

ΨΗΦΙΑΚΕΣ
ΠΛΗΡΩΜΕΣ
ΑΠΑΤΕΣ &
ΤΥΧΕΡΑ
ΠΑΙΧΝΙΔΙΑ



ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ
ΕΥΡΩΣΥΣΤΗΜΑ

ΚΕΝΤΡΟ ΠΟΛΙΤΙΣΜΟΥ
ΕΡΕΥΝΑΣ ΚΑΙ ΤΕΚΜΗΡΙΩΣΗΣ

Κεντρικό Συμβούλιο της Ένωσης Οικονομολόγων
Εκπαιδευτικών Δευτεροβάθμιας Εκπαίδευσης

Ψηφιακές απάτες και έφηβοι:
Πρόληψη, αναγνώριση και προστασία

Γιώργος Τσιατούρας

Δ/νη Χρηματοπιστωτικής Σταθερότητας, ΤτΕ

Αθήνα, 4 Σεπτεμβρίου 2026



Περιεχόμενα Παρουσίασης

1. Το Οικοσύστημα των Ψηφιακών Απατών
2. Γιατί οι έφηβοι αποτελούν στόχο
3. Τεχνικές χειραγώγησης
4. Κλοπή στοιχείων (Phishing)
5. Εξαπάτηση για αποστολή κεφαλαίων (APP Fraud)
6. Εκμετάλλευση ως μέσο τέλεσης απάτης (money mule)
7. Θεσμικές εξελίξεις
8. Εκπαιδευτικοί – Πεδίο για καθοριστική συμβολή

Το Οικοσύστημα των Ψηφιακών Απατών

Οι περισσότερες
ψηφιακές απάτες
εντάσσονται σε **δύο**
βασικές κατηγορίες

Phishing

(κλοπή στοιχείων)

Στόχος

- Κωδικοί πρόσβασης (passwords)
- Κωδικοί μίας χρήσης (OTPs)
- Στοιχεία καρτών
- Προσωπικά δεδομένα

Κανάλια

- Fake websites
- e-mail
- SMS
- Social media
- QR codes

APP Fraud

(αποστολή κεφαλαίων)

Στόχος

- Χειραγώγηση του θύματος ώστε να πραγματοποιήσει το ίδιο μία ή πολλαπλές συναλλαγές

Παραδείγματα

- Ψευδείς επενδύσεις
- Δήθεν συγγενής ή φίλος σε ανάγκη
- Ρομαντικές απάτες
- Απάτες μέσω αγγελίας
- Απάτες με κρυπτοστοιχεία

Γιατί οι έφηβοι αποτελούν στόχο;

ΟΟΣΑ

- Οι διαδικτυακές απάτες αναγνωρίζονται **ως σημαντικός ψηφιακός κίνδυνος** για τα παιδιά και τους εφήβους.

OECD (2021), Children in the Digital Environment.

- **98%** των 15χρονων διαθέτουν smartphone με πρόσβαση στο διαδίκτυο.

OECD (2025), How's Life for Children in the Digital Age.

Οι απατεώνες δεν
στοχεύουν την ηλικία.

Στοχεύουν τις
συμπεριφορές και τις
συνήθειες των χρηστών.



Αυξημένη ψηφιακή παρουσία

- Εκτεταμένη χρήση social media και εφαρμογών ανταλλαγής μηνυμάτων.
- Συχνή συμμετοχή σε online gaming και διαδικτυακές κοινότητες.



Αυξημένη ευαλωτότητα σε τεχνικές χειραγώγησης

- Περιορισμένη εμπειρία στην αναγνώριση απατών.
- Περιέργεια και αυθορμητισμός. Επιρροή από συνομηλίκους και influencers.
- Αυξημένη «ψηφιακή εμπιστοσύνη» σε μηνύματα και προφίλ χρηστών



Ελκυστικότητα του «εύκολου κέρδους»

- Giveaways, gaming rewards, ψεύτικες επενδύσεις.
- Απάτες με κρυπτοστοιχεία και γρήγορο πλουτισμό.

Τεχνικές Χειραγώγησης

Οι περισσότερες ψηφιακές απάτες δεν βασίζονται στην παραβίαση συστημάτων, αλλά στη χειραγώγηση του ίδιου του ανθρώπου (Social Engineering).



Επείγον: «Αν δεν ενεργήσεις τώρα, ο λογαριασμός σου θα απενεργοποιηθεί.»



Εύκολο κέρδος: «Κέρδισες iPhone.» | «Εγγυημένη απόδοση 20%.»



Φόβος: «Ο λογαριασμός σου παραβιάστηκε.» «Θα δημοσιεύσουμε φωτογραφίες σου.»



Προσωπικές σχέσεις: Romance scam | Fake friend | Δήθεν συγγενής σε ανάγκη

Κλοπή στοιχείων (Phishing)



Σκοπός: Απόκτηση κωδικών και προσωπικών στοιχείων

- Πλαστή ιστοσελίδα (τραπεζικές και άλλες υπηρεσίες κ.α.)
- Gaming scams
- Fake giveaways
- SMS / e-mail / social media phishing



Αποτέλεσμα: Κλοπή λογαριασμών ή μέσων πληρωμής. Εγγραφή συσκευής υπό τον έλεγχο του απατεώνα.



- ✓ Ελέγχω διεύθυνση URL
- ✓ Δεν ακολουθώ συνδέσμους από ύποπτα e-mails/SMS
- ✓ Μελετάω καλά την επεξήγηση στα μηνύματα OTP και ενεργοποιώ alerts
- ✓ Αμφιβάλλω όταν υπάρχει πίεση χρόνου
- ✓ Αν έχω αμφιβολία επικοινωνώ εγώ με την τράπεζα ή με την εταιρεία.

Εξαπάτηση για αποστολή κεφαλαίων (APP Fraud)

 **Σκοπός:** Να πειστεί το θύμα να στείλει χρήματα.

- Κλήση δήθεν συγγενούς ή φίλου σε ανάγκη
- Παραβιασμένος λογαριασμός SM που ζητά χρήματα
- Romance scams
- Fake investments
- Crypto investment scams
- Ponzi / Pyramid schemes

 **Αποτέλεσμα:** Το θύμα θεωρώντας ότι συναλλάσσεται με νόμιμα πρόσωπα πραγματοποιεί συναλλαγή/ές.



- ✓ Δεν στέλνω χρήματα επειδή κάποιος επικαλείται επείγουσα ανάγκη.
- ✓ Επιβεβαιώνω πάντα την ταυτότητα φίλου ή συγγενή από διαφορετικό κανάλι επικοινωνίας.
- ✓ Ελέγχω προσεκτικά τον δικαιούχο πριν εγκρίνω μεταφορά χρημάτων.
- ✓ Οι επενδύσεις και τα κρυπτοστοιχεία δεν είναι κατάλληλα για ανηλίκους.
- ✓ Μία πρόταση για γρήγορο κέρδος αποτελεί ισχυρή ένδειξη απάτης.

Εκμετάλλευση ως μέσο τέλεσης απάτης (money mules)



Σκοπός: Να χρησιμοποιηθεί ο λογαριασμός ενός τρίτου για τη διακίνηση κεφαλαίων εγκληματικής προέλευσης.

- «Εύκολη δουλειά από το σπίτι»
- «Κέρδισε χρήματα χωρίς εμπειρία»
- «Αξιοποίησε τον λογαριασμό σου για να έχεις κέρδος»
- Προσέγγιση μέσω TikTok, Instagram, Telegram ή αγγελιών εργασίας



Αποτέλεσμα: Ο λογαριασμός του θύματος χρησιμοποιείται για τη διακίνηση παράνομων κεφαλαίων και το ίδιο μπορεί να βρεθεί αντιμέτωπο με σοβαρές ποινικές συνέπειες.



Κανείς δεν πληρώνει νόμιμα για να χρησιμοποιήσει τον λογαριασμό πληρωμών ενός τρίτου. Αν σου το προτείνουν, πιθανότατα επιχειρούν να σε στρατολογήσουν ως money mule.

Θεσμικές εξελίξεις

Ενίσχυση του κανονιστικού πλαισίου

Νέες υποχρεώσεις για τις τράπεζες και τους παρόχους υπηρεσιών πληρωμών και μέτρα ενίσχυσης προστασίας των χρηστών. Συμμετοχή και άλλων εμπλεκόμενων φορέων (π.χ. τεχνολογικών παρόχων) στην αντιμετώπιση της απάτης.

Δικλείδες ασφαλείας

Ισχυρή Ταυτοποίηση Πελάτη (Strong Customer Authentication – SCA) για την επιβεβαίωση των ηλεκτρονικών συναλλαγών. Επιβεβαίωση Δικαιούχου (Verification of Payee – VoP) ώστε ο χρήστης να ενημερώνεται όταν το όνομα του δικαιούχου δεν αντιστοιχεί στον λογαριασμό που πρόκειται να πιστώσει.

Ενίσχυση των μηχανισμών παρακολούθησης συναλλαγών για τον έγκαιρο εντοπισμό ύποπτης δραστηριότητας.

Συνεργασία και ανταλλαγή πληροφοριών

Δημιουργία πλαισίων συνεργασίας μεταξύ τραπεζών, εποπτικών αρχών, αρχών επιβολής του νόμου και τεχνολογικών παρόχων. Ανάπτυξη μηχανισμών και πλατφορμών ανταλλαγής πληροφοριών για νέες μεθόδους απάτης.

Ενημέρωση και ευαισθητοποίηση

Υποχρεώσεις ενημέρωσης από τους παρόχους υπηρεσιών πληρωμών. Προώθηση δράσεων ψηφιακής και χρηματοοικονομικής παιδείας.

Εκπαιδευτικοί – Πεδίο για καθοριστική συμβολή



Καλλιέργεια κριτικής σκέψης

Ενθαρρύνετε τους μαθητές να αμφισβητούν ό,τι φαίνεται «πολύ καλό για να είναι αληθινό».

Διδάξτε τους να αναγνωρίζουν τις τεχνικές χειραγώγησης (επείγον, φόβος, εύκολο κέρδος, συναισθηματική πίεση).



Δημιουργία κουλτούρας συζήτησης

Ενθαρρύνετε τους μαθητές να μιλούν όταν δέχονται ύποπτα μηνύματα ή διαδικτυακές προσεγγίσεις.

Υπενθυμίστε ότι κανείς δεν πρέπει να ντρέπεται επειδή παραλίγο να πέσει θύμα μιας απάτης.



Καλλιεργήστε υπεύθυνη ψηφιακή συμπεριφορά

Προστατεύουμε τα προσωπικά μας δεδομένα. Δεν ενεργούμε βιαστικά όταν υπάρχει οικονομικό αίτημα. Διαβάζουμε με προσοχή πάντα τα μηνύματα έγκρισης συναλλαγών. Ζητούμε δεύτερη γνώμη όταν κάτι μας δημιουργεί αμφιβολία.



Αλληλεγγύη μεταξύ των γενεών

Οι νέοι μπορούν να βοηθήσουν τους γονείς και τους γηραιότερους στο οικογενειακό περιβάλλον τους να αναγνωρίζουν τις ψηφιακές απάτες. Μια απλή συζήτηση στο σπίτι μπορεί να αποτρέψει μια σημαντική οικονομική απώλεια.



Οι μαθητές δεν είναι μόνο αποδέκτες γνώσης. Μπορούν να γίνουν "πρεσβευτές ασφάλειας" για τις οικογένειές τους στο ψηφιακό περιβάλλον.

Ευχαριστούμε