DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Ας ξεκινήσουμε!

Περιηγηθείτε με ασφάλεια στο διαδίκτυο και ασφαλίστε τον υπολογιστή σας

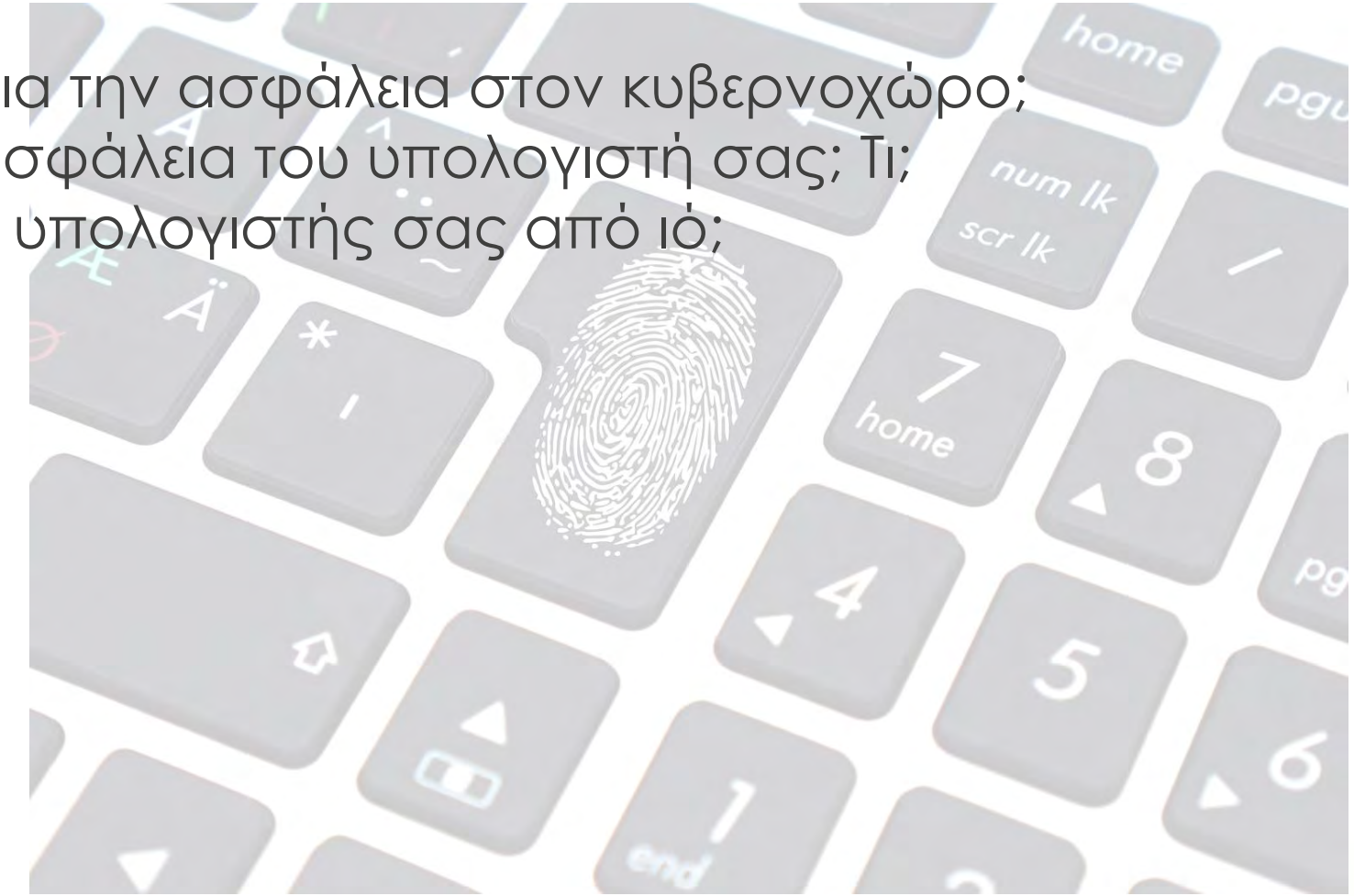
Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union

Ας Ξεκινήσουμε!

Αναρωτηθείτε:

1. Έχετε ακούσει ποτέ για την ασφάλεια στον κυβερνοχώρο;
2. Κάνετε κάτι για την ασφάλεια του υπολογιστή σας; Τι;
3. Έχει μολυνθεί ποτέ ο υπολογιστής σας από ιό;



Ας ξεκινήσουμε!

Τι είναι η ασφάλεια στον κυβερνοχώρο και γιατί έχει σημασία;

Η ασφάλεια στον κυβερνοχώρο γίνεται ολοένα και πιο σημαντική στο σημερινό κόσμο, καθώς καθημερινά περισσότερα από 230.000 νέα δείγματα κακόβουλου λογισμικού κάνουν την εμφάνισή τους.

Οι απειλές για την ασφάλεια δεν αντιμετωπίζονται μόνο από Οι μεγάλες εταιρείες που διεξάγουν online επιχειρήσεις δεν είναι οι μόνες που αντιμετωπίζουν απειλές για την ασφάλεια του δικτύου τους. Όποιος περιηγείται στο διαδίκτυο είναι ένα πιθανό θύμα εγκληματιών στον κυβερνοχώρο.

Οι μεγαλύτερες απειλές στον κυβερνοχώρο περιλαμβάνουν:

- συνδέσμους σε κακόβουλες ιστοσελίδες,
- Κακόβουλο λογισμικό
- μεταφορτώσεις δίσκου και
- ιούς.

Ας ξεκινήσουμε!

Λίγες Συμβουλές

- Το Διαδίκτυο δεν είναι ασφαλές μέρος, διότι ο οποιοσδήποτε υπολογιστής μπορεί να γίνει ένας εύκολος στόχος για τους εγκληματίες του κυβερνοχώρου.
- Πρέπει να αποφεύγονται οι επικίνδυνες ιστοσελίδες που δεν διαθέτουν πιστοποιητικό ασφαλείας. Αναζητήστε το HTTPS στην αρχή της διεύθυνσης URL.
- Δεν πρέπει ποτέ να ανοίγετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια άγνωστη πηγή.
- Ένα λογισμικό προστασίας από ιούς πρέπει να εγκατασταθεί για να αποτρέψει τις απειλές.

Let’s start!

Η Κύβερνο-ασφάλεια είναι η προστασία των συστημάτων που συνδέονται με το Διαδίκτυο, συμπεριλαμβανομένου του υλικού, του λογισμικού και των δεδομένων, από Κύβερνο-επιθέσεις. Σε ένα περιβάλλον πληροφορικής, η ασφάλεια περιλαμβάνει την ασφάλεια στον κυβερνοχώρο και τη φυσική ασφάλεια – και τα δύο αυτά χρησιμοποιούνται από τις επιχειρήσεις για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση στα κέντρα δεδομένων τους και άλλα μηχανογραφικά τους συστήματα. Η ασφάλεια των πληροφοριών, η οποία έχει σχεδιαστεί για να διατηρεί την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα δεδομένων, αποτελεί υποσύνολο της ασφάλειας στον κυβερνοχώρο.

Ας ξεκινήσουμε!

Είχατε ποτέ έναν ιό;

Οι ιοί υπολογιστών είναι σαν μια γρίπη, είναι σχεδιασμένοι για να εξαπλώνονται από τον ξενιστή στον κεντρικό υπολογιστή και έχουν την ικανότητα να αναπαράγονται. Με τον ίδιο τρόπο που οι ιοί της γρίπης δεν μπορούν να αναπαραχθούν χωρίς κύτταρο ξενιστή, οι ιοί υπολογιστών δεν μπορούν να αναπαραχθούν και να εξαπλωθούν χωρίς προγραμματισμό, όπως ένα αρχείο ή ένα έγγραφο. Σε έναν κόσμο που είναι όλο και περισσότερο συνδεδεμένος, οι ιοί μπορούν να εξαπλωθούν μέσω:

- συνημμένων σε μηνύματα email και κειμένου,
- λήψεις αρχείων από το διαδίκτυο,
- και κακόβουλους συνδέσμους στα κοινωνικά δίκτυα.

Τα κινητά σας τηλέφωνα μπορούν να μολυνθούν από ιούς μέσω λήψεων μη ασφαλών εφαρμογών. Οι ιοί μπορεί να κρύβονται, μεταμφιεσμένοι σε συνημμένα περιεχομένου κοινής χρήσης, όπως αστείες εικόνες, ευχετήριες κάρτες ή αρχεία ήχου και βίντεο.

Ας ξεκινήσουμε!

ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ!

- Κανείς δεν το θέλει ή το έχει ζητήσει ποτέ.
- Κανείς δεν το θεωρεί χρήσιμο.
- Μερικές φορές είναι πράγματι ενδιαφέρον, όπως το 1% του ανεπιθύμητου ταχυδρομείου που είναι πραγματικά χρήσιμο σε μερικούς ανθρώπους.

*Το **spam** είναι ηλεκτρονικό ταχυδρομείο ανεπιθύμητης αλληλογραφίας ή ομαδικών ανεπιθύμητων δημοσιεύσεων. Μερικοί άνθρωποι ορίζουν το **spam** ακόμα γενικότερα ως οποιοδήποτε ανεπιθύμητο ηλεκτρονικό ταχυδρομείο.*

Παρακολουθείστε αυτό το Βίντεο:

https://www.youtube.com/watch?v=_QdPW8JrYzQ

Ας ξεκινήσουμε!

Γιατί υπάρχει η ανεπιθύμητη αλληλογραφία!

Το Spam είναι ένα μήνυμα ηλεκτρονικού ταχυδρομείου που αποστέλλεται σε χιλιάδες ή και εκατομμύρια ανθρώπους, χωρίς προηγούμενη έγκριση, προωθώντας ένα συγκεκριμένο προϊόν, υπηρεσία ή απάτη για να κερδηθούν χρήματα εις βάρος άλλων ανθρώπων.

η απάντηση σε αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου δείχνει ότι η διεύθυνση ηλεκτρονικού ταχυδρομείου σας είναι έγκυρη και η διεύθυνση ηλεκτρονικού ταχυδρομείου σας μπορεί να σταλεί σε άλλες λίστες ανεπιθύμητων μηνυμάτων.

Ποτέ μην το κάνετε αυτό όταν λαμβάνετε μηνύματα ηλεκτρονικού ταχυδρομείου που είναι ανεπιθύμητα. είναι συνήθως καλύτερο να τα διαγράψετε.

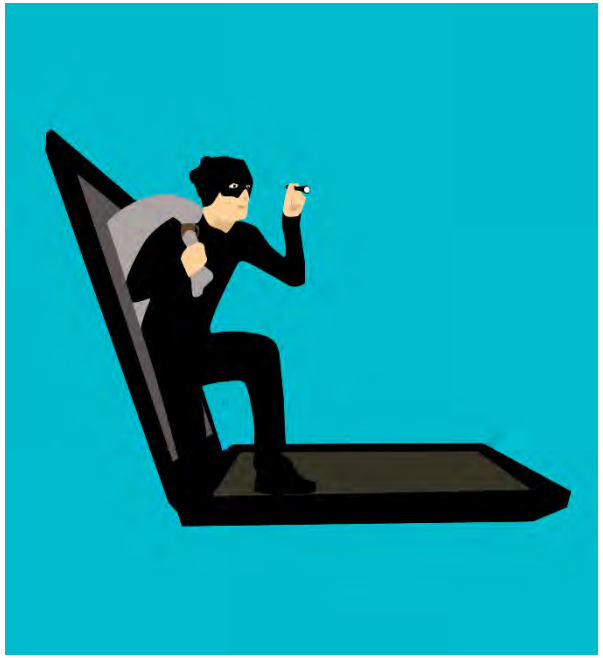
Να είστε προσεκτικοί όταν δημοσιεύετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας. Μην τη δημοσιεύετε ποτέ σε άλλους δημόσιους χώρους.

Όταν συμπληρώνετε οποιαδήποτε φόρμα στο Internet, ψάξτε προσεκτικά για οποιοδήποτε πλαίσιο ελέγχου που από προεπιλογή μπορεί να συμπληρωθεί για να λαμβάνετε ενημερωτικά δελτία ή να μοιράζεστε το ηλεκτρονικό σας ταχυδρομείο με τρίτο πρόσωπο.

Ας ξεκινήσουμε!

Πειρατεία

Η πειρατεία είναι μια προσπάθεια να εκμεταλλευτείς ένα σύστημα υπολογιστή ή ένα ιδιωτικό δίκτυο μέσα σε έναν υπολογιστή. Με απλά λόγια, είναι η μη εξουσιοδοτημένη πρόσβαση ή έλεγχος των συστημάτων ασφαλείας δικτύων υπολογιστών για κάποιο παράνομο σκοπό.



Ποιος είναι?

Ένας χάκερ δεν είναι πάντα κάποιος που κάνει παράνομα πράγματα! Οι επαγγελματίες χάκερς των **λευκών καπέλων** ελέγχουν τα δικά τους συστήματα ασφαλείας για να τα κάνουν πιο ανθεκτικά. Οι χάκερς των **μαύρων καπέλων** παίρνουν τον έλεγχο του συστήματος για προσωπικά κέρδη. Μπορούν να καταστρέψουν, να κλέψουν ή ακόμη και να εμποδίσουν τους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στο σύστημα. Οι χάκερς των **γκρίζων καπέλων** είναι περίεργοι άνθρωποι που διαθέτουν αρκετές δεξιότητες για να τους επιτρέψουν να κάνουν πειρατεία σε ένα σύστημα και να εντοπίσουν πιθανά κενά στο σύστημα ασφάλειας δικτύου.

Ας ξεκινήσουμε!

Η τέχνη του χειρισμού ανθρώπων: Κοινωνική Μηχανική

Η κοινωνική μηχανική είναι η τέχνη της χειραγώγησης ανθρώπων, ώστε να δίνουν εμπιστευτικές πληροφορίες. Οι τύποι πληροφοριών που αναζητούν αυτού του είδους οι εγκληματίες μπορούν να ποικίλουν, αλλά όταν οι εγκληματίες στοχεύσουν κάποια άτομα συνήθως προσπαθούν να τα εξαπατήσουν έτσι ώστε να τους δώσουν τους κωδικούς τους πρόσβασης ή τις πληροφορίες των τραπεζών τους ή να αποκτήσουν πρόσβαση στον υπολογιστή τους για να εγκαταστήσουν κρυφά κακόβουλο λογισμικό.

Παρακολουθείστε αυτό το Βίντεο:
https://www.youtube.com/watch?v=Ic7scxvKQOo

Ας ξεκινήσουμε!

Πως μοιάζει μια επίθεση Κοινωνικής Μηχανικής;

Ηλεκτρονικό μήνυμα από έναν φίλο

- Εάν ένας εγκληματίας καταφέρει να χακάρει τον κωδικό ηλεκτρονικού ταχυδρομείου ενός ατόμου, έχει πρόσβαση στη λίστα επαφών αυτού του ατόμου. Μόλις ο εγκληματίας έχει αυτόν τον λογαριασμό ηλεκτρονικού ταχυδρομείου υπό τον έλεγχό του, στέλνει μηνύματα σε όλες τις επαφές του ατόμου ή αφήνει μηνύματα σε όλες τις κοινωνικές σελίδες των φίλων του ατόμου και πιθανόν στις σελίδες των φίλων του φίλου του ατόμου.

Αξιοποιώντας την εμπιστοσύνη σας και την περιέργειά σας

- Περιέχει έναν σύνδεσμο που απλά πρέπει να ανοίξετε - και επειδή ο σύνδεσμος προέρχεται από έναν φίλο και είστε περίεργοι, θα εμπιστευτείτε τον σύνδεσμο και θα κάνετε κλικ - και έτσι θα μολυνθείτε από κακόβουλο λογισμικό, με το οποίο ο εγκληματίας μπορεί να αναλάβει τον έλεγχο του υπολογιστή σας και να συλλέξει τις επαφές σας και να τους εξαπατήσει όπως ακριβώς εξαπατηθήκατε και εσείς.

Ας ξεκινήσουμε!

Πως μοιάζει μια επίθεση Κοινωνικής Μηχανικής;

Ηλεκτρονικό μήνυμα από άλλη έμπιστη πηγή

- Οι επιθέσεις ηλεκτρονικού "ψαρέματος" είναι ένα υποσύνολο στρατηγικής κοινωνικής μηχανικής που μιμείται μια αξιόπιστη πηγή και δημιουργεί ένα φαινομενικά λογικό σενάριο για την παράδοση διαπιστευτηρίων σύνδεσης ή άλλων ευαίσθητων προσωπικών δεδομένων. Σύμφωνα με τα στοιχεία του Webroot, τα χρηματοπιστωτικά ιδρύματα αντιπροσωπεύουν τη συντριπτική πλειοψηφία των εταιρειών που πλαστοπροσωπούν και, σύμφωνα με την ετήσια έκθεση Verizon Investigations Report της Verizon, οι επιθέσεις κοινωνικής μηχανικής, συμπεριλαμβανομένου του phishing και του προσχήματος (βλέπε παρακάτω), ευθύνονται για το 93% των επιτυχών παραβιάσεων δεδομένων.

Χρησιμοποιώντας μια συναρπαστική ιστορία ή πρόσχημα

- Ζητείτε επειγόντως η βοήθεια σας. Ο "φίλος" σας έχει κολλήσει στη χώρα Χ, τον έχουν ληστέψει, κτυπήσει και βρίσκεται στο νοσοκομείο. Πρέπει να στείλετε χρήματα για να επιστρέψει σπίτι και σας λένε πώς να στείλετε τα χρήματα στον εγκληματία.
- Παρουσιάζετε ένα πρόβλημα που απαιτεί να "επαληθεύσετε" τις πληροφορίες σας κάνοντας κλικ στον εμφανιζόμενο σύνδεσμο και παρέχοντας πληροφορίες στη φόρμα τους. Η τοποθεσία του συνδέσμου μπορεί να φαίνεται πολύ νόμιμη με όλα τα σωστά λογότυπα (στην πραγματικότητα, οι εγκληματίες μπορεί να έχουν αντιγράψει την ακριβή μορφή και το περιεχόμενο του νόμιμου ιστότοπου).

Ευχαριστούμε για την προσοχή σας !

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the
Erasmus+ Programme
of the European Union

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Εμβάθυνση!

Περιηγηθείτε με ασφάλεια στο διαδίκτυο και ασφαλίστε τον υπολογιστή σας

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union

Εμβάθυνση!

Πώς να αποτρέψετε τους κινδύνους: ξεκινήστε απλά

Το διαδίκτυο δεν είναι ένας ασφαλής χώρος επειδή ο κάθε Η/Υ μπορεί να είναι ένας εύκολος στόχος για τους κυβερνοεγκληματίες.

- Πρέπει να αποφεύγονται οι επικίνδυνες ιστοσελίδες που δεν διαθέτουν πιστοποιητικό ασφαλείας. Αναζητήστε το HTTPS στην αρχή της διεύθυνσης URL.
- Μήνυμα ηλεκτρονικού ταχυδρομείου από άγνωστη πηγή δεν πρέπει να ανοίξει.
- Ένα λογισμικό προστασίας από ιούς πρέπει να εγκατασταθεί για να αποτρέψει τις απειλές.

Εμβάθυνση!

Δημιουργήστε ισχυρούς κωδικούς πρόσβασης

- Ένας καλός, ισχυρός κωδικός πρόσβασης πρέπει να είναι μακρύς και σύνθετος, με μικρά γράμματα, κεφαλαία γράμματα, σύμβολα και αριθμούς.

Χρησιμοποιήστε λογισμικό ασφαλείας

- Η συσκευή σας - υπολογιστής, φορητός υπολογιστής, tablet ή έξυπνο τηλέφωνο - θα πρέπει να διαθέτει αξιόπιστο λογισμικό προστασίας από ιούς. Ενημερώστε τα τακτικά.

Προσαρμόστε τις ρυθμίσεις ασφαλείας του προγράμματος περιήγησης

- Τα πιο δημοφιλή προγράμματα περιήγησης όπως το Google Chrome, το Firefox και η Opera έχουν ειδικές ρυθμίσεις που σας επιτρέπουν να αποκλείσετε δυνητικά επιβλαβείς πόρους, όπως τα αναδυόμενα παράθυρα.

Εμβάθυνση!

Θυμηθείτε να αποσυνδεθείτε

- Όταν τελειώσετε με τη χρήση ενός ιστότοπου ή μιας εφαρμογής, βεβαιωθείτε ότι έχετε αποσυνδεθεί από αυτές, αλλιώς, καθιστάτε τα δεδομένα σας πιο ευάλωτα.

Ξανασκεφτείτε πριν κάνετε κλικ σε συνδέσμους στα μηνύματα ηλεκτρονικού ταχυδρομείου

- Οι πιθανότητες είναι ότι θα λάβετε μηνύματα από κυβερνο-εγκληματίες που τα σχεδιάζουν για να είναι πολύ πειστικά

Προσέξτε τι κάνετε λήψη

- Υπάρχουν τόσοι πολλοί διαθέσιμοι πόροι εκεί έξω, που μερικές φορές δεν δίνουμε μια δεύτερη σκέψη για το τι κατεβάζουμε. Φυσικά, το Διαδίκτυο έχει πάρα πολλούς νόμιμους ιστότοπους με ασφαλές περιεχόμενο, αλλά υπάρχουν και οι ιστότοποι που προσφέρουν επιβλαβές περιεχόμενο γεμάτο από κακόβουλο λογισμικό.

Εμβάθυνση!

Τα συμπτώματα ενός ιού!

Συχνά αναδυόμενα παράθυρα.

Τα αναδυόμενα παράθυρα ενδέχεται να σας ενθαρρύνουν να επισκεφτείτε ασυνήθιστους ιστότοπους. Ή μπορεί να σας ενθαρρύνουν να κατεβάσετε προγράμματα προστασίας από ιούς ή άλλα προγράμματα λογισμικού.

Αλλαγές στην αρχική σας σελίδα.

Η αρχική σας σελίδα μπορεί να αλλάξει σε κάποιον άλλο ιστότοπο, για παράδειγμα. Επιπλέον, ίσως δεν μπορείτε να το επαναφέρετε.

Μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από τον λογαριασμό σας.

Ένας εγκληματίας μπορεί να πάρει τον έλεγχο του λογαριασμού σας ή να στείλει μηνύματα ηλεκτρονικού ταχυδρομείου στο όνομά σας από άλλο μολυσμένο υπολογιστή.

Εμβάθυνση!

Τα συμπτώματα ενός ιού!

Συχνά Κράς.

Ένας ιός μπορεί να προκαλέσει σοβαρή ζημιά στον σκληρό σας δίσκο. Αυτό μπορεί να προκαλέσει το πάγωμα ή το κρασάρισμα της συσκευής σας. Μπορεί επίσης να εμποδίσει τη συσκευή σας να επανέλθει

Ασυνήθιστα αργή απόδοση του υπολογιστή

Μια ξαφνική αλλαγή της ταχύτητας επεξεργασίας μπορεί να σημάνει ότι ο υπολογιστής σας έχει ιό.

Άγνωστα προγράμματα που ξεκινούν όταν ενεργοποιείτε τον υπολογιστή σας

Ίσως να γνωρίζετε το άγνωστο πρόγραμμα κατά την εκκίνηση του υπολογιστή σας. Ή ίσως να το παρατηρήσετε ελέγχοντας τον κατάλογο ενεργών εφαρμογών του υπολογιστή σας.

Ασυνήθιστες δραστηριότητες όπως οι αλλαγές κωδικού πρόσβασης

Αυτό θα μπορούσε να σας εμποδίσει να συνδεθείτε στον υπολογιστή σας.

Εμβάθυνση!

Ήρθε η ώρα να δράσετε!

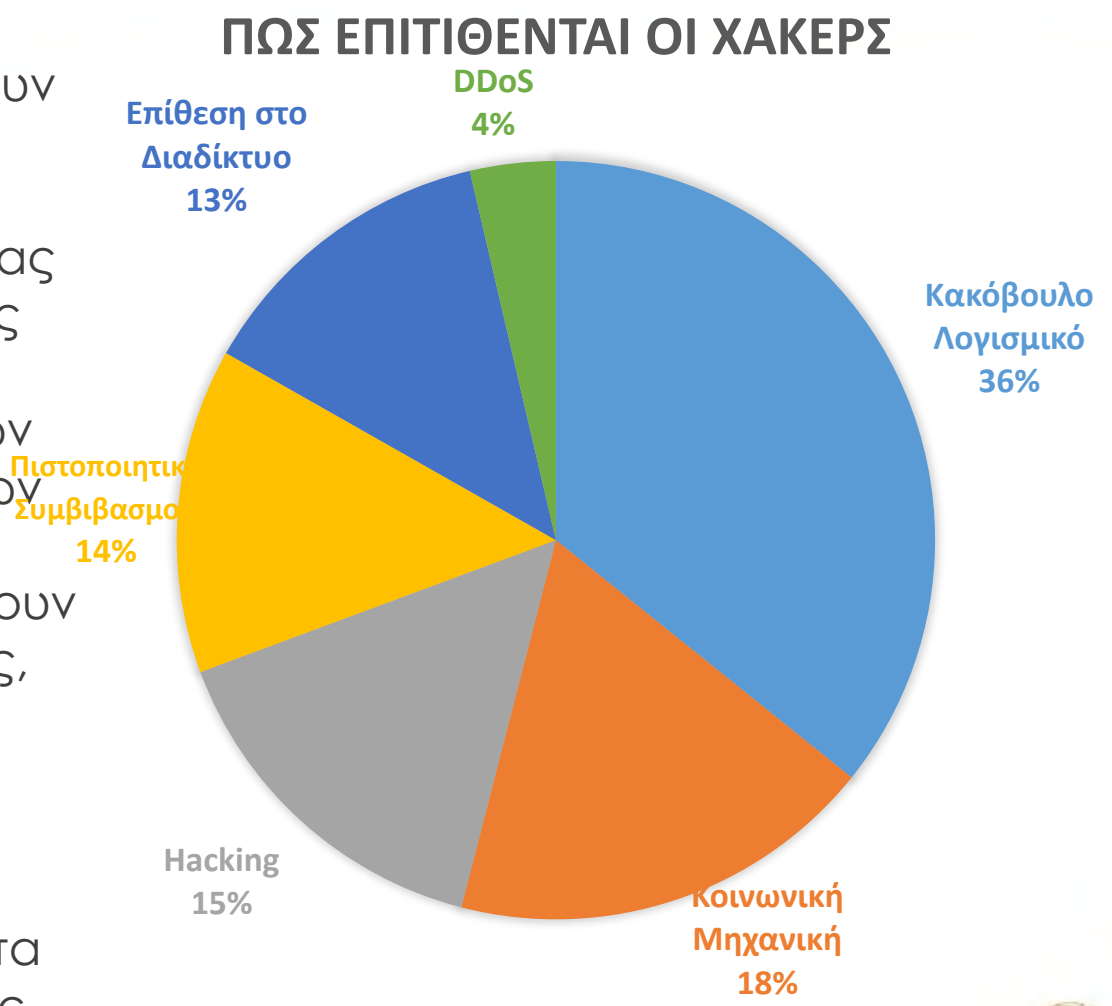
Προστατευτείτε από ιούς και κακόβουλα προγράμματα

1. Κρατήστε το λογισμικό σας ενημερωμένο
2. Μην κάνετε κλικ σε συνδέσμους εντός μηνυμάτων ηλεκτρονικού ταχυδρομείου
3. Χρησιμοποιήστε δωρεάν λογισμικό προστασίας από ιούς
4. Δημιουργήστε αντίγραφα ασφαλείας του υπολογιστή σας
5. Χρησιμοποιήστε έναν ισχυρό κωδικό πρόσβασης
6. Χρησιμοποιήστε ένα τείχος προστασίας
7. Ελαχιστοποιήστε τις λήψης.
8. Αποκλείστε τα αναδυόμενα παράθυρα

Εμβάθυνση!

Κυβερνο-επιθέσεις και ιοί: ποιος είναι πίσω τους;

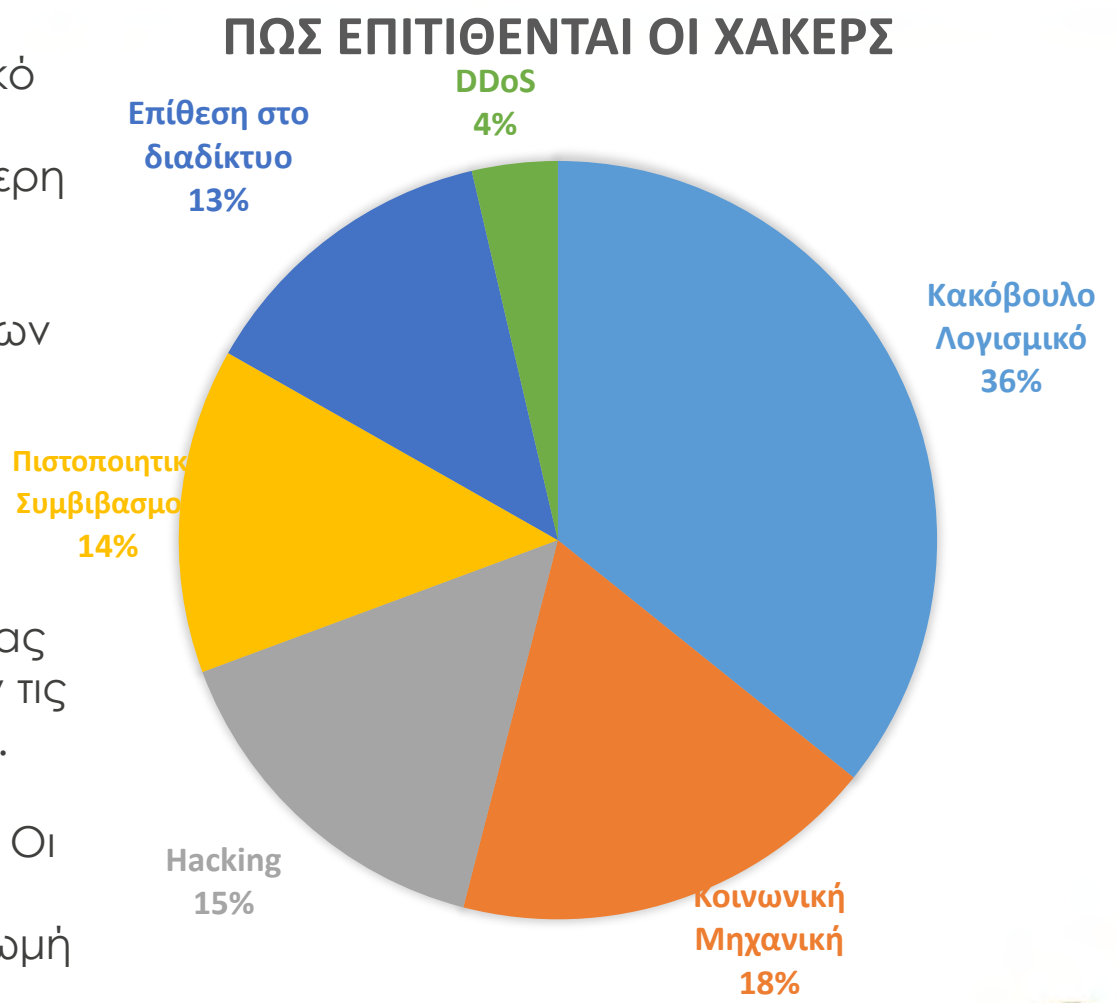
1. Κακόβουλο Λογισμικό: Οι κυβερνο-εγκληματίες κλέβουν δεδομένα από τους υπολογιστές των θυμάτων, συνήθως χρησιμοποιώντας λογισμικό υποκλοπής spyware ή απομακρυσμένη διοίκηση χρησιμοποιώντας τρωτά σημεία, κοινωνική μηχανική ή βίαιους κωδικούς πρόσβασης, φύτευση κακόβουλου λογισμικού στις συσκευές των θυμάτων μέσω μολυσμένων ιστοτόπων και αποστολή κακόβουλων συνημμένων ή συνδέσμων μέσω ηλεκτρονικού ταχυδρομείου.
2. Κοινωνική Μηχανική: Οι κυβερνο-εγκληματίες συνεχίζουν να καινοτομούν στον χώρο της κοινωνικής μηχανικής, αναπτύσσοντας νέες μεθόδους για να χειραγωγούν τους χρήστες στο να πιστεύουν ότι ένα μήνυμα, σύνδεσμος ή συνημμένο προέρχεται από αξιόπιστη πηγή και, στη συνέχεια, μολύνουν τα στοχευμένα συστήματα με κακόβουλο λογισμικό, κλέβουν χρήματα ή αποκτούν πρόσβαση σε εμπιστευτικές πληροφορίες.



Εμβάθυνση!

Κυβερνο-επιθέσεις και ιοί: ποιος είναι πίσω τους;

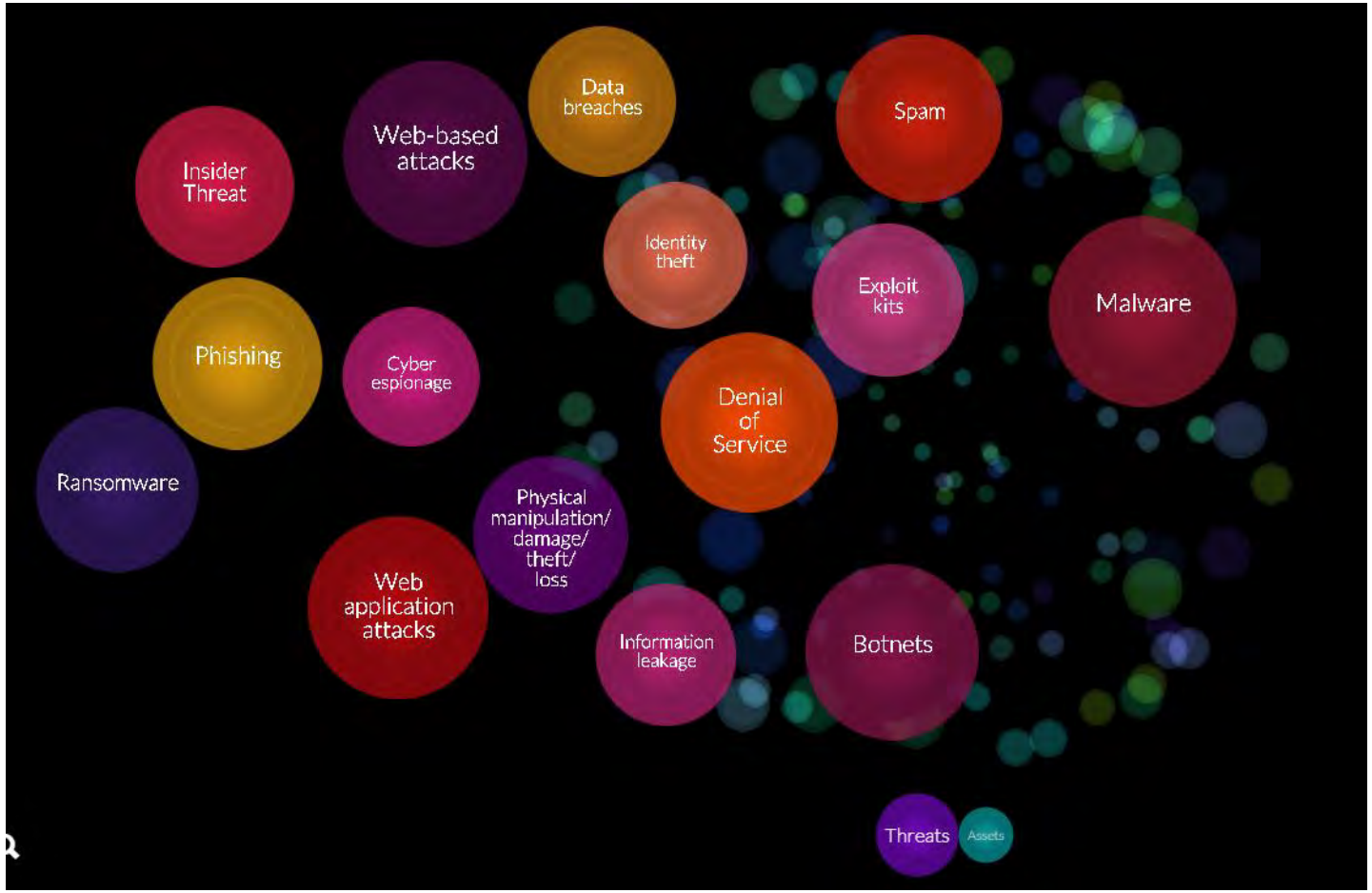
3. Hacking: η εκμετάλλευση των τρωτών σημείων στο λογισμικό και το υλικό είναι συχνά το πρώτο βήμα σε μια επίθεση, ανέφερε η έκθεση. Οι χάκερ προκαλούν σήμερα τη μεγαλύτερη ζημιά στις κυβερνήσεις, τις τράπεζες και τις πλατφόρμες κρυπτοεικονισμού.
4. Πιστοποιητικό Συμβιβασμού: Ενώ οι χρήστες των επιχειρήσεων προσβλέπουν όλο και περισσότερο σε λογισμικά για την αποθήκευση και την παρακολούθηση των κωδικών πρόσβασης, αυτά τα λογισμικά μπορούν επίσης να είναι ευάλωτα σε επίθεση, ανέφερε η έκθεση.
5. Επιθέσεις στο Διαδίκτυο: Οι εγκληματίες του κυβερνοχώρου μπορούν να αποσπάσουν τους διαχειριστές μιας ιστοσελίδας με σκοπό το κέρδος, μερικές φορές απειλώντας να κλέψουν τις βάσεις δεδομένων του πελάτη ή να κλείσουν την ιστοσελίδα.
6. DDoS: Οι επιθέσεις Άρνησης Παροχής Υπηρεσιών χτυπούν συνήθως κυβερνητικούς θεσμούς και πολιτικές εκδηλώσεις. Οι εγκληματίες εκτελούν επίσης επιθέσεις ΑΠΥ για κέρδος, θέτοντας ιστοσελίδες χωρίς σύνδεση και απαιτώντας πληρωμή από τα θύματα για να σταματήσουν την επίθεση



Εμβάνθυση!

Τσεκάρετε εδώ για να μάθετε τις μεγάλες απειλές στην Ευρώπη:

https://etl.enisa.europa.eu/#/



Εμβάνθυση!

Μερικές συμβουλές για σας

Ηρεμήστε. Οι spammers θέλουν να ενεργήσετε πρώτα και να σκεφτείτε αργότερα. Αν το μήνυμα μεταφέρει μια αίσθηση επείγουσας ανάγκης ή χρησιμοποιεί τακτικές πωλήσεων υψηλής πίεσης να είστε σκεπτικιστές, μην αφήσετε ποτέ την επείγουσα επιρροή τους να επηρεάσει την κρίση σας.

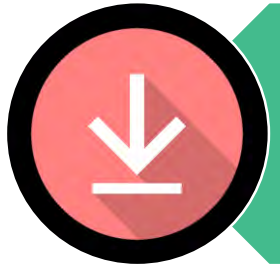
Ερευνήστε τα γεγονότα. Να είστε καχύποπτοι για τυχόν ανεπιθύμητα μηνύματα. Αν το μήνυμα ηλεκτρονικού ταχυδρομείου μοιάζει να προέρχεται από εταιρεία που χρησιμοποιείτε, κάντε τη δική σας έρευνα. Χρησιμοποιήστε μια μηχανή αναζήτησης για να μεταβείτε στην τοποθεσία της πραγματικής εταιρείας ή έναν τηλεφωνικό κατάλογο για να βρείτε τον αριθμό τηλεφώνου τους.

Μην αφήνετε έναν σύνδεσμο να ελέγχει τον ιστότοπο που επισκέπτεστε. Έχετε τον έλεγχο στα χέρια σας μόνο όταν βρίσκεται οι ίδιοι τον ιστότοπο που θέλετε να επισκεφτείτε χρησιμοποιώντας μια μηχανή αναζήτησης. Περνώντας πάνω από τις συνδέσεις στο ηλεκτρονικό ταχυδρομείο εμφανίζεται η πραγματική διεύθυνση URL στο κάτω μέρος, αλλά μια καλοφτιαγμένη απάτη μπορεί να σας καθοδηγήσει σε κακόβουλο ιστότοπο.

Εμβάθυνση!

Μερικές συμβουλές για σας

Η πειρατεία ηλεκτρονικού ταχυδρομείου είναι ανεξέλεγκτη. Οι χάκερ, οι spammers και οι κοινωνικοί μηχανικοί που καταλαμβάνουν τον έλεγχο των λογαριασμών ηλεκτρονικού ταχυδρομείου (και άλλων λογαριασμών επικοινωνίας) ανθρώπων έχουν γίνει πολύ συνηθισμένοι. Αφού ελέγξουν έναν λογαριασμό ηλεκτρονικού ταχυδρομείου, τρέφονται με την εμπιστοσύνη των επαφών του ατόμου. Ακόμη και όταν ο αποστολέας φαίνεται να είναι κάποιος που γνωρίζετε, αν δεν περιμένετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου με σύνδεσμο ή συνημμένου επικοινωνήστε με τον φίλο σας πριν ανοίξετε τον σύνδεσμο ή τον μεταφορτώσετε.



Προσέχετε όταν πρόκειται για λήψη. Αν δεν γνωρίζετε προσωπικά τον αποστολέα τότε η λήψη οποιουδήποτε αρχείου είναι λάθος.

Οι ξένες προσφορές είναι ψεύτικες. Εάν λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από ξένη λαχειοφόρο αγορά , ή για χρήματα από έναν άγνωστο συγγενή ή αιτήματα για μεταφορά κεφαλαίων από μια ξένη χώρα με υπόσχεση για ένα μερίδιο των χρημάτων, είναι σίγουρο ότι είναι απάτη.

Εμβάνθυση!

Μάθετε ποιος είναι υπεύθυνος για να σας προστατεύσει!

European Union Agency for Network and information Security: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

EUROPOL: https://www.europol.europa.eu/newsroom/news/15-ways-you-could-be-next-victim-of-cybercrime

Ευχαριστούμε για την προσοχή σας!

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Σύνοψη!

Περιηγηθείτε με ασφάλεια στο διαδίκτυο και ασφαλίστε τον υπολογιστή σας

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union

Σύνοψη!

Τι έμαθα?

Ελέγξτε τι κάνετε τώρα για να προστατέψετε τον υπολογιστή σας από ιούς ή να πλοηγηθείτε με ασφάλεια.

Υπάρχουν αλλαγές που θα κάνατε μετά από αυτή τη σειρά μαθημάτων;

Σύνοψη!

Πώς να προστατεύσετε τον υπολογιστή σας από ιούς και χάκερ

Σύνοψη!

Κοινωνική μηχανική - Πώς να εξαπατήσετε οτιδήποτε

Ερωτηματολόγιο Αξιολόγησης

Εξωτερικές Πηγές

Ευχαριστούμε για την προσοχή σας!

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union