



Μπορείς να εντοπίσεις μια απάτη;

Στο διαδίκτυο, δεν μπορούμε να είμαστε πάντα σίγουροι ότι οι άνθρωποι είναι αυτοί που λένε ότι είναι. Αν συνειδητοποιήσετε ότι υπάρχουν απατεύונες στο διαδίκτυο είναι ένα από τα πιο σημαντικά πράγματα που μπορείτε να κάνετε για τους αποφύγετε. Όταν μάθετε τα κόλπα τους, θα πρέπει να είναι ευκολότερο να εντοπίσετε μια απάτη όταν τη δείτε.



Απάτες με ηλεκτρονικό "ψάρεμα"

Οι απάτες με ηλεκτρονικό "ψάρεμα" (Phishing) είναι η συνηθέστερη μορφή απάτης στο διαδίκτυο. Μπορεί να φαίνονται ότι είναι από κάποιον αξιόπιστο οργανισμό και είναι σχεδιασμένες να σας εξαπατήσουν για να δώσετε τα προσωπικά σας στοιχεία όπως τραπεζικός λογαριασμός, αριθμός της πιστωτικής κάρτας, όνομα χρήστη και κωδικούς πρόσβασης.

Μπορεί να εμφανιστούν σε πολλές μορφές:

- απροσδόκητα email, γραπτά μηνύματα ή τηλεφωνικές κλήσεις που σας ζητούν να επιβεβαιώσετε, να ενημερώσετε ή να καταχωρίσετε ξανά τα προσωπικά σας στοιχεία
- επείγοντα ή απειλητικά μηνύματα που σας λένε κάτι περίεργο συμβαίνει με το λογαριασμό σας ή ότι ο λογαριασμός σας θα κλείσει ώστε να αναγκαστείτε να κάνετε κλικ σ' ένα σύνδεσμο για να το διορθώσετε
- απροσδόκητα email που σας ζητάνε να ανοίξετε ή να κατεβάσετε κάποιο αρχείο σε μορφή '.exe' ή '.zip'.

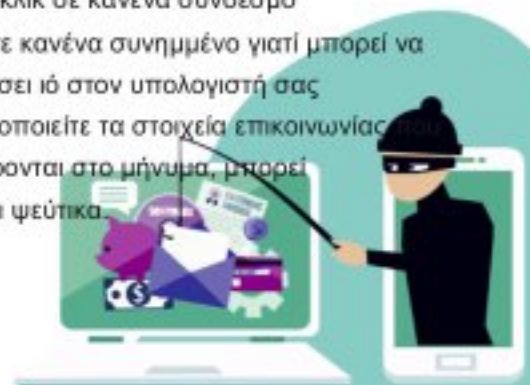
Χρήσιμη συμβουλή: Εάν δεν είστε σίγουροι για ένα μήνυμα που λάβατε, κάντε μια αναζήτηση στο διαδίκτυο για την εταιρεία που φαίνεται ότι έστειλε το μήνυμα και επικοινωνήστε απευθείας με την εταιρεία αυτή.

Μη βιάζεστε. Ξαναδιαβάστε το μήνυμα.

- Ποιος είναι ο αποστολέας; Είναι μια επίσημη διεύθυνση email ή μια περίεργη διεύθυνση;
- Σε ποιον απευθύνεται; Να υποπτευθείτε ότι κάτι συμβαίνει αν γράφει «Αγαπητέ πελάτη» αντί το όνομά σας.
- Είναι κακογραμμένο με ορθογραφικά λάθη; Αυτό μπορεί να είναι ένα σημάδι ότι το έχει στείλει κάποιος απατεύοντας.

Μην:

- κάνετε κλικ σε κανένα σύνδεσμο
- ανοίγετε κανένα συνημμένο γιατί μπορεί να κατεβάσει ιό στον υπολογιστή σας
- χρησιμοποιείτε τα στοιχεία επικοινωνίας αναφέρονται στο μήνυμα, μπορεί να είναι ψεύτικα.





Απάτες που αφορούν την Εφορία (ΑΑΔΕ)

Οι απατεώνες μιμούνται την Εφορία (ΑΑΔΕ) και άλλους κρατικούς οργανισμούς για να πάρουν χρήματα και προσωπικά στοιχεία από θύματα μέσω ψεύτικων ιστότοπων, email, γραπτών μηνυμάτων και τηλεφωνικών κλήσεων.

Είναι σημαντικό να θυμάστε ότι η Ανεξάρτητη Αρχή Δημοσίων Εσόδων (ΑΑΔΕ) δεν πρόκειται ποτέ:

- να σας στείλει email ή γραπτό μήνυμα για να ζητήσει τα προσωπικά σας στοιχεία, συμπεριλαμβανομένου του Αριθμού Φορολογικού Μητρώου (ΑΦΜ), της πιστωτικής κάρτας ή των τραπεζικών σας στοιχείων
- να σας ζητήσει να πληρώσετε μια χρέωση για να πάρετε την επιστροφή του φόρου σας ή να αποφύγετε τη σύλληψή σας για φοροδιαφυγή
- να σας στείλει email με έναν σύνδεσμο για μια διαδικτυακή υπηρεσία που ζητάει τα προσωπικά σας στοιχεία
- να στείλει αρχεία που μπορείτε να κατεβάσετε ή να σας δώσει οδηγίες για να εγκαταστήσετε κάποιο λογισμικό.

Τι μπορείτε να κάνετε για να είστε ενήμεροι και ασφαλείς;

- Μην κάνετε κλικ σε οποιονδήποτε σύνδεσμο και μην κατεβάζετε κανένα συνημμένο.
- Μη δίνετε προσωπικά στοιχεία όπως ο αριθμός του φορολογικού σας μητρώου (ΑΦΜ), η ημερομηνία γέννησής σας, ο τραπεζικός σας λογαριασμός ή τα στοιχεία της πιστωτικής σας κάρτας.
- Εάν δεν είστε βέβαιοι αν ένα τηλεφωνικό μήνυμα είναι πραγματικό, μην χρησιμοποιήσετε τα στοιχεία επικοινωνίας που παρέχονται, αλλά κάντε μια αναζήτηση στο διαδίκτυο για τον αριθμό του οργανισμού.
- Να είστε ενήμεροι για την κατάσταση των φορολογικών υποθέσεών σας - υπάρχει πιθανότητα να σας επιστραφεί φόρος ή να χρωστάτε κάποια πληρωμή;
- Συνδεθείτε με τον επίσημο λογαριασμό σας στο Gov.gr πληκτρολογώντας τη διεύθυνση μόνοι σας αντί να κάνετε κλικ σε κάποιον σύνδεσμο.
- Ελέγξτε αν το email που λάβατε προέρχεται από πραγματική διεύθυνση της Εφορίας που λήγει σε @aade.gr
- Ακόμα κι αν φαίνεται ότι βρίσκεστε σε ιστοσελίδα της Εφορίας ή Gov.gr, ελέγξτε αν η διεύθυνση τελειώνει σε .gov.gr (αντί για παράδειγμα .com.gr, .org.gr ή .net.gr).
- Κοιτάξτε αν είναι κακογραμμένο με ορθογραφικά λάθη.
- Να υποπτευθείτε ότι κάτι συμβαίνει αν δεν απευθύνετε σε εσάς προσωπικά.





Απάτες που αφορούν γνωριμίες και ειδύλλια

Οι απατεώνες δημιουργούν ψεύτικα διαδικτυακά προφίλ στα μέσα κοινωνικής δικτύωσης ή ιστοσελίδες γνωριμιών για να έρθουν σε επαφή με τα θύματα. Σκοπός τους είναι να κερδίσουν την εμπιστοσύνη σας πριν σας ζητήσουν χρήματα.

Τι μπορείτε να κάνετε για να είστε ενήμεροι και ασφαλείς;

Προσέχετε για:

- άτομα που εκφράζουν πολύ γρήγορα τη βαθιά αγάπη τους για εσάς πριν σας ζητήσουν χρήματα ή "δάνειο"
- άτομα που αποφεύγουν να σας συναντήσουν προσωπικά και βρίσκουν δικαιολογίες για το λόγο που δεν μπορούν να ταξιδέψουν να σας δουν
- άτομα των οποίων το προφίλ στο διαδίκτυο δεν ταιριάζει με αυτά που σας έχουν πει για τον εαυτό τους.

Τι πρέπει να κάνετε:

- ελέγξτε εάν οι φωτογραφίες τους είναι πραγματικά δικές τους ή αν τις έχουν πάρει από κάπου αλλού στο διαδίκτυο κάνοντας μια αναζήτηση φωτογραφιών στο Google. Πηγαίστε στο images.google.com και κάντε κλικ στο εικονίδιο της κάμερας
- να υποπτευθείτε ότι κάτι συμβαίνει όταν αρχίζουν να αναφέρουν για οικονομικά προβλήματα ή χρειάζονται χρήματα για μια «έκτακτη» ανάγκη.

Μην:

- μεταφέρετε οποιαδήποτε χρήματα σε κάποιον που έχετε μιλήσει μόνο μέσω τηλεφώνου ή email
- στείλετε προσωπικά στοιχεία όπως ημερομηνία γέννησης, στοιχεία της τράπεζας ή της πιστωτικής σας κάρτας.

Απάτες που αφορούν τεχνική υποστήριξη

Αυτές οι απάτες συνήθως αρχίζουν με μια κλήση ή email που φαίνεται να προέρχεται από έναν μεγάλο, γνωστό οργανισμό που σας λέει ότι έχετε πρόβλημα με τον υπολογιστή ή το διαδίκτυο και μπορούν να το διορθώσουν.

Τι μπορείτε να κάνετε για να είστε ενήμεροι και ασφαλείς;

- Μην παρέχετε απομακρυσμένη πρόσβαση στον υπολογιστή σας.
- Μην τους δίνετε προσωπικά στοιχεία, όπως στοιχεία για τον τραπεζικό λογαριασμό ή την πιστωτική κάρτα σας.
- Μην αγοράζετε λογισμικό από αυθαίρετη κλήση ή email.
- Αγνοήστε τα αναδυόμενα μηνύματα που σας λένε να καλέσετε για τεχνική υποστήριξη.



Οι μεγάλοι οργανισμοί αναμένουν από εσάς να καλέσετε όταν έχετε κάποιο πρόβλημα με το διαδίκτυο ή τον υπολογιστή σας. Δεν σας καλούν αυτοί.



ΔΡΑΣΕΙΣ ΨΗΦΙΑΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ
& ΨΗΦΙΑΚΟΥ ΕΓΓΡΑΜΜΑΤΙΣΜΟΥ
ΣΤΗΝ ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ

WEBINARS ΓΙΑ ΓΟΝΕΙΣ - ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ - ΠΟΛΙΤΕΣ

 tinyurl.com/atticadigital  [digitalattiki](https://www.facebook.com/digitalattiki)

Βοήθεια, υποπτεύομαι ότι με εξαπάτησαν

Εάν νομίζετε ότι έχετε πέσει θύμα απάτης, μη ντρέπεστε και να μην το κρατάτε μυστικό. Μπορείτε να λάβετε μέτρα για να διορθώσετε το πρόβλημα:

- επικοινωνήστε με την τράπεζά σας και σταματήστε τυχόν περαιτέρω πληρωμές στον απατεώνα
- καταγγείλετε την απάτη στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στο [ΚΑΤΑΝΑΛΩΤΕΣ – CYBERALERT](https://www.katanaalotes.gr) όπου μπορούν να σας βοηθήσουν με περαιτέρω συμβουλές
- ενημερώστε τους άλλους. Αν υπάρχει κάποιος άλλος που γνωρίζετε ότι μπορεί να έχει πέσει θύμα, ενημερώστε τον.

Εάν δεν είστε σίγουροι ότι το μήνυμα που λάβατε είναι πραγματικά από την Εφορία, ή έχετε πέσει θύμα απάτης φοροδιαφυγής, καλέστε την **Άμεση Γραμμή στο 11188**.

Φροντίστε να είστε ενημερωμένοι για τις απάτες που αφορούν την Εφορία πηγαίνοντας στο λογιστή σας.

Αν ανησυχείτε ότι τα προσωπικά σας στοιχεία έχουν εκτεθεί και χρησιμοποιηθεί καταχρηστικά, επικοινωνήστε με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα **ΑΠΔΠΧ** στο site [| Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα \(dpa.gr\)](https://www.dpa.gr)

Να θυμάστε ότι:

Πάντα υπάρχει κάποιος που μπορεί να σας βοηθήσει - είτε είναι τα στελέχη στο [ΚΑΤΑΝΑΛΩΤΕΣ – CYBERALERT](https://www.katanaalotes.gr), κάποιος τεχνογνώστης φίλος ή μέλος της οικογένειας, ή ακόμα κι ένας σύλλογος χρηστών υπολογιστών στην περιοχή σας.

Σκοπός των απατεώνων είναι να αξιοποιήσουν τον καλό σας χαρακτήρα, αλλά το διαδίκτυο μπορεί να είναι ένα ασφαλές μέρος για εξερεύνηση εάν είστε προσεκτικοί σχετικά με την ανταλλαγή προσωπικών στοιχείων στο διαδίκτυο, να χρησιμοποιείτε την κοινή λογική για το πού στέλνετε χρήματα και σε ποιον και να είστε πάντοτε προσεκτικοί.



ΔΡΑΣΕΙΣ ΨΗΦΙΑΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ
& ΨΗΦΙΑΚΟΥ ΕΓΓΡΑΜΜΑΤΙΣΜΟΥ
ΣΤΗΝ ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ

Αφιερώστε χρόνο για να ανακαλύψετε τον Ψηφιακό Εγγραμματισμό

Οι δράσεις Ψηφιακής Εκπαίδευσης είναι ένας ολοκληρωμένος θεματικός κύκλος με δωρεάν ενημερωτικό υλικό ειδικά σχεδιασμένο για να βοηθάει ενήλικες να συνδέονται με ασφάλεια στο διαδίκτυο και να περιηγηθούν με σιγουριά στον ψηφιακό κόσμο. Ο ιστότοπος είναι επίσης χρήσιμος για οικογένειες και κοινοτικούς συλλόγους που θέλουν να βοηθήσουν τα ενήλικα μέλη να έχουν πρόσβαση σε όλα τα οφέλη του διαδικτύου.



ΠΕΡΙΦΕΡΕΙΑΚΟ
ΤΑΜΕΙΟ
ΑΝΑΠΤΥΞΗΣ
ΑΤΤΙΚΗΣ



Ευρωπαϊκή Ένωση
Κοινωνία της
Γνώσης και της
Πολιτιστικής Ανάπτυξης



ΠΕΡΙΦΕΡΕΙΑΚΟ
ΕΠΙΧΕΙΡΗΣΙΑΚΟ
ΠΡΟΓΡΑΜΜΑ
ΑΤΤΙΚΗΣ



ΕΣΠΑ
2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



Προστατευθείτε από τις απάτες

Απάτη είναι μια ανέντιμη ή παράνομη δραστηριότητα που εξαπατά τους ανθρώπους να δώσουν χρήματα, προσωπικά στοιχεία, προσωπικές φωτογραφίες ή κάτι άλλο αξίας. Μια διαδικτυακή απάτη συνήθως διαπράττεται από κάποιον με ψεύτικο προφίλ ή ψεύτικη επιχείρηση. Έτσι ενώ το διαδίκτυο μπορεί να είναι ένα θαυμάσιο μέρος για εξερεύνηση και είναι χρήσιμο, πρέπει να είστε προσεκτικοί!

Αν συνειδητοποιήσετε ότι υπάρχουν απατεώνες είναι ένα από τα πιο σημαντικά πράγματα που μπορείτε να κάνετε για τους αποφύγετε. Όταν μάθετε τα κόλπα τους, είναι πιθανότερο να εντοπίσετε μια απάτη. Η συνεχής προσοχή είναι η καλύτερη άμυνά σας.

Διαβάστε παρακάτω μερικές πολύ χρήσιμες συμβουλές για να αναγνωρίζετε και να αποφεύγετε τις απάτες.



Προστατέψτε τα προσωπικά σας στοιχεία

Οι απατεώνες προσπαθούν να πάρουν τα προσωπικά σας στοιχεία κάνοντάς σας ερωτήσεις ή δίνοντάς σας οδηγίες από το τηλέφωνο, email, γραπτό μήνυμα ή από τα μέσα κοινωνικής δικτύωσης. Οι απατεώνες θα χρησιμοποιήσουν τα προσωπικά σας στοιχεία για να κλέψουν τα χρήματά σας ή να διαπράξουν κάποια άλλη παράνομη πράξη.

Τι ζητούν οι απατεώνες;

Οι απατεώνες προσπαθούν να κερδίσουν την εμπιστοσύνη σας προσποιούμενοι ότι είναι από κάποιον γνωστό οργανισμό ή υπηρεσία όπως ΑΑΔΕ, Εθνική ή άλλη Τράπεζα, Microsoft, Ελληνικά Ταχυδρομεία, Εφορία, Αστυνομία ή Υπηρεσίες της Ελλάδας (Gov.gr).

Για να σας εξαπατήσουν να δώσετε τα προσωπικά ή οικονομικά στοιχεία σας, οι απατεώνες μπορεί:

- να σας πείσουν να κάνετε κλικ σε έναν σύνδεσμο
- να σας ζητήσουν να τους δώσετε απομακρυσμένη πρόσβαση στον υπολογιστή σας
- να σας ζητήσουν να πληρώσετε κάποιο χρέος
- να σας ζητήσουν να αγοράσετε κάποιο κουπόνι για να πληρώσετε ένα πρόστιμο
- να σας ζητήσουν να μεταφέρετε ή να στείλετε χρήματα στο εξωτερικό.

Ενδείξεις ότι μπορεί να είναι απάτη

Να προσέχετε:

- email, μηνύματα ή κλήσεις που δεν τα περιμένατε ή έρχονται από κάποιον που δεν γνωρίζετε
- υποσχέσεις για οικονομικό όφελος
- απειλές για επιβολή προστίμου ή χρέους
- απειλές να κλείσουν ή να "κλειδώσουν" τον λογαριασμό σας
- σύνδεσμοι που δεν φαίνονται γνήσιοι, όπως αν έχει ασυνήθιστη διεύθυνση ιστοσελίδας
- μια ασυνήθιστη αίσθηση επείγουσας ανάγκης ή προθεσμίας.

Χρήσιμη Συμβουλή: Εάν δεν είστε βέβαιοι αν ένα γραπτό μήνυμα ή κλήση είναι γνήσια, μην χρησιμοποιήσετε τα στοιχεία επικοινωνίας που παρέχονται, αλλά κάντε μια αναζήτηση στο διαδίκτυο για τον αριθμό ή email του οργανισμού.



Να είστε προσεκτικοί για φίλους που κάνετε στο διαδίκτυο

Οι διαδικτυακοί απατεώνες έρχονται συχνά σε επαφή με άτομα μέσω των μέσων κοινωνικής δικτύωσης. Χρησιμοποιούν την τακτική τους με απάτες που αφορούν ειδήλλια και γνωριμίες. Στοχεύουν επίσης άτομα που παίζουν παιχνίδια στο διαδίκτυο όπως Words with Friends και Scrabble. Στόχος τους είναι να δημιουργήσουν μια σχέση (δεν χρειάζεται να είναι ρομαντική) για να κερδίσουν την εμπιστοσύνη σας για να μπορέσουν να σας ζητήσουν χρήματα, προσωπικά στοιχεία, προσωπικές φωτογραφίες ή κάτι άλλο αξίας.

Ενδείξεις ότι μπορεί να είναι απάτη

Προσέχετε για άτομα τα οποία:

- εκφράζουν γρήγορα μια βαθιά τρυφερότητα
- προσπαθούν να μεταφέρουν τη συνομιλία σας από το διαδίκτυο όπου συναντηθήκατε σε ένα πιο προσωπικό κανάλι επικοινωνίας, όπως με απευθείας μηνύματα ή email
- σας λένε περίτεχνες ιστορίες για οικονομικά προβλήματα
- λένε ότι θέλουν να σας συναντήσουν αλλά προβάλλουν δικαιολογίες ή ζητούν χρήματα για να μπορέσουν να «ταξιδέψουν» ώστε να σας συναντήσουν
- ρωτάνε για την οικονομική σας κατάσταση
- γίνονται επίμονοι, πιο άμεσοι ή ακόμα και επιθετικοί όταν δεν στέλνετε χρήματα
- φαίνεται ότι έχουν ασυνέπειες στο διαδικτυακό τους προφίλ - για παράδειγμα, η φωτογραφία τους δεν μοιάζει με την περιγραφή που δίνουν για τον εαυτό τους ή λένε ότι έχουν σπουδάσει στο πανεπιστήμιο αλλά η γραμματική τους είναι κακή.

Είναι επίσης συνηθισμένο για τους απατεώνες να παρουσιάζονται ως εργαζόμενοι σε φιλανθρωπικά ιδρύματα ή προσποιούνται ότι είναι στρατιωτικό προσωπικό ή επαγγελματίες που εργάζονται στο εξωτερικό.

Χρήσιμη συμβουλή: Κάντε μια αναζήτηση φωτογραφίας σε ορισμένες ιστοσελίδες όπως Google (images.google.com) ή TinEye (tineye.com), για να σας βοηθήσει να ελέγξετε αν το άτομο είναι αυτό που λέει ότι είναι.

Πώς να προστατευθείτε

- Μη δίνετε προσωπικά ή οικονομικά στοιχεία σε άτομα που δεν έχετε συναντηθεί ποτέ προσωπικά.
- Μην κάνετε πληρωμές με χρηματική εντολή,

- τραπεζικό έμβασμα, διεθνή μεταφορά χρημάτων ή ηλεκτρονικό νόμισμα όπως το bitcoin. (Είναι δύσκολο να πάρετε πίσω χρήματα που στάλθηκαν με αυτόν τον τρόπο εάν αποδειχθεί ότι είναι απάτη.)
- Μην συμφωνείτε να μεταφέρετε πακέτα στο εξωτερικό ή να μεταφέρετε χρήματα για κάποιον άλλο, επειδή μπορεί να διαπράττετε παράνομη πράξη χωρίς να το γνωρίζετε.
- Μην ανταλλάσσετε προσωπικές φωτογραφίες και μην χρησιμοποιείτε κάμερες σε προσωπικό περιβάλλον.
- Διακόψτε κάθε επικοινωνία εάν το άτομο αρχίσει να σας ζητάει κάποια χάρη ή χρήματα.
- Να έχετε υποψίες αν βλέπετε ορθογραφικά λάθη, κακή γραμματική και ασυνέπειες στις ιστορίες.





Προσέχετε τις απάτες που αφορούν επενδύσεις

Οι απατεώνες με επενδύσεις αφιερώνουν πολύ χρόνο, προσπάθεια και χρήματα για να δημιουργήσουν πειστικές ιστορίες, φανταχτερούς ιστότοπους και προσεγμένα φυλλάδια για να εξαπατήσουν ενήλικες που θέλουν να αυξήσουν τις «οικονομίες τους για τα γηρατεία τους» ή τις αποταμιεύσεις τους.

Πώς καταφέρνουν οι απατεώνες να σας κάνουν να δείξετε ενδιαφέρον;

Αυτές είναι μερικές από τις μεθόδους που χρησιμοποιούν οι απατεώνες με επενδύσεις:

- Σας καθοδηγούν σε ψεύτικη ιστοσελίδα που κάνει ψευδείς δηλώσεις για επενδύσεις με πολλή καλή απόδοση και πολλά κέρδη.
- Αναρτούν μια διαφήμιση ή άρθρο σε ιστοσελίδα μέσω κοινωνικής δικτύωσης όπως το Facebook.
- Σας στέλνουν ένα αίτημα «φιλίας» στα μέσα κοινωνικής δικτύωσης προσποιούμενοι ότι είναι κάποιος που γνωρίζετε ή έχετε διασυνδεθεί, προκειμένου να έχουν πρόσβαση στα στοιχεία του προφίλ σας και σας στέλνουν εξατομικευμένες προσφορές για επένδυση.

Ενδείξεις ότι μπορεί να είναι απάτη

- Ο απατεώνας σας τηλεφωνάει ή σας στέλνει email συνεχώς.
- Μεταβιβάζουν την κλήση σας ιεραρχικά - πρώτα σας μιλάει ένα κατώτερο στέλεχος και μετά ένα πιο ανώτερο στέλεχος προσπαθεί να κλείσει τη συμφωνία.
- Σας πιέζουν να ενεργήσετε γρήγορα γιατί διαφορετικά θα χάσετε την ευκαιρία.

- Λένε ότι δεν έχουν ελληνική άδεια παροχής χρηματοοικονομικών υπηρεσιών ή ότι δεν χρειάζονται άδεια.
- Προσπαθούν να σας σταματήσουν να μην αποσυρθείτε από τη συμφωνία.



Συνταξιοδοτική ασφάλεια

Οι απατεώνες με επενδύσεις προσφέρουν γρήγορους και εύκολους τρόπους για να πάρετε πιο νωρίς τη σύνταξή σας. Μπορεί να σας ζητήσουν να συμφωνήσετε σε μια ιστορία για να διασφαλίσουν την πρόωρη αποδέσμευση των χρημάτων σας και στη συνέχεια, ενεργώντας ως ο οικονομικός σας σύμβουλος, εξαπατούν το ασφαλιστικό σας ταμείο για να μεταβιβάσουν τα χρήματα της συνταξιοδοτικής σας ασφάλειας απευθείας σε αυτούς.

Μόλις πάρει τα χρήματά σας, ο απατεώνας μπορεί να πάρει μια μεγάλη «προμήθεια» από τα αποδεσμευμένα χρήματα ή να μην αφήσει τίποτα για εσάς.



Προσοχή! Συνήθως δεν μπορείτε να πάρετε νόμιμα στο δεσμευμένο τμήμα της σύνταξής σας έως ότου είστε μεταξύ 60 και 65 ετών, ανάλογα το έτος που γεννηθήκατε. Υπάρχουν ορισμένες εξαιρέσεις όπως σοβαρές οικονομικές δυσκολίες ή παρηγορητικοί λόγοι - αλλά σε αντίθετη περίπτωση αν κάποιος προσφέρει πρόωρη πρόσβαση στη σύνταξή σας τότε ενεργεί παράνομα.



**ΔΡΑΣΕΙΣ ΨΗΦΙΑΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ
& ΨΗΦΙΑΚΟΥ ΕΓΓΡΑΜΜΑΤΙΣΜΟΥ
ΣΤΗΝ ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ**

WEBINARS ΓΙΑ ΓΟΝΕΙΣ - ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ - ΠΟΛΙΤΕΣ

tinyurl.com/atticadigital  digitalattiki

Τεχνητή διόγκωση της τιμής μιας μετοχής

Οι απατεώνες με επενδύσεις αγοράζουν μετοχές σε μια μικρή εταιρεία σε χαμηλή τιμή και μετά στέλνουν ψευδείς συμβουλές για την εταιρεία ότι έχει μεγάλες προοπτικές. Καθώς όλο και περισσότεροι άνθρωποι επενδύουν, η τιμή της μετοχής αυξάνεται και οι απατεώνες πωλούν τις μετοχές τους όταν είναι στο ανώτερο σημείο αύξησης της τιμής. Μετά η τιμή της μετοχής πέφτει και οι μέτοχοι υποχρεούνται να κρατήσουν τη μετοχή στη μειωμένη αξία.

Απάτες με την έγκριση διασημοτήτων

Οι απατεώνες με επενδύσεις χρησιμοποιούν ψεύτικες εγκρίσεις από επιτυχημένους και αξιόπιστους επιχειρηματίες ή διασημότητες σε μια προσπάθεια να παρασύρουν τους ανθρώπους να πιστέψουν ότι το πλάνο υποστηρίζεται από κάποιον που εμπιστεύονται. Αυτές οι απάτες εμφανίζονται συχνά ως διαφημίσεις στο διαδίκτυο ή διαφημιστικές καμπάνιες σε αναρτήσεις στα μέσα κοινωνικής δικτύωσης ή φαινομενικά νόμιμοι, αξιόπιστοι ιστότοποι.

Πώς να προστατευθείτε

- Να υποπτευθείτε ότι κάτι συμβαίνει όταν ακούτε για ευκαιρίες που φαίνονται πολύ καλές για να είναι αληθινές.
- Να υποπτευθείτε ότι κάτι συμβαίνει όταν ακούτε για διαφημίσεις ή ιστορίες που τις έχουν εγκρίνει διασημότητες.
- Μην αφήνετε κανέναν να σας πιέσει.
- Εάν είστε κάτω των 60 ετών, να προσέχετε τις προσφορές που προωθούν την εύκολη πρόσβαση στη σύνταξη σας.
- Κάντε την έρευνά σας και ψάξτε για αξιόπιστες ή ανεξάρτητες οικονομικές ή νομικές συμβουλές.

- Μη δίνετε προσωπικά ή οικονομικά στοιχεία έως ότου:
 - ελέγξετε στην ιστοσελίδα [Αναζήτηση Βασικών Στοιχείων Μητρώου Επιχειρήσεων | ΑΑΔΕ \(aade.gr\)](#) εάν ο οικονομικός σύμβουλος και η εταιρεία που εργάζεται έχουν άδεια.
 - ελέγξετε τη λίστα των εταιρειών που διατηρεί η ΑΑΔΕ στη σελίδα [Επιχειρήσεις | ΑΑΔΕ \(aade.gr\)](#).

Βοήθεια, υποπτεύομαι ότι έπεσα θύμα απάτης

Αν νομίζετε ότι πέσατε θύμα απάτης, μη ντρέπεστε και μην το κρατάτε μυστικό. Μπορείτε να λάβετε μέτρα για να διορθώσετε το πρόβλημα:

- Επικοινωνήστε με την τράπεζά σας και σταματήστε τυχόν περαιτέρω πληρωμές στον απατεώνα.
- Επικοινωνήστε με την ΑΠΔΠΧ εάν έχει γίνει παραβίαση ή κατάχρηση των προσωπικών σας στοιχείων.
- Για οποιοσδήποτε απάτες που αφορούν το Gov.gr, καλέστε τη Δίωξη Ηλεκτρονικού Εγκλήματος στο 1188 ή στείλτε email στο ccu@cybercrimeunit.gov.gr
- Καταγγείλετε την απάτη στην Ένωση Καταναλωτών - Η Ποιότητα Της Ζωής | Ε.Κ.ΠΟΙ.ΖΩ. | (ekpizo.gr) για να ενημερώσουν τους άλλους ώστε να αποφύγουν αυτή την απάτη.

Για να είστε ενημερωμένοι σχετικά με τις πιο πρόσφατες απάτες που πρέπει να αποφεύγετε, επισκεφθείτε το [Url Scanner to Detect Phishing in Real-time | CheckPhish](#)

Αφιερώστε χρόνο για να ανακαλύψετε τον Ψηφιακό Εγγραμματισμό

Οι δράσεις Ψηφιακής Εκπαίδευσης είναι ένας ολοκληρωμένος θεματικός κύκλος με δωρεάν ενημερωτικό υλικό ειδικά σχεδιασμένο για να βοηθάει ενήλικες να συνδέονται με ασφάλεια στο διαδίκτυο και να περιηγηθούν με σιγουριά στον ψηφιακό κόσμο. Ο ιστότοπος είναι επίσης χρήσιμος για οικογένειες και κοινοτικούς συλλόγους που θέλουν να βοηθήσουν τα ενήλικα μέλη να έχουν πρόσβαση σε όλα τα οφέλη του διαδικτύου.



**ΔΡΑΣΕΙΣ ΨΗΦΙΑΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ
& ΨΗΦΙΑΚΟΥ ΕΓΓΡΑΜΜΑΤΙΣΜΟΥ
ΣΤΗΝ ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ**



ΠΕΡΙΦΕΡΕΙΑΚΟ
ΤΑΜΕΙΟ
ΑΝΑΠΤΥΞΗΣ
ΑΤΤΙΚΗΣ



Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο
Περιφερειακής Ανάπτυξης



ΠΕΡΙΦΕΡΕΙΑΚΟ
ΕΠΙΧΕΙΡΗΣΙΑΚΟ
ΠΡΟΓΡΑΜΜΑ
ΑΤΤΙΚΗΣ



ΕΣΠΑ
2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης