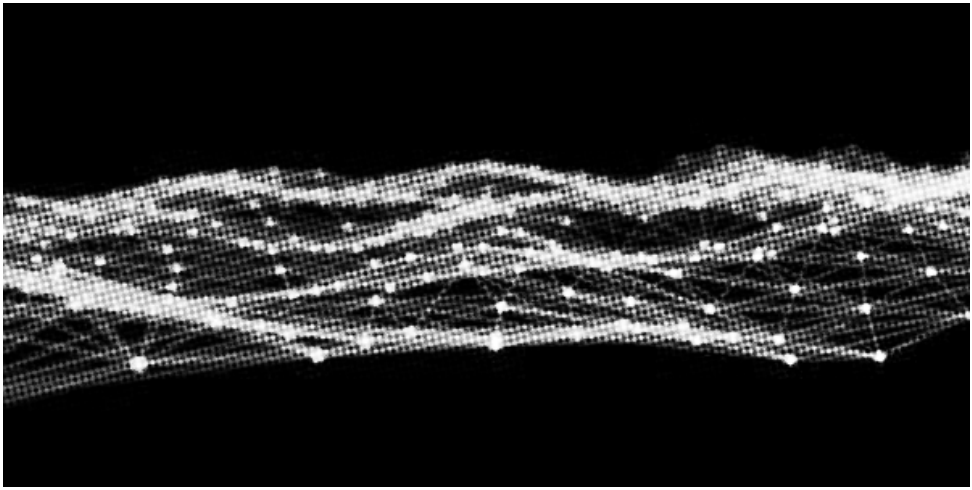
Παιρνοντας τις εαυτους
μας σοβαρα:

μειωση ψηφιακων κινδυνων



Related resource: Outrun the Bear: ProtonMail is Not for Activists (notrace.how/resources/el/#protonmail)

Παιρνοντας τις εαυτους μας σοβαρα: μειωση ψηφιακων κινδυνων

Original text in Greek

2020

web.archive.org/web/20210625013117/https://radiofragmata.org/2020/11/11/pairnontas-tis-eaytoys-mas-sovara

Layout

No Trace Project

notrace.how/resources/el/#meiose-psephiakon-kindunon

Contents

Εισαγωγή

Η Ελλάδα εισέρχεται σε μια νέα εποχή, στην οποία το FBI, το MI5 και άλλα πιο προηγμένα κράτη στον κόσμο, ενεργούν ως σύμβουλοι για την ελληνική καταστολή. Είναι ευθύνη οποιουδήποτε αφοσιωμένου επαναστάτη, εξεγερσιακού ή ενεργού αναρχικού να προσαρμοστεί και να αναπτυχθεί, σύμφωνα με αυτές τις εξελίξεις για την επιδίωξη της μακροχρόνιας πάλης, αλλά και την ευρύτερη διατήρηση της ατομικής και συλλογικής μας ασφάλειας.

Για πάρα πολύ καιρό, το οποιοδήποτε κίνημα στην Ελλάδα δεν έδινε την απαραίτητη σημασία στις απαιτήσεις για μια κουλτούρα ασφάλειας που θα λειτουργήσει ως μορφή αυτοάμυνας. Ανεξάρτητα από το πόσο επικίνδυνη είναι αυτή η στάση, αποτελεί επίσης ένα είδος υποκρισίας στην προσέγγισή μας. Περιμένουμε να γίνουν σεβαστά τα δικαιώματά μας; Παίρνουμε σοβαρά τον εαυτό μας; Η θέση του αναρχικού είναι εχθρική προς κάθε έθνος-κράτος, κάθε σύνορο και την παγκόσμια οικονομία. Επιλέγουμε την πιο αμφιλεγόμενη και επαναστατική απάντηση σε αυτήν την φρικτή κοινωνία. Στην επιλογή μας να λάβουμε θέση για την πραγματική απελευθέρωση, πρέπει να περιμένουμε πολιτική καταστολή χωρίς καμιά συμπόνια.

Μην έχοντας μια κουλτούρα ασφάλειας, βλάπτουμε τον εαυτό μας και τις κοινότητές μας, ενώ βοηθάμε τους εχθρούς μας. Δεν είναι απλώς θέμα χρήσης αυτής της εφαρμογής ή της άλλης. Υπάρχουν διάφορες διαδικασίες και προσεγγίσεις στην καθημερινή ζωή που πρέπει να λάβουμε υπόψη, προκειμένου να περιπλέξουμε τις προσπάθειες καταστολής από τους εχθρούς μας, να προστατεύσουμε τους εαυτούς μας και τις συντρόφισσές μας, ώστε να είμαστε επιτυχημένοι στα έργα και στις ενέργειές μας.

Αυτό το άρθρο είναι το πρώτο από μια σειρά άρθρων που σκοπεύουν να βοηθήσουν στη δημιουργία μιας ευρύτερης κουλτούρας ασφάλειας στον αναρχικό χώρο στην Ελλάδα. Σκοπεύει, επίσης, να αμφισβητήσει συγκεκριμένες συμπεριφορές που καθιστούν το χώρο μη ασφαλή.

Παρακάτω συμπεριλάβαμε κάποιες προτάσεις από έναν ανώνυμο σύντροφο σχετικά με μερικούς βασικούς καθημερινούς τρόπους για την καλύτερη προστασία του εαυτού μας. Είναι πεποίθησή μας πως σε

κάθε πρακτική, όταν κάποιος δεσμεύεται, αναπτύσσεται και γίνεται πιο ικανός στην πορεία. Επιπλέον, παραθέτουμε μετάφραση ενός κειμένου από έναν σύντροφο στις Η.Π.Α. σχετικά με τη «μείωση των κινδύνων» και τη σημασία της κρυπτογράφησης και των καλύτερων τεχνολογιών, ενόσω ζούμε στον σύγχρονο κόσμο.

Μερικές απλές προτάσεις για μια καθημερινή προσέγγιση στην «εξυπνότερη επικοινωνία» και το ψηφιακό αποτύπωμα

Είναι σημαντικό να προτείνουμε μερικές συνεπείς προσεγγίσεις που έγιναν από επαναστάτες. Πρώτον, μην συζητάτε ποτέ κάτι τυπικά παράνομο μέσω τηλεφώνου. Είναι αλήθεια ότι ορισμένες εφαρμογές και η τεχνολογία κρυπτογράφησης προστατεύουν την επικοινωνία σας από την επιτήρηση του κράτους, ωστόσο τίποτα δεν είναι σίγουρο και πρέπει να διατηρήσουμε μια ψύχραιμη ανησυχία επί τούτου. Αυτό ισχύει και για τον παλιό τρόπο τηλε-επικοινωνίας!

Δεν είναι ποτέ απαραίτητες οι συζητήσεις που συγκαταλέγονται στο έγκλημα ή σε ρητά παράνομες ενέργειες στο τηλέφωνο. Να είστε δημιουργικές στην επικοινωνία σας και προσεγγίστε κάθε συνομιλία που γράφετε ή στέλνετε στο τηλέφωνό σας ρωτώντας τον εαυτό σας, εάν αυτό θα μπορούσε να σταθεί εναντίον σας στο δικαστήριο.

Μην παίρνετε μαζί τα τηλέφωνά σας σε δράσεις. Εάν είναι απαραίτητη η επικοινωνία, μπορείτε να αναζητήσετε τα λεγόμενα τηλέφωνα «burner», αν και καλό θα ήταν να το αποφύγετε με κάθε κόστος. Εάν υπάρχει πιθανότητα σύλληψης, το τηλέφωνό σας μπορεί να είναι το μεγαλύτερο καρφί στο δωμάτιο.

Να είστε προσεκτικοί με τα μέσα κοινωνικής δικτύωσης. Εάν η ταυτότητά σας είναι εκτεθειμένη, ακόμη και με ψευδές όνομα, ένας ενδιαφερόμενος εχθρός θα μπορούσε να βρει κίνητρο να το διερευνήσει, εάν δημοσιεύετε μαχητικές πολιτικές θέσεις και ούτω καθεξής. Προσοχή σε αυτό και μην υποθέσετε ποτέ ότι έχετε «ελευθερία λόγου»· βασικά, έχετε μέχρι το κράτος να αποφασίσει πως δεν έχετε. Επιπλέον, η χρήση

των κοινωνικών δικτύων, όπως το messenger του facebook ως πηγή των συνομιλιών σας, ενώ παράλληλα δημοσιεύετε πολιτικές ιδέες που μπορεί η πολιτεία να κρίνει αμφιλεγόμενες, παρουσιάζει ουσιαστικά ένα ολοκληρωμένο χαρτοφυλάκιο πληροφοριών για έναν αστυνομικό ερευνητή. Η πολιτική σας θέση σχετίζεται με τα λόγια σας, και αυτοί με τους οποίους επικοινωνείτε με την πολιτική σας θέση, οι οποίοι μπορούν εξίσου να επισημανθούν ως πρόσωπα ενδιαφέροντος. Πρέπει να σκεφτούμε να μεταφέρουμε όλη την επικοινωνία μας σε πιο ασφαλείς πλατφόρμες, όπως το Signal. Σε πολιτικό ή όχι επίπεδο, το κράτος έχει ατελείωτη χρηματοδότηση για την καταστολή των πολιτικών του αντιπάλων και μια συνεπής προσέγγιση ασφαλούς επικοινωνίας καθ 'όλη τη διάρκεια της ζωής μας, περιπλέκει τις προσπάθειές του. Δεν είναι μόνο οι παράνομες ενέργειες που ενδιαφέρουν το κράτος, είναι κι οι σύντροφοί μας, τα δίκτυά μας και οι ευρύτερες κοινότητές μας.

Εξετάστε το ενδεχόμενο να διαχωρίσετε τους λογαριασμούς ηλεκτρονικού ταχυδρομείου (email), τους λογαριασμούς στα κοινωνικά δίκτυα και τις μεθόδους επικοινωνίας. Προσπαθήστε να έχετε ξεχωριστά email για την εργασία και τις πολιτικές σας δραστηριότητες. Προσπαθήστε να έχετε ξεχωριστούς λογαριασμούς ανάλογα με το πού είναι απαραίτητο να έχετε νομική υπόσταση/ταυτότητα και πού δεν είναι. Εφαρμόστε το επίσης, στα κοινωνικά δίκτυα. Εφαρμόστε το ακόμη και στην περίπτωση του αριθμού τηλεφώνου σας. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε ανώνυμες κάρτες sim για να ενεργοποιήσετε έναν λογαριασμό Signal ή έναν νέο προσωρινό αριθμό τηλεφώνου. Μπορείτε ακόμη να «υπερβάλλετε» κάπως, και να αλλάζετε το όνομά σας (στο λογαριασμό) για ορισμένες συναντήσεις ή όταν επισκέπτεστε την οικογένειά σας. Όλες αυτές οι προσπάθειες, ενώ θεωρούνται τρελές από κάποιους, περιπλέκουν την καταστολή και την επιτήρηση του κράτους.

Βεβαιωθείτε ότι διαγράφετε τα cookies και τα δεδομένα στις συσκευές σας, όταν είναι δυνατόν. Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε διακομιστές vpn, όπως το protonvpn, κατά την έρευνα πληροφοριών ή τη δημοσίευση πολιτικού περιεχομένου.

Δεν υπάρχει σίγουρη διαδρομή για την τέλεια ασφάλεια, ούτε ξέρουμε πότε θα έρθει το κράτος να χτυπήσει τις πόρτες μας και για ποιο λόγο θα επιλέξουν να το κάνουν. Αλλά αν προκαλέσουμε τους εαυτούς μας, και ο

ένας τον άλλον για να διατηρήσουμε ένα αξιοπρεπές επίπεδο ασφάλειας ενάντια στο κράτος, θα προσαρμόζουμε και θα αναπτύσσουμε συνεχώς μια κατεύθυνση σταθερής αυτοάμυνας στην ατελείωτη επίθεση από το κράτος. Αυτή η συμβουλή δεν είναι μόνο για τον επαναστάτη/αντάρτη ή τον φυγά, είναι για όλους, και είναι πολύ απλό να εξασκηθείτε και να το διατηρήσετε σε οποιαδήποτε στιγμή της ζωής σας ή διαχρονικά. Στις Η.Π.Α. εκδότες και συγγραφείς έχουν αντιμετωπίσει ποινές φυλάκισης· στην Ισπανία η ίδια η αναρχική ταυτότητα έχει ποινικοποιηθεί κι υπό το φως της πρόσφατης ετυμηγορίας για τη Χρυσή Αυγή στην Ελλάδα, το καθεστώς της Νέας Δημοκρατίας είναι πιθανό να εφαρμόσει νέα μέτρα για την ποινικοποίηση των αναρχικών, ισχυριζόμενο απλά ότι είναι δίκαιο («θεωρία δύο άκρων»).

Καθώς ποινικοποιούν τις συγκεντρώσεις, για παράδειγμα, ας φανταστούμε την πορεία αυτής της δικαστικής οδού. Τι ακολουθεί; Ίσως έρευνες για «συνωμοσίες» περί συγκεντρώσεων. Αποδίδοντας κατηγορίες εγκληματικού περιεχομένου σε εκείνους που κατηγορούνται για διοργάνωση εκδηλώσεων, όπου συνέβησαν επεισόδια, με μοναδικό κριτήριο μια έκκληση/εκδήλωση στο facebook ή το twitter. Αυτές οι περιπτώσεις δίωξης είναι πραγματικότητα στις ΗΠΑ και ορισμένα άτομα έχουν κάνει πολλά χρόνια στη φυλακή ως αποτέλεσμα αυτής. Αυτού του τύπου οι μικρές πρακτικές μπορούν να αποτρέψουν την επιτυχία του κράτους στην επιδίωξη τέτοιων στόχων/κατηγοριών.

Αυτή είναι μια μακροπρόθεσμη δέσμευση για να ζούμε με έναν πιο ασφαλή τρόπο πολιτικής ζωής. Αλλά δε θα έπρεπε να το προσεγγίσουμε ως «όλα ή τίποτα». Είναι ενοχλητικό, άβολο κι ίσως μερικές φορές φαίνεται περιττό· έως ότου δεν είναι.

Ένα επιχείρημα για τη μείωση του ψηφιακού κινδύνου στο χώρο

Ένα «φάντασμα» στοιχειώνει τις υπηρεσίες πληροφοριών του κόσμου, το φάντασμα του «σκοτεινού διαδικτύου» (dark web). Πρόκειται για μια έννοια που μεταφράζεται συχνά ως σενάριο τελικής κρίσεως για το εγγύς μέλλον, όπου οι έρευνες δεν είναι πλέον δυνατές και οι εγκληματίες διαφεύγουν από όλα τα εγκλήματά τους, επειδή η κρυπτογράφηση έχει

γίνει τόσο πανταχού παρούσα που δεν μπορούν να ληφθούν αναγνώσιμα δεδομένα από την επιβολή του νόμου, είτε νόμιμα είτε παράνομα· απλά δεν έχουν πια αυτή τη δυνατότητα.

Αυτό ξεκίνησε σε μεγάλο βαθμό ως μια απειλή που προορίστηκε να τρομάξει τους συντηρητικούς Αμερικάνους, αλλά ενέχει αλήθεια· δεν θα έλεγαν αυτό το παραμύθι και παράλληλα θα πολεμούσαν την κρυπτογράφηση τόσο σκληρά, αν δεν ήταν πραγματική απειλή για αυτούς. Ποικιλοτρόπως ζούμε σε ενδιαφέρουσες εποχές. Μια έκφραση αυτού είναι η χαμηλού επιπέδου σύγκρουση σχετικά με την ιδιωτικότητα μεταξύ του τεχνολογικού κόσμου και των αρχών επιβολής του νόμου. Θα έπρεπε να είναι φυσικοί σύμμαχοι και είναι με πολλούς άλλους τρόπους, αλλά στο ζήτημα της κρυπτογράφησης δεν θα μπορούσαν να διαφωνούν περισσότερο. Όλοι οι εμπειρογνώμονες ασφαλείας (συμπεριλαμβανομένων εκείνων εντός των κυβερνήσεων) συμφωνούν πως η κρυπτογράφηση είναι αποτελεσματική μόνο εάν είναι συνολική. Δεν μπορεί να υπάρχει μυστικό «backdoors», ούτε ειδικοί κωδικοί πρόσβασης που επιτρέπουν στους μπάτσους να εισέλθουν με ένταλμα. Αυτό θα υπονόμευε ολόκληρο το μοντέλο ασφαλείας. Υπάρχει συναίνεση στο γεγονός ότι αυτή «η ειδική πόρτα» θα μπορούσε να αποκαλυφθεί σε λάθος πλευρές (εγκληματίες, εχθρικές κυβερνήσεις κ.λπ.) και έτσι έχει δημιουργηθεί μια αντίφαση: προκειμένου να λειτουργήσει η κρυπτογράφηση για όλους, συμπεριλαμβανομένων των κρατικών φορέων, πρέπει η παρακολούθηση από τους ίδιους να γίνει πιο δύσκολη ή σε ορισμένες περιπτώσεις σχεδόν αδύνατη.

Η κρυπτογράφηση υπάρχει με διάφορες μορφές εδώ και χρόνια. Η τεχνολογία που επιτρέπει κρυπτογραφημένες τηλεφωνικές κλήσεις υπάρχει τουλάχιστον από τη δεκαετία του '80. Αλλά αυτά τα συστήματα ήταν ακριβά, περίπλοκα και στην πραγματικότητα λιγότερο ασφαλή από τις δωρεάν λύσεις που έχουμε σήμερα. Κόστιζαν χιλιάδες δολάρια για την εγκατάσταση και θα μπορούσες να επικοινωνήσεις μόνο με άλλα μέρη που έχουν επενδύσει επίσης στη δική τους εγκατάσταση. Προφανώς, το χρησιμοποιούσαν μόνο εκείνοι στα ανώτερα κλιμάκια της εξουσίας: διευθύνοντες σύμβουλοι μεγάλων εταιρειών και υψηλόβαθμοι πολιτικοί. Αλλά τότε ήρθε το Διαδίκτυο κι ακολούθησαν οι ευπρόσιτοι υπολογιστές και τα «έξυπνα κινητά τηλέφωνα» (smartphones). Κι ενώ

αυτή η συμβολή τεχνολογιών έχει εξαπολύσει πολλές φρίκες στον κόσμο κι έχει διευκολύνει το κράτος να παρακολουθεί τα κινήματά μας, έχει ενεργοποιήσει επίσης αντιφάσεις, όπως είναι η προσβάσιμη και εύχρηστη στρατιωτικού-προτύπου κρυπτογράφηση σε μαζική κλίμακα. Η σύγχρονη εποχή του διαδικτύου δημιούργησε μαζική παρακολούθηση, όπως ποτέ άλλοτε δεν γνώριζε ο κόσμος, αλλά επίσης έδωσε ένα φόρουμ για διάφορες επικοινωνίες εις βάρος των κρατικών συμφερόντων.

Βλέπουμε όλο και περισσότερο έρευνες να παρεμποδίζονται από την κρυπτογράφηση, αλλά το πιο σημαντικό και πιο αποτελεσματικό που βλέπουμε, είναι ότι παρεμποδίζεται η μαζική επιτήρηση. Κάτι που καθιστά πιο δύσκολο το να προσδιοριστεί ποιος ενάντια σε ποιον θα κάνει εντατικότερη στοχευμένη παρακολούθηση. Αυτή είναι η μεγαλύτερη δύναμη της μαζικής κρυπτογράφησης, κρύβοντας τους «κακούς παίχτες» μέσα στο μεγαλύτερο πλήθος, καθιστώντας το πρώτο βήμα των ερευνών πιο δύσκολο κι αυτό που χρήζει εντατικής προσπάθειας. Υπάρχουν ορισμένα πράγματα που μακροπρόθεσμα μπορεί να εξαφανιστούν ή θα πρέπει να αναδιαμορφωθούν πλήρως, όπως ο κοριός ή η επιδρομή της αστυνομίας και η κατάσχεση ενοχοποιητικών αποδεικτικών στοιχείων. Καθώς το μεγαλύτερο μέρος της ζωής μας κινείται στο διαδίκτυο και στις συσκευές μας, οι επιλογές που κάνουμε σχετικά με τον τρόπο χρήσης αυτών των συσκευών έχουν τεράστιο αντίκτυπο στην ικανότητα του εχθρού να μας καταπιέσει.

Μην πιστεύετε την προπαγάνδα του εχθρού ότι η κρυπτογράφηση είναι άσκοπη και «σπασμένη», πώς το κράτος είναι πάντα πιο ισχυρό από την ικανότητά μας να προστατεύουμε τον εαυτό μας από αυτό, πως πρέπει απλά να παραμένουμε απλοί παρατηρητές. Σε σχέση με αυτό το ζήτημα, τρέχουν φοβισμένοι και δεν ξέρουν τι να κάνουν, οπότε χρησιμοποιούν σε μεγάλο βαθμό την παραπληροφόρηση εξυπηρετώντας έτσι την υπερεκτίμηση των ικανοτήτων τους. Ορισμένες εταιρείες το αναγνωρίζουν αυτό, βλέπουν την οικονομική ευκαιρία και αυτά είναι όλα όσα συμβαίνουν, όταν βλέπετε άλλο ένα άρθρο σχετικά με μια κυβέρνηση που πληρώνει εκατομμύρια για νέο εξοπλισμό παρακολούθησης διαδικτύου. Βλέπετε φοβισμένους ανόητους να κατασπαταλούν χρήματα σε κοράκια της βιομηχανίας ασφάλειας.

Βεβαίως, έχουν μερικούς άσσους στο μανίκι τους. Ναι, οι λύσεις που περιγράφουμε γενικά δεν είναι τέλειες, υπάρχουν ψεγάδια. Και δεν υποστηρίζουμε ούτε λέμε ότι η τελειότητα είναι δυνατή. Θα ήταν καλύτερο, από άποψη ασφάλειας, εάν δεν χρησιμοποιούσαμε καμία από αυτές τις τεχνολογίες και ζούσαμε εκτός δικτύου. Αλλά αυτό δεν ισχύει ή είναι δύσκολο για τους περισσότερους από εμάς. Ζούμε στον σύγχρονο κόσμο και πρέπει να χρησιμοποιήσουμε αυτές τις συσκευές για να επιβιώσουμε. Αυτό που υποστηρίζουμε είναι «η μείωση των κινδύνων» (harm reduction). Ο όρος αυτός χρησιμοποιείται συχνά για να περιγράψει ασφαλέστερους τρόπους χρήσης ναρκωτικών και σεξουαλικών πρακτικών: καθαρές βελόνες και προφυλακτικά. Σίγουρα, «σύμφωνα με το γιατρό», θα ήταν καλύτερα να μην κάνετε ναρκωτικά και αν δεν έχετε κάνει ποτέ σεξ, δεν θα κολλούσατε ένα σεξουαλικώς μεταδιδόμενο νόσημα. Αλλά αν πρόκειται να κάνετε «αυτά τα πράγματα» ούτως ή άλλως, θα πρέπει να μειώσετε τους κινδύνους αλλάζοντας μερικές πρακτικές.

Η μείωση των ψηφιακών κινδύνων είναι αυτό που χρειαζόμαστε. Μερικές απλές πρακτικές μπορούν να έχουν μεγάλο αντίκτυπο. Για παράδειγμα:

1. Χρήση του Signal για κλήσεις και μηνύματα κειμένου αντί για… οτιδήποτε άλλο (κανονικές κλήσεις, κανονικά SMS, Viber, WhatsApp). Το Signal είναι η ασφαλέστερη κι ευκολότερη σε χρήση, διαθέσιμη, κρυπτογραφημένη εφαρμογή επικοινωνίας και δημιουργήθηκε από αναρχικούς.
2. Κρυπτογραφήστε τον υπολογιστή σας με έναν καλό κωδικό πρόσβασης.
3. Κρυπτογραφήστε το τηλέφωνό σας με ένα καλό κωδικό πρόσβασης.
4. Χρησιμοποιήστε ένα δωρεάν κρυπτογραφημένο e-mail, όπως το protonmail, για… τα πάντα.
5. Μην συγχρονίζετε τίποτα στο cloud ή μην δημιουργείτε αντίγραφα ασφαλείας οποιουδήποτε άλλου, χρησιμοποιώντας την online υπηρεσία δημιουργίας αντιγράφων ασφαλείας του τηλεφώνου σας. Συνήθως, αυτό που δημιουργείται δεν είναι κρυπτογραφημένο, ακόμα κι αν το τηλέφωνό σας είναι. Μπορείτε με ασφάλεια να

δημιουργήσετε αντίγραφα ασφαλείας του τηλεφώνου σας με μη αυτόματο τρόπο (χειροκίνητα) στον κρυπτογραφημένο υπολογιστή σας. Είναι εύκολο να το κάνετε, ακόμα κι αν είναι θέλει λίγο παραπάνω κόπο.

Ποιος είναι ένας καλός κωδικός πρόσβασης; Μια σειρά λέξεων που επιλέγονται τυχαία και είναι εύκολο να τον θυμάστε, μα δύσκολο να τον μαντέψει κανείς (βάλτε φαντασία και λίγη τρέλα!).

Παραδείγματα καλών κωδικών πρόσβασης:

- orderly likely english distance melody
- column maryland possible burning happened weight

Μπορείτε να τοποθετήσετε τα κενά στον κωδικό πρόσβασης. Τα κενά είναι «ελεύθερα», καθώς προσθέτουν επιπλέον μήκος χωρίς να είναι πιο δύσκολο να θυμηθείτε. Το μήκος είναι πιο σημαντικό από την πολυπλοκότητα, επομένως αυτά τα παραδείγματα κωδικών πρόσβασης είναι πολύ πιο ασφαλή από το «ifgiityj993», παραδείγματος χάρη. Κατά την επιλογή αυτών των λέξεων, μπορείτε να χρησιμοποιήσετε μια τυχαία γεννήτρια λέξεων ή να ανατρέξετε σε τυχαίες σελίδες σε ένα λεξικό. Μην χρησιμοποιείτε τον εγκέφαλό σας. Δεν είναι τυχαίο. Ο εγκέφαλός σας θα σας πει να κοιτάξετε γύρω στο δωμάτιο ή έξω από το παράθυρο και να επιλέξετε ένα κάθε άλλο παρά τυχαίο κωδικό πρόσβασης, όπως «καρέκλα γραφείο παράθυρο σύννεφο».

Απενεργοποιήστε τις συσκευές σας, όταν είναι δυνατόν. Εάν η συσκευή σας είναι κρυπτογραφημένη με έναν καλό κωδικό πρόσβασης και απενεργοποιημένη, είστε πολύ προστατευμένοι. Εάν η συσκευή είναι ενεργοποιημένη, υπάρχουν περισσότερες πιθανότητες πρόσβασης σε αυτήν. Προσπαθήστε να κάνετε συνήθεια να απενεργοποιείτε τελείως τον υπολογιστή σας (να μην είναι απλά κλειδωμένος ή σε αδράνεια), όταν φεύγετε από το σπίτι ή όταν κοιμάστε. Εάν η συσκευή σας είναι κρυπτογραφημένη με ένα καλό κωδικό πρόσβασης και πιστεύετε ότι ενδέχεται να κατασχεθεί πολύ σύντομα, προσπαθήστε να την απενεργοποιήσετε εντελώς. Αυτό θα αυξήσει σημαντικά την προστασία των δεδομένων σας. Επαναλαμβάνουμε, όμως, εάν η συσκευή σας δεν είναι κρυπτογραφημένη, αυτό δεν θα σας βοηθήσει, τίποτα δεν θα βοηθήσει.

Ως προειδοποιητικό/διδακτικό παραμύθι, μπορούμε να δούμε την ιστορία του μαύρου μπλοκ που ήταν πολιορκημένο για πολλές ώρες στην Ουάσινγκτον κατά τη διάρκεια της εκδήλωσης έναρξης της θητείας του Ντόναλντ Τραμπ πριν από αρκετά χρόνια στις Η.Π.Α. Πάνω από εκατό άνθρωποι στέκονταν έξω για ώρες, παγιδευμένοι όλοι μαζί από την αστυνομία, ουσιαστικά περιμένοντας να συλληφθούν. Κατά τη διάρκεια αυτών των πολλών ωρών, οι άνθρωποι χρησιμοποίησαν τα τηλέφωνά τους για να μιλήσουν με φίλους και να δημοσιεύσουν στο twitter και έτσι για λίγο υπήρχε μια ζωντανή συνομιλία και μια σειρά ενημερώσεων που έβγαιναν από αυτήν την παγιδευμένη ομάδα στο διαδίκτυο. Κατά τη διάρκεια όλης αυτής της ώρας, κανείς στην ομάδα δεν φάνηκε να έχει την αίσθηση ή τη γνώση να πει στους άλλους να κρυπτογραφήσουν το τηλέφωνό τους με έναν καλό κωδικό πρόσβασης, εάν δεν το είχαν ήδη κάνει. Επιπλέον, κανένας από τους χιλιάδες ανθρώπους που παρακολουθούσαν αυτήν την κατάσταση δεν σκέφτηκε να το κάνει. Αναφορές από το πεδίο, έδειξαν ότι οι μικρές συμβουλές που μοιράστηκαν μεταξύ τους ήταν εντελώς άχρηστες· έτσι, σε άτομα που είχαν μη κρυπτογραφημένα τηλέφωνα, απλώς με «μοτίβα ξεκλειδώματος οθόνης» (τα οποία είναι άχρηστα ενάντια στην αστυνομία) ζητήθηκε να απενεργοποιήσουν τα τηλέφωνά τους, πριν συλληφθούν, για να «καθαρίσουν τη μνήμη» πίσω από το μοτίβο ξεκλειδώματος που υποτίθεται (λανθασμένα) θα έδινε μεγαλύτερη ασφάλεια. Τελικά, τουλάχιστον οι μισοί από τους παρευρισκόμενους είδαν την αστυνομία να αποκτά πρόσβαση στα τηλέφωνά τους και να έχουν εκτεθεί ευαίσθητα μηνύματα και επαφές τους. Συγκεκριμένα, η μεγαλύτερη ομοιότητα μεταξύ των περισσότερων τηλεφώνων που δεν χακαρίστηκαν επιτυχώς ήταν τα iPhone. Το σύστημα ενός iPhone είναι κρυπτογραφημένο από προεπιλογή, οπότε όταν ρυθμίζετε το τηλέφωνό σας, σάς αναγκάζει να επιλέξετε έναν κωδικό πρόσβασης ανεξάρτητα από το πόσο χάλια μπορεί να είναι αυτός και στη συνέχεια χρησιμοποιεί αυτόν τον κωδικό πρόσβασης για την κρυπτογράφηση του τηλεφώνου. Στα Android, τουλάχιστον εκείνη την εποχή, δεν υπήρχε κρυπτογράφηση από προεπιλογή και έπρεπε να το κάνει κανείς από τις ρυθμίσεις. Έτσι, σε αυτό το σημείο, η Apple ήταν στην πραγματικότητα «ο μεγαλύτερος σύμμαχος» αυτών των συντρόφων από οποιονδήποτε άλλο. Δεδομένου του πόσο κακές ήταν οι γνώσεις/πρακτικές ασφάλειας

σε αυτό το πλήθος, είναι σχεδόν βέβαιο ότι οι χρήστες του iPhone είχαν πολύ αδύναμους κωδικούς πρόσβασης, πιθανότατα έναν τετραψήφιο αριθμό στις περισσότερες περιπτώσεις. Και όμως, σε αυτήν την περίπτωση αυτό ήταν υπεραρκετό για να κρατήσει εκτός τους μπάτσους, οι οποίοι έκαναν επίσης τόσο κακή δουλειά προσπαθώντας «να σπάσουν» αυτά τα τηλέφωνα.

Μέρος αυτής της αφέλειας της παραπάνω ομάδας ατόμων, μπορεί να αποδοθεί στο νεαρό της ηλικίας και την απειρία της. Ωστόσο υπήρχαν επίσης αναρχικοί σύντροφοι με παρουσία άνω των 15 ετών, που δεν ενήργησαν καλύτερα. Για την περίπτωση των χιλιάδων υποστηρικτών που δεν κατάφεραν να δώσουν χρήσιμες συμβουλές, στην πραγματικότητα δεν υπάρχουν δικαιολογίες και είμαστε όλοι υπεύθυνοι ως κίνημα, για την μη αρκετά καλή κουλτούρα μας σε πρακτικό επίπεδο σχετικά με την ψηφιακή ασφάλεια.

Άρα, ας μην πέσουμε στις ίδιες παγίδες με άλλους συντρόφους κι ας κάνουμε πράξη αυτές τις απλές πρακτικές που μπορούν να μειώσουν σε μεγάλο βαθμό τους κινδύνους για το χώρο μας. Ναι, υπάρχουν πολλά περισσότερα που μπορούν να γίνουν και αυτό δεν είναι ένας διεξοδικός οδηγός για να ζήσεις σαν τον Edward Snowden. Μπορείτε πάντα να κάνετε περισσότερα· ο ρεαλιστικός στόχος δεν μπορεί να είναι κάθε συντρόφισσα να έχει την εξειδίκευση ενός χάκερ υπολογιστών, αλλά να προσπαθήσουμε όλοι να συναντηθούμε σε ένα ελάχιστο στάνταρ που μπορεί να μας βοηθήσει συνολικά.

Αυτό το άρθρο είναι το πρώτο από μια σειρά άρθρων που σκοπεύουν να βοηθήσουν στη δημιουργία μιας ευρύτερης κουλτούρας ασφάλειας στον αναρχικό χώρο στην Ελλάδα. Σκοπεύει, επίσης, να αμφισβητήσει συγκεκριμένες συμπεριφορές που καθιστούν το χώρο μη ασφαλή.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.

Depending on your context, possession of certain documents may be criminalized or attract unwanted attention. Be careful about what zines you print and where you store them.