EUROBANK Cyber Noesis

Cyber Security: Τάσεις & Νέες Απειλές

Konstantinos Papadatos

Founder / Managing Director - Cyber Noesis

MSc Infosec, CISSP-ISSMP, CISM, ISO27001 LA, ISO27005 RM, PMP, MBCI, CDPO, Lead SCADA Security Manager

27/06/2023

Περιεχόμενα

Σύγχρονες Απειλές & Πραγματικά Περιστατικά

Τεχνικές Επιθέσεων & Πρακτικές Αντιμετώπισης

Cyber Security Quick Wins

- Πως να προστατεύσω την επιχείρηση & τους εργαζομένους από Κυβερνοεπιθέσεις.

WEF: Global Risks …

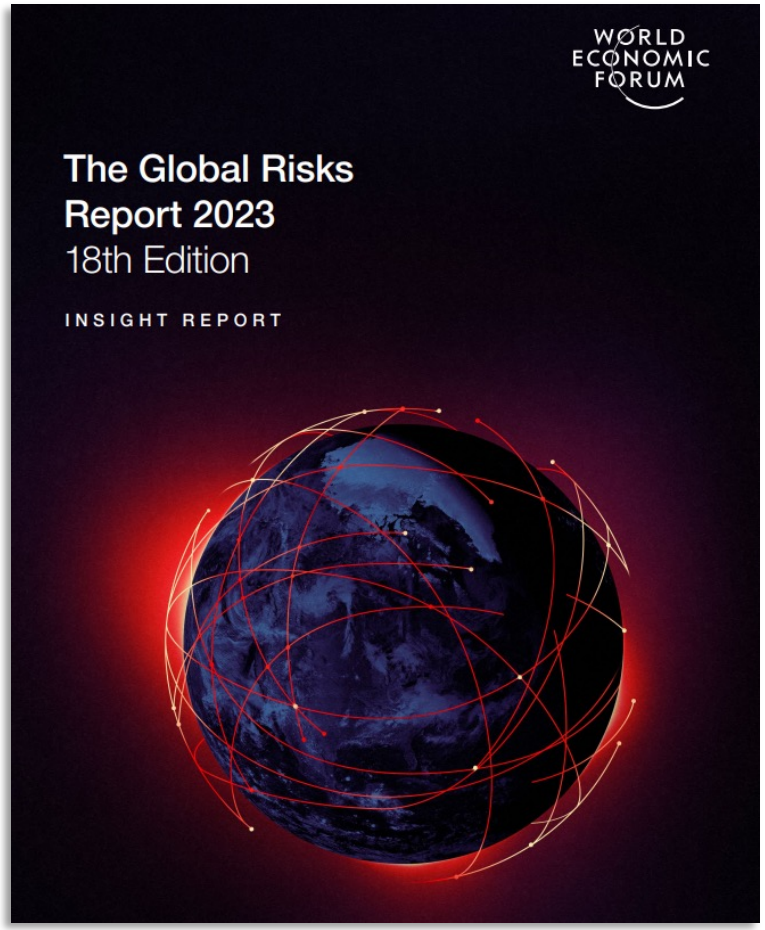
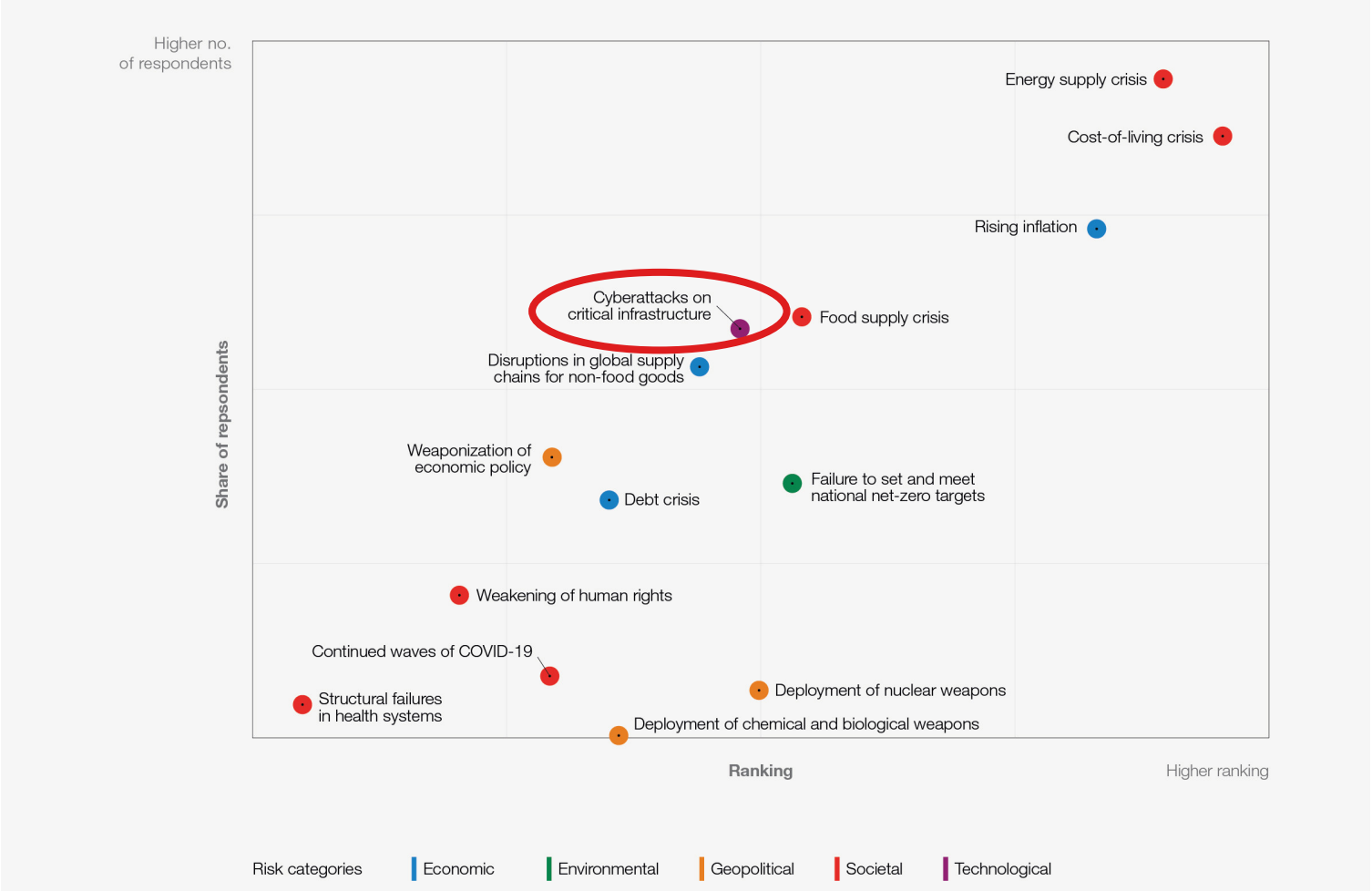
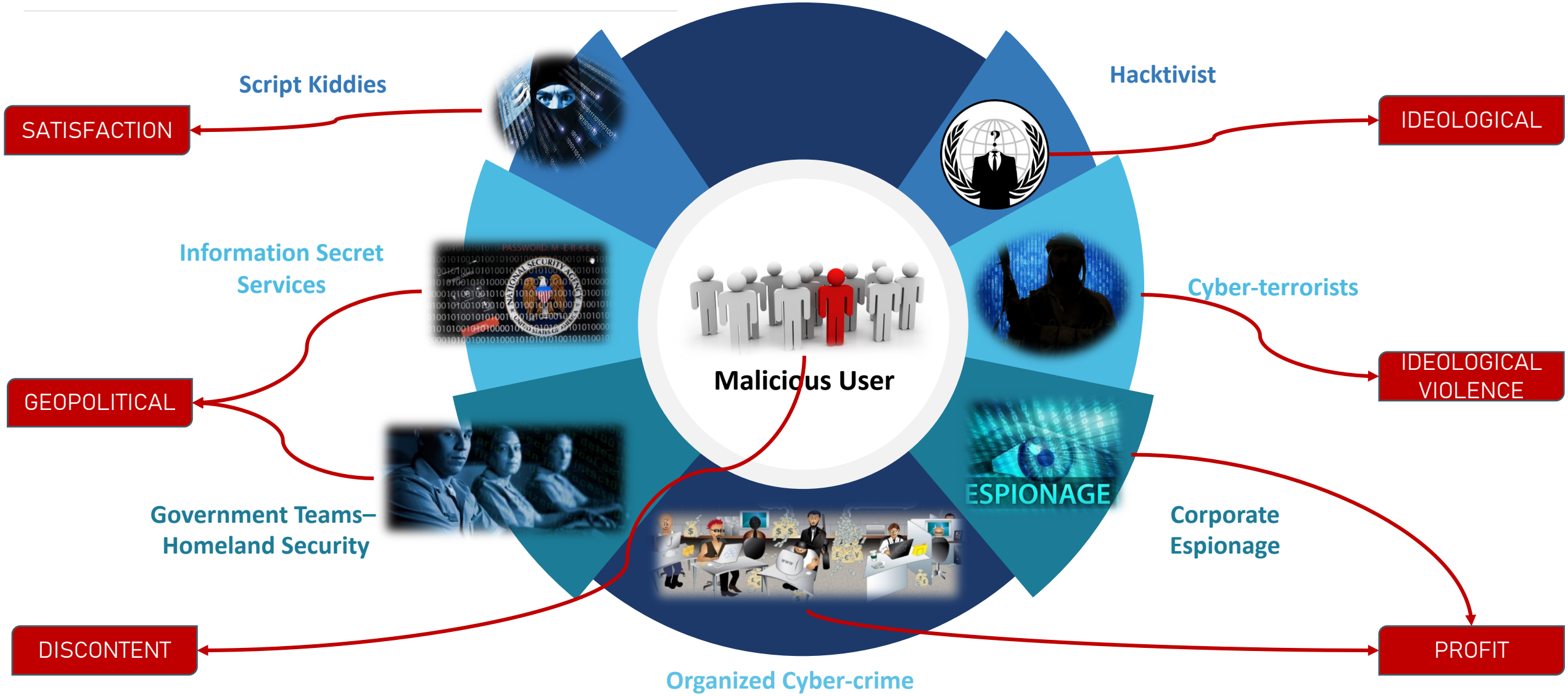


FIGURE 1.1 **Currently manifesting risks**

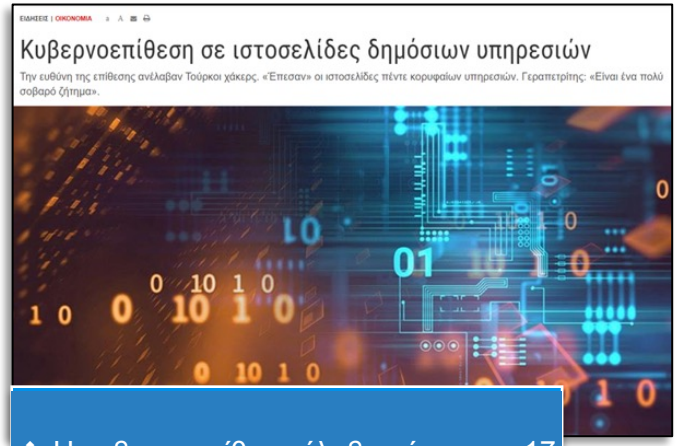
"Please rank the top 5 currently manifesting risks in order of how severe you believe their impact will be on a global level in 2023"



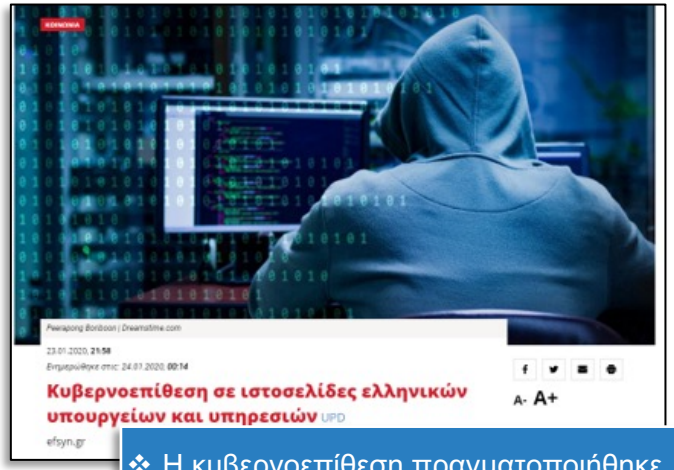
Τύποι & Κίνητρα Επιτιθέμενων



Περιστατικά Ασφάλειας στην Ελλάδα …



- Η κυβερνοεπίθεση έλαβε χώρα στις 17 Ιανουαρίου 2020.
- Μαζική κυβερνοεπίθεση δέχθηκαν οι ιστοσελίδες της Βουλής, του Υπ.Εξ., του υπουργείου Οικονομικών, του Χρηματιστηρίου Αθηνών και της ΕΥΠ.



- Η κυβερνοεπίθεση πραγματοποιήθηκε στις 23 Ιανουαρίου 2020.
- Επιθέσεις τύπου DDoS κατά κυβερνητικών ιστοσελίδων.

- Χάκερ επιτέθηκαν σε μεγάλα νοσοκομεία της Αττικής, το «Σωτηρία» και το «Ασκληπιείο» της Βούλας.

- Η κυβερνοεπίθεση σημειώθηκε στις 15 Αυγούστου 2020.
- Θύμα της επίθεσης είναι η εταιρία Carnival Corporation.

ENISA Threat Landscape 2022


TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030
1
Supply chain compromise of software dependencies
2
Advanced disinformation campaigns
3
Rise of digital surveillance authoritarianism/ loss of privacy
4
Human error and exploited legacy systems within cyber-physical ecosystems
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
10
Artificial Intelligence Abuse
THREATS 2030
5
Targeted attacks enhanced by smart device data
6
Lack of analysis and control of space-based infrastructure and objects
9
Cross border ICT service providers as a single point of failure
8
Skill shortage
7
Rise of advanced hybrid threats

Περιεχόμενα

Σύγχρονες Απειλές &
Πραγματικά Περιστατικά

Τεχνικές Επιθέσεων & Πρακτικές Αντιμετώπισης

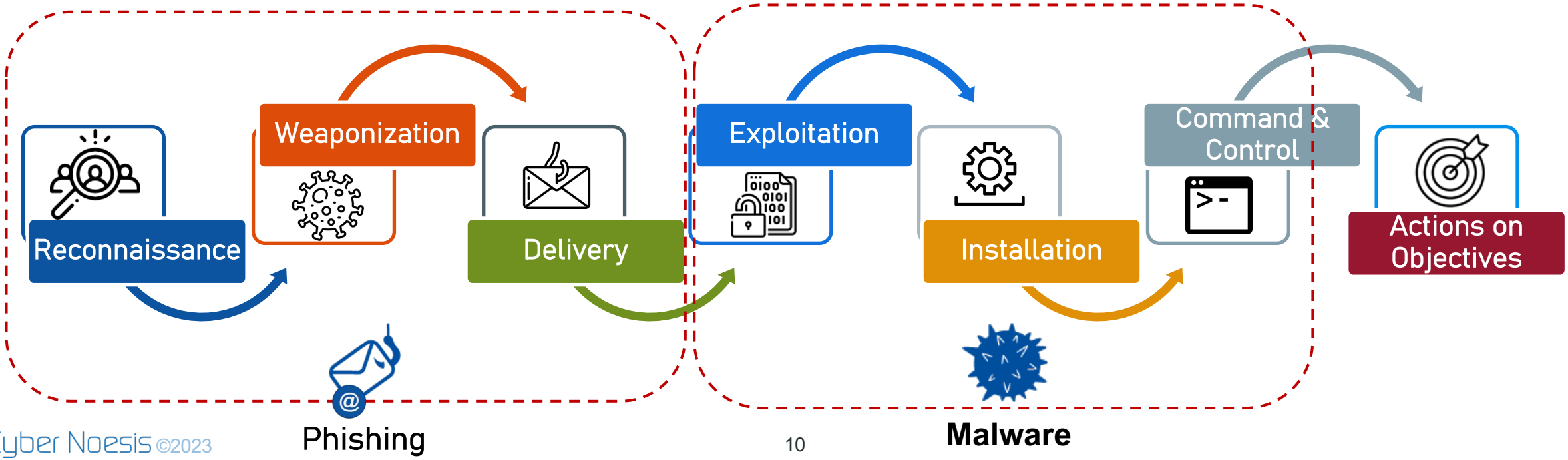
Cyber Security Quick Wins

- Πως να προστατεύσω την επιχείρηση & τους εργαζομένους από Κυβερνοεπιθέσεις.

Πως Λειτουργούν οι Εξελιγμένες Σύγχρονες Επιθέσεις…

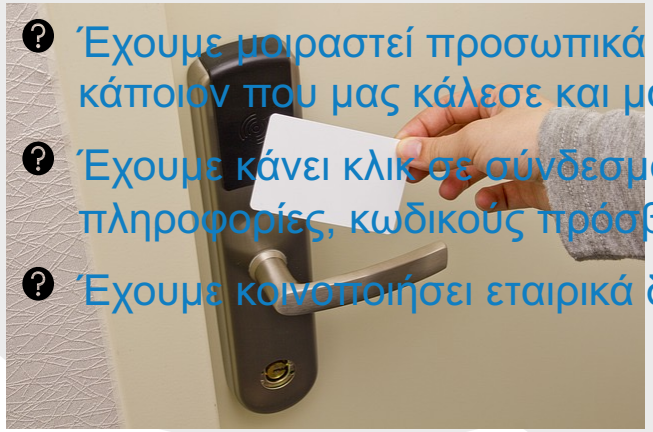
- Το **Cyber Kill Chain framework** είναι μέρος του Intelligence Driven Defense model για την ταυτοποίηση και πρόληψη κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.

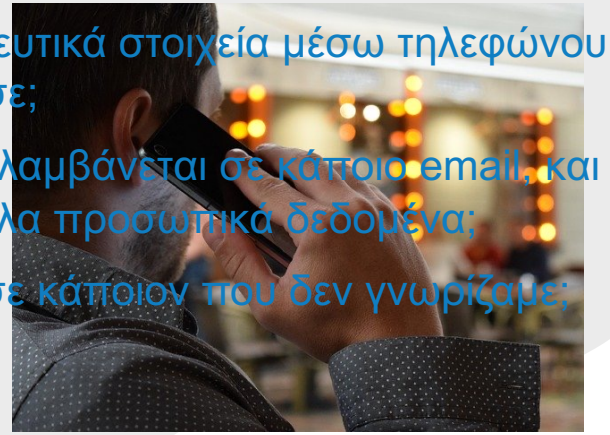
- Το μοντέλο αυτό προσδιορίζει τα στάδια που ολοκληρώνουν οι επιτιθέμενοι για να επιτύχουν τον στόχο τους



Ας αναλογιστούμε…

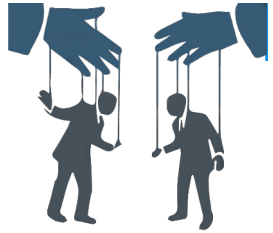
- Έχουμε ανοίξει την πόρτα σε κάποιον που δεν γνωρίζουμε αν έχει πρόσβαση στο χώρο της εταιρείας;
- Έχουμε μοιραστεί προσωπικά και εμπιστευτικά στοιχεία μέσω τηλεφώνου με κάποιον που μας κάλεσε και μας τα ζήτησε;
- Έχουμε κάνει κλικ σε σύνδεσμο που περιλαμβάνεται σε κάποιο email, και δώσαμε πληροφορίες, κωδικούς πρόσβασης ή άλλα προσωπικά δεδομένα;
- Έχουμε κοινοποιήσει εταιρικά δεδομένα σε κάποιον που δεν γνωρίζαμε;





Εάν ναι, θα μπορούσαμε να είχαμε πέσει θύμα μιας επίθεσης κοινωνικής μηχανικής...

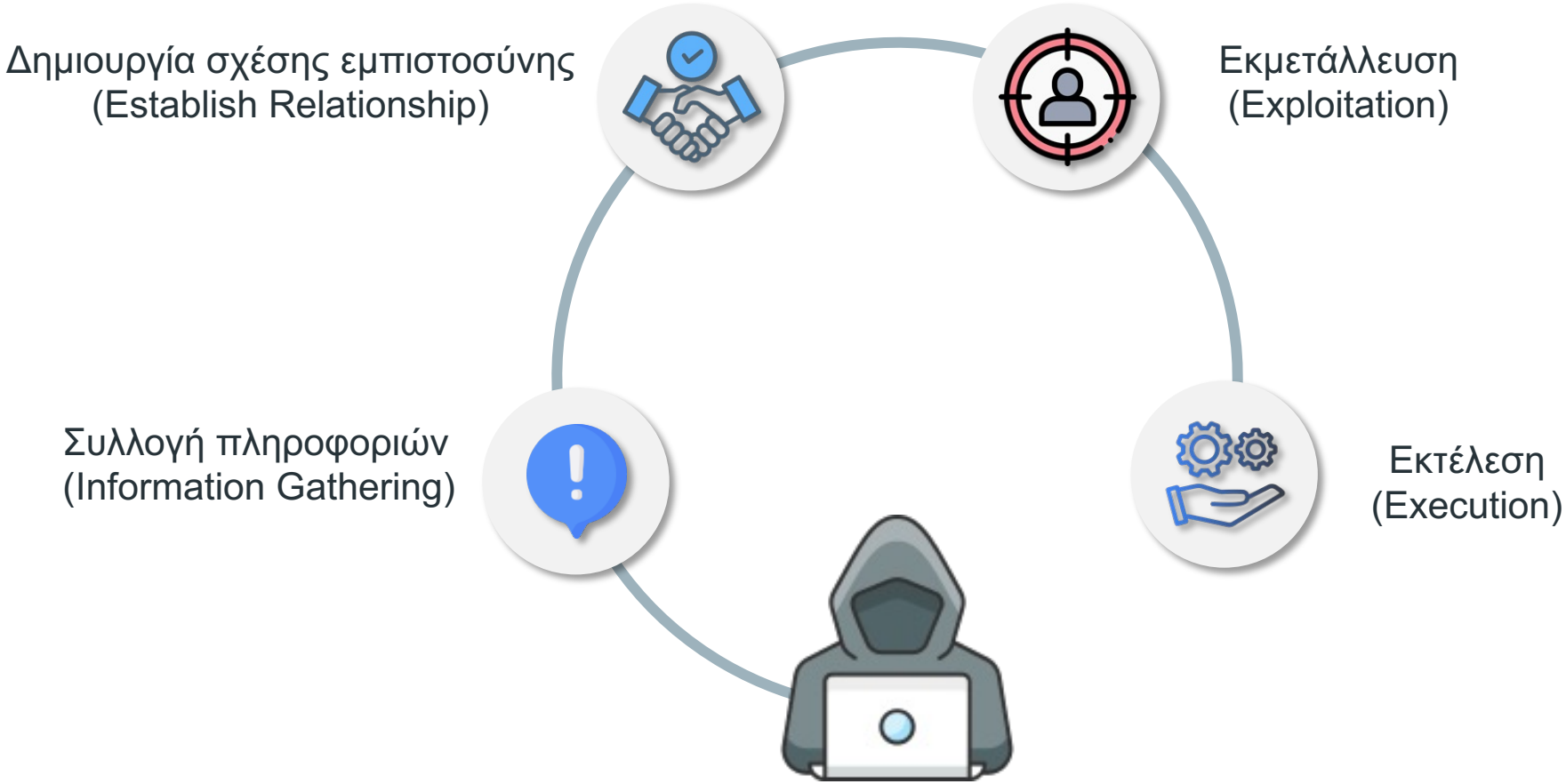
Κοινωνική Μηχανική – Social Engineering



Είναι η τεχνική που, με τη χρήση μεθόδων **εξαπάτησης**, αποσκοπεί στην απόκτηση **εμπιστευτικής πληροφορίας** ή στην παρακίνηση να πραγματοποιηθεί μια ενέργεια από τον χρήστη που αντίκειται στις πολιτικές και στις διαδικασίες του οργανισμού με στόχο την παραβίαση της **ασφάλειας**.

Η Ασφάλεια Πληροφοριών εξαρτάται κυρίως από τους ανθρώπους και δευτερευόντως από την τεχνολογία.

Στάδια Επιθέσεων Κοινωνικής Μηχανικής



Quiz

Ποιος είναι ο πρώτος γνωστός επιτιθέμενος που χρησιμοποίησε τεχνικές Κοινωνικής Μηχανικής (Social Engineering);

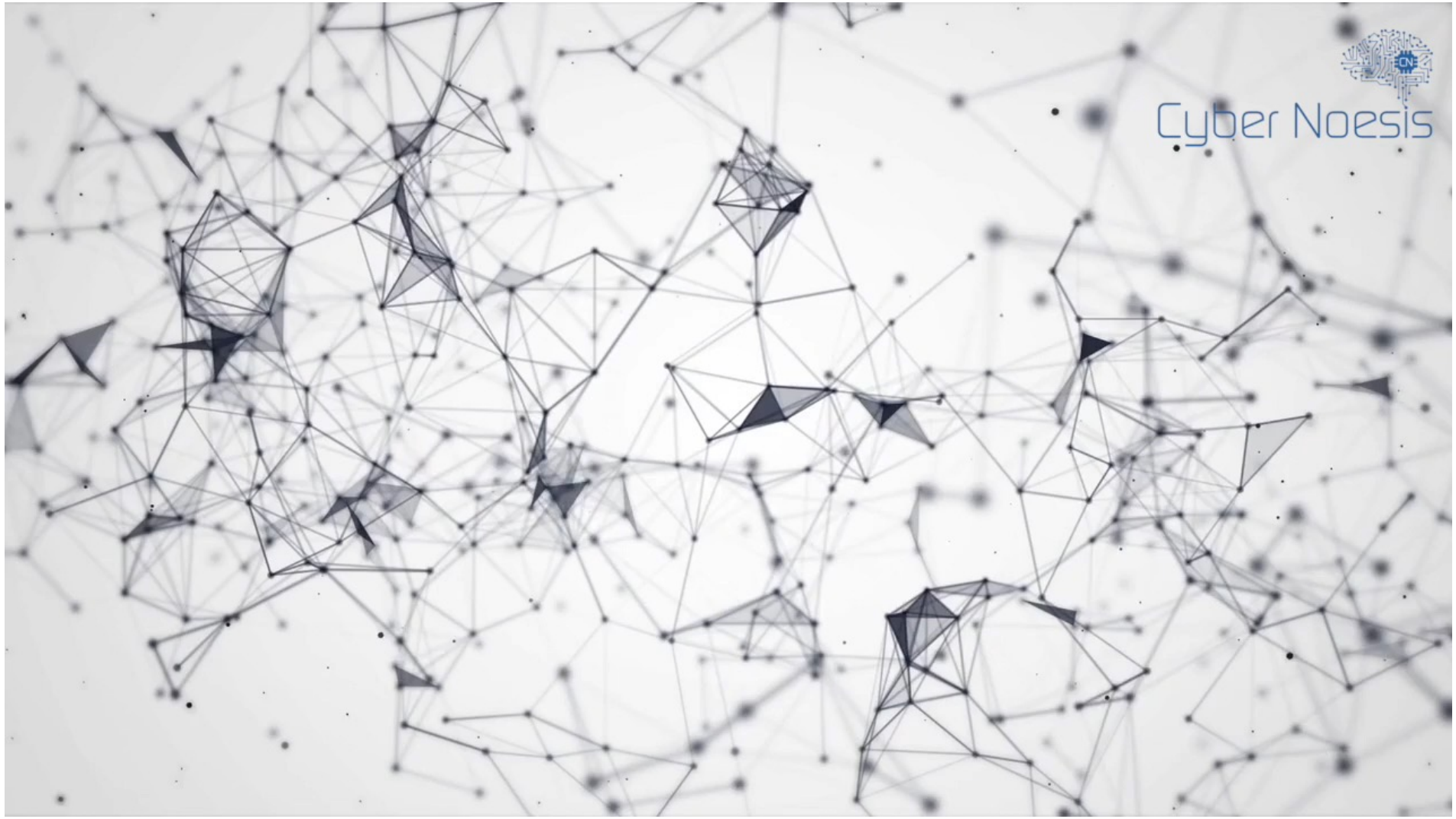
Α  Kevin Mitnick

Β  Αλίκη Βουγιουκλάκη

Γ  Vladimir Putin

Δ  Sandra Bullock (Angela Bennett)

Social Engineering Video



Συμπεριφορά Επιτιθέμενων

Οι επιτιθέμενοι δύναται να εκμεταλλευθούν:

Χαρακτηριστικά της Ανθρώπινης Συμπεριφοράς

- Συναδελφική Αλληλεγγύη
- Ανθρωπιά / Συμπόνια
- Άγνοια Κινδύνων και Τεχνολογίας

Δημοσιοποιημένες Εταιρικές Πληροφορίες για να γίνουν Πειστικοί

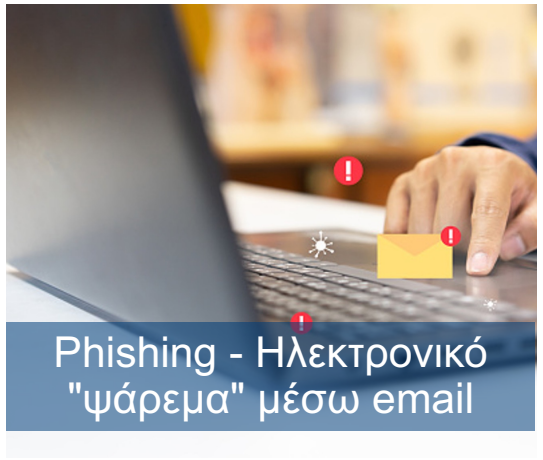
- Εσωτερικές Διαδικασίες
- Ονόματα Προσωπικού
- Οργανωτική Δομή Εταιρείας

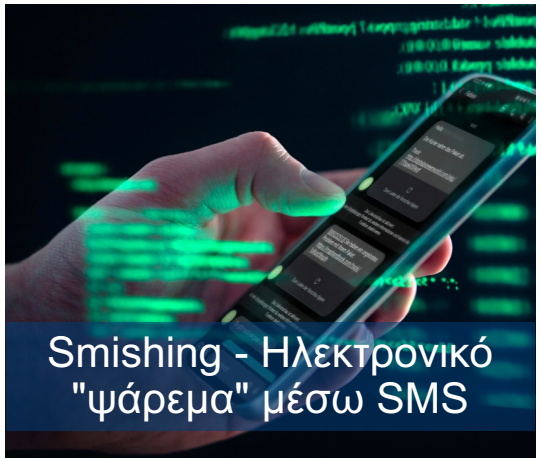
Ευγενική ή Επιτακτική Συμπεριφορά

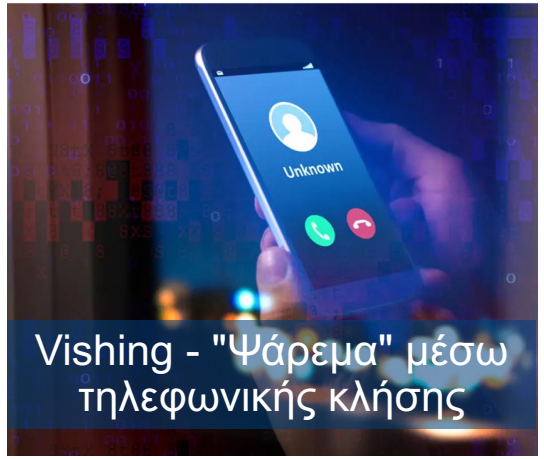
- Αίτημα για άμεση εξυπηρέτηση
- Προθυμία να μας βοηθήσουν σε πρόβλημα που αντιμετωπίζουμε
- Άσκηση πίεσης για ζήτημα που θα ωφελήσει τον οργανισμό μας

Είδη Επιθέσεων Κοινωνικής Μηχανικής

Επιτιθέμενοι θα προσπαθήσουν να μας χειραγωγήσουν και να εκμεταλλευτούν την **αμέλεια**, την **άγνοια** ή την **καλοσύνη** μας, προκειμένου να αποσπάσουν πληροφορίες.


Phishing - Ηλεκτρονικό "ψάρεμα" μέσω email


Smishing - Ηλεκτρονικό "ψάρεμα" μέσω SMS



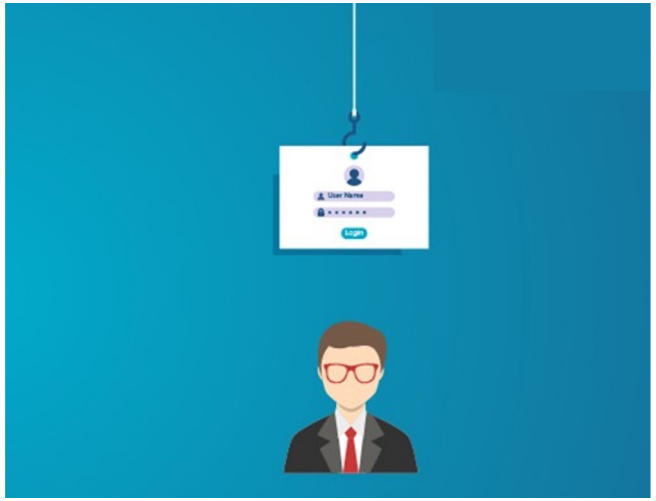
Vishing - "Ψάρεμα" μέσω τηλεφωνικής κλήσης


Pretexting - Χρήση Αληθοφανούς Σεναρίου


Baiting – Χρήση Δολωμάτων


Tailgating - Φυσική Παρουσία

Είδη Phishing

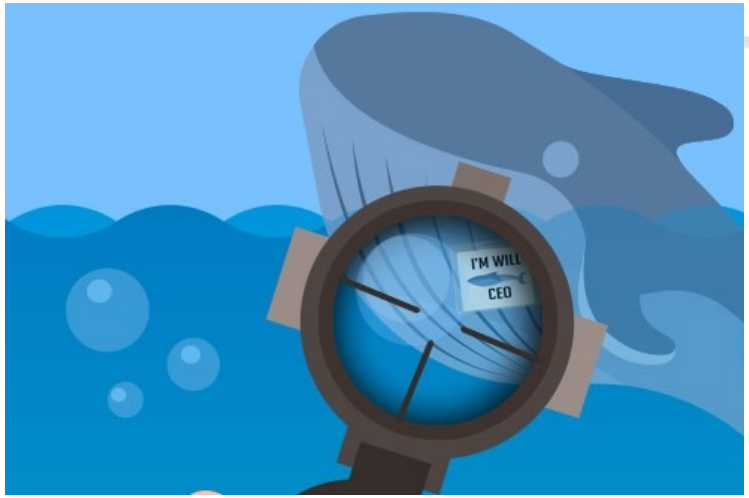


Spear Phishing

Συγκεκριμένο άτομο
(ή ομάδα ατόμων)

Mass Phishing

Δεν υπάρχουν συγκεκριμένοι στόχοι και η τεχνική αποστέλλεται συνήθως σε μυριάδες ανθρώπους.



Whaling

Υψηλόβαθμα Στελέχη, όπως CEO, CFO κοκ.

Προσοχή στα email που λαμβάνουμε!

Ενδείξεις Παραπλανητικού (fake) email

Γενικός χαιρετισμός

Θέμα επιτακτικό, επείγον, υβριστικό

Απουσία θέματος, υπογραφής, πληροφορίας επικοινωνίας

Ορθογραφικά ή Συντακτικά Λάθη

Ζητούνται προσωπικές ή εσωτερικές εταιρικές πληροφορίες

Περίεργη Διεύθυνση Αποστολέα

Περιλαμβάνει περίεργα links και attachments

Η πιστωτική σας κάρτα έχει αποκλειστεί προσωρινά!

Εθνική Τράπεζα <ewd32qwd@t-online.de>
Προς: Individuals@i-bnk.gr

ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ

Αγαπητέ πελάτη,

Αυτή είναι μια τρίτη ειδοποίηση, η ΕΤΕ 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 Eemail

Τις καλύτερες ευχές,
Εθνική Τράπεζα της Ελλάδος

Η πρόσβασή σας δεν είναι ενεργή!

Yahoo/Ενοχλητι...

EuroBank-GR <accounts@icoms.co>
Προς:

Παρ, 26 Φεβ στις 1:57 μ.μ.

Για την ασφάλειά σας, έχουμε απενεργοποιήσει τους συνδέσμους σε αυτό το e-mail. Αν πιστεύετε ότι η χρήση τους είναι ασφαλής, επισημάνετε αυτό το μήνυμα ως μη ανεπιθύμητη αλληλογραφία.

Eurobank

Αγαπητέ πελάτη

Έχουμε τοποθετήσει προσωρινά κλειδαριά στην κάρτα σας!

Οι διαδικτυακές πληρωμές και αναλήψεις μετρητών δεν μπορούν να γίνουν έως ότου επιλυθεί αυτό το ζήτημα.
Επιβεβαιώστε την πρόσβασή σας εντός των επόμενων 48 ωρών.

Ενεργοποίηση τώρα

Απαντήστε σε αυτό το e-mail εάν έχετε περαιτέρω απορίες ή θέλετε να επικοινωνήσετε μαζί μας.

Από: ALPHA BANK [customerserviceweb@alpha.gr]
Προς: info@moneyonline.gr
Κοιν.:
Θέμα: ALERT

ALPHA BANK

Αγαπητε πελατη,

Εχετε λαβει ενα νεο κοινοποιηση

Κανε κλικ εδω για να διαβασετε.

Copyright © 2016 Alpha Bank. All rights reserved.

winbank

Έχετε κινήσει τη διαδικασία πληρωμής του ποσού των 600,00 ευρώ σε υπηρεσία Λεφτά στο Λεπτό

* Λεπτομέρειες πληρωμής *

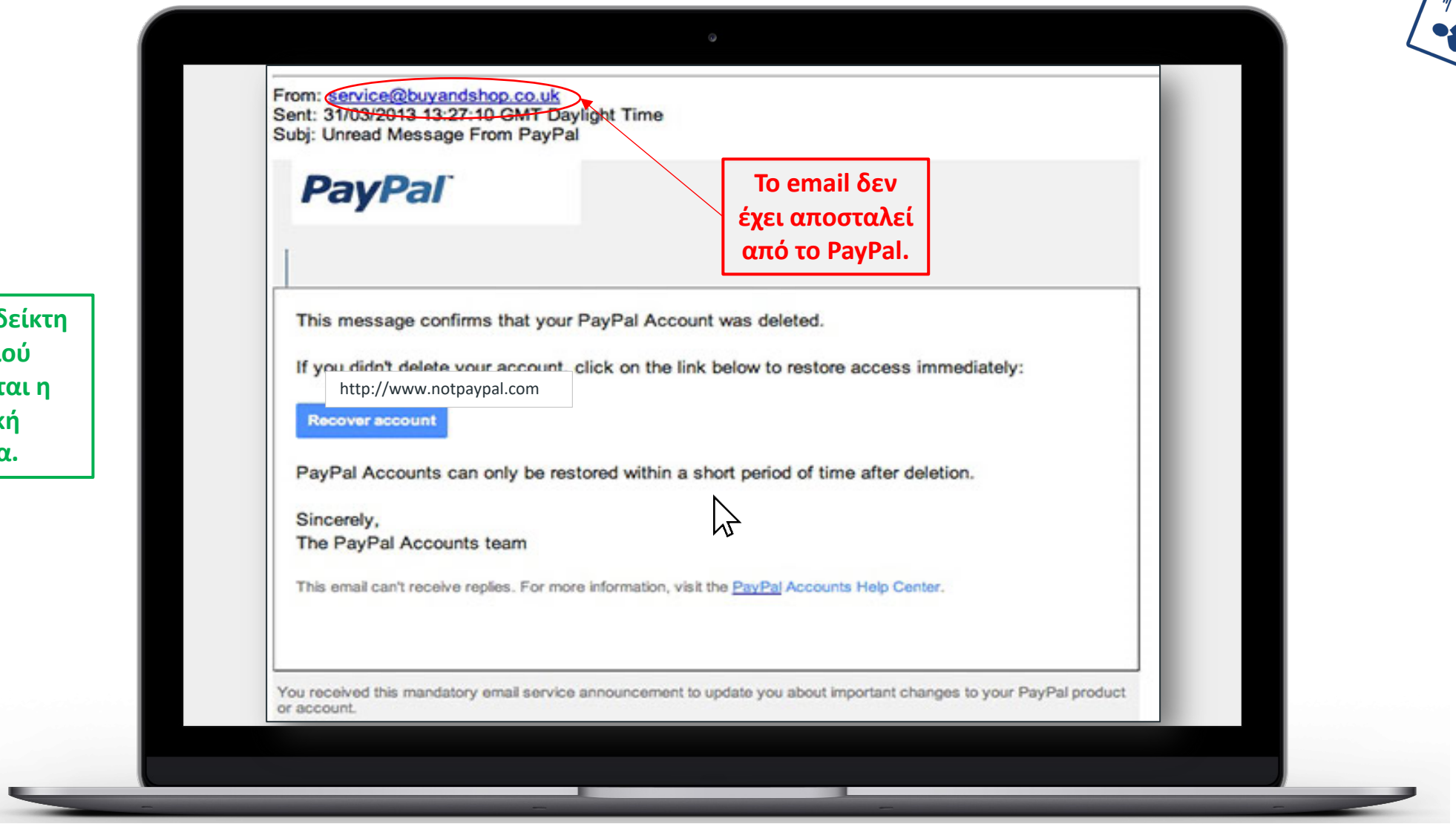
Ποσό: 600.00 EUR
ID της συναλλαγής: 5C53687F7327933R

Γι 'αυτό η πληρωμή γίνεται από μια εξωτερική διεύθυνση IP, έβαλα τη συναλλαγή ID 5C53687F7327933R εκκρεμότητα.

Για να ακυρώσετε την πληρωμή αυτή, παρακαλώ ακολουθήστε τον παρακάτω σύνδεσμο:

https://www.winbank.gr/el/Pages4985/Home.aspx

Παράδειγμα Παραπλανητικού email

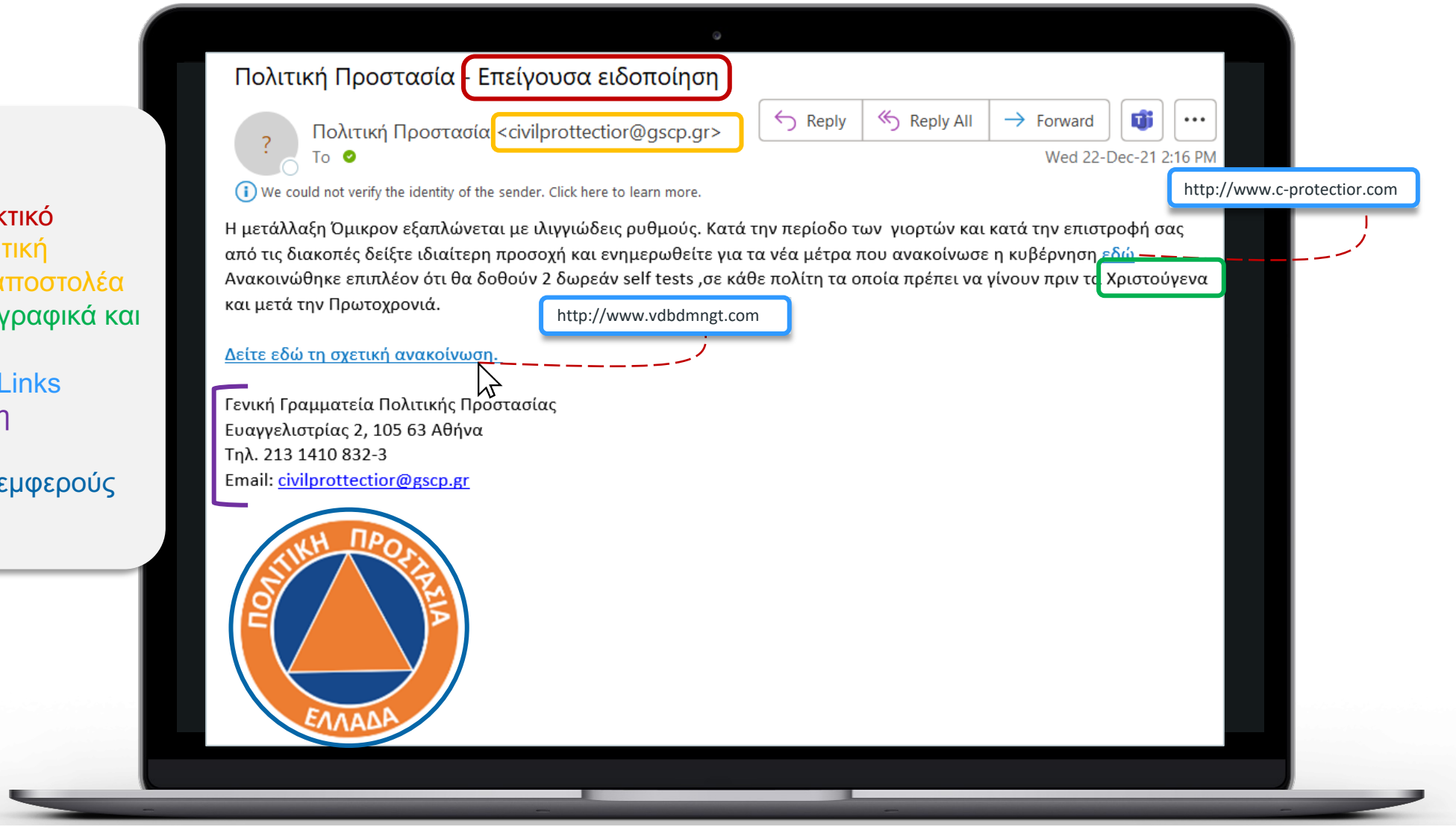


Βάζοντας τον δείκτη του ποντικιού αποκαλύπτεται η πραγματική ιστοσελίδα.

Ποιες ενδείξεις υποδεικνύουν τη μη εγκυρότητα του email;

Ενδείξεις

1. Θέμα επιτακτικό
2. Παραπλανητική διεύθυνση αποστολέα
3. Λάθη Ορθογραφικά και συντακτικά
4. Μη έγκυρα Links
5. Λανθασμένη Υπογραφή
6. Χρήση παρεμφερούς λογοτύπου.



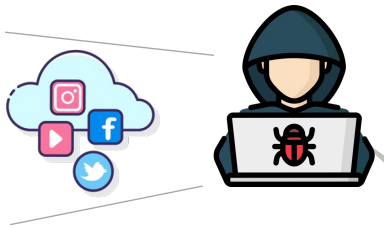
Smishing Attack Timeline

7. Unauthorized Transactions

Hacker's New Mobile

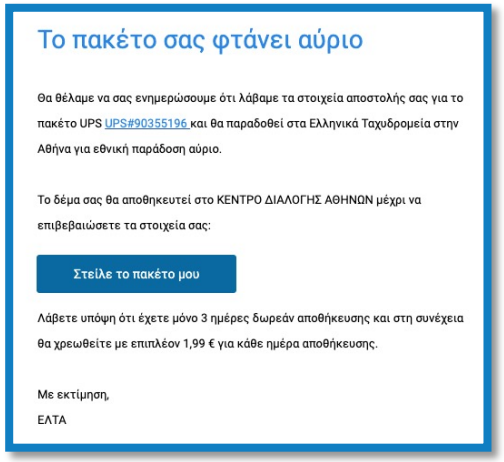
3. New Bank Wallet Installation Request

6. Permit Bank Wallet Installation in new Mobile



0. Data Collection

Fake e-banking site



2. Steal Credentials

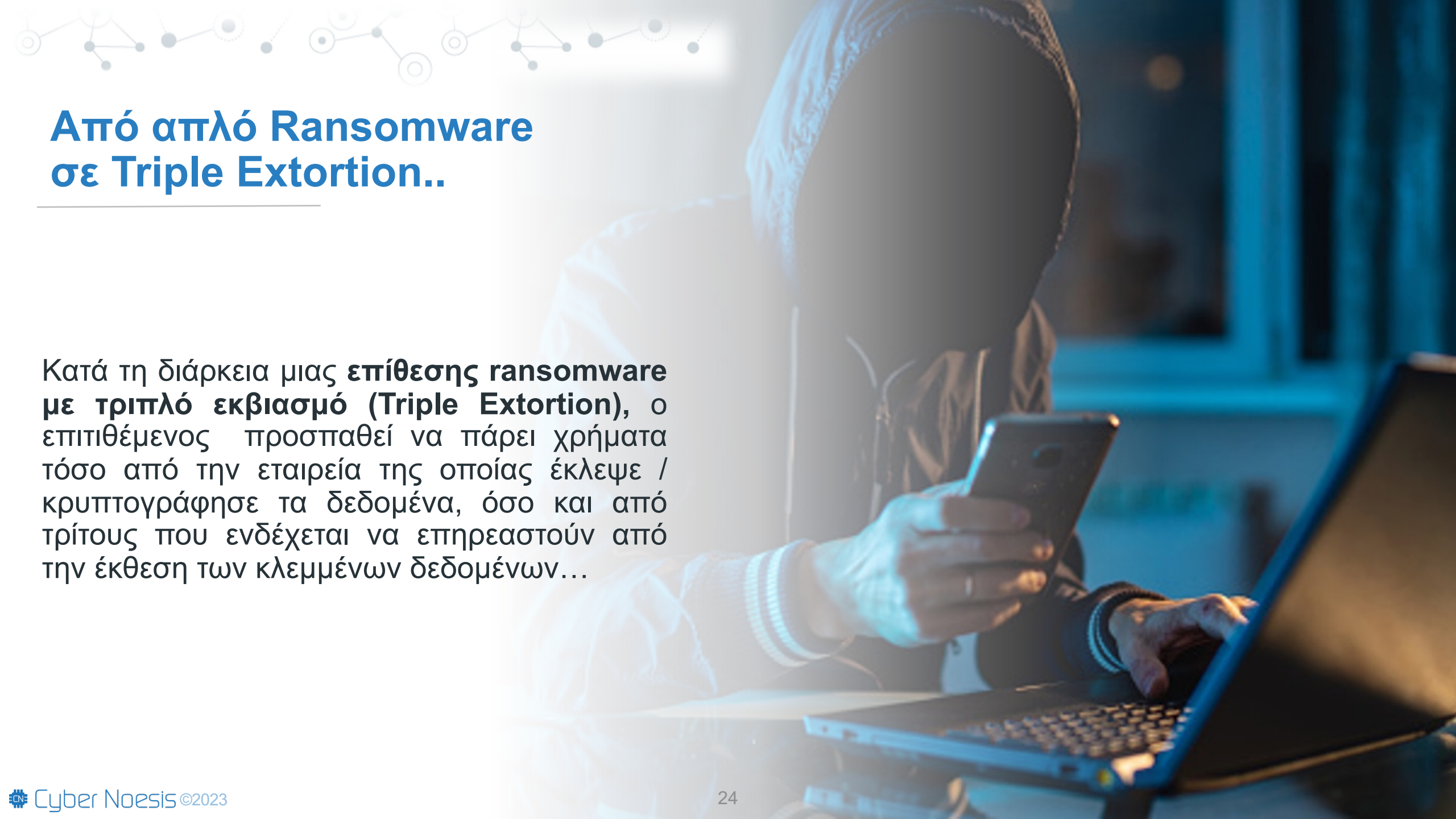
4. New Bank Wallet Authorization Request

1. Contact & Temptation

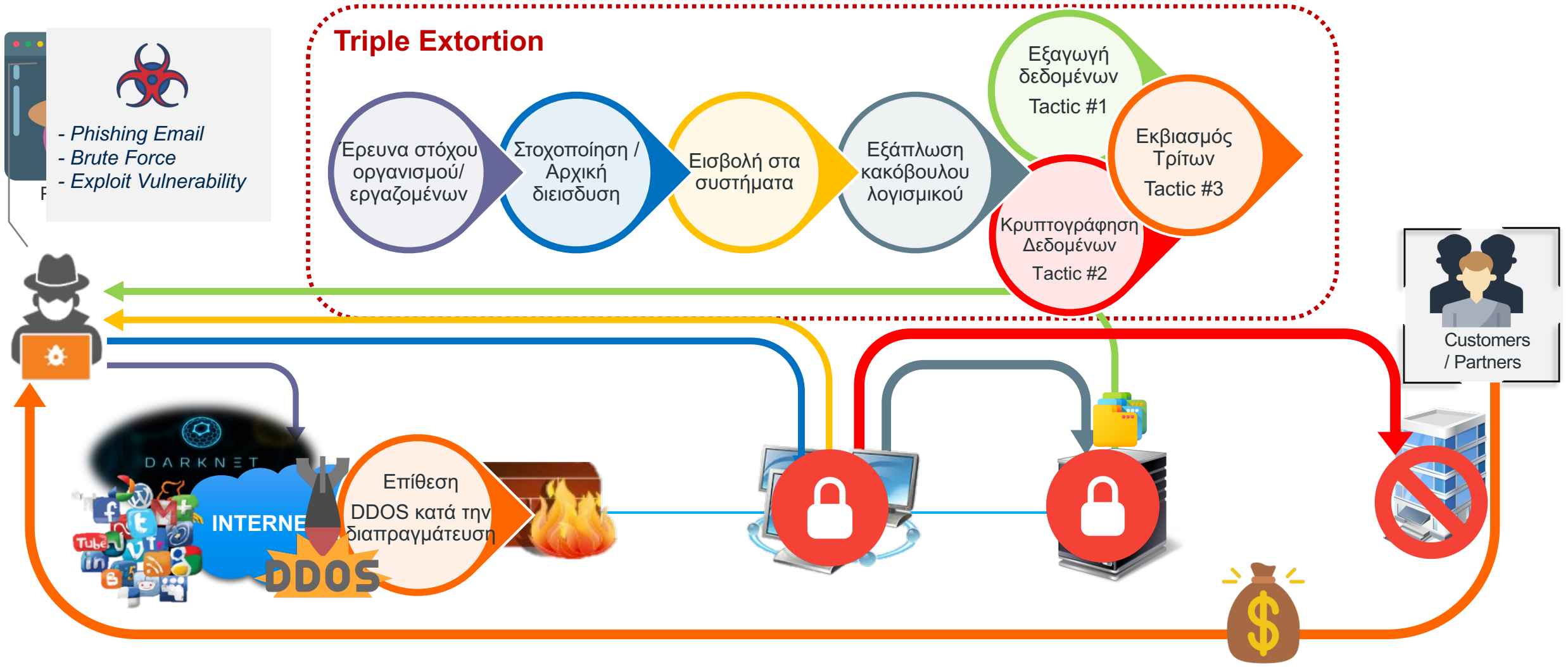
5. Unintentional New Bank Wallet Installation Authorization

Από απλό Ransomware σε Triple Extortion..

Κατά τη διάρκεια μιας **επίθεσης ransomware με τριπλό εκβιασμό (Triple Extortion),** ο επιτιθέμενος προσπαθεί να πάρει χρήματα τόσο από την εταιρεία της οποίας έκλεψε / κρυπτογράφησε τα δεδομένα, όσο και από τρίτους που ενδέχεται να επηρεαστούν από την έκθεση των κλεμμένων δεδομένων…



Triple Extortion…



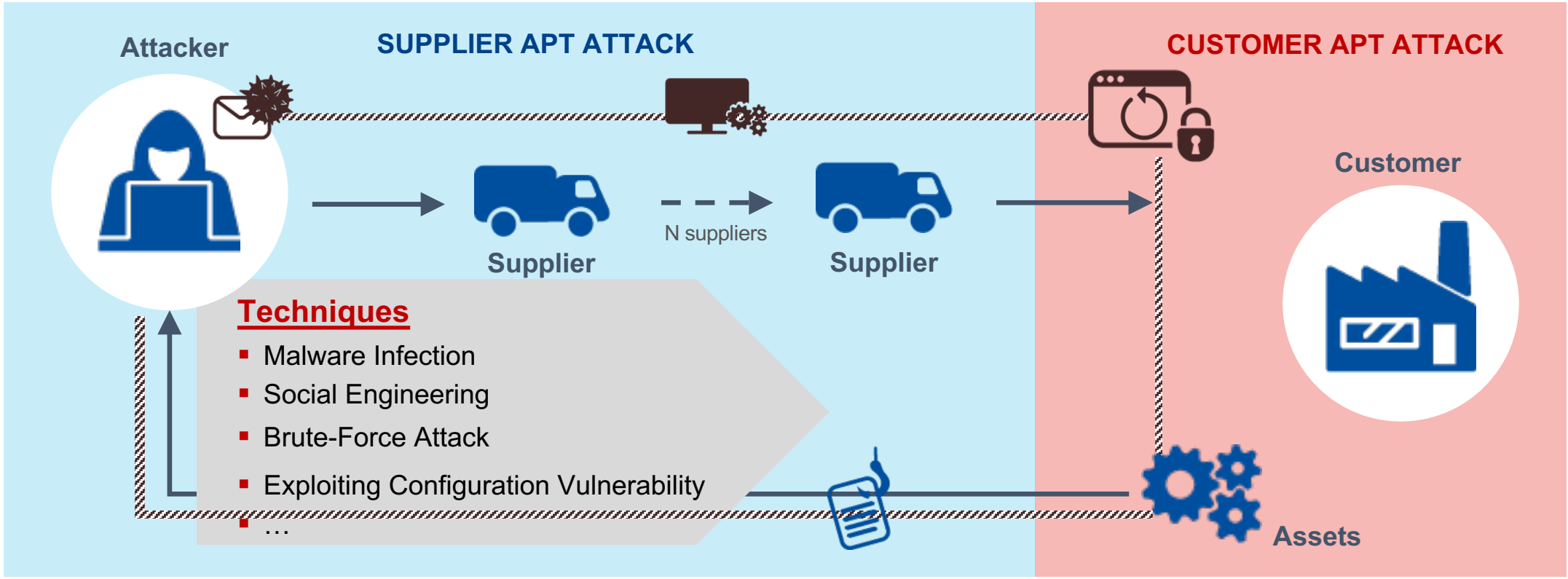
Supply Chain Attacks

> Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.
>
> NIST

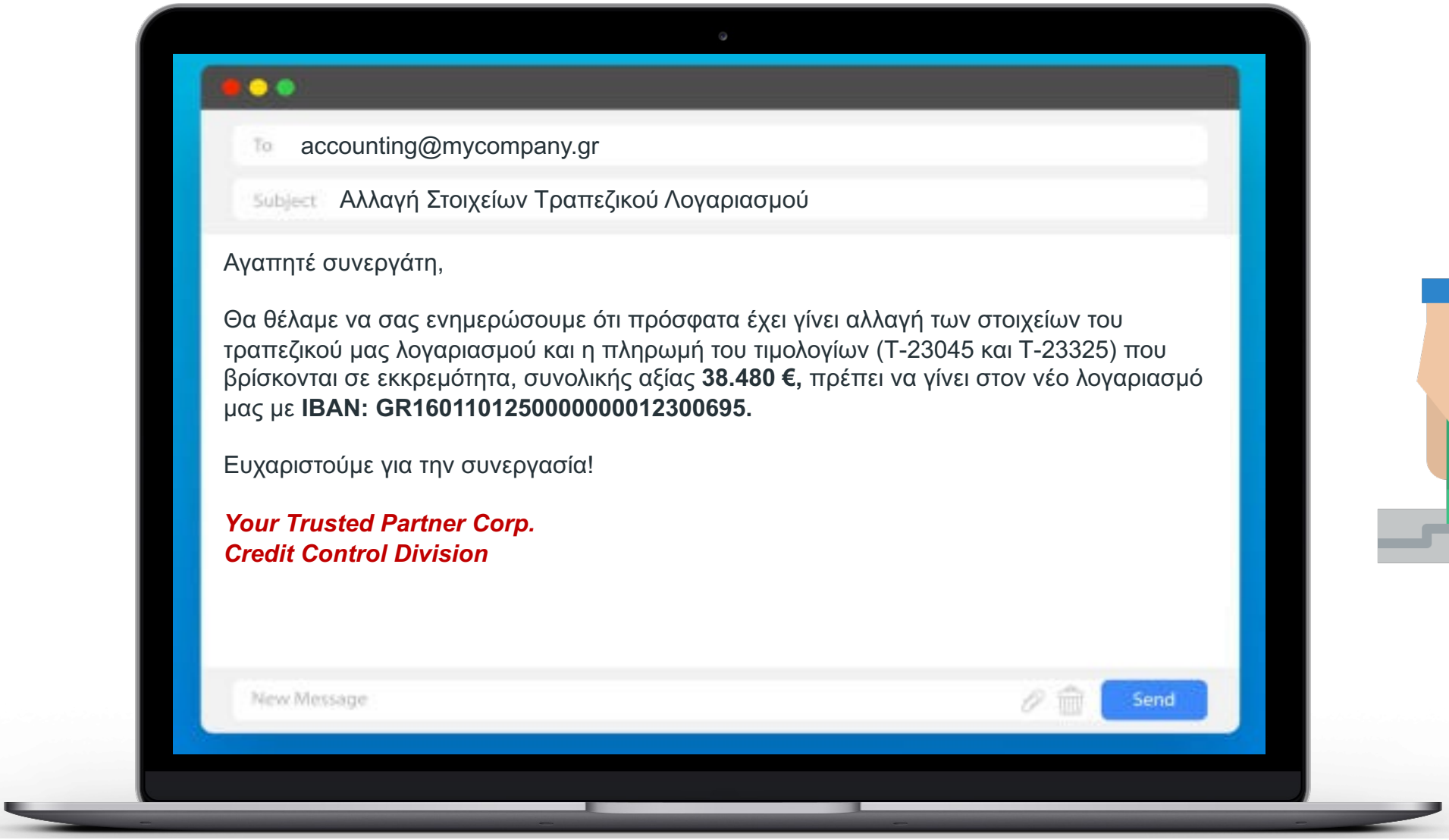
Οι επιτιθέμενοι εκμεταλλεύονται το κανάλι προμηθευτή-πελάτη – διευρύνοντας έτσι την επιφάνεια επίθεσης (attack surface) του θύματος.

Software supply chains – εξαρτήσεις πάνω σε λογισμικό.

Supply Chain Attacks



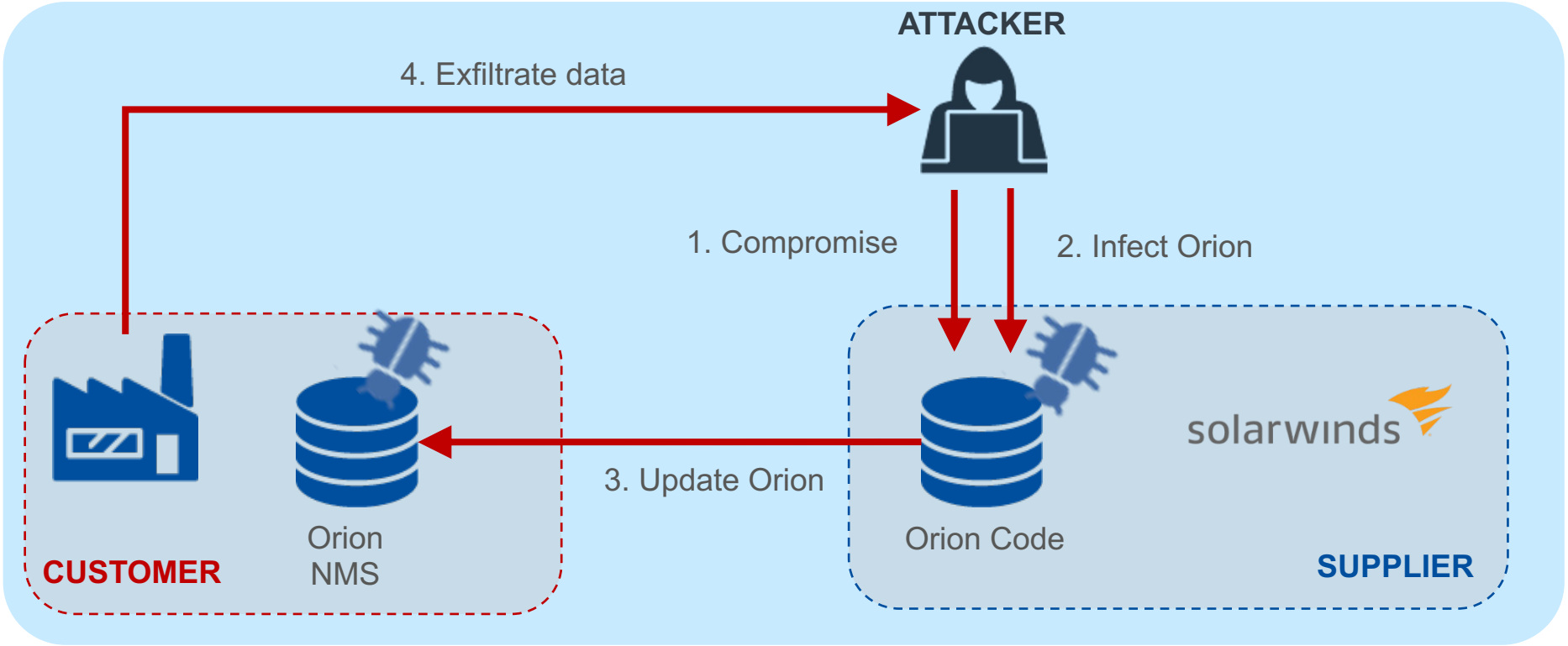
Business email Compromise (BEC) attacks



Malware Inflection Attacks

December 2020

SolarWinds Orion – December 2020

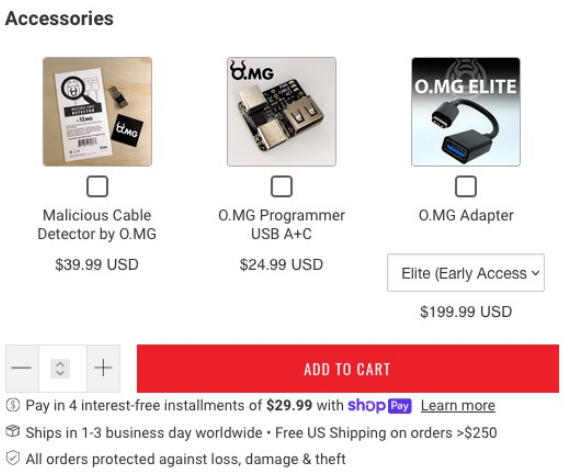



Expect the
Unexpected

O.MG Cable

The O.MG Cable is a hand made USB cable with an advanced implant hidden inside. It is designed to allow your Red Team to emulate attack scenarios of sophisticated adversaries. Until now, a cable like this would cost $20,000 (ex: COTTONMOUTH-I). These cables will allow you to test new detection opportunities for your de

shop.hak5.org



- *Easy Wifi controls Control everything remotely with a web browser.*
- *1 click payload deploy.*
- *Built in IDE helps guide you.*

Μην πείτε ποτέ "Δεν θα συμβεί σε μένα"

Συνειδητοποιήστε ότι είστε ένας ελκυστικός στόχος για τους χάκερς.

Cyber Security Tips για τον απλό χρήστη…

Διατηρήστε το λογισμικό σας ενημερωμένο.

Χρησιμοποιήστε antivirus σε όλες τις συσκευές σας.

Μην συνδέεστε σε μη έμπιστα και ανοιχτά δίκτυα Wi-Fi.

Χρησιμοποιήστε ένα ισχυρό μείγμα χαρακτήρων.

Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για πολλούς ιστότοπους.

Μην αφήνετε τις συσκευές σας εκτεθειμένες.

Να είστε πάντα προσεκτικοί όταν κάνετε κλικ σε συνημμένα ή συνδέσμους στο ηλεκτρονικό ταχυδρομείο.

Δημιουργήστε αντίγραφα ασφαλείας των δεδομένων σας τακτικά.

Να είστε ιδιαίτερα προσεκτικοί με οποιαδήποτε συσκευή συνδέετε στον υπολογιστή σας.

Να είστε προσεκτικοί με τα μέσα κοινωνικής δικτύωσης (social media).

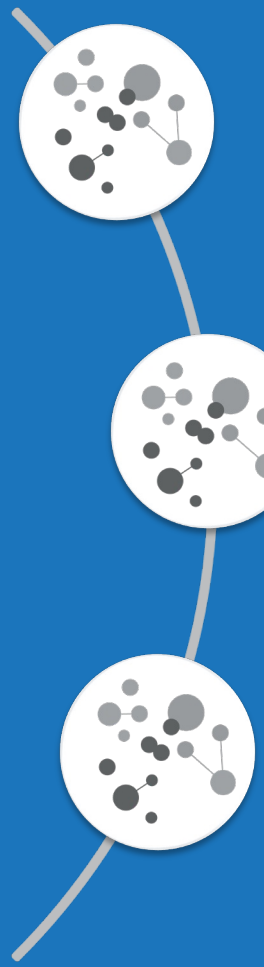
Να είστε πολύ προσεκτικοί όταν κάποιος προσπαθεί να αποκτήσει ευαίσθητες πληροφορίες από εσάς μέσω της χειραγώγησης.

Τι Πρέπει Να Κάνω Αν Πέσω Θύμα Ηλεκτρονικής Απάτης

Θα πρέπει να καταγγείλετε το περιστατικό απάτης:

- στο πλησιέστερο σε εσάς αστυνομικό τμήμα ή
- στη **Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙΔΗΕ)** της Ελληνικής Αστυνομίας
  - Τηλέφωνο : 11188
  - Email: ccu@cybercrimeunit.gov.gr
  - μέσω του portal στη διεύθυνση: https://goo.gl/vOHdVb (https://www.gov.gr/org/astynomia/kataggelies)
  - Fax: 213-1527471
  - Ταχυδρομική διεύθυνση: Λ. Αλεξάνδρας 173, Τ.Κ. 11522, Αθήνα

Περιεχόμενα



Σύγχρονες Απειλές &
Πραγματικά Περιστατικά

Τεχνικές Επιθέσεων & Πρακτικές
Αντιμετώπισης

Cyber Security Quick Wins

- Πως να προστατεύσω την επιχείρηση &
  τους εργαζομένους από Κυβερνοεπιθέσεις.

Υφιστάμενο Κανονιστικό Πλαίσιο

NIS2 (Network and Information Systems)

GDPR (General Data Protection Regulation)

DORA (Digital Operational Resilience Act)

Cyber Security Tips για Μικρομεσαίες Επιχειρήσεις

Βασικοί τομείς της κυβερνοασφάλειας για τις μικρομεσαίες επιχειρήσεις

https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Cyber Security for SMEs

People

Αρμοδιότητα	Πρέπει να οριστούν ρόλοι και αρμοδιότητες σχετικά με την ασφάλεια πληροφοριών.
Προσλήψεις Εργαζομένων	Το σύνολο του προσωπικού γραπτή πρέπει να έχει διαβάσει, κατανοήσει και αποδεχτεί την πολιτική ασφάλειας πληροφοριών.
Ευαισθητοποίηση Εργαζομένων	Όλοι οι χρήστες των συστήματα πρέπει να λαμβάνουν τακτική εκπαίδευση σχετικά με τις ευθύνες ασφαλείας, καθώς και τον τρόπο αναγνώρισης και αντιμετώπισης ποικίλων απειλών ασφάλειας. Πρέπει να επιβεβαιώνεται ότι όλο το προσωπικό γνωρίζει και έχει πρόσβαση στα σημεία επαφής και τα κανάλια επικοινωνίας για τα θέματα ασφάλειας πληροφοριών.
Εκπαίδευση Cybersecurity	Τα μέλη του προσωπικού με συγκεκριμένες ευθύνες ασφάλειας πρέπει να λαμβάνουν κατάλληλη και τακτική εκπαίδευση για να υποστηρίξουν τον ρόλο τους.
Πολιτικές Cybersecurity	Η πολιτική ασφαλείας, με τις σχετικές διαδικασίες λειτουργίας, πρέπει να προβάλλεται και να υποστηρίζεται από τα ανώτερα στελέχη της διοίκησης.
Διαχείριση Τρίτων μελών	Η πρόσβαση τρίτων σε εμπιστευτικές και/ή ευαίσθητες πληροφορίες πρέπει να εξουσιοδοτείται από την ανώτερη διοίκηση, και εφόσον έχουν υπογραφεί τα κατάλληλα έντυπα εμπιστευτικότητας.

Cyber Security for SMEs

Process

Έλεγχοι	Τα κρίσιμα συστήματα, όπως Firewalls και δρομολογητές (Routers) πρέπει να ελέγχονται τακτικά για τρωτά σημεία. Οι υπολογιστές πρέπει να ελέγχονται για αντίγραφα παράνομου λογισμικού.
Σχεδιασμός και αντιμετώπιση περιστατικών	Πρέπει να υπάρχουν τεκμηριωμένα (και να δοκιμάζονται τακτικά) Πλάνα Αντιμετώπισης Περιστατικών Ασφάλειας, με σαφώς καθορισμένους ρόλους και ευθύνες, ώστε να διασφαλιστεί ότι η εταιρεία μπορεί να ανταποκριθεί σε τυχόν παραβιάσεις ασφάλειας, όπως επίθεση ιού, απάτη, φυσικές καταστροφές (πχ. Πυρκαγιά) κλπ.
Κωδικοί Πρόσβασης	Πρέπει να καθοριστεί και να εφαρμόζεται Ισχυρή Πολιτική Χρήσης Κωδικών Πρόσβασης (πχ. επαναφορά όλων των προεπιλεγμένων κωδικών πρόσβασης σε όλα τα συστήματα από τους προεπιλεγμένους κωδικούς πρόσβασης που έχει εγκαταστήσει ο προμηθευτής και χρήση σύνθετων κωδικών πρόσβασης)
Ενημερωμένες εκδόσεις λογισμικού	Πρέπει να υπάρχει μηχανισμός που να διασφαλίζει ότι οι κρίσιμες ενημερώσεις ασφάλειας (security updates) εφαρμόζονται στα πληροφοριακά συστήματα εγκαίρως και ελεγχόμενα.
Προστασία Δεδομένων	Σε πληροφοριακά συστήματα και βάσεις δεδομένων που αποθηκεύουν Δεδομένα Προσωπικού Χαρακτήρα πρέπει να εφαρμόζονται κατάλληλα μέτρα προστασίας για τη διασφάλιση της συμμόρφωσης με ρυθμιστικές και νομικές απαιτήσεις όπως ο GDPR της ΕΕ.

Cyber Security for SMEs

Technology

Ασφάλεια Δικτύου	Οι εξωτερικές συνδέσεις, πχ στο Διαδίκτυο, πρέπει να είναι εξουσιοδοτημένες από τα ανώτερα στελέχη και να είναι κατάλληλα προστατευμένες (πχ με χρήση firewall).
Anti-Virus	Σ' όλα τα συστήματα υπολογιστών πρέπει να έχει εγκατασταθεί και να είναι «ενημερωμένο» λογισμικό προστασίας από ιούς. Οι χρήστες πρέπει να εκπαιδευτούν σχετικά με τον τρόπο αναγνώρισης και αντιμετώπισης ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή αρχείων που ενδέχεται να περιέχουν ιούς υπολογιστών.
Κρυπτογράφηση	Όλες οι συσκευές που αποθηκεύουν δεδομένα πρέπει να έχουν πλήρη κρυπτογράφηση δίσκου. Πρέπει να γίνεται χρήση εικονικών ιδιωτικών δικτύων (VPNs) κατά τη σύνδεση μέσω μη έμπιστων δικτύων (πχ. Internet).
Παρακολούθηση Ασφάλειας	Πρέπει να γίνεται παρακολούθηση των αρχείων καταγραφής (log files) όλων των κρίσιμων συστημάτων ασφαλείας για τον έγκαιρο εντοπισμό πιθανών παραβιάσεων ασφάλειας.
Φυσική Ασφάλεια	Όλοι οι κρίσιμοι πόροι πληροφορικής, όπως file servers, πρέπει να βρίσκονται σε ασφαλή περιοχή που προστατεύεται από μη εξουσιοδοτημένη πρόσβαση. Στην εξ΄ αποστάσεως εργασία (home office), πρέπει να εφαρμόζονται κατάλληλα μέτρα φυσικής προστασίας
Αντίγραφα Ασφάλειας	Πρέπει να λαμβάνονται τακτικά αντίγραφα ασφάλειας των κρίσιμων δεδομένων και συστημάτων. Πρέπει να εκπονείται τακτικά δοκιμή επαναφοράς αντιγράφων ασφάλειας, προκειμένου να επαληθευτεί η πλήρης ανάκτηση δεδομένων και συστημάτων.

Cyber Noesis

Lack of knowledge is not the users' fault!

Ευχαριστούμε για την προσοχή σας!

Cyber Noesis

We position...
CYBER SECURITY FIRST!

www.cybernoesis.com