

ΤΟ ΔΙΑΔΙΚΤΥΟ.

ΕΙΝΑΙ ΠΡΩΤΟ, ΓΡΗΓΟΡΟ ΚΑΙ ΠΑΓΚΟΣΜΙΟ.

Αλλά είναι επίσης και περίπλοκο. Μερικές φορές μπορεί να είναι δύσκολο να δούμε ότι βρισκόμαστε σε κίνδυνο και ότι τα ιδιωτικά μας δεδομένα σε απευθείας σύνδεση (online) μπορούν να διαβαστούν και να χρησιμοποιηθούν από άλλους. Ευτυχώς, στο παράλληλο σύμπαν μας, όπου οι ΨΗΦΙΑΚΟΙ ΥΠΕΡΑΣΠΙΣΤΕΣ πολεμούν τους κακούς ΕΙΣΒΟΛΕΙΣ ΔΕΔΟΜΕΝΩΝ, είναι εύκολο να δούμε ποιοι είναι με το μέρος μας και ποιοι εναντίον μας:

www.edri.org



Ο ΟΔΗΓΟΣ ΣΟΥ ΣΤΟ

DIGITAL DEFENDERS

ΨΗΦΙΑΚΟΙ
ΥΠΕΡΑΣΠΙΣΤΕΣ

ENANTION

ΕΙΣΒΟΛΕΙΣ
ΔΕΔΟΜΕΝΩΝ

DATA INTRUDERS

ΠΑΡΕ ΤΟΝ
ΕΛΕΓΧΟ
ΤΩΝ
ΠΡΑΓΜΑΤΩΝ
ΣΟΥ
ONLINE!

Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΓΙΑ ΝΕΟΥΣ!

Το διαδίκτυο. Είναι πρώτο, γρήγορο και παγκόσμιο!

Αλλά είναι επίσης και πολύπλοκο, μερικές φορές. Μερικές φορές μπορεί να είναι δύσκολο να δει κανείς τους κινδύνους, όταν τα ιδιωτικά μας δεδομένα σε απευθείας σύνδεση μπορούν να διαβαστούν και να χρησιμοποιηθούν από άλλους.

Ευτυχώς, στο παράλληλο σύμπαν μας, εκεί που οι ΨΗΦΙΑΚΟΙ ΥΠΕΡΑΣΠΙΣΤΕΣ πολεμούν τους κακούς ΕΙΣΒΟΛΕΙΣ ΔΕΔΟΜΕΝΩΝ, είναι εύκολο να δούμε το ποιοι είναι οι καλοί και ποιοι οι κακοί.

Οι ΥΠΕΡΑΣΠΙΣΤΕΣ θα σου δείξουν μερικές συμβουλές και κόλπα για να προστατεύσεις τον εαυτό σου σε απευθείας σύνδεση. Θα σε διδάξουν αυτοάμυνα για να πολεμήσεις τους ΕΙΣΒΟΛΕΙΣ.

» Δες αυτό το φυλλάδιο και ετοιμάσου να γίνεις μέλος της ομάδας των υπερηρώων μας, τους ΨΗΦΙΑΚΟΥΣ

Ο φίλος σου,
EDRi-former



» Α, ΚΑΙ ΕΧΕ ΤΑ ΜΑΤΙΑ ΣΟΥ ΑΝΟΙΧΤΑ ΓΙΑ ΤΟ ΠΑΙΧΝΙΔΙ ΤΟΥ EDRi-former

Θα βρεις γρίφους σε όλο το φυλλάδιο. Κάθε γρίφος έχει μόνο μία σωστή απάντηση που θα σου δώσει ένα γράμμα. Μαζί, τα γράμματα θα αποτελέσουν τη λέξη λύση. Συμβουλή: είναι μια λέξη που αποτελείται από έξι γράμματα. Το επίτευγμα είναι για να ξεκλειδώσεις: ΜΙΑ ΙΣΧΥΡΗ ΨΗΦΙΑΚΗ ΠΑΝΟΠΛΙΑ. Μόλις βρεις τη λέξη, θα πρέπει να πας σε μια μυστική σελίδα στο διαδίκτυο. Εδώ είναι το πώς:

1. Βρες το μέρος που λείπει από τον σύνδεσμο: <https://edri.org/xxxxxx>
2. Αντικατέστησε το **xxxxxx** με τη λέξη λύση (έξι γράμματα) από τους γρίφους του παιχνιδιού και βάλε τον πλήρη σύνδεσμο στο πρόγραμμα περιήγησής σου.

- 1 ΤΙ ΕΙΝΑΙ ΤΟ ΔΙΑΔΙΚΤΥΟ;
- 2 ΤΙ ΕΙΝΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ;
- 3 ΠΡΟΣΤΑΤΕΨΕ ΤΟΝ ΕΑΥΤΟ ΣΟΥ ΣΤΑ ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ
- 4 ΤΡΕΙΣ ΚΟΡΥΦΑΙΕΣ ΣΥΜΒΟΥΛΕΣ ΚΑΙ ΚΟΛΠΑ
- 5 ΠΙΟ ΑΣΦΑΛΗ ΑΝΤΑΛΛΑΓΗ ΜΗΝΥΜΑΤΩΝ
- 6 ΑΣΦΑΛΕΙΑ ΣΤΑ ΕΞΥΠΝΑ ΤΗΛΕΦΩΝΑ
- 7 ΣΕΡΦΑΡΙΣΜΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
- 8 ΑΣΦΑΛΕΙΑ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ
- 9 ΔΙΑΜΟΙΡΑΣΜΟΣ ΦΩΤΟΓΡΑΦΙΩΝ ΚΑΙ ΒΙΝΤΕΟ
- 10 ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΕΡΓΑΛΕΙΑ ΠΟΥ ΜΑΣ ΑΡΕΣΟΥΝ
- 11 ΕΥΧΡΗΣΤΟΣ ΟΔΗΓΟΣ ΓΙΑ ΤΗΝ ΕΦΑΡΜΟΓΗ SIGNAL

Συντάχθηκε από τους:

Kirsten Fiedler, EDRi
Theresia Reinhold, EDRi

Καλλιτεχνικά & σχεδιασμός από τους:

Gregor Sedlag
Heini Jarvinen
(Απεικονίσεις του EDRi-former)

Συνεισφορές από:

ApTI Romania
Bits of Freedom
CCC / Chaos macht Schule
Cryptoparty.in
Digitale Gesellschaft e. V.
EDRi (Brussels office)
Open Rights Group
Mediamocracy

Ιδιαίτερες ευχαριστίες στους:

Gloria González Fuster,
Vrije Universiteit Brussel (VUB)
Hans Martens,
Better Internet for Kids, EUN
Partnership AISBL

Μετάφραση στα ελληνικά και επιμέλεια ελληνικής έκδοσης:

Σίμος Δαλκυριάδης, μέλος στο Κόμμα Πειρατών Ελλάδας

Europen Digital Rights 20
Rue Belliard
B-1000 Brussels

edri.org
@edri
brussels@edri.org
+32 2 274 25 70



Τι είναι το διαδίκτυο;

Το διαδίκτυο είναι ένα παγκόσμιο δίκτυο συσκευών. Ένα από τα ιδιαίτερα χαρακτηριστικά του διαδικτύου είναι ότι πολλές διαφορετικές τεχνολογίες μπορούν όλες να χρησιμοποιηθούν μέσα στο ίδιο δίκτυο.

» **Όταν χρησιμοποιείς το διαδίκτυο ο φορητός σου υπολογιστής, το tablet ή το τηλέφωνό σου, είναι ένα μέρος του δικτύου.**

Το διαδίκτυο είναι παγκόσμιο, είναι γρήγορο και μας δίνει έναν ολόκληρο κόσμο από ευκαιρίες.

Το διαδίκτυο είναι μια καταπληκτική και ισχυρή εφεύρεση. Πριν το διαδίκτυο διαδοθεί ευρέως, δεν υπήρχε κάποιος εύκολος τρόπος σύνδεσης πολλών ανθρώπων μεταξύ τους.

Ήταν πολύ πιο δύσκολο να ακούσεις μουσική ή να παρακολουθήσεις μια ταινία.

Επίσης, το διαδίκτυο είναι ένα εξαιρετικό μέρος για μάθηση, καθώς όλο και περισσότερες πληροφορίες και γνώση μοιράζονται online. Η τεχνολογία του διαδικτύου είναι λίγο σαν ένας μεγάλος λόφος καλυμμένος με χιόνι, μπορούμε να τον χρησιμοποιήσουμε για να κάνουμε σκι, σνόουμπορντ ή για να φτιάξουμε έναν χιονάνθρωπο. Το μόνο που χρειαζόμαστε είναι χιόνι!

Στον online κόσμο, ο λόφος είναι η σύνδεση μας στο διαδίκτυο και το χιόνι είναι η γλώσσα που μιλά το δίκτυο, το “διαδικτυακό πρωτόκολλο” (internet protocol)!

Τα κοινωνικά δίκτυα και οι άλλες online υπηρεσίες μοιάζουν να είναι δωρεάν, αλλά στην πραγματικότητα χρηματοδοτούνται με τις προσωπικές μας πληροφορίες, αυτές που οικειοθελώς βάζουμε σε απευθείας σύνδεση. Πληροφορίες σχετικά με το τι γράφουμε ή με το τι διαβάζουμε ή με το τι βλέπουμε, παρακολουθούνται και χρησιμοποιούνται από τις online εταιρείες.

» **Πώς μπορείς να διατηρήσεις τον έλεγχο των πληροφοριών που μοιράζεις στο διαδίκτυο;**

Θα βρεις την απάντηση σε αυτό το ερώτημα σε αυτό εδώ το φυλλάδιο.

Τι είναι ιδιωτικότητα;

Αν έχουμε ιδιωτικότητα, έχουμε τον έλεγχο. Αλλά τι σημαίνει αυτό;

» **Η ιδιωτικότητα είναι το δικαίωμά μας να αποφασίζουμε το τι μοιραζόμαστε και με ποιους το μοιραζόμαστε.**

Αυτό σημαίνει, για παράδειγμα, ότι έχεις το δικαίωμα να ρωτήσεις την Google, το Facebook και τους άλλους, το τι είδους πληροφορίες έχουν συλλέξει για εσένα. Μπορείς επίσης να τους ζητήσεις να διαγράψουν αυτά τα δεδομένα.

Όταν προστατεύουμε την ιδιωτικότητα μας, μπορούμε να νιώθουμε πιο ασφαλείς και προστατευμένοι, γιατί μπορεί να υπάρχουν πληροφορίες που θα μπορούσαν να μας βλάψουν, αν τις μάθαινε το λάθος άτομο.

Θα μπορούσε να είναι πληροφορίες που θέλουμε να μοιραστούμε με κάποιους ανθρώπους, όπως με τους γονείς ή με τους δασκάλους μας, αλλά όχι με κάποιον άλλον.

Αλλά μπορούμε επίσης να βοηθήσουμε και τους άλλους, όταν προστατεύουμε την ιδιωτικότητά μας, γιατί ίσως να θέλουν να μοιραστούν κάτι μαζί μας που δεν πρέπει να μοιραστεί με κανέναν άλλο.

» **Όλοι έχουμε κάτι που δεν θέλουμε να μοιραστούμε με άλλους.**

Το φροντίζουμε την δική μας ιδιωτικότητα, αυτό έχει πολλά να κάνει και με τη φροντίδα των φίλων μας επίσης, γιατί μας βοηθάει να είμαστε ελεύθεροι, ασφαλείς και αξιόπιστοι.

Οι γονείς μας, οι φίλοι μας ή όποιος χρησιμοποιεί τον υπολογιστή μετά από εμάς, μπορεί επίσης μερικές φορές να δει σε τι έχουμε κάνει αναζήτηση. Αυτό μπορεί να συμβεί αν ξεχάσεις να αποσυνδεθείς ή απλά αν κοιτάξουν στο ιστορικό του υπολογιστή.

» **ΤΟ ΗΞΕΡΕΣ;**

Μόλις μόνο πριν από 20 χρόνια, τα περισσότερα σπίτια είχαν μόνο μία τηλεφωνική γραμμή που μόνο ένα άτομο μπορούσε να χρησιμοποιήσει σε μια δεδομένη στιγμή. Σχεδόν κανένας δεν είχε κινητό τηλέφωνο και πολλοί άνθρωποι δεν είχαν e-mail.

[A] ...ένα δίκτυο συσκευών.

[B] ...ένα αποτελεσματικό εργαλείο για την αλιεία σε διεθνή ύδατα.

[C] ...ένα κοινωνικό δίκτυο.

» **ΓΡΙΦΟΣ 1: ΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ...**



Προσάτεψε τον εαυτό σου στα κοινωνικά δίκτυα

Μπορεί να είναι όντως πολύ διασκεδαστικό να χρησιμοποιείς τα κοινωνικά δίκτυα. Στα κοινωνικά δίκτυα, μπορούμε να συνομιλήσουμε με τους φίλους και την οικογένειά μας, να μοιραστούμε φωτογραφίες, να στείλουμε προσωπικά μηνύματα και να κοινοποιήσουμε πληροφορίες δημόσια.

Σε ορισμένες χώρες, τα παιδιά κάτω από τα 13 δεν επιτρέπεται να χρησιμοποιούν κάποιο από τα κοινωνικά δίκτυα. Αν θέλεις να χρησιμοποιήσεις τα κοινωνικά δίκτυα, το καλύτερο είναι να ρωτήσεις την οικογένειά σου και τους δασκάλους σου.

» **To YouTube, το Facebook, το Instagram, το Snapchat, το Diaspora και άλλα, είναι όλα κοινωνικά δίκτυα.**

» ΤΟ ΗΞΕΡΕΣ;

Ότι πληκτρολογείς σε μια μηχανή αναζήτησης ή γράφεις σε ένα μήνυμα συνομιλίας με ένα φίλο σου, δεν διαγράφεται πλήρως. Οι εταιρείες που παρέχουν τις υπηρεσίες που χρησιμοποιούμε (όπως το YouTube, το Facebook, το Snapchat και τα άλλα) μπορεί να καταγράφουν ότι γράφουμε, τις ιστοσελίδες που επισκεπτόμαστε και τα πράγματα που ψάχνουμε online.

Έχεις κάποια αγαπημένα από αυτά; Γιατί σου αρέσουν;

Ορισμένα κοινωνικά δίκτυα αποθηκεύουν ακόμα και τα μηνύματα που δεν στέλνουμε! Φαντάσου ότι γράφεις ένα μήνυμα σε κάποιον φίλο σου στο Facebook και δεν το στέλνεις, ο φίλος σου δεν θα ξέρει για το μήνυμα. Αλλά το Facebook το αποθηκεύει!

Να θυμάσαι ότι όλα όσα κάνουμε σε ένα κοινωνικό δίκτυο καταγράφονται στους υπολογιστές των εταιρειών. Αυτό δεν σημαίνει ότι πρόκειται να κάνουν κάτι κακό με αυτά, αλλά θα πρέπει να γνωρίζεις ότι αυτό συμβαίνει.

MS. ANONYMITY



ΟΜΑΔΑ:

DIGITAL
DEFENDERS

ΔΥΝΑΜΕΙΣ:

Πειράματα από την κυβέρνηση έχουν αυξήσει το ανοσοποιητικό της σύστημα. Έχει επίσης τη δυνατότητα να χρησιμοποιεί τα κοινωνικά δίκτυα ανώνυμα, έτσι κανείς δεν ξέρει ποια είναι πραγματικά.

ΟΠΛΑ:

Είναι εξειδικευμένη σε μάχη σώμα-με-σώμα.

I.D. THIEF



ΟΜΑΔΑ:

DATA
INTRUDERS

ΔΥΝΑΜΕΙΣ:

Μπορεί να δει τι κάνεις σε απευθείας σύνδεση και, στη συνέχεια, να κλέψει τα προσωπικά σου στοιχεία. Προσποιείται ότι είσαι εσύ και προσπαθεί να χρησιμοποιήσει το όνομά σου, στα κοινωνικά δίκτυα και στους λογαριασμούς ηλεκτρονικού ταχυδρομείου σου για εγκληματικές δραστηριότητες.

ΟΠΛΑ:

Ο ιός άλφα - τον οποίο χρησιμοποιεί για να διεισδύσει σε υπολογιστές και σε κινητά τηλέφωνα.



» **ΓΡΙΦΟΣ 2: Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΕΙΝΑΙ ΣΗΜΑΝΤΙΚΗ ΕΠΕΙΔΗ...**

[T] ...μας βοηθά να παρακολουθούμε μουσικά βίντεο.

[R] ...μας βοηθά να είμαστε ελεύθεροι και να έχουμε τον έλεγχο σε απευθείας σύνδεση.

[G] ...μας βοηθά να μοιραστούμε τις φωτογραφίες μας με ολόκληρο τον κόσμο.

Τρεις κορυφαίες συμβουλές και κόλπα

1. Δεν χρειάζεται ο καθένας να πρέπει να ξέρει τα πάντα για εμάς

Όπως και στον πραγματικό κόσμο, είναι καλύτερα να επιλέξεις προσεκτικά το τι θέλεις να μοιραστείς και το τι όχι. Ενστικτωδώς, μοιραζόμαστε κάποια πράγματα με κάποιους ανθρώπους και όχι με κάποιους άλλους. Το διαδίκτυο, μερικές φορές, καθιστά δύσκολο να κάνουμε αυτή την επιλογή.

Αυτό είναι εν μέρει επειδή δεν είναι πάντα σαφές το τι είναι ιδιωτικό σε απευθείας σύνδεση και τι δεν είναι, και αυτό γίνεται εν μέρει επειδή το διαδίκτυο έχει διαφορετικούς κανόνες από τον εκτός σύνδεσης (offline) κόσμο.

Για παράδειγμα: Οι φίλοι μας θα συγχωρήσουν ένα ηλίθιο σχόλιο που κάναμε όταν ήμασταν οργισμένοι και θα κατανοήσουν τη συμπεριφορά μας, επειδή μας ξέρουν. Αν κάποιος άλλος διαβάσει το σχόλιό μας στο διαδίκτυο, δεν θα μπορούσε να καταλάβει τι εννοούσαμε και μπορεί να σκεφτεί ότι είμαστε κακεντρεχείς.

2. Η ασφάλεια και η ιδιωτικότητα σε απευθείας σύνδεση δεν είναι τόσο δύσκολη

Δεν χρειάζεται να είμαστε σούπερ σπασίγκλες για να είμαστε ασφαλείς στο διαδίκτυο. Μπορούμε να χρησιμοποιήσουμε ένα tablet, ένα τηλέφωνο ή το laptop μας, και οι άλλοι να μην έχουν πρόσβαση σε αυτό, με έναν κωδικό που κανένας δεν μπορεί να μαντέψει, να δούμε ένα βίντεο online χωρίς να μας παρακολουθούν. Μπορούμε να τα κάνουμε αυτά με πολύ απλό τρόπο.

3. Μαθαίνοντας σε τι ή απέναντι σε ποιον, να προστατευθούμε

Ακριβώς όπως οι τράπεζες προστατεύονται από τους κλέφτες, έτσι και εμείς θα πρέπει επίσης να προστατευθούμε -απέναντι στις εταιρείες που μας παρακολουθούν ηλεκτρονικά, στους συμμαθητές μας που μπορεί να κρατούν κάποια κακία ή στους αδιάκριτους γονείς μας... όταν αυτοί είναι αδιάκριτοι.

Θα πρέπει να αναρωτηθούμε ποιες είναι οι πραγματικές απειλές και τι μπορούμε να κάνουμε γι' αυτές. Μόλις ξεκαθαρίσουμε τις απειλές, θα δούμε ότι είναι εφικτό να είμαστε ασφαλείς και να έχουμε τον έλεγχο της ιδιωτικής μας ζωής.

Πιο ασφαλή αποστολή μηνυμάτων

Όλοι χρησιμοποιούμε τα τηλέφωνα μας για να στείλουμε μηνύματα στους φίλους και στην οικογένεια μας.

Αλλά μερικές εφαρμογές ανταλλαγής μηνυμάτων διαβάζουν το περιεχόμενο των μηνυμάτων μας και παρακολουθούν το σε ποιον μιλάμε. Ορισμένες εφαρμογές το κάνουν αυτό, έτσι ώστε να μπορούν να επωφεληθούν από αυτές τις πληροφορίες.

» Το τι λες και το τι κάνεις σε απευθείας σύνδεση (online) είναι πολύτιμο για τις εταιρείες.

Οι εταιρείες που φτιάχνουν τις εφαρμογές ανταλλαγής μηνυμάτων συχνά σαρώνουν το τι λέμε. Μπορεί να παρακολουθούν το σε ποιον μιλάμε, έτσι ώστε να μπορούν να μας δείχνουν στοχευμένες διαφημίσεις για να μας κάνουν να αγοράσουμε κάτι ή για να μοιραστούν αυτές τις πληροφορίες με άλλες εταιρείες.

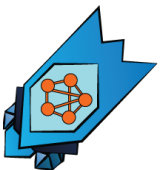
Μπορείς να δεις μια λίστα με πολύ καλές εφαρμογές ανταλλαγής μηνυμάτων στο τέλος του φυλλαδίου. Αυτές οι εφαρμογές ανταλλαγής μηνυμάτων διασφαλίζουν επίσης ότι δεν θα λαμβάνεις κείμενα από αγνώστους.

Και υπάρχει και ένας οδηγός για το πώς να εγκαταστήσεις το Signal, σε αυτό το φυλλάδιο, το Signal είναι μια cool εφαρμογή για να κρατήσεις τα μηνύματά σου ασφαλή.

[Q] ...είμαι σίγουρος ότι ποτέ δεν θα χρησιμοποιήσουν ή θα πουλήσουν τα δεδομένα μου.

[M] ...μπορώ να βρίσκομαι σε επαφή με τους φίλους και την οικογένεια μου.

[N] ...είμαι σίγουρος ότι μόνο οι φίλοι μου θα δουν τις φωτογραφίες που δημοσιεύω εκεί.



» ΓΡΙΦΟΣ 3: ΤΑ ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ ΕΙΝΑΙ ΥΠΕΡΟΧΑ ΓΙΑΤΙ...

Ασφάλεια στα έξυπνα τηλέφωνα (smartphones)

Τα τηλέφωνα μας έχουν γίνει πολύ σημαντικά στη χρησιμοποίηση του διαδικτύου.

Τα χρησιμοποιούμε όταν θέλουμε να επικοινωνήσουμε με τους φίλους και την οικογένειά μας, μέσα από την χρήση των κοινωνικών δικτύων ή απλά τα χρησιμοποιούμε για να περιηγηθούμε στο διαδίκτυο.

Αλλά τα τηλέφωνα μας είναι επίσης χρήσιμα και για πολλά άλλα πράγματα, όπως να τα χρησιμοποιήσουμε ως φακούς, να παίξουμε παιχνίδια ή για να δούμε πότε θα φτάσει στην στάση το επόμενο λεωφορείο.

Όταν εγκαθιστάς μια νέα εφαρμογή, διαβάζεις άραγε τι άδεια δίνεις στην εφαρμογή και σε τι μπορεί να έχει πρόσβαση στις πληροφορίες στο τηλέφωνό σου; Χρειάζεται άραγε πραγματικά μια εφαρμογή φακός να έχει πρόσβαση στον κατάλογο με τις επαφές σου;

Είναι πολύ δελεαστικό το να προσπεράσεις στα γρήγορα την οθόνη "Αποδοχή", αλλά είναι καλό να σταματήσεις και να σκεφτείς. Υπάρχουν καλοί λόγοι να μην εμπιστευτείς μια εφαρμογή που ζητά πράγματα που προφανώς δεν χρειάζεται.

» ΤΟ ΗΞΕΡΕΣ;

Πρέπει να υπάρχει ένας καλός λόγος για να δώσεις σε μια εφαρμογή άδεια για κάτι, μια εφαρμογή για φωτογραφίες για παράδειγμα, πρέπει να έχει πρόσβαση στη φωτογραφική μηχανή, τότε δεν χρειάζεται να ανησυχείς ιδιαίτερα. Αλλά αν νομίζεις ότι μια εφαρμογή σου ζητά πάρα πολλά, μπορείς να ψάξεις για το αν υπάρχουν και άλλες εκδόσεις της εφαρμογής που να ζητούν λιγότερα δικαιώματα.

Με λίγα μόνο κλικ μπορούμε επίσης να ελέγξουμε ακόμα και να περιορίσουμε τα δικαιώματα που έχουν οι ήδη εγκατεστημένες εφαρμογές στα τηλέφωνα μας. Στις περισσότερες συσκευές μπορούμε να βρούμε αυτές τις παραμέτρους στο "Ρυθμίσεις". Ρίξε μια ματιά εκεί στο τηλέφωνό σου, είναι καλό να μάθεις το πώς λειτουργεί το τηλέφωνό σου.

» Πολλές εφαρμογές έχουν πρόσβαση στα προσωπικά σου πράγματα που είναι αποθηκευμένα στο τηλέφωνό σου.

Μπορούμε να περιορίσουμε την πρόσβαση στην τοποθεσία μας, να προσθέσουμε έναν κωδικό πρόσβασης για να ξεκλειδώνει η οθόνη του τηλεφώνου μας, θα μπορούσαμε επίσης να κρυπτογραφήσουμε (προστασία) ολόκληρο το τηλέφωνο με λίγα μόνο κλικ.

Το να κάνουμε τα τηλέφωνα μας πιο ασφαλή και πιο φιλικά στην ιδιωτικότητα, δεν παίρνει πολύ χρόνο. Προς το τέλος αυτού του φυλλαδίου, μπορείς να βρεις μια λίστα με πολύ καλές εφαρμογές για αυτό το θέμα.

MIND FREER



ΟΜΑΔΑ:

DIGITAL DEFENDERS

ΔΥΝΑΜΕΙΣ:

Αγωνίζεται για το δικαίωμά μας να αποφασίζουμε το τι θα μοιραζόμαστε και με ποιον. Έχει τη δυνατότητα να δημιουργήσει ένα ιδιωτικό και ασφαλές περιβάλλον, όπου μπορείς να λες ότι σκέφτεσαι.

ΟΠΛΑ:

Το μυαλό του.

MAN IN THE MIDDLE



ΟΜΑΔΑ:

DATA INTRUDERS

ΔΥΝΑΜΕΙΣ:

Έχει μυστικιστικές δυνάμεις στο να παρακολουθεί τι κάνεις στο διαδίκτυο. Μπορεί να προσποιείται ότι είναι ένα νόμιμο πρόσωπο σε απευθείας σύνδεση και στη συνέχεια να το χρησιμοποιήσει αυτό για να χακάρει κατευθείαν στην επικοινωνία σου, να διαβάσει τα μηνύματά σου, να βλέπει τις φωτογραφίες σου και να παρακολουθεί τα βίντεό σου.

ΟΠΛΑ: Η αμφίεση του και οι κεραίες του.

DATA
INTRUDERS

ΕΙΣΒΟΛΕΙΣ
ΔΕΔΟΜΕΝΩΝ

DIGITAL
DEFENDERS

ΨΗΦΙΑΚΟΙ
ΥΠΕΡΑΣΠΙΣΤΕΣ



Σερφάρισμα στο διαδίκτυο

Με ένα πρόγραμμα περιήγησης είναι συχνά το πώς χρησιμοποιούμε το διαδίκτυο.

» **Είναι εύκολο να ξεχάσουμε ότι ο browser είναι κι αυτός ένα κομμάτι λογισμικού.**

Μερικές φορές είναι το πρώτο πράγμα που ανοίγεις στο τηλέφωνο, στο tablet ή στον υπολογιστή σου και το τελευταίο που κλείνεις. Αλλά συμβαίνουν πάρα πολλά στο εσωτερικό του προγράμματος περιήγησης που εσύ δεν τα γνωρίζεις και από αυτά κάποια είναι κακά (ή καλά) για την ιδιωτικότητά σου.

Όταν βγαίνουμε online για να αγοράσουμε κάτι, να δούμε ένα βίντεο ή να δούμε τι ποστάρουν οι φίλοι μας, αφήνουμε ψηφιακά αποτυπώματα. Ορισμένες ιστοσελίδες και κοινωνικά δίκτυα χρησιμοποιούν αυτά τα χνάρια για να μας παρακολουθούν.

» ΤΟ ΗΞΕΡΕΣ;

Σιγουρέψου ότι έχεις δει τα “privacy options” στον browser σου και έχεις αλλάξει τις προεπιλεγμένες ρυθμίσεις, ώστε να αποκτήσεις τον έλεγχο! Πολλοί πιστεύουν ότι ο καλύτερος browser για την προστασία της ιδιωτικότητας και για την ασφάλεια τους είναι ο Firefox, το ίδιο πιστεύει και ο PERFECT WAVE! Γιατί; Επειδή μπορείς να τον προσαρμόσεις, να τον ελέγξεις και να δεις το πώς λειτουργεί. Είναι πιθανό να μην είναι εγκατεστημένος στον υπολογιστή σου, αλλά μπορείς να τον κατεβάσεις πολύ εύκολα.



» ΓΡΙΦΟΣ 4: ΟΡΙΣΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ...

» **Οι ιστοσελίδες συλλέγουν πολλά πράγματα για εμάς!**

Ποιοι είναι οι φίλοι μας, τι μας αρέσει, τι ψάχνουμε και τι ακούμε, όλα τους είναι πράγματα που παρακολουθούνται. Αυτές οι ιστοσελίδες μπορεί να το κάνουν αυτό επειδή χρησιμοποιούν τα “cookies” στα προγράμματα περιήγησης μας. Αυτά τα “cookies” είναι μικρά κομμάτια λογισμικού.

Είναι αόρατα σε εμάς, αλλά αρκετά από τα δεδομένα μας συλλέγονται και συνδυάζονται με άλλες πληροφορίες, προσωπικά στοιχεία που θεωρούμε ότι είναι μυστικά γίνονται γνωστά σε πολλούς ανθρώπους και σε εταιρείες.

Οι περισσότερες συσκευές έρχονται με έναν browser. Στα Windows υπάρχει ο Internet Explorer, οι Apple συσκευές έχουν το Safari και ο προεπιλεγμένος browser στις Android συσκευές είναι το Google Chrome. Αλλά αυτοί δεν είναι αναγκαία και οι καλύτεροι browsers για μας.

PERFECT WAVE



ΟΜΑΔΑ:

DIGITAL DEFENDERS

ΔΥΝΑΜΕΙΣ:

Μπορεί να σερφάρει στο διάστημα, στο υπερδιάστημα και στον κυβερνοχώρο πάνω στην σανίδα του. Ο PERFECT WAVE δεν χρειάζεται φαγητό και νερό, μπορεί να επιβιώσει με τη μετατροπή των δεδομένων σε ενέργεια. Είναι σχεδόν ολοκληρωτικά άφθαρτος.

ΟΠΛΑ: Η σανίδα του.

KRAZY KOOKIE



ΟΜΑΔΑ:

DATA INTRUDERS

ΔΥΝΑΜΕΙΣ:

Πάντα ψάχνει για καυγά. Μισεί όλους τους υπερασπιστές αλλά θεωρεί τον PERFECT WAVE τον χειρότερο από τους εχθρούς του. Έχει μια τερατώδη όρεξη για τα μυστικά σου.

ΟΠΛΑ:

Ο ρομποτικός περιστρεφόμενος βραχίονας του.

[F] ...είναι τόσο ασφαλείς που δεν χρειάζεται να νοιαστώ καθόλου για τα δεδομένα μου.

[L] ...είναι καλύτερες από σοκολάτα.

[O] ...μπορούν να έχουν πρόσβαση στις επαφές μου, στις φωτογραφίες μου και στα μηνύματα.

Ασφάλεια κωδικών πρόσβασης

Οι κωδικοί πρόσβασης. Πολύ σημαντικοί στην ψηφιακή εποχή.

Πραγματικά εξαιρετικά σημαντικοί. Αποτελούν τη βάση της ασφάλειας και της ιδιωτικότητας μας. Και οι κωδικοί πρόσβασης των περισσότερων ανθρώπων είναι πολύ, πολύ αδύναμοι, ο πιο συχνά χρησιμοποιούμενος κωδικός πρόσβασης είναι η λέξη "password" ή το "12345".

Η δημιουργία ενός ασφαλούς κωδικού πρόσβασης δεν είναι πολύ δύσκολη υπόθεση.

1. Ποτέ μην χρησιμοποιείς τον ίδιο κωδικό πρόσβασης πάνω από μια φορά

Αυτός είναι πραγματικά ένας από τους πιο σημαντικούς κανόνες! Τουλάχιστον, προσπάθησε να κάνεις διαφορετικές εκδόσεις του κωδικού πρόσβασης που έχεις φτιάξει.

Γιατί; Διότι, αν οι εγκληματίες (όπως ο DATA SMUGGLER) αποκτήσουν πρόσβαση στους κωδικούς μίας υπηρεσίας, συχνά προσπαθούν να συνδεθούν και σε άλλες υπηρεσίες με τον ίδιο κωδικό πρόσβασης. Ξέρουν ότι οι άνθρωποι τείνουν να χρησιμοποιούν τον ίδιο κωδικό.

2. Ποτέ μην χρησιμοποιείς μια λέξη από το λεξικό

...δεν έχει σημασία πόσο μεγάλη είναι ή πόσο περίπλοκη μπορεί να φαίνεται.

Γιατί; Επειδή υπάρχουν προγράμματα υπολογιστών που δοκιμάζουν κάθε λέξη από το λεξικό ως έναν τρόπο για να "μαντέψουν" τον κωδικό πρόσβασης σου. Κάθε superhero στην ομάδα των υπερασπιστών μας χρησιμοποιεί ισχυρούς και ευφάνταστους κωδικούς πρόσβασης. Μπορείς να παραδειγματιστείς από αυτούς, ο κωδικός πρόσβασης σου είναι το όπλο σου για να παραμείνεις εκτός κινδύνου!

3. Ο κωδικός σου πρέπει να είναι τουλάχιστον μήκους 12 χαρακτήρων

Κι αυτό το μήκος είναι το ελάχιστο. Όσο μακρύτερος είναι ένας κωδικός πρόσβασης, τόσο πιο δύσκολο είναι να τον χακάρουν.

Γιατί; Επειδή όσο πιο μεγάλος ο κωδικός τόσο πιο δύσκολο είναι να τον μαντέψει κάποιος. Μερικοί εμπειρογνώμονες λένε ότι είναι εντάξει να τον καταγράψεις κάπου, απλά θα πρέπει να κρύψεις το χαρτί πάρα πολύ καλά!

QUEEN OF LOCKS



ΟΜΑΔΑ:

DIGITAL DEFENDERS

ΔΥΝΑΜΕΙΣ:

Αγωνίζεται για την προστασία της ιδιωτικής ζωής και για την ασφάλεια. Δίνει ισχυρά ιδιωτικά κλειδιά στους ανθρώπους που βρίσκονται σε κίνδυνο και τους βοηθά να εξασφαλίσουν τα προσωπικά τους δεδομένα στο διαδίκτυο.

ΟΠΛΑ:

Το κράνος της, το χρησιμοποιεί για να ρίξει ακτίνες ενέργειας από τα μάτια της. Μπορεί να διαπεράσει το επικίνδυνο δίκτυο του FINN PHISHER.

FINN PHISHER



ΟΜΑΔΑ:

DATA INTRUDERS

ΔΥΝΑΜΕΙΣ:

Κατέχει υπεράνθρωπη αντοχή, ταχύτητα και αντανakλαστικά. Χρησιμοποιεί τις δυνάμεις του για να διεισδύσει στο τηλέφωνο σου και να "ψαρέψει" όλα τα μυστικά σου.

ΟΠΛΑ:

Ρίχνει ένα ηλεκτροστατικό δίχτυ για δεδομένα για να αναισθητοποιήσει τους αντιπάλους του.



» ΓΡΙΦΟΣ 5: ΟΤΑΝ ΠΕΡΙΗΓΟΥΜΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ...

[X] ...μπορώ να κάνω ότι θέλω και να είμαι ασφαλής, δεν είναι ένας πραγματικός κόσμος!
[U] ...μπορώ να προστατευτώ αν δεν επιτρέπω τα cookies και το ιστορικό στον browser.
[Y] ...δεν είμαι πάρα πολύ προσεκτικός, επειδή δεν έχω τίποτα να κρύψω.

Διαμοιρασμός φωτογραφιών και βίντεο

Λέμε στους φίλους μας για την καθημερινή μας ζωή μέσα από τον διαμοιρασμό φωτογραφιών και βίντεο για εμάς σε απευθείας σύνδεση.

» **Ο διαμοιρασμός είναι cool, αλλά οι φωτογραφίες και τα βίντεο μπορούν να αντιγραφούν εύκολα.**

Να θυμάσαι ότι είναι πάντα σημαντικό να βεβαιώνεις ότι δεν μοιράζεις πράγματα με τους ανθρώπους που δεν θέλεις να μοιραστείς το οτιδήποτε. Οι άνθρωποι μπορεί να είναι σε θέση να δουν τις ιδιωτικές μας εικόνες και να κάνουν κακή χρήση αυτών.

Ποιο είναι το πρόβλημα; Αν στείλεις μια εικόνα ή ένα βίντεο, στέλνεις ένα αντίγραφο τους από τη συσκευή σου στην συσκευή ενός φίλου. Φαντάσου ότι ο φίλος σου θα μοιραστεί την εικόνα ή το βίντεο και πάλι με άλλους. Κάθε αντίγραφο μπορεί να αντιγραφεί και πάλι.

Αν μοιράσουμε μια φωτογραφία ή ένα βίντεο σε απευθείας σύνδεση, θα υπάρχουν πάντα πολλά αντίτυπα τους σε διάφορες συσκευές.

Ακόμα και αν διαγράψεις την αρχική εικόνα από τις δικές σου συσκευές, τα υπόλοιπα αντίγραφα θα συνεχίσουν να υπάρχουν.

Όταν μοιραζόμαστε κάτι, αυτό μπορεί να φτάσει στα χέρια ανθρώπων που δεν θα θέλαμε να το αποκτήσει. Μερικοί άνθρωποι θα μπορούσαν ακόμη και να προσπαθήσουν να κλέψουν την ταυτότητά μας, χρησιμοποιώντας τις εικόνες μας, ακριβώς όπως κάνει ο I.D. THIEF.

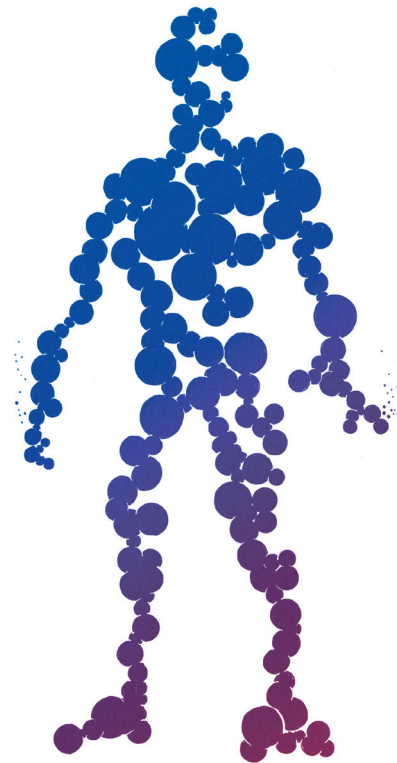
Το Snapchat είναι μια εφαρμογή για να μοιράζεις τις φωτογραφίες κι αυτές να εξαφανίζονται γρήγορα. Δυστυχώς, παραμένει και εκεί δυνατό να αποθηκευτεί μια φωτογραφία, με μερικά κόλπα και να την μοιράσουν και πάλι. Χιλιάδες εικόνες στο Snapchat έχουν ήδη βγει στο διαδίκτυο.

Αυτό σημαίνει ότι όλοι πρέπει να ζουν με την πιθανότητα ότι τα κοινωνικά δίκτυα μπορούν να χρησιμοποιηθούν με καλούς τρόπους, καθώς και με κακούς τρόπους. Γι' αυτό και πρέπει να σκεφτούμε πριν δημοσιεύσουμε ή πριν στείλουμε φωτογραφίες και βίντεο μέσω διαδικτύου! Θα πρέπει να αναρωτηθούμε για το αν θα βάλουμε μια φωτογραφία στο δημόσιο ιστοχώρο του σχολείου μας. Αν δεν πρέπει, ίσως να μην είναι καλή ιδέα να την μοιραστείς σε απευθείας σύνδεση.

Εάν η φωτογραφία μας δείχνει και άλλους ανθρώπους, θα πρέπει να ζητήσεις την άδειά τους πριν από τον διαμοιρασμό της, διότι είναι δικαίωμά τους να αποφασίσουν σχετικά.

Για εικόνες που δεν είναι δικές μας, θα πρέπει να ζητήσουμε από τον ιδιοκτήτη τους να μας δώσει άδεια πριν τις μοιράσουμε στο διαδίκτυο.

JOHNNY RANDOM



ΟΜΑΔΑ:

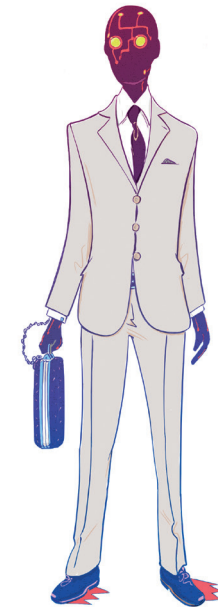
DIGITAL DEFENDERS

ΔΥΝΑΜΕΙΣ:

Γεννήθηκε στον πλανήτη Entropia, κάπου σε έναν μακρινό γαλαξία. Όπως όλα τα μέλη του είδους του, έχει τη δυνατότητα να αλλάξει το σχήμα του κατά βούληση. Μπορεί να προστατεύσει τα μυστικά σας με τυχαία αλλαγή των κωδικών πρόσβασης.

ΟΠΛΑ: Τα κύρια όπλα του είναι τα ενεργειακά φορτισμένα μέρη του σώματός του, που μπορεί να τα ρίξει και να τα ανακτήσει οποιαδήποτε στιγμή.

DATA SMUGGLER



ΟΜΑΔΑ:

DATA INTRUDERS

ΔΥΝΑΜΕΙΣ:

Είναι πολύ πλούσιος και έχει ικανότητες πολύ ανώτερες από άνθρωπο. Είναι απίστευτα ευέλικτος και έχει υπεράνθρωπη αντοχή. Συλλέγει τα πολύτιμα προσωπικά δεδομένα (όπως τις φωτογραφίες και τα μηνύματά σας) και τα πουλά στη μαύρη αγορά.

ΟΠΛΑ:

Κουβαλάει διάφορους τύπους όπλων στη βαλίτσα του.

ΚΕΦΑΛΑΙΟ 10

Εφαρμογές & εργαλεία που μας αρέσουν

ΕΦΑΡΜΟΓΕΣ ΓΙΑ SMARTPHONE

Εφαρμογή	Τι κάνει	Δυσκολία στη χρήση
Signal	Μηνύματα, SMS και κρυπτογράφηση κλήσεων τηλεφώνου (εναλλακτικό του WhatsApp)	Εύκολο
OrBot & OrFox	Ανώνυμο серφάρισμα στο διαδίκτυο	Εύκολο
KeePassDroid	Διαχειρίζεται όλους τους κωδικούς πρόσβασης σου	Εύκολο
F-Droid	Αποθετήριο λογισμικού με εφαρμογές που είναι ανοιχτές και δωρεάν (εναλλακτικό του Google Play)	
K9 Mail	Διαχειρίζεται τα email σου	Εύκολο
ChatSecure	Εφαρμογή μηνυμάτων για πολλούς λογαριασμούς όπως για το Facebook και για το Google	Μεσαίας δυσκολίας
Transportr	Δημόσιες συγκοινωνίες, δες χρονοδιαγράμματα για γραμμές λεωφορείων και τρένων	Εύκολο
Csip Secure	Κρυπτογραφημένες κλήσεις (εναλλακτικό του Skype)	Μεσαίας δυσκολίας
APG	Για την κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου με το K9 Mail	Δύσκολο

ΛΟΓΙΣΜΙΚΟ ΓΑ WINDOWS, MAC ΚΑΙ LINUX

Εφαρμογή	Τι κάνει	Δυσκολία στη χρήση
Jitsi	Κρυπτογραφημένες κλήσεις βίντεο	Μεσαίας δυσκολίας
Tor Browser	Ανώνυμο серφάρισμα στο διαδίκτυο	Εύκολο
Pidgin και OTR Plugin	Αποστολή μηνυμάτων (συμβατό με το ChatSecure)	Μεσαίας δυσκολίας
Thunderbird & Enigmail	Διαχείριση λογαριασμών e-mail, το Enigmail Add-on κρυπτογραφεί τα emails	Μεσαίας δυσκολίας

BROWSER PLUG-INS, ADD-ONS AND EXTENSIONS

Plug-in	Τι κάνει	Δυσκολία στη χρήση
Disconnect.me	Μπλοκάρει τα cookies και τους trackers	Εύκολο
Privacy Badger	Μπλοκάρει τους trackers	Εύκολο
HTTPS Everywhere	Αναγκάζει τις ιστοσελίδες να χρησιμοποιούν μια πιο ασφαλή μέθοδο, εάν είναι δυνατό	Εύκολο
Destructing Cookies	Αφαιρεί τα cookies όταν δεν χρησιμοποιούνται πλέον από ανοιχτές καρτέλες στον browser	Μεσαίας δυσκολίας
NoScript	Μπλοκάρει τα JavaScript	Δύσκολο



» ΓΡΙΦΟΣ 6: ΠΡΕΠΕΙ ΝΑ ΕΠΙΛΕΓΩ ΩΣ ΚΩΔΙΚΟ ΠΡΟΣΒΑΣΗΣ...

ΚΕΦΑΛΑΙΟ 11

Εύχρηστος οδηγός για την εφαρμογή Signal

Το Signal είναι μια δωρεάν εφαρμογή για Android και για iPhone. Δεν παρακολουθεί το τι λες ή με ποιους μιλάς. Μπορείς να το χρησιμοποιήσεις για αποστολή κειμένου, για κλήσεις και για να μοιράσεις φωτογραφίες, βίντεο και επαφές.

Δεν είναι η μόνη εφαρμογή που μπορούμε να χρησιμοποιήσουμε για να επικοινωνούμε με ασφάλεια, αλλά είναι μια από τις πιο εύκολες στη χρήση. Εδώ είναι ένας εύχρηστος οδηγός για αυτήν την εφαρμογή σε πέντε απλά βήματα:

1. Πηγαίνεις στο Play Store (Android) ή το App Store (iPhone). Ψάχνεις να βρεις το "Signal". Επιλέγεις την εφαρμογή "Signal Private Messenger" και επιλέγεις >Εγκατάσταση<. Μετά την εγκατάσταση του Signal, ανοίγεις την εφαρμογή.

2. Καταχωρείς τον αριθμό του τηλεφώνου σου με το Signal εισάγοντας τον αριθμό του κινητού σου τηλεφώνου και επιλέγοντας >Register< ή >Verify your Device<. Θα λάβεις ένα μήνυμα κειμένου με έναν εξαψήφιο κωδικό. Βάλε αυτόν τον κωδικό στο Signal.

3. Επιλέγεις το μολύβι κάτω δεξιά (Android) ή το σύμβολο »+« στην επάνω δεξιά γωνία (iPhone) για να ξεκινήσεις μια συζήτηση.

4. Επιλέγεις το άτομο που θέλεις να αποστείλεις κείμενο ή να καλέσεις.

5. Εάν θέλεις να αλλάξεις κατάσταση από την ασφαλή αποστολή μηνυμάτων μέσω της σύνδεσης σου στο διαδίκτυο με τα ανασφαλή SMS, απλά κρατάς πατημένο το κουμπί »Send« για λίγο παραπάνω χρόνο από το κανονικό.

Είναι πολύ πιο ασφαλές όταν το πρόσωπο με το οποίο επικοινωνείς χρησιμοποιεί επίσης το Signal. Χρησιμοποιεί την σύνδεση μας στο διαδίκτυο, όταν επικοινωνούμε με έναν άλλο χρήστη του Signal και με κανονικό SMS ή minutes, όταν επικοινωνούμε με κάποιον που δεν χρησιμοποιεί το Signal.

Να θυμάσαι! Δεν χρειάζεται ο καθένας που ξέρεις να χρησιμοποιεί το Signal. Απλά πες στους πιο στενούς φίλους σου και στους ανθρώπους με τους οποίους επικοινωνείς πιο συχνά, να εγκαταστήσουν την εφαρμογή και έτσι όλο και πιο πολλοί θα αρχίσουν να την χρησιμοποιούν.

Το φυλλάδιο αυτό δημιουργήθηκε χάρη στους:

- μεμονωμένους χορηγούς στο GlobalGiving.com - Σας ευχαριστούμε όλους για τη συμβολή σας!
- τα Ιδρύματα Adessium Foundation και Open Society Foundations

Το έγγραφο αυτό διανέμεται με μια άδεια [Creative Commons 2.0 Licence \(CC BY 2.0\)](#)

[R] ...έναν τυχαίο συνδυασμό γραμμάτων και ειδικών χαρακτήρων.

[V] ...το 123456789 - είναι εύκολο να το θυμάμαι.

[D] ...την πρώτη λέξη που βλέπω όταν ανοίγω ένα τυχαίο βιβλίο από μια τυχαία σελίδα.