ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΜΠΟΡΙΟΥ, ΒΙΟΜΗΧΑΝΙΑΣ ΚΑΙ ΤΟΥΡΙΣΜΟΥ

ΠΡΟΓΡΑΜΜΑ

"ΕΠΙΧΕΙΡΕΙΤΕ ΔΙΑΔΙΚΤΥΑΚΑ"

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Γραφείο eΔράση
www.go-e.mcit.gov.cy

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Περιεχόμενα

Ύποπτες εμπορικές σελίδες	1
Πιθανά προβλήματα	2
Αναγνώριση αξιόπιστων εμπορικών ιστοσελίδων	2
Αναγνώριση ασφαλών μεθόδων συναλλαγών	2
Τι είναι κλοπή ταυτότητας;	3
Phishing	3
Pharming	4
Scams - Χρήματα χωρίς αντίκρισμα	5
Κέρδη από διεθνή λαχεία	6
E-mail που προέρχονται δήθεν από τράπεζες ζητώντας στοιχεία μας	7
Προμήθεια από κληρονομιές	8
Συμβουλές για προστασία από τις ηλεκτρονικές απάτες	9
Διαφήμιση και Διαδίκτυο	10
Η διαφήμιση μέσα στο παιχνίδι	10
Χρήσιμες συμβουλές προς τους γονείς	11
Διαφήμιση μέσα από τις ιστοσελίδες κοινωνικής δικτύωσης	11
Συμβουλές για ασφαλείς ηλεκτρονικές συναλλαγές	12

Το Πρόγραμμα «Επιχειρείτε Διαδικτυακά» αποτελεί πρωτοβουλία του Υπουργείου Εμπορίου, Βιομηχανίας και Τουρισμού και έχει σκοπό την προώθηση και ανάπτυξη του Ηλεκτρονικού Εμπορίου στην Κύπρο. Για την επίτευξη του σκοπού αυτού έχει ιδρυθεί το Γραφείο eΔράση το οποίο είναι υπεύθυνο να υλοποιήσει συγκεκριμένο Στρατηγικό Σχέδιο.

Ο Οδηγός Ασφάλειας στο Διαδίκτυο έχει ετοιμαστεί στα πλαίσια του Προγράμματος «Επιχειρείτε Διαδικτυακά», σε μια προσπάθεια ενημέρωσης των καταναλωτών αναφορικά με την ασφαλή πλοήγηση στο διαδίκτυο και τα μέτρα ασφαλείας που θα πρέπει να λαμβάνονται, με στόχο την ενίσχυση του βαθμού εμπιστοσύνης τους προς το διαδίκτυο και το ηλεκτρονικό εμπόριο.

Πηγή του περιεχομένου του εντύπου αυτού καθώς και τα πνευματικά δικαιώματα ανήκουν στη δράση Saferinternet.gr, η οποία υλοποιείται από την ΜΚΟ Safer Internet Hellas.

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ύποπτες εμπορικές σελίδες

Το ηλεκτρονικό εμπόριο διευκολύνει καθημερινά εκατομμύρια ανθρώπους και επιχειρήσεις. Είναι όμως βασικό η πρόσβαση σε εμπορικές ιστοσελίδες να γίνεται με ιδιαίτερη προσοχή και με τη σιγουριά ότι αυτές λαμβάνουν υπόψη τους την επικείμενη νομοθεσία και παρέχουν την υποχρεωτική ασφάλεια συναλλαγών και προσωπικών δεδομένων.

Δυστυχώς υπάρχει μια ανησυχητική αύξηση ύποπτων εμπορικών ιστοχώρων που ζητούν την αποστολή προσωπικών δεδομένων και πληρωμή μέσω πιστωτικής κάρτας. Σε πολλές από τις περιπτώσεις αυτές τα αγαθά που έχουν αγοραστεί ουδέποτε φθάνουν στα χέρια σας, σε κάποιες άλλες ακόμα, τα προσωπικά δεδομένα σας και πολύ χειρότερα η πιστωτική σας κάρτα χρησιμοποιείται από τρίτους χωρίς τη δική σας γνώση και συναίνεση.

Συνήθως αυτές οι ιστοσελίδες προέρχονται από τις λιγότερο ανεπτυγμένες χώρες, στις οποίες δεν υπάρχει η πρέπουσα νομοθεσία. Ένας ιστοχώρος μπορεί να δημοσιευθεί στο Διαδίκτυο από οποιαδήποτε χώρα και μέσω οποιουδήποτε Παροχέα Υπηρεσιών Διαδικτύου (Internet Service Provider). Στους εμπορικούς ιστοχώρους συνήθως δίνεται ελεγχόμενη πρόσβαση μέσω κωδικών. Πολλές φορές συνδρομητικοί ιστοχώροι λειτουργούν σε βάση τέτοιων κωδικών που παρέχουν πρόσβαση σε συγκεκριμένες υπηρεσίες (ανάλογα της συνδρομής) στον ιστοχώρο και για ορισμένο χρονικό διάστημα. Υπάρχουν και οι δημόσιοι εμπορικοί ιστοχώροι, όπου μέσω ασφαλούς ηλεκτρονικής συναλλαγής (secure electronic transaction) ο οποιοσδήποτε μπορεί να ολοκληρώσει από οπουδήποτε και σε οποιαδήποτε στιγμή μια εμπορική συναλλαγή.

Είναι πολύ βασικό, όταν γίνεται μια τέτοια συναλλαγή να προσέχετε ότι η ηλεκτρονική διεύθυνση στην οποία βρίσκεστε ξεκινά με «https://» και όχι με «http://». Έτσι θα γνωρίζετε εάν το πρωτόκολλο που χρησιμοποιείται από τον ιστοχώρο σας παρέχει ασφαλή συναλλαγή ή όχι.

Οι ύποπτοι εμπορικοί ιστοχώροι συνήθως δεν έχουν μια τέτοια διεύθυνση και πουθενά στον ιστοχώρο τους δεν θα βρείτε πληροφορίες σχετικά με τον τρόπο ασφαλούς συναλλαγής. Τέτοιοι ιστοχώροι μπορεί να ασχολούνται με πώληση αγαθών, με ηλεκτρονικό τζόγο, ή ακόμα και με πορνογραφία.

Επίσης, εάν η σύνδεσή σας στο Διαδίκτυο γίνεται μέσω της τηλεφωνικής σας γραμμής (dial-up), σε τέτοιες ιστοσελίδες μπορεί χωρίς να το καταλάβετε να διακοπεί η σύνδεση με τον οικείο Παροχέα Υπηρεσιών Διαδικτύου για κάποια δευτερόλεπτα και να επανέλθει αυτή τη φορά ως σύνδεση από κάποιο «εξωτικό» μέρος (συνήθως κλήση από το σταθερό σας τηλέφωνο σε κάποιον αριθμό αντίστοιχου του γνωστού μας «090» στο εξωτερικό) στο οποίο θα κληθείτε στον επόμενο λογαριασμό του τηλεφώνου σας να πληρώσετε αστρονομικά ποσά σύνδεσης.

Πιθανά προβλήματα

Μη αξιόπιστες ιστοσελίδες ενδέχεται:

- *να μην εκτελούν τα καθήκοντά τους προς τους πελάτες τους, π.χ. μπορεί να μην παραδώσουν προϊόντα που έχουν αγοραστεί.*
- *να κάνουν κακή χρήση των προσωπικών δεδομένων που καταχωρούνται σε αυτές.*
- *να κάνουν κακή χρήση των πληροφοριών πληρωμής (στοιχεία πιστωτικής κάρτας).*

Τέτοιοι εμπορικοί ιστοχώροι μπορεί ακόμη να προσφέρουν ανεπιθύμητες ή παράνομες υπηρεσίες σε παιδιά (τζόγος, πορνογραφικό υλικό κ.α.).

Συνήθως, οι ιστοσελίδες αυτές προέρχονται από χώρες όπου δεν υπάρχει το κατάλληλο νομοθετικό πλαίσιο που να απαγορεύει τέτοιου είδους δραστηριότητες.

Αναγνώριση αξιόπιστων εμπορικών ιστοσελίδων

Οι γνωστές και εδραιωμένες εταιρείες είναι πιθανότατα το ίδιο αξιόπιστες στο Διαδίκτυο όσο και στην πραγματική ζωή.

Κριτήρια που μας βοηθούν να αναγνωρίσουμε τις αξιόπιστες εμπορικές σελίδες:

- *Ξεκάθαρος προσδιορισμός της εταιρείας με το όνομα της, τη διεύθυνση, τον αριθμό τηλεφώνου, την ηλεκτρονική διεύθυνση (e-mail), στοιχεία επικοινωνίας κ.λπ.*
- *Οι όροι των συμβάσεων είναι εύκολα προσβάσιμοι και διαφανείς.*
- *Τα χαρακτηριστικά του προϊόντος και οι όροι της εγγύησης είναι σαφή και εύκολα προσβάσιμα.*
- *Η τιμή του προϊόντος περιλαμβάνει όλες τις τυχόν χρεώσεις.*
- *Ο ιστοχώρος παρέχει ασφαλή τρόπο πληρωμής, βάσει διεθνών πιστοποιήσεων.*
- *Οι παραγγελίες επιβεβαιώνονται με e-mail.*
- *Οι καταναλωτές έχουν ένα σαφώς καθορισμένο δικαίωμα ανάκλησης της παραγγελίας.*

Σε περίπτωση που υπάρξουν προβλήματα σε κάποια ηλεκτρονική συναλλαγή, τότε είναι ευκολότερη η αντιμετώπισή τους αν η συναλλαγή έχει γίνει με κάποιο ηλεκτρονικό κατάστημα, που εδρεύει στην ίδια χώρα με αυτή του πελάτη.

Αναγνώριση ασφαλών μεθόδων συναλλαγών

Οι αξιόπιστες εμπορικές ιστοσελίδες παρέχουν συναλλαγές μόνο μέσω «ασφαλών ηλεκτρονικών συναλλαγών» (secure electronic transaction).

Πιο αναλυτικά για παράδειγμα, ο Internet Explorer χρησιμοποιεί ένα κρυπτογραφημένο πρωτόκολλο, το οποίο ονομάζεται Secure Sockets Layer (SSL) για την πρόσβαση σε ασφαλείς ιστοσελίδες. Έτσι είναι πολύ σημαντικό, όταν καταχωρείτε τις πληροφορίες πληρωμής (π.χ. δεδομένα της πιστωτικής κάρτας), να ελέγχετε πάντα αν η διεύθυνση της ιστοσελίδας που έχετε επισκεφθεί ξεκινά με "https://" και όχι με "http://". Με αυτό τον τρόπο, θα γνωρίζετε αν η ιστοσελίδα προσφέρει ασφαλείς συναλλαγές ή όχι.

Τι είναι η Κλοπή Ταυτότητας;

Μιλάμε για κλοπή ταυτότητας, όταν προσωπικές πληροφορίες έχουν κλαπεί και χρησιμοποιούνται παράνομα. Στις περισσότερες περιπτώσεις η κλοπή ταυτότητας γίνεται μέσω του phishing και του pharming.

Κατά τη διάρκεια της εγγραφής μας σε διάφορες ιστοσελίδες και σε υπηρεσίες που αυτές προσφέρουν μας ζητείται να συμφωνήσουμε με τους όρους και τις προϋποθέσεις χρήσης. Σχεδόν ποτέ όμως δεν διαβάζουμε το περιεχόμενό τους και αγνοούμε ότι ανάμεσα σε άλλα δίνουμε τη συγκατάθεσή μας στο να δεχόμαστε ενοχλητικά μηνύματα (spam) και στο να αποκαλυφθούν οι προσωπικές μας πληροφορίες σε διαφημιστές, συμβούλους αλλά και σε τρίτους.

Phishing

Τι είναι;
Πρόκειται για ιδιαίτερα διαδεδομένη τεχνική οικονομικής εξαπάτησης μέσω του «ψαρέματος» των προσωπικών σας δεδομένων και ειδικότερα των στοιχείων που αφορούν τις οικονομικές σας συναλλαγές (αριθμό λογαριασμού, κωδικό πιστωτικής κάρτας, κ.λ.π.).

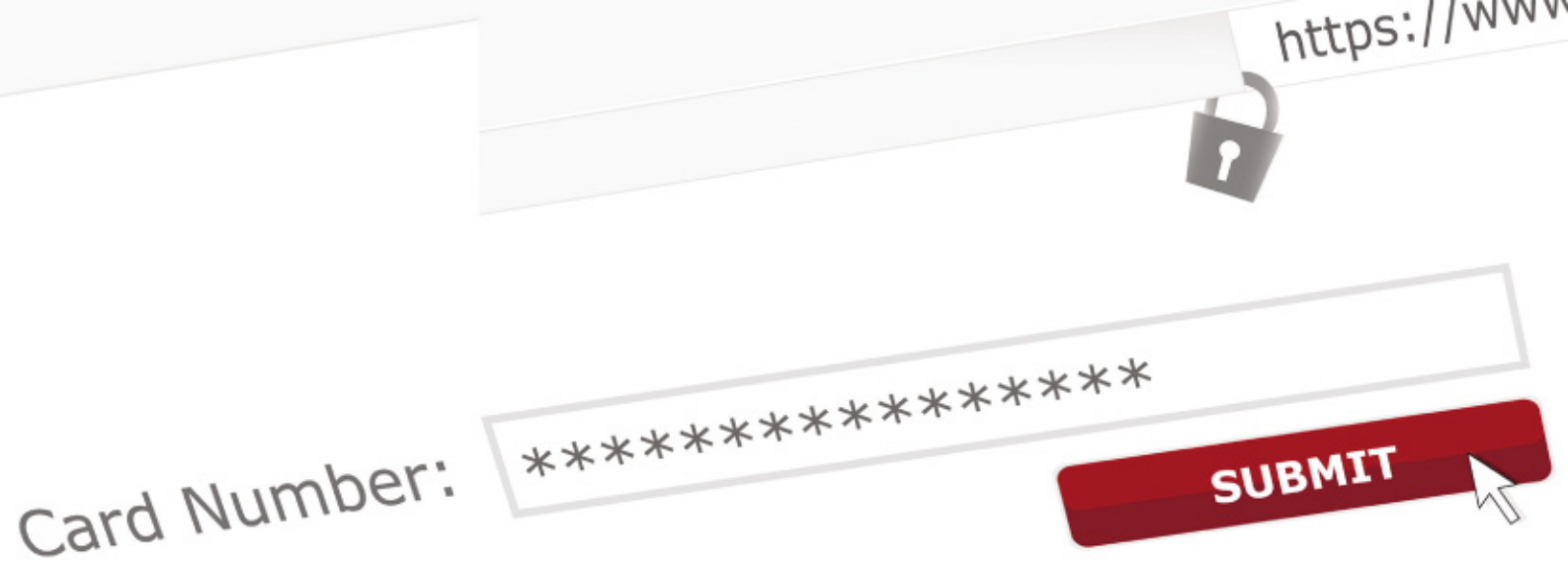
Πώς γίνεται η απάτη;
Όνομα γνωστής τράπεζας, τηλεπικοινωνιακού παρόχου ή άλλης νόμιμης εταιρείας εμφανίζεται ως αποστολέας ηλεκτρονικού μηνύματος που ενημερώνει τους παραλήπτες του για την ύπαρξη κενών ασφαλείας σε κάποιο λογαριασμό ή συνδρομή. Μέσα στο κείμενο παρατίθεται και ένας σύνδεσμος προς πλαστή ιστοσελίδα της εταιρίας η οποία πλασάρεται ως η επίσημη ιστοσελίδα του αποστολέα. Πηγαίνοντας στον ιστοχώρο αυτό, το θύμα καλείται να συμπληρώσει τα στοιχεία του π.χ. για να μην κλειστεί ο λογαριασμός του. Την ίδια ώρα αυτοί που κρύβονται πίσω από το ψεύτικο μήνυμα αποκτούν πρόσβαση στα στοιχεία αυτά και στη συνέχεια μπορούν να κάνουν ηλεκτρονικές απάτες εις βάρος σας.

Εναλλακτικές μορφές:

Spear Phishing: *Πρόκειται για στοχευμένα μηνύματα που μοιάζουν αυθεντικά για κάποιες ομάδες ανθρώπων. Για παράδειγμα, στους υπαλλήλους μιας εταιρείας μπορεί να φτάσει μήνυμα με αποστολέα τον εργοδότη τους, στο οποίο τους απευθύνεται προσωπικά και τους ζητά όνομα χρήστη και κωδικούς πρόσβασης. Απαντώντας κανείς σε ένα μήνυμα spear phishing θέτει προσωπικές και συχνά απόρρητες πληροφορίες στη διάθεση των απατεώνων.*

Vishing: *Σε αυτή την εκδοχή του phishing, για να πειστεί ευκολότερα το θύμα, του δίνεται τηλεφωνικός αριθμός εξυπηρέτησης ή του ζητείται το δικό του τηλέφωνο ώστε να μπορούν να επικοινωνήσουν μαζί του οι υποτιθέμενοι εκπρόσωποι της εταιρείας. Η πρακτική αυτή στηρίζεται στις τεχνολογίες VoIP που προσφέρει το Διαδίκτυο. Το "VoIP" είναι τα αρχικά για την τεχνολογία που ονομάζεται Voice Over Internet Protocol, δηλαδή Φωνή Πάνω από Πρωτόκολλο του Διαδικτύου. Με απλά λόγια, η τεχνολογία VoIP μας επιτρέπει να αξιοποιήσουμε οποιαδήποτε δικτυακή υποδομή που χρησιμοποιεί το πρωτόκολλο IP για να μεταφέρουμε φωνή.*

Social Networking Phishing: *Αντλώντας πληροφορίες και πολλά προσωπικά δεδομένα από τα προφίλ των χρηστών των ιστοσελίδων κοινωνικής δικτύωσης, οι απατεώνες στέλνουν εξατομικευμένα μηνύματα. Η επιτυχία της μεθόδου είναι μεγάλη. Σε πρόσφατο πείραμα που πραγματοποιήθηκε στις Ηνωμένες Πολιτείες το 70% όσων έλαβαν το εξατομικευμένο παραπλανητικό μήνυμα πάτησε το σύνδεσμο που περιέχετο σε αυτό και συμπλήρωσε τα στοιχεία του στο εικονικό site.*



ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Τι είναι η Κλοπή Ταυτότητας;

Pharming

Τι είναι;
Το Pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (domain name) που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη.

Πώς γίνεται η απάτη;
Εκμεταλλευόμενοι κάποια κενά στην ασφάλεια μιας ιστοσελίδας στην οποία οι χρήστες μπαίνουν για να πραγματοποιήσουν διάφορες συναλλαγές, οι απατεώνες καταφέρνουν να εκτρέψουν την ροή των επισκεπτών σε άλλο ιστοχώρο όπου τα στοιχεία των συναλλαγών που καταχωρούνται, χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. Τέτοιου είδους εκτροπή δεν μπορεί να γίνει σε ιστοσελίδες που χρησιμοποιούν το πρωτόκολλο SSL. Για να διαπιστώσετε αν οι συναλλαγές που κάνετε είναι ασφαλείς, δείτε στο πεδίο της διεύθυνσης αν υπάρχει η ένδειξη https:// αντί για το συμβατικό http://.

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Scams - Χρήματα χωρίς αντίκρισμα

Τι είναι;
Σε γενικές γραμμές αυτού του είδους οι απάτες που είναι γνωστές με τον όρο scam αφορούν κάποια συναλλαγή που για να ολοκληρωθεί χρειάζεται κάποια χρήματα από το υποψήφιο θύμα - παραλήπτη του παραπλανητικού μηνύματος. Ωστόσο το θύμα δεν παραλαμβάνει ποτέ τα προσφερόμενα ανταλλάγματα.

Εναλλακτικές μορφές:

Νιγηριανά scam ή απάτη 419: *Μέσω ηλεκτρονικού ταχυδρομείου αποστέλλεται μήνυμα που ενημερώνει με συγκινησιακά φορτισμένο τόνο τον παραλήπτη ότι μπορεί να βοηθήσει στην διεκπεραίωση κάποιας συναλλαγής. Ως αποτέλεσμα της βοήθειάς του θα έχει προμήθεια το 40% του ποσού που θα καταφέρει να αποδεσμεύσει / κληρονομήσει ο αποστολέας του μηνύματος. Οι συναλλαγές που εμφανίζονται συχνότερα είναι: η διεκδίκηση ανύπαρκτων κληρονομιών, η αποδέσμευση χρημάτων από τραπεζικούς λογαριασμούς, η παραλαβή και αποθήκευση των χρημάτων του αποστολέα σε ασφαλές μέρος και η επένδυση των χρημάτων αυτών στη χώρα του θύματος. Η συντριπτική πλειοψηφία των μηνυμάτων προέρχεται από τη Νιγηρία. Για το λόγο αυτό η πρακτική αυτή αποκαλείται νιγηριανό scam, αλλά και απάτη 419 από το άρθρο του ποινικού κώδικα της χώρας που αφορά στις οικονομικές απάτες. Οι απατεώνες διατηρούν την επικοινωνία και στέλνουν μάλιστα και αποδεικτικά στοιχεία της ταυτότητάς τους (που είναι όλα πλαστά) ώστε το θύμα να μην έχει την παραμικρή αμφιβολία. Κάποια στιγμή ζητούν χρήματα από τον παραλήπτη για τα έξοδα της συναλλαγής, φόρους κ.λ.π. Από τη στιγμή που θα παραλάβουν τα χρήματα, κάθε δίοδος επικοινωνίας διακόπτεται και φυσικά το θύμα δεν καταφέρνει να αποκτήσει το αστρονομικό ποσό που του είχαν τάξει.*

Διεθνή Λαχεία: *«Διεθνή λαχεία» αποστέλλουν emails, ανακοινώνοντας κέρδη. Στη συνέχεια και αφού τα θύματα έχουν πεισθεί για τα κέρδη, ζητούν από αυτούς να καταβάλουν χρήματα για διαδικαστικά έξοδα. Με αυτό τον τρόπο κατορθώνουν να αποσπούν σημαντικά χρηματικά ποσά.*

Δημοπρασίες: *Σε μη αξιόπιστες ιστοσελίδες δημοπρασιών ενδέχεται να γίνεται πλειστηριασμός ανύπαρκτων αντικειμένων. Τα θύματα πληρώνουν προκαταβολές και διαδικαστικά έξοδα, ωστόσο δεν παραλαμβάνουν ποτέ το αντικείμενο για το οποίο πλειοδότησαν.*

Ransomware: *Μέσω ηλεκτρονικού ταχυδρομείου το θύμα λαμβάνει μήνυμα με ένα συνημμένο αρχείο ή πρόγραμμα. Μόλις το ανοίξει αρχίζει διαδικασία κρυπτογράφησης των αρχείων που είναι αποθηκευμένα στον υπολογιστή του. Το θύμα δεν μπορεί να ανοίξει κανένα αρχείο του εκτός από το μήνυμα που του άφησαν οι scammers στο οποίο του εξηγούν ότι μόνο αφού πληρώσει ένα συγκεκριμένο ποσό θα του αποσταλεί ο κωδικός πρόσβασης. Πρόκειται ουσιαστικά για απαγωγή των αρχείων σας, για την ανάκτηση των οποίων πρέπει να καταβάλετε λύτρα!*

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Scams - Χρήματα χωρίς αντίκρισμα

Κέρδη από διεθνή λαχεία

Απατεώνες χρησιμοποιούν τα ονόματα εξεχόντων επιχειρήσεων για να αποστείλουν e-mails σχετικά με «Διεθνή λαχεία», ανακοινώνοντας κέρδη στο υποψήφιο θύμα. Στη συνέχεια, και αφού οι απατεώνες που βρίσκονται πίσω από αυτά τα e-mails έχουν πείσει τα θύματα για τα κέρδη, ζητούν από αυτά να καταβάλουν χρήματα για διαδικαστικά έξοδα. Με αυτό τον τρόπο κατορθώνουν να αποσπούν σημαντικά χρηματικά ποσά.

Ένα τέτοιο e-mail μπορεί να είναι της εξής μορφής:

Our company promotions presents free email computer ballot summer bonanza (Coupon winning number: XWIN-01257DEN)

Dear Winner,
You have won the sum of EUR 1.000.000 from our database of internet e-mail users held today, from which your email address was randomly balloted which came out attached to the winning coupon number XWIN-01257DEN.

This winning prize is of a totally cash money of five millions euros which under five lucky winners with their e-mail in appendix to this same coupon winning number is shared one million to each five winners.

This lottery is an Easter promotional program by our internationally established and prestigious company, to advertise to the world its existence. All participants were selected through a computer ballot system drawn from over 50,000 companies and 2,000,000 individual email addresses from all over the world, as part of our international promotions program, which we intend to conduct several times a year.

Being one of the luck winners, we hereby contact you to claim your winning amount quickly as this is a free email computer ballot bonanza lottery promotion. Failure to claim your winning will result to rollover or reversion of the winning sum. We also use this medium to notify you that the expiring or lapse date to claim your winning prize is within 5 days of receipt of this email. To claim your winning prize, contact the manager with your coupon winning number XWIN-01257DEN.

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Scams - Χρήματα χωρίς αντίκρισμα

E-mail που προέρχονται δήθεν από τράπεζες ζητώντας στοιχεία μας

Οι απατεώνες στέλνουν e-mails στα υποψήφια θύματα στα οποία χρησιμοποιούν ονόματα και λογότυπα έγκυρων τραπεζών. Σε αυτά ενημερώνουν για δήθεν προβλήματα που εκδηλώθηκαν στην τράπεζα και αχετίζονται με λογαριασμούς (π.χ. στον τομέα της ασφάλειας των συναλλαγών) και παραπλανούν το θύμα να εισάγει προσωπικά του στοιχεία σε εικονική διαδικτυακή φόρμα εισαγωγής στοιχείων αναγνώρισης χρήστη.

Με αυτόν τον τρόπο πλαστογραφούν μετά τα στοιχεία του θύματος και αποκτούν παράνομη πρόσβασης σε δεδομένα αυτού, όπως τραπεζικούς λογαριασμούς, usernames, passwords, αριθμούς πιστωτικών καρτών, PIN, TAN, κ.λ.π. Η απάτη δεν γίνεται εύκολα αντιληπτή.

Πρέπει να γνωρίζουμε ότι ποτέ καμία έγκυρη τράπεζα δεν θα μας ζητήσει προσωπικά μας δεδομένα μέσω τηλεφώνου, ηλεκτρονικού ταχυδρομείου ή μέσω του Διαδικτύου!

Ένα τέτοιο μήνυμα μπορεί να μοιάζει με το παρακάτω:

Αγαπητέ online πελάτη της τράπεζάς μας,

Στα πλαίσια μέτρων ασφαλείας, εξετάζεται κατά τακτά χρονικά διαστήματα η δραστηριότητα στο σύστημα της τράπεζας. Πρόσφατα παρατηρήσαμε το εξής ζήτημα σχετικά με τον λογαριασμό σας. Μετά από πρόσφατο έλεγχο του λογαριασμού σας θα πρέπει να απαιτήσουμε κάποιες πρόσθετες πληροφορίες από εσάς έτσι ώστε να σας παρέχουμε ασφαλείς υπηρεσίες. Μονοσήμαντος αριθμός σας: CA9908-8989. Για την ασφάλειά σας, περιορίσαμε την πρόσβαση στον λογαριασμό σας, έως ότου ολοκληρωθούν τα πρόσθετα μέτρα ασφαλείας.

Σας ζητούμε συγγνώμη για οποιαδήποτε πιθανή ενόχληση. Παρακαλείσθε να κάνετε εισαγωγή στο σύστημα της τράπεζας μέσω της περιοχής TAN για να ανακτήσετε την πρόσβαση στο λογαριασμό σας το συντομότερο δυνατόν.

Θα πρέπει να πατήσετε τον παρακάτω σύνδεσμο και μέσω της περιοχής TAN να κάνετε εισαγωγή στο σύστημα, στην ιστοσελίδα της Διαδικτυακής Τραπεζικής μας για την ολοκλήρωση της διαδικασίας επαλήθευσης. http://homebank.xyz.gr/homebank/logon.asp

Σύμφωνα με την Συμφωνία Χρήστη της τράπεζας, η πρόσβαση στο λογαριασμό σας θα παραμείνει περιορισμένη έως ότου λυθεί το ζήτημα. Δυστυχώς, εάν η πρόσβαση στο λογαριασμό σας παραμείνει περιορισμένη για εκτεταμένη χρονική περίοδο, είναι πιθανό να υπάρξουν επιπλέον περιορισμοί ή ακόμη και κλείσιμο του λογαριασμού. Σας προτρέπουμε να κάνετε εισαγωγή το συντομότερο δυνατόν για να την αποφυγή των παραπάνω.

Σας ευχαριστούμε για την άμεση προσοχή σας στο θέμα. Παρακαλούμε να λάβετε υπόψη σας ότι αυτό είναι ένα μέτρο το οποίο αποσκοπεί στη δική σας ασφάλεια και την προστασία του λογαριασμού σας.

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Scams - Χρήματα χωρίς αντίκρισμα

Προμήθεια από κληρονομιές

Σε υποτιθέμενο μήνυμα από διεθνή τράπεζα, υψηλόβαθμο στέλεχος, σας ενημερώνει ότι ένας πελάτης της τράπεζας με καταθέσεις πολλών εκατομμυρίων απεβίωσε, χωρίς διαθήκη και απογόνους. Ενημερώνει λοιπόν, ότι υπάρχει η δυνατότητα να σας εμφανίσουν ως τον πλησιέστερο συγγενή του θανόντα, έτσι ώστε να μπορέσουν να έχουν πρόσβαση στις καταθέσεις του, και για τη βοήθειά σας προσφέρουν παχυλή προμήθεια.

Φυσικά, εάν κάποιος πέσει θύμα ενός τέτοιου μηνύματος και προχωρήσει σε συνεργασία με τους απατεώνες, κάποια στιγμή θα του ζητηθεί, εκτός από το να δώσει προσωπικά του στοιχεία ή στοιχεία της τράπεζάς του, να πληρώσει για διαδικαστικά έξοδα για να λάβει την προμήθεια αυτή. Μόλις το θύμα δώσει τα χρήματα που του ζητούνται, οι απατεώνες θα διακόψουν κάθε δίοδο επικοινωνίας και φυσικά δεν θα του παραδώσουν ποτέ τα ανταλλάγματα που είχαν υποσχεθεί.

Ένα τέτοιο μήνυμα είναι συνήθως στην Αγγλική γλώσσα και περιέχει π.χ. τα εξής:

I am Maria Smith, Chief Auditor of Bank International.
By virtue of our official positions we where able to discovered an abandoned account with the sum of US$17.5 in a non-resident account that belongs to one foreign customer who died in November 1999 in a ghastly motor accident.
Since we got the information about his death, we have been monitoring the account to see his next of kin to come over and claim his money ... I want to let you know in confidence that till date know one has ever come forward for the claim.

It is therefore on this note that we decided to write you if possible make business with you and release the money to you as the next of kin or relative to the deceased... if such money remained unclaimed after eight years, it will be transferred into the State/Government accounts as unclaimed fund. If you are interested in this deal we shall guide you on how to apply for it ...

With the appropriate documentation the ownership of the sum will be transferred to you after the validation and the authentication of the documents at the bank. I intend arriving at your place with the relevant original papers/documents within 48 hours as soon as you receive the notification of transfer from the bank. And I want to assure you that this business is 100% risk free as long as you and we maintain maximum confidentiality...

And please even if you are not interested I require you to keep this matter confidential and to yourself only as we are still in active government service as such would not want to be exposed. The sharing of the fund shall been agreed by both of us. If interest is shown we agreed to offer you 20% of the total money for your help. Reply by e-mail as regards to the confidential nature of this matter.

Regards,
Maria Smith

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Συμβουλές για προστασία από τις ηλεκτρονικές απάτες

- *Θα πρέπει να είστε βέβαιοι ότι ο υπολογιστής σας δεν έχει προσβληθεί από κακόβουλο λογισμικό όπως για παράδειγμα από Δούρειο Ίππο που καταγράφει τα προσωπικά δεδομένα που καταχωρείτε σε φόρμες του Διαδικτύου. Ενημερωθείτε για τους τρόπους προστασίας από τέτοιου είδους λογισμικό.*

- *Εγκαταστήστε φίλτρο ανεπιθύμητης αλληλογραφίας. Ακόμη και αν κάποιο e-mail από άγνωστο αποστολέα φτάσει στα εισερχόμενα σας, μην πατάτε ποτέ τους συνδέσμους (links) που περιέχονται σε αυτό.*

- *Θα πρέπει να γνωρίζετε ότι καμία αξιόπιστη εταιρεία ή τράπεζα δεν θα επικοινωνούσε μαζί σας μέσω ηλεκτρονικού ταχυδρομείου για ζητήματα που αφορούν προσωπικούς λογαριασμούς. Αν λάβετε ένα τέτοιο μήνυμα, καλό είναι να απευθυνθείτε στην εξυπηρέτηση πελατών της εταιρείας ή της τράπεζας για να τους ενημερώσετε.*

- *Πριν καταχωρήσετε τα στοιχεία ενός λογαριασμού στο Διαδίκτυο βεβαιωθείτε πρώτα ότι βρίσκεστε στην επίσημη ιστοσελίδα της εταιρείας, ότι στο κάτω μέρος του browser υπάρχει ένα λουκετάκι και ότι η διεύθυνση αρχίζει με https://.*

- *Μην κλικάρετε με το ποντίκι σας σε διευθύνσεις ιστοχώρων που σας δίνονται σε ύποπτα e-mails, γιατί ενδέχεται να σας κατευθύνουν σε εικονικές ιστοσελίδες που μοιάζουν με την πρωτότυπη της εταιρείας ή τράπεζας, από όπου απατεώνες θα προσπαθήσουν να σας αποσπάσουν προσωπικά δεδομένα. Για αυτό, γράφετε πάντα από μόνοι σας την ηλεκτρονική διεύθυνση στον browser.*

- *Ένα ακόμα κόλπο για να δοκιμάσετε τη γνησιότητα ενός ιστοχώρου, είναι να καταχωρήσετε λανθασμένο κωδικό πρόσβασης. Εάν το site είναι πλαστό, θα τον αποδεχτεί και τότε θα σας εμφανίσει μια σελίδα που θα σας λέει ότι παρουσιάστηκαν τεχνικά προβλήματα. Στο γνήσιο site δεν θα σας επιτραπεί εξ αρχής η πρόσβαση.*

- *Αποφύγετε να κάνετε ηλεκτρονικές συναλλαγές από υπολογιστές τρίτων ή δημόσια προσβάσιμους (π.χ. από Ίντερνετ καφέ). Επίσης αν παραπάνω από ένας χρήστης έχει πρόσβαση στον υπολογιστή σας, καλό θα ήταν να απενεργοποιήσετε τη δυνατότητα απομνημόνευσης κωδικών του browser σας.*

- *Φυλάξτε τους κωδικούς σας σε ασφαλές μέρος. Μη χρησιμοποιείτε για κωδικό ονόματα, ημερομηνίες γέννησης, επετείων κ.λπ. που εύκολα μπορεί να μαντέψει κανείς.*

Διαφήμιση και Διαδίκτυο

Η διαφήμιση μέσα στο παιχνίδι: Τι θα πρέπει να γνωρίζουμε

Τα τελευταία χρόνια η διαφήμιση στο Διαδίκτυο κερδίζει έδαφος σε σχέση με τη διαφήμιση σε άλλα μέσα όπως η τηλεόραση. Τα παιδιά λοιπόν, βρίσκονται πολλές φορές μπροστά σε εμπορικές ιστοσελίδες, έχοντας προσελκυθεί από τα διαδραστικά παιχνίδια και κουίζ που προσφέρουν.

Οι διαφημίσεις με τη μορφή παιχνιδιού και οι διαφημίσεις ενσωματωμένες σε παιχνίδια γίνονται όλο και πιο συχνές. Γίνονται μάλιστα όλο και πιο δυσδιάκριτες, με αποτέλεσμα τα παιδιά συχνά να μην αντιλαμβάνονται ότι πρόκειται για διαφήμιση.

Πρωταρχικός στόχος των εμπορικών ιστοσελίδων σχετικά με την προσέγγιση των παιδιών είναι να τους εμπνεύσουν θετική προδιάθεση απέναντι σε ένα προϊόν ή σε μια μάρκα (brand name). Απώτερος σκοπός είναι να επηρεάσουν τις προθέσεις και την καταναλωτική συμπεριφορά του γονέα.

Ήδη τα μικρά παιδιά δυσκολεύονται να διαχωρίσουν τη διαφήμιση από το κύριο πρόγραμμα στην τηλεόραση παρ' όλο που τα όρια εκεί παραμένουν ευδιάκριτα. Στο Διαδίκτυο, ωστόσο, τα όρια μεταξύ μιας εμπορικής και μιας ιστοσελίδας ψυχαγωγίας είναι πάρα πολύ δυσδιάκριτα, σχεδόν ανύπαρκτα. Αυτός ακριβώς είναι και ο στόχος άλλωστε. Τα παιδιά παίζουν σε μια κοινωνία «brand names» όπου δεν ξεχωρίζουν την ψυχαγωγία από τη διαφήμιση.

Ελάχιστα παιδιά στην ηλικία 9 έως 11 ετών αντιλαμβάνονται ότι το αγαπημένο τους site έχει εμπορικούς σκοπούς. Τα περισσότερα θεωρούν ότι οι ιστοσελίδες έχουν φτιαχτεί αποκλειστικά για να τα διασκεδάζουν. Μέσα στα παιχνίδια τα εμπορικά μηνύματα εμφανίζονται ως λογότυπα, φιγούρες και χαρακτήρες μασκότ που τα παιδιά ταυτίζουν με το ίδιο το προϊόν που αντιπροσωπεύουν. Αυτά τα παιχνίδια είναι συχνά ανταγωνιστικά και ελκυστικά, κάτι που ενθαρρύνει τα παιδιά να παραμείνουν για μεγάλο διάστημα σε μια ιστοσελίδα ή να την επισκέπτονται επανειλημμένως. Επιπλέον, μετά την εγγραφή τους σε μια υπηρεσία/παιχνίδι, τα παιδιά αρχίζουν να λαμβάνουν πληροφορίες και διαφημίσεις και για άλλα προϊόντα. Υπάρχουν ακόμα και κωδικοί κρυμμένοι σε προϊόντα που τα παιδιά πρέπει να αγοράσουν ώστε να εντοπίσουν τον κρυμμένο κωδικό με τον οποίο θα «περάσουν πίστα» σε κάποιο διαδικτυακό παιχνίδι.

Δεύτερος στόχος των εμπορικών ιστοσελίδων είναι να συλλέξουν στοιχεία για την αγορά. Για την εγγραφή στους ιστοχώρους αυτούς ζητείται από τα παιδιά να δώσουν στοιχεία (δημογραφικά και επικοινωνίας σχετικά με τις προτιμήσεις τους, κ.α.). Από εκείνο το σημείο και έπειτα, τα παιδιά γίνονται χρήσιμα για την εταιρεία.

Το advert-gaming, όπως θα μπορούσαμε να αποκαλέσουμε το φαινόμενο αυτό, εγείρει πολλά ερωτήματα για τα όρια της διαφήμισης. Ακόμα και αν τα παιδιά αντιληφθούν ότι πρόκειται για ένα διαφημιστικό παιχνίδι, είναι εξαιρετικά αμφίβολο το αν αυτό θα τους αποθαρρύνει να ασχοληθούν με αυτό, αφού είναι κάτι τόσο διασκεδαστικό! Έρευνες δείχνουν ότι το advert-gaming συνδέεται στις ΗΠΑ με την παιδική παχυσαρκία καθώς η μέθοδος εφαρμόζεται κατά κόρον από εταιρείες τροφίμων με αγοραστικό κοινό τα παιδιά.

Διαφήμιση και Διαδίκτυο

Χρήσιμες συμβουλές προς τους γονείς:

Για παιδιά ηλικίας 6-9

- *Βεβαιωθείτε ότι το παιδί δε δίνει προσωπικές πληροφορίες. Συχνά τα παιδιά δίνουν όλα τα στοιχεία που τους ζητούνται σε μια ηλεκτρονική φόρμα, δίνουν μάλιστα στοιχεία που αφορούν τους φίλους και την οικογένειά τους.*

Για παιδιά ηλικίας 9-13

- *Δώστε εναλλακτικές λύσεις στα advert-games. Εξηγήστε στα παιδιά τη διαφορά μεταξύ διαφήμισης και πληροφορίας και ενημερώστε για τον τρόπο που η διαφήμιση λειτουργεί στο Διαδίκτυο.*

- *Μάθετε στα παιδιά να είναι υπεύθυνα στη χρήση των προσωπικών τους δεδομένων.*

Για παιδιά ηλικίας 13 +

- *Ενθαρρύνετε την κριτική σκέψη. Οι έφηβοι είναι πολύ κερδοφόρα ομάδα – στόχος για τους διαφημιστές στο Διαδίκτυο και γ' αυτό θα πρέπει να είναι πάντα υποψιασμένοι, ώστε να ξεχωρίζουν την πληροφορία από το διαφημιστικό περιεχόμενο.*

Διαφήμιση μέσα από τις ιστοσελίδες κοινωνικής δικτύωσης

Αν χρησιμοποιείτε κάποια ιστοσελίδα κοινωνικής δικτύωσης αναρωτηθείτε: Πόσα χρήματα πληρώνετε για τις υπηρεσίες τους; Πριν γελάσετε με την ερώτηση αυτή, αναλογιστείτε... από πού κερδίζουν χρήματα οι ιστοσελίδες αυτές;

Η απάντηση είναι απλή:
Από τα προσωπικά σας δεδομένα!

Τα προσωπικά σας δεδομένα δεν είναι πολύτιμα μόνο για εσάς! Οι ιστοσελίδες κοινωνικής δικτύωσης χρησιμοποιούν τα στοιχεία που οι ίδιοι οι χρήστες παραχωρούν απλόχερα για να τους προσφέρουν διαφημίσεις ανάλογα με τις ανάγκες τους. Στοιχεία όπως οι επισκέψεις σε ιστοσελίδες, οι λέξεις κλειδιά που χρησιμοποιούν, κ.λ.π., καταγράφονται και εν συνεχεία χρησιμοποιούνται για τη δημιουργία του καταναλωτικού τους προφίλ. Για παράδειγμα, αν κάποιος δηλώνει στο προφίλ του ότι του αρέσει η λογοτεχνία, είναι πολύ πιθανό να δει στο προφίλ του διαφημιστική καταχώριση για κάποιο βιβλίο.

Σήμερα, εκατοντάδες χιλιάδες επιχειρηματίες δραστηριοποιούνται στις ιστοσελίδες κοινωνικής δικτύωσης, οι οποίοι βέβαια αποκομίζουν χρηματικό όφελος εκμεταλλευόμενοι την τεράστια απήχηση των ιστοσελίδων αυτών. Στους όρους χρήσης πολλών ιστοχώρων κοινωνικής δικτύωσης αναφέρεται μάλιστα, ότι τα δεδομένα των χρηστών όχι μόνο δίνονται σε τρίτους, αλλά επίσης ότι από τη στιγμή που καταχωρούνται γίνονται αντικείμενο επεξεργασίας σε ξένες χώρες, όπου βέβαια ισχύει άλλη - πιθανώς ελαστικότερη - νομοθεσία σε σχέση με τα ζητήματα των προσωπικών δεδομένων.

ΟΔΗΓΟΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Συμβουλές για ασφαλείς ηλεκτρονικές συναλλαγές

Προτού παραγγείλετε ένα προϊόν μέσω διαδικτύου:

- *Να ενημερώνεστε σχετικά με την ταυτότητα και την αξιοπιστία του ηλεκτρονικού καταστήματος. Πρέπει να προσδιορίζονται ξεκάθαρα τα στοιχεία της εταιρείας, δηλαδή το όνομα, αριθμός εγγραφής, τα στοιχεία επικοινωνίας όπως η διεύθυνση, ο αριθμός τηλεφώνου, το e-mail.*

- *Να κάνετε τις αγορές σας σε ιστοσελίδες που παρέχουν «ασφαλείς συναλλαγές», βάσει διεθνών πιστοποιήσεων.*

- *Για αγορές είναι προτιμότερες οι προπληρωμένες πιστωτικές κάρτες, που ελαχιστοποιούν τον κίνδυνο οικονομικής ζημίας.*

- *Οι όροι χρήσης της συναλλαγής πρέπει να είναι προσβάσιμοι και διαφανείς.*

- *Να αποφεύγετε τις ηλεκτρονικές συναλλαγές από υπολογιστές τρίτων ή δημόσια προσβάσιμους (π.χ. από Ίντερνετ καφέ).*

- *Να φυλάσσετε τους κωδικούς σε ασφαλές μέρος. Να μην χρησιμοποιείται για κωδικό ονόματα οικείων, ημερομηνίες γέννησης, επετείων, κ.λ.π., που εύκολα μπορεί να μαντέψει κανείς.*

- *Πρέπει τα χαρακτηριστικά του προϊόντος να είναι σαφή, αληθή και εύκολα προσβάσιμα. Ιδιαίτερη προσοχή να δίνεται στην τιμή του προϊόντος, τις τυχόν επιβαρύνσεις, τον τρόπο πληρωμής, το χρόνο παράδοσης και την πολιτική επιστροφών του καταστήματος.*

- *Θα πρέπει να σας δίνεται η δυνατότητα να εκτυπώσετε ή να αποθηκεύσετε στον υπολογιστή σας τη συναλλαγή που πραγματοποιήσατε. Επιπλέον, οι συναλλαγές πάντοτε να επιβεβαιώνονται με e-mail.*

- *Να διατηρείτε όλα τα στοιχεία επικοινωνίας- ίσως τα χρειαστείτε σε περίπτωση αργοπορίας ή προβλήματος με τη παράδοση του προϊόντος.*

- *Να γνωρίζετε ότι έχετε τα ίδια δικαιώματα σαν να κάνετε αγορές από κανονικό κατάστημα (π.χ. σε περίπτωση ελαττωματικού προϊόντος, μη εκπλήρωσης παραγγελίας, κ.λ.π.)*

Να θυμάστε ότι:

- ***Υπάρχει δικαίωμα υπαναχώρησης εντός 14 ημερών από την ημερομηνία παραλαβής των προϊόντων.***
- ***Σε περίπτωση επιστροφής, οι καταναλωτές επιβαρύνονται με τα έξοδα αποστολής.***

Οι πληροφορίες που περιλαμβάνονται στο έντυπο αυτό δεν αποσκοπούν στο να υποκαταστήσουν επίσημα κείμενα, νομικά ή άλλα ούτε και αποτελούν νομική ερμηνεία αυτών.
Ο Οδηγός Ασφάλειας στο Διαδίκτυο έχει πληροφοριακό χαρακτήρα και παρέχει εισηγήσεις και συμβουλές για ασφαλή χρήση του διαδικτύου και του ηλεκτρονικού εμπορίου.
Κατά συνέπεια το Υπουργείο Εμπορίου, Βιομηχανίας και Τουρισμού δεν φέρει απολύτως καμία ευθύνη για ζημιές, κίνδυνο, βλάβη που τυχόν θα προκύψουν από τη χρήση του εντύπου αυτού.

Γραφείο eΔράση
www.go-e.mcit.gov.cy

Υπηρεσία Εμπορίου
Υπουργείο Εμπορίου, Βιομηχανίας και Τουρισμού
1421 Λευκωσία
Τηλέφωνα επικοινωνίας: 22 867106/323/324