



A. EVANS, K. MARTIN, M. A. POATSY

Εισαγωγή στην
πληροφορική
Θεωρία και πράξη
3η έκδοση

Κεφάλαιο 9

Διασφάλιση του συστήματός σας:
Προστατεύστε τα ψηφιακά
δεδομένα και τις συσκευές σας

Στόχοι (1 από 3)

- 9.1 Διάπραξη κλοπής ταυτότητας και είδη εξαπάτησης με στόχο την ταυτότητα.
- 9.2 Οι διαφορετικοί τύποι χάκερ και τα εργαλεία που χρησιμοποιούν.
- 9.3 Τι είναι ο ιός υπολογιστή, γιατί απειλεί την ασφάλειά σας, πώς «κολλάει» μια ψηφιακή συσκευή τον ιό και τα συμπτώματα που μπορεί να εμφανίσει.
- 9.4 Οι διαφορετικές κατηγορίες ιών υπολογιστών και οι συμπεριφορές τους.
- 9.5 Τι είναι το κακόβουλο λογισμικό, το spam και τα cookie και πώς επηρεάζουν την ασφάλειά σας.

Στόχοι (2 από 3)

- 9.6 Τεχνικές κοινωνικής μηχανικής και στρατηγικές αποφυγής τους.
- 9.7 Τι είναι το τείχος προστασίας και πώς προστατεύει τον υπολογιστή σας από χάκερ.
- 9.8 Προστασία υπολογιστή από μόλυνση από ιό.
- 9.9 Χρήση κωδικών πρόσβασης και βιομετρικών χαρακτηριστικών για ταυτοποίηση χρήστη.
- 9.10 Τρόποι ανώνυμης περιήγησης στο Web.

Στόχοι (3 από 3)

- 9.11 Τύποι πληροφοριών που δεν πρέπει να κοινοποιείτε ποτέ στο διαδίκτυο.
- 9.12 Διάφοροι τύποι αντιγράφων ασφαλείας στις ψηφιακές συσκευές σας και τα διάφορα μέρη όπου μπορείτε να αποθηκεύετε αντίγραφα ασφαλείας.
- 9.13 Αρνητικές επιπτώσεις που μπορεί να έχει το περιβάλλον και οι αυξομειώσεις της τάσης του ρεύματος σε ψηφιακές συσκευές.
- 9.14 Οι κυριότερες ανησυχίες που προκύπτουν από την κλοπή μιας συσκευής και στρατηγικές επίλυσης των προβλημάτων.

Κλοπή ταυτότητας και χάκερ

Χάκερ (1 από 4)

(Στόχος 9.2)

- Χάκερ: οποιοσδήποτε εισβάλλει παράνομα σε ένα σύστημα υπολογιστή
- Τύποι χάκερ
 - Χάκερ με τα λευκά καπέλα (ηθικοί χάκερ)
 - Χάκερ με τα μαύρα καπέλα
 - Χάκερ με γκρι καπέλα
- Πρόγραμμα ανάλυσης πακέτων (sniffer)
- Keylogger



Κλοπή ταυτότητας και χάκερ

Χάκερ (2 από 4)

(Στόχος 9.2)

- Δούρειος ίππος: φαίνεται να είναι ένα χρήσιμο πρόγραμμα, αλλά όταν εκτελεστεί, λειτουργεί κακόβουλα χωρίς να το γνωρίζετε
- Οι κερκόπορτες και τα rootkit είναι προγράμματα τα οποία δίνουν στους χάκερ τον έλεγχο ενός υπολογιστή

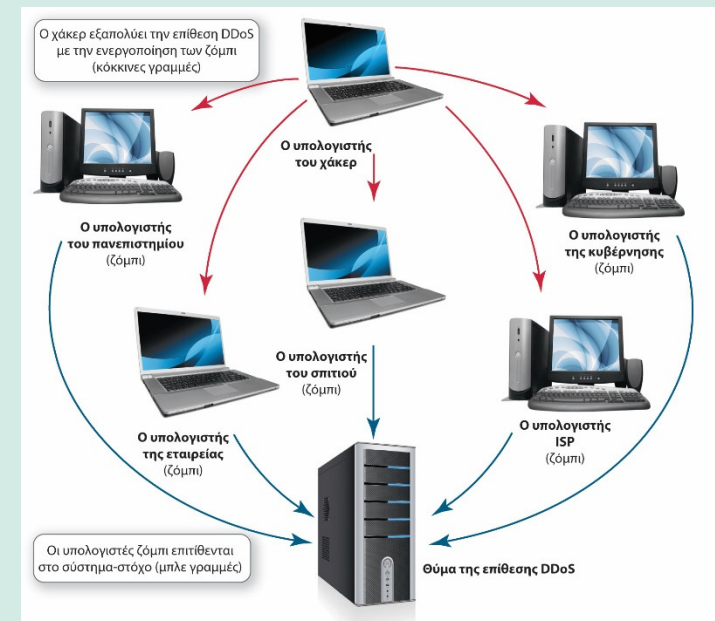


Κλοπή ταυτότητας και χάκερ

Χάκερ (3 από 4)

(Στόχος 9.2)

- Υπολογιστές ζόμπι: υπολογιστές που ελέγχονται από χάκερ
- Επίθεση άρνησης εξυπηρέτησης
 - Οι νόμιμοι χρήστες αποκλείονται από την πρόσβαση σε ένα σύστημα υπολογιστή
 - Ο υπολογιστής τερματίζει τη λειτουργία του
- DDoS
- Botnet: μια μεγάλη ομάδα προγραμμάτων λογισμικού που εκτελούνται αυτόνομα σε υπολογιστές ζόμπι

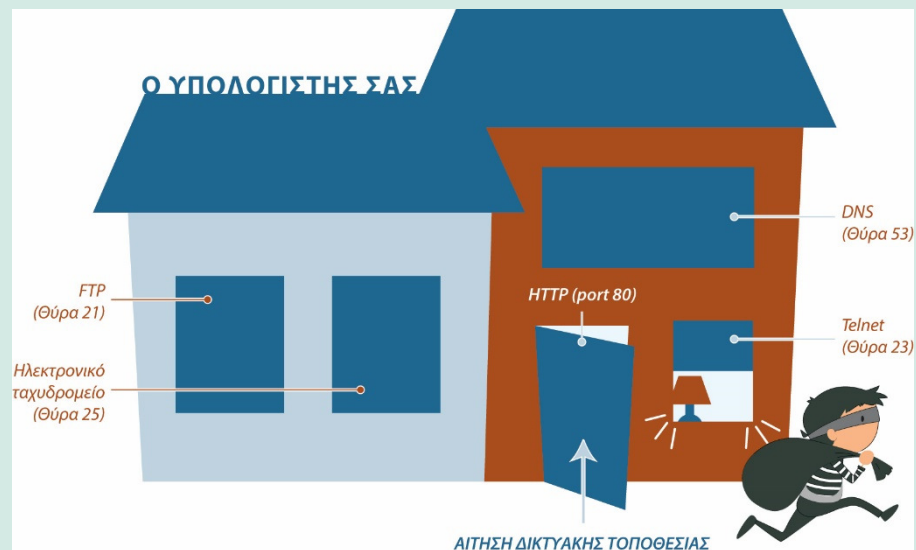


Κλοπή ταυτότητας και χάκερ

Χάκερ (4 από 4)

(Στόχος 9.2)

- Πακέτα εκμετάλλευσης: προγράμματα λογισμικού τα οποία εκτελούνται σε διακομιστές και αναζητούν ευπαθή σημεία
- Οι λογικές θύρες είναι εικονικές, όχι φυσικές, πύλες επικοινωνίας



Ιοί υπολογιστών

Τα βασικά για τους ιούς (1 από 2)

(Στόχος 9.3)

- Ιός: πρόγραμμα υπολογιστή που προσκολλάται σε κάποιο άλλο προσπαθώντας να εξαπλωθεί σε άλλους υπολογιστές
 - Κύριος σκοπός: να αντιγράψει τον εαυτό του και τον κώδικά του σε όσο το δυνατόν περισσότερα αρχεία φιλοξενίας
 - Δευτερεύοντες στόχοι: μπορεί να είναι καταστροφικοί
 - Τα smartphone, τα tablet και άλλες συσκευές μπορούν να μολυνθούν

Ιοί υπολογιστών

Τα βασικά για τους ιούς (2 από 2)

(Στόχος 9.3)



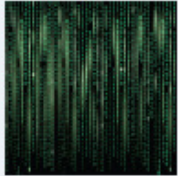



Ιοί υπολογιστών

Τύποι ιών (1 από 2)

(Στόχος 9.4)

- Ιοί τομέα εκκίνησης
- Βόμβες λογικής και ωρολογιακές βόμβες
- Ιοί δέσμης ενεργειών και μακροεντολών
- Ιοί ηλεκτρονικού ταχυδρομείου
- Ιοί κρυπτογράφησης

Κύριες κατηγορίες ιών		
<p>Ιοί τομέα εκκίνησης</p>  <p>Εκτελούνται κατά την έναρξη του υπολογιστή</p>	<p>Βόμβες λογικής/ωρολογιακές βόμβες</p>  <p>Εκτελούνται κάτω από συγκεκριμένες συνθήκες ή σε συγκεκριμένες ημερομηνίες</p>	<p>Σκουλήκια</p>  <p>Εξαπλώνονται μόνο τους χωρίς να χρειάζεται ανθρώπινη αλληλεπίδραση</p>
<p>Ιοί δεσμών ενεργειών και μακροεντολών</p>  <p>Σειρές από κακόβουλες εντολές</p>	<p>Ιοί ηλεκτρονικού ταχυδρομείου</p>  <p>Εξαπλώνονται με την επισύναψη στο ηλεκτρονικό ταχυδρομείο, συνήθως χρησιμοποιώντας το βιβλίο διευθύνσεων</p>	<p>Ιοί κρυπτογράφησης</p>  <p>Κρατούν «αιχμάλωτα» τα αρχεία, κρυπτογραφώντας τα. Ζητούν λύτρα για να τα ξεκλειδώσουν</p>

(Gillskaja Olga/Shutterstock, Oleksandr_Delyk/Shutterstock, David Martyn Hughes/123RF, Neyro2008/123RF, Bannosuke/Shutterstock, Lukas Gojda/Shutterstock)

Ιοί υπολογιστών

Τύποι ιών (2 από 2)

(Στόχος 9.4)

- Ταξινόμηση με βάση τις μεθόδους που χρησιμοποιούν έτσι ώστε να αποφύγουν τον εντοπισμό τους
 - Πολυμορφικός: τροποποιεί τον κώδικά του ή τον ξαναγράφει σε τακτά διαστήματα, έτσι ώστε να αποφύγει τον εντοπισμό
 - Πολυμερής: έχει σχεδιαστεί έτσι ώστε να μολύνει πολλούς τύπους αρχείων
 - Αόρατος: διαγράφει προσωρινά τον κώδικά του από τα αρχεία στα οποία εδρεύει και στη συνέχεια κρύβεται στην ενεργή μνήμη του υπολογιστή

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Διαδικτυακές οχλήσεις (1 από 3)

(Στόχος 9.5)

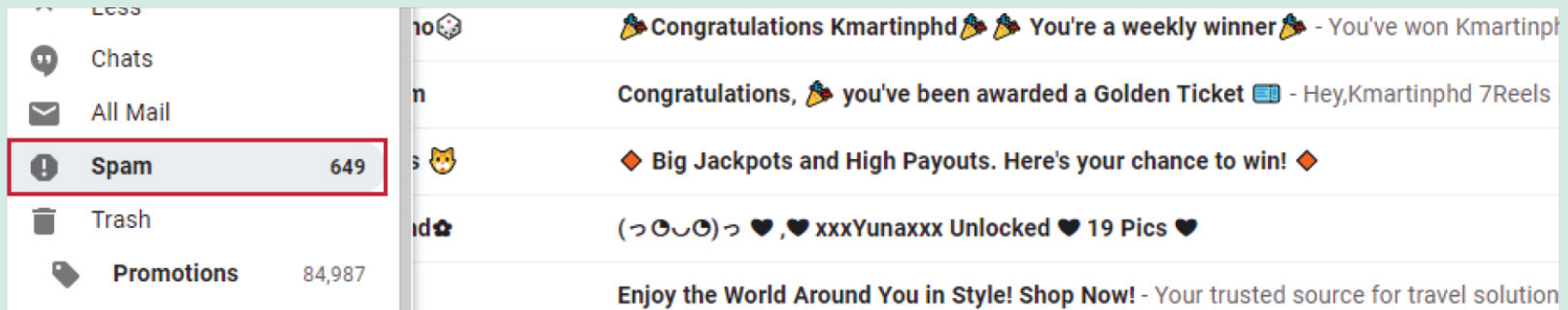
- Κακόβουλο λογισμικό: πρόγραμμα με κακές προθέσεις
 - Adware: λογισμικό που προβάλλει χορηγούμενες διαφημίσεις
 - Spyware: ανεπιθύμητο πρόγραμμα που λαμβάνει και άλλα προγράμματα μαζί με όσα λαμβάνετε
 - Μεταδίδει πληροφορίες
 - Χρησιμοποιεί cookie παρακολούθησης
 - Παρακολουθεί όσα πληκτρολογεί ο χρήστης

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Διαδικτυακές οχλήσεις (2 από 3)

(Στόχος 9.5)

- Spam: ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου
- Τακτικές αποφυγής των spam (φίλτρο spam)



Διαδικτυακές οχλήσεις και κοινωνική μηχανική - Διαδικτυακές οχλήσεις (1 από 3)

(Στόχος 9.5)

- Cookie: μικρά αρχεία κειμένου τα οποία αποθηκεύουν αυτόματα στον σκληρό σας δίσκο ορισμένους διαδικτυακούς τόπους όταν τους επισκέπτεστε
 - Βοηθούν τις εταιρείες να καθορίσουν την αποτελεσματικότητα της στρατηγικής μάρκετινγκ που υιοθετούν
 - Δεν αναζητούν προσωπικές πληροφορίες στον σκληρό σας δίσκο
 - Ίσως σας κάνουν να αισθάνεστε ότι η προστασία του απορρήτου σας παραβιάζεται
 - Δεν αποτελούν απειλή για την ασφάλεια

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Κοινωνική μηχανική (1 από 3)

(Στόχος 9.6)

- Κοινωνική μηχανική: οποιαδήποτε τεχνική χρησιμοποιεί κοινωνικές δεξιότητες προκειμένου να δημιουργήσει μια ανθρώπινη αλληλεπίδραση
 - Παρακινεί τα εμπλεκόμενα άτομα να αποκαλύψουν ευαίσθητες πληροφορίες
- Pretexting: δημιουργία ενός σεναρίου το οποίο ακούγεται απολύτως νομότυπο

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Διαδικτυακές οχλήσεις (2 από 3)

(Στόχος 9.5)

- Phishing: δελεάζει τους χρήστες του διαδικτύου ώστε να αποκαλύπτουν προσωπικές πληροφορίες
- Pharming: κακόβουλος κώδικας εισβάλλει στον υπολογιστή σας για να συλλέξει πληροφορίες
- Οδηγίες για να μην πέσετε θύματα τέτοιων επιθέσεων

Διαδικτυακές οχλήσεις και κοινωνική μηχανική

Διαδικτυακές οχλήσεις (3 από 3)

(Στόχος 9.5)

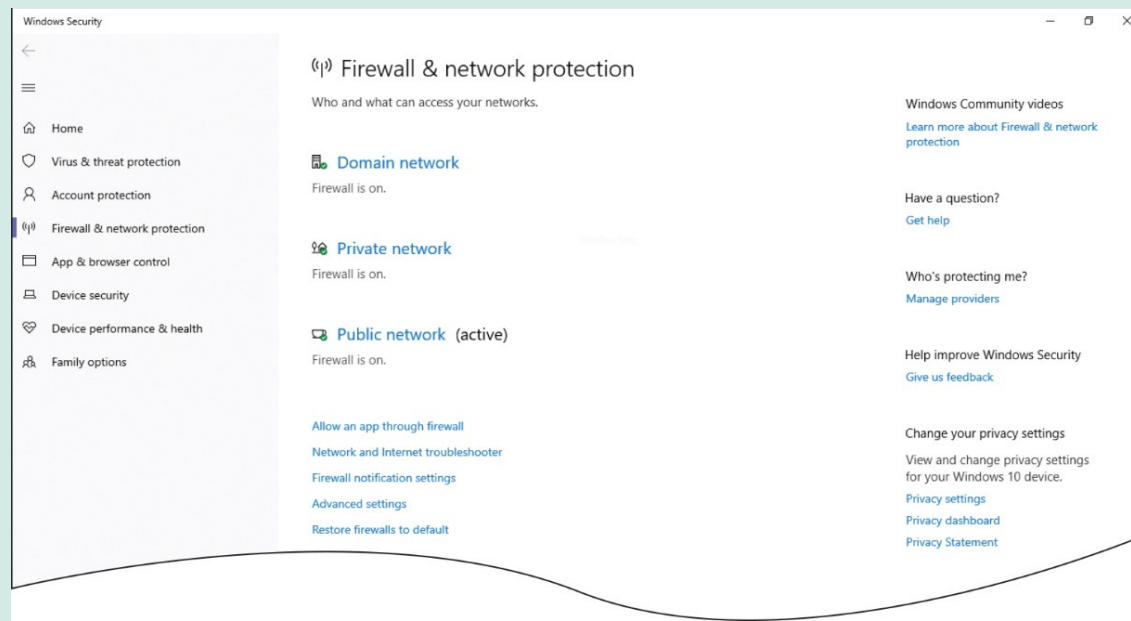
- Ransomware: κακόβουλο λογισμικό που επιτίθεται στο σύστημά σας κρυπτογραφώντας κρίσιμα αρχεία, ώστε το σύστημά σας να μην είναι πλέον λειτουργικό operational
- Scareware: κακόβουλο λογισμικό που προσπαθεί να σας πείσει πως κάτι δεν πάει καλά... και να πληρώσετε για να το διορθώσετε

Περιορισμός της πρόσβασης σε ψηφιακούς πόρους

Τείχη προστασίας (1 από 3)

(Στόχος 9.7)

- Τείχος προστασίας: πρόγραμμα λογισμικού ή μια συσκευή υλικού που έχουν σχεδιαστεί έτσι ώστε να προστατεύουν τους υπολογιστές από τους χάκερ

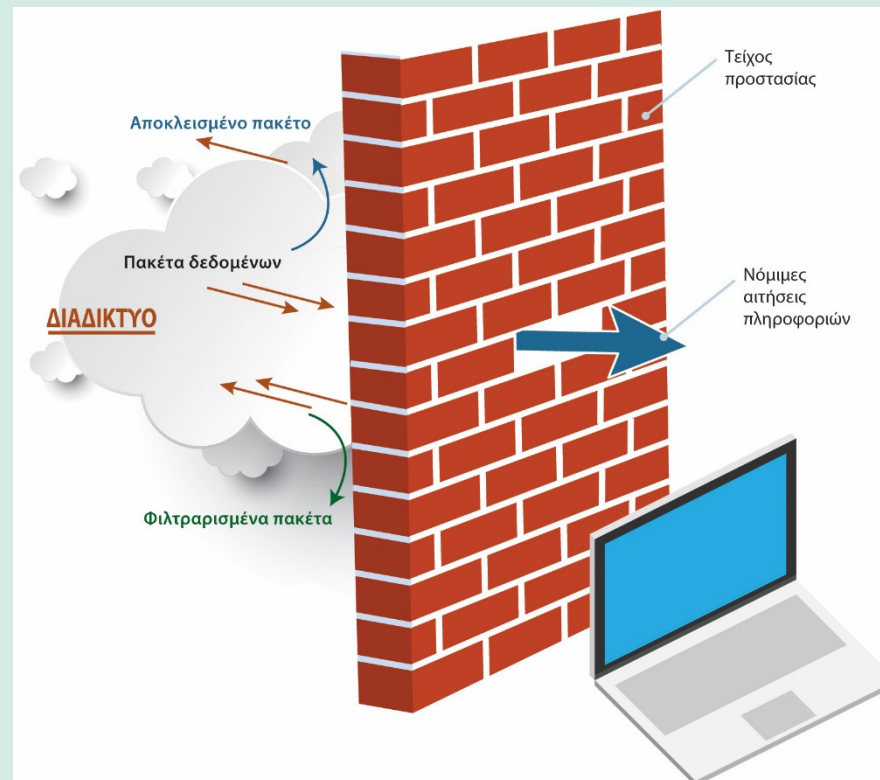


Περιορισμός της πρόσβασης σε ψηφιακούς πόρους

Τείχη προστασίας (2 από 3)

(Στόχος 9.7)

- Τα Windows και το macOS περιλαμβάνουν τείχη προστασίας



Περιορισμός της πρόσβασης σε ψηφιακούς πόρους

Τείχη προστασίας (3 από 3)

(Στόχος 9.7)

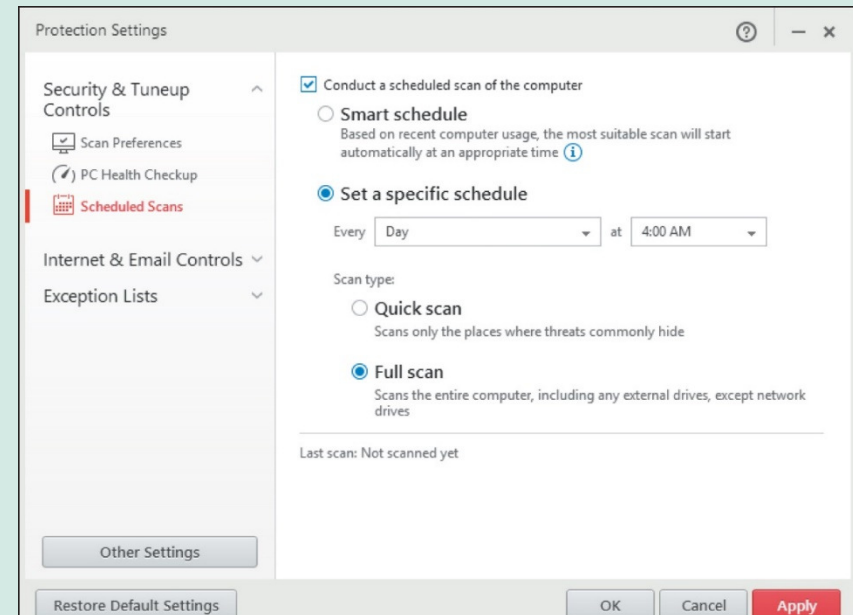
- Φιλτράρισμα πακέτων
 - Φιλτράρουν τα πακέτα που αποστέλλονται σε λογικές θύρες
- Αποκλεισμός λογικής θύρας
 - Αγνοούν τελείως το αίτημα που προέρχεται από το διαδίκτυο και ζητά πρόσβαση σε ορισμένες θύρες
- Μετάφραση διεύθυνσης δικτύου
 - Εκχωρούν διευθύνσεις IP σε ένα δίκτυο

Περιορισμός της πρόσβασης σε ψηφιακούς πόρους

Αποτροπή μολύνσεων από ιούς (1 από 3)

(Στόχος 9.8)

- Λογισμικό προστασίας από ιούς
 - Ανίχνευση ιών και προστασία του υπολογιστή
- Δημοφιλή προγράμματα
 - Norton
 - Trend Micro



Περιορισμός της πρόσβασης σε ψηφιακούς πόρους

Αποτροπή μολύνσεων από ιούς (2 από 3)

(Στόχος 9.8)

- Υπογραφή ιού

- Τμήμα του κώδικα του ιού που τον χαρακτηρίζει μοναδικά

- Καραντίνα

- Απομονώνει τον ιό σε έναν ασφαλή χώρο, έτσι ώστε να μην εξαπλωθεί σε άλλα αρχεία

- Εμβολιασμός

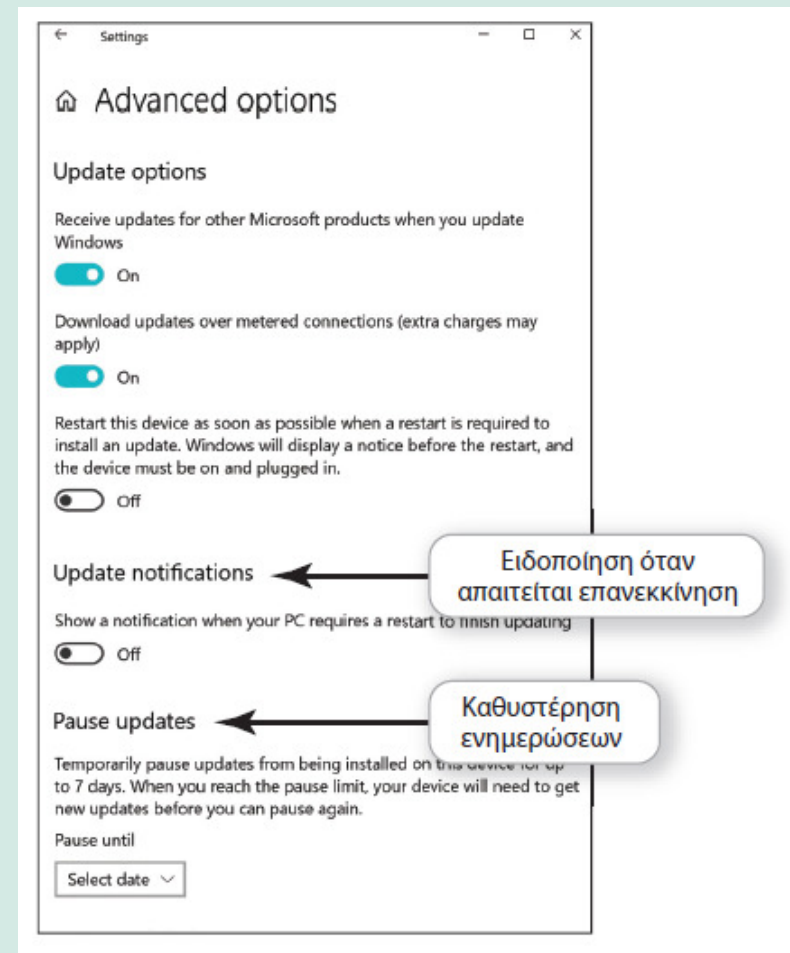
- Καταγράφονται τα βασικά χαρακτηριστικά των αρχείων του υπολογιστή σας και διατηρούνται σε ασφαλές μέρος

Περιορισμός της πρόσβασης σε ψηφιακούς πόρους

Αποτροπή μολύνσεων από ιούς (3 από 3)

(Στόχος 9.8)

- Drive-by download
 - Εκμεταλλεύεται αδυναμίες των λειτουργικών συστημάτων
 - Καταπολεμείται όταν το ΛΣ σας είναι ενημερωμένο και περιέχει τις τελευταίες διορθώσεις ασφαλείας



Περιορισμός της πρόσβασης σε ψηφιακούς πόρους - Ταυτοποίηση: Κωδικοί πρόσβασης και βιομετρικά στοιχεία

(1 από 2)

(Στόχος 9.9)

- Ισχυροί κωδικοί πρόσβασης: τουλάχιστον οκτώ χαρακτήρες και να περιέχουν:
 - Κεφαλαίους χαρακτήρες
 - Πεζούς χαρακτήρες
 - Αριθμούς
 - Σύμβολα

Περιορισμός της πρόσβασης σε ψηφιακούς πόρους - Ταυτοποίηση: Κωδικοί πρόσβασης και βιομετρικά στοιχεία

(1 από 2)

(Στόχος 9.9)

- Συσκευές βιομετρικής ταυτοποίησης
 - Δακτυλικό αποτύπωμα
 - Σάρωση ίριδας ματιών
 - Αναγνώριση φωνής
 - Αναγνώριση προσώπου
 - Παρέχουν υψηλό επίπεδο ασφάλειας



Περιορισμός της πρόσβασης σε ψηφιακούς πόρους - Ταυτοποίηση: Κωδικοί πρόσβασης και βιομετρικά στοιχεία

(1 από 2)

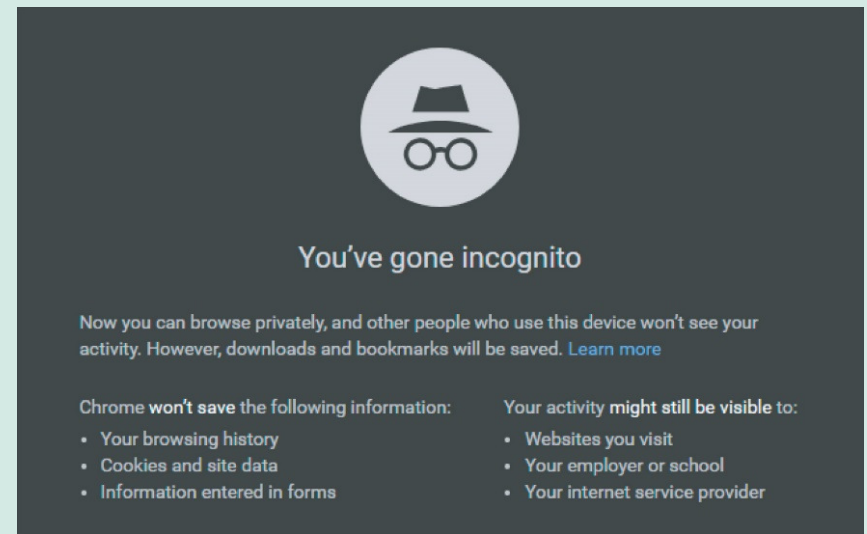
(Στόχος 9.9)

- Εργαλεία απορρήτου

- Private Browsing
- InPrivate
- Incognito

- Εικονικά ιδιωτικά δίκτυα (VPN)

- Ασφαλή δίκτυα που δημιουργούνται αξιοποιώντας τη δημόσια υποδομή του διαδικτύου



Περιορισμός της πρόσβασης σε ψηφιακούς πόρους - Ανώνυμη περιήγηση στο web: Κρυφτείτε από τα περίεργα βλέμματα (Στόχος 9.10)



Κάτι που ΓΝΩΡΙΖΕΤΕ:

Κάτι που γνωρίζει ο χρήστης
(κωδικός πρόσβασης, PIN)



Κάτι που ΕΧΕΤΕ:

Κάτι που έχει ο χρήστης
(κάρτα ATM, κινητό τηλέφωνο,
κλειδί YUBI)



Κάτι που ΕΙΣΤΕ:

Κάτι που μόνο ο χρήστης διαθέτει
(δακτυλικά αποτυπώματα,
μοτίβο ίριδας)



Ισχυρή ταυτοποίηση:



Δύο από τους παραπάνω τρεις
παράγοντες

Διατηρήστε τα δεδομένα σας ασφαλή

Προστασία προσωπικών πληροφοριών

(Στόχος 9.11)

- Να αποκαλύπτετε όσο το δυνατόν λιγότερα στοιχεία
- αλλάξει τις
- Αλλάξτε τις προεπιλεγμένες ρυθμίσεις απορρήτου σας στο Facebook

Πληροφορίες τις οποίες αναζητούν οι κλέφτες ταυτοτήτων	
	<ul style="list-style-type: none">• Αριθμός κοινωνικής ασφάλισης• Πλήρης ημερομηνία γέννησης• Αριθμός τηλεφώνου• Διεύθυνση <p>Ποτέ μην κοινοποιείτε αυτές τις πληροφορίες σε διαδικτυακές τοποθεσίες!</p>
Άλλες ευαίσθητες πληροφορίες	
	<ul style="list-style-type: none">• Πλήρες όνομα• Διεύθυνση ηλεκτρονικού ταχυδρομείου• Ταχυδρομικός κώδικας• Φύλο• Σχολείο ή τόπος εργασίας <p>Αποκαλύπτετε αυτές τις πληροφορίες μόνο σε ανθρώπους που γνωρίζετε – μην τις κοινοποιείτε σε οποιονδήποτε!</p>

Διατηρήστε τα δεδομένα σας ασφαλή

Αντίγραφα ασφαλείας δεδομένων (1 από 2)

(Στόχος 9.12)

- Αντίγραφα ασφαλείας—αντίγραφα των αρχείων τα οποία μπορείτε να χρησιμοποιήσετε ώστε να αντικαταστήσετε τα πρωτότυπα, αν χαθούν ή καταστραφούν
- Τύποι αρχείων που χρειάζονται αντίγραφα ασφαλείας
 - Αρχεία δεδομένων
 - Αρχεία προγραμμάτων
- Μέθοδοι δημιουργίας αντιγράφων ασφαλείας
 - Πλήρες αντίγραφο ασφαλείας
 - Αυξητικό αντίγραφο ασφαλείας
 - Αντίγραφο ασφαλείας ειδώλου

Διατηρήστε τα δεδομένα σας ασφαλή

Αντίγραφα ασφαλείας δεδομένων (2 από 2)

(Στόχος 9.12)

- Τοποθεσίες αποθήκευσης των αντιγράφων ασφαλείας

Μια σύγκριση κοινών τοποθεσιών για τη δημιουργία αντιγράφων ασφαλείας δεδομένων

Τοποθεσία αντιγράφων ασφαλείας	Υπέρ	Κατά
Στο διαδίκτυο (στο cloud) 	<ul style="list-style-type: none">• Τα αρχεία φυλάσσονται σε μια ασφαλή, απομακρυσμένη τοποθεσία• Τα αρχεία και τα αντίγραφα ασφαλείας είναι προσβάσιμα από παντού, μέσω του προγράμματος περιήγησης	<ul style="list-style-type: none">• Τα περισσότερα δωρεάν πακέτα δεν προσφέρουν αρκετή χωρητικότητα για τα αντίγραφα ασφαλείας ειδώλων συστήματος
Εξωτερική μονάδα σκληρού δίσκου 	<ul style="list-style-type: none">• Οικονομική λύση με κόστος που καταβάλλεται μόνο μία φορά• Γρήγορα αντίγραφα ασφαλείας με μια συσκευή USB 3.0, που συνδέεται απευθείας στον υπολογιστή σας	<ul style="list-style-type: none">• Υπάρχουν πιθανότητες η μονάδα να καταστραφεί από κάποιο συμβάν (φωτιά/πλημμύρα) μαζί με τον υπολογιστή σας• Πιθανότητες κλοπής• Ελαφρώς πιο δύσκολη η δημιουργία αντιγράφων από πολλαπλούς υπολογιστές μόνο με μια συσκευή
Δικτυακές συσκευές αποθήκευσης (NAS) ή οικιακοί διακομιστές 	<ul style="list-style-type: none">• Διευκολύνει τη δημιουργία αντιγράφων ασφαλείας για πολλαπλές συσκευές	<ul style="list-style-type: none">• Πιο ακριβή λύση από μια ανεξάρτητη εξωτερική μονάδα σκληρού δίσκου• Υπάρχουν πιθανότητες η μονάδα να καταστραφεί από κάποιο συμβάν (φωτιά/πλημμύρα) μαζί με τον υπολογιστή σας• Πιθανότητες κλοπής

(Mipan/Shutterstock, Gleb Semenov/123RF, Prapass/Shutterstock)

Προστασία φυσικών ψηφιακών συσκευών Περιβαλλοντικοί παράγοντες και αυξομειώσεις τάσης ρεύματος (1 από 2)

(Στόχος 9.13)

- Αυξομειώσεις της τάσης του ρεύματος
 - Παλιά ή ελαττωματική καλωδίωση
 - Κεραυνοί
 - Δυσλειτουργίες σε ηλεκτρικούς υποσταθμούς

Προστασία φυσικών ψηφιακών συσκευών

Περιβαλλοντικοί παράγοντες και αυξομειώσεις τάσης ρεύματος (2 από 2)

(Στόχος 9.13)

- Πολύπριζο ασφαλείας/Ολοκληρωμένο σύστημα προστασίας από αυξομείωση τάσης για όλο το σπίτι
 - Αντικατάσταση κάθε δύο με τρία χρόνια
- UPS
 - Εφεδρική μπαταρία αν διακοπεί το ρεύμα



Προστασία φυσικών ψηφιακών συσκευών

Παρεμπόδιση και αντιμετώπιση κλοπής

(1 από 2)

(Στόχος 9.14)

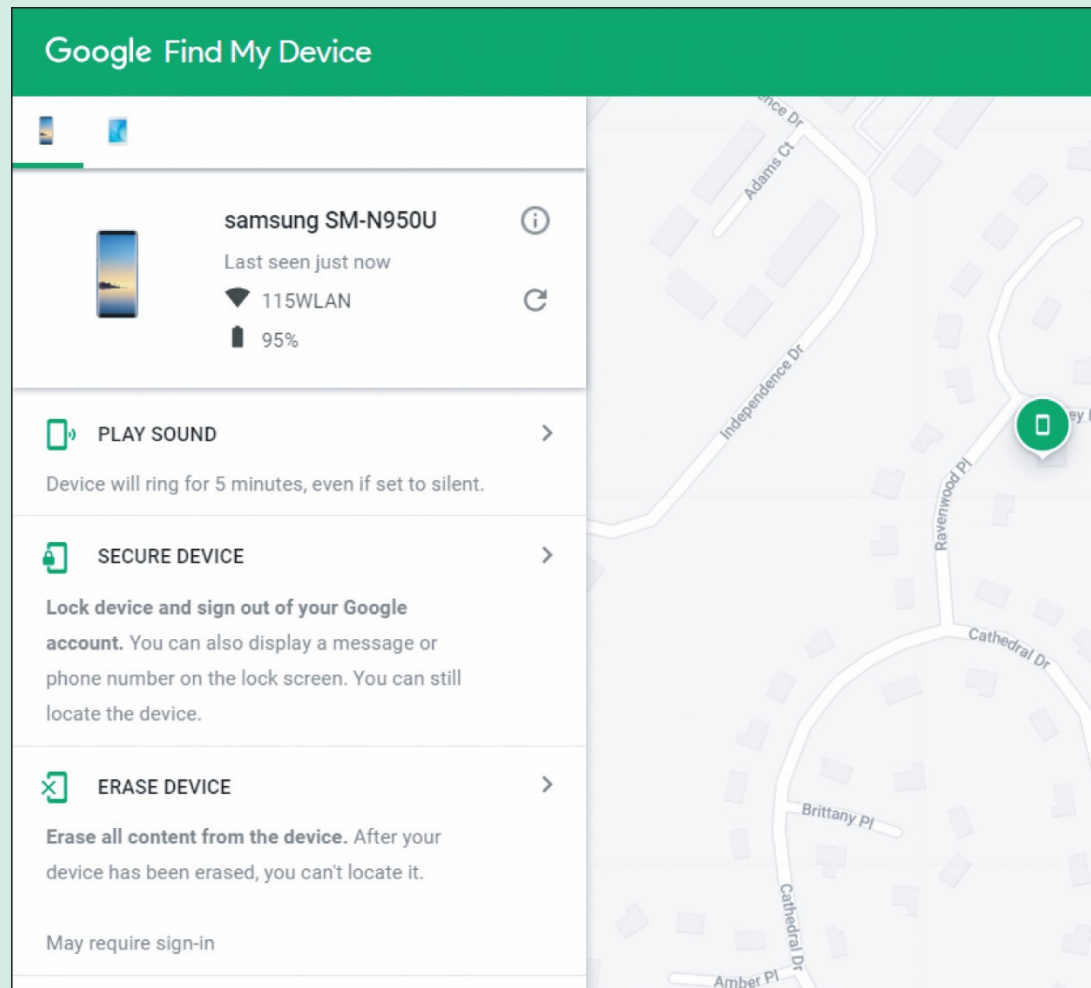
- Τρία πράγματα που θα πρέπει να έχετε υπόψη σας σχετικά με την ασφάλεια των φορητών σας συσκευών:
 - Να τις προστατεύετε από κλοπή
 - Να διατηρείτε τα δεδομένα σας ασφαλή σε περίπτωση κλοπής
 - Να βρείτε τη συσκευή αν έχει κλαπεί

Προστασία φυσικών ψηφιακών συσκευών

Παρεμπόδιση και αντιμετώπιση κλοπής

(2 από 2)

(Στόχος 9.14)



Απαγορεύεται η αναδημοσίευση ή αναπαραγωγή του παρόντος έργου με οποιονδήποτε τρόπο χωρίς γραπτή άδεια του εκδότη, σύμφωνα με το Ν. 2121/1993 και τη Διεθνή Σύμβαση της Βέρνης (που έχει κυρωθεί με τον Ν. 100/1975)