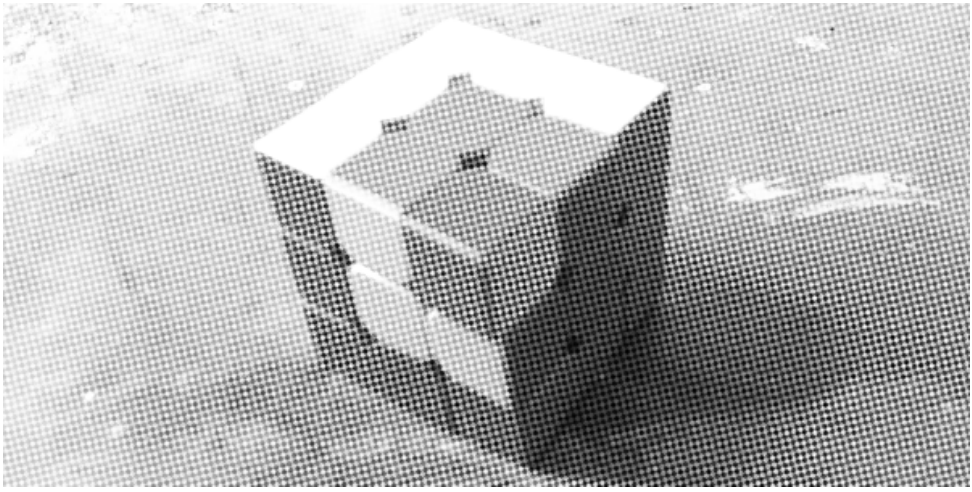
Briarthorn

Οδηγός επιχειρησιακής ασφάλειας



Briarthorn: Οδηγός επιχειρησιακής ασφάλειας

Original text in English
The Briarthorn OpSec Guide
Anonymous
2025

Greek translation
athens.indymedia.org/post/1637598

Layout
No Trace Project
notrace.how/resources/el/#briarthorn

Contents

Σημείωση Μετάφρασης: Το «Briarthorn» είναι ένας αγκαθωτός θάμνος. Συμβολίζει την ανθεκτικότητα, καθώς ανθίζει παρά τις αντιξοότητες και αναπτύσσεται στα πιο δύσκολα σημεία.

Εισαγωγή

Απαιτείται αρκετή δουλειά για να αντιληφθείτε πώς να μην σας συλλάβουν και πώς να ελαχιστοποιήσετε τη ζημιά αν τελικά συλληφθείτε. Για να προσπαθήσουμε να διευκολύνουμε τα συντρόφια μας, θέλουμε να μοιραστούμε τις τεχνικές που αναπτύξαμε λειτουργώντας μια παράνομη ακτιβιστική οργάνωση. Αυτός είναι ένας οδηγός για μη ειδικούς, αλλά σε κάποιες μεθόδους θα βοηθούσε να είστε λίγο τεχνολογικά καταρτισμένες ή τουλάχιστον να συνεργαστείτε με κάποιους τεχνολογικά καταρτισμένους φίλους.

Προειδοποιήσεις

ΜΗΝ ΜΑΣ ΕΜΠΙΣΤΕΥΕΣΤΕ ΠΑΡΑ ΠΟΛΥ. Έχουμε σκεφτεί πολύ σοβαρά το θέμα και δεν μας έχουν πιάσει ακόμα, αλλά είναι πάντα πιθανό να είμαστε απλά τυχεροί. Όπου είναι δυνατόν, κάντε τη δική σας έρευνα και σκεφτείτε το μόνα σας. Αυτές οι πρακτικές αποτελούν σημεία αφετηρίας για να προχωρήσετε, νοουμένου ότι είναι ένα καλύτερο σημείο εκκίνησης από τους συνήθεις ανασφαλείς τρόπους με τους οποίους γίνονται τα πράγματα. Προσπαθήσαμε να το κάνουμε όσο πιο δύσκολο να μας εμπιστευτείτε τυφλά, σημειώνοντας ρητά πότε υπάρχει κάτι που δεν γνωρίζουμε.

ΑΥΤΕΣ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ ΘΑ ΞΕΠΕΡΑΣΤΟΥΝ. Το γράφουμε αυτό το 2025. Όσο πιο μετά διαβαστεί αυτό το κείμενο, τόσο πιο πιθανό κάποιες λεπτομέρειες να μην είναι πλέον αληθινές.

ΟΙ ΕΚΤΙΜΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΤΙ ΜΠΟΡΕΙ Ή ΘΑ ΚΑΝΕΙ Η ΑΣΤΥΝΟΜΙΑ ΕΙΝΑΙ ΣΧΕΤΙΚΕΣ ΜΕ ΤΟ ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ, επειδή εκεί δραστηριοποιούμαστε.

Και ίσως το πιο σημαντικό, ΜΗΝ ΑΦΗΣΕΤΕ ΤΗΝ ΑΝΗΣΥΧΙΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΝΑ ΣΑΣ ΣΤΑΜΑΤΗΣΕΙ ΑΠΟ ΤΟ ΝΑ ΚΑΝΕΤΕ ΚΑΤΙ! Αν γίνεστε παρανοϊκά και δεν κάνετε κάτι επειδή είναι πολύ δύσκολο να το κάνετε με απόλυτη ασφάλεια, το κράτος επιτήρησης κερδίζει. Κάντε τα πράγματα με αρκετή ασφάλεια για το επίπεδο του κινδύνου που ενέχουν, και πάντα εκμεταλλευτείτε *εύκολες* ευκαιρίες για να κάνετε τα πράγματα πιο ασφαλή, αλλά αν ξοδέψετε μέρες για να οργανώσετε τα

πράγματα με απόλυτη ασφάλεια μόνο και μόνο για να κάνετε κάποιο γκράφιτι ή κάτι τέτοιο, τότε έχουν κερδίσει λόγω του ότι σταμάτησαν οτιδήποτε άλλο θα μπορούσατε να κάνετε με όλη αυτή την προσπάθεια.

Γενικές αρχές

Υπάρχουν δύο θεμελιώδεις αρχές που πρέπει να έχετε κατά νου σε όλα αυτά.

Μοντέλο απειλών

Για να ξέρετε τι πρέπει να κάνετε ώστε να είστε ασφαλείς, πρέπει να γνωρίζετε ποιοι είναι οι πιθανοί κίνδυνοι. Ένα μοντέλο απειλής είναι μια ιδέα για το ποιος προσπαθεί να σας σταματήσει και τι μπορεί να κάνει, και αν ασχολείστε με την επιχειρησιακή ασφάλεια, τότε πρέπει να έχετε ένα τέτοιο μοντέλο. Οι πρακτικές σε αυτό το κείμενο έχουν γραφτεί με την υπόθεση ότι έχετε να αντιμετωπίσετε κυρίως την αστυνομία του Ηνωμένου Βασιλείου και ότι δεν είναι διατεθειμένη να επενδύσει περισσότερους πόρους για να σας σταματήσει από ό,τι οποιαδήποτε τυχαία παράνομη ομάδα ακτιβιστών χαμηλού έως μεσαίου επιπέδου (δηλαδή δεν κάνετε τρομοκρατία ή κάτι τέτοιο). Υποθέτει επίσης ότι δεν κάνετε κάτι πολύ δημόσιο, ότι οι περισσότερες από τις δράσεις σας δεν θα αναφερθούν ποτέ στην αστυνομία. Αν κάνετε προπαγανδιστικά πράγματα που τραβάνε τα πρωτοσέλιδα, τότε μπορεί να αντιμετωπίσετε διαφορετικό επίπεδο απειλής, για παράδειγμα δεν χρειάζεται να κρατήσετε μυστική την ύπαρξη της ομάδας, αλλά μπορεί να ανησυχείτε περισσότερο για τυχόν διεισδύσεις στο εσωτερικό της. Ο λόγος για τον οποίο επιλέξαμε αυτό το μοντέλο απειλών είναι ότι είναι η κατάσταση με την οποία έχουμε εμπειρία, και επίσης πιστεύουμε ότι περισσότερες ομάδες θα μπορούσαν να επικεντρωθούν στο να αλλάξουν τον κόσμο άμεσα οι ίδιες, αντί να προσπαθούν να πείσουν την κυβέρνηση να το κάνει για εμάς.

Αμυνα εις βάθος

Πάντα θα υπάρχουν πράγματα που παραβλέπετε και πράγματα που δεν μπορούσατε να γνωρίζετε. Όταν ο αμυντικός σχεδιασμός σας αναπόφευκτα αποτύχει, θα πρέπει να έχετε άλλες άμυνες στη θέση

τους, ώστε να μην είναι μια ολοκληρωτική καταστροφή. Αυτό σημαίνει ότι ακόμη και αν εμπιστεύεστε κάποιον απόλυτα, δεν του λέτε ενοχοποιητικά πράγματα που δεν χρειάζεται να γνωρίζει. Ακόμη και αν ο κρυπτογραφημένος δίσκος σας είναι ασφαλής, εξακολουθείτε να διαγράφετε πράγματα από αυτόν όταν δεν τα χρειάζεστε. Ακόμη και αν χρησιμοποιείτε μια κρυπτογραφημένη εφαρμογή ανταλλαγής μηνυμάτων, εξακολουθείτε να χρησιμοποιείτε ψευδώνυμα. Όταν τα σκατώσατε σε κάτι, δεν θα πρέπει να είναι το τέλος του κόσμου.

Διαδικασίες/Πρακτικές

Αυτή η ενότητα αποτελεί το μεγαλύτερο μέρος του οδηγού. Περιέχει ένα σύνολο πρακτικών για να κάνετε διάφορα πράγματα με μεγαλύτερη ασφάλεια. Συχνά παραπέμπουν η μία στην άλλη, π.χ. μέρος της διαδικασίας για την ασφαλή αγορά πραγμάτων από το διαδίκτυο είναι η εφαρμογή των πρακτικών για την ασφαλή χρήση του διαδικτύου. Κάθε διαδικασία έχει τρεις ολοένα και πιο ασφαλείς εκδοχές: Αποδεκτή, Καλή και Παρανοϊκή. Οι πιο ασφαλείς εκδοχές περιλαμβάνουν την εκτέλεση όλων των πραγμάτων που αναφέρονται και στις λιγότερο ασφαλείς εκδοχές, εκτός αν ορίζεται διαφορετικά. Κάναμε αυτόν τον διαχωρισμό ώστε τα συντρόφια να μην κολλάνε σε ανησυχίες σχετικά με την ασφάλεια που είναι υπερβολικές σε σχέση με αυτό που κάνουν. Ως πρόχειρος οδηγός, θεωρούμε ότι για εγκλήματα που δεν προκαλούν απαραίτητα την προσοχή της αστυνομίας κάθε φορά, όπως περιγράφεται στην εισαγωγή, το επίπεδο Αποδεκτό είναι κατάλληλο για όταν διακινδυνεύουμε έως και έξι μήνες, το Καλό για μέχρι δύο χρόνια, το Παρανοϊκό έως και πέντε ή έξι χρόνια. Αλλά αυτό είναι απλώς το προσωπικό μας επίπεδο άνεσης σε αυτό το συγκεκριμένο στάδιο της ζωής μας, οπότε μην το πάρετε ως ευαγγέλιο. Για τα εγκλήματα που προκαλούν την προσοχή της αστυνομίας, πιθανώς θα μετακινούσαμε τα πάντα κατά μία κατηγορία—καμία ποινή φυλάκισης, έξι μήνες, δύο χρόνια.

1. Πηγαίνοντας κάπου

Αποδεκτή

Φορέστε μάσκα και διακριτικά ρούχα.

Καλή

Αφήστε το τηλέφωνό σας πίσω—η τηλεφωνική εταιρεία γνωρίζει τη θέση του ανά πάσα στιγμή και διατηρεί αρχεία για χρόνια. Πληρώστε τα μέσα μαζικής μεταφοράς με μετρητά, αν είναι δυνατόν. Προσέξτε τις κάμερες κλειστού κυκλώματος παρακολούθησης, ιδίως τις κάμερες που μπορεί να είναι κρατικές αντί να ανήκουν σε ιδιωτικές επιχειρήσεις, καθώς η αστυνομία έχει ευκολότερη πρόσβαση σε αυτές.

Παρανοϊκή

Μην φέρετε τίποτα που να γράφει το όνομά σας. Πιθανόν να κανονίσετε να σας δώσει άλλοθι ένας σύντροφος, αν χρειαστεί.[1]

2. Χρησιμοποιώντας το διαδίκτυο

Αποδεκτή

Χρησιμοποιήστε το Tor Browser. Αν δεν είστε εξοικειωμένα με αυτό, το Tor Browser είναι ένα πρόγραμμα περιήγησης που δρομολογεί τη σύνδεσή σας μέσω μιας σειράς άλλων υπολογιστών πριν φτάσει στον ιστότοπο στον οποίο συνδέεστε. Αυτό σημαίνει ότι ο ιστότοπος δεν γνωρίζει ποιος είστε, επειδή η σύνδεσή σας φαίνεται να προέρχεται από κάπου αλλού, εκτός φυσικά αν του πείτε εσείς ο ίδιος ποιος είστε (π.χ. με την εγγραφή σας σε έναν λογαριασμό με το όνομά σας). Είναι εύκολο να το εγκαταστήσετε και να το χρησιμοποιήσετε σχεδόν σε οποιονδήποτε υπολογιστή, συμπεριλαμβανομένων των smartphones. Βλέπε torproject.org.

Καλή

Χρησιμοποιήστε το Tails. Αν δεν είστε εξοικειωμένα με αυτό, το Tails είναι ένα πρόγραμμα που μπορείτε να τοποθετήσετε σε ένα USB stick ή μια κάρτα SD (βλ. τη διαδικασία για την αποθήκευση ψηφιακών πληροφοριών), το οποίο σας επιτρέπει να εκκινήσετε τον υπολογιστή

[1] *Σημείωση από No Trace Project (N.T.P.):* Για αυτό το επίπεδο, μπορεί να θέλετε να λάβετε προφυλάξεις για να διασφαλίσετε ότι δεν σας ακολουθούν. Για περισσότερες πληροφορίες, ανατρέξτε στα μέτρα αντιμετώπισης της Βιβλιοθήκης Απειλών «Ανίχνευση παρακολούθησης»[2] και «Αντιπαρακολούθηση».[3]

[2] https://notrace.how/threat-library/mitigations/surveillance-detection.html

[3] https://notrace.how/threat-library/mitigations/anti-surveillance.html

στον οποίο το συνδέετε χρησιμοποιώντας ένα ασφαλές λειτουργικό σύστημα. Το Tails διασφαλίζει ότι όλη η κίνηση στο διαδίκτυο περνάει από το Tor και δεν αφήνει κανένα ίχνος στον υπολογιστή για το τι κάνατε. Βλέπε tails.net.

Παρανοϊκή

Χρησιμοποιήστε το Tails σε κάποιο δημόσιο δίκτυο wifi, όπως σε μια καφετέρια. Αυτό πιθανότατα θα περιλαμβάνει την εφαρμογή της διαδικασίας για να πάτε κάπου, εκτός αν μένετε απέναντι από μια καφετέρια ή κάτι τέτοιο και μπορείτε να συνδεθείτε στο wifi από το σπίτι σας. Έχετε υπόψη σας τις κάμερες κλειστού κυκλώματος, αλλά οι περισσότερες επιχειρήσεις δεν αποθηκεύουν αρχεία από κάμερες κλειστού κυκλώματος για πολύ καιρό. Αν πάρετε καφέ, πληρώστε με μετρητά. Μην συνηθίζετε να χρησιμοποιείτε το ίδιο μέρος κάθε φορά.

3. Αποστολή μηνυμάτων μέσω του Διαδικτύου

Αποδεκτή

Χρησιμοποιήστε το Signal. Αν δεν το γνωρίζετε, το Signal είναι μια κρυπτογραφημένη εφαρμογή ανταλλαγής μηνυμάτων. Απαιτεί έναν αριθμό τηλεφώνου για την εγγραφή, αλλά μπορεί να χρησιμοποιηθεί σε υπολογιστή, αρκεί ο λογαριασμός να είναι συνδεδεμένος με ένα τηλέφωνο. Εφαρμόστε τη διαδικασία αποθήκευσης ψηφιακών πληροφοριών σε οποιαδήποτε συσκευή εγκαθιστάτε το Signal. Εάν πιστεύετε ότι ενδέχεται να συλληφθείτε, απεγκαταστήστε το Signal. Όταν το επανεγκαταστήσετε, θα έχετε χάσει όλα τα μηνύματά σας. Αυτό είναι μια αναπόφευκτη συνέπεια των χαρακτηριστικών ασφαλείας που εμποδίζουν την αστυνομία να ανακτήσει τα μηνύματά σας από το Signal από μια συσκευή από την οποία το έχετε απεγκαταστήσει. Σημειώστε ότι ο πιο πιθανός τρόπος διαρροής των μηνυμάτων σας στο Signal με κάποιον είναι αν η αστυνομία πάρει τη συσκευή σας ή τη μη επαρκώς ασφαλισμένη συσκευή του άλλου ατόμου και απλά την ξεκλειδώσει και διαβάσει τα μηνύματα με τον ίδιο τρόπο που θα τα διάβαζε ο παραλήπτης. Ωστόσο, αν συμβεί αυτό, δεν θα γνωρίζουν απαραίτητα ποιος είναι ο άλλος συνομιλητής (εκτός αν αποκαλύψατε την ταυτότητά σας σε ένα από τα μηνύματα που έχουν διαβάσει). Βλέπε signal.org.

Υπάρχουν και άλλες κρυπτογραφημένες πλατφόρμες ανταλλαγής μηνυμάτων, αλλά το Signal είναι πολύ δημοφιλές, οπότε, πρώτον, η χρήση του είναι λιγότερο ύποπτη και, δεύτερον, έχει δοκιμαστεί εκτενώς στην πράξη. Εάν το Signal δεν είναι επιλογή, μας φαίνεται καλό το Matrix ή το SimpleX, αλλά δεν έχουμε εμπειρία σε αυτά.[4]

Καλή

Χρησιμοποιήστε ξεχωριστούς λογαριασμούς Signal για διαφορετικούς σκοπούς, έτσι ώστε αν ένας από αυτούς ταυτοποιηθεί ως δικός σας, οι άλλοι να μην ταυτοποιηθούν. Χρειάζεστε ξεχωριστό αριθμό τηλεφώνου για κάθε λογαριασμό, οπότε θα πρέπει να προμηθευτείτε μια κάρτα SIM, οι οποίες πωλούνται σε πολλά σούπερ μάρκετ (ακολουθήστε τη διαδικασία για να αγοράσετε κάτι αυτοπροσώπως ή απλά ακολουθήστε τη διαδικασία για να πάτε κάπου και να κλέψετε μία). Δεν χρειάζεται να ενεργοποιήσετε την κάρτα SIM για να λάβετε το μήνυμα επαλήθευσης, οπότε μην το κάνετε—αυτό θα συνδέσει τον τραπεζικό σας λογαριασμό με την κάρτα. Θα πρέπει να κρατήσετε την κάρτα SIM σε περίπτωση που χάσετε την πρόσβαση στον λογαριασμό σας (π.χ. επειδή πρέπει να απεγκαταστήσετε το Signal), αλλά θα πρέπει να την κρατήσετε κρυμμένη, γιατί αν η αστυνομία ψάξει το σπίτι σας και τη βρει, μπορεί να ανακαλύψει και ίσως ακόμη να προσποιηθεί τον λογαριασμό με τον οποίο είναι συνδεδεμένη. Εναλλακτικά, αν ορίσετε έναν κωδικό PIN για το Signal (βλ. παρακάτω), μπορεί να είναι εφικτό να τον χρησιμοποιήσετε για να ανακτήσετε τον λογαριασμό σας χωρίς την κάρτα SIM.

Ρυθμίστε τις επιλογές του Signal για μεγαλύτερη ασφάλεια—ορίστε τις επιλογές «Ποιοι χήστες μπορούν να δουν τον αριθμό μου» και «Ποιοι χήστες μπορούν να με βρουν με τον αριθμό μου» σε «Κανένας», ορίστε ένα προκαθορισμένο χρονόμετρο για την εξαφάνιση μηνυμάτων, απενεργοποιήστε την προεπισκόπηση συνδέσμων, τα αποδεικτικά

[4] *Σημείωση από Ν.Τ.Ρ.:* Συνιστούμε το SimpleX αντί του Matrix, καθώς το Matrix δεν προστατεύει τα μεταδεδομένα επικοινωνίας τόσο καλά όσο το SimpleX. Σε σύγκριση με το Signal, το SimpleX δεν απαιτεί αριθμό τηλεφώνου για τη δημιουργία λογαριασμού. Για περισσότερες πληροφορίες, ανατρέξτε στον οδηγό του AnarSec «Encrypted Messaging for Anarchists»[5] (Κρυπτογραφημένη Ανταλλαγή Μηνυμάτων για Αναρχικά).

[5] https://anarsec.guide/posts/e2ee

ανάγνωσης και τους δείκτες πληκτρολόγησης, ενεργοποιήστε την αναμετάδοση κλήσεων, ενεργοποιήστε το κλείδωμα οθόνης, ορίστε έναν κωδικό PIN (χρησιμοποιήστε έναν ασφαλή αλφαριθμητικό κωδικό PIN) και ενεργοποιήστε το κλείδωμα εγγραφής.

Σκεφτείτε να χρησιμοποιήσετε το Molly (molly.im). Το Molly είναι ένα εναλλακτικό frontend για το Signal. Κάνει πιο δύσκολο για κάποιον που έχει το τηλέφωνό σας να μπει στον λογαριασμό σας, αλλά δεν είναι αρκετά διαδεδομένο για να είμαστε σίγουροι ότι είναι καλά φτιαγμένο και ασφαλές.

Παρανοϊκή

Αντί να χρησιμοποιείτε τηλέφωνο, δημιουργήστε τους ευαίσθητους λογαριασμούς Signal σας στο Tails χρησιμοποιώντας το signal-cli. Δεν θα αναφερθούμε λεπτομερώς στο signal-cli, διότι αν έχετε τις τεχνικές γνώσεις για να το χρησιμοποιήσετε, θα μπορείτε να το καταλάβετε μόνοι σας. Μπορείτε να συνδέσετε το signal-desktop στον λογαριασμό για ευκολία χρήσης. Μην βάζετε την κάρτα SIM στο δικό σας τηλέφωνο, χρησιμοποιήστε ένα τηλέφωνο μιας χρήσης (που αποκτάται με τις διαδικασίες αγοράς που ισχύουν είτε online είτε αυτοπροσώπως). Μην ενεργοποιείτε ποτέ το τηλέφωνο μιας χρήσης στο σπίτι ή σε τοποθεσία που συνδέεται με εσάς, ή παρουσία των τηλεφώνων σας ή των συντρόφων σας, καθώς η τηλεφωνική εταιρεία θα γνωρίζει πού βρίσκεται και ποια άλλα τηλέφωνα βρίσκονται κοντά και θα αποθηκεύσει αυτές τις πληροφορίες. Μόλις καταχωρίσετε τον λογαριασμό σας, ξεφορτωθείτε το τηλέφωνο μιας χρήσης. Εφαρμόστε τη διαδικασία αποθήκευσης αντικειμένων για το τηλέφωνο μιας χρήσης και την κάρτα SIM. Πρέπει να αποθηκεύονται μαζί, καθώς η πρόσβαση σε ένα από τα δύο θα αποκαλύψει όλες τις πληροφορίες που θα μπορούσαν να αποκτηθούν από το ένα ή το άλλο, εκτός αν αποφασίσετε να πετάξετε το τηλέφωνο και να αγοράσετε ένα καινούργιο αν το χρειάζεστε.

Σταδιακά, η τηλεφωνική εταιρεία απενεργοποιεί τις μη καταχωρημένες ή καταχωρημένες αλλά αχρησιμοποίητες κάρτες SIM και επιτρέπει την έκδοση νέας κάρτας με τον ίδιο αριθμό. Όταν συμβεί αυτό, δεν θα μπορείτε πλέον να ανακτήσετε τον λογαριασμό σας χρησιμοποιώντας την κάρτα SIM και είναι πιθανό το άτομο που αγοράζει τη νέα κάρτα SIM να τη χρησιμοποιήσει για να εγγραφεί στο Signal, πετώντας σας

έξω από τον λογαριασμό σας (σημειώστε ότι δεν θα αποκτήσουν πρόσβαση στον λογαριασμό σας, απλώς θα χαθεί). Για να το αποφύγετε αυτό, σημειώστε πότε λήγει η κάρτα SIM σας και μεταφέρετε τον λογαριασμό σας σε νέο αριθμό πριν συμβεί αυτό. Εάν αποκτάτε σχετικά καινούργιες κάρτες SIM, αυτό δεν θα πρέπει να συμβαίνει συχνότερα από μία φορά κάθε δύο χρόνια. Θα πρέπει να το κάνετε αυτό ακόμα και αν δεν έχετε κρατήσει την κάρτα SIM και χρησιμοποιείτε μόνο τον PIN για να συνδεθείτε ξανά σε περίπτωση που χάσετε την πρόσβαση.

4. Χρησιμοποιώντας κρυπτονόμισμα

Ένας λεπτομερής οδηγός για τις μη-ασφαλείς πτυχές της χρήσης κρυπτονομισμάτων δεν εμπίπτει στο πεδίο εφαρμογής του παρόντος κειμένου, οπότε η παρούσα διαδικασία γράφεται με την προϋπόθεση ότι γνωρίζετε πώς να χρησιμοποιείτε κρυπτονομίσματα.

Αποδεκτή

Ακολουθήστε τη διαδικασία για τη χρήση του διαδικτύου και χρησιμοποιήστε το monero. Το monero είναι ένα κρυπτονόμισμα που εστιάζει στην προστασία της ιδιωτικότητας, κάτι που είναι σημαντικό, καθώς, αντίθετα με την κοινή πεποίθηση, τα περισσότερα κρυπτονομίσματα είναι εξαιρετικά ανιχνεύσιμα. Για νομικούς λόγους, είναι δύσκολο να αγοράσετε monero στο Ηνωμένο Βασίλειο, αλλά μπορείτε να αγοράσετε άλλα νομίσματα και να τα ανταλλάξετε εύκολα. Ακολουθήστε τη διαδικασία για την αποθήκευση ψηφιακών πληροφοριών για το ψηφιακό πορτοφόλι σας. Μπορείτε να αγοράσετε κρυπτονομίσμα από μια υπηρεσία onramp ή ένα ανταλλακτήριο χρημάτων.

Εάν το προϊόν που θέλετε να αγοράσετε δεν μπορεί να αγοραστεί με κρυπτονομίσματα, μπορείτε να αγοράσετε ψηφιακές προπληρωμένες χρεωστικές κάρτες χρησιμοποιώντας monero σε ιστότοπους όπως το coinsbee.com (μην ξεχάσετε να ακολουθήσετε τη διαδικασία χρήσης του διαδικτύου) και να τις χρησιμοποιήσετε για να το πληρώσετε.

Δεδομένου ότι η ασφαλής αποθήκευση πληροφοριών αυξάνει τον κίν-

δυνο απώλειας, ίσως θελήσετε να κρατήσετε ένα αντίγραφο του seed[6] του πορτοφολιού σας. Αυτό θα πρέπει να αποθηκευτεί με ασφάλεια, είτε ως ψηφιακή πληροφορία είτε γραπτώς. Όποιος αποκτήσει πρόσβαση σε αυτό, αποκτά πλήρη πρόσβαση στο πορτοφόλι.

Καλή

Βεβαιωθείτε ότι χρησιμοποιείτε τοπικό πορτοφόλι και όχι πλατφόρμα ανταλλαγής χρημάτων (αν και είναι απίθανο να βρείτε monero σε κάποια πλατφόρμα αυτές τις μέρες). Αποκτήστε πρόσβαση στο δίκτυο monero μέσω Tor, το πορτοφόλι «feather» διαθέτει ενσωματωμένη λειτουργία για αυτό (featherwallet.org). Βεβαιωθείτε ότι μεταφέρετε τα monero μεταξύ δύο πορτοφολιών που ελέγχετε, έτσι ώστε να πρέπει να παραβιαστούν περισσότερες από μία συναλλαγές για να εντοπιστεί σε τι τα ξοδεύετε. Εάν αγοράζετε κρυπτονόμισμα, εξετάστε το ενδεχόμενο να το αγοράσετε από ένα ανταλλακτήριο peer-to-peer, ώστε να είναι πιο δύσκολο να συνδεθεί με τον τραπεζικό σας λογαριασμό.

Όταν αποθηκεύετε το seed του πορτοφολιού, σκεφτείτε να γράψετε τις λέξεις-κλειδιά σε τυχαία σειρά, αρκεί να μπορείτε να θυμηθείτε πώς να τις ξαναβάλετε στη σωστή σειρά.

Παρανοϊκή

Όταν μεταφέρετε χρήματα μέσω οποιασδήποτε αλυσίδας λογαριασμών, πάντα να βάζετε περισσότερα από όσα βγάζετε στο τέλος, έτσι ώστε κάποιος που παρακολουθεί και τα δύο άκρα να μην μπορεί να μαντέψει ότι πρόκειται για τα ίδια χρήματα επειδή θα είναι ίδιο το ποσό. Επιπλέον, μην τα κάνετε όλα με τη μία, αφήστε διαστήματα μεταξύ των συναλλαγών.

Εάν διατηρείτε τις λέξεις-seed γραμμένες σε τυχαία σειρά, ανακτήστε το πορτοφόλι που αντιστοιχεί στη σειρά με την οποία είναι γραμμένες και πραγματοποιήστε μια μικρή, μη ενοχοποιητική συναλλαγή με αυτό, έτσι ώστε εάν βρεθεί το seed του πορτοφολιού, να μπορείτε να υποστηρίξετε ότι αυτό είναι το πραγματικό πορτοφόλι.

---

[6] *Σημείωση Μετάφρασης:* Το seed phrase ενός πορτοφολιού είναι μια λίστα λέξεων που αποθηκεύει όλες τις πληροφορίες που απαιτούνται για την ανάκτηση των κρυπτονομισμάτων σας στην αλυσίδα των συναλλαγών.

5. Αγοράζοντας κάτι αυτοπροσώπως

Αποδεκτή

Εφαρμόστε τη διαδικασία για να πάτε κάπου. Πληρώστε με μετρητά.

Η καλή και η παρανοϊκή εκδοχή αυτής της διαδικασίας είναι ακριβώς η ίδια με τη χρήση της καλής και της παρανοϊκής εκδοχής της διαδικασίας για να πάτε κάπου.

6. Αγοράζοντας κάτι στο Διαδίκτυο

Αποδεκτή

Αν πρόκειται για κάτι που δεν είναι παράνομο από μόνο του, βάλτε κάποιον που δεν κάνει κάτι ύποπτο να το παραγγείλει και να το παραλάβετε από αυτόν. Μπορείτε να τον αποζημιώσετε σε μετρητά. Μην ξεχάσετε να αφαιρέσετε την ετικέτα με τη διεύθυνσή του από το κουτί, αν το κρατήσετε, ώστε αν γίνει έρευνα στο σπίτι σας η αστυνομία να μην μάθει για το άτομο αυτό από την ετικέτα.

Καλή

Εφαρμόστε τη διαδικασία για τη χρήση του διαδικτύου και παραγγείλτε το χρησιμοποιώντας τη διαδικασία για τη χρήση κρυπτονομισμάτων, είτε σε διεύθυνση τρίτου προσώπου είτε σε poste restante (ταχυδρομική θυρίδα)[7] σε ένα όνομα για το οποίο έχετε μια καλή πλαστή ταυτότητα (αν δεν μπορείτε να δώσετε έγκυρη ταυτότητα, το ταχυδρομείο μπορεί να αρνηθεί να σας δώσει το δέμα).

Δεν υπάρχει παρανοϊκό επίπεδο γι' αυτό, επειδή δεν έχουμε την εμπειρία με την παραγγελία οτιδήποτε που να δικαιολογεί αυτό το επίπεδο ασφάλειας, ώστε να μπορούμε να μιλήσουμε με βεβαιότητα γι' αυτό. Οτιδήποτε θα μπορούσαμε να πούμε θα ήταν εικασία.

[7] *Σημείωση από N.T.P.:* Το Poste restante είναι μια υπηρεσία κατά την οποία το ταχυδρομείο κρατά την αλληλογραφία μέχρι ο παραλήπτης να την παραλάβει.

7. Ξέπλυμα χρήματος

Αποδεκτή

Αγοράστε πράγματα με τα χρήματα και πουλήστε τα. Αγοράστε και/ή πουλήστε πράγματα με παρόμοιο τρόπο με τα δικά σας χρήματα για να το συγκαλύψετε. Αυτή η διαδικασία είναι εντάξει με την πρώτη ματιά, αλλά δεν θα αντέξει σε πραγματική έρευνα και δεν είναι πρακτική για μεγάλα χρηματικά ποσά.

Καλή

Χρησιμοποιώντας τη διαδικασία πρόσβασης στο διαδίκτυο, αγοράστε monero με τα χρήματα (δείτε τη διαδικασία χρήσης κρυπτονομισμάτων). Σε αυτό το σημείο, τα χρήματα θα πρέπει να αποσυνδεθούν από την πηγή τους. Χρησιμοποιήστε το monero για να αγοράσετε προπληρωμένες ψηφιακές χρεωστικές κάρτες, όπως αναφέρεται στη διαδικασία χρήσης κρυπτονομισμάτων. Σημειώστε ότι, αν και η πηγή των χρημάτων είναι ασαφής, το γεγονός ότι προέρχονται από monero εξακολουθεί να φαίνεται ύποπτο.

Παρανοϊκή

Αγοράστε monero με τα χρήματα και μεταφέρετέ τα μεταξύ δύο λογαριασμών. Σε αυτό το σημείο, τα χρήματα θα πρέπει να έχουν αποσυνδεθεί από την πηγή τους. Ανταλλάξτε το monero με μετρητά που σας έχουν σταλεί ταχυδρομικά σε μια πλατφόρμα ανταλλαγής peer-to-peer, όπως το retoswap (retoswap.com) (ακολουθώντας τις συμβουλές της διαδικασίας αγοράς προϊόντων στο διαδίκτυο για την ασφαλή παραλαβή τους από το ταχυδρομείο).

8. Αποστολή αλληλογραφίας

Αποδεκτή

Ακολουθήστε τη διαδικασία για να πάτε κάπου. Αγοράστε τα γραμματόσημα με μετρητά. Πηγαίνετε σε διαφορετικά ταχυδρομεία. Ακολουθήστε τους κανόνες του ταχυδρομείου (π.χ. σχετικά με τον σωστό τρόπο αποστολής υγρών) όσο το δυνατόν περισσότερο, για να μειώσετε τις πιθανότητες να ανοιχτούν τα πακέτα σας.

Καλή

Αγοράστε γραμματόσημα και φακέλους με μετρητά και ταχυδρομήστε τα σε γραμματοκιβώτια. Χρησιμοποιήστε διαφορετικά γραμματοκιβώτια. Αν πρέπει να στείλετε μεγάλα αντικείμενα, χρησιμοποιήστε γραμματοκιβώτια για δέματα, αλλά αν δεν βρίσκεστε σε πόλη, μπορεί να μην υπάρχουν πολλά για να επιλέξετε. Μην ταχυδρομείτε πολλά αντικείμενα ταυτόχρονα σε ένα γραμματοκιβώτιο, καθώς αυτό μπορεί να προκαλέσει υποψίες και να τα ανοίξουν. Όσον αφορά τα γραμματόσημα, λάβετε υπόψη ότι οι γραμμωτοί κώδικες που φέρουν δεν μπορούν να χρησιμοποιηθούν για να εντοπιστεί πού αγοράστηκαν, αλλά σαρώνονται από το κέντρο διαλογής, ώστε να μπορούν να χρησιμοποιηθούν για να εντοπιστεί τουλάχιστον το κέντρο διαλογής του τόπου από τον οποίο ταχυδρομήθηκε κάτι (και αυτός είναι ένας από τους σκοπούς τους).

Παρανοϊκή

Για περιστασιακές αποστολές, χρησιμοποιήστε αναμνηστικά γραμματόσημα, καθώς δεν έχουν γραμμωτούς κώδικες (η αποστολή πολλών δεμάτων με αναμνηστικά γραμματόσημα από ένα μόνο μέρος θα ήταν ύποπτη). Αγοράστε φακέλους από διαφορετικά μέρη, ώστε η μάρκα των φακέλων που χρησιμοποιείτε να μην μπορεί να χρησιμοποιηθεί για να προσδιοριστεί από πού τους αγοράζετε (ή, πιο πιθανό, ως έμμεση απόδειξη μετά το συμβάν, με βάση το γεγονός ότι επισκεπτόσασταν συχνά ένα μέρος που πωλούσε αυτούς τους φακέλους). Επιλέξτε γραμματοκιβώτια σε τοποθεσίες έτσι ώστε το σπίτι σας να μην βρίσκεται στο κέντρο όλων των τοποθεσιών που χρησιμοποιείτε.

9. Αποθήκευση ενός αντικειμένου

Αποδεκτή

Εάν η διεύθυνσή σας δεν είναι πιθανό να αποτελέσει στόχο έρευνας, απλά κρατήστε το στο σπίτι σας. Εάν εσείς ή οι συγκατοικοί σας κινδυνεύετε να συλληφθείτε ή εάν η διεύθυνση χρησιμοποιείται για παραγγελίες, κρύψτε το. Μικρά αντικείμενα όπως κάρτες SD και SIM είναι εύκολο να κρυφτούν πολύ καλά, οπότε μην τα κολλήσετε απλά πίσω από μια κορνίζα και τέλος, ξεβιδώστε το πίσω μέρος από κάτι που δεν ανοίγεται ποτέ υπό κανονικές συνθήκες ή κάτι τέτοιο.

Καλή

Ακόμα κι αν το σπίτι σου δεν είναι πιθανό να υποστεί έρευνα, κρύψ' το ούτως ή άλλως. Αν δεν χρειάζεται να έχεις τακτική πρόσβαση σε αυτό, φύλαξέ το στο σπίτι κάποιου που δεν κάνει τίποτα ύποπτο.

Μην μπείτε στον πειρασμό να κρύψετε πράγματα σε δημόσιους χώρους, καθώς τότε δεν θα χρειαστεί ένταλμα έρευνας για να τα βρουν.[8] Οι αποθήκες είναι πιθανώς επίσης κακή ιδέα, καθώς θα συνδέονται με όποιον τις πληρώνει.

Παρανοϊκή

Εάν το αντικείμενο είναι αναπληρώσιμο, φθηνό και/ή σπάνια χρησιμοποιούμενο, σκεφτείτε να μην το αποθηκεύσετε καθόλου και να αγοράζετε καινούργιο όποτε το χρειάζεστε. Εάν το αντικείμενο μπορεί να χωριστεί σε μέρη που δεν είναι (τόσο) ενοχοποιητικά από μόνα τους, αποθηκεύστε τα σε σπίτια διαφόρων ατόμων. Δεν γνωρίζουμε κανέναν καλό τρόπο για να κρύψετε ένα μοναδικό, μεμονωμένο αντικείμενο σύμφωνα με τα παρανοϊκά πρότυπα ασφάλειας, οπότε αν χρειαστεί να το κάνετε, το μόνο που μπορούμε να σας προτείνουμε είναι να ελαχιστοποιήσετε το χρόνο που χρειάζεστε για να το έχετε αποθηκευμένο.

10. Αποθήκευση ψηφιακών πληροφοριών

Αποδεκτή

Αποθηκεύστε το σε έναν υπολογιστή με πλήρη κρυπτογράφηση δίσκου. Αν δεν ξέρετε πώς να το στήσετε, ανατρέξτε στο VeraCrypt (veracrypt.fr).[10]

---

[8] *Σημείωση από Ν.Τ.Ρ.:* Πιστεύουμε ότι η αποθήκευση αντικειμένων σε δημόσιους χώρους μπορεί να είναι μια βιώσιμη λύση, αν γίνεται με τον σωστό τρόπο. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα «Σημείο αποθήκευσης ή ασφαλές καταφύγιο»[9] της βιβλιοθήκης απειλών.

[9] https://notrace.how/threat-library/mitigations/stash-spot-or-safe-house.html

[10] *Σημείωση από Ν.Τ.Ρ.:* Σε υπολογιστές (όχι σε smartphone) συνιστούμε την κρυπτογράφηση όλων των ψηφιακών σας πληροφοριών χρησιμοποιώντας το σύστημα πλήρους κρυπτογράφησης δίσκου Linux Unified Key Setup (LUKS), το οποίο είναι διαθέσιμο από προεπιλογή στα περισσότερα σύγχρονα συστήματα Linux και, ως εκ τούτου, δεν απαιτεί την εγκατάσταση πρόσθετου λογισμικού όπως το VeraCrypt.

Εάν πρέπει να το αποθηκεύσετε σε smartphone, π.χ. επειδή είναι μια εφαρμογή ανταλλαγής μηνυμάτων που είναι δύσκολο να λειτουργήσει σε υπολογιστή ή επειδή χρειάζεστε πρόσβαση σε αυτό εν κινήσει, τότε ορίστε έναν ισχυρό κωδικό πρόσβασης στο τηλέφωνό σας (δηλ. ΟΧΙ μόνο έναν αριθμητικό PIN) και απενεργοποιήστε το ξεκλείδωμα με δακτυλικό αποτύπωμα. Εάν πιστεύετε ότι ενδέχεται να συλληφθείτε, απενεργοποιήστε το τηλέφωνό σας, καθώς ορισμένες μέθοδοι ξεκλειδώματος λειτουργούν μόνο εάν έχει προηγουμένως ξεκλειδώσει από τη στιγμή που ενεργοποιήθηκε.

Εάν η αστυνομία πιστεύει ότι τα κρυπτογραφημένα δεδομένα που βρήκε είναι σχετικά με μια έρευνα και ότι γνωρίζετε τον κωδικό πρόσβασης, μπορεί να σας υποχρεώσει νομικά να τα αποκρυπτογραφήσετε. Η ποινή για την άρνηση μπορεί να είναι έως και δύο χρόνια φυλάκιση, ή πέντε αν πρόκειται για έρευνα για τρομοκρατία. Για αυτόν τον λόγο, μην υποθέτετε ότι ακόμη και η απόλυτα ασφαλής κρυπτογράφηση θα κρατήσει την αστυνομία μακριά αν τα αποδεικτικά στοιχεία που προστατεύονται αξίζουν λιγότερο από δύο χρόνια. Υπάρχει μια υπερασπιστική γραμμή αν μπορείτε να δημιουργήσετε αμφιβολίες για το αν υπάρχουν πραγματικά κρυπτογραφημένα δεδομένα (αυτό απαιτεί τεχνικές δεξιότητες για να το επιτύχετε) ή για το αν γνωρίζετε πραγματικά τον κωδικό πρόσβασης.

Η χρήση του cryptpad (cryptpad.org) είναι εντάξει, αρκεί να θυμάστε να βάλετε κωδικό πρόσβασης και να μην έχετε τον κωδικό δίπλα στον link, γιατί έτσι χάνεται το νόημα του κωδικού.

Όταν δεν χρειάζεστε πλέον τις πληροφορίες, εφαρμόστε τη διαδικασία καταστροφής ψηφιακών πληροφοριών.

Καλή

Αποθηκεύστε τα σε μια κρυπτογραφημένη κάρτα microSD και κρατήστε τα κρυμμένα, ή αποθηκεύστε τα σε ένα VeraCrypt κρυφό τμήμα (hidden volume) σε έναν παραδοσιακό σκληρό δίσκο (δηλαδή όχι σε SSD, USB stick ή κάρτα SD, καθώς αυτά δεν μπορούν να κρύψουν αξιόπιστα την ύπαρξη ενός κρυφού τμήματος). Εάν χρησιμοποιείτε κάρτα SD ή USB stick, λάβετε υπόψη ότι μερικές φορές μπορεί να παρουσιάσουν βλάβη. Εάν οι πληροφορίες είναι σημαντικές, κρατήστε ένα

αντίγραφο ασφαλείας, επίσης κρυπτογραφημένο. Εάν χρησιμοποιείτε Tails (δείτε τη διαδικασία για τη χρήση του διαδικτύου), μπορείτε να χρησιμοποιήσετε την μόνιμη αποθήκευση (persistent storage) για να αποθηκεύσετε πληροφορίες με αυτόν τον τρόπο, και μερικές φορές σας προειδοποιεί πριν η συσκευή παρουσιάσει βλάβη.[11]

Παρανοϊκή

Δεν διαθέτουμε μια καλή στρατηγική για την αποθήκευση ψηφιακών πληροφοριών σε παρανοϊκό επίπεδο ασφάλειας.[12] Μπορούμε μόνο να σας προτείνουμε να ελαχιστοποιήσετε το χρονικό διάστημα αποθήκευσης και να κάνετε όσο το δυνατόν πιο δύσκολο να αποδειχθεί ότι κάποιος γνωρίζει τον κωδικό πρόσβασης.

11. Καταστροφή ψηφιακών πληροφοριών

Δεν υπάρχει αποδεκτό επίπεδο για αυτή τη διαδικασία, επειδή η επανεγγραφή (overwrite) είναι αρκετά καλή για να θεωρηθεί καλή, αλλά η απλή διαγραφή δεν είναι αρκετά καλή για να θεωρηθεί αποδεκτή.

Καλή

Όταν ένα αρχείο διαγράφεται, δεν αφαιρείται από τη μνήμη, απλώς επισημαίνεται ως διαγραμμένο μέχρι να αντικατασταθεί από κάτι άλλο που αποθηκεύεται στην ίδια θέση. Για να το διαγράψετε σωστά, θα πρέπει πρώτα να το αντικαταστήσετε με άσχετα δεδομένα. Αυτό μπορεί να επιτευχθεί με εργαλεία όπως το sdelete και το secure-delete. Ωστόσο, αυτό ισχύει μόνο αν χρησιμοποιείτε έναν παραδοσιακό σκληρό δίσκο, σε αντίθεση με έναν SSD (που είναι σχεδόν σίγουρα η περίπτωση σε έναν φορητό υπολογιστή), ένα USB stick ή μια κάρτα SD. Αν χρησιμοποιείτε ένα από αυτά, αυτή η μέθοδος δεν θα λειτουργήσει για μεμονωμένα αρχεία. Αντ' αυτού, θα πρέπει να διαγράψετε τα πάντα με μία κίνηση, αντικαθιστώντας ολόκληρο το δίσκο με ένα εργαλείο όπως το DBAN ή το dd.

---

[11] *Σημείωση από Ν.Τ.Ρ.:* Η μόνιμη αποθήκευση στο Tails χρησιμοποιεί LUKS.

[12] *Σημείωση από Ν.Τ.Ρ.:* Επιπλέον στρατηγική για αυτό το επίπεδο είναι η αποθήκευση συσκευών που περιέχουν ψηφιακές πληροφορίες με τρόπο που να αποτρέπει την παραβίαση. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα «Προετοιμασία για αποτροπή παραβίασης»[13] της βιβλιοθήκης απειλών.

[13] https://notrace.how/threat-library/mitigations/tamper-evident-preparation.html

Παρανοϊκή

Επανεγγράψτε ολόκληρο το δίσκο πολλές φορές (ακόμα και αν πρόκειται για παραδοσιακό σκληρό δίσκο, στην περίπτωση που κάποιο αντίγραφο ασφάλειας έχει δημιουργηθεί αυτόματα ή κάτι παρόμοιο). Εναλλακτικά, αν και είναι πιθανώς υπερβολικό αλλά πιο γρήγορο αν βιάζεστε, καταστρέψτε φυσικά το δίσκο στον οποίο ήταν αποθηκευμένες οι πληροφορίες. Θα πρέπει να βεβαιωθείτε ότι καταστρέφετε πραγματικά το σημείο όπου αποθηκεύονται τα δεδομένα. Η παραδοσιακή μέθοδος τρυπήματος ενός σκληρού δίσκου δεν είναι στην πραγματικότητα τόσο αξιόπιστη, ιδανικά θα χρειαστείτε έντονη θερμότητα ή ισχυρό μαγνητισμό.

Αν συλληφθείτε

(Υπενθυμίζουμε ότι το παρόν κείμενο βασίζεται στις πρακτικές της αστυνομίας του Ηνωμένου Βασιλείου.)

Εάν, παρά τις προφυλάξεις σας, συλληφθείτε, υπάρχουν ακόμα πράγματα που μπορείτε να κάνετε—ή κυρίως, να αποφύγετε να κάνετε—για να ελαχιστοποιήσετε τη ζημιά. Το συμπέρασμα είναι: ΜΗΝ ΜΙΛΗΣΕΤΕ ΣΤΗΝ ΑΣΤΥΝΟΜΙΑ ΓΙΑ ΚΑΝΕΝΑ ΛΟΓΟ. Η αστυνομία είναι πολύ καλή στο να σας παρασύρει να πείτε κάτι ενοχοποιητικό ή που μπορεί να χρησιμοποιήσει ως βάση για εύλογη υποψία. Υπάρχουν πολλές περιπτώσεις στις οποίες το να μιλήσετε στην αστυνομία μπορεί να κάνει τη ζωή σας πιο δύσκολη. Δεν υπάρχουν περιπτώσεις υπό τις οποίες το να μιλήσετε στην αστυνομία θα κάνει τη ζωή σας ευκολότερη (με ίσως δύο εξαιρέσεις, που θα συζητηθούν αργότερα). Εάν σας υποπτεύονται, τίποτα από όσα μπορείτε να πείτε δεν θα τους κάνει να σας υποπτεύονται λιγότερο. Δεν έχει σημασία πώς αρνείστε να μιλήσετε μαζί τους —μπορείτε να πείτε «όχι σχόλιο», «δεν θα απαντήσω σε αυτό», «είμαι νομικά υποχρεωμένος να απαντήσω σε αυτό;», τίποτα απολύτως, απλά μην τους πείτε τίποτα. Ακολουθεί μια λίστα με τις περιστάσεις υπό τις οποίες δεν πρέπει να απαντάτε στις ερωτήσεις της αστυνομίας:

- Αν σου πουν ότι θα σε αφήσουν να φύγεις πιο γρήγορα αν μιλήσεις, ή ότι θα σε κρατήσουν περισσότερο αν δεν μιλήσεις. Αυτό

γενικά δεν είναι αλήθεια, και δεν μπορούν να σε κρατήσουν για πολύ χωρίς να σου επιβάλουν κατηγορίες ούτως ή άλλως.

- Εάν σου κάνουν οποιαδήποτε πρόταση για μείωση της ποινής σου. Η αστυνομία δεν έχει την εξουσία να μειώσει την ποινή σου, αυτό είναι θέμα που αφορά το δικαστήριο.
- Αν σου προτείνουν να σε κατηγορήσουν μόνο για ένα μικρό αδίκημα αν το παραδεχτείς και να αποσύρουν μια πιο σοβαρή κατηγορία. Λένε ψέματα.
- Αν σου πουν ότι έχουν ήδη αρκετά στοιχεία για να σε καταδικάσουν ή ότι ένας συνεργός έχει ομολογήσει. Πιθανότατα λένε ψέματα, και ακόμα κι αν δεν είναι έτσι, εκτός αν ένας ικανός δικηγόρος σου πει το αντίθετο, εξακολουθείς να έχεις περισσότερες πιθανότητες να μειώσεις την ποινή σου αν παραμείνεις σιωπηλός.
- Αν κάνουν ευγενική κουβεντούλα. Μόλις αρχίσεις να μιλάς, είναι πιο εύκολο για αυτούς να σε κρατήσουν σε συζήτηση. Να θυμάσαι, είναι εκπαιδευμένοι να αποσπούν πληροφορίες από τους ανθρώπους.
- Εάν σου κάνουν ερωτήσεις των οποίων οι απαντήσεις σίγουρα δεν είναι ενοχοποιητικές. Εάν απαντήσεις σε αυτές τις ερωτήσεις αλλά μετά αρνηθείς να απαντήσεις στις ερωτήσεις που είναι ενοχοποιητικές, αυτό θα φανεί πολύ κακό στο δικαστήριο.
- Εάν έχεις άλλοθι, κράτα το για τον δικηγόρο σου και το δικαστήριο. Η αστυνομία δεν χρειάζεται να γνωρίζει το άλλοθι σου και δεν θα το πιστέψει. Οτιδήποτε πεις στην αστυνομία, ουσιαστικά δεσμεύεσαι να το πεις και στο δικαστήριο. Δεν χρειάζεται να δεσμευτείς για τίποτα, οπότε μην το κάνεις.
- Επίσης, αν σε κατηγορούν για κάτι που μπορείς εύκολα να αποδείξεις ότι δεν έκανες. Είναι προς όφελός σου αν προσπαθήσουν να σε κατηγορήσουν για κάτι που μπορείς εύκολα να αποδείξεις ότι δεν έκανες, καθώς αυτό κάνει τις υπόλοιπες κατηγορίες να φαίνονται λιγότερο αξιόπιστες. Κράτα το για τον δικηγόρο σου και το δικαστήριο.
- Αν δείχνουν άγνοια. Μπορεί να είναι πραγματική, ή μπορεί να σε ψαρεύουν για να παρουσιάσεις τις γνώσεις σου σχετικά με ένα

θέμα που σχετίζεται με τις κατηγορίες. Σε κάθε περίπτωση, δεν αξίζει τον κόπο να τους κοροϊδεύεις.

- ΟΠΟΙΑΔΗΠΟΤΕ ΑΛΛΗ ΠΕΡΙΠΤΩΣΗ, εκτός από τις εξαιρέσεις που αναφέρονται παρακάτω.

Οι δύο περιπτώσεις στις οποίες θα ήταν πιθανώς προς όφελός σας να πείτε κάτι στην αστυνομία είναι οι εξής:

- Όταν φτάσετε στο αστυνομικό τμήμα (και όχι πριν), ίσως θελήσετε να τους δώσετε το όνομά σας και τη διεύθυνσή σας. Αυτό γιατί, αν αρνηθείτε να δώσετε το όνομά σας και τη διεύθυνσή σας και αποφασίσουν να σας απαγγείλουν κατηγορίες, μπορούν να σας κρατήσουν υπό κράτηση μέχρι την ημερομηνία της δίκης, ανεξάρτητα από το τι σας κατηγορούν (γιατί αν σας αφήσουν ελεύθερο, δεν θα μπορούν να σας βρουν ξανά). Η παροχή ψευδών στοιχείων αποτελεί αδίκημα και συνήθως μπορούν να τα ελέγξουν πολύ εύκολα. Σημειώστε ότι αν δώσετε τη διεύθυνσή σας, μπορεί να πάνε να την ψάξουν.
- Σε ορισμένες σπάνιες περιπτώσεις, η άρνηση απάντησης σε ορισμένες ερωτήσεις μπορεί να αποτελεί από μόνη της αδίκημα. Ένα συγκεκριμένο παράδειγμα αυτού αναφέρεται στην ενότητα σχετικά με την αποθήκευση ψηφιακών πληροφοριών—σε ορισμένες περιπτώσεις μπορεί να αποτελεί αδίκημα η μη αποκάλυψη του κωδικού πρόσβασης για κρυπτογραφημένα δεδομένα. Αυτό το είδος περιστατικών δεν συμβαίνει πολύ συχνά, και αν συμβεί, θα σας το πουν (ή τουλάχιστον θα έπρεπε, και πιθανότατα θα το κάνουν αν σκοπεύουν να σας κατηγορήσουν για αυτό, καθώς το δικαστήριο πιθανότατα θα τους ζητήσει να αποδείξουν ότι το έκαναν). Αντίθετα, αν σας πουν ότι είστε νομικά υποχρεωμένοι να απαντήσετε σε μια ερώτηση, μπορεί να λένε ψέματα—αν είναι δυνατόν, επιβεβαιώστε το με τον δικηγόρο σας.

Τελευταία λόγια

Αφού διαβάσατε όλα αυτά, το πιο σημαντικό για εμάς είναι να μην σας τρομάξει η διαδικασία. Όπως είπαμε στην αρχή, αν η προσπάθεια να είστε ασφαλείς σας αποτρέπει από το να αναλάβετε δράση, τότε το

κράτος επιτήρησης κερδίζει χωρίς να κάνει τίποτα. Αν δεν αισθάνεστε ικανοί να επιτύχετε το επίπεδο ασφάλειας που θεωρείτε απαραίτητο για τις ενέργειες που θέλετε να κάνετε, αναλάβετε λιγότερο επικίνδυνες ενέργειες στο ενδιάμεσο, αντί να επικεντρώνεστε αποκλειστικά στο να μάθετε τα πάντα για την ασφάλεια. Η εμπειρία μέσα από την δράση είναι ο καλύτερος τρόπος για να μάθεις.

<3

Απαιτείται αρκετή δουλειά για να αντιληφθείτε πώς να μην σας συλλάβουν και πώς να ελαχιστοποιήσετε τη ζημιά αν τελικά συλληφθείτε. Για να προσπαθήσουμε να διευκολύνουμε τα συντρόφια μας, θέλουμε να μοιραστούμε τις τεχνικές που αναπτύξαμε λειτουργώντας μια παράνομη ακτιβιστική οργάνωση. Αυτός είναι ένας οδηγός για μη ειδικούς, αλλά σε κάποιες μεθόδους θα βοηθούσε να είστε λίγο τεχνολογικά καταρτισμένες ή τουλάχιστον να συνεργαστείτε με κάποιους τεχνολογικά καταρτισμένους φίλους.

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.