Τηλέφωνο

Για ασφαλείς, άρα κρυπτογραφημένες, τηλεφωνικές κλήσεις, υπάρχουν ειδικές εφαρμογές που μπορούμε να εγκαταστήσουμε στο τηλέφωνό μας ή στον υπολογιστή μας. Τέτοια εργαλεία είναι το RedPhone [1] για Android, το SilentCircle [2] για iPhone και το jitsi για υπολογιστές [3]. Αντίστοιχα θα βρούμε και ειδικές εφαρμογές για κρυπτογράφηση SMS, πχ TextSecure [1].Φυσικά πρέπει πάντα να συνειδητοποιούμε τι σημαίνει να κουβαλάμε πάντα μαζί μας ένα smartphone και τι επιπτώσεις έχει ακόμα και αυτή η κίνησή μας για την ιδιωτικότητά μας [4].

[1] https://whispersystems.org/
[2] https://silentcircle.com/
[3] https://jitsi.org
[4] https://skytal.es/blog/articles/ase-to-kinito-sou-spiti-1/

Περισσότερη ενημέρωση

Περισσότερες πληροφορίες στα Ελληνικά σχετικά με θέματα ψηφιακών δικαιωμάτων και ψηφιακών ελευθεριών μπορεί υπάρχουν στο site [1] και στην mailing list [2] του Digital Liberation Network (DLN) καθώς και στο skytal.es [3]. Μια σειρά σχετικών παρουσιάσεων βρίσκονται και στις σελίδες του hackerspace.gr [4]. Σε Ευρωπαικό επίπεδο πολύ μεγάλο ενδιαφέρον παρουσιάζουν οι κινήσεις των ομάδων La Quadrature du Net [5], European Digital Rights (EDRI), Bits of Freedom [6] και Chaos Computer Club [7]. Μεγάλη ευαισθητοποίηση όμως σε σχέση με τα ψηφιακά δικαιώματα έχουν ομάδες και ΜΚΟ που βρίσκονται στην Αμερική, είτε γιατί εκεί είναι και εντονότερο το πρόβλημα της παρακολούθησης είτε γιατί υπάρχουν πολυπλυθέστερες ομάδες με βαθύτερες τεχνικές γνώσεις. Μερικά σημεία για να ξεκινήσει κανείς είναι σίγουρα το EFF [8], η mailing list liberationtech [9], η βιβλιοθήκη cryptome [10], η mailing list cryptography [11], κτλ. Ένα site με λίστα εργαλείων για την προστασία της ιδιωτικότητας μπορεί να βρει κανείς και στο tacticaltech [12]

1] https://dln.gr/
[2] https://lists.espiv.net/cgi-bin/mailman/listinfo/information_society
[3] https://skytal.es/
[4] https://www.hackerspace.gr/wiki/CryptoParty
[5] https://www.laquadrature.net/
[6] http://www.edri.org
[7] https://www.ccc.de/
[8] https://www.eff.org/
[9] https://mailman.stanford.edu/mailman/listinfo/liberationtech
[10] http://cryptome.org/
[11] http://www.mail-archive.com/cryptography@metzdowd.com/
[12] https://alternatives.tacticaltech.org

Δίκτυο για την Ψηφιακή Απελευθέρωση
dln.gr | info@dln.gr

skytales

Σκοπός αυτού του φυλλαδίου δεν είναι να σου μάθει τα πάντα για την ψηφιακή ασφάλεια και την προστασία της ιδιωτικότητάς σου, αλλά να σου δείξει τον δρόμο, κάποια βασικά βήματα που μπορείς να κάνεις, και το σημαντικότερο, να τα δείξεις έπειτα και στους φίλους σου, στους γνωστούς σου και στην οικογένειά σου. Δεν έχει νόημα να προστατεύεις μόνο τις δικές σου επικοινωνίες όταν οι γύρω σου δεν προσέχουν, θα παρακολουθείσαι μέσω των γνωστών σου...

Δίκτυο για την Ψηφιακή Απελευθέρωση
dln.gr | info@dln.gr

Διεκδικώντας Ψηφιακή Ελευθερία στην εποχή της μαζικής παρακολούθησης

Μετά τις αποκαλύψεις του Edward Snowden είναι πλέον γνωστό σε όλους, με τον πιο επίσημο τρόπο, πως υπάρχουν υπηρεσίες χωρών που με τον ένα ή τον άλλο τρόπο παρακολουθούν όσες περισσότερες επικοινωνίες πολιτών μπορούν, σε παγκόσμιο επίπεδο. Προβάλλοντας τον μανδύα της "προστασίας από τους τρομοκράτες", έχουν επενδύσει στη δημιουργία ενός κλίματος φόβου ώστε να μπορούν, με νόμιμα ή μη μέσα, να δικαιολογούν την παρακολούθηση των πάντων. Είτε είναι πολίτες της δικής τους χώρας είτε πολίτες άλλων χωρών.

Τι σημαίνει όμως παρακολούθηση στην ψηφιακή εποχή; Και πώς γίνεται να μπορούν να μας παρακολουθούν όλους μας κάθε στιγμή; Η παρακολούθηση δεν συμβαίνει πλέον με τον τρόπο που βλέπαμε στις παλιές ταινίες όπου κάποια υπηρεσία στέλνει 1-2 ανθρώπους να παρακολουθούν από κοντά όλες τις κινήσεις κάποιου γιατί απλά αυτό δεν είναι πλέον απαραίτητο. Μιας και ό,τι κάνουμε πλέον καταλήγει ή περνάει από κάποιο ψηφιακό μέσο, το μόνο που έχει να κάνει κάποιος είναι να συγκεντρώσει μαζικά και έπειτα να συνδυάσει όλες αυτές τις πληροφορίες. Παρακολούθηση είναι να ξέρεις ποιος μίλησε με ποιον και πότε, ποιος αντάλλαξε μήνυμα/email και με ποιον. Αν μπορείς να μάθεις και το περιεχόμενο των μηνυμάτων/συνομιλιών ακόμα καλύτερα...αλλα και τα metadata [1] από μόνα τους μιλάνε για μας. Ποια sites διαβάζει κανείς; Ποια βιβλία; Ποιοι είναι οι κωδικοί που χρησιμοποιεί κανείς και τι λένε αυτοί για τον ίδιο τον άνθρωπο; Ποιοι είναι οι φίλοι κάποιου; Ποιους και πότε τους συναντάει και πώς κανονίζονται οι συναντήσεις; Τι γράφει ο κάποιος στα social media, και τι λένε τα γραπτά του για τα πολιτικά του πιστεύω; Υπάρχει κάποιο μυστικό που κρύβει κανείς, είτε προσωπικό είτε επαγγελματικό; Ποια από αυτά τα στοιχεία αξίζει να αποθηκευτούν για το μέλλον;

Ακούγεται επιστημονική φαντασία, αλλά δεν είναι καθόλου, συμβαίνει εδώ και πάνω από 10 χρόνια. Όμως η συλλογή και ο συνδυασμός γίνεται όλο και πιο εύκολος γιατί έχει αλλάξει ο τρόπος που οι άνθρωποι επικοινωνούν. Όλο και μεγαλύτερο κομμάτι της επικοινωνίας μας είναι πλέον καθαρά ψηφιακό και μάλιστα χρησιμοποιούμε κάποιες λίγες, μεγάλες, εταιρείες κολοσσούς που μας προσφέρουν τα εργαλεία/υπηρεσίες τους τα οποία ισχυρίζονται πως "μας κάνουν την ζωή πιο εύκολη", και μάλιστα υποτίθεται το κάνουν και δωρεάν. Η δωρεάν αυτή χρήση των εργαλείων/υπηρεσιών έχει ένα βαρύ τίμημα, την αποποίηση της ιδιωτικότητάς μας και κατ' επέκταση της ελευθερίας μας, μέσω της δυνατότητας που δίνουμε σε αυτές τις εταιρίες να ξέρουν τα πάντα για μας και τους γύρω μας. Το πρόβλημα δυστυχώς είναι πως στην ψηφιακή επικοινωνία δεν υπάρχει εύκολος τρόπος να αντιληφθείς πως κάποιος σε παρακολουθεί, δεν θα δεις κάποιον τύπο με μάυρα γυαλιά, καπέλο και κάπα σε κάποια γωνία, οπότε με τον καιρό ξεχνιέσαι και σιγά σιγά απελευθερώνεις όλο και περισσότερες προσωπικές λεπτομέρειες σε emails, chat, social media, κτλ. Μιας και δεν βλέπεις κάποιον να σε παρακολουθεί ποτέ, δεν νοιώθεις τον κίνδυνο, αυτή όμως είναι μια τεράστια ψευδαίσθηση. Ο κίνδυνος να σε παρακολουθούν και να καταγράφουν το τι κάνεις βρίσκεται πλέον σε περισσότερα μέρη από όσα μπορείς να φανταστείς την ώρα που εσύ νομίζεις πως επικοινωνείς ανενόχλητος. Ο μόνος τρόπος να συγκριθεί η ψηφιακή παρακολού-

θηση με την παραδοσιακή είναι να υποθέσεις πως αυτός ο περίεργος τύπος όχι απλά είναι στην απέναντι γωνία, αλλά είναι συνέχεια ακριβώς πάνω από τον ώμο σου και βλέπει ό,τι κάνεις ακριβώς την στιγμή που το κάνεις.

Πώς πραγματικά γίνεται η επικοινωνία στο Internet, ποια και πόσα διαφορετικά μονοπάτια στο Internet περνάει ένα μήνυμα για να φτάσει στον παραλήπτη; Ποιοί ελέγχουν όλα αυτά τα μονοπάτια; Η απάντηση πολλές φορές είναι πως δεν μπορούμε να ξέρουμε. Γι αυτό και πρέπει να προστατεύουμε την επικοινωνία μας προκαταβολικά και πάντα. Και ο μόνος τρόπος να το κάνουμε αυτό είναι να εκπαιδευτούμε στην ορθή χρήση μερικών εργαλείων. Θέλει χρόνο και κόπο, αλλά πότε η ελευθερία ήταν κάτι το δεδομένο; Πότε οι άνθρωποι δεν χρειαζόταν να εκπαιδευτούν και να παλέψουν γι αυτή; Όλα τα εργαλεία που χρειαζόμαστε για να αποφύγουμε όσο μπορούμε την μαζική παρακολούθηση έχουν ένα κοινό παράγοντα, χρησιμοποιούν την καλή κρυπτογραφία σαν βάση τους. Καλή κρυπτογραφία είναι η δημόσια κρυπτογραφία, αυτή που ξέρουμε τον τρόπο με τον οποίο δουλεύει, αυτή που οι αλγόριθμοι που χρησιμοποιεί είναι ανοιχτοί ώστε να βασίζει την ασφάλειά της όχι σε μαγικά τρικ αλλά σε δύσκολα μαθηματικά προβλήματα, άλλωστε η κρυπτογραφία είναι τομέας των μαθηματικών. Αυτά τα εργαλεία είναι τα μόνο που μπορούν να προστατέψουν πλέον την ελευθερία μας. Δεν χρειάζεται φυσικά να μάθουμε όλοι ανώτερα μαθηματικά! Αρκεί να μάθουμε να χρησιμοποιούμε τα σωστά προγράμματα. Σκοπός δεν είναι να γίνουμε όλοι guru των υπολογιστών, σκοπός είναι να προστατευτούμε από τη φασιστική νοοτροπία της μαζικής παρακολούθησης η οποία φυσικά συμβαίνει..."για το καλό μας".

[1] https://mat.boum.org/

Προσοχή στο cloud!

Ο μεγαλύτερος κίνδυνος για την ιδιωτικότητα προέρχεται από την υπερσυγκέντρωση των δεδομένων στα χέρια λίγων εταιριών κολοσσών. Ιδανικά θα έπρεπε να ξαναγυρίσουμε στις απαρχές του Internet όπου η πληροφορία ήταν διασκορπισμένη και η κάθε ομάδα δημιουργούσε δικές της υπηρεσίες χρησιμοποιώντας δικούς της πόρους. Αυτό δεν είναι καθόλου εύκολο, αλλά δεν είναι και ακατόρθωτο. Όσο πιο κοντά σε εμάς είναι τα δεδομένα μας, τόσο μεγαλύτερο έλεγχο έχουμε σε αυτά και άρα λιγότερους κινδύνους. Αν χρειαζόμαστε μια εφαρμογή τύπου cloud, πχ για αποθήκευση και συγχρονισμό δεδομένων, είτε στήνουμε μια δική μας [1] είτε χρησιμοποιούμε κάποια που διαπιστωμένα κρυπτογραφούν και προστατεύουν τα δεδομένα μας [2].

[1] https://owncloud.org/
[2] https://spideroak.com/

Web Browsing

Το μεγαλύτερο κομμάτι των επικοινωνιών στο web γίνεται χωρίς καμία κρυπτογράφηση. Κρυπτογραφημένα, άρα προστατευμένα, είναι μόνο τα δεδομένα που ανταλλάσσονται όταν η πλοήγηση γίνεται σε sites που η διεύθυνση τους ξεκινάει με https:// αντί για http://. Επειδή όμως δεν υποστηρίζουν όλα τα sites https, και δεν μπορούμε να θυμόμαστε ποια το κάνουν, την δουλειά αυτή την αναλαμβάνει ένα plugin για Firefox και Chrome με το όνομα '''HTTPS Everywhere''' [1].Περισσότερα στο αντίστοιχο άρθρο στο skytal.es [2]. Σημείωση : ! (βλέπε παρακάτω)

Το ασφαλές browsing δεν εξισώνεται με το ανώνυμο browsing

[1] https://www.eff.org/https-everywhere
[2] https://skytal.es/wiki/Browsing
[3] https://www.riseup.net/en/chat-clients
[4] http://www.cypherpunks.ca/otr/
[5] https://jitsi.org/
[6] https://skytal.es/wiki/Chat

Chat

Δυστυχώς τα περισσότερα προγράμματα/υπηρεσίες που χρησιμοποιούνται δεν προσφέρουν καμία προστασία από ενδιάμεσους που μπορεί να παρακολουθούν τις συνομιλίες ή οι ίδιες οι εταιρίες έχουν πλέον ομολογήσει πως όταν τους ζητείται δίνουν μηνύματα των χρηστών τους στις όποιες αρχές. Γι' αυτό καλό είναι να αποφεύγουμε με κάθε τρόπο να χρησιμοποιούμε MSN, Yahoo!Chat, Skype, FacebookChat, Google chat/Hangouts. Προτιμούμε κάποιο προτόκολλο chat που βασίζεται στο XMPP/Jabber. Προτιμούμε chat servers που λειτουργούνται από ομάδες ακτιβιστών ([1],[2]). Χρησιμοποιούμε πάντα open source clients [3]. Την κρυπτογράφηση του περιεχομένου των συνομιλιών από άκρη σ'άκρη αναλαμβάνει το 'Off-The-Record (OTR) messaging''' [4]. Ανάγκες voice/video chat καλύπτει το open source πρόγραμμα jitsi [5]. Περισσότερα μπορείτε να διαβάσετε στο αναλυτικό άρθρο που υπάρχει στο skytal.es [6]

[1] https://web.jabber.ccc.de/
[2] https://www.riseup.net/en/chat
[3] https://www.riseup.net/en/chat-clients
[4] http://www.cypherpunks.ca/otr/
[5] https://jitsi.org/
[6] https://skytal.es/wiki/Chat

Email

Στην περίπτωση του email δεν γίνεται να κρυπτογραφηθεί το ποιος είναι ο αποστολέας και ποιος ο παραλήπτης ενός email, αυτό που μπορεί όμως να γίνει με την βοήθεια προγραμμάτων όπως το PGP/GPG είναι να κρυπτογραφηθεί το περιεχόμενο ενός email. Αρκεί κάποιος να κατεβάσει το Enigmail plugin του Thunderbird [1] για να ξεκινήσει. Αντίστοιχα plugins υπάρχουν και για πολλά άλλα open source email clients.
Αναλυτικά το πως γίνεται αυτό θα το διαβάσει κανείς στο παρακάτω link [2]. Είναι γνωστό πως οι μεγάλοι πάροχοι email υπηρεσιών συνεργάζονται με κυβερνήσεις και υπηρεσίες και δίνουν πρόσβαση στα δεδομένα των χρηστών γι αυτό καλό είναι να αποφεύγουμε όσο γίνεται να χρησιμοποιούμε τις υπηρεσίες email παρόχων όπως Google, Yahoo! και Microsoft και να στραφούμε σε προσπάθειες όπως το riseup [3] που το λειτουργούν ακτιβιστές και άνθρωποι με έντονο ενδιαφέρον για την ιδιωτικότητα.

[1] https://www.enigmail.net
[2] https://skytal.es/wiki/Email
[3] https://riseup.net

Είναι γνωστό πως οι μεγάλοι πάροχοι email υπηρεσιών συνεργάζονται με κυβερνήσεις και υπηρεσίες και δίνουν πρόσβαση στα δεδομένα των χρηστών

Ανωνυμία

Ασφάλεια και ανωνυμία είναι δύο διαφορετικά ζητήματα που όταν συνδυαστούν μας δίνουν μια αρκετά καλή λύση για να προστατέψουμε την ιδιωτικότητά μας. Ένα πρόγραμμα που μπορεί να μας βοηθήσει σε αυτό τον τομέα είναι το Tor [1], ενώ με την χρήση του Tor Browser Bundle έχουμε πλέον τη δυνατότητα για ασφαλή και ανώνυμη πλοήγηση στο Internet. Προσοχή όμως! Κανένα εργαλείο δεν μπορεί να μας προστατέψει από τα δικά μας λάθη που μπορεί να φανερώσουν την ταυτότητά μας, πχ login στο προσωπικό μας email, στο προσωπικό μας λογαριασμό στο Facebook, κτλ. Το εργαλείο αυτό μας βοηθάει να "κρυφτούμε" μέσα σε μια μάζα ανθρώπων με παρόμοια χαρακτηριστικά. Αν όμως οι κινήσεις μας, αυτά που γράφουμε, κτλ μας ξεχωρίζουν ως άτομα, τότε χρησιμοποιούμε το εργαλείο με λάθος τρόπο. Για όσους έχουν ακόμα μεγαλύτερες ανάγκες ανωνυμίας, πχ δημοσιογράφοι, δικηγόροι, ακτιβιστές, κτλ συνίσταται η χρήση πιο ανεπτυγμένων εργαλείων που χρησιμοποιούν το Tor όπως το Tails [2] και το whonix [3]. Περισσότερα για το θέμα στο skytal.es [4].

[1] https://torproject.org/
[2] https://tails.boum.org/
[3] https://www.whonix.org
[4] https://skytal.es/wiki/Anon