Περραιβού 40, Άνω Τούμπα
54352, Θεσσαλονίκη
W: www.servicepack.gr
T: 2310.943.054
M: 6978.284.405
E: info@servicepack.gr

Κορυφαίες συμβουλές πρόληψης

Η πρόληψη των κυβερνοεγκλημάτων μπορεί να είναι πολύ απλή, η Service Pack σας δίνει κάποιες χρήσιμες και απλές συμβουλές. Όταν είστε οπλισμένοι με λίγες τεχνικές συμβουλές και κοινή λογική, μπορείτε να αποφύγετε πολλές επιθέσεις. Μην ξεχνάτε, οι online εγκληματίες προσπαθούν να κερδίσουν χρήματα με τη μεγαλύτερη δυνατή ταχύτητα και ευκολία. Όσο πιο πολύ τους δυσκολεύετε το έργο, τόσο πιο πιθανό είναι να σας αφήσουν ήσυχους και να περάσουν σε έναν πιο εύκολο στόχο. Οι παρακάτω συμβουλές παρέχουν βασικές πληροφορίες για το πώς μπορείτε να διαφυλάσσετε τον υπολογιστή και την ταυτότητά σας.

1. Προστατεύετε τον υπολογιστή σας με λογισμικό ασφαλείας.
2. Βεβαιωθείτε ότι ο υπολογιστής σας είναι διαμορφωμένος με ασφάλεια.
3. Επιλέγετε ισχυρούς κωδικούς πρόσβασης και διατηρείτε τους με ασφάλεια.
4. Θωρακίστε τα προσωπικά σας δεδομένα.
5. Αν σας φαίνεται ότι μια online προσφορά φαίνεται πολύ καλή για να είναι αληθινή, μάλλον έτσι είναι.
6. Ελέγχετε τακτικά τα αντίγραφα κινήσεων τραπεζικών λογαριασμών και πιστωτικών καρτών.
7. Αποφύγετε «πειράματα» με προγράμματα και παιχνίδια αμφίβολης προέλευσης.

1. Προστατεύετε τον υπολογιστή σας με λογισμικό ασφαλείας.

Για βασική ασφάλεια online, είναι αναγκαίοι διάφοροι τύποι λογισμικού ασφαλείας. Τα βασικά προγράμματα λογισμικού ασφαλείας περιλαμβάνουν προγράμματα firewall και antivirus. Ένα firewall είναι συνήθως η πρώτη γραμμή άμυνας του υπολογιστή σας: Ελέγχει ποιος και τι μπορεί να επικοινωνεί με τον υπολογιστή σας online. Μπορείτε να δείτε το firewall ως κάποιο είδος "τροχονόμου" που παρακολουθεί όλα τα δεδομένα που προσπαθούν να ανταλλαχθούν μεταξύ του υπολογιστή σας και του Internet, επιτρέποντας όσες επικοινωνίες γνωρίζει ότι είναι ασφαλείς και μπλοκάροντας την "ακατάλληλη" κυκλοφορία δεδομένων, όπως οι επιθέσεις, από το να φτάσει καν στον υπολογιστή σας.

Η επόμενη γραμμή άμυνας είναι το λογισμικό σας antivirus, που παρακολουθεί όλες τις online δραστηριότητες και προστατεύει τον υπολογιστή σας από ιούς, worms, trojan horses και άλλα είδη κακόβουλων προγραμμάτων. Οι πιο πρόσφατες

εκδόσεις προγραμμάτων antivirus, όπως το Norton AntiVirus, προστατεύουν κι αυτές από spyware και ενδεχομένως ανεπιθύμητα προγράμματα, όπως το adware. Το να έχετε λογισμικό ασφαλείας που σας προσφέρει έλεγχο στο λογισμικό που ίσως να μην θέλετε και που σας προστατεύει από online απειλές είναι ζωτικό για να παραμένετε ασφαλείς στο Internet. Το λογισμικό σας antivirus και antispyware πρέπει να διαμορφωθεί ώστε να ενημερώνεται αυτόματα και θα πρέπει να το κάνει αυτό κάθε φορά που συνδέεστε στο Internet.

Οι ολοκληρωμένες οικογένειες προγραμμάτων ασφαλείας, όπως το Norton Internet Security, συνδυάζουν δυνατότητες firewall, antivirus και antispyware με άλλες όπως antispam και γονικούς ελέγχους. Πολλά άτομα θεωρούν τη χρήση μιας οικογένειας προγραμμάτων ασφαλείας ελκυστική εναλλακτική λύση στην εγκατάσταση και διαμόρφωση πολλών διαφορετικών ειδών λογισμικού ασφαλείας, καθώς και στη διατήρηση όλων τους ενημερωμένων ξεχωριστά.

2. Βεβαιωθείτε ότι ο υπολογιστής σας είναι διαμορφωμένος με ασφάλεια.

Μην ξεχνάτε ότι ένας πρόσφατα αγορασμένος υπολογιστής μπορεί να μην έχει το κατάλληλο για σας επίπεδο ασφαλείας. Όταν εγκαθιστάτε τον υπολογιστή σας στο σπίτι, προσέξτε να μην κάνετε απλά το νέο σας σύστημα να λειτουργεί, αλλά και να το κάνετε να δουλεύει με ασφάλεια.

Η διαμόρφωση δημοφιλών εφαρμογών για το Internet, όπως το πρόγραμμα περιήγησης στο web και το λογισμικό email είναι ένα από τα πιο σημαντικά σημεία στα οποία πρέπει να επικεντρωθείτε. Για παράδειγμα, οι ρυθμίσεις στο πρόγραμμα περιήγησης καθορίζουν τι συμβαίνει όταν επισκέπτεστε ιστοσελίδες στο Internet. Οι ισχυρότερες ρυθμίσεις ασφαλείας σας προσφέρουν το μεγαλύτερο έλεγχο για το τι συμβαίνει online, αλλά μπορεί να σας ταλαιπωρούν με πάρα πολλές ερωτήσεις ("Αυτό ίσως να μην είναι ασφαλές, θέλετε οπωσδήποτε να το κάνετε;") ή να μην σας επιτρέπουν να κάνετε αυτό που θέλετε.

Η επιλογή του κατάλληλου ιδιωτικού επιπέδου ασφάλειας εξαρτάται από το άτομο που χρησιμοποιεί τον υπολογιστή. Πολλές φορές οι ιδιωτικές ρυθμίσεις ασφαλείας μπορούν να διαμορφωθούν σωστά χωρίς ειδική εμπειρία, χρησιμοποιώντας απλά την επιλογή "Βοήθεια" του λογισμικού σας ή διαβάζοντας την ιστοσελίδα του κατασκευαστή. Αν δεν αισθάνεστε άνετα να διαμορφώσετε μόνοι σας τον υπολογιστή σας, ζητήστε βοήθεια από κάποιον που γνωρίζετε και εμπιστεύεστε ή επικοινωνήστε απευθείας με τον προμηθευτή.

3. Επιλέγετε ισχυρούς κωδικούς πρόσβασης και διατηρείτε τους με ασφάλεια.

Σήμερα, οι κωδικοί πρόσβασης είναι μέρος της καθημερινής ζωής στο Internet. Τους χρησιμοποιούμε για τα πάντα, από την παραγγελία λουλουδιών και τις τραπεζικές εργασίες online μέχρι τη σύνδεση στην ιστοσελίδα της αεροπορικής μας εταιρείας για να δούμε πόσα μίλια έχουμε μαζέψει. Οι συμβουλές που ακολουθούν μπορεί να σας βοηθήσουν να κάνετε ασφαλείς τις online εμπειρίες σας:

- Επιλέξτε έναν κωδικό πρόσβασης που δεν μπορεί εύκολα να τον μαντέψει κάποιος, για να διατηρείτε τους κωδικούς πρόσβασής σας ασφαλείς και μακριά από τα λάθος χέρια. Οι ισχυροί κωδικοί πρόσβασης διαθέτουν τουλάχιστον οκτώ χαρακτήρες και χρησιμοποιούν συνδυασμό γραμμάτων, αριθμών και συμβόλων (π.χ. # $ % !) ?).
- Αποφύγετε τη χρήση οποιουδήποτε από τα παρακάτω ως κωδικού πρόσβασής σας: Το όνομα εισόδου σας, οτιδήποτε βασίζεται σε προσωπικά δεδομένα όπως το επώνυμό σας και λέξεις που μπορούν να βρεθούν στο λεξικό. Δοκιμάστε να επιλέγετε ιδιαίτερα ισχυρούς, μοναδικούς κωδικούς πρόσβασης για να προστατεύετε δραστηριότητες όπως online τραπεζικές συναλλαγές.
- Διατηρείτε τους κωδικούς πρόσβασής σας σε ασφαλές σημείο και προσπαθήστε να μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για κάθε υπηρεσία που χρησιμοποιείτε online.
- Αλλάζετε τους κωδικούς πρόσβασης σε τακτική βάση. Έτσι μπορείτε να περιορίσετε τη ζημιά που μπορεί να έχει προκαλέσει κάποιος που έχει ήδη αποκτήσει πρόσβαση στον λογαριασμό σας. Αν παρατηρήσετε κάτι ύποπτο με έναν από τους online λογαριασμούς σας, ένα από τα πρώτα βήματα που μπορείτε να κάνετε είναι να αλλάξετε τον κωδικό πρόσβασής σας.

4. Θωρακίστε τα προσωπικά σας δεδομένα.

Προσέχετε όταν μοιράζεστε προσωπικά δεδομένα όπως το όνομά σας, τη διεύθυνση του σπιτιού σας, τον αριθμό τηλεφώνου σας και την e-mail διεύθυνσή σας online. Για να εκμεταλλευτείτε πολλές υπηρεσίες online, θα χρειαστεί αναπόφευκτα να παρέχετε προσωπικά δεδομένα για τη διαχείριση της χρέωσης και αποστολής των αγαθών που θα αγοράζετε. Η μη αποκάλυψη προσωπικών δεδομένων είναι σπάνια δυνατή, για αυτό και η παρακάτω λίστα περιλαμβάνει κάποιες συμβουλές για τον τρόπο διαμοιρασμού προσωπικών δεδομένων online με ασφάλεια:

- Έχετε το νου σας για ψεύτικα μηνύματα e-mail. Τα μηνύματα μπορεί να είναι παραπλανητικά αν περιλαμβάνουν ορθογραφικά λάθη, λάθη γραμματικής, περίεργες διατυπώσεις, διευθύνσεις URL με παράξενες επεκτάσεις ή που αποτελούνται αποκλειστικά από αριθμούς και οτιδήποτε άλλο ασυνήθιστο. Επιπλέον, τα μηνύματα phishing σας λένε συχνά ότι πρέπει να δράσετε γρήγορα για να διατηρήσετε το λογαριασμό σας ανοικτό, να ενημερώσετε την ασφάλειά σας, ή σας προτρέπουν να παρέχετε πληροφορίες αμέσως, αλλιώς θα συμβεί κάτι κακό. Μην τσιμπάτε το δόλωμα.
- Μην απαντάτε σε μηνύματα e-mail που ζητούν προσωπικά δεδομένα. Οι νόμιμες εταιρείες δεν χρησιμοποιούν μηνύματα e-mail για να σας ζητήσουν τα προσωπικά σας δεδομένα. Αν έχετε αμφιβολίες, επικοινωνήστε με την εταιρεία μέσω τηλεφώνου ή πληκτρολογώντας τη διεύθυνση web της εταιρείας στο πρόγραμμα περιήγησής σας. Μην κάνετε κλικ σε συνδέσεις στα μηνύματα αυτά, γιατί μπορεί να σας μεταφέρουν σε παραπλανητικές, κακόβουλες ιστοσελίδες.
- Αποφύγετε τις παραπλανητικές ιστοσελίδες που χρησιμοποιούνται για να κλέβουν προσωπικά δεδομένα. Όταν επισκέπτεστε μια ιστοσελίδα, πληκτρολογήστε τη διεύθυνση URL απευθείας στο πρόγραμμα περιήγησης αντί να ακολουθείτε μια σύνδεση σε ένα e-mail ή άμεσο μήνυμα. Οι απατεώνες πλαστογραφούν συχνά αυτές τις συνδέσεις ώστε να τις κάνουν να μοιάζουν πειστικές. Η διεύθυνση μιας ιστοσελίδας αγορών, τραπεζικής ή

άλλου τύπου που απαιτεί τις ευαίσθητες πληροφορίες σας πρέπει να ξεκινά από "https:" (δηλ. https://www.yourbank.com και όχι http://www.yourbank.com)/. Το "s" σημαίνει secure (ασφαλές) και πρέπει να εμφανίζεται όταν βρίσκεστε στο σημείο που σας ζητά να πραγματοποιήσετε είσοδο ή να παρέχετε άλλα ευαίσθητα δεδομένα. Ένα άλλο σημάδι ότι έχετε ασφαλή σύνδεση είναι το μικρό εικονίδιο λουκέτου στο κάτω μέρος του προγράμματος περιήγησης (συνήθως στην κάτω δεξιά γωνία).

- Προσέξτε τις πολιτικές απορρήτου σε ιστοσελίδες και σε λογισμικό. Είναι σημαντικό να κατανοήσετε πώς ένας οργανισμός μπορεί να συλλέγει και να χρησιμοποιεί τα προσωπικά σας δεδομένα πριν του τα γνωστοποιήσετε.
- Διαφυλάξτε τη διεύθυνση του e-mail σας. Οι spammer και phisher στέλνουν μερικές φορές εκατομμύρια μηνύματα σε διευθύνσεις e-mail που μπορεί να υπάρχουν ή να μην υπάρχουν, ελπίζοντας να βρουν ένα πιθανό θύμα. Αν απαντήσετε στα μηνύματα αυτά, εξασφαλίζετε ότι θα μπείτε στις λίστες τους για περισσότερα παρόμοια μηνύματα στο μέλλον. Προσέχετε επίσης όταν αναρτάτε τη διεύθυνση του e-mail σας σε ομάδες συζήτησης, blog ή online κοινότητες.

5. Αν σας φαίνεται ότι μια online προσφορά φαίνεται πολύ καλή για να είναι αληθινή, μάλλον έτσι είναι.

Η ρήση "τίποτα σε αυτό τον κόσμο δεν είναι πλέον δωρεάν" ταιριάζει απόλυτα!!! Υποθετικά "δωρεάν" λογισμικό όπως προγράμματα προφύλαξης οθόνης ή εικονίδια συναισθημάτων (smileys), μυστικές επενδυτικές συμβουλές που θα σας εξασφαλίσουν τεράστια περιουσία και διαγωνισμοί στους οποίους κερδίσατε ξαφνικά χωρίς να έχετε ποτέ συμμετάσχει είναι τα δολώματα που χρησιμοποιούν εταιρείες για να τραβήξουν την προσοχή σας.

Αν και ίσως να μην πληρώνετε απευθείας για το λογισμικό ή την υπηρεσία με χρήματα, το δωρεάν λογισμικό ή η υπηρεσία που ζητήσατε μπορεί να συνδυάζεται με διαφημιστικό λογισμικό ("adware") που παρακολουθεί τη συμπεριφορά σας και εμφανίζει ανεπιθύμητες διαφημίσεις. Ίσως να χρειαστεί να αποκαλύψετε προσωπικά δεδομένα ή να αγοράσετε κάτι άλλο για να εξαργυρώσετε τα υποτιθέμενα κέρδη σας από τον διαγωνισμό. Αν μια προσφορά φαίνεται τόσο καλή που δυσκολεύεστε να την πιστέψετε, ζητήστε τη γνώμη κάποιου τρίτου, διαβάστε τα ψιλά γράμματα ή, ακόμα καλύτερα, απλά αγνοήστε την.

6. Ελέγχετε τακτικά τα αντίγραφα κινήσεων τραπεζικών λογαριασμών και πιστωτικών καρτών.

Οι επιπτώσεις της κλοπής ταυτότητας και των online εγκλημάτων μπορεί να μειωθούν σημαντικά αν μπορείτε να τα διαπιστώσετε ελάχιστα αφότου συμβούν ή όταν γίνει η πρώτη προσπάθεια χρήσης των στοιχείων σας. Ένας από τους πιο εύκολους τρόπους να αντιληφθείτε ότι κάτι πάει στραβά είναι να ελέγχετε τις μηνιαίες κινήσεις των τραπεζικών σας λογαριασμών και των πιστωτικών σας καρτών για οτιδήποτε ασυνήθιστο.

Επιπλέον, πολλές τράπεζες και υπηρεσίες χρησιμοποιούν συστήματα πρόληψης απάτης που ξεχωρίζουν την ασυνήθιστη αγοραστική συμπεριφορά (π.χ. ζείτε στη Θεσσαλονίκη και ξαφνικά αρχίζετε να αγοράζετε ψυγεία στη Νέα Υόρκη). Για να

επιβεβαιώσουν αυτές τις ασυνήθιστες συναλλαγές, μπορεί να σας καλέσουν και να σας ζητήσουν να τις επιβεβαιώσετε. Μην παραμελείτε αυτά τα τηλεφωνήματα, είναι ένδειξη ότι μπορεί να συνέβη κάτι κακό και ότι πρέπει να ενεργήσετε.

7. **Αποφύγετε «πειράματα» με προγράμματα και παιχνίδια αμφίβολης προέλευσης.**

Μην πειραματίζεστε με προγράμματα και παιχνίδια αμφίβολης προέλευσης καθώς μπορεί να βλάψουν τον υπολογιστή σας και να υποκλέψουν προσωπικά στοιχεία και κωδικούς. Όταν δεν είστε σίγουροι για κάποιο πρόγραμμα ή δεν είστε σίγουροι ότι ξέρετε τι κάνετε, αποφύγετε τις δοκιμές.

Οι απλές αυτές συμβουλές μπορούν να σας προφυλάξουν από ένα σύνολο απειλών και ως ένα βαθμό. Σε περίπτωση που αντιληφτείτε κάποια απειλή στον υπολογιστή σας, από την εμπειρία μας, θεωρούμε ως ασφαλέστερη λύση τον έλεγχο του υπολογιστή με εξειδικευμένα εργαλεία στα εργαστήρια της εταιρείας μας.

Έλα στους ειδικούς.

Με εκτίμηση,