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

08/11/2023

Περιεχόμενα

Σύγχρονες Απειλές & Πραγματικά Περιστατικά

Επιθέσεις και Πρακτικές Αντιμετώπισης

Cyber Security Quick Wins

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

WEF: Global Risks …

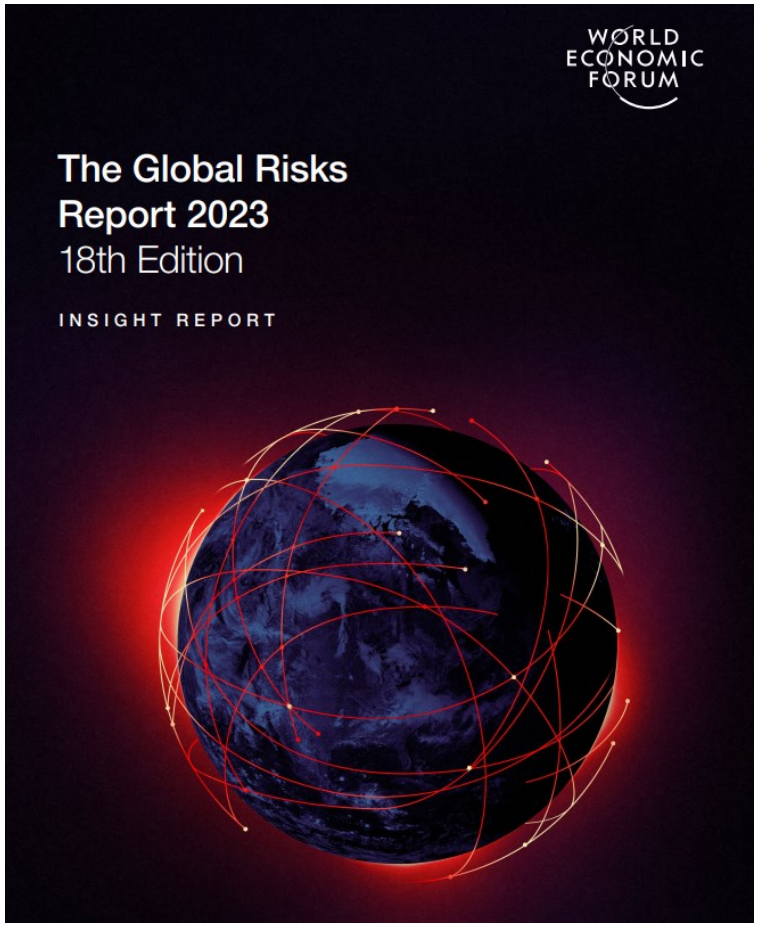


FIGURE 1.1 **Currently manifesting risks**

"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"

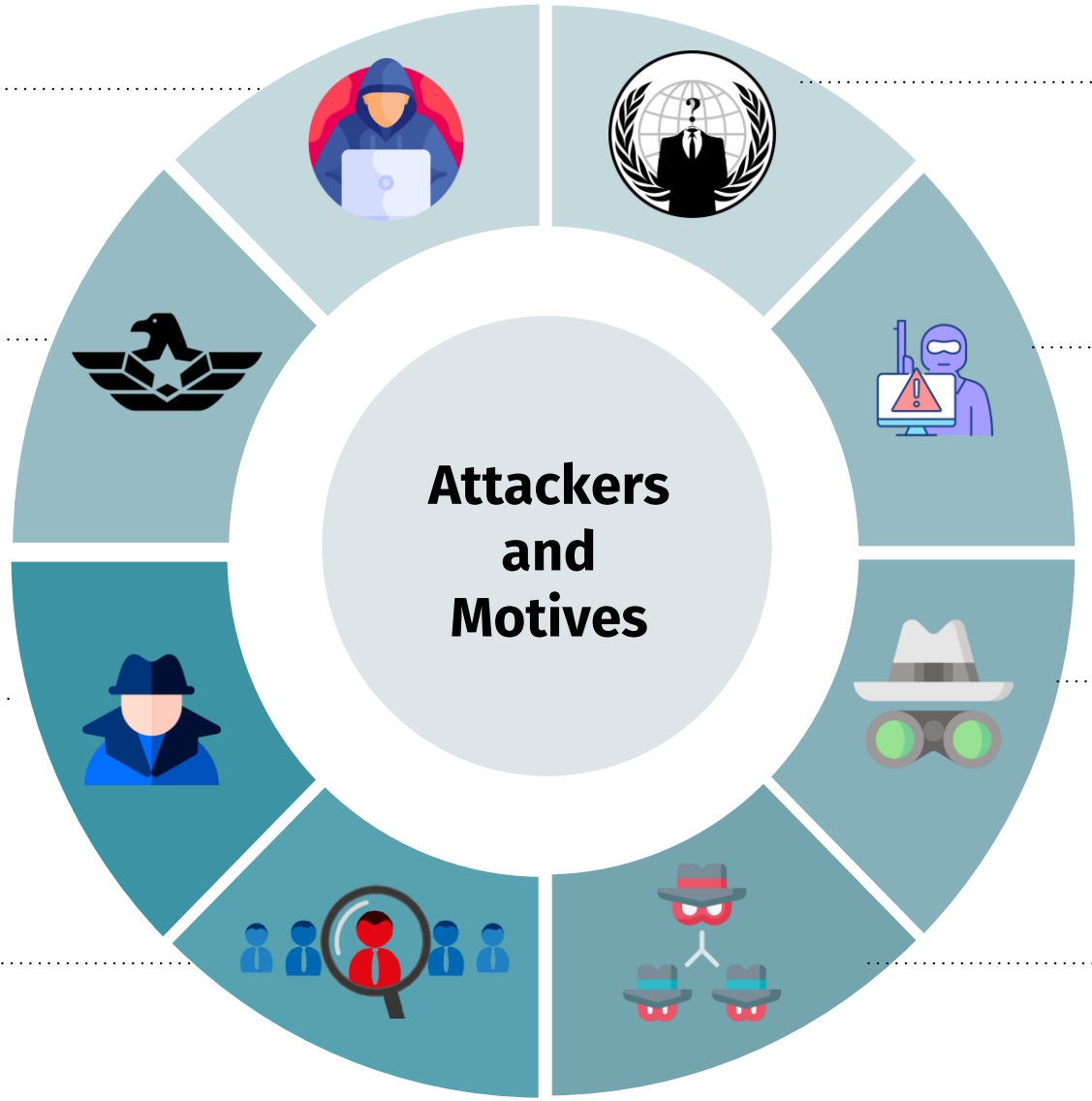
Τύποι & Κίνητρα Επιτιθέμενων

Script Kiddies
Satisfaction

Information Secret Services
Geopolicical

Government Teams – Homeland Security
Geopolicical

Malicious User
Discontent



Hackactivists
Ideological

Cyber Terorists
Idrreological
Violence

Corporate Espionage
Profit

Organised Cyber Crime
Profit

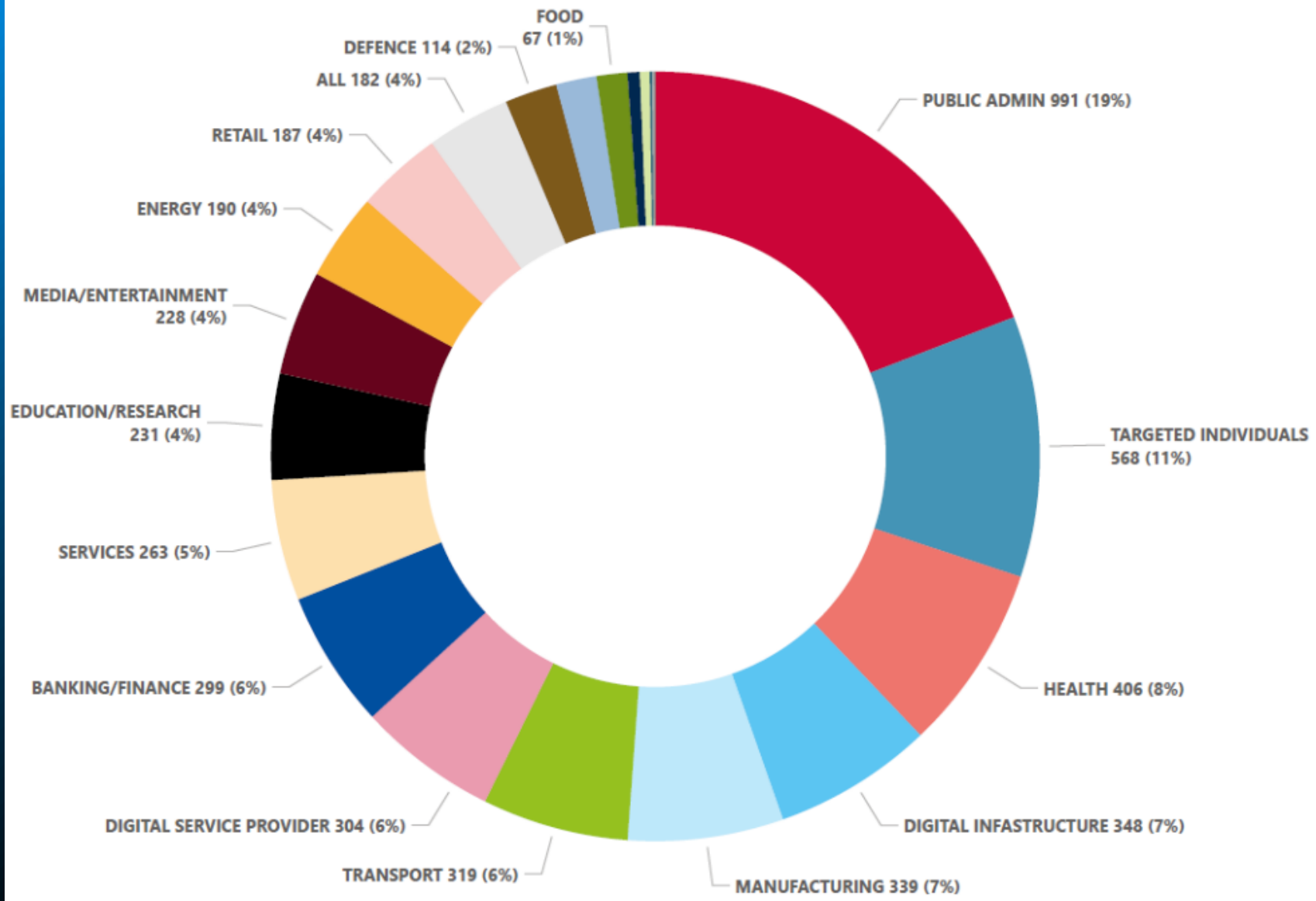
ENISA Threat Landscape 2023

ENISA Threat Landscape 2023

[Cybersecurity Threats Fast-Forward 2030]

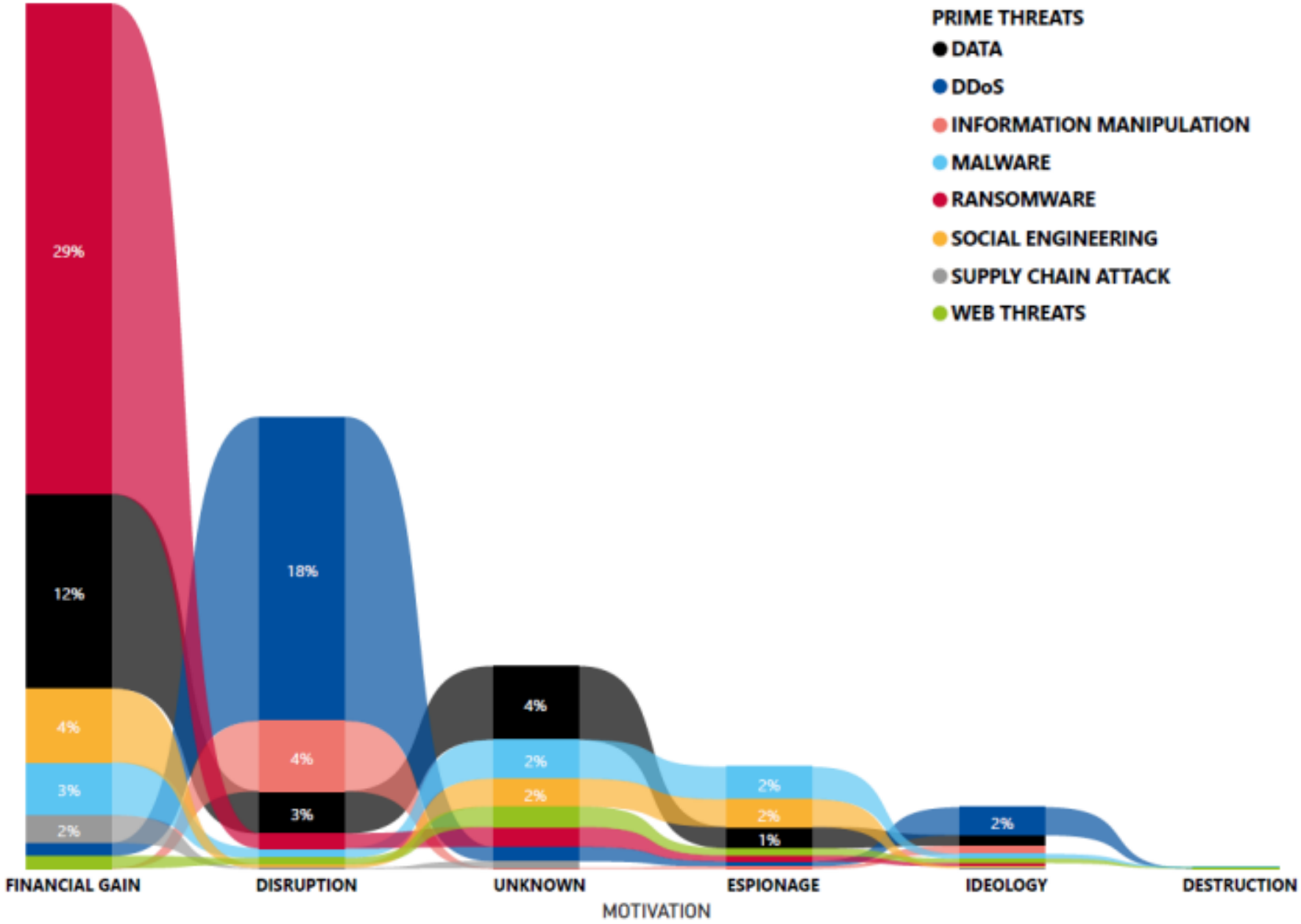
Targeted sectors per number of incidents

(July 2022 - June 2023)



Motivation of threat actors per threat category

(July 2022 - June 2023)



Πραγματικά Περιστατικά Κυβερνοεπιθέσεων

2023

IOTW: Ransomware gang steals 1.3TB of data from Sabre

Ransomware gang Dunghill Leak posted screenshots of the allegedly stolen data to its dark web site

Ransomware gang Dunghill Leak has claimed responsibility for a cyber attack against travel booking company Sabre.

Dunghill claimed in a post on its dark web **data leaks** site that it had stolen 1.3 terabytes of data from Sabre, including corporate financial information, passenger turnover and ticket sales data and personal employee information.

MGM Resorts Computers Back Up After 10 Days as Analysts Eye Effects of Casino Cyberattacks

MGM Resorts brought its computer systems back online on September 20th after ransomware disrupted operations for 10 days.

MGM Resorts brought to an end a 10-day computer shutdown prompted by efforts to shield from a cyberattack data including hotel reservations and credit card processing, the casino giant said Wednesday, as analysts and academics measured the effects of the event.

IOTW: Microsoft SAS misconfiguration causes 38TB data leak

The leak was caused by an "overly-permissive" SAS token being included in a storage URL

Technology company Microsoft has revealed that it suffered a data leak in July 2020 which exposed 38 terabytes of private employee data.

News of the leak was made public via a blog post on September 18. In it, Microsoft explained that the leak was caused by a software misconfiguration.

Ransomware gang steals 6.8TB of data from Save The Children

The charity has had financial, medical and health data stolen in the cyber attack

Ransomware gang BianLian has claimed responsibility for a cyber attack against nonprofit Save The Children International.

The ransomware gang has been active since June 2022, and primarily targets critical infrastructure and healthcare organizations. In previous attacks, BianLian has extorted these organziations for their data.

X-based NFT phishing attack causes losses of over $691,000

Malicious actors targeted Ethereum co-founder, Vitalik Buterin, to spread the phishing attack

Add bookmark

A phishing attack has led to the loss of over US$691,000 following the compromise of the X (formerly Twitter) account of co-founder of decentralized blockchain Ethereum and cryptocurrency Ether, Vitalik Buterin.

The hack was discovered on September 9, following suspicious activity on Buterin's X account. After compromising Buterin's account,

Περιστατικά Ασφάλειας στην Ελλάδα 1/2

Κυβερνοεπίθεση στον ΔΕΣΦΑ: Στο dark web έβγαλαν κρίσιμα αρχεία οι εκβιαστές χάκερ

Δεν έχουμε καμία επικοινωνία με τους χάκερ, λένε από τον ΔΕΣΦΑ, εκφράζοντας προβληματισμό για την πρωτοφανή υπόθεση εκβιασμού - Δείτε έγγραφα που ανήρτησαν - Άγνωστο το αντάλλαγμα που ζητούν οι χάκερ

Greetings!

For everyone who was waiting for the news - here they are!

Unfortunately DESFA company didn't pay any attention on the possible risk of data leakage.

So, as we promised today we are publishing the full Data which were downloaded from DESFA network.

We always keep our word and since management of this company didn't contact us or even made any public claims, it's clear for us that they doesn't care about information or network security.

We believe that everyone who treats this firm one way or another should hold them accountable and join the class actions against DESFA to make them take all the responsibility for such an issue.

They had all the chances to avoid leak and to fix the holes in security perimeter but the didn't.

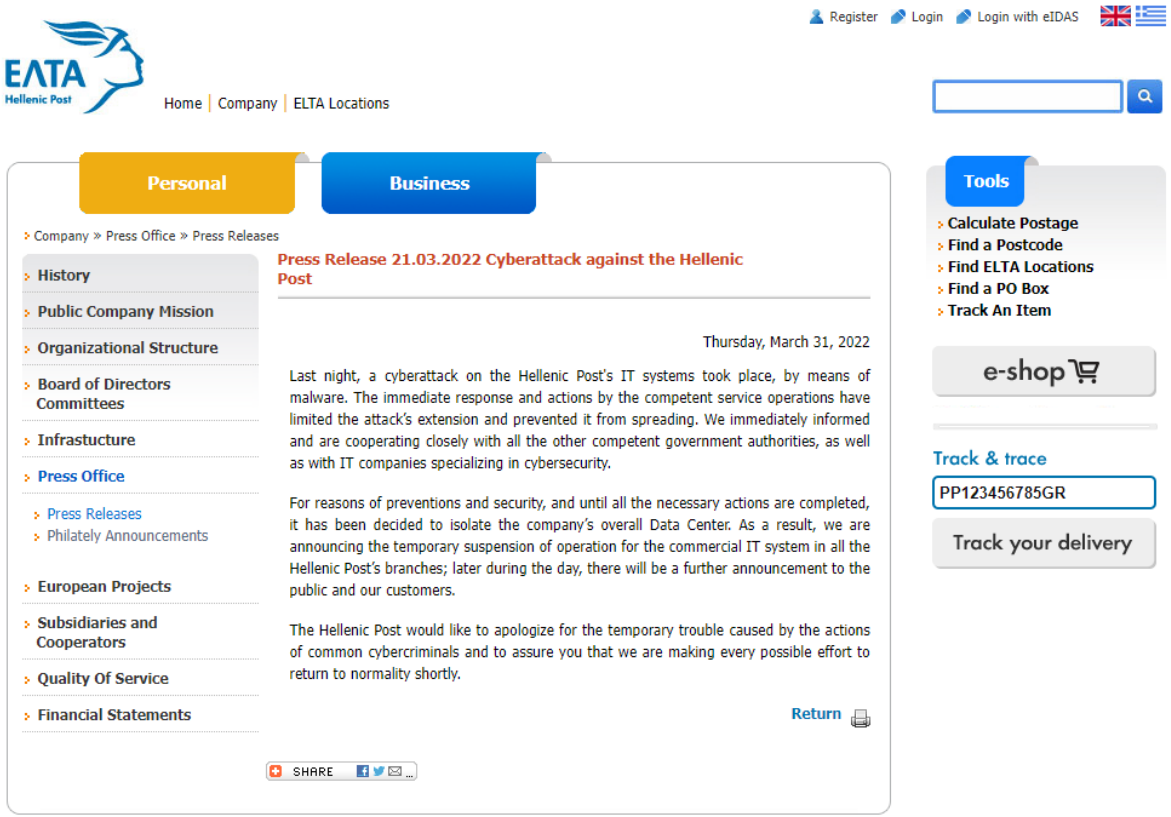
Well, according to our rules we can't keep silence about the negligence and irresponsibility when it comes to information privacy and network security.

> *As always, we are saying: Those organizations who collecting and storing private data, should be in charge of it's privacy.*

Below you can find the link with all the sensitive Data:

DOWNLOAD

Περιστατικά Ασφάλειας στην Ελλάδα 2/2



ΕΛΤΑ Hellenic Post

Register | Login | Login with eIDAS

Home | Company | ELTA Locations

Personal | Business

Company » Press Office » Press Releases

- History
- Public Company Mission
- Organizational Structure
- Board of Directors Committees
- Infrastucture
- Press Office
  - Press Releases
  - Philately Announcements
- European Projects
- Subsidiaries and Cooperators
- Quality Of Service
- Financial Statements

Press Release 21.03.2022 Cyberattack against the Hellenic Post

Thursday, March 31, 2022

Last night, a cyberattack on the Hellenic Post's IT systems took place, by means of malware. The immediate response and actions by the competent service operations have limited the attack's extension and prevented it from spreading. We immediately informed and are cooperating closely with all the other competent government authorities, as well as with IT companies specializing in cybersecurity.

For reasons of preventions and security, and until all the necessary actions are completed, it has been decided to isolate the company's overall Data Center. As a result, we are announcing the temporary suspension of operation for the commercial IT system in all the Hellenic Post's branches; later during the day, there will be a further announcement to the public and our customers.

The Hellenic Post would like to apologize for the temporary trouble caused by the actions of common cybercriminals and to assure you that we are making every possible effort to return to normality shortly.

Return

SHARE

Tools

- Calculate Postage
- Find a Postcode
- Find ELTA Locations
- Find a PO Box
- Track An Item

e-shop

Track & trace

PP123456785GR

Track your delivery

ANNOUNCEMENT-Tuesday, March 22nd, 2022

Tuesday, March 22, 2022

As part of providing the public and its customers with continuous and responsible information, the Hellenic Post hereby announces that the competent IT services, in cooperation with the expert partners in IT Security, are working 24/7 to fully restore the IT systems and to resume the secure network operation.

It has been determined that the targeted cyberattack that was aiming at coding the crucial systems for the Hellenic Post's business operation started from a zero-day malware, which was installed on a work station and, using the https reverse shell technique, connected to an IT system controlled by a group of cybercriminals.

In order to resolve this technically difficult project, more than 2500 terminal systems are being examined for IT security reasons, while agents programs are also being installed. This aims at the immediate reoperation of the commercial IT system, the security of all the data and the faster restoration of operations in the Hellenic Post branches.

It is noted that, today, Tuesday, March 22nd, post and parcels will be delivered normally, but the Hellenic Post branches will not pay bills, send post or carry out financial services. However, all these services, except for the financial services, will be served normally by the Hellenic Post Courier, since this event is note related to its operation.

The Hellenic Post would like once more to ask for the pubic and its customers' understanding as regards any trouble they may suffer due to the targeted malicious attack by common cybercriminals, and it will provide responsible information on the progress in restoring the problem.

Return

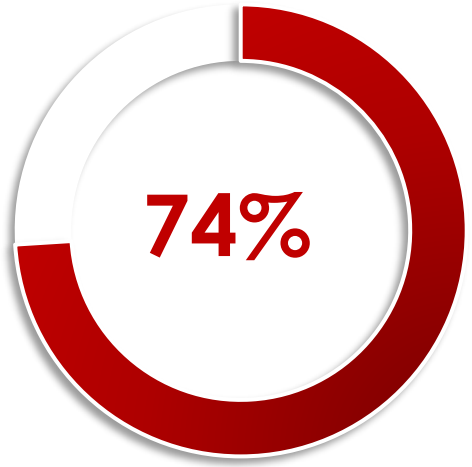
Περιεχόμενα

Σύγχρονες Απειλές &
Πραγματικά Περιστατικά

Επιθέσεις και Πρακτικές Αντιμετώπισης

Cyber Security Quick Wins

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



of Data Breaches
are due to **Human Element**

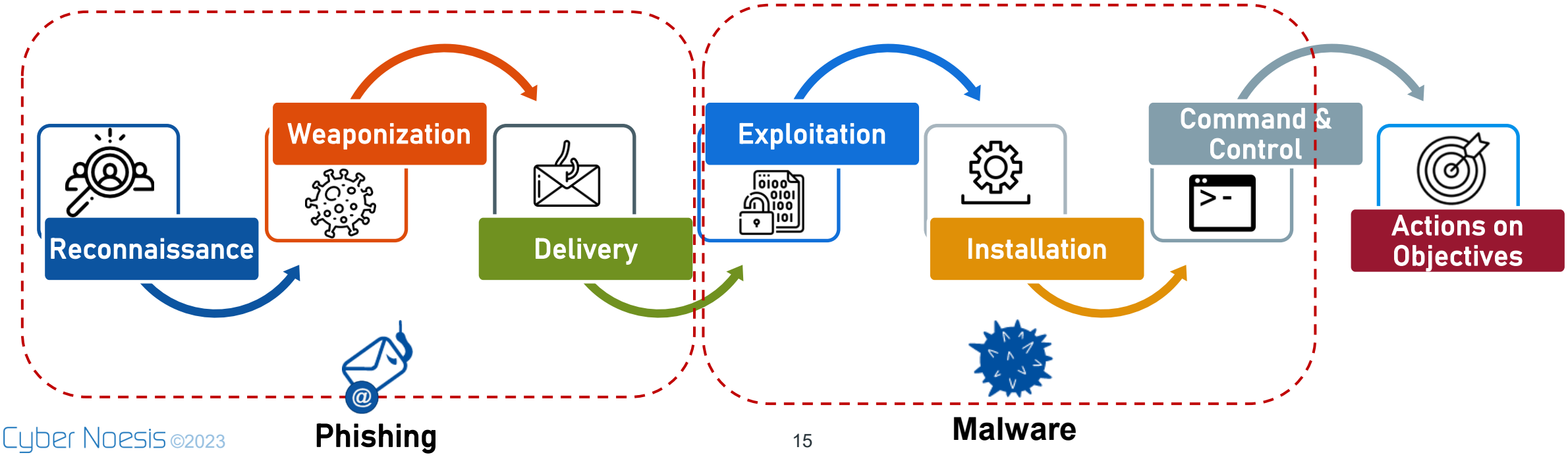
with people being involved
via Error, Privilege Misuse,
Use of stolen credentials or **Social Engineering.**

Verizon's 2023 Data Breaches Investigations Report

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.

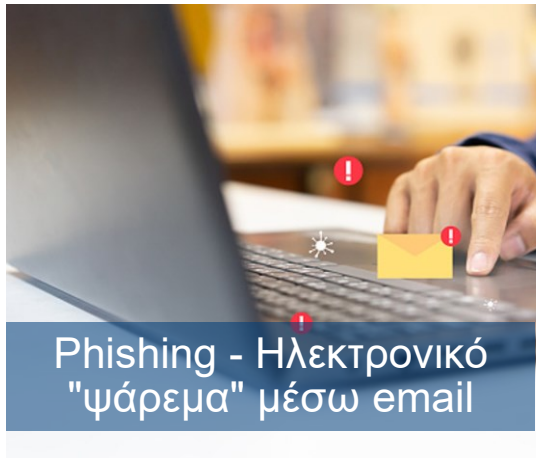
- Το μοντέλο αυτό προσδιορίζει τα στάδια που ολοκληρώνουν οι επιτιθέμενοι για να επιτύχουν τον στόχο τους

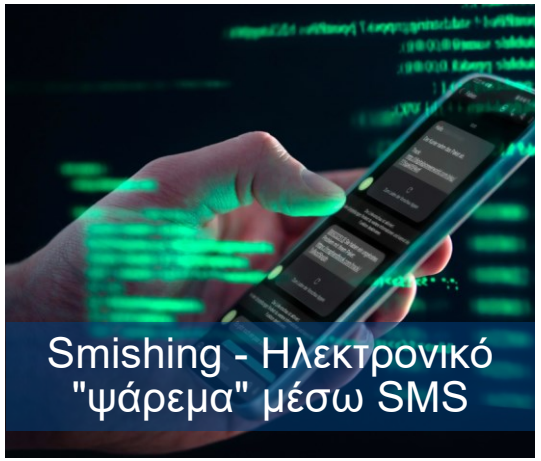


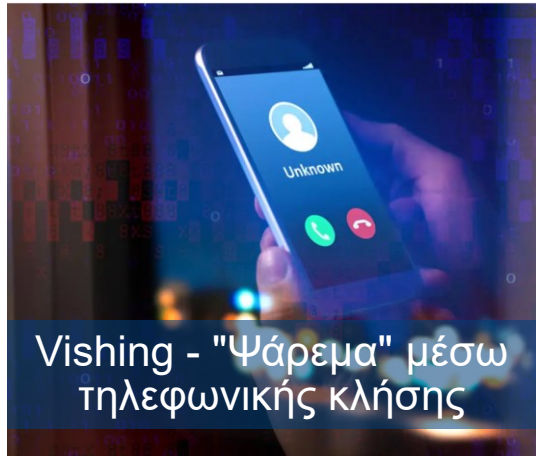
Social Engineering

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



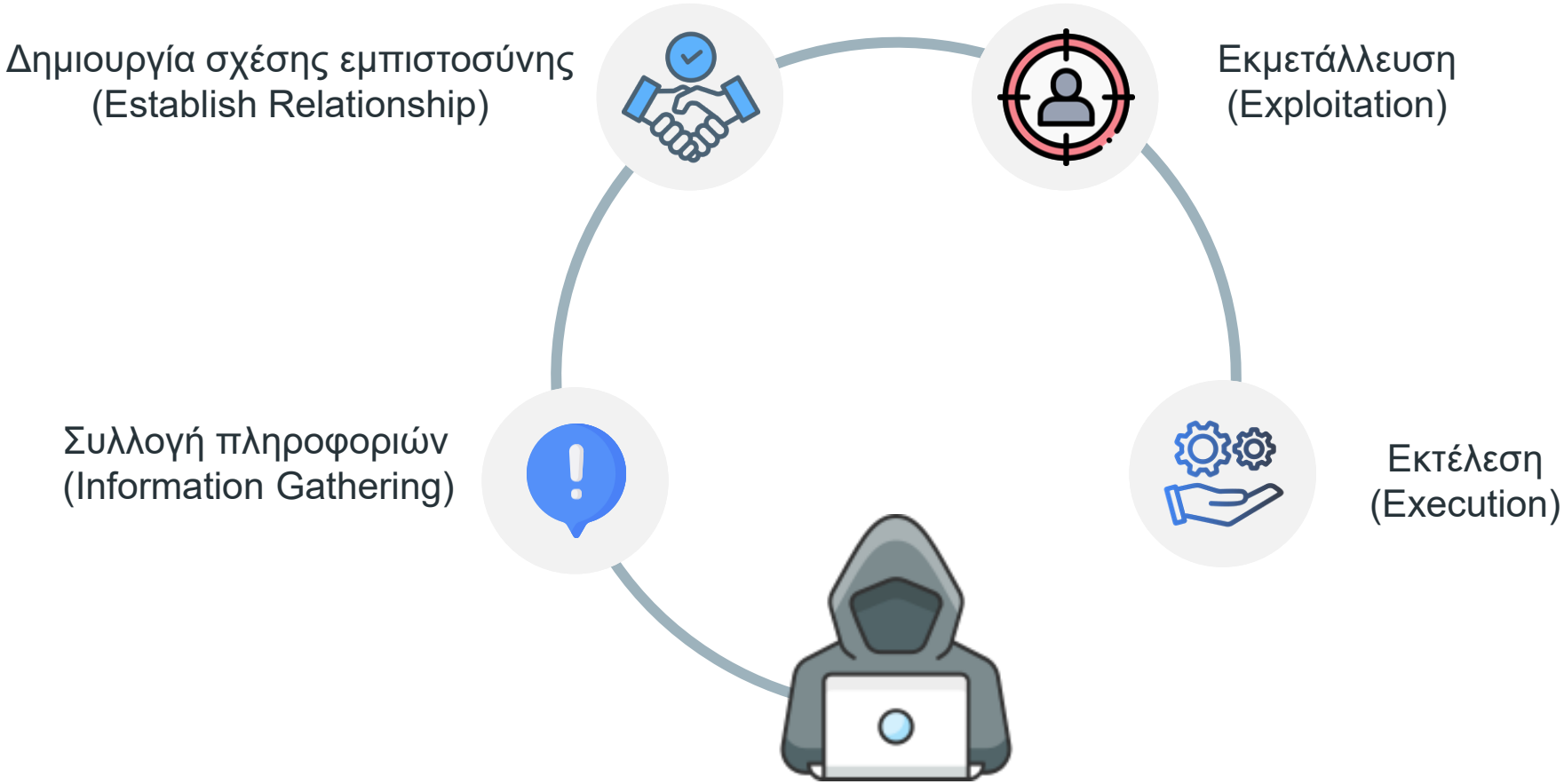
Vishing - "Ψάρεμα" μέσω τηλεφωνικής κλήσης

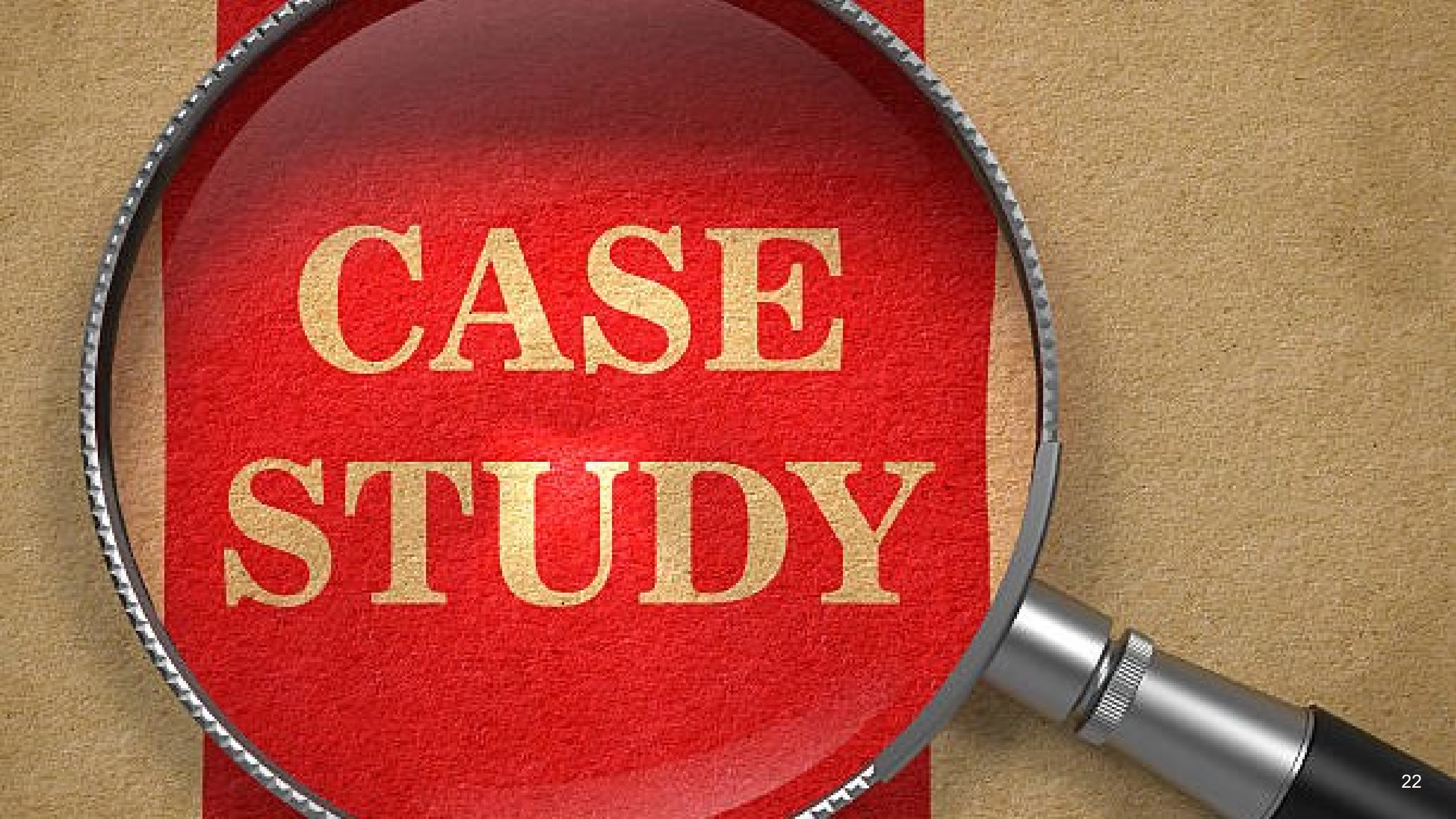

Pretexting - Χρήση Αληθοφανούς Σεναρίου


Baiting – Χρήση Δολωμάτων


Tailgating - Φυσική Παρουσία

Στάδια Επιθέσεων Κοινωνικής Μηχανικής




CASE
STUDY

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

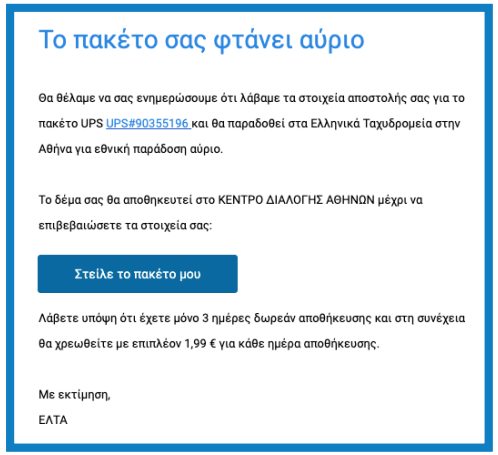
Fake e-banking site

2. Steal Credentials
username
password

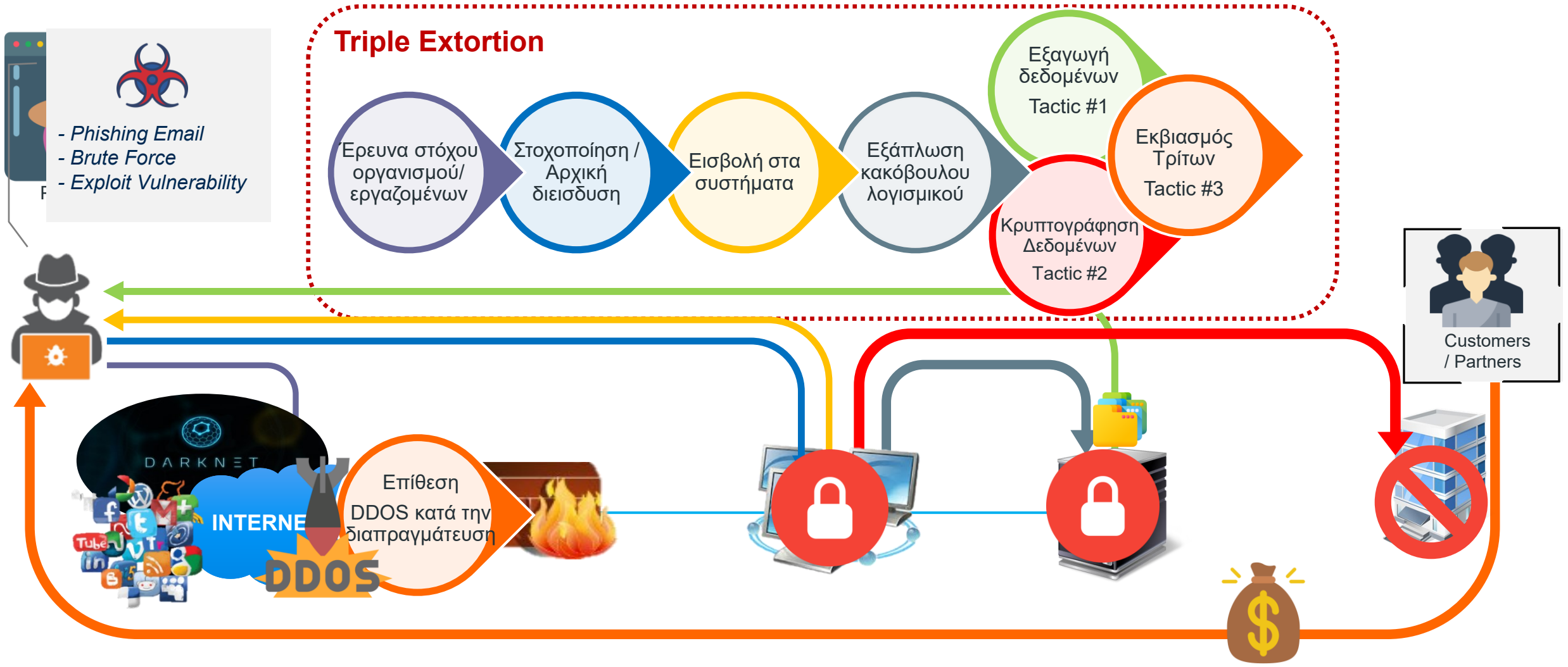
4. New Bank Wallet Authorization Request

5. Unintentional New Bank Wallet Installation Authorization

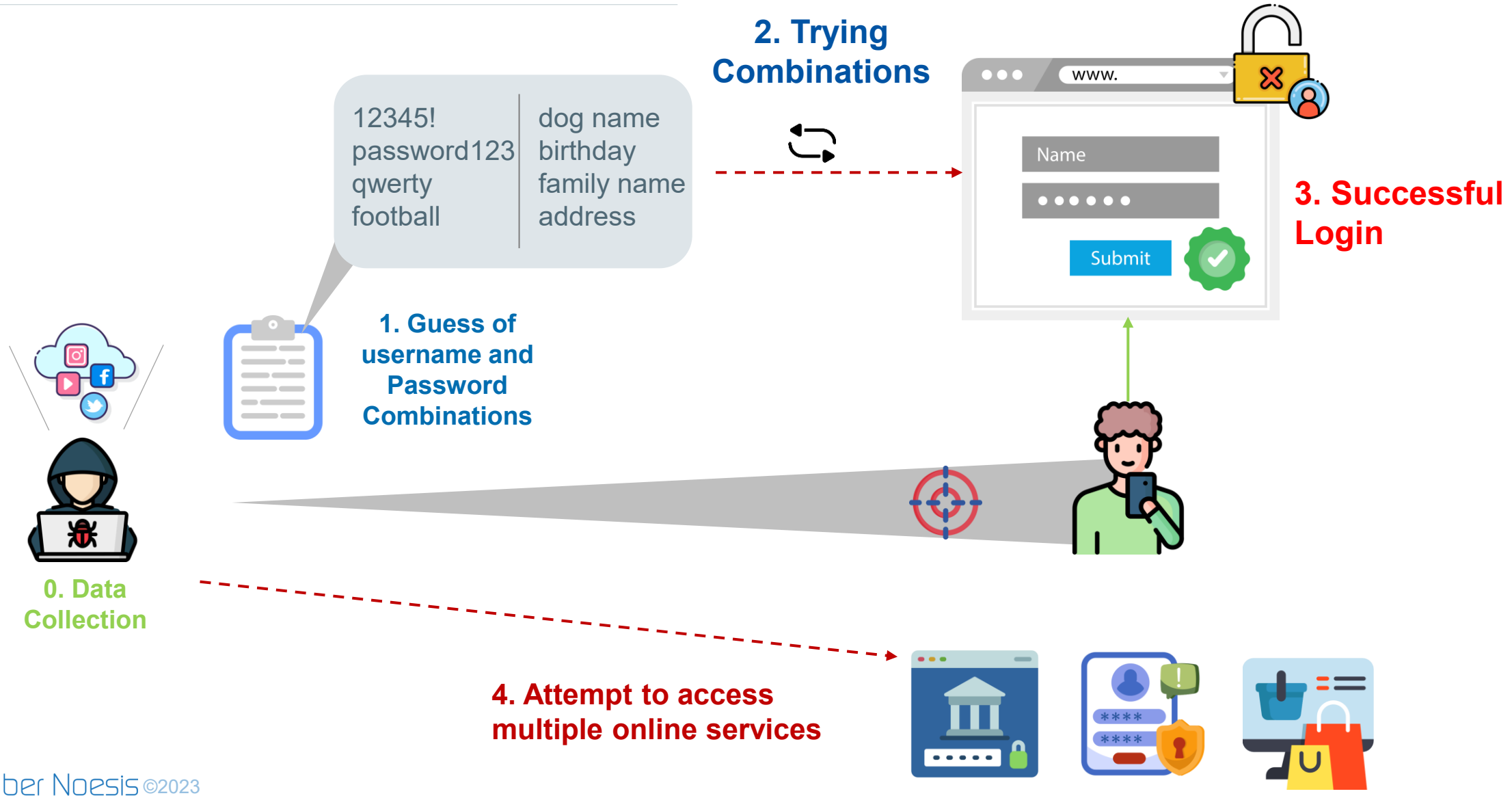
1. Contact & Temptation



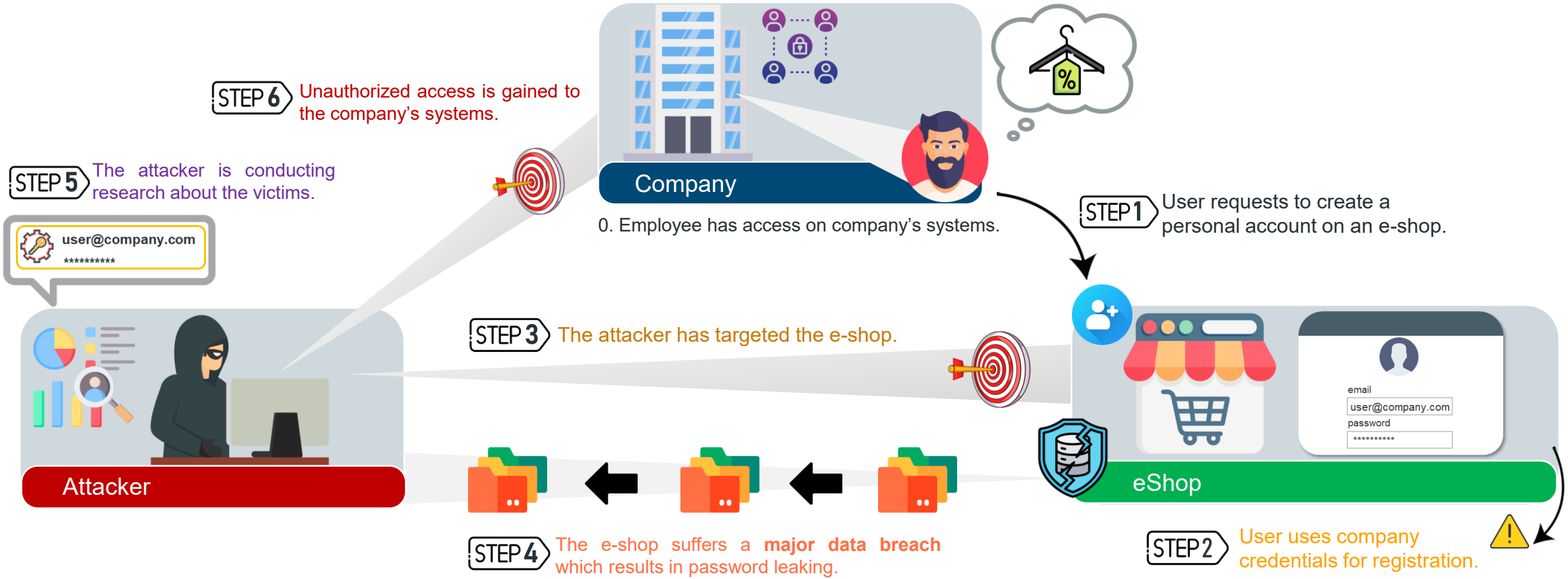
Triple Extortion…

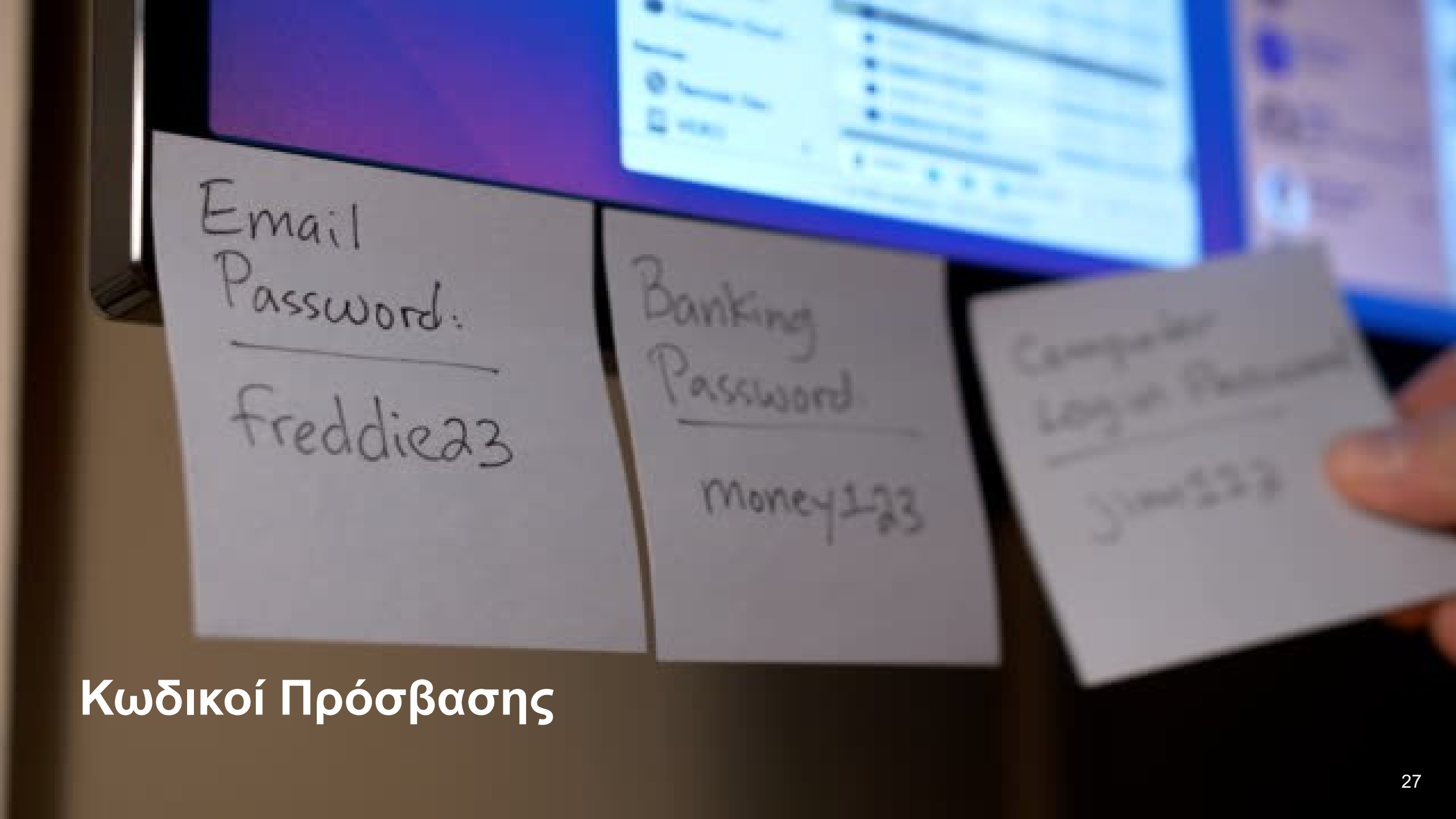


Brute-force Attack (παράδειγμα)



Data Breach – Stolen Credentials





Κωδικοί Πρόσβασης

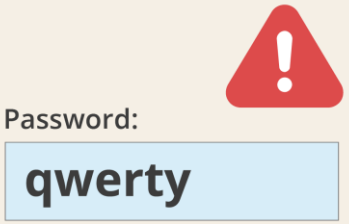
Βλέπετε τον Κωδικό σας?

25 most common passwords of 2023

123456	123456789	qwerty	password	12345
qwerty123	1q2w3e	12345678	111111	1234567890
123123	abc123	1234	password1	iloveyou
1q2w3e4r	000000	qwerty123	zaq12wsx	dragon
sunshine	princess	letmein	654321	monkey

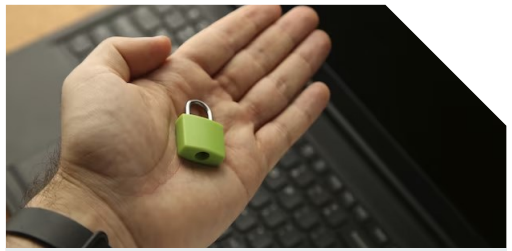
Πως διαρρέουν οι κωδικοί πρόσβασης

Κλοπή βάσεων & διαμοιρασμός στο ίντερνετ!



Εύκολα προβλέψιμοι!
(δημοσιοποιημένες πληροφορίες)

Απώλεια χειρόγραφων σημειώσεων!



Διαμοιρασμός με τρίτους (έμπιστους;)!

Phishing Email

Vishing

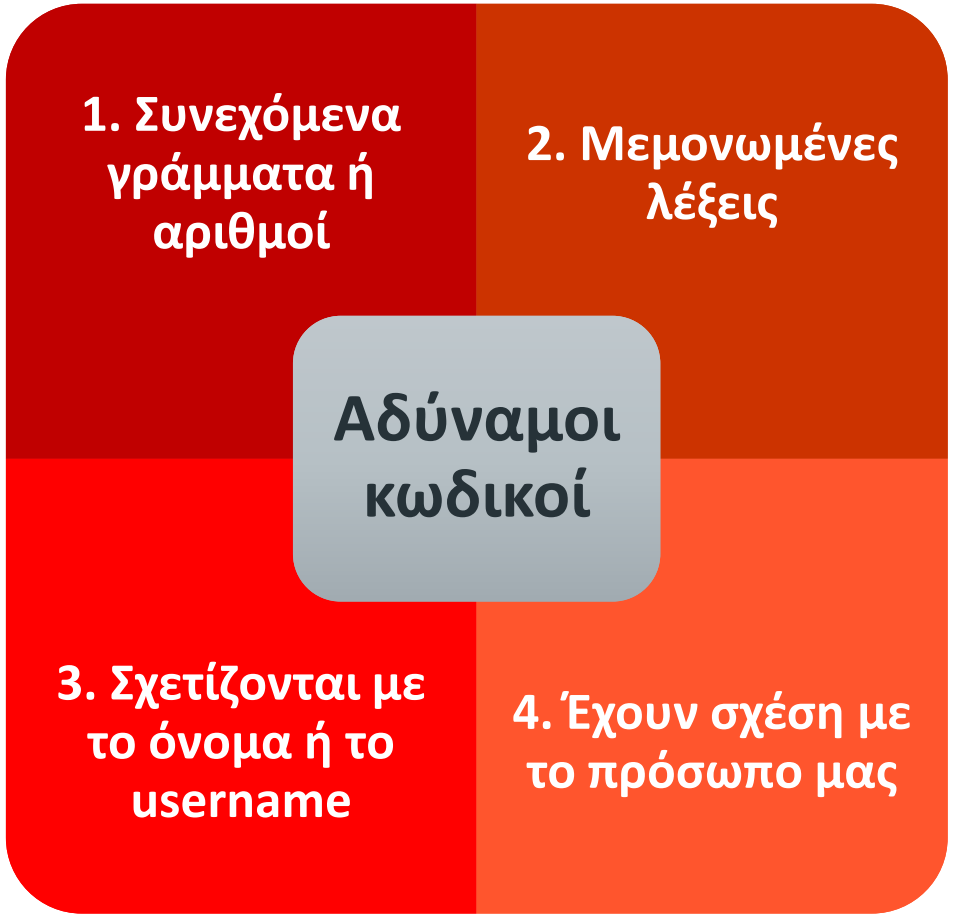
Μη ασφαλής αποθήκευση
(Excel, Notepad, Browser)

Σύνδεση σε
μη έμπιστα δίκτυα.

Που αποθηκεύουμε τους κωδικούς μας;

Video

Αδύναμοι VS Ισχυροί Κωδικοί Πρόσβασης



- 1234, 1111, 12345678, 123123, 987654321, aaaa, qwerty, asdfghk, %^&*()
- love, password, google, letmein, login
- Giannis1, @nt0n1$
- Ημερομηνία γέννησης, γάμου, ηλικία, τηλεφωνικός αριθμός, ονόματα συγγενών ή φίλων

Weak

Αδύναμοι VS Ισχυροί Κωδικοί Πρόσβασης

- “1u@Vk#_Lz”
  - 8 χαρακτήρες, 4 εβδομάδες για να σπάσει
- “qv!8Zvkl@48FG^”
  - 14 χαρακτήρες, δεν σπάει πρακτικά ποτέ
- “alogospitipinakas940@”
  - 20 χαρακτήρες, ακόμα πιο δύσκολο να σπάσει
  - εύκολο να τους θυμόμαστε

Strong

Τακτική Αλλαγή Κωδικών

- Τραπεζικά ιδρύματα (κάθε 3 ή 6 μήνες)
- Κρατικές υπηρεσίες (κάθε 6 μήνες)
- Υπολογιστή (κάθε 6 μήνες)
- Υποψία διαρροής

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Συνοψίζοντας …

Ισχυροί Κωδικοί

Χρησιμοποιείτε ισχυρούς και μοναδικούς κωδικούς μεγάλη πολυπλοκότητα (μήκος χαρακτήρων, αριθμοί και σύμβολα).

Ασφαλής Αποθήκευση

Χρησιμοποιείτε εφαρμογή **password manager** για την ασφαλή αποθήκευση και διαχείριση.

Αυθεντικοποίηση MFA

Ενεργοποιήστε όπου είναι δυνατό την αυθεντικοποίηση πολλών παραγόντων (MFA, 2FA).

Ενεργοποίηση Ειδοποιήσεων

Ενεργοποιείστε την αποστολή ειδοποιήσεων για νέες συνδέσεις και σημαντικές ενημερώσεις στους λογαριασμούς σας.

Προσεκτική Περιήγηση

Να ελέγχετε προσεκτικά τις σελίδες στις οποίες συνδέεστε (ένδειξη HTTP**S**) και να μην διαμοιράζεστε τους κωδικούς σας σε **καμία** περίπτωση.

- Χρησιμοποιούμε διαφορετικούς κωδικούς.
- Δεν μοιραζόμαστε του κωδικούς μας με τρίτους (αγνώστους αλλά και έμπιστους).
- Αλλάζουμε τακτικά τους κωδικούς μας.

Ασφαλής Εξ' Αποστάσεως Εργασία

Ασφαλής Εξ Αποστάσεως Εργασία

- Που συνδεόμαστε;
- Τι εξοπλισμό χρησιμοποιούμε;
- Πώς διαμοιραζόμαστε πληροφορίες;
- Περιηγούμαστε στο διαδίκτυο ελεύθερα;
- Πού αποθηκεύουμε τη δουλειά μας;

Απειλές στην εξ αποστάσεως εργασία (Work from home)

Καθώς η εξ αποστάσεως εργασίας γίνεται όλο και πιο διαδεδομένη, είναι απολύτως αναγκαίο να ληφθούν υπόψην οι απειλές που πλήττουν τον χώρο αυτό.

1. Πιθανή χρήση προσωπικού υπολογιστή και το αντίστροφο
2. Σύνδεση στο δίκτυο της εταιρείας από μη ασφαλή συσκευή.
3. Σύνδεση σε μη Ασφαλή Δίκτυα
4. Κακόβουλες Ενέργειες - Πρακτικές (π.χ. μη ασφαλή περιήγηση στο internet)

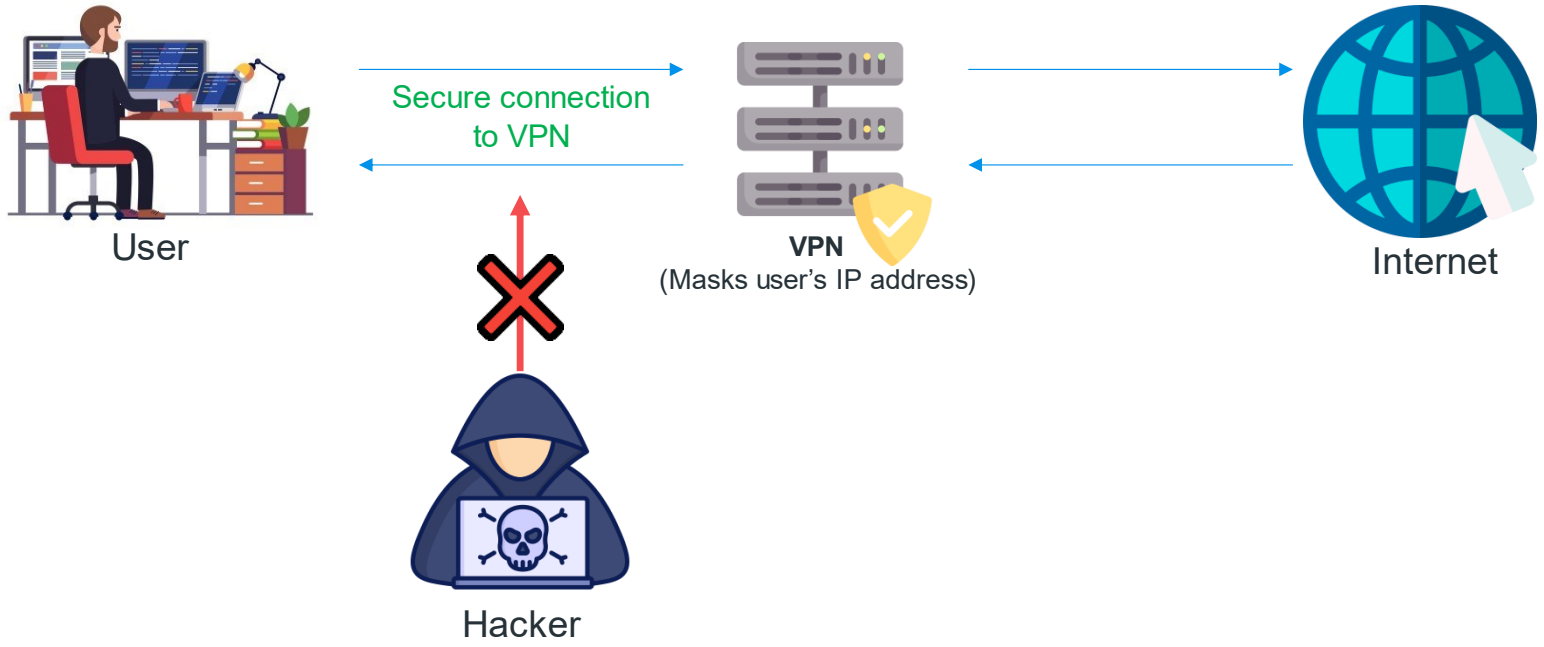
Δικτυακή Ασφάλεια στο Σπίτι

Ασφαλίστε το οικιακό σας δίκτυο:

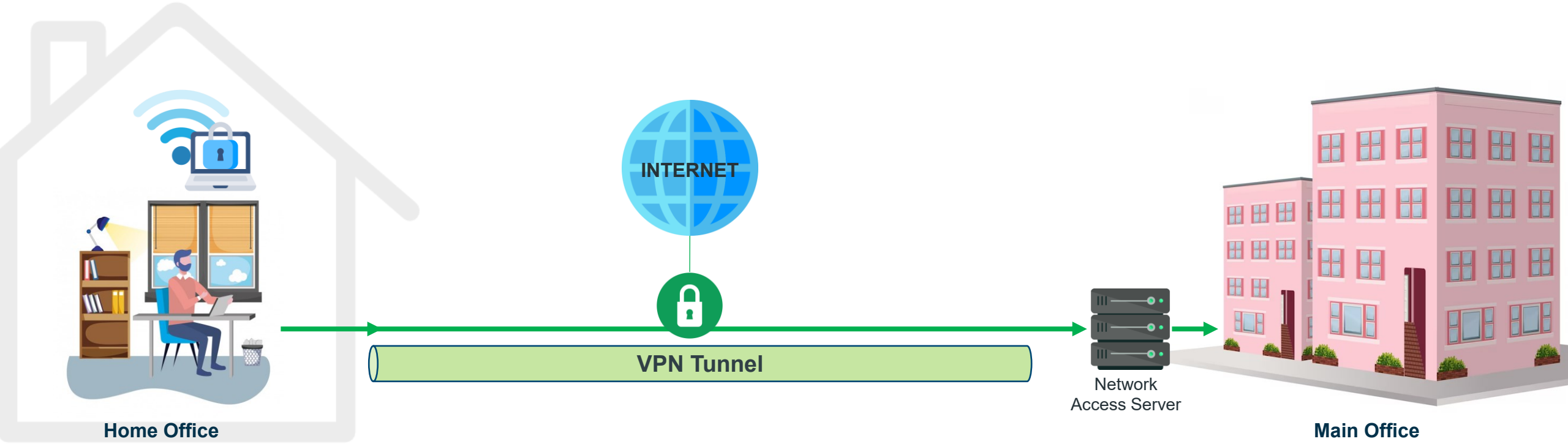
- Αλλάξτε το προεπιλεγμένο **όνομα χρήστη**, τον **κωδικό πρόσβασης** και το **όνομα του οικιακού δικτύου (SSID)**.
- Χρησιμοποιήστε ισχυρή κρυπτογράφηση, όπως **WPA2** (μην χρησιμοποιείτε ποτέ WEP).
- Ορίστε **ισχυρούς κωδικούς πρόσβασης** για τις συσκευές σύνδεσης.
- Χρησιμοποιήστε ένα **VPN** για πρόσθετη ασφάλεια.

VPN

- Δημιουργεί μια ασφαλή και κρυπτογραφημένη σύνδεση μεταξύ ενός υπολογιστή ή ενός smartphone με έναν διακομιστή στο Διαδίκτυο.
- Όταν χρησιμοποιείτε ένα VPN, όλη η δικτυακή σας κίνηση πηγαίνει μέσα από αυτή την ασφαλή σύνδεση, κρυπτογραφώντας τα δεδομένα που ανταλλάσσετε με το Διαδίκτυο.



Work from home Diagram



Expect the Unexpected!

What about Deepfakes …

Hot Impersonation Using Artificial Intelligence

- In 2019, hackers used highly advanced AI software to impersonate an executive's voice and made off with €220,000.
- AI was used to mimic a C-Suite boss at a German company who made a call to subsidiary's UK CEO.
- The recipient didn't suspect when the German exec (his boss) requested to make the urgent payment to a supplier.
- The UK CEO recognized "***his boss's slight German accent and the melody of his voice on the phone***".

Nowadays …

Many of the most convincing deepfake cases have been created with the help of impersonators that mimic the source's voice and gestures…

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

Επιθέσεις και Πρακτικές
Αντιμετώπισης

Cyber Security Quick Wins

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

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