Erasmus+

GoDIGITAL

Αναλυτικό Κείμενο

SPOŁECZNA AKADEMIA NAUK
UNIVERSITY OF SOCIAL SCIENCES

EUnipartners

PUBLICA FIDES

Emphasys CENTRE

2.2 ΑΝΑΛΥΤΙΚΟ ΚΕΙΜΕΝΟ

2.2.1 ΘΕΜΑ 1: ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Το Διαδίκτυο θα μπορούσε να συγκριθεί με τον ωκεανό. Ο ωκεανός μπορεί να είναι ένα πολύ επικίνδυνο μέρος: οι άνθρωποι μπορούν να χαθούν ή να πνιγούν προσπαθώντας να απολαύσουν τη θάλασσα ή να εξερευνήσουν τη μαγευτική απεραντοσύνη της. Αλλά η μητέρα στη φωτογραφία δεν απαγορεύει την επαφή των παιδιών της με τη θάλασσα. Αντίθετα, τα διατηρεί σε επαφή μαζί της και τα διδάσκει να την απολαμβάνουν, εξηγώντας τους κάποιους κανόνες για την ασφαλή "χρήση" της. Στην αρχή στέκεται δίπλα τους και τα συμβουλεύει με απώτερο σκοπό να αποκτήσουν σταδιακά αυτονομία και να απολαύσουν μόνα τους τη θάλασσα αργότερα.

Έτσι ακριβώς πρέπει να σκεφτούμε και τη χρήση του Διαδικτύου. Πρέπει να εντοπίσουμε τους πιθανούς κινδύνους του διαδεδομένου πλέον Διαδικτύου και να αποκτήσουμε γνώσεις και τρόπους για να αποφύγουμε όλες τις πιθανές κακοτοπιές. Στη συνέχεια, οι νέοι σπουδαστές είναι απαραίτητο να μυηθούν στην υιοθέτηση καλών πρακτικών σε σχέση με την ασφαλή χρήση του Διαδικτύου.

Οι κίνδυνοι στο Διαδίκτυο είναι πολλών ειδών. Περιγράφουμε δέκα (10) από τους σημαντικότερους κινδύνους:

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

1. Ο εθισμός στο Διαδίκτυο και η αποξένωση των χρηστών από τον πραγματικό κόσμο
2. Ακατάλληλο και προσβλητικό περιεχόμενο ιστότοπου
3. Ανεπιθύμητα μηνύματα (spam)
4. Εκφοβισμός στο Διαδίκτυο
5. Ηλεκτρονική αποπλάνηση των χρηστών - Αναφορά σχετικά με την παιδική πορνογραφία, τα τυχερά παιχνίδια στο Διαδίκτυο, τα βίαια παιχνίδια και άλλες επιβλαβείς συμπεριφορές
6. Παραβίαση της ιδιωτικής ζωής των χρηστών
7. Παραπληροφόρηση που διαδόθηκε στο Διαδίκτυο (ψευδείς ειδήσεις, αστικοί μύθοι, ψηφιακές φάρσες)
8. Παρακράτηση δεδομένων προσωπικού χαρακτήρα μέσω "phishing" και "pharming"
9. Κακόβουλο λογισμικό που μολύνει τους υπολογιστές
10. Προβλήματα υγείας που προκύπτουν από παρατεταμένη χρήση υπολογιστών

Θεωρούμε ότι σήμερα, η θεωρητική γνώση των παραπάνω δεν αρκεί για έναν δάσκαλο. Απαιτείται εξοικείωση και πρακτικές γνώσεις. Για το λόγο αυτό, στις επόμενες παραγράφους θα αναπτυχθούν ορισμένα τεχνικά ζητήματα, έτσι ώστε οι χρήστες, και ειδικότερα οι εκπαιδευτικοί, να είναι υποψιασμένοι, αλλά και να μπορούν να αντιδρούν σε ενδεχόμενους κινδύνους στο Διαδίκτυο, προστατεύοντας και εκπαιδεύοντας ταυτόχρονα και αναλόγως τους μαθητές τους από μικρή ηλικία.

2.2.1.1 Πώς να αποφύγετε κακές τοποθεσίες

Πριν ξεκινήσουμε να εξετάζουμε τρόπους αποφυγής των "κακών" ιστότοπων, πρέπει να απαντήσουμε στην ερώτηση: πότε ένας ιστότοπος θεωρείται "κακός"; "Κακός" θεωρείται γενικά οποιοσδήποτε ιστότοπος περιέχει υλικό που εμπίπτει στις κατηγορίες 1 έως 8, όπως αυτές αναφέρονται στην παραπάνω εισαγωγή.

Μερικοί από τους τρόπους αποφυγής αυτού του είδους των ιστότοπων είναι οι εξής:

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

- **Χρησιμοποιήστε φίλτρα Διαδικτύου**
  Υπάρχουν πολλά φίλτρα Διαδικτύου που κάποιος μπορεί να αγοράσει ή να "κατεβάσει", τα οποία θα αποτρέψουν αυτόν ή μέλη της οικογένειάς του να ανοίξουν τυχόν αμφισβητούμενες τοποθεσίες στο Διαδίκτυο. Αυτά τα φίλτρα λειτουργούν παρεμποδίζοντας την πρόσβαση των χρηστών σε ιστότοπους που θεωρούνται αμφισβητήσιμοι από άποψη ασφάλειας ή παρουσιάζουν ακατάλληλο περιεχόμενο ή περιεχόμενο NSFW (δεν είναι ασφαλές για εργασία). Πολλοί γονείς χρησιμοποιούν αυτά τα φίλτρα για να βεβαιωθούν ότι τα παιδιά τους επισκέπτονται μόνο ιστότοπους κατάλληλους για την ηλικία τους, αλλά άτομα κάθε ηλικίας καθώς και εκπαιδευτικοί μπορούν να τα χρησιμοποιήσουν για να βεβαιωθούν ότι οι αναζητήσεις τους στον Παγκόσμιο Ιστό είναι πάντα ασφαλείς.

- **Επωφεληθείτε από τα ενσωματωμένα φίλτρα των μηχανών αναζήτησης**
  Πολλές μηχανές αναζήτησης δίνουν στους χρήστες του Διαδικτύου τη δυνατότητα να επιλέγουν μια "ασφαλέστερη" αναζήτηση όταν χρησιμοποιούν τις υπηρεσίες τους. Για παράδειγμα, η Google προσφέρει "φιλτράρισμα ασφαλών αναζητήσεων". Αυτό ισχύει για όλες τις αναζητήσεις εικόνων και βίντεο, καθώς επίσης για τις ειδήσεις αλλά και τις αναζητήσεις γενικότερου περιεχομένου.

- **Μην μαντεύετε τη διεύθυνση μιας τοποθεσίας Web**
  Αυτός είναι ίσως ο "νούμερο ένα" τρόπος με τον οποίο οι χρήστες του Διαδικτύου παγιδεύονται. Στο Διαδίκτυο υπάρχουν πολλοί ιστότοποι που χρησιμοποιούν παρόμοιες διευθύνσεις με νόμιμους και ασφαλείς ιστότοπους, έτσι ώστε όταν οι χρήστες προσπαθούν να θυμηθούν ποιον ιστότοπο επιθυμούν να επισκεφθούν, καταλήγουν τυχαία σε λάθος τοποθεσία.

- **Ποτέ μην κάνετε κλικ σε ιστότοπους που αμφισβητείτε**
  Όταν κάποιος αμφιβάλλει, καλύτερα να μην κάνει "κλικ". Εάν η περιγραφή του ιστότοπου, ο τίτλος ή η διεύθυνση URL μοιάζουν αμφισβητήσιμα, καλό είναι ο χρήστης να βρει έναν άλλο ιστότοπο περισσότερο αξιόπιστο, ειδικά όταν θέλει να χρησιμοποιήσει το περιεχόμενό του για έρευνα.

2.2.1.2 Εισαγωγή στο κακόβουλο λογισμικό – Πώς να το αποφύγετε

Ο κίνδυνος με τον αριθμό 9 στην εισαγωγή αναφέρεται στο κακόβουλο λογισμικό. Το κακόβουλο λογισμικό είναι ένας όρος που χρησιμοποιείται για το λογισμικό που έχει σχεδιαστεί για να κάνει ζημιές ή ανεπιθύμητες ενέργειες σε ένα σύστημα υπολογιστή. Παραδείγματα κακόβουλου λογισμικού είναι τα ακόλουθα: Ιοί, σκουλήκια, δούρειοι ίπποι, λογισμικό κατασκοπίας και λογισμικό παραπλάνησης.

Erasmus+

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

Ακολουθεί μια σύντομη περιγραφή καθενός από αυτούς τους τύπους κακόβουλου λογισμικού, έτσι ώστε ο δάσκαλος να είναι εξοικειωμένος με την ορολογία και ειδικά με τον τρόπο που κάθε ένα από αυτά τα λογισμικά λειτουργεί.

- **Ιοί υπολογιστών**

  Ο ιός υπολογιστών είναι ένα μικρό πρόγραμμα λογισμικού που απλώνεται από τον έναν υπολογιστή στον άλλο και παρεμβαίνει στη λειτουργία του υπολογιστή. Ένας ιός υπολογιστών μπορεί να καταστρέψει ή να διαγράψει ορισμένα δεδομένα σε έναν υπολογιστή, να χρησιμοποιήσει ένα πρόγραμμα ηλεκτρονικού ταχυδρομείου για να διαδώσει τον ιό σε άλλους υπολογιστές ή ακόμα και να διαγράψει όλα τα δεδομένα από το σκληρό δίσκο.

  Οι ιοί υπολογιστών συχνά μεταδίδονται από συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου ή με άμεσα μηνύματα. Ως εκ τούτου, ο χρήστης δεν πρέπει ποτέ να ανοίγει ένα συνημμένο αρχείο ηλεκτρονικού ταχυδρομείου εκτός αν γνωρίζει ποιος έστειλε το μήνυμα. Οι ιοί μπορούν να κρύβονται σε αστείες εικόνες, ευχετήριες κάρτες ή αρχεία ήχου και βίντεο. Οι ιοί υπολογιστών διαδίδονται, επίσης, μέσω λήψης αρχείων από το Διαδίκτυο (download). Μπορεί ακόμα να κρύβονται σε πειρατικό λογισμικό ή σε άλλα αρχεία/προγράμματα που κάποιος “κατεβάσει” στον υπολογιστή του.

- **Σκουλήκια υπολογιστών**

  Ένα σκουλήκι είναι κώδικας υπολογιστή που εξαπλώνεται χωρίς την αλληλεπίδραση χρηστών. Τα περισσότερα σκουλήκια ξεκινούν ως συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου που μολύνουν έναν υπολογιστή όταν ανοίξουν. Το σκουλήκι σαρώνει το μολυσμένο υπολογιστή για αρχεία, όπως βιβλία διευθύνσεων ή προσωρινές ιστοσελίδες, που περιέχουν διευθύνσεις ηλεκτρονικού ταχυδρομείου. Το σκουλήκι χρησιμοποιεί τις διευθύνσεις για να στείλει μολυσμένα μηνύματα ηλεκτρονικού ταχυδρομείου και συχνά μιμείται τις διευθύνσεις "Από" σε μεταγενέστερα μηνύματα ηλεκτρονικού ταχυδρομείου, έτσι ώστε αυτά τα μολυσμένα μηνύματα να φαίνονται από κάποιον που γνωρίζετε. Τα σκουλήκια μεταδίδονται αυτόματα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, δικτύων ή τρωτών σημείων του λειτουργικού συστήματος, συχνά συντρίβοντας αυτά τα συστήματα πριν γίνει γνωστό το αίτιο. Τα σκουλήκια δεν είναι πάντοτε καταστροφικά για τους

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

υπολογιστές, αλλά συνήθως προκαλούν προβλήματα στην υπολογιστική ισχύ και απόδοση ενός δικτύου καθώς και προβλήματα σταθερότητας.

- **Δούρειοι ίπποι**
  Ένας δούρειος ίππος είναι ένα κακόβουλο πρόγραμμα λογισμικού που κρύβεται μέσα σε άλλα προγράμματα. Εισέρχεται σε έναν υπολογιστή κρυμμένο μέσα σε ένα νόμιμο πρόγραμμα, όπως μια προφύλαξη οθόνης (screen saver). Στη συνέχεια, εγκαθιστά κώδικα στο λειτουργικό σύστημα, ο οποίος επιτρέπει σε έναν χάκερ να έχει πρόσβαση στο μολυσμένο υπολογιστή. Οι δούρειοι ίπποι συνήθως δεν διαδίδονται από μόνοι τους. Διαδίδονται μέσω ιών, σκουληκιών ή λήψης λογισμικού από το Διαδίκτυο.

- **Λογισμικό κατασκοπίας**
  Το λογισμικό κατασκοπίας μπορεί να εγκατασταθεί σε έναν υπολογιστή χωρίς ο χρήστης να το αντιληφθεί. Αυτού του είδους τα προγράμματα μπορούν να αλλάξουν τις παραμέτρους διαμόρφωσης του υπολογιστή ή να συλλέξουν διαφημιστικά δεδομένα και προσωπικά στοιχεία. Το λογισμικό κατασκοπείας μπορεί να παρακολουθήσει τις συνήθειες αναζήτησης του χρήστη στο Διαδίκτυο και μπορεί, επίσης, να ανακατευθύνει το πρόγραμμα περιήγησης στον Παγκόσμιο Ιστό σε έναν διαφορετικό ιστότοπο από αυτόν στον οποίο ο χρήστης προτίθεται να μεταβεί.

- **Λογισμικό παραπλάνησης**
  Ένα λογισμικό παραπλάνησης προσπαθεί να κάνει το χρήστη να πιστέψει ότι ο υπολογιστής του είναι μολυσμένος από έναν ιό και συνήθως τον προτρέπει να κατεβάσει ή να αγοράσει ένα προϊόν που αφαιρεί τον ιό αυτό. Τα ονόματα αυτών των προϊόντων περιέχουν συχνά λέξεις όπως Antivirus, Shield, Security, Protection, ή Fixer. Οι λέξεις αυτές το κάνουν να μοιάζει νόμιμο. Τα προγράμματα αυτού του τύπου συχνά “τρέχουν” αμέσως μετά την λήψη τους ή κατά την επόμενη εκκίνηση του υπολογιστή. Τα λογισμικά παραπλάνησης - υποκλοπής είναι δυνατό να εμποδίσουν το άνοιγμα εφαρμογών, όπως για παράδειγμα ο Internet Explorer. Ενδέχεται επίσης, να εμφανίζουν νόμιμα και σημαντικά αρχεία των Windows ως μολύνσεις.

Προκειμένου να αποφύγει όλα αυτά τα είδη κακόβουλου λογισμικού, ο χρήστης του Διαδικτύου πρέπει να εξοικειωθεί με ορισμένες τεχνικές όπως:

- Εγκατάσταση ποιοτικών προγραμμάτων προστασίας από ιούς

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

- Εγκατάσταση προγραμμάτων προστασίας κατά των προγραμμάτων κατασκοπίας σε πραγματικό χρόνο
- Συνεχής αναβάθμιση (τελευταία έκδοση) των εγκατεστημένων εφαρμογών κατά του κακόβουλου λογισμικού
- Καθημερινή σάρωση του Η/Υ για εντοπισμό κακόβουλου λογισμικού
- Απενεργοποίηση του autorun
- Απενεργοποίηση της προεπισκόπησης εικόνων στο Outlook
- Αποφυγή κλικ σε συνδέσμους ηλεκτρονικού ταχυδρομείου ή συνημμένα αρχεία
- Έξυπνο σερφάρισμα
- Χρήση τείχους προστασίας βασισμένου στο υλικό του Η/Υ
- Ανάπτυξη προστασίας DNS

Ωστόσο, το κακόβουλο λογισμικό μπορεί να προληφθεί εύκολα αρκεί να έχουμε έξυπνη ηλεκτρονική συμπεριφορά. Ο κύριος παράγοντας για την πρόληψη μολύνσεων από κακόβουλο λογισμικό σε έναν Η/Υ είναι ο ίδιος ο χρήστης. Οι χρήστες υπολογιστών δε χρειάζονται άπειρες ειδικές γνώσεις ή υψηλή ειδική εκπαίδευση. Χρειάζονται μόνο επαγρύπνηση για να αποφύγουν τη λήψη και την εγκατάσταση οποιουδήποτε προγράμματος δεν αντιλαμβάνονται ή δεν εμπιστεύονται, ανεξάρτητα από το πόσο δελεαστικό αυτό παρουσιάζεται, από τις ακόλουθες πηγές:

- **Από έναν ιστότοπο:** Εάν δεν είστε σίγουροι, αφήστε τον ιστότοπο και αναζητήστε το λογισμικό που σας ζητείται να εγκαταστήσετε. Εάν είναι εντάξει, μπορείτε πάντα να επιστρέψετε στο site και να το εγκαταστήσετε. Αν δεν είναι εντάξει, θα αποφύγετε έναν πονοκέφαλο κακόβουλου λογισμικού.
- **Από το ηλεκτρονικό ταχυδρομείο:** Μην εμπιστεύεστε τίποτα που σχετίζεται με ένα μήνυμα ηλεκτρονικού ταχυδρομείου ανεπιθύμητης αλληλογραφίας. Προσεγγίστε τα μηνύματα ηλεκτρονικού ταχυδρομείου από άτομα που γνωρίζετε με προσοχή όταν αυτά περιέχουν συνδέσμους ή συνημμένα αρχεία. Αν έχετε αμφιβολίες για όσα σας ζητούνται να δείτε ή να εγκαταστήσετε, μην το κάνετε.
- **Από τα φυσικά μέσα:** Οι φίλοι, οι συγγενείς και οι συνεργάτες σας μπορεί να σας δώσουν εν αγνοία τους σκληρό δίσκο ή άλλη αποθηκευτική μονάδα με ένα ή και περισσότερα μολυσμένα αρχεία. Μη δεχτείτε τυφλά αυτά τα αρχεία. Πραγματοποιήστε σάρωση με λογισμικό ασφαλείας. Εάν δεν είστε σίγουροι, μην αποδεχτείτε τα αρχεία.
- **Από ένα αναδυόμενο παράθυρο:** Ορισμένα αναδυόμενα παράθυρα ή πλαίσια θα προσπαθήσουν να σας καθοδηγήσουν στη λήψη λογισμικού ή στην αποδοχή μιας δωρεάν "σάρωσης συστήματος" κάποιου τύπου. Συχνά αυτά τα αναδυόμενα παράθυρα θα χρησιμοποιήσουν τακτικές για να σας κάνουν να πιστεύετε ότι

Erasmus+

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

χρειάζεστε αυτό που προσφέρουν για να είστε ασφαλείς. Κλείστε το αναδυόμενο παράθυρο χωρίς να κάνετε κλικ σε κάτι μέσα σε αυτό (συμπεριλαμβανομένου του Χ στη γωνία). Κλείστε το παράθυρο μέσω του Task Manager των Windows (πατήστε Ctrl-Alt-Delete).

- **Από άλλο λογισμικό:** Ορισμένα προγράμματα επιχειρούν να εγκαταστήσουν κακόβουλο λογισμικό ως μέρος της δικής τους διαδικασίας εγκατάστασης. Κατά την εγκατάσταση λογισμικού, δώστε ιδιαίτερη προσοχή στα πλαίσια μηνυμάτων πριν κάνετε κλικ στο κουμπί "Επόμενο", "Εντάξει" ή "Συμφωνώ". Σαρώστε τους όρους συμφωνίας με το χρήστη για οτιδήποτε υποδηλώνει ότι κακόβουλο λογισμικό μπορεί να αποτελεί μέρος της εγκατάστασης. Αν δεν είστε σίγουροι, ακυρώστε την εγκατάσταση, ελέγξτε το πρόγραμμα και εκτελέστε ξανά την εγκατάσταση μόνο αφού διαπιστώσετε ότι είναι ασφαλής.
- **Από παράνομες υπηρεσίες κοινής χρήσης αρχείων:** Είστε πραγματικά μόνοι αν μπείτε σε αυτή τη σφαίρα. Υπάρχει ελάχιστος ποιοτικός έλεγχος στον κόσμο του παράνομου λογισμικού και είναι εύκολο για έναν εισβολέα να ονομάσει ένα κομμάτι κακόβουλου λογισμικού με το όνομα μιας δημοφιλούς ταινίας, άλμπουμ ή προγράμματος προκειμένου να σας βάλει σε πειρασμό να το "κατεβάσετε".

2.2.1.3. Πώς να αφαιρέσετε κακόβουλο λογισμικό

Εάν κάποιος υποπτεύεται ότι υπάρχει κακόβουλο λογισμικό στον Η/Υ του - ή απλά θέλει να είναι προσεκτικός - υπάρχουν μερικά βήματα που πρέπει να ακολουθήσει.

α) Δημιουργία αντιγράφων ασφαλείας όλων των αρχείων και άλλων δεδομένων

Τα αρχεία και τα δεδομένα είναι πολύ σημαντικά. Επομένως, τη στιγμή που κάποιος αντιληφθεί ότι ο υπολογιστής του είναι μολυσμένος με κακόβουλο λογισμικό, πρέπει να δημιουργήσει αντίγραφα ασφαλείας όλων των αρχείων και άλλων δεδομένων, προτού το κακόβουλο λογισμικό φτάσει σε αυτά και τα μολύνει. Η ενέργεια αυτή θα βοηθήσει το χρήστη να επανέλθει γρήγορα στην κανονικότητά του.

Erasmus+

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

β) Αποσύνδεση από το Διαδίκτυο
Η αμέσως επόμενη καλύτερη ενέργεια είναι η αποσύνδεση του υπολογιστή από το Διαδίκτυο προκειμένου να αποφευχθούν περαιτέρω ζημιές, καθώς το Διαδίκτυο είναι ο τόπος αναπαραγωγής του κακόβουλου λογισμικού. Και κάθε στιγμή που ο χρήστης παραμένει συνδεδεμένος με αυτό, ειδικά μετά από μια "λοίμωξη" κακόβουλου λογισμικού, μόνο θα επιδεινώνει την κατάστασή του.

γ) Σάρωση υπολογιστή σε ασφαλή λειτουργία
Μεταβείτε σε ασφαλή λειτουργία και σαρώστε τον υπολογιστή. Χωρίς να μπούμε σε τεχνικές λεπτομέρειες, η ασφαλής λειτουργία είναι μια περιορισμένη λειτουργία που επιτρέπει μόνο την εκτέλεση υγιειών εφαρμογών, μειώνοντας έτσι τον κίνδυνο εξάπλωσης κακόβουλου λογισμικού σε άλλα μέρη του υπολογιστή. Στην καλύτερη περίπτωση, ένας τέτοιος καθαρισμός μπορεί να βελτιώσει την απόδοση του υπολογιστή. Ένα άλλο απλό αλλά αποτελεσματικό μέτρο θα ήταν να καθαρίσετε τα προσωρινά καθώς και τα αρχεία λήψης.

δ) Χρήση του εργαλείου αφαίρεσης κακόβουλου λογισμικού
Εάν δεν υπάρχει ήδη, κατεβάστε ένα νόμιμο πρόγραμμα κατά του κακόβουλου λογισμικού. Στη συνέχεια, εγκαταστήστε το και εκτελέστε το. Αυτά τα προγράμματα έχουν σχεδιαστεί για την αναζήτηση και την εξάλειψη κάθε κακόβουλου λογισμικού σε μια ηλεκτρονική συσκευή.

Μόλις η συσκευή είναι "καθαρή", καλό θα ήταν να αλλάξετε τους κωδικούς πρόσβασης, όχι μόνο για τον υπολογιστή ή την κινητή συσκευή, αλλά και για το ηλεκτρονικό ταχυδρομείο, τους λογαριασμούς στα μέσα κοινωνικής δικτύωσης, τους αγαπημένους ιστότοπους αγορών και για τις ηλεκτρονικές τραπεζικές συναλλαγές.

Η αφαίρεση κακόβουλων προγραμμάτων δεν είναι ούτε εύκολη ούτε ελκυστική υπόθεση. Επομένως, είναι καλύτερα να αφήσουμε τους ειδικούς να χειριστούν την κατάσταση αν νομίζουμε ότι δεν μπορούμε να λύσουμε το πρόβλημα μόνοι μας.

2.2.1.4 Διασφάλιση λογαριασμών στο Διαδίκτυο

Οι κωδικοί πρόσβασης είναι σαν τα κλειδιά του προσωπικού μας σπιτιού στον Παγκόσμιο Ιστό. Πρέπει να κάνουμε ό,τι μπορούμε για να εμποδίσουμε άλλους ανθρώπους να αποκτήσουν πρόσβαση στο δικό μας κωδικό. Μπορούμε να διασφαλίσουμε περαιτέρω τους λογαριασμούς μας χρησιμοποιώντας πρόσθετες μεθόδους ελέγχου ταυτότητας. Μερικές βασικές συμβουλές είναι:

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

- Απενεργοποίηση λογαριασμών που δε χρησιμοποιούνται για μεγάλο χρονικό διάστημα
- Δημιουργία ισχυρού κωδικού πρόσβασης (π.χ. κωδικός: ολόκληρη πρόταση)
- Μοναδικός λογαριασμός - μοναδικός κωδικός πρόσβασης
- Καταγραφή και αποθήκευση κωδικού σε ασφαλές μέρος
- Αλλαγή των κωδικών πρόσβασης τακτικά
- Κλείδωμα σύνδεσης (ισχυρός έλεγχος ταυτότητας)
- Έλεγχος δραστηριότητας λογαριασμών
- Τακτική ενημέρωση λογισμικού (τελευταία έκδοση)
- Καθορισμός αξιόπιστων επαφών

Περισσότερες πληροφορίες για την ασφάλεια στο Διαδίκτυο μπορείτε να βρείτε στην προτεινόμενη πρόσθετη βιβλιογραφία.

2.2.1.5 GDPR

Ένα άλλο σημαντικό θέμα που πρέπει να γνωρίζουν οι εκπαιδευτικοί είναι το GDPR. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR) είναι ένας κανονισμός της νομοθεσίας της ΕΕ για την προστασία των δεδομένων και την ιδιωτική ζωή όλων των ατόμων εντός της Ευρωπαϊκής Ένωσης (ΕΕ) και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Αφορά επίσης την εξαγωγή δεδομένων προσωπικού χαρακτήρα εκτός των περιοχών της ΕΕ και του ΕΟΧ. Το GDPR στοχεύει πρωτίστως στον έλεγχο που έχουν τα άτομα σχετικά με τα προσωπικά τους δεδομένα και στην απλούστευση του ρυθμιστικού περιβάλλοντος για τις διεθνείς επιχειρήσεις με την ενοποίηση του κανονισμού εντός της ΕΕ. Ο κανονισμός περιέχει διατάξεις και απαιτήσεις σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα ατόμων (επίσημα ονομαζόμενων υποκειμένων δεδομένων στο GDPR) εντός του ΕΟΧ και ισχύει για μια επιχείρηση εγκατεστημένη στον ΕΟΧ ή - ανεξαρτήτως της θέσης της και της ιθαγένειας των προσώπων στα οποία αναφέρονται τα δεδομένα - που επεξεργάζεται τις προσωπικές πληροφορίες των υποκειμένων των δεδομένων εντός του ΕΟΧ.

Οι υπεύθυνοι επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την εφαρμογή των αρχών προστασίας δεδομένων. Οι επιχειρηματικές διαδικασίες που χειρίζονται τα προσωπικά δεδομένα πρέπει να σχεδιάζονται και να κατασκευάζονται λαμβάνοντας υπόψη τις αρχές

Erasmus+

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

και να παρέχουν διασφαλίσεις για την προστασία των δεδομένων (για παράδειγμα, χρησιμοποιώντας pseudonymization ή πλήρες ανώνυμο, όπου χρειάζεται) και να χρησιμοποιούν τις υψηλότερες δυνατές ρυθμίσεις απορρήτου από προεπιλογή. Δεν επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, εκτός εάν γίνεται σύμφωνα με τη νομοθεσία που ορίζεται από τον κανονισμό ή εκτός εάν ο υπεύθυνος επεξεργασίας ή ο μεταποιητής έχει λάβει σαφή και εξατομικευμένη επιβεβαίωση της συναίνεσης από το υποκείμενο των δεδομένων. Το υποκείμενο των δεδομένων έχει το δικαίωμα να ανακαλέσει αυτή τη συγκατάθεση ανά πάσα στιγμή. (Από την Βικιπαίδεια, την ελεύθερη εγκυκλοπαίδεια)

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543