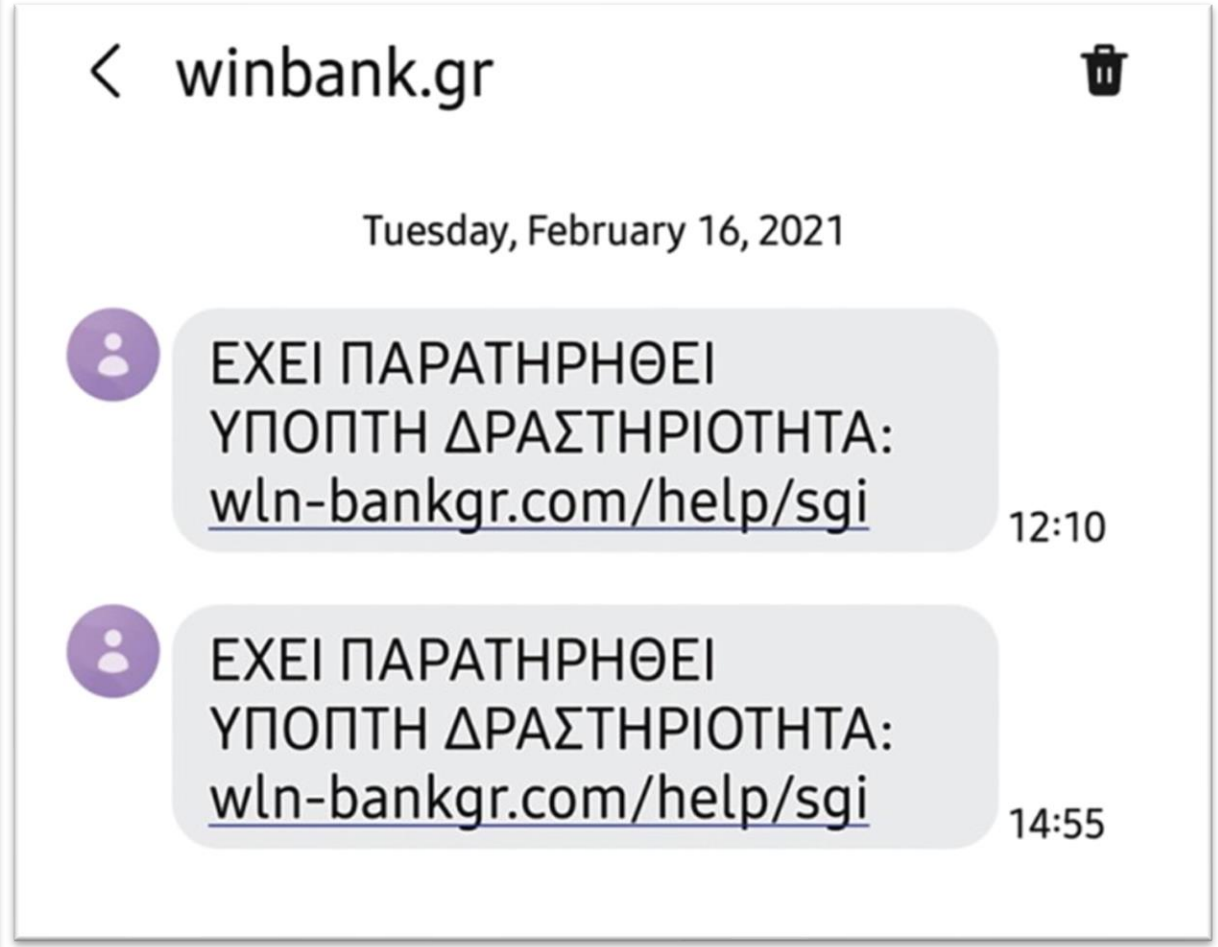
Επικυρώνω

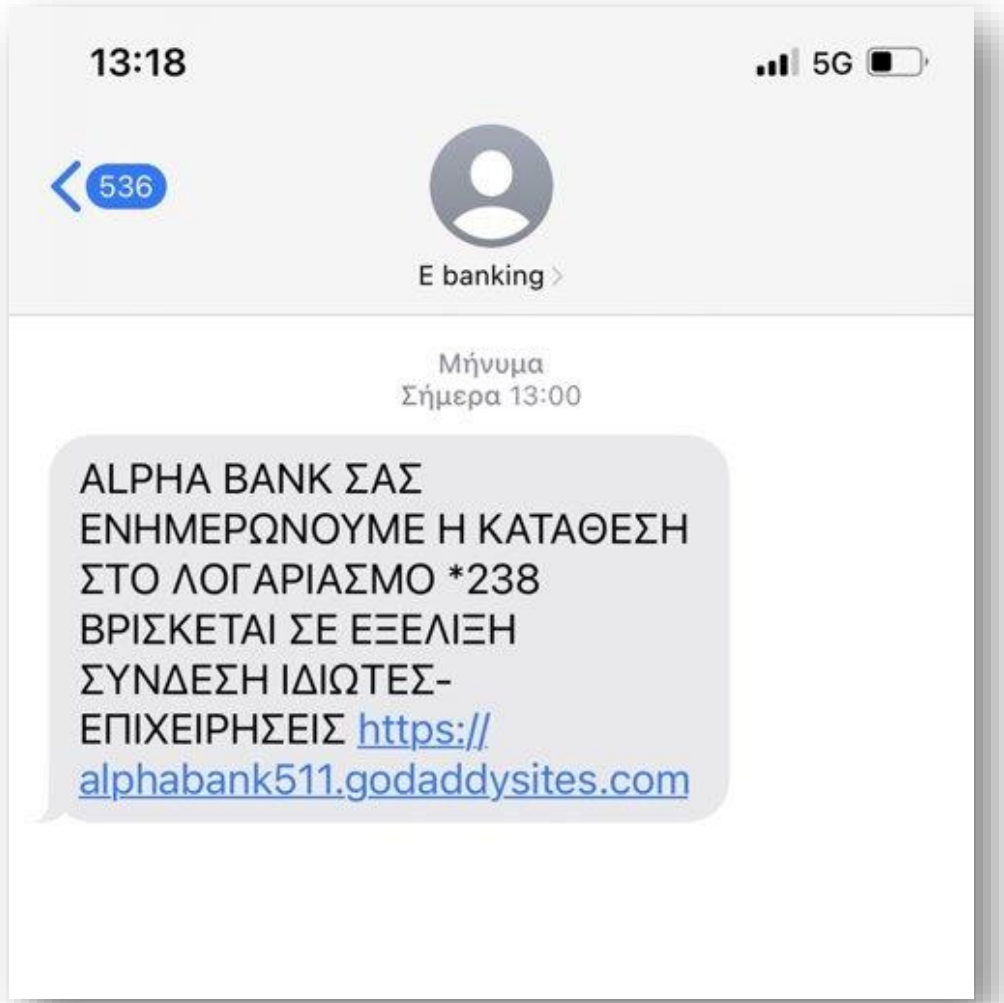
Εάν θέλετε να επικοινωνήσετε μαζί μας, παρακαλούμε απαντήστε σε αυτό το email

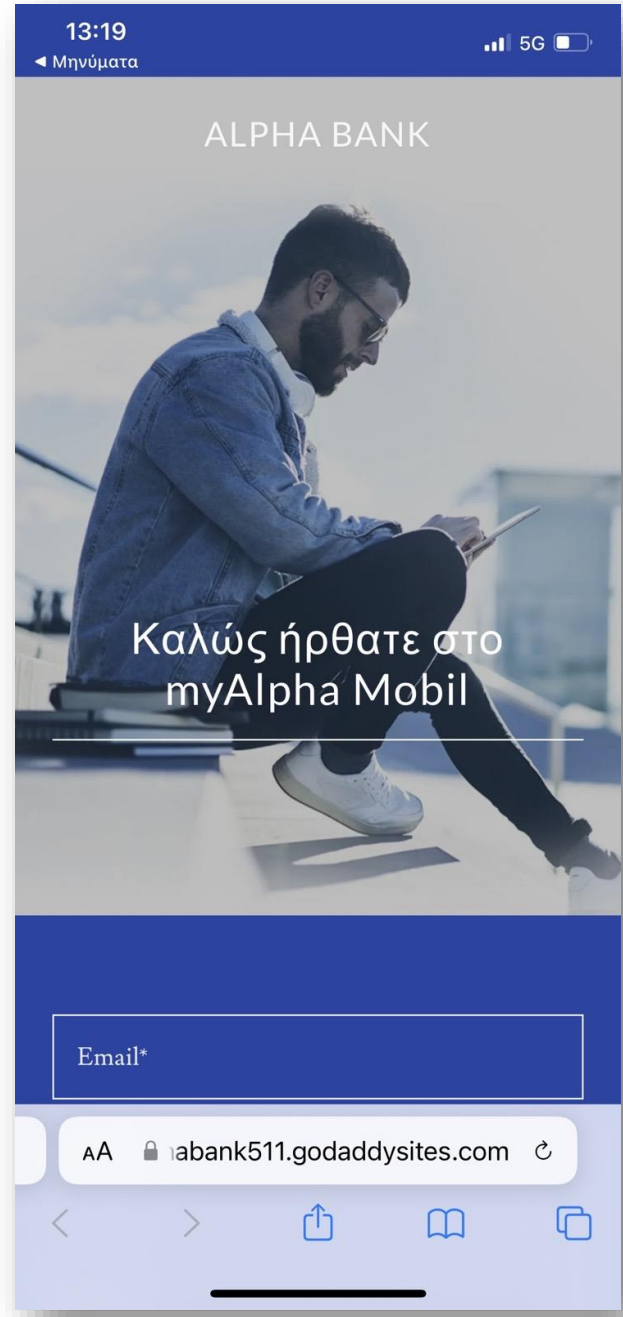
Τις καλύτερες ευχές,
NBG

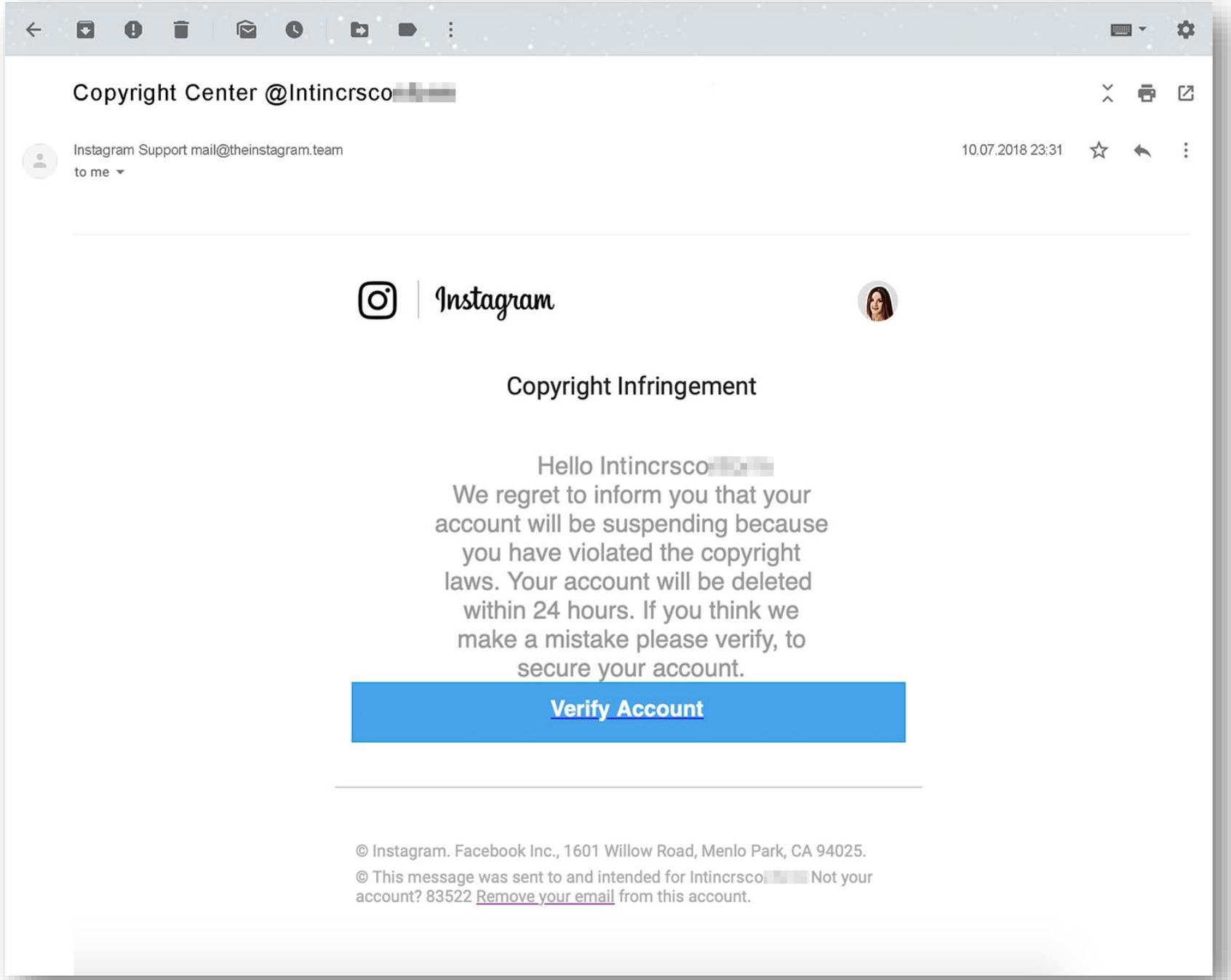
Στείλτε μας email:
contact@myid.nbg.gr

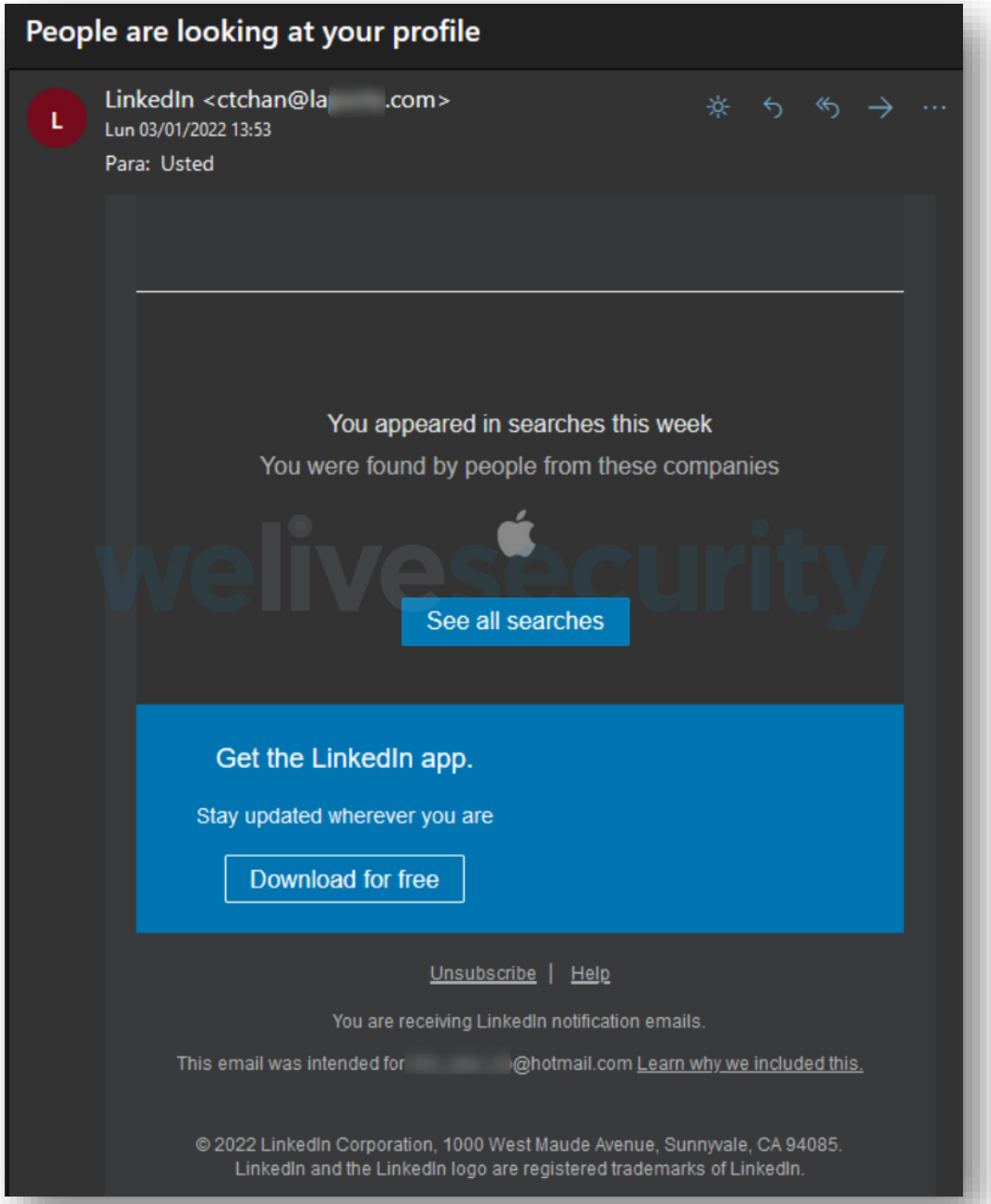

I-BANK
Μήνυμα κειμένου
Πέμπτη, Σήμερα
Η ΚΑΡΤΑ ΣΑΣ 5351***
ΕΙΝΑΙ ΠΡΟΣΩΡΙΝΑ
ΜΠΛΟΚΑΡΙΣΜΕΝΗ ΓΙΑ
ΛΟΓΟΥΣ ΑΣΦΑΛΕΙΑΣ.
ΠΑΡΑΚΑΛΟΥΜΕ
ΕΠΙΚΟΙΝΩΝΗΣΤΕ
ΜΑΖΙ ΜΑΣ ΣΤΟ
https://ngb-retail.info
14:42

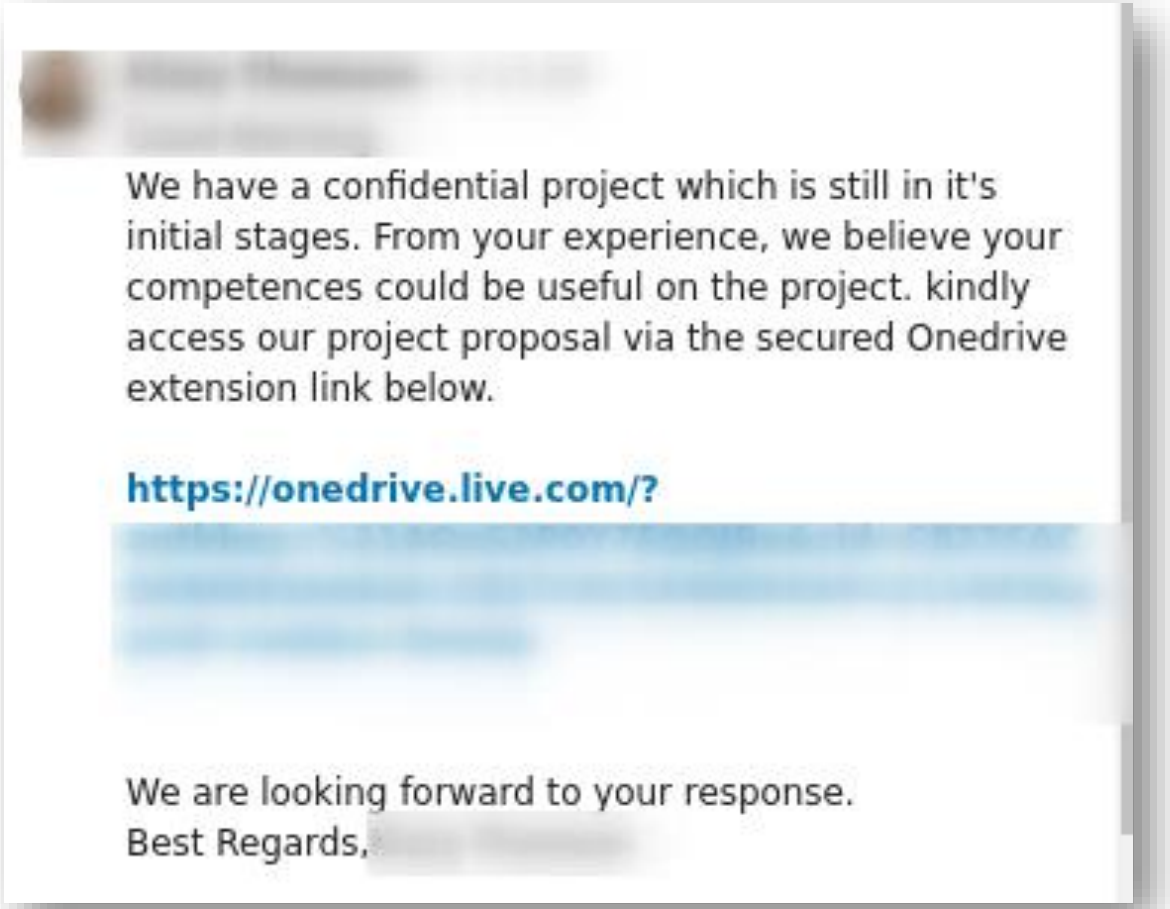

winbank.gr
Tuesday, February 16, 2021
ΕΧΕΙ ΠΑΡΑΤΗΡΗΘΕΙ
ΥΠΟΠΤΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ:
wln-bankgr.com/help/sgi
12:10
ΕΧΕΙ ΠΑΡΑΤΗΡΗΘΕΙ
ΥΠΟΠΤΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ:
wln-bankgr.com/help/sgi
14:55


13:18
5G
536
E banking
Μήνυμα
Σήμερα 13:00
ALPHA BANK ΣΑΣ ΕΝΗΜΕΡΩΝΟΥΜΕ Η ΚΑΤΑΘΕΣΗ ΣΤΟ ΛΟΓΑΡΙΑΣΜΟ *238 ΒΡΙΣΚΕΤΑΙ ΣΕ ΕΞΕΛΙΞΗ ΣΥΝΔΕΣΗ ΙΔΙΩΤΕΣ-ΕΠΙΧΕΙΡΗΣΕΙΣ https://alphabank511.godaddysites.com

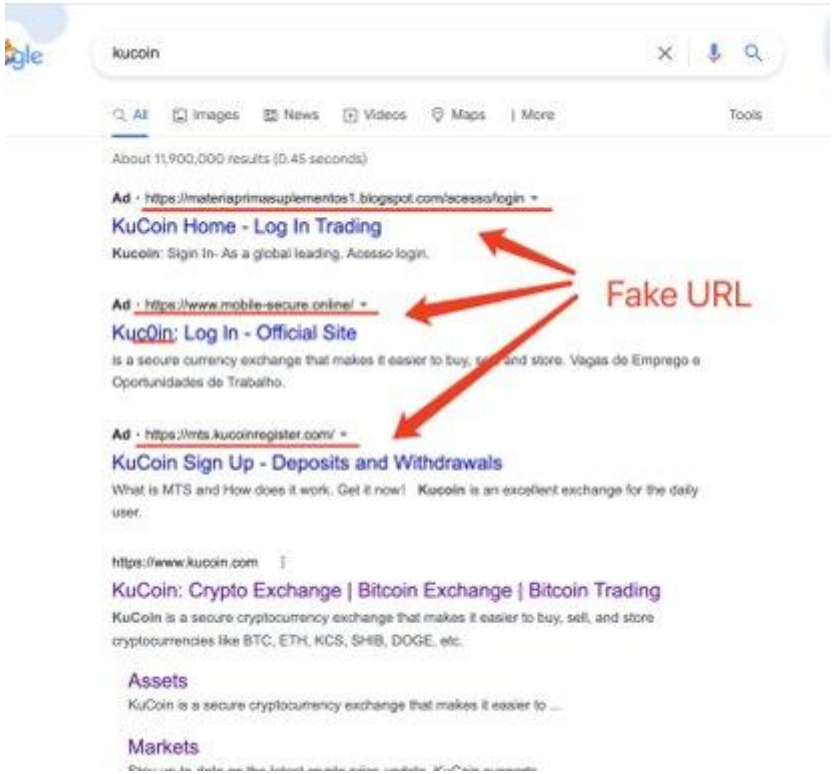

13:19
◀ Μηνύματα
5G
ALPHA BANK
Καλώς ήρθατε στο myAlpha Mobil
Email*
AA
abank511.godaddysites.com


Copyright Center @Intincrsco
Instagram Support mail@theinstagram.team
to me
10.07.2018 23:31
Instagram
Copyright Infringement
Hello Intincrsco
We regret to inform you that your account will be suspending because you have violated the copyright laws. Your account will be deleted within 24 hours. If you think we make a mistake please verify, to secure your account.
Verify Account
© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025.
© This message was sent to and intended for Intincrsco Not your account? 83522 Remove your email from this account.


People are looking at your profile
LinkedIn <ctchan@la .com>
Lun 03/01/2022 13:53
Para: Usted
You appeared in searches this week
You were found by people from these companies
See all searches
Get the LinkedIn app.
Stay updated wherever you are
Download for free
Unsubscribe | Help
You are receiving LinkedIn notification emails.
This email was intended for @hotmail.com Learn why we included this.
© 2022 LinkedIn Corporation, 1000 West Maude Avenue, Sunnyvale, CA 94085.
LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.


We have a confidential project which is still in it's initial stages. From your experience, we believe your competences could be useful on the project. kindly access our project proposal via the secured Onedrive extension link below.
https://onedrive.live.com/?
We are looking forward to your response.
Best Regards,

Αποτελέσματα Google



Μέθοδοι εξαπάτησης σε βάρος επαγγελματιών

Man-in-the-middle

CEO Fraud

Αλίευση διαπιστευτηρίων web banking & λοιπών online λογαριασμών

Χρήση κακόβουλων λογισμικών

Man-in-the-middle (MITM)

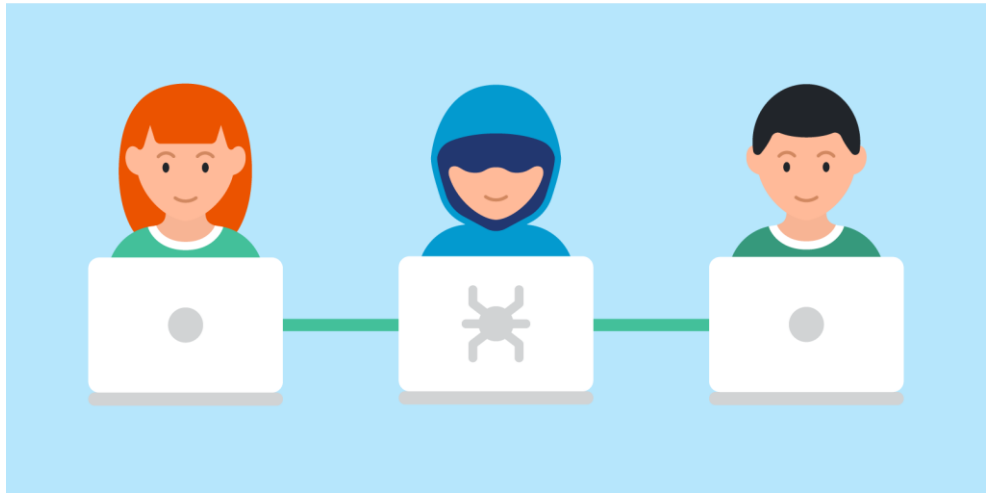
Παρέμβαση στην επικοινωνία μέσω email

MITM

Επικοινωνία μεταξύ Α και Β

Ο Γ παραβιάζει τη θυρίδα ηλεκτρονικού ταχυδρομείου του Β και διαβάζει την αλληλογραφία του

Ο Γ φτιάχνει μια θυρίδα email σχεδόν πανομοιότυπη με του Β, επικοινωνεί με τον Α και ζητάει **αλλαγή του τραπεζικού λογαριασμού πληρωμών**



Παραπλανητικό email

Από: **mycompany@goog1e.com**

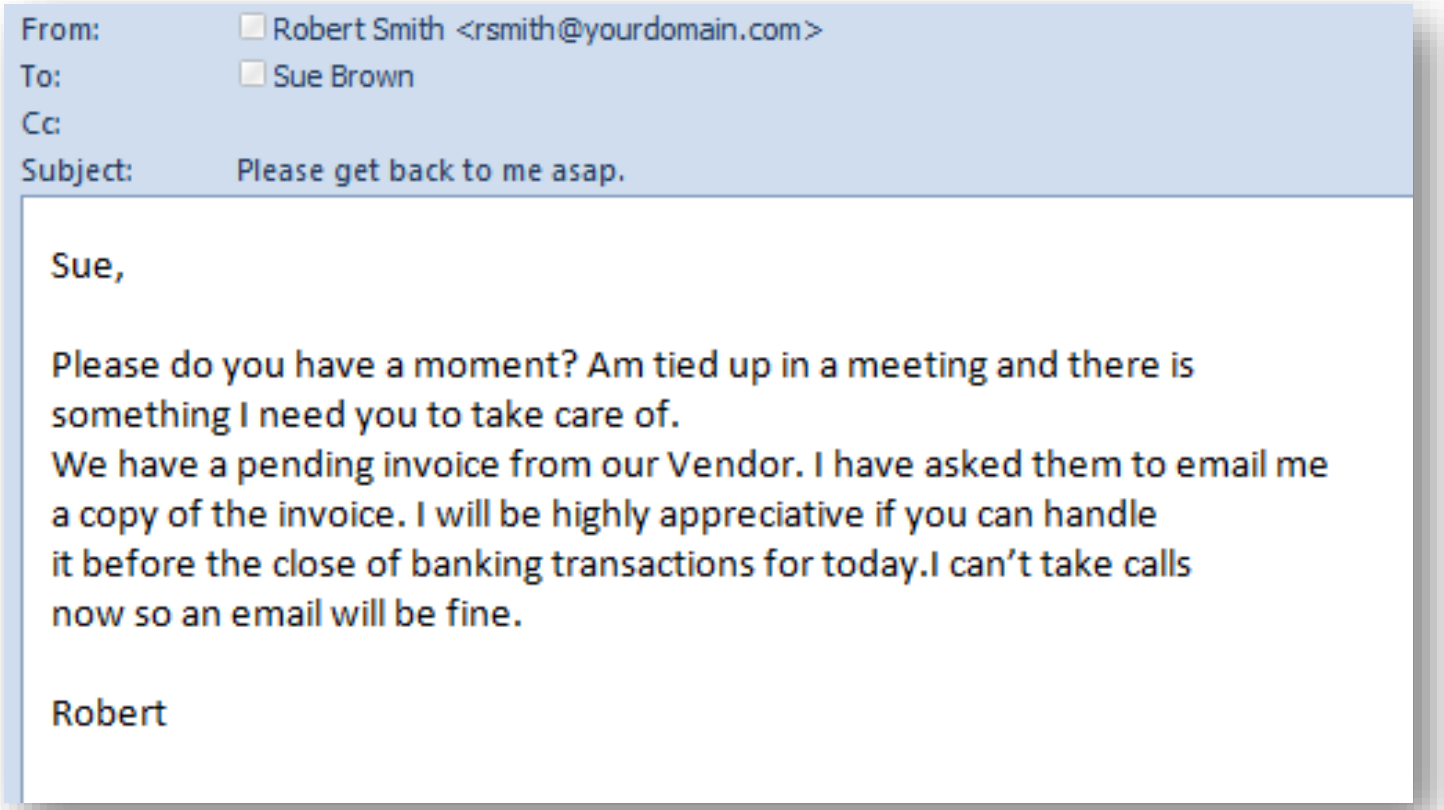
Θέμα: Πληρωμή - διόρθωση στοιχείων

Επειδή ο λογαριασμός που χρησιμοποιούμε για τις πληρωμές έχει προσωρινά κλειδωθεί, παρακαλούμε να προχωρήσετε στην πληρωμή του οφειλόμενου ποσού στο λογαριασμό με IBAN .....

Απάτη CEO

Επείγουσα εντολή μεταφοράς χρημάτων από τον CEO
ή άλλο υψηλόβαθμο

Μήνυμα από τον CEO



From: Robert Smith <rsmith@yourdomain.com>
To: Sue Brown
Cc:
Subject: Please get back to me asap.

Sue,

Please do you have a moment? Am tied up in a meeting and there is something I need you to take care of.
We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice. I will be highly appreciative if you can handle it before the close of banking transactions for today.I can't take calls now so an email will be fine.

Robert

Επιπλέον λεπτομέρειες

Εναλλακτικά, αντί για email:

- ❖SMS
- ❖Viber / WhatsApp / Signal κ.λπ.
- ❖Τηλεφωνική κλήση

Αίσθηση επείγοντος

Πίεση για ολοκλήρωση διαδικασίας το ταχύτερο δυνατό

Δυνατότητα spoofing:

- ➢με το κατάλληλο λογισμικό μπορώ να ορίσω ως **εμφανιζόμενο αποστολέα ενός email ή SMS οποιονδήποτε**

Το ίδιο ισχύει και για τον τηλεφωνικό αριθμό του καλούντος

Συλλογή πληροφοριών για την εταιρεία - στόχο

- Επίσημη ιστοσελίδα της εταιρείας
- Επίσημα έγγραφα
- Εξερχόμενα emails προσωπικού
- Social media προσωπικού

Είδη πληροφοριών

- Ονοματεπώνυμα υπαλλήλων
- Διευθύνσεις emails
- Φυσικές διευθύνσεις
- Αριθμοί τηλεφώνου
- Φωτογραφίες
- Θέση / καθήκοντα

Κακόβουλο λογισμικό

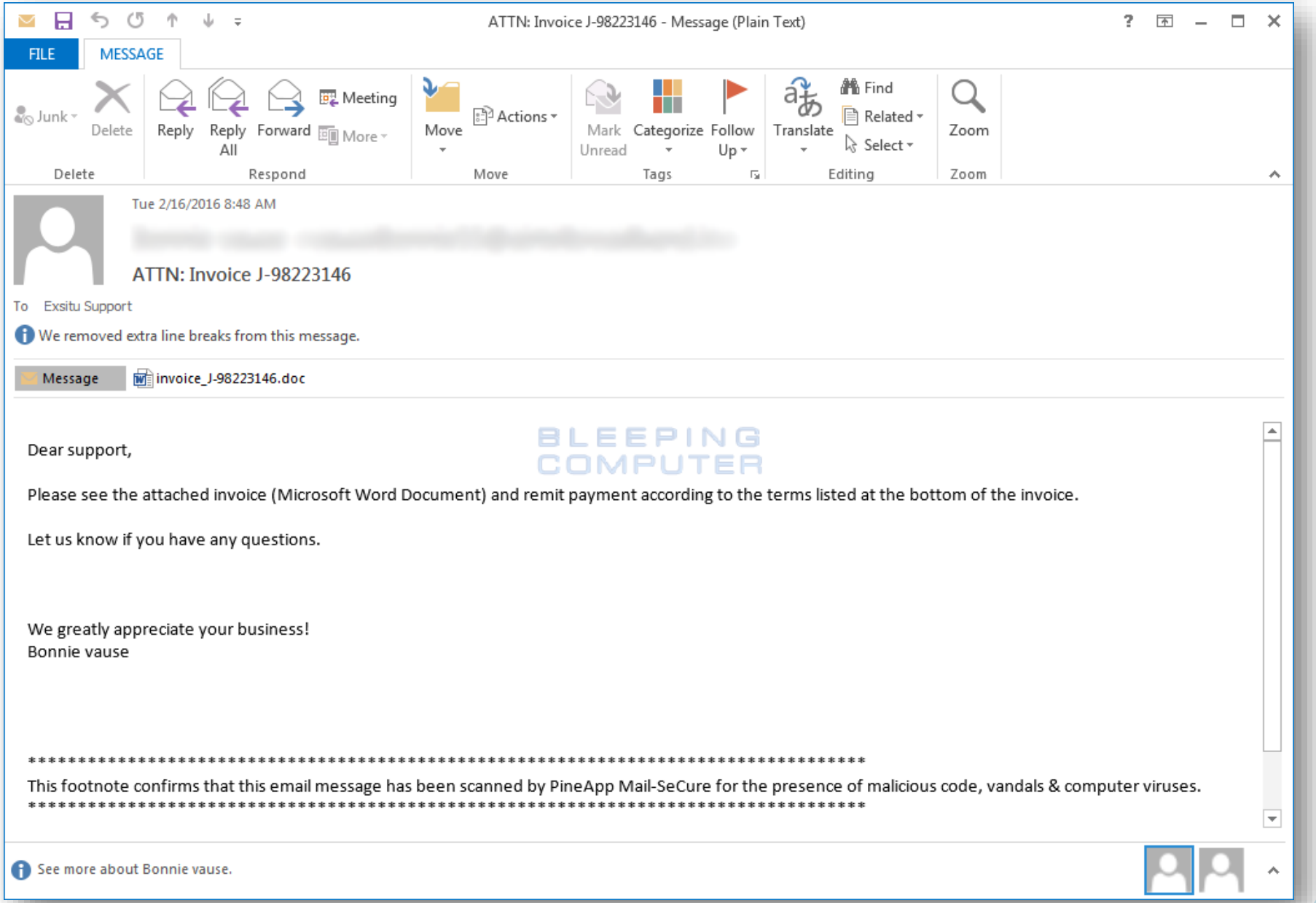
malicious software

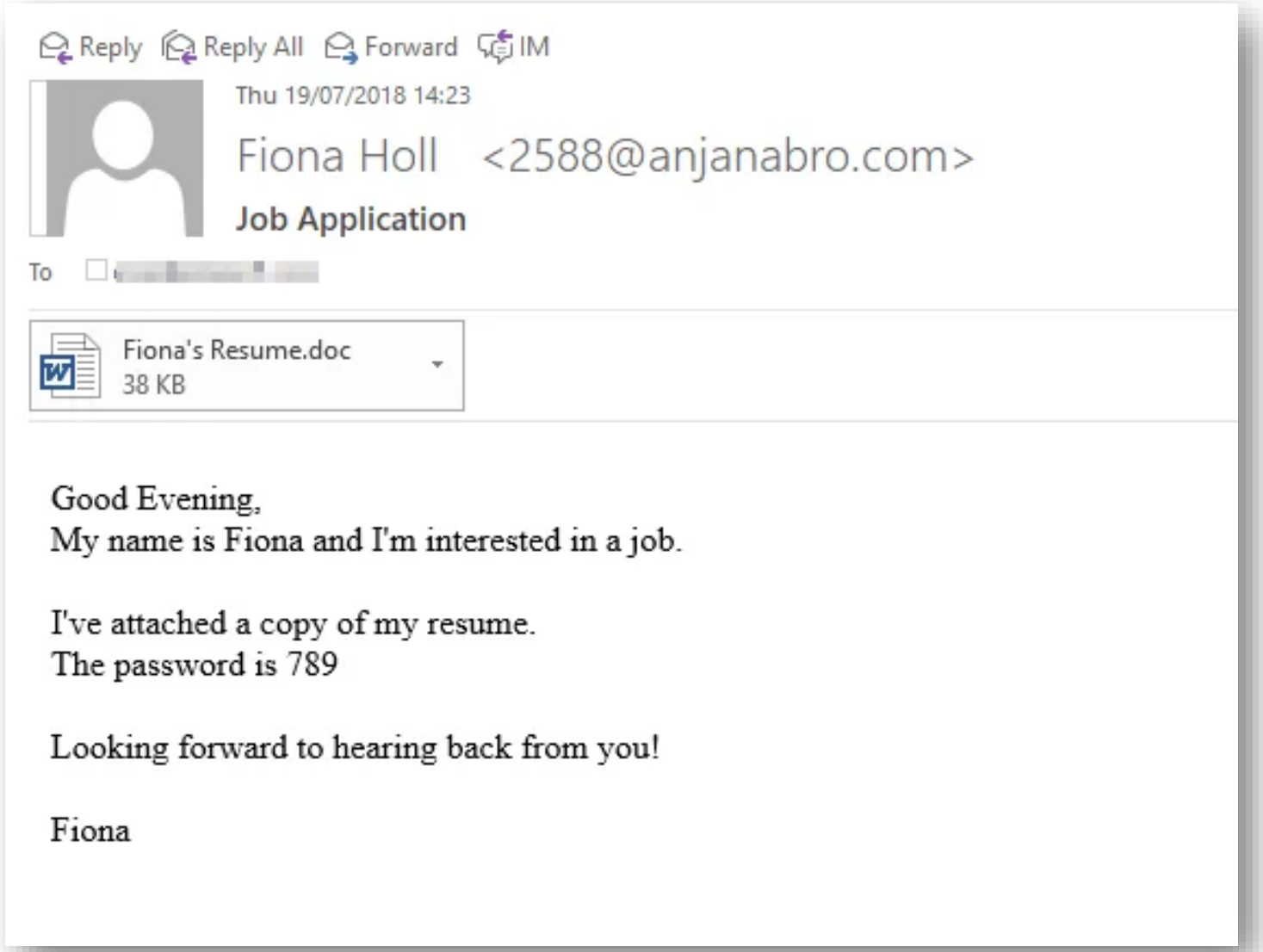
Malware

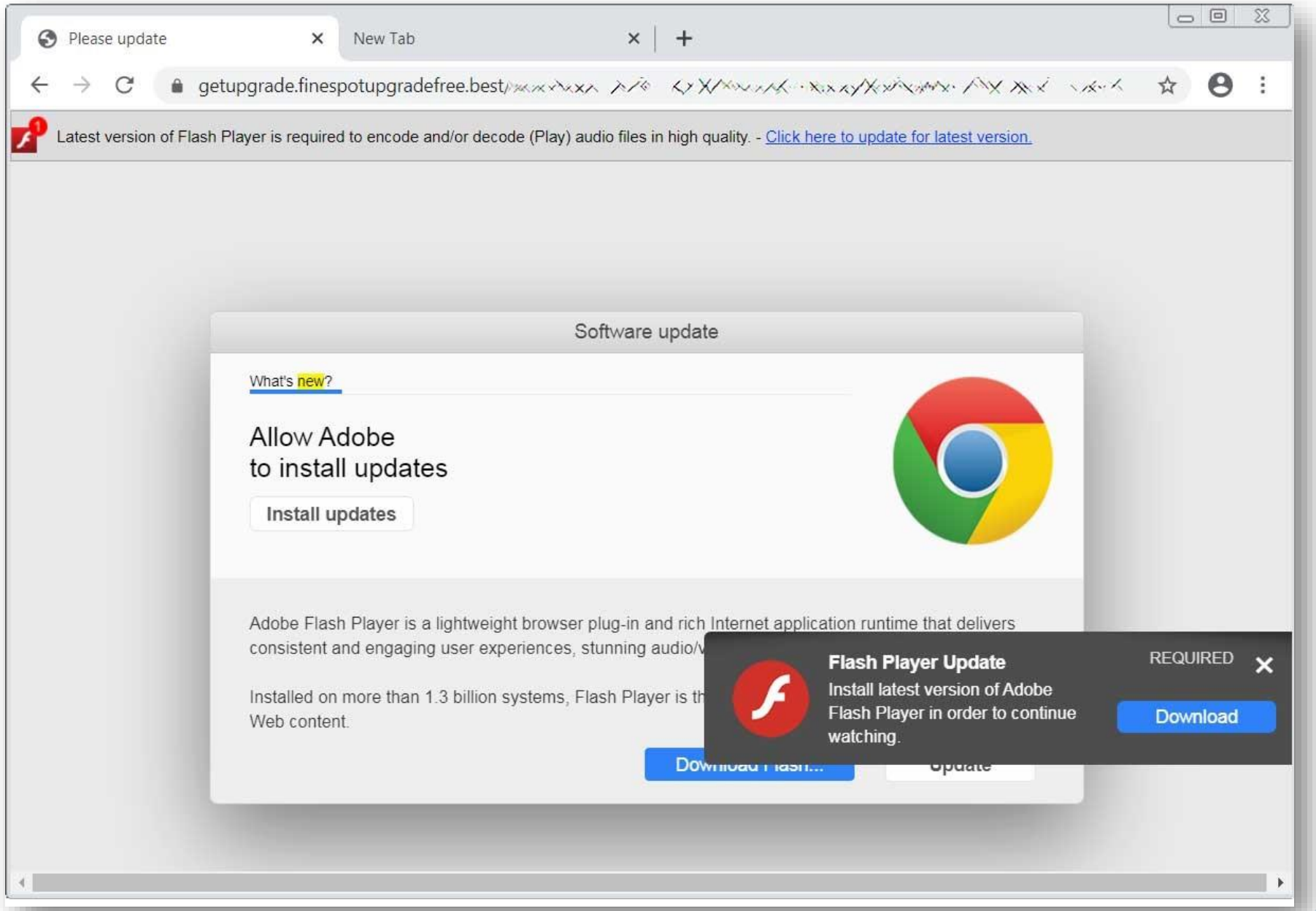
Λογισμικό σχεδιασμένο ώστε να εγκαθίσταται σε ένα σύστημα (υπολογιστή, κινητό, tablet) και να πραγματοποιεί τις ενέργειες που επιθυμεί ο δημιουργός του

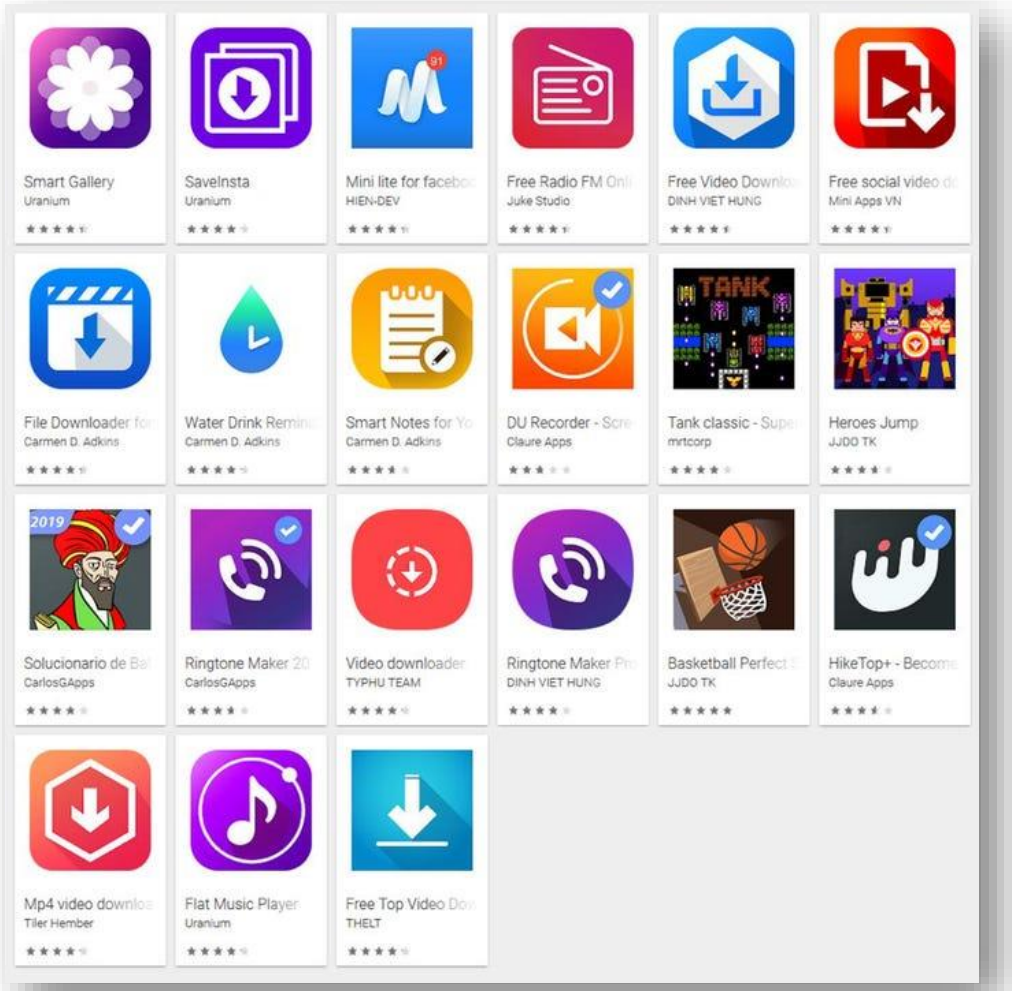
Τρόποι μόλυνσης

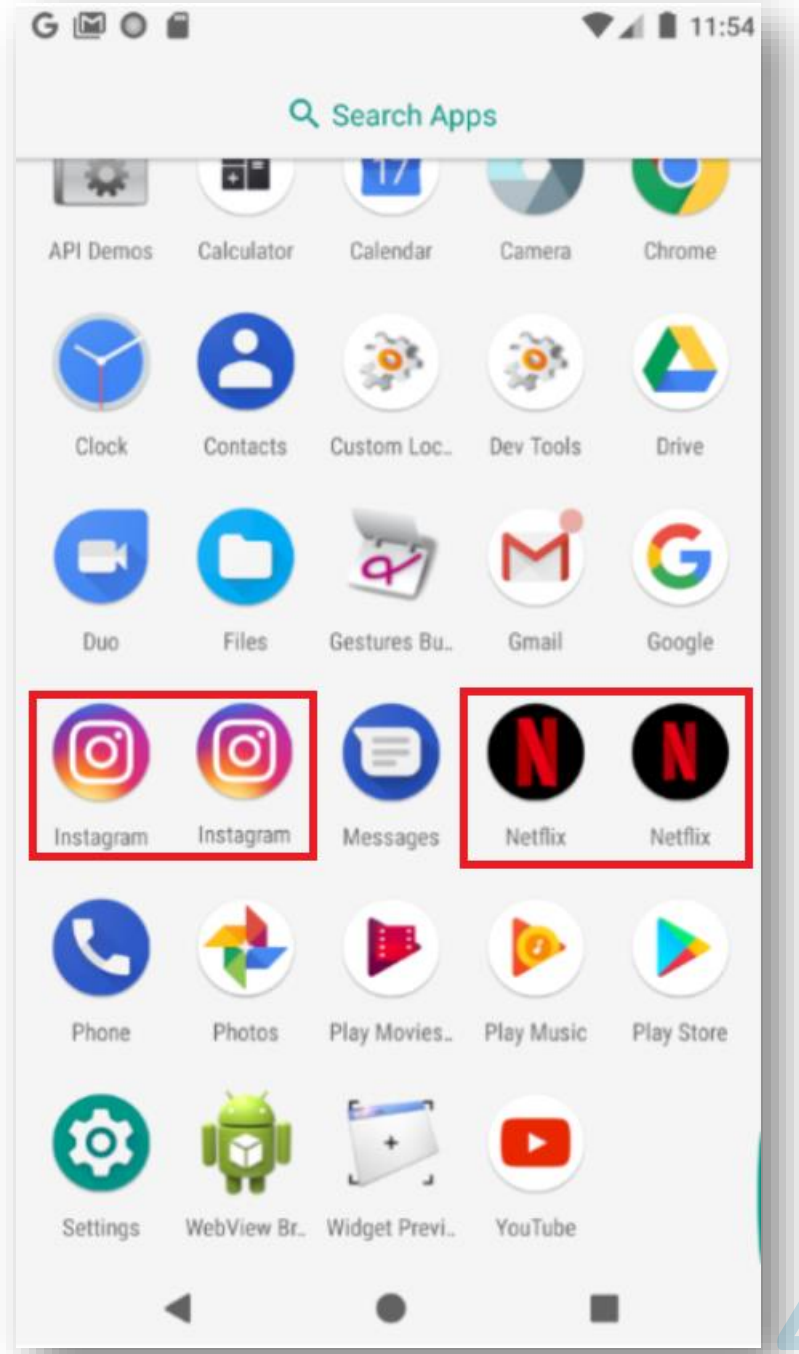
- Συνημμένο σε email ("καμουφλαρισμένο")
- USB stick
- "Κακόβουλη" ιστοσελίδα
- Άγνωστης προέλευσης αρχεία
- Ψεύτικη εφαρμογή


ATTN: Invoice J-98223146 - Message (Plain Text)
FILE
MESSAGE
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Move
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Move
Tags
Editing
Zoom
Tue 2/16/2016 8:48 AM
ATTN: Invoice J-98223146
To Exsitu Support
We removed extra line breaks from this message.
Message
invoice_J-98223146.doc
BLEEPING COMPUTER
Dear support,
Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.
Let us know if you have any questions.
We greatly appreciate your business!
Bonnie vause
****
This footnote confirms that this email message has been scanned by PineApp Mail-SeCure for the presence of malicious code, vandals & computer viruses.
****
See more about Bonnie vause.


Reply
Reply All
Forward
IM
Thu 19/07/2018 14:23
Fiona Holl <2588@anjanabro.com>
Job Application
To
Fiona's Resume.doc
38 KB
Good Evening,
My name is Fiona and I'm interested in a job.
I've attached a copy of my resume.
The password is 789
Looking forward to hearing back from you!
Fiona


Please update
New Tab
getupgrade.finespotupgradefree.best
Latest version of Flash Player is required to encode and/or decode (Play) audio files in high quality. - Click here to update for latest version.
Software update
What's new?
Allow Adobe
to install updates
Install updates
Adobe Flash Player is a lightweight browser plug-in and rich Internet application runtime that delivers
consistent and engaging user experiences, stunning audio/
Installed on more than 1.3 billion systems, Flash Player is th
Web content.
Flash Player Update
Install latest version of Adobe
Flash Player in order to continue
watching.
REQUIRED
Download

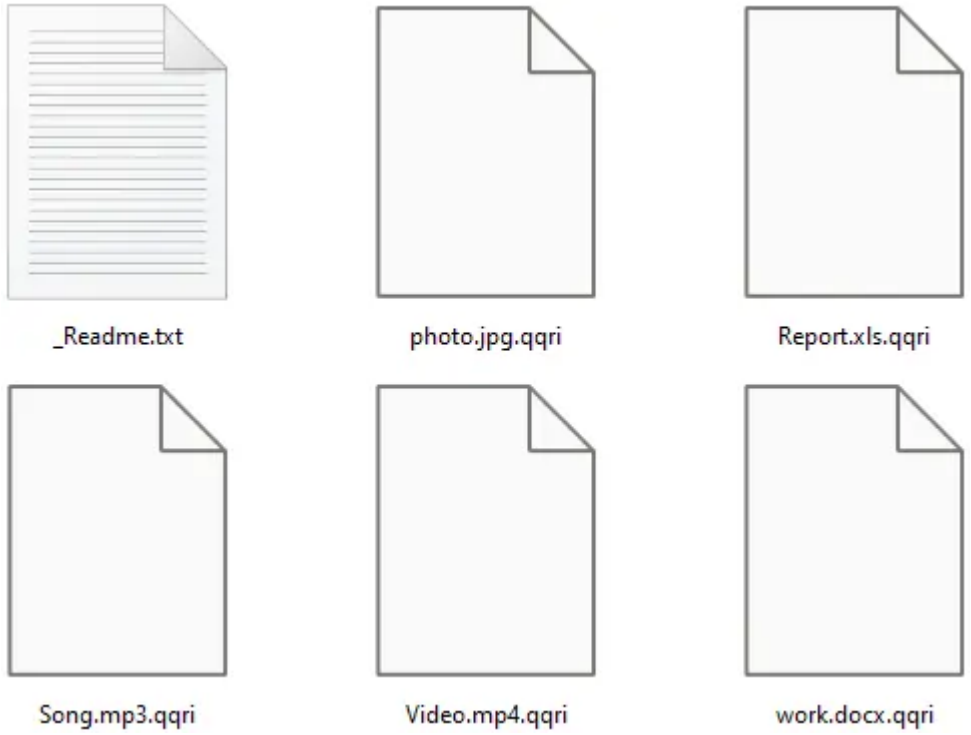

Smart Gallery
Uranium
SaveInsta
Uranium
Mini lite for faceb
HIEN-DEV
Free Radio FM Onl
Juke Studio
Free Video Downlo
DINH VIET HUNG
Free social video d
Mini Apps VN
File Downloader fo
Carmen D. Adkins
Water Drink Remin
Carmen D. Adkins
Smart Notes for Yo
Carmen D. Adkins
DU Recorder - Scre
Claure Apps
Tank classic - Supe
mrtcorp
Heroes Jump
JJDO TK
Solucionario de Ba
CarlosGApps
Ringtone Maker 20
CarlosGApps
Video downloader
TYPHU TEAM
Ringtone Maker Pro
DINH VIET HUNG
Basketball Perfect
JJDO TK
HikeTop+ - Become
Claure Apps
Mp4 video downlo
Tiler Hember
Flat Music Player
Uranium
Free Top Video Do
THELT


11:54
Search Apps
API Demos
Calculator
Calendar
Camera
Chrome
Clock
Contacts
Custom Loc..
Dev Tools
Drive
Duo
Files
Gestures Bu..
Gmail
Google
Instagram
Instagram
Messages
Netflix
Netflix
Phone
Photos
Play Movies..
Play Music
Play Store
Settings
WebView Br..
Widget Previ..
YouTube

Αφού περάσει στη συσκευή μας, θα μπορούσε να:

- Προκαλέσει δυσλειτουργίες στο σύστημά μας
- Υποκλέψει usernames & passwords
- Υποκλέψει όλες τις επικοινωνίες μας
- Υποκλέψει / Αλλοιώσει / διαγράψει δεδομένα
- Κρυπτογραφήσει όλα τα δεδομένα, απαιτώντας λύτρα

Ransomware


_Readme.txt
photo.jpg.qqri
Report.xls.qqri
Song.mp3.qqri
Video.mp4.qqri
work.docx.qqri

Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
KurtSchweickardt@protonmail.com
or
KurtSchweickardt@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe

Απαίτηση για "λύτρα"

The Biggest Ransomware Payouts of 2021

Data Source: Information is Beautiful; Data: USD

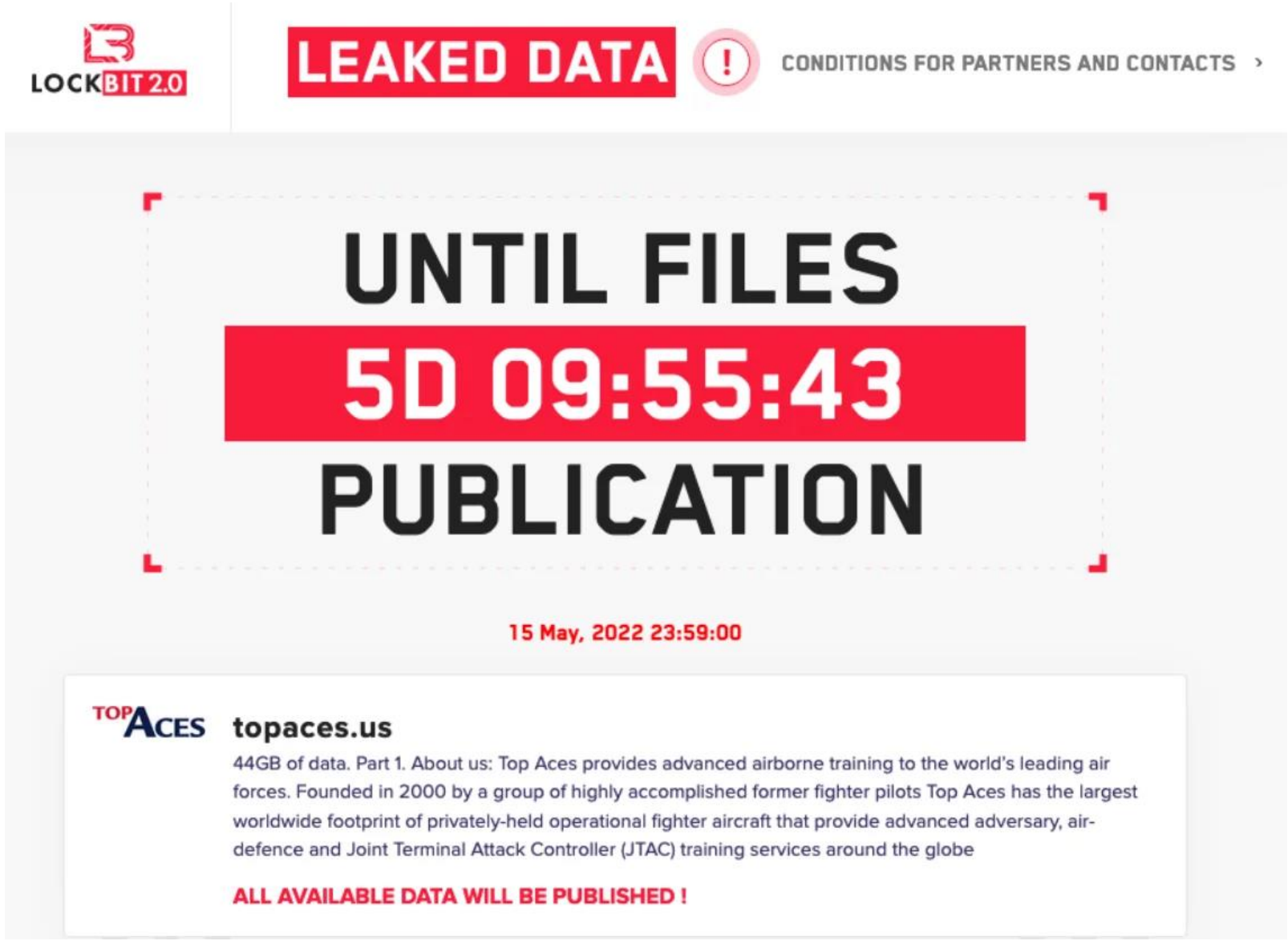
Τελευταία τάση

Ransomware

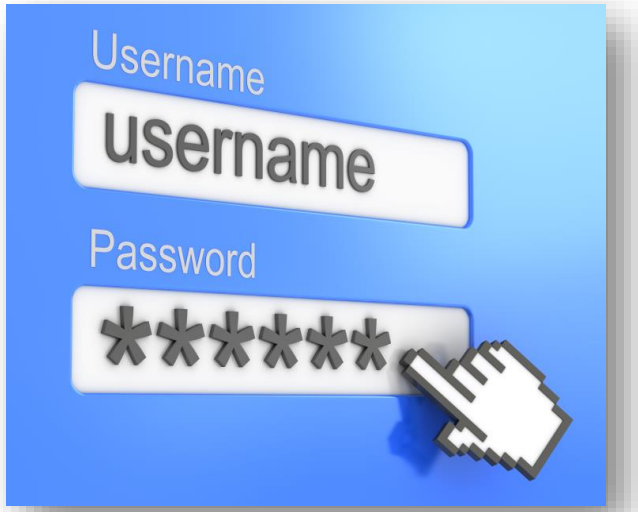
- Κρυπτογράφηση αρχείων
- Υποκλοπή αρχείων

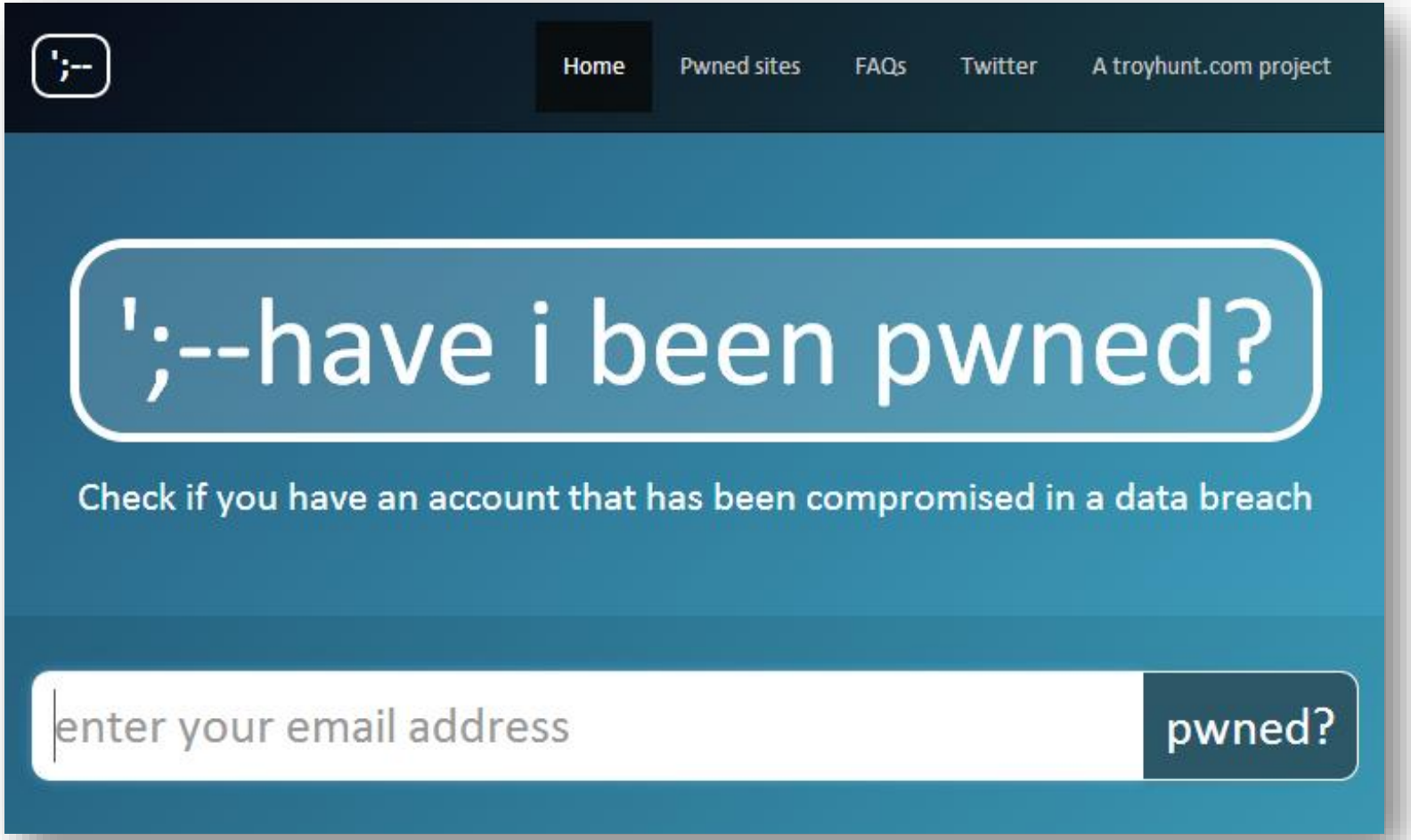
Απαίτηση για λύτρα

- Αποκρυπτογράφηση των κλειδωμένων αρχείων
- Μη αποκάλυψη / διαρροή των αρχείων στο ευρύ κοινό


LOCKBIT 2.0
LEAKED DATA
CONDITIONS FOR PARTNERS AND CONTACTS
UNTIL FILES
5D 09:55:43
PUBLICATION
15 May, 2022 23:59:00
TOP ACES
topaces.us
44GB of data. Part 1. About us: Top Aces provides advanced airborne training to the world's leading air forces. Founded in 2000 by a group of highly accomplished former fighter pilots Top Aces has the largest worldwide footprint of privately-held operational fighter aircraft that provide advanced adversary, air-defence and Joint Terminal Attack Controller (JTAC) training services around the globe
ALL AVAILABLE DATA WILL BE PUBLISHED !

Πρόληψη & προστασία


Username
username
Password
******


Home
Pwned sites
FAQs
Twitter
A troyhunt.com project
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
enter your email address
pwned?

Κωδικοί πρόσβασης – passwords

Μήκος κωδικού

- Σύνθεση
- Γράμματα (κεφαλαία & μικρά), αριθμοί, ειδικοί χαρακτήρες

Ιστορικότητα

- Ίδιος κωδικός στο παρελθόν

Επαναληψιμότητα

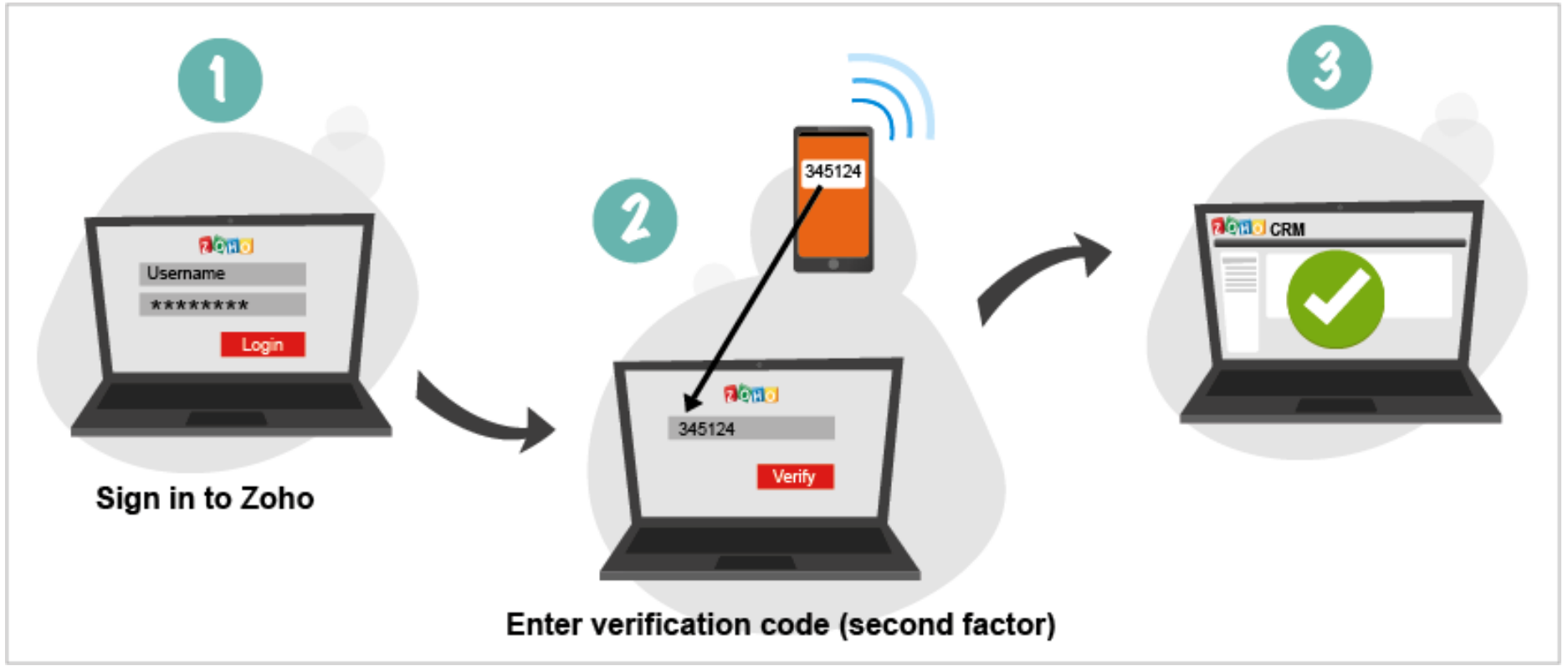
- Ίδιος κωδικός σε διαφορετικές υπηρεσίες

Διάρκεια

Κωδικοί πρόσβασης – passwords

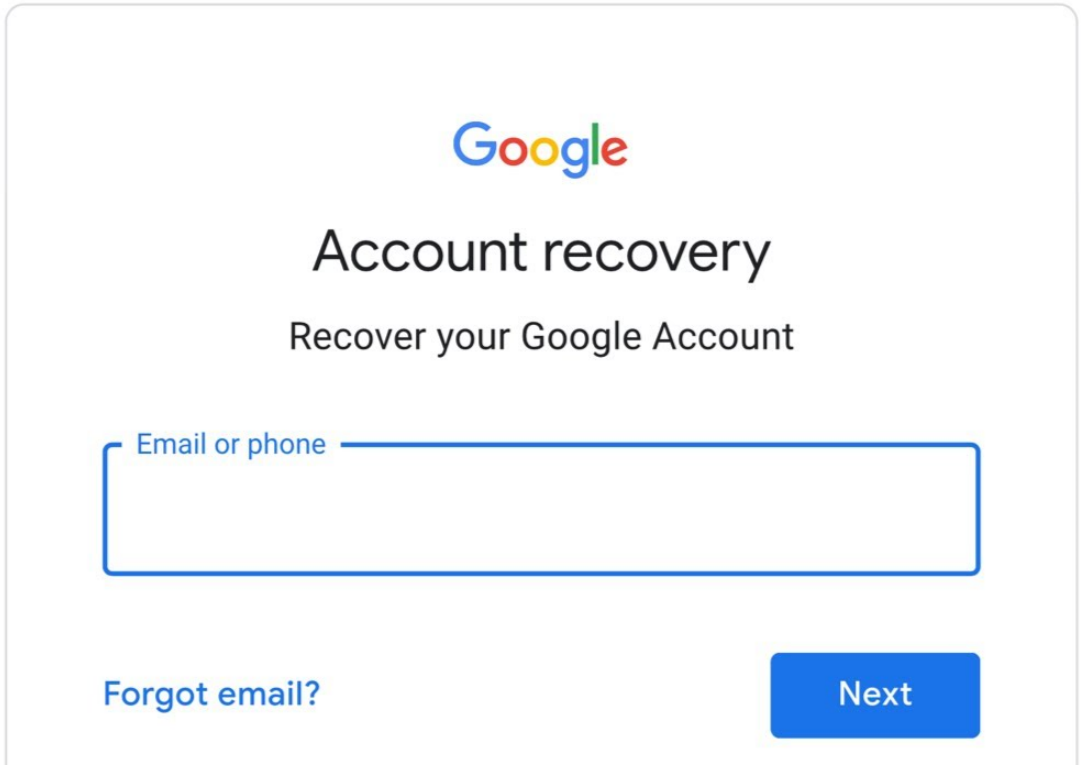
- Εργοστασιακοί κωδικοί
- Επίθεση «brute force»
- Συνδυασμός με επιπλέον χαρακτηριστικά
  - π.χ. βιομετρικά
- Αυθεντικοποίηση δύο βημάτων

2-step verification

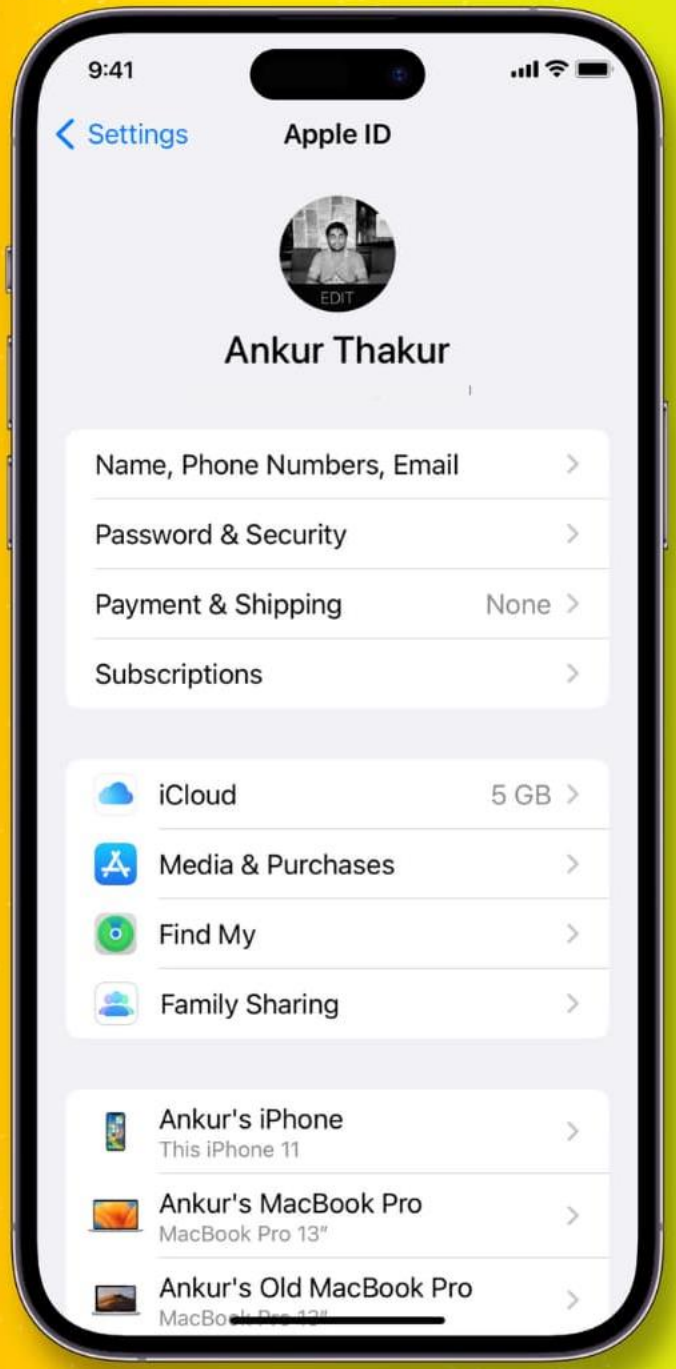


2-step verification

Ανάκτηση λογαριασμού / προφίλ



Ρυθμίσεις ασφαλείας



Λογισμικό & προστασία

- ✓Γνησιότητα λογισμικού
  - ❖ Ενημερώσεις ασφαλείας / διορθώσεις σφαλμάτων
  - ❖ «πειρατικά» / «σπασμένα» προγράμματα
  - ❖ Λογισμικό «ανοιχτού κώδικα»
- ✓Anti-virus & anti-malware
  - ❖ Ενημερώσεις βάσεων ιών

Τήρηση αντιγράφων ασφαλείας

- **Back up**
- Συχνότητα δημιουργίας αντιγράφων
  - ✓ Ανάλογα με τις δραστηριότητες του οργανισμού
- Τρόπος δημιουργίας
  - ✓ Αυτόματα ή χειροκίνητα
- Τοποθεσία τήρησης αντιγράφων
  - ✓ Τοπικά ή απομακρυσμένα

Απομακρυσμένη πρόσβαση & BYOD

- Χρήση προσωπικών φορητών συσκευών
  - Laptops
  - Smartphones
  - Tablets
- για πρόσβαση σε εταιρικά δεδομένα από απόσταση
- Προσοχή στα άγνωστα δίκτυα WiFi (π.χ. αεροδρόμια)

Εκτυπωτές & Φωτοτυπικά

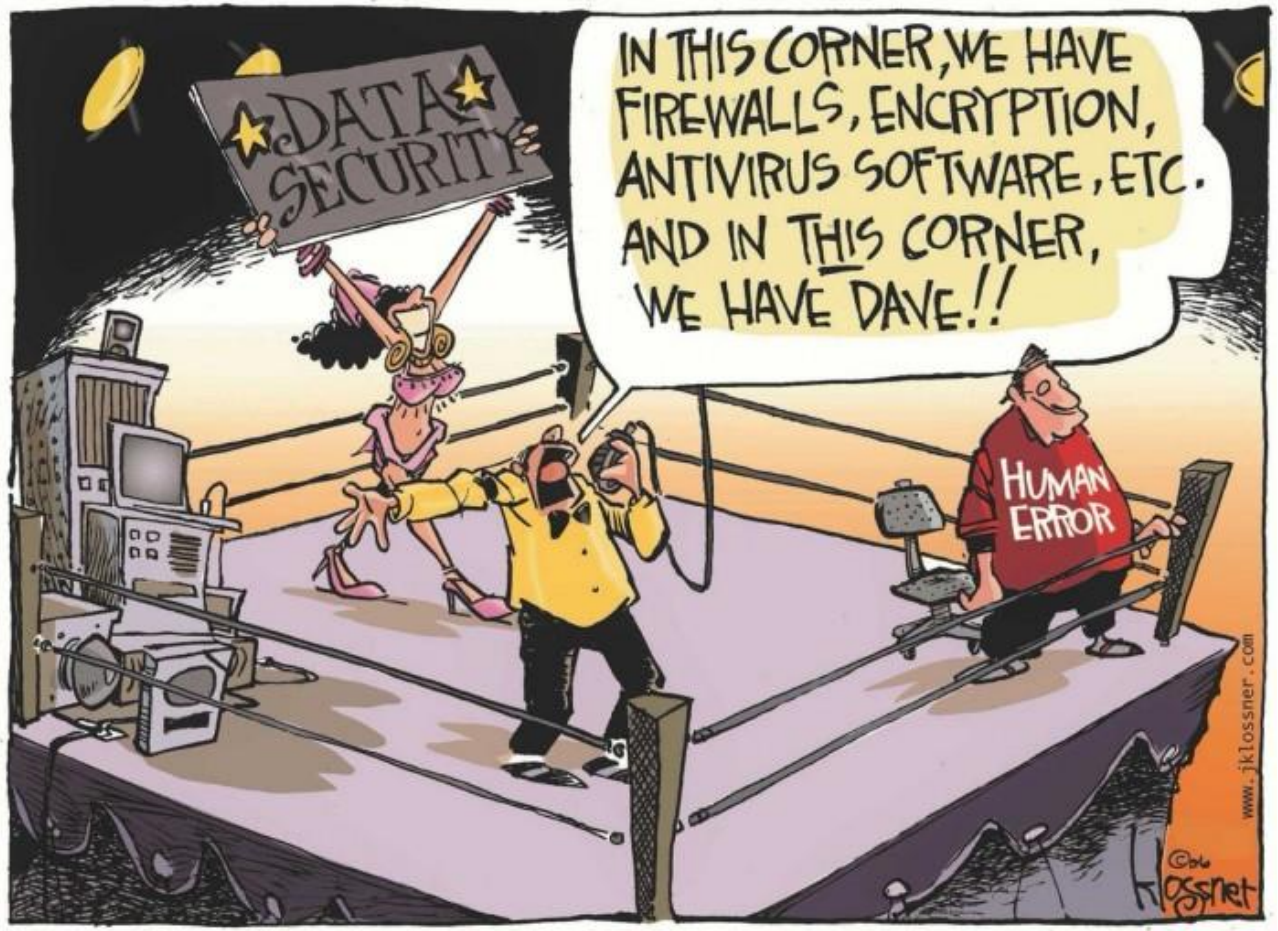
- Τοποθεσία
- Δίκτυα
- Ποιος έχει φυσική πρόσβαση;
- Χρήση PIN εκτύπωσης

Πολιτική «καθαρού γραφείου»

Κρυπτογράφηση – encryption

- ✓ **Μετασχηματισμός δεδομένων**
- ✓ σε μορφή που δε μπορεί να διαβαστεί από κανένα
- ✓ παρά μόνο από αυτόν που διαθέτει ένα κατάλληλο κλειδί

- ❖ Μπορεί να εφαρμοστεί σε:
  - ➢ Αρχείο (file)
  - ➢ Μονάδες αποθήκευσης (full disc)
  - ➢ Ηλεκτρονικό ταχυδρομείο
  - ➢ Δίκτυα επικοινωνίας
    - ✓ *HTTPS*
    - ✓ *Δημόσιο WiFi (μέσω VPN)*
  - ➢ Ψηφιακή υπογραφή



Εκπαίδευση
προσωπικού / χρηστών

Ο άνθρωπος παραμένει ο «αδύναμος κρίκος»

Καταγγελία εγκλήματος

- Ελληνική Αστυνομία / Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
- gov.gr

Ερωτήσεις & συζήτηση

Ευχαριστώ
για την προσοχή σας!

Γεώργιος Αθ. Γέρμανος // germanos@uop.gr

Τρίπολη: μήνας αφιερωμένος στην Τεχνολογία & στην Επιστήμη

Την Άνοιξη του 2023
από το Τμήμα Πληροφορικής & Τηλεπικοινωνιών
στο Επιμελητήριο Αρκαδίας

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΠΕΛΟΠ

ΕΠΙΜΕΛΗΤΗΡΙΟ ΑΡΚΑΔΙΑΣ

Ομιλίες για όλους τους πολίτες!

ΠΡΟΓΡΑΜΜΑ ΟΜΙΛΙΩΝ

Τετάρτη 3 Μαΐου
Διαδικτυακοί κίνδυνοι και πώς να προστατευτείτε
Γεώργιος Γέρμανος, Ειδικός στην πρόληψη και στη διερεύνηση κυβερνοεγκλημάτων
Υπ. Διδάκτορας στο Τμήμα Πληροφορικής & Τηλεπικοινωνιών

Τετάρτη 17 Μαΐου
Οι μελανές οπές και η αιχμαλωσία του φωτός
Δρ. Αντώνιος Α. Αντωνίου, Αστροφυσικός
Εκπαιδευτικό Προσωπικό στο Τμήμα Πληροφορικής & Τηλεπικοινωνιών

Τετάρτη 24 Μαΐου
4 bit ιστορίας: ασυνήθιστα συμβάντα που επηρέασαν τον κόσμο της πληροφορικής
Δρ. Χρήστος Τρυφωνόπουλος, Ειδικός σε θέματα διαχείρισης πληροφορίας
Καθηγητής στο Τμήμα Πληροφορικής & Τηλεπικοινωνιών

Πέμπτη 1 Ιουνίου
Ο μαγικός κόσμος του διαδικτύου των πραγμάτων
Δρ. Κωνσταντίνος Βασιλάκης, Ειδικός στα πληροφοριακά συστήματα
Κοσμήτορας της Σχολής Οικονομίας και Τεχνολογίας, Καθηγητής στο Τμήμα Πληροφορικής & Τηλεπικοινωνιών