

Έπεσα θύμα ηλεκτρονικής απάτης. Τι πρέπει να κάνω;

Πρακτικός νομικός οδηγός με άμεσα βήματα προστασίας και βασικό νομοθετικό πλαίσιο

Ιούλιος 2026

Ο χρόνος αντίδρασης είναι κρίσιμος. Επικοινωνήστε αμέσως με την τράπεζα ή τον πάροχο πληρωμών σας, ζητήστε φραγή και αμφισβήτηση της συναλλαγής και διατηρήστε όλα τα αποδεικτικά στοιχεία.

Οι ηλεκτρονικές απάτες εμφανίζονται πλέον με πολλές μορφές: παραπλανητικά e-mail και SMS, ψεύτικες ιστοσελίδες τραπεζών ή δημόσιων φορέων, τηλεφωνικές κλήσεις από δήθεν υπαλλήλους, αγγελίες πώλησης, υποτιθέμενες επενδύσεις, παραβίαση λογαριασμών και αλλοίωση τραπεζικών στοιχείων σε τιμολόγια. Το πρώτο εικοσιτετράωρο μπορεί να αποδειχθεί καθοριστικό τόσο για τον περιορισμό της ζημίας όσο και για τη συγκέντρωση αποδείξεων.

1. Οι συνηθέστερες μορφές ηλεκτρονικής απάτης

- **Phishing / smishing:** Παραπλανητικό e-mail ή SMS που οδηγεί σε πλαστή ιστοσελίδα και ζητά κωδικούς, στοιχεία κάρτας ή επιβεβαίωση μέσω εφαρμογής.
- **Vishing και caller ID spoofing:** Τηλεφωνική κλήση από πρόσωπο που εμφανίζεται ως υπάλληλος τράπεζας, λογιστής, αστυνομικός ή εκπρόσωπος δημόσιου φορέα. Ο αριθμός μπορεί να φαίνεται γνήσιος.
- **Απάτη με απομακρυσμένη πρόσβαση:** Ο δράστης πείθει το θύμα να εγκαταστήσει πρόγραμμα απομακρυσμένου ελέγχου και αποκτά πρόσβαση στη συσκευή ή στην ηλεκτρονική τραπεζική.
- **Απάτη σε αγγελίες και ηλεκτρονικές αγορές:** Πseudonymous αγοραστής ή πωλητής ζητά πληρωμή, στοιχεία κάρτας ή χρήση πλαστού συνδέσμου μεταφορικής ή τράπεζας.
- **Αλλαγή IBAN / business e-mail compromise:** Παραβιάζεται εταιρικό e-mail και αποστέλλεται παραποιημένο τιμολόγιο ή μήνυμα με διαφορετικό τραπεζικό λογαριασμό.
- **Επενδυτική απάτη:** Υποσχέσεις για υψηλές και εγγυημένες αποδόσεις σε μετοχές, κρυπτονομίσματα ή άλλες επενδύσεις, συχνά μέσω μη αδειοδοτημένων πλατφορμών.

Ανεξάρτητα από τη μορφή της ηλεκτρονικής απάτης, η έγκαιρη αντίδραση του παθόντος αποτελεί συνήθως τον σημαντικότερο παράγοντα τόσο για τον περιορισμό της ζημίας όσο και για τη διατήρηση κρίσιμων αποδεικτικών στοιχείων. Αν και κάθε υπόθεση παρουσιάζει τις δικές της ιδιαιτερότητες, οι ακόλουθες ενέργειες είναι, κατά κανόνα, σκόπιμο να πραγματοποιούνται χωρίς καθυστέρηση.

2. Οι πρώτες ενέργειες μετά το περιστατικό

Βήμα 1: Επικοινωνήστε αμέσως με την τράπεζα ή τον πάροχο πληρωμών σας

Η άμεση επικοινωνία με τον επίσημο αριθμό εξυπηρέτησης της τράπεζας αποτελεί, κατά κανόνα, την πρώτη ενέργεια που απαιτείται. Ζητήστε φραγή καρτών, λογαριασμών, e-banking και οποιουδήποτε μέσου

πληρωμών έχει κινδυνεύσει λόγω της απάτης. Δηλώστε ρητά ότι αμφισβητείτε τη συναλλαγή ως μη εγκεκριμένη, εφόσον πράγματι δεν την εγκρίνατε.

Βήμα 2: Ζητήστε ανάκληση, δέσμευση ή εντοπισμό της μεταφοράς

Αν πρόκειται για τραπεζικό έμβασμα, ζητήστε άμεσα διαδικασία recall και επικοινωνία με την τράπεζα του δικαιούχου για πιθανή δέσμευση του ποσού. Η τράπεζα συνήθως δεν παρέχει εγγύηση επιστροφής, αλλά ακόμα και η πιθανότητα επιστροφής μειώνεται όσο περνά ο χρόνος.

Βήμα 3: Υποβάλετε αμφισβήτηση της συναλλαγής εγγράφως

Η τηλεφωνική ενημέρωση είναι σημαντική, πλην όμως συνήθως δεν αρκεί από μόνη της. Στείλτε e-mail ή υποβάλετε αίτημα μέσω του ασφαλούς περιβάλλοντος της τράπεζας. Ζητήστε αριθμό πρωτοκόλλου ή αποδεικτικό παραλαβής για το αίτημά σας.

Βήμα 4: Διατηρήστε όλα τα αποδεικτικά στοιχεία

Κρατήστε screenshots, e-mail με πλήρεις κεφαλίδες όπου είναι δυνατό, SMS, αριθμούς τηλεφώνων, συνδέσμους, αποδείξεις μεταφοράς, IBAN, ονόματα δικαιούχων, συνομιλίες, αγγελίες, ημερομηνίες και ώρες. Μην διαγράψετε την εφαρμογή στην οποία έλαβε χώρα η επικοινωνία ή τη συνομιλία πριν κρατήσετε αντίγραφα.

Βήμα 5: Ασφαλίστε τους λογαριασμούς και τις συσκευές σας

Αλλάξτε κωδικούς χρησιμοποιώντας νέα, ασφαλή συσκευή, αρχίζοντας από το e-mail σας. Ενεργοποιήστε την δυνατότητα ελέγχου δύο παραγόντων, αποσυνδέστε άγνωστες συσκευές από τους λογαριασμούς σας και επικοινωνήστε με την εταιρεία κινητής τηλεφωνίας που συνεργάζεστε αν υπάρχει υποψία SIM swap.

Βήμα 6: Καταγγείτε το περιστατικό

Μπορείτε να απευθυνθείτε στη Διεύθυνση Δίωξης Κυβερνοεγκλήματος, στη γραμμή 11188, να προχωρήσετε σε ηλεκτρονική καταγγελία στο gov.gr, ή να προχωρήσετε σε κατάθεση εγκλήσεως ενώπιον της αρμόδιας αστυνομικής/εισαγγελικής αρχής.

Βήμα 7: Ελέγξτε αν έχουν διαρρεύσει και άλλα δεδομένα

Αν δώσατε φωτογραφία ταυτότητας, κωδικούς Taxisnet, στοιχεία κάρτας ή προσωπικά δεδομένα, ενημερώστε τους αντίστοιχους φορείς και παρακολουθείτε λογαριασμούς και πιστωτικές κινήσεις για νέες απόπειρες απάτης.

Βήμα 8: Μην πληρώσετε ξανά για δήθεν ανάκτηση χρημάτων

Μετά την πρώτη απάτη συχνά ακολουθεί δεύτερη: πρόσωπα εμφανίζονται ψευδώς ως δικηγόροι, λογιστές, τεχνικοί ή “εταιρείες ανάκτησης” και ζητούν προκαταβολή. Αποφύγετε οποιαδήποτε τέτοια επικοινωνία.

3. Τι προβλέπει ο νόμος για τις τραπεζικές συναλλαγές

Ο ν. 4537/2018, ο οποίος ενσωμάτωσε την ευρωπαϊκή νομοθεσία για τις υπηρεσίες πληρωμών, ρυθμίζει τα δικαιώματα και τις υποχρεώσεις του χρήστη και του παρόχου υπηρεσιών πληρωμών. Η εφαρμογή των διατάξεων εξαρτάται από τα πραγματικά περιστατικά και ιδίως από το αν η συναλλαγή ήταν πραγματικά μη εγκεκριμένη ή αν ο χρήστης εξαπατήθηκε και την ενέκρινε ο ίδιος.

Άρθρο 69: Ο χρήστης οφείλει να χρησιμοποιεί το μέσο πληρωμών σύμφωνα με τους όρους ασφαλείας, να φυλάσσει τα διαπιστευτήριά του και να ειδοποιεί χωρίς υπαίτια καθυστέρηση μόλις αντιληφθεί απώλεια, κλοπή, υπεξαίρεση ή μη εγκεκριμένη χρήση.

Άρθρο 71: Η αμφισβήτηση τυχόν συναλλαγής πρέπει να γνωστοποιείται χωρίς υπαίτια καθυστέρηση και, κατά κανόνα, το αργότερο εντός δεκατριών μηνών από τη χρέωση. Η ύπαρξη της ανώτατης προθεσμίας δεν σημαίνει ότι πρέπει να περιμένει κανείς: η αναφορά πρέπει να γίνει αμέσως, για την μέγιστη νομική διασφάλιση του θύματος.

Άρθρο 72: Όταν ο χρήστης αρνείται ότι ενέκρινε μια συναλλαγή, ο πάροχος φέρει το βάρος να αποδείξει τη γνησιότητα, την ακριβή καταγραφή και την ορθή λειτουργία. Η απλή καταγραφή χρήσης του μέσου πληρωμών δεν αρκεί, από μόνη της, για να αποδείξει έγκριση, δόλο ή βαριά αμέλεια.

Άρθρο 73: Σε περίπτωση μη εγκεκριμένης πράξης πληρωμής, προβλέπεται καταρχήν άμεση επιστροφή του ποσού, το αργότερο έως το τέλος της επόμενης εργάσιμης ημέρας, εκτός αν υπάρχουν βάσιμες υπόνοιες απάτης που γνωστοποιούνται αρμοδίως.

Άρθρο 74: Η ευθύνη του του προσώπου που έδωσε την εντολή πληρωμής διαφοροποιείται ανάλογα με τις περιστάσεις. Για καταναλωτές, η νομοθεσία προβλέπει ειδικά όρια, ενώ σε περίπτωση δόλου ή βαριάς αμέλειας μπορεί να μετακυλιστεί μεγαλύτερο μέρος ή το σύνολο της ζημίας. Η κρίση περί βαριάς αμέλειας δεν είναι αυτόματη και πρέπει να στηρίζεται σε συγκεκριμένα αποδεικτικά στοιχεία.

Κρίσιμη διάκριση: Άλλο η μη εγκεκριμένη συναλλαγή (π.χ. ο δράστης έκανε τη μεταφορά χωρίς συναίνεση) και άλλο η συναλλαγή που ο ίδιος ο χρήστης ενέκρινε επειδή εξαπατήθηκε. Στη δεύτερη περίπτωση η τραπεζική αξίωση είναι συχνά δυσκολότερη και απαιτεί εξατομικευμένη νομική αξιολόγηση και πιθανώς προσφυγή στην δικαιοσύνη.

4. Ποινικές διατάξεις που μπορεί να εφαρμόζονται

Ανάλογα με τα πραγματικά περιστατικά και τον τρόπο τέλεσης της απάτης, μπορεί να εφαρμόζονται περισσότερες ποινικές διατάξεις:

- **Άρθρο 386 Ποινικού Κώδικα - Απάτη:** Καλύπτει την πρόκληση περιουσιακής βλάβης μέσω εν γνώσει παράστασης ψευδών γεγονότων ως αληθινών, αθέμιτης απόκρυψης ή παρασιώπησης αληθινών γεγονότων, με σκοπό παράνομου περιουσιακού οφέλους.
- **Άρθρο 386Α Ποινικού Κώδικα - Απάτη με υπολογιστή:** Αφορά περιουσιακή βλάβη που προκαλείται μέσω μη ορθής διαμόρφωσης αποτελέσματος επεξεργασίας δεδομένων, χωρίς δικαίωμα επέμβασης σε πληροφοριακό σύστημα ή δεδομένα, ή με άλλους τρόπους που προβλέπει η διάταξη.
- **Άρθρο 370B Ποινικού Κώδικα - Παράνομη πρόσβαση:** Μπορεί να εξεταστεί όταν ο δράστης παραβιάζει μέτρο προστασίας και αποκτά χωρίς δικαίωμα πρόσβαση σε σύστημα πληροφοριών ή ηλεκτρονικά δεδομένα.
- **Συναφή αδικήματα:** Ανάλογα με την υπόθεση μπορεί να συντρέχουν τα αδικήματα της πλαστογραφίας, της παράνομης επεξεργασίας προσωπικών δεδομένων, της παραβίασης απορρήτου επικοινωνιών, της εγκληματικής οργάνωσης ή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες.

5. Τι πρέπει να περιλαμβάνει ο φάκελος του θύματος

- ☐ Αναλυτικό ιστορικό του περιστατικού με ημερομηνίες και ώρες.
- ☐ Αντίγραφο κίνησης λογαριασμού και αποδεικτικά των συναλλαγών.
- ☐ Γραπτή δήλωση αμφισβήτησης της συναλλαγής προς την τράπεζα και αριθμός πρωτοκόλλου.

- ☐ Απαντήσεις της τράπεζας και όροι χρήσης e-banking ή κάρτας.
- ☐ Screenshots, μηνύματα, e-mail, σύνδεσμοι και στοιχεία προφίλ του δράστη.
- ☐ IBAN, στοιχεία δικαιούχου, αριθμοί καρτών ή λογαριασμών που χρησιμοποιήθηκαν.
- ☐ Αποδεικτικό καταγγελίας στην αστυνομία ή στη Δίωξη Κυβερνοεγκλήματος.
- ☐ Τεχνική έκθεση ή έλεγχος συσκευής, όταν υπάρχει υποψία παραβίασης αυτής.
- ☐ Κάθε επικοινωνία με πλατφόρμα, πάροχο ή τρίτο εμπλεκόμενο φορέα.

6. Συχνές ερωτήσεις

Θα μου επιστρέψει οπωσδήποτε η τράπεζα τα χρήματα;

Όχι αυτομάτως σε κάθε περίπτωση. Η απάντηση εξαρτάται από το αν η πράξη ήταν μη εγκεκριμένη, από τον τρόπο ταυτοποίησης, από τη συμπεριφορά του χρήστη, από την τήρηση των υποχρεώσεων ασφαλείας και από τα διαθέσιμα αποδεικτικά στοιχεία.

Αν έδωσα εγώ τον κωδικό μιας χρήσης, χάνω κάθε δικαίωμα;

Όχι κατ' ανάγκη. Πρέπει να εξεταστούν ο τρόπος εξαπάτησης, οι προειδοποιήσεις της τράπεζας, η ισχυρή ταυτοποίηση, η αλληλουχία ενεργειών και αν συντρέχει βαριά αμέλεια.

Αρκεί η τηλεφωνική καταγγελία στην τράπεζα;

Η τηλεφωνική επικοινωνία είναι αναγκαία για άμεση φραγή, αλλά δεν αρκεί και πάντοτε πρέπει να την ακολουθεί έγγραφη καταγγελία και αμφισβήτηση της συναλλαγής αλλά και να κρατηθεί αποδεικτικό.

Μπορεί να ανακτηθεί έμβασμα που έχει ήδη πιστωθεί;

Ενδέχεται, ιδίως αν η αντίδραση σας είναι άμεση και τα χρήματα παραμένουν στον λογαριασμό του δικαιούχου. Όμως η ανάκληση δεν είναι πάντοτε δυνατή και δεν πρέπει να θεωρείται δεδομένη.

Πρέπει να πάω αμέσως σε δικηγόρο;

Σε μικρή απόπειρα χωρίς οικονομική ζημία μπορεί να αρκούν τα άμεσα μέτρα ασφαλείας. Σε πραγματική χρέωση, σημαντικό ποσό, παραβίαση λογαριασμού, εταιρική απάτη ή αρνητική απάντηση τράπεζας, η έγκαιρη νομική αξιολόγηση από δικηγόρο είναι σκόπιμη για την αποτελεσματικότερη επίλυση του προβλήματος.

7. Συμπέρασμα

Η ηλεκτρονική απάτη αποτελεί ένα σύνθετο ζήτημα, το οποίο απαιτεί συνδυασμό τεχνικών, τραπεζικών και νομικών ενεργειών. Η πρώτη προτεραιότητα είναι να διακοπεί η πρόσβαση του δράστη και να περιοριστεί η οικονομική ζημία. Ακολουθούν η έγγραφη αμφισβήτηση της συναλλαγής, η διατήρηση των αποδεικτικών στοιχείων, η καταγγελία του περιστατικού και, όπου απαιτείται, η εξωδικαστική ή δικαστική προστασία των δικαιωμάτων του θύματος.

Χρήσιμη επισήμανση

Κάθε περιστατικό ηλεκτρονικής απάτης παρουσιάζει διαφορετικά πραγματικά και νομικά χαρακτηριστικά. Η αξιολόγηση των δικαιωμάτων του θύματος δεν μπορεί να βασίζεται αποκλειστικά σε γενικές πληροφορίες, αλλά απαιτεί εξέταση των ειδικών περιστάσεων κάθε υπόθεσης. Εφόσον έχει προκληθεί οικονομική ζημία ή ανακύψει διαφωνία με την τράπεζα ή άλλον εμπλεκόμενο φορέα, η έγκαιρη επικοινωνία με τον δικηγόρο σας μπορεί να αποδειχθεί καθοριστική για την αποτελεσματική προστασία των δικαιωμάτων σας.

Σημείωση: Το άρθρο έχει γενικό ενημερωτικό χαρακτήρα και δεν υποκαθιστά νομική συμβουλή. Οι εφαρμοστέες διατάξεις και οι απαιτούμενες ενέργειες εξαρτώνται από τα συγκεκριμένα περιστατικά κάθε υπόθεσης.

Πηγές και βασικό νομοθετικό πλαίσιο

- Ν. 4537/2018, ιδίως άρθρα 69, 71, 72, 73 και 74, όπως ισχύουν.
- Ν. 5019/2023, τροποποιήσεις της ευθύνης του πληρωτή για μη εγκεκριμένες πράξεις πληρωμής.
- Ποινικός Κώδικας (ν. 4619/2019), ιδίως άρθρα 386, 386Α και 370Β, όπως ισχύουν.
- Διεύθυνση Δίωξης Κυβερνοεγκλήματος, cyberalert.gr και γραμμή 11188.
- Gov.gr, υπηρεσία υποβολής επώνυμης καταγγελίας για εγκλήματα στον κυβερνοχώρο.