ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το διαδίκτυο είναι μια τεράστια πηγή πληροφοριών. Προσφέρει γρήγορα και εύκολα πλούσιο οπτικοακουστικό υλικό. Με ένα κλικ μπορείς να έχεις μπροστά στην οθόνη σου σχεδόν όποια πληροφορία θέλεις. Κρύβει όμως και πολλούς κινδύνους, γι' αυτό χρειάζεται μεγάλη προσοχή.

Σκοπός της ενημέρωσης αυτής, είναι να ενημερωθούν οι μαθητές/τριες και οι εκπαιδευτικοί προκειμένου να είναι σε θέση να βοηθήσουν τον εαυτό τους και τα παιδιά τους. (μιλάμε πάντοτε για ενήλικους μαθητές) .

Να αξιοποιήσουν με ασφάλεια τις σημαντικές δυνατότητες που προσφέρει το διαδίκτυο, και παράλληλα να μπορούν, να προστατεύσουν και τα παιδιά τους από τους κινδύνους που κρύβονται μέσα σε αυτό.

Η ασφάλεια στο Διαδίκτυο ή η **διαδικτυακή ασφάλεια** είναι η γνώση των κινδύνων προσωπικής ασφάλειας και ασφάλειας του χρήστη σε ιδιωτικές πληροφορίες και περιουσίες που σχετίζονται με τη χρήση του Διαδικτύου και την αυτοπροστασία από το ηλεκτρονικό έγκλημα.

Δεδομένου ότι ο αριθμός των χρηστών του Διαδικτύου συνεχίζει να αυξάνεται παγκοσμίως, διαδικτυακοί οργανισμοί, κυβερνήσεις και οι οργανισμοί εξέφρασαν ανησυχίες για την ασφάλεια των παιδιών που χρησιμοποιούν το Διαδίκτυο.

ΚΟΙΝΈΣ ΑΙΤΊΕΣ ΠΑΡΑΒΙΆΣΕΩΝ ΤΗΣ ΑΣΦΆΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΏΝ ΠΕΡΙΛΑΜΒΆΝΟΥΝ:


Microsoft
ΟΔΗΓΟΣ
Ασφαλούς
Χρήσης του
Διαδικτύου
για Γονείς και Παιδιά
Ο Φιλελεύθερος

1. Διαδικτυακές απάτες

Πρόκειται για προγράμματα που εξαπατούν τον χρήστη με διάφορους τρόπους, προσπαθώντας να εκμεταλλευτούν πληροφορίες του χρήστη. Οι απάτες στο Διαδίκτυο προσπαθούν να εξαπατήσουν το θύμα με πράγματα της προσωπικής ιδιοκτησίας παρά με προσωπικές πληροφορίες μέσω ψευδών υποσχέσεων, τεχνάσματα εμπιστοσύνης και πολλά άλλα.

Το κακόβουλο λογισμικό , ιδιαίτερα το **λογισμικό υποκλοπής spyware** , είναι κακόβουλο λογισμικό που μεταμφιέζεται ως λογισμικό που έχει σχεδιαστεί για τη συλλογή και τη μετάδοση ιδιωτικών πληροφοριών, όπως κωδικών πρόσβασης, χωρίς τη συγκατάθεση ή τη γνώση του χρήστη.

Συχνά διανέμεται μέσω ηλεκτρονικού ταχυδρομείου, από ανεπίσημες τοποθεσίες. Το κακόβουλο λογισμικό είναι ένα από τα πιο διαδεδομένα προβλήματα ασφαλείας, καθώς συχνά είναι αδύνατο να προσδιοριστεί εάν ένα αρχείο έχει μολυνθεί, ακόμα και αν είναι ασφαλής η πηγή του αρχείου.

Το ηλεκτρονικό "ψάρεμα" είναι ένας τύπος απάτης στον οποίο οι απατεώνες εμφανίζονται με ψεύτικα στοιχεία για την απόκτηση ιδιωτικών πληροφοριών, όπως κωδικών πρόσβασης, πληροφοριών πιστωτικών καρτών κ.λπ. μέσω του διαδικτύου.

Το ηλεκτρονικό "ψάρεμα" (phishing) συμβαίνει συχνά μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και άμεσων μηνυμάτων και μπορεί να περιέχει συνδέσμους σε ιστότοπους που κατευθύνουν τον χρήστη να εισαγάγει τις προσωπικές του πληροφορίες.

Αυτές οι ψεύτικες ιστοσελίδες είναι συχνά σχεδιασμένες ώστε να φαίνονται όμοιοι με τους νόμιμους ομολόγους τους, για να αποφεύγεται η υποψία από τον χρήστη.

Η **ηλεκτρονική παρενόχληση** είναι η επίθεση εναντίον ενός ατόμου ή μιας ομάδας μέσω της χρήσης ηλεκτρονικών μέσων όπως η άμεση ανταλλαγή μηνυμάτων, τα κοινωνικά δίκτυα, το ηλεκτρονικό ταχυδρομείο και άλλες μορφές ηλεκτρονικής επικοινωνίας με σκοπό την κατάχρηση, τον εκφοβισμό ή την υπερνίκηση.

Σε μια μελέτη του 2012 με περισσότερους από 11.925 φοιτητές στις Ηνωμένες Πολιτείες, αναφέρθηκε ότι το 23% των εφήβων ανέφερε ότι ήταν θύμα της παρενόχλησης στον κυβερνοχώρο, το 30% των οποίων ανέφερε ότι αντιμετώπιζε αυτοκτονική συμπεριφορά.

Οι κοινές απειλές για την **προσωπική ασφάλεια** περιλαμβάνουν: phishing, ηλεκτρονικές απάτες, κακόβουλο λογισμικό, cyberstalking, ηλεκτρονική παρενόχληση, online προσθήκες και σεξουαλικότητα.

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική, ταχύτατη και αξιόπιστη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο.

Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου.

Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και, μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών.

Ενοχλητική αλληλογραφία (spam mail)

Είναι το λεγόμενο spam ή junk mail, δηλαδή μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο.

Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ.ανεπιθύμητα newsletters).

Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.

Προστασία προσωπικών δεδομένων

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα.

Τα mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία.

Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού email. Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail , οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων

Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή").

ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΟΥΜΕ

Βεβαιωθείτε ότι κάθε ιστοσελίδα μέσω της οποίας αποστέλλετε προσωπικές πληροφορίες (κωδικοί πρόσβασης, αριθμό πιστωτικής κάρτας κ.α.) λειτουργεί με το πρωτόκολλο https. Αυτό σημαίνει ότι:

- η διεύθυνση αρχίζει με “https://” και
- αριστερά του “https://” υπάρχει ένα μικρό λουκέτο, που δηλώνει ότι η σύνδεση είναι ασφαλής και ότι η ιστοσελίδα διαθέτει ισχύον πιστοποιητικό (valid certificate).

Προσέξτε τα παραπλανητικά emails (phishing emails). Σε εισερχόμενο email που φαίνεται ύποπτο (π.χ. το όνομα του αποστολέα είναι άγνωστο, το περιεχόμενο εμφανίζει μία αίσθηση «επείγοντος», το email του αποστολέα δεν δείχνει νόμιμο) μην ανοίξετε το επισυναπτόμενο αρχείο και μην επισκεφθείτε το σύνδεσμο (link) που εμφανίζεται στο κείμενο του email.

Δώστε ιδιαίτερη προσοχή στο είδος των πληροφοριών της προσωπικής και επαγγελματικής σας ζωής που αναρτάτε στα κοινωνικά δίκτυα.

ΓΙΑ ΤΟ ΛΟΓΟ ΑΥΤΌ ΠΡΕΠΕΙ

- Να χρησιμοποιούμε ισχυρούς κωδικούς πρόσβασης παντού και πως να προστατεύουμε τους κωδικούς μας
- Τι είναι ο έλεγχος ταυτότητας πολλαπλών παραγόντων (2Factor Authentication) και πως να τον χρησιμοποιούμε

- Πως να προστατεύουμε τις συσκευές μας και τα αρχεία μας από το κακόβουλο λογισμικό
- Πως να κάνουμε ασφαλείς αγορές στο διαδίκτυο

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

1. Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

2. Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

3. Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

4. Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

ΑΣΦΑΛΗΣ ΠΑΡΟΥΣΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- Τα άτομα που γνωρίζετε στο Διαδίκτυο δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι. Μπορεί να σας λένε ψέματα για να κερδίσουν την εμπιστοσύνη σας.
- Μην δίνετε ποτέ τα προσωπικά σας στοιχεία, ούτε να αποκαλύπτετε σε άλλους χρήστες του Διαδικτύου πληροφορίες που αφορούν τους φίλους σας, την οικογένειά σας ή το σχολείο σας.

- Μην αποκαλύπτετε τους κωδικούς πρόσβασης (password) που χρησιμοποιείτε.
- Μην επιχειρείτε συναλλαγές μέσω του Διαδικτύου για την αγορά προϊόντων και μην δίνετε στοιχεία που αφορούν πιστωτικές κάρτες.

- Να είστε επιφυλακτικός/ή ως προς την αποδοχή όσων διαβάζετε στο Διαδίκτυο ή αυτών που σας λένε οι άλλοι χρήστες του, πριν το υποβάλετε στην κρίση σας.

- Συζητήστε με τους εκπαιδευτικούς σας, τους γονείς σας και με πρόσωπα που εμπιστεύεστε για τις δραστηριότητες σας στο Διαδίκτυο, ιδιαίτερα αν αντιμετωπίσετε οτιδήποτε περίεργο ή ασυνήθιστο.

- Να έχετε πάντα υπόψη σας ότι τα προϊόντα της πνευματικής δημιουργίας (μουσική, λογοτεχνία, κινηματογράφος, video κτλ.) προστατεύονται από τους νόμους και η διανομή τους μέσω του Διαδικτύου είναι παράνομη πράξη.

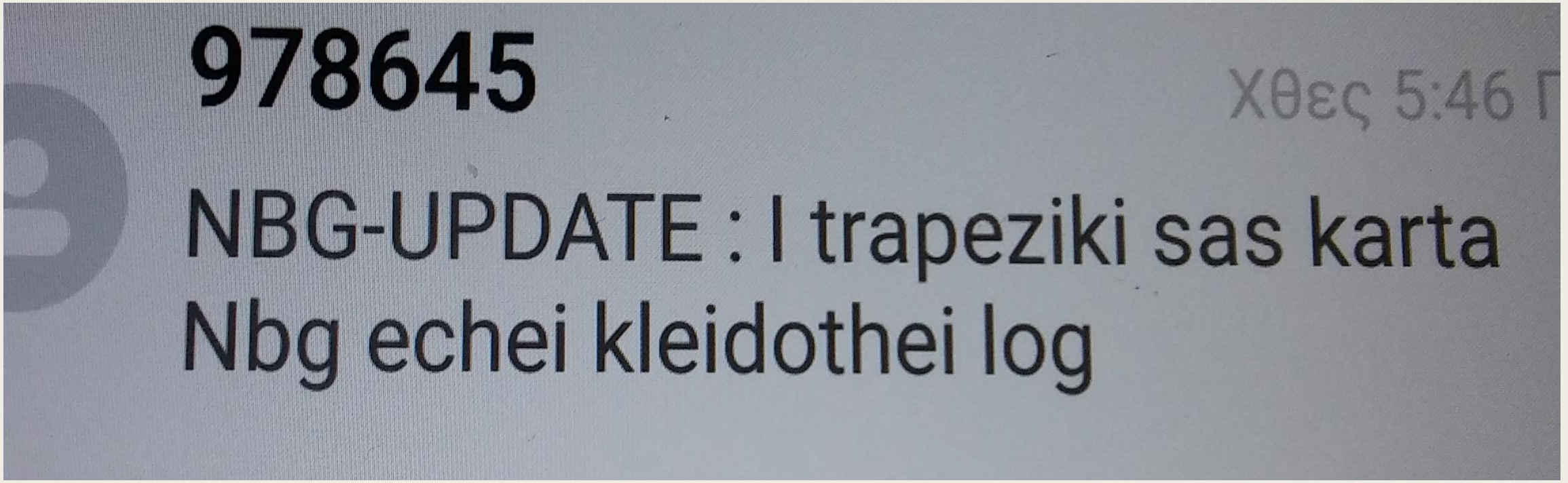
- Το ίδιο παράνομη πράξη θεωρείται και η διακίνηση προγραμμάτων υπολογιστών (Software), εκτός και αν ανήκουν στην κατηγορία του Ελεύθερου Λογισμικού (Open source software).

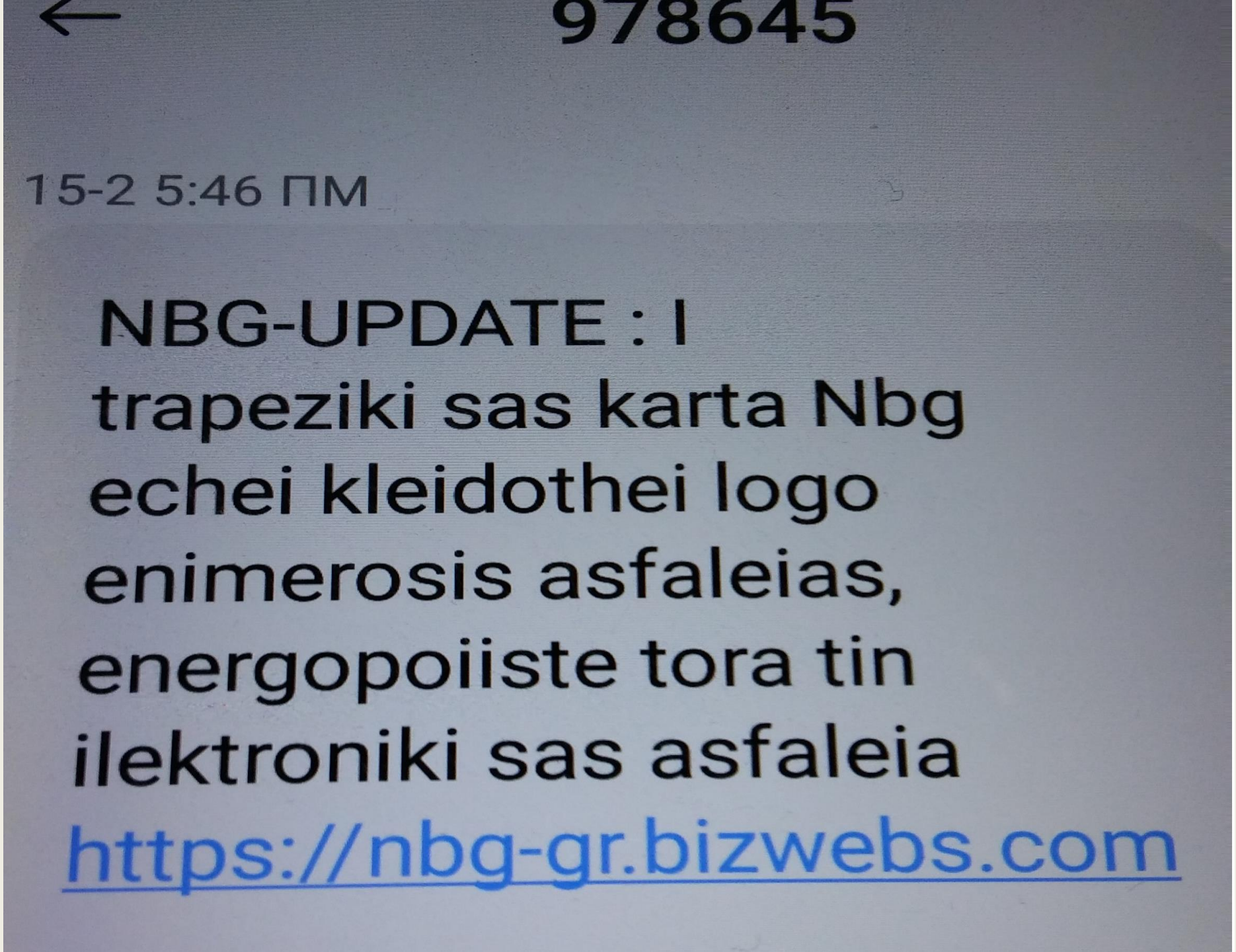
- Μην ανοίγετε μηνύματα e-mail και επισυναπτόμενα αρχεία από άγνωστους αποστολείς με περίεργα θέματα (subject) ή χωρίς θέμα. Είναι πολύ πιθανό να περιέχουν ιούς και να προκαλέσουν σοβαρά προβλήματα στον υπολογιστή σας.

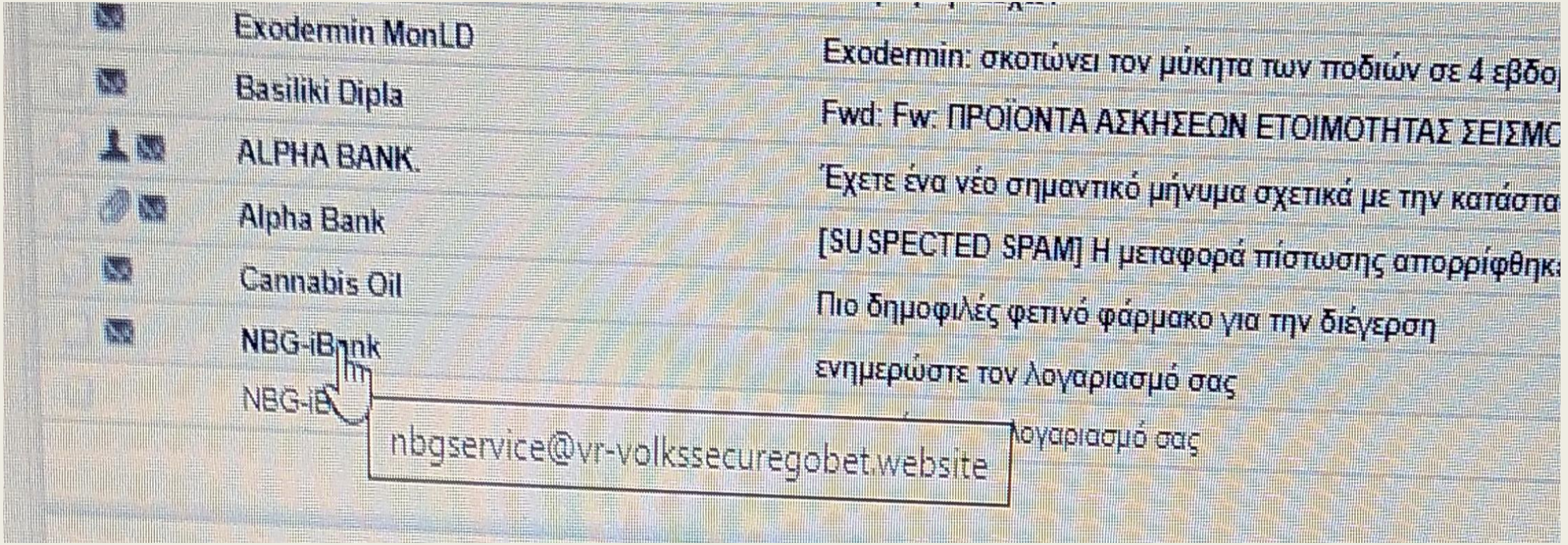
- Μην χρησιμοποιείτε οποιοδήποτε πρόγραμμα βρίσκετε στο Διαδίκτυο. Δεν είναι όλα τα προγράμματα ασφαλή, ακόμα και αν εμφανίζονται ως παιχνίδια

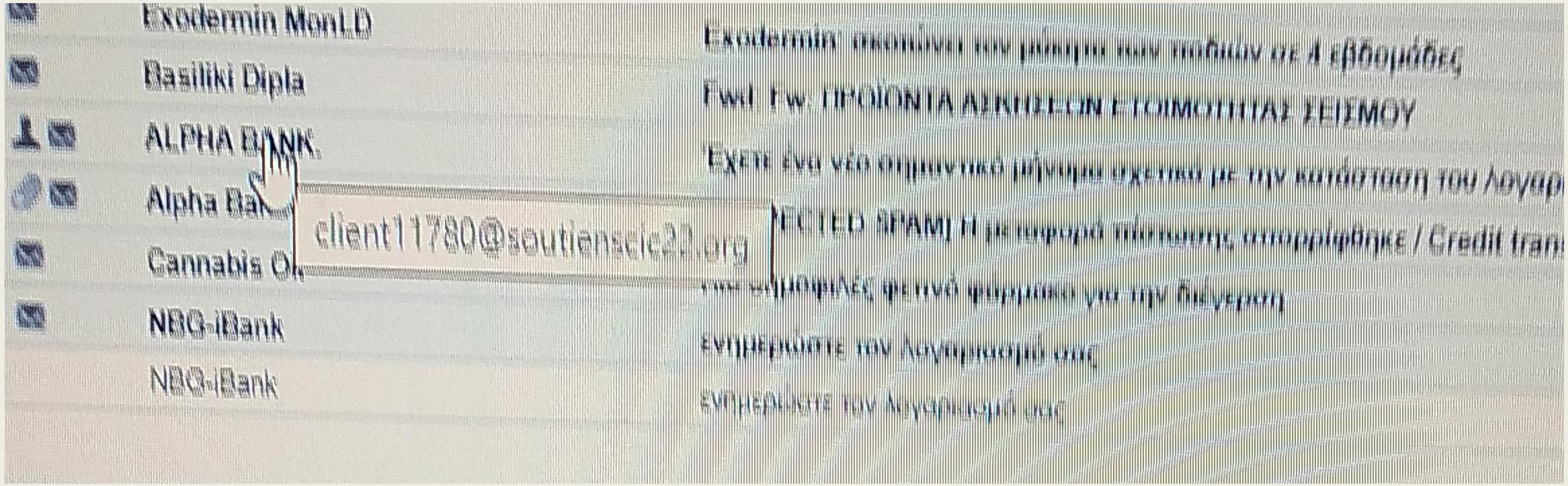
Στη διεύθυνση http://www.safeline.gr/ έχουμε ίσως τη μοναδική ελληνική ανοικτή γραμμή για καταγγελία παράνομου περιεχομένου στο διαδίκτυο. Μη διστάσετε να τη χρησιμοποιήσετε.

ΠΡΟΣΟΧΗ
ΤΑ ΠΑΡΑΚΑΤΩ ΜΗΝΥΜΑΤΑ ΕΧΟΥΝ ΣΚΟΠΟ ΤΗΝ ΥΠΟΚΛΟΠΗ ΔΕΔΟΜΕΝΩΝ


978645
Χθες 5:46 Π
NBG-UPDATE : I trapeziki sas karta
Nbg echei kleidothei log


978645
15-2 5:46 ΠΜ
NBG-UPDATE : I
trapeziki sas karta Nbg
echei kleidothei logo
enimerosis asfaleias,
energopoiiste tora tin
ilektroniki sas asfaleia
https://nbg-gr.bizwebs.com


Exodermin MonLD
Exodermin: σκοτώνει τον μύκητα των ποδιών σε 4 εβδο
Basiliki Dipla
Fwd: Fw: ΠΡΟΪΟΝΤΑ ΑΣΚΗΣΕΩΝ ΕΤΟΙΜΟΤΗΤΑΣ ΣΕΙΣΜΟ
ALPHA BANK.
Έχετε ένα νέο σημαντικό μήνυμα σχετικά με την κατάστα
Alpha Bank
[SUSPECTED SPAM] Η μεταφορά πίστωσης απορρίφθηκ
Cannabis Oil
Πιο δημοφιλές φετινό φάρμακο για την διέγερση
NBG-iBank
ενημερώστε τον λογαριασμό σας
NBG-iB
λογαριασμό σας
nbgservice@vr-volkssecuregobet.website


Exodermin MonLD
Basiliki Dipla
ALPHA BANK
Alpha Bank
client11780@soutiensecle20.org
Cannabis Oil
NBG-iBank
NBG-iBank

ΣΚΕΨΟΥ ΛΟΙΠΟΝ ΠΡΙΝ ΟΛΟΚΛΗΡΩΣΕΙΣ ΤΑ ΒΗΜΑΤΑ ΣΟΥ


Σκέψου πριν δημοσιεύσεις! Προστάτευσε την ιδιωτική ζωή, τη δική σου, της οικογένειάς σου, των φίλων σου.
Δεν είμαστε ανώνυμοι στο Διαδίκτυο. Όλοι αφήνουμε ηλεκτρονικά ίχνη!
Οι φίλοι που γνωρίζουμε μόνο μέσα από το Διαδίκτυο παραμένουν άγνωστοι!
Έλεγξε την εγκυρότητα της πληροφορίας στο Διαδίκτυο
Μην ξεχνάς να ζεις στον πραγματικό κόσμο για χάρη του Διαδικτύου
Ό,τι ανεβαίνει στο Διαδίκτυο, παραμένει εκεί για πάντα!


Download from
Dreamstime.com

ΠΗΓΕΣ

- **http://www.safeline.gr/**
- **https://eucpn.org/sites/default/files/document/files/thematic_paper_youth_internet_safety_0.pdf**
- **https://www.europol.europa.eu/about-europol**
- **https://wayback.archive-it.org/**
- **http://photodentro.edu.gr/**
- **https://privacy.thewaltdisneycompany.com/el/internet-safety-el/**