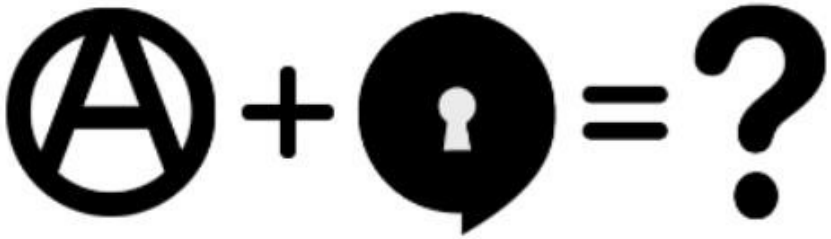


Η ελληνική μετάφραση έγινε από την Ελευθεριακή Παρέμβαση ΑΣΟΕΕ τον Δεκέμβριο του 2021.
Η συγκεκριμένη μπροσούρα βρέθηκε στην ιστοσελίδα sproutdistro.com.
Διανέμεται με ελεύθερη οικονομική συνεισφορά για τα έξοδα εκτύπωσης.

Το Signal είναι μία κρυπτογραφημένη εφαρμογή ανταλλαγής μηνυμάτων το οποίο συναντάμε εδώ και περίπου 10 χρόνια σε διάφορες μορφές. Από τότε, έχω παρατηρήσει αυτό το λογισμικό να χρησιμοποιείται συχνότερα από τα αναρχικά δίκτυα στον Καναδά και στις ΗΠΑ. Όλο και περισσότερο, προς το καλύτερο και προς το χειρότερο, οι διαπροσωπικές μας συζητήσεις έχουν μεταναστεύσει στην πλατφόρμα του Signal, στο σημείο που έχει μετατραπεί στο κύριο μέσο επικοινωνίας μεταξύ των αναρχικών σε αυτήν την ήπειρο, συνοδευόμενο με πολύ λίγη κριτική πάνω στις επιπτώσεις που μπορεί να έχει.

Το Signal είναι απλά μία εφαρμογή κινητού. Η πραγματική στροφή που παίρνει ο κόσμος είναι προς μία ζωή με μεσολαβητή τις οθόνες των κινητών και τα κοινωνικά δίκτυα. Μέσα σε πολύ λίγα χρόνια έγινε αναγκαστική η κατοχή ενός κινητού για οποιοδήποτε άτομο θέλει φίλους ή χρειάζεται δουλειά, εκτός από μικρές μερίδες ατόμων. Μέχρι πρόσφατα, η αναρχική υποκουλτούρα ήταν μία από αυτές τις μερίδες ατόμων, όπου μπορούσες να αρνηθείς να κουβαλάς μαζί σου κινητό και να είναι κοινωνικά αποδεκτό. Τώρα δεν είμαι τόσο σίγουρο και αυτό είναι γαμημένα λυπηρό. Συνεπώς θα επιμείνω μέσω αυτής της μπροσούρας ότι δεν υπάρχει υποκατάστατο για τις δια ζώσης, από-κοντά σχέσεις, που εμπεριέχουν την πλουσιότητα και περιπλοκότητα της γλώσσα του σώματος, των συναισθημάτων και του φυσικού περιεχομένου, και συνεχίζουν να είναι ο πιο ασφαλής τρόπος για να γίνει μία προσωπική κουβέντα. Οπότε παρακαλώ, ας αφήσουμε τα κινητά μας στο σπίτι, ας βρεθούμε στον δρόμο ή σε κάποιο δάσος, ας σχεδιάσουμε μαζί, ας συνθέσουμε μουσική, ας φτιάξουμε πράγματα, ας σπάσουμε πράγματα, και ας καλλιεργήσουμε την ζωή εκτός διαδικτύου. Πιστεύω πως αυτό είναι πολύ πιο σημαντικό από το να μάθουμε να χρησιμοποιούμε το Signal σωστά.

Η ιδέα για αυτήν την μπροσούρα μου ήρθε πριν ένα χρόνο, όταν επισκεπτόμουν φίλα μου σε μια άλλη πόλη και αστειευόμασταν σχετικά με τους τρόπους που οι συζητήσεις στο Signal μετατρέπονται σε τεράστιες καταστροφές. Τα κοινά λάθη έγιναν εμφανή και άρχισα να συνειδητοποιώ πως αυτή η κουβέντα γίνεται συχνά και σε άλλα μέρη. Όταν άρχισα να ρωτάω τους γύρω μου, όλα είχαν παρατηρήσεις και γνώμες, όμως πολύ λίγες κοινές πρακτικές είχαν ανακαλυφθεί ως λύσεις. Οπότε δημιούργησα μία λίστα με ερωτήσεις και την έβαλα στην κυκλοφορία. Εξεπλάγην θετικά όταν μου δόθηκαν δεκάδες λεπτομερείς απαντήσεις, που ταίριαζαν με πολλές ανεπίσημες συζητήσεις.

Δεν είμαι ειδικό - δεν έχω μελετήσει το θέμα της κρυπτογραφίας και δεν γνωρίζω πως να γράφω κώδικα. Είμαι ένα αναρχικό με ενδιαφέρον για την ασφάλεια σε ένα ευρύτερο πλαίσιο για την ερμηνεία της, και με μια περίεργη σχέση με την τεχνολογία. Ο στόχος μου με την συγκεκριμένη μπροσούρα είναι να αποτυπώσω τον τρόπο με τον οποίο το Signal έχει γίνει κεντρικό σημείο αναφοράς στην αναρχική επικοινωνία, να εκτιμήσω τις επιπτώσεις του τόσο πάνω στην *συλλογική ασφάλεια* όσο και στην *κοινωνική οργάνωση*, και να προάγω κάποιες προκαταρκτικές προτάσεις με σκοπό την δημιουργία κοινών πρακτικών.

Μία σύντομη ιστορία για το Signal

25 χρόνια πριν, οι τεχνολογικά αισιόδοξοι ανάμεσά μας ανακάλυψαν μία τεράστια ευκαιρία στο αναδυόμενο διαδίκτυο βλέποντάς το ως εργαλείο ελευθερίας. Θυμάστε εκείνο το παλιό άρθρο εφημερίδας που επαινούσε το “υπολογιστικό δίκτυο που ονομάζεται ‘Ιντερνετ” ως “ελεγχόμενη αναρχία”; Παρόλο που υπάρχουν ακόμα δυνατοί τρόποι για ασφαλή επικοινωνία, που περιγράφονται ελεύθερα στο ίντερνετ, είναι ξεκάθαρο ότι το κράτος και οι επιχειρηματικές οντότητες καταλαμβάνουν όλο και μεγαλύτερο μέρος του διαδικτύου και το χρησιμοποιούν για να μας υποβάλουν σε όλο και πιο έντονες μορφές παρακολούθησης και κοινωνικού ελέγχου.

Το διαδίκτυο πάντα ήταν έδαφος ανταγωνισμού μεταξύ χωρών. Το 1991, ένας κρυπτογράφος,ελευθεριακός και ειρηνικός ακτιβιστής, ο Φίλ Ζίμμερμαν, δημιούργησε την Pretty Good Privacy (PGP), μία εφαρμογή ελεύθερου λογισμικού για την κρυπτογράφηση αρχείων και end-to-end κρυπτογράφησης (από έναν διακομιστή σε έναν άλλον χωρίς παρεμβολή δευτερευόντων διακομιστών) για το ηλεκτρονικό ταχυδρομείο. Θα παραλείψω τεχνικές λεπτομέρειες, αλλά βασικά το πιο σημαντικό κομμάτι της end-to-end κρυπτογράφησης είναι ότι μπορείς να επικοινωνήσεις ασφαλώς και άμεσα με ένα άλλο άτομο, και η υπηρεσία ηλεκτρονικού ταχυδρομείου δεν μπορεί να δει το μήνυμα που έστειλες, είτε είναι η Google είτε είναι η Riseup. Μέχρι σήμερα, με όλα όσα ξέρουμε, κανένας δεν έχει καταφέρει να “σπάσει” την κρυπτογράφηση PGP.

Εδώ και χρόνια, κομπιουτεράκηδες και φυτά της ασφάλειας σε συγκεκριμένους κύκλους – αναρχικούς, δημοσιογραφικούς, εγκληματικούς, κλπ – έχουν προσπαθήσει να διαδώσουν το PGP στα κοινωνικά τους δίκτυα ως μία κάπως ασφαλή δίοδο επικοινωνίας, με κάποιες επιτυχίες. Όμως, όπως με όλα τα πράγματα, υπήρξαν εμπόδια. Η μεγαλύτερη μου ανησυχία σχετικά με το PGP είναι η απουσία του Forward Secrecy, το οποίο σημαίνει ότι αν ποτέ “σπάσουν” ένα ιδιωτικό κλειδί κρυπτογράφησης, όλα τα μηνύματα που έχουν σταλθεί μέσω αυτού του κλειδιού μπορούν να αποκρυπτογραφηθούν από έναν εισβολέα. Αυτό είναι μία πραγματική ανησυχία, καθώς η NSA (Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ) αποθηκεύει σίγουρα όλα τα κρυπτογραφημένα σου μηνύματα κάπου, και μία μέρα οι κβαντικοί υπολογιστές θα μπορούσαν να “σπάσουν” την κρυπτογράφηση του PGP. Μη με ρωτήσετε πώς λειτουργούν οι κβαντικοί υπολογιστές – για εμένα είναι μαύρη γαμημένη μαγεία.

Το μεγάλο κοινωνικό πρόβλημα με την PGP, αυτό που έθεσε γερά τα θεμέλια για το Signal, είναι το γεγονός ότι δεν χρησιμοποιήθηκε αρκετά εκτός κάποιων κλειστών κύκλων. Από τη δική μου εμπειρία , ήταν δύσκολο να καταφέρουν τα αναρχικά να αρχίσουν να χρησιμοποιούν την PGP και μάλιστα με σωστό τρόπο. Γινόντουσαν παρουσιάσεις, αρκετά άτομα μάθαιναν για την χρήση του, αλλά την στιγμή που ένας υπολογιστής κράσαρε ή χανόταν ένας κωδικός, όλη η πρόοδος γκρεμιζόταν. Απλά δεν δούλευε.

Κάποια στιγμή το 2010, τα κινητά τηλέφωνα άρχισαν να γίνονται πιο δημοφιλή και τα πάντα άλλαξαν. Η έντονη παρουσία των κοινωνικών δικτύων, των συνεχών άμεσων μηνυμάτων, και η ικανότητα των τηλεφωνικών εταιριών (συνεπώς του κράτους) να καταγράφουν κάθε κίνηση του χρήστη ενός κινητού άλλαξε για πάντα τον τρόπο με τον οποίο απειλούμαστε. Όλη η δουλειά που είχε γίνει με σκοπό την ασφάλεια των υπολογιστών πήγε πίσω σε βάθος δεκαετιών: τα κινητά τηλέφωνα βασίζονται σε μία τελείως διαφορετική αρχιτεκτονική από ότι οι υπολογιστές, οδηγώντας στην μείωση του ποσοστού ελέγχου που έχουν οι χρήστες, και η άφιξη μη-δεσμευτικών αδειών στις εφαρμογές έχει κάνει την ιδέα ιδιωτικότητας ενός κινητού σχεδόν γελοία.

Μέσα σε αυτές τις συνθήκες δημιουργήθηκε το Signal από τον αναρχικό “κρυπτοπάνκη” Μόξι Μάρλινσπαικ, ο οποίος άρχισε να δουλεύει πάνω σε λογισμικό το οποίο θα έφερνε την end-to-end κρυπτογράφηση με Forward Secrecy στα κινητά τηλέφωνα, επεξεργαζόμενος την ιδέα ότι η

μαζική παρακολούθηση θα μπορούσε να αντιμετωπιστεί με μαζική κρυπτογράφηση. Το Signal σχεδιάστηκε ώστε να είναι χρήσιμο, όμορφο και ασφαλές. Ο Μόξι συμφώνησε να δουλέψει μαζί με τεχνολογικούς κολοσσούς όπως η WhatsApp, το Facebook, η Google και το Skype, ώστε να αναπτύξει το κρυπτογραφικό πρωτόκολλο του Signal και σε εκείνες τις πλατφόρμες.

“Η μεγάλη νίκη για εμάς θα είναι όταν δισεκατομμύρια άνθρωποι θα χρησιμοποιούν το WhatsApp και δεν θα γνωρίζουν ότι είναι κρυπτογραφημένο” – Μόξι Μάρλινσπαικ

Είναι απολύτως κατανοητό πως τα αναρχικά θα αποθέσουν την εμπιστοσύνη τους στο Signal – μία μη-κερδοσκοπική δομή που διαχειρίζεται ένας αναρχικός – έναντι μίας μεγάλης τεχνολογικής εταιρίας, της οποίας το κύριο μοντέλο εργασίας είναι η καλλιέργεια και πώληση προσωπικών δεδομένων των χρηστών της. Επίσης το Signal έχει κάποια πλεονεκτήματα έναντι όλων των άλλων εφαρμογών όπως: ελεύθερο λογισμικό (άρα μπορεί να τεθεί υπό την κριτική των χρηστών της), κρυπτογράφηση των μεταδεδομένων, αποθήκευση όσα λιγότερων δεδομένων του χρήστη γίνεται και προσφορά πολλών χρήσιμων εργαλείων όπως τα εξαφανιζόμενα μηνύματα και η επιβεβαίωση ενός κωδικού ασφαλείας με σκοπό την φύλαξη των συζητήσεων από τρίτα πρόσωπα.

Το Signal έχει λάβει παγκόσμια αναγνώριση από ειδικούς του τομέα της ασφάλειας, ακόμα και στήριξη από τον ‘Εντουαρντ Σνόουντεν, πληροφοριοδότη της NSA, και μεγάλους τίτλους από την αναγνωρισμένη Electronic Founder Foundation. Το 2014, διέρρευσαν έγγραφα από την NSA τα οποία περιέγραφαν το Signal ως “μεγάλη απειλή” για εκείνη (καθώς δουλειά της είναι να γνωρίζει τα πάντα για όλα). Προσωπικά, εμπιστεύομαι την κρυπτογράφηση του.

Αλλά το Singal προστατεύει μόνο ένα πράγμα, και αυτό είναι η επικοινωνία σου όσο αυτή «ταξιδεύει» ανάμεσα στην συσκευή σου και μια άλλη συσκευή. Αυτό είναι μεν πολύ καλό, αλλά είναι μόνο ένα μέρος μίας στρατηγικής ασφάλειας. Γι’ αυτό είναι σημαντικό όταν μιλάμε για ασφάλεια, να ξεκινάμε με το **Threat Modeling** (μοντέλο απειλής). Οι πρώτες ερωτήσεις που πρέπει να τεθούν για οποιαδήποτε στρατηγική ασφάλειας είναι *ποιος* είναι ο αναμενόμενος εχθρός, *τι* προσπαθεί να απομονώσει, και *πως* θα προσπαθήσει να το κάνει.

Η βασική ιδέα είναι ότι τα πράγματα και οι τεχνικές είναι μόνο ασφαλείς ή ανασφαλείς σχετικά με το είδος επίθεσης που περιμένεις να δεχθείς. Για παράδειγμα, μπορεί να έχεις τα δεδομένα σου δεσμευμένα με στερεά κρυπτογράφηση και τον πιο ισχυρό κωδικό, αλλά αν ο εισβολέας έχει την πρόθεση να σε βασανίσει μέχρι να του δώσεις αυτά τα δεδομένα, δεν έχει ιδιαίτερη σημασία πόσο ασφαλή είναι.

Για τον σκοπό αυτής της μπροσούρας, θα πρότεινα ένα επιτυχημένο στην πράξη μοντέλο απειλής το οποίο ασχολείται με δύο τύπους εχθρών. Ο πρώτος τύπος είναι παγκόσμιες υπηρεσίες πληροφοριών ή δυνατοί χάκερς που ασχολούνται με την μαζική παρακολούθηση και τον αφούγκρασμα συζητήσεων. Ο δεύτερος τύπος είναι αστυνομικές υπηρεσίες που δρουν σε μέρη ελεγχόμενα από το Καναδικό ή Αμερικανικό κράτος και ασχολούνται με την στοχευμένη παρακολούθηση αναρχικών. Για την αστυνομία, οι βασικές τεχνικές παρακολούθησης περιέχουν την παρακολούθηση των λιστών ηλεκτρονικής αλληλογραφίας και των μέσων κοινωνικής δικτύωσης, το να στέλνουν ασφαλίτες σε εκδηλώσεις, και τους απλούς πληροφοριοδότες. Στις περιόδους που έχουν περισσότερη χρηματοδότηση, ή όταν τα δίκτυά μας παίρνουν μεγαλύτερη προτεραιότητα, αρχίζουν να χρησιμοποιούν πιο αναβαθμισμένες τεχνικές όπως την τοποθέτηση ενός ασφαλίτη σε ένα πολιτικό χώρο ή οργάνωση για ένα μεγάλο χρονικό διάστημα, συχνή ή συνεχή φυσική παρακολούθηση (μαζί με προσπάθειες ανακάλυψης κωδικών), τοποθέτηση κοριών, παρεμβολή σε συζητήσεις (μέσω ηλεκτρονικών συσκευών) και επιδρομές σε σπίτια όπου όλες οι συσκευές του σπιτιού ξηλώνονται και μπαίνουν κάτω από το μικροσκόπιο.

Πρέπει να τονίσω πως πολλές Ευρωπαϊκές περιφέρειες υλοποιούν **νόμους για την παράδοση κωδικών**, οι οποίοι νομικά αναγκάζουν ατομικότητες να παραδώσουν τους κωδικούς τους σε μορφές εξουσίας (όπως η αστυνομία) κάτω από συγκεκριμένες συνθήκες, αλλιώς θα προχωρήσουν σε προφυλάκιση αυτών των ατομικοτήτων. Ίσως να είναι θέμα χρόνου, αλλά για την ώρα στον Καναδά και στις ΗΠΑ δεν είμαστε αναγκασμένα να κάνουμε κάτι τέτοιο, με εξαίρεση την συνθήκη που θα περάσουμε τα σύνορα.

Αν η συσκευή σου βρίσκεται σε κίνδυνο με έναν καταγραφέα κωδικών ή άλλο επικίνδυνο λογισμικό, δεν έχει σημασία πόσο ασφαλής είναι η επικοινωνία σου μέσω αυτού. Αν αράζεις με ένα ρουφιάνο ή ένα ασφαλίτη δεν έχει σημασία αν θα βγάλεις την μπαταρία από το κινητό σου και μιλήσεις σε μία πλατεία. Η ασφάλεια συσκευών και η κουλτούρα της ασφάλειας είναι δύο έννοιες που δεν αναλύονται σε αυτήν την μπροσούρα.

Επίσης είναι άξιο να αναφερθεί ότι το Signal δεν είναι σχεδιασμένο για ανωνυμία. Ο λογαριασμός σου στο Signal έχει συνδεθεί με τον αριθμό του κινητού σου, άρα εκτός και αν συνδέσεις τον λογαριασμό σου με μία SIM μίας-χρήσης ή έναν αριθμό μίας-χρήσης που βρήκες στο διαδίκτυο, δεν είσαι ανώνυμο. Αν χάσεις τον έλεγχο του αριθμού κινητού τηλεφώνου που έχει συνδεθεί με τον λογαριασμό σου στο Signal, κάποιο άλλο άτομο θα μπορούσε να μπει στον λογαριασμό σου. Για αυτό είναι πολύ σημαντικό αν χρησιμοποιήσεις έναν ανώνυμο αριθμό για να συνδεθείς, να ενεργοποιήσεις το “registration lock” στις ρυθμίσεις.

Κυρίως για λόγους ασφαλείας, το Signal έχει μετατραπεί στο κύριο μέσο επικοινωνίας στους αναρχικούς χώρους τα τελευταία 4 χρόνια, σβήνοντας οποιοδήποτε άλλο ανταγωνιστικό μέσο. Όμως το ίδιο το Signal επηρεάζει τον τρόπο με τον οποίο τα αναρχικά οργανώνονται και αυτό δεν συζητιέται αρκετά.

Η Δημοτικότητα του Signal

“Το Signal είναι χρήσιμο μέχρι το σημείο που αντικαταστεί λιγότερο ασφαλείς μορφές επικοινωνίας στο διαδίκτυο, αλλά γίνεται επικίνδυνο… όταν αντικαταστεί την επικοινωνία πρόσωπο με πρόσωπο.” - Συνεργάτης

Οι περισσότερες κοινωνικές επιπτώσεις του Signal δεν έχουν να κάνουν συγκεκριμένα με την εφαρμογή καθ’ αυτή. Είναι οι επιπτώσεις που δημιουργήθηκαν μέσω της συνεχούς μετακίνησης των επικοινωνιών μας, της προσωπικής μας έκφρασης, των οργανωμένων δράσεων, και όλων των άλλων πραγμάτων σε διαδικτυακές πλατφόρμες και η παρεμβολή οθονών σε αυτές. Αλλά κάτι που συνειδητοποίησα καθώς μελετούσα τις απαντήσεις των ερωτηματολογίων είναι ότι πριν από το Signal, γνώριζα αρκετά άτομα που διαφωνούσαν με την χρήση κινητών τηλεφώνων (συγκεκριμένα smartphones) για λόγους ασφαλείας αλλά και κοινωνικούς. Όταν το Signal έδωσε απαντήσεις σε προβληματισμούς αναφορικά με το θέμα της ασφάλειας, αυτή η διαφωνία κατέρρευσε σημαντικά. Σήμερα, τα περισσότερα από αυτά τα άτομα έχουν κινητά τηλέφωνα, είτε επειδή πείστηκαν να χρησιμοποιούν το Signal είτε επειδή γεννήθηκε η επιτακτική ανάγκη χρήσης τηλεφώνων ώστε να μείνουν συνδεδεμένα με τους αναρχικούς χώρους. Το Signal έπαιξε τον ρόλο εξοικείωσης με τα κινητά τηλέφωνα για κάποια αναρχικά.

Από την άλλη όμως, το Signal δρα ως μείωση ζημιάς για κάποια από εμάς που ήμασταν ήδη παγιδευμένα στον κόσμο των κινητών τηλεφώνων, και αυτό είναι καλό. Είμαι χαρούμενο βλέποντας άτομα που κοινωνικοποιούνταν και οργανώνονταν πολιτικά κυρίως σε μη-κρυπτογραφημένες πλατφόρμες όπως το Facebook να αλλάζουν πλατφόρμα και να χρησιμοποιούν το Signal. Στην δικιά μου ζωή, η ομαδική συνομιλία έχει αντικαταστήσει τις “μικρές λίστες ηλεκτρονικής αλληλογραφίας” και είναι αρκετά χρήσιμη για την οργάνωση πραγμάτων με φίλα μου ή για τον διαμοιρασμό συνδέσμων. Στις απαντήσεις που μάζεψα από τα ερωτηματολόγια, οι ομαδικές συνομιλίες του Signal που είχαν μεγαλύτερη αξία για τα περισσότερα άτομα, ή τουλάχιστον ήταν οι λιγότερο ενοχλητικές, ήταν αυτές που είναι μικρές, οργανωμένες γύρω από ένα συγκεκριμένο θέμα και πρακτικές. Το Signal επίσης μπορεί να αποτελέσει ένα δυνατό εργαλείο για την κυκλοφορία της πληροφορίας άμεσα και με ασφάλεια, σχετικά με μία κατάσταση που χρειάζεται άμεση απόκριση. Αν η οργάνωση πραγμάτων που έχει ως κέντρο το Facebook έχει στρέψει πολλά αναρχικά στο να πιστέψουν ότι δεν μπορεί να

υπάρξει η οργάνωση χωρίς το στοιχείο της έκπληξης, το Signal έχει περισώσει αυτήν την ιδέα, και είμαι ευγνώμων για αυτό.

Αποτυχίες του Signal

Αρχικά φαντάστηκα αυτήν την μπροσούρα ως μία μικρή σειρά κωμικών χρονογραφημάτων που σχεδίαζα να ονομάσω “Signal Fails”, ελάχιστα βασισμένο στο βιβλίο *Come Hell or High Water: A Handbook on Collective Process Gone Awry*. Από ό,τι φαίνεται είναι δύσκολο να ζωγραφίσεις ενδιαφέρουσες εικόνες που αντιπροσωπεύουν ομιλίες μέσω του Signal και είμαι άθλιο στην ζωγραφική. Συγγνώμη αν το είχα υποσχεθεί σε κάποιο, ίσως στην δεύτερη έκδοση… Όπως και να έχει, θα ήθελα να συμπεριλάβω κάποιες Αποτυχίες του Signal, ως ένα τρόπο να κοροιδέψω εμας (βάζω και τον εαυτό μου μέσα!) και ίσως να προτρέψω ευγενικά τους πάντες να σταματήσουν να είναι τόσο γαμημένα ενοχλητικά.

Μποντ, Τζέιμς Μποντ: Το να έχεις κατεβασμένο το Signal δεν σε κάνει άτρωτο. Δίνεις στον κόσμο λίγη κρυπτογράφηση και αμέσως θα υποβάλουν όλη την λίστα επαφών τους στα πιο ύπουλα πράγματα. Το κινητό σου είναι μία συσκευή εντοπισμού και η εμπιστοσύνη ακόμα χτίζεται. Μίλα με τους ανθρώπους σου σχετικά με ποια πράγματα νιώθεις άνετα να συζητάς μέσω τηλεφώνου και με ποια όχι.

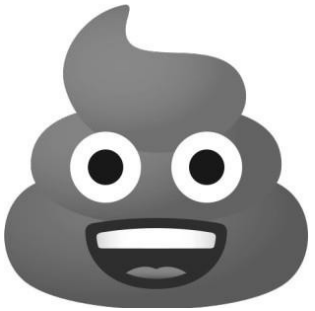
Η σιωπή δεν είναι συναίνεση: Έχεις πάει ποτέ σε μία συνέλευση, που έχετε σχεδιάσει πράγματα με άλλα άτομα, έχετε φτιάξει μία ομαδική συνομιλία στο Signal για να προσδιορίσετε τις λεπτομέρειες και τότε ένα ή δύο άτομα ανταλλάσουν γρήγορα μηνύματα τα οποία αλλάζουν το συλλογικό πλάνο που είχατε φτιάξει στην συνέλευση; Καθόλου σωστό.

Η κόλαση είναι μια ατέλειωτη συνέλευση: Μία ομαδική συνομιλία στο Signal δεν είναι μία συνεχής συνέλευση. Είμαι ήδη υπερβολικά κολλημένο στο κινητό μου, οπότε δεν μου αρέσει όταν μία συνομιλία χτυπάει συνέχεια στο κινητό μου και είναι μία απλή, άσχετη συζήτηση μεταξύ δύο ατόμων ή ή ενημέρωση από ένα άτομο για γεγονότα που είναι άσχετα με τον σκοπό της ομαδικής συνομιλίας. Το εκτιμώ όταν οι συζητήσεις έχουν αρχή και τέλος.

Χρειάζεται Μία Αρχική: Αυτό είναι κάτι που μισώ πάνω από όλα. Ίσως λόγω των μέσων κοινωνικής δικτύωσης, κάποια από εμάς έχουν συνηθίσει την είσπραξη πληροφοριών μέσω της επιμέλειας μιας πλατφόρμας. Αλλά το Signal δεν είναι μέσο κοινωνικής δικτύωσης, πάλι καλά. Οπότε πρόσεχε όταν μία μεγάλη ομαδική συνομιλία στο Signal γίνεται Η ΑΡΧΙΚΗ ΣΟΥ, βρίσκεσαι σε κίνδυνο. Αυτό σημαίνει πως όταν δεν είσαι στο κινητό σου και δεν του δίνεις σημασία, θα χάσεις όλες τις σημαντικές πληροφορίες, όπως εκδηλώσεις που πλησιάζουν, άτομα που αλλάζουν τις αντωνυμίες τους, ή μεγάλες συζητήσεις που οδηγούν σε τσακωμούς. Τα άτομα ξεχνούν την ύπαρξή σου και τελικά, εξαφανίζεσαι. Σκότωσε ΤΗΝ ΑΡΧΙΚΗ ΣΟΥ.

Ο ψεύτης βοσκός που φώναζε λύκος: δηλαδή, το πρόβλημα με το κουμπί πανικού. Αράζεις σε μία ομαδική στο Signal με όλα τα “εγκληματικά” φίλα σου και όλους τους πραγματικούς αριθμούς τηλεφώνων τους, όταν ξαφνικά κάποιο άτομο τρώει προσαγωγή επειδή έκλεψε ή κάτι παρόμοιο και **έκπληξη** το κινητό του δεν είναι κρυπτογραφημένο! Όλα τα άτομα φρικάρουν και βγαίνουν από την ομαδική, αλλά είναι πολύ αργά επειδή αν οι μπάτσοι επεξεργάζονται το κινητό αυτή τη στιγμή, μπορούν να δουν ποια άτομα έφυγαν από την ομαδική και το φακέλωμα έχει γίνει ήδη. Γουα-γουα.

Αποστολή Φάντασμα: Κάποιο δημιούργησε μία ομαδική στο Signal για τον συντονισμό ενός συγκεκριμένου, περιορισμένου χρόνου γεγονότος. Το γεγονός έχει λήξει, αλλά κανένα δεν θέλει να βγει από την ομαδική. Κάπως περίεργα, αυτό το συγκεκριμένο συνοθήλευμα ατόμων είναι τώρα η ΚΥΡΙΑ ΣΥΝΕΛΕΥΣΗ που έχει αναθέσει στον εαυτό της να παίρνει αποφάσεις για τα πάντα – για πάντα.



Με βλέψη τις κοινές πρακτικές

Αν νόμιζες ότι αυτός ήταν ένας οδηγός για καλύτερες πρακτικές για το Signal ή για την επικοινωνία μέσω μηνυμάτων, συγγνώμη που κατάφερες να φτάσεις μέχρι εδώ για να συνειδητοποιήσεις ότι δεν πρόκειται περί αυτού. Αυτή η μπροσούρα στοχεύει περισσότερο στην ρητορική “πρέπει να μιλήσουμε για το Signal”. Πιστεύω πραγματικά στην ανάπτυξη κοινών πρακτικών για συγκεκριμένες περιστάσεις και προτείνω να ξεκινήσουμε αυτήν την συζήτηση αποκλειστικά στα δίκτυά μας. Σχετικά με αυτό, έχω κάποιες προτάσεις.

Υπάρχουν κάποια εμπόδια σχετικά με τις κοινές πρακτικές. Κάποια άτομα δεν έχουν Signal. Αν αυτό είναι λόγω του ότι χτίζουν σχέσεις χωρίς την χρήση κινητών, το μόνο που έχω για αυτά τα άτομα είναι σεβασμός. Αν αυτό είναι επειδή περνάνε όλη την μέρα τους στο Facebook αλλά το Signal είναι “πολύ δύσκολο να το μάθεις”, δεν το χάβω. Αν μη τι άλλο, το Signal είναι εύκολο να εγκατασταθεί και να χρησιμοποιηθεί από το οποιοδήποτε με ένα κινητό και σύνδεση σε κάποιο δίκτυο.

Επίσης διαφωνώ με την Οργουελιανή μοιρολατρία που κρίνει την κρυπτογράφηση άχρηστη: “Οι μπάτσοι ξέρουν ήδη τα πάντα!” Είναι ακραία αποδυναμωτικό να κοιτάμε με αυτόν τον τρόπο το κράτος, και ευτυχώς αυτή η άποψη δεν είναι αληθινή – η αντίσταση δεν είναι μάταιη ακόμα. Η CSEC (υπηρεσία ασφάλειας του Καναδά) και η NSA έχουν εφιαλτικές δυνατότητες, συμπεριλαμβανομένων αυτών που δεν γνωρίζουμε ακόμα. Αλλά υπάρχουν επαρκείς αποδείξεις ότι η κρυπτογράφηση βάζει εμπόδια σε αστυνομικές έρευνες, για αυτό οι κυβερνήσεις προσπαθούν να περνάνε νόμους που αντικρούουν αυτά τα εργαλεία.

Ίσως το μεγαλύτερο εμπόδιο στις κοινές πρακτικές είναι η γενική έλλειψη του “εμείς” – μέχρι ποιο όριο είμαστε υπεύθυνα για οποιοδήποτε, και σε ποιο ακριβώς; Πώς ξεκινάμε να χτίζουμε ηθικούς, κοινούς κοινωνικούς «κανόνες»; Τα περισσότερα αναρχικά συμφωνούν ότι είναι λάθος να ρουφιανεύουμε, για παράδειγμα, αλλά πώς φτάσαμε μέχρι εδώ; Θεωρώ πως αυτός ο χυδαίος, ελευθεριακός ατομικισμός επηρεάζει τον αναρχισμό και μετατρέπει την αναζήτηση “προσδοκιών” σε ένα ταμπού ζήτημα προς συζήτηση. Αλλά αυτό είναι θέμα για μία άλλη μπροσούρα.

Μερικές Προτάσεις για Καλύτερες Πρακτικές

1. *Διατήρησε το από κοντά* – Όπως ένας συνεργάτης μου το έθεσε, “Η επικοινωνία δεν είναι απλά ο διαμοιρασμός πληροφοριών¨. Η δια ζώσης επικοινωνία χτίζει σχέσεις, συμπεριλαμβανομένης της εμπιστοσύνης, και παραμένει ο πιο ασφαλής τρόπος επικοινωνίας.

2. *Άσε τις ηλεκτρονικές συσκευές σου στο σπίτι* – τουλάχιστον κάποιες φορές; Ειδικά αν πας να περάσεις τα σύνορα όπου μπορεί να σε αναγκάσουν να αποκρυπτογραφήσεις τα δεδομένα σου. Αν χρειάζεσαι ένα κινητό όταν ταξιδεύεις, αγόρασε ένα τηλέφωνο μόνο για ταξίδια με τα φίλα σου το οποίο δεν θα περιέχει ευαίσθητα δεδομένα, ούτε την λίστα επαφών σου.

3. *Ασφάλισε τις συσκευές σου* – Οι περισσότερες συσκευές (κινητά τηλέφωνα και υπολογιστές) έχουν πια την επιλογή της πλήρους κρυπτογράφησης του δίσκου. Η κρυπτογράφηση είναι τόσο καλή όσο και ένας κωδικός και προστατεύει τα δεδομένα σου “όταν κοιμούνται”, για παράδειγμα όταν η συσκευή σου είναι απενεργοποιημένη ή τα δεδομένα σου δεν χρησιμοποιούνται από άλλα προγράμματα. Η οθόνη κλειδώματος σου προσφέρει μερική προστασία όταν η συσκευή σου είναι ενεργοποιημένη, αλλά μπορεί να παρακαμφθεί από ένα έμπειρο εισβολέα. Κάποια λειτουργικά συστήματα σε αναγκάζουν να χρησιμοποιήσεις τον ίδιο κωδικό για την κρυπτογράφηση και για την οθόνη κλειδώματος, το οποίο δεν είναι καθόλου πρακτικό καθώς θα αναγκάζεσαι να πληκτρολογείς ένα μεγάλο κωδικό 25 φορές την ημέρα (κάποιες φορές κάτω από την επίβλεψη περίεργων ματιών ή καμερών ασφαλείας).

4. *Απενεργοποίησε τις συσκευές σου* – Αν αφήσεις την συσκευή σου χωρίς επίβλεψη ή πας για ύπνο, απενεργοποίησέ την. Αγόρασε ένα φθηνό ρολόι με αφύπνιση. Αν γίνει επιδρομή στο σπίτι σου το βράδυ θα είσαι ευγνώμων που θα το έχεις αγοράσει. Αν η συσκευή σου είναι απενεργοποιημένη και κρυπτογραφημένη με ένα δυνατό κωδικό όταν κατασχεθεί, οι μπάτσοι δεν έχουν πολλές ελπίδες να το παραβιάσουν. Αν θες να το πας ένα βήμα πιο πέρα, απόκτησε ένα αξιοπρεπές χρηματοκιβώτιο και κλείδωσε τις συσκευές σου μέσα του όταν δεν τις χρησιμοποιείς, το οποίο θα μειώσει το ρίσκο να παραβιαστούν μέσω φυσικής παρουσίας.

5. *Θέσε τα όριά σου* – Έχουμε διαφορετική αντίληψη πάνω στο τι αποτελεί ασφαλές θέμα να συζητηθεί μέσω τηλεφώνου και τι όχι. Συζήτησε και ανάπτυξε συλλογικά όρια και όταν υπάρχει διαφωνία, σεβάσου τα όρια των άλλων ακόμα και αν θεωρείς ότι το θέμα είναι ασφαλές προς συζήτηση.

6. *Συμφωνήστε πάνω σε ένα σύστημα εγγύησης* – Αν βρίσκεσαι σε μία ομαδική συνομιλία για ευαίσθητα θέματα, αναπτύξτε μία συλλογική θέση πάνω στα πράγματα που αποτελούν δυνατή εγγύηση για ένα νέο άτομο που θέλει να πάρει μέρος. Ζώντας σε μία περίοδο όπου τα αναρχικά φορτώνονται με το κατηγορητήριο των εγκληματικών οργανώσεων, ασυνεννοησίες όπως αυτή μπορεί να στείλει άτομα στην φυλακή.

7. *Ρώτα πρώτα* – Αν θέλεις να προσθέσεις ένα άτομο σε μία ομαδική συνομιλία, συνεπώς αποκαλύπτοντας τον αριθμό τηλεφώνου του σε όλα τα υπόλοιπα άτομα, πάρε την συναίνεση του ατόμου και όλης της ομαδικής συνομιλίας πρώτα.

8. *Μείωση λήψης συλλογικών αποφάσεων μέσω μηνυμάτων* – Εξέτασε την περίπτωση του να παίρνονται αποφάσεις πέρα από τις αποφάσεις “ναι ή όχι” στις συνελεύσεις, αν είναι δυνατό. Βάσει της δικιάς μου εμπειρίας, το Signal καταργεί την οριζοντιότητα της λήψης αποφάσεων.

9. *Ξεκάθαρος σκοπός* – Ιδανικά, μία ομαδική συνομιλία στο Signal πρέπει να έχει ένα συγκεκριμένο σκοπό. Κάθε νέο άτομο το οποίο μπαίνει σε μία ομαδική πρέπει να έχει ξεκάθαρη γνώση αυτού του σκοπού. Αν ο σκοπός έχει επιτευχθεί, αποχώρησε από την ομαδική και διέγραψε την από το κινητό σου.

10. *Εξαφανιζόμενα μηνύματα* – Πολύ χρήσιμο για την οργάνωση μηνυμάτων. Ξεκινώντας από 5 δευτερόλεπτα μέχρι 1 εβδομάδα, τα Εξαφανιζόμενα Μηνύματα μπορούν να εφαρμοστούν επιλέγοντας το εικονίδιο ρολογιού στο πάνω μέρος του πλαισίου μιας συνομιλίας. Πολλά άτομα χρησιμοποιούν την συνηθισμένη επιλογή 1 εβδομάδας για όλα τα μηνύματα, ανεξαρτήτως αν η συνομιλία είναι ευαίσθητη ή μη. Επίλεξε τον χρόνο εξαφάνισης βασισμένο στο μοντέλο απειλής. Αυτό σε προστατεύει κάπως αν το άτομο με το οποίο επικοινωνείς χρησιμοποιεί όχι-και-τόσο ιδανικές πρακτικές ασφάλειας για το κινητό του.

11. *Επιβεβαίωσε τους αριθμούς ασφαλείας* – Αυτή είναι η καλύτερη προστασία που έχεις έναντι ενός ατόμου που θα προσπαθήσει να παρεμβάλει στην συνομιλία. Είναι αρκετά απλό να το κάνεις και ευκολότερο από κοντά – άνοιξε την συνομιλία που έχεις με το άτομο το οποίο θες να επιβεβαιώσεις και πήγαινε στις Ρυθμίσεις Συνομιλίας > Δες τον αριθμό ασφαλείας (Conversation Settings > View safety number) και σκάναρε τον κωδικό QR ή σύγκρινε τους αριθμούς. Τα περισσότερα άτομα που απάντησαν στο ερωτηματολόγιο διάλεξαν το “Θα έπρεπε να το κάνω, αλλά δεν το κάνω”. Εκμεταλλεύσου τις μεγάλες συγκεντρώσεις ώστε να επιβεβαιώσεις τις επαφές σου. Είναι εντάξει το να είσαι φυτό!

12. *Ενεργοποίησε το Κλείδωμα Εγγραφής (Registration Lock)* – Ενεργοποίησε αυτήν την δυνατότητα στις Ρυθμίσεις Ασφαλείας του Signal έτσι ώστε αν κάποιο άτομο μπορέσει ποτέ να χακάρει τον αριθμό τηλεφώνου που έχει χρησιμοποιηθεί για να εγγραφείς στην εφαρμογή, θα είναι αναγκασμένο να βρει το PIN σου για να χρησιμοποιήσει τον λογαριασμό σου. Αυτό είναι ιδιαίτερα σημαντικό για ανώνυμους λογαριασμούς στο Signal με αριθμούς μίας χρήσης, καθώς είναι σχεδόν σίγουρο πως κάποιο άλλο θα προσπαθήσει να χρησιμοποιήσει ξανά αυτόν τον αριθμό.

13. *Απενεργοποίησε την προεπισκόπηση μηνυμάτων* – Μην επιτρέψεις τα μηνύματά σου να εμφανίζονται στην οθόνη κλειδώματος σου. Στην συσκευή μου, έπρεπε να το ρυθμίσω αυτό στις ρυθμίσεις του κινητού (και όχι στις ρυθμίσεις του Signal) πηγαίνοντας στο Επιλογές Οθόνης Κλειδώματος > Απόκρυψη Ευαίσθητου Περιεχομένου (Lock Screen Preferences > Hide Sensitive Content).

Συμπερασματικά

Ξεκίνησα αυτήν την μπροσούρα με σκοπό να αποτυπώσω και να μαζέψω υλικό πάνω στην επιρροή που έχει αφήσει το Signal στα αναρχικά δίκτυα στις ΗΠΑ και στον Καναδά, μέσω του φακού της ασφάλειας και της κοινωνικής οργάνωσης. Κάνοντάς το, πιστεύω πως έφερα στην επιφάνεια κοινές ανησυχίες που έχουμε όλα, κυρίως όσον αφορά μεγάλες ομαδικές συνομιλίες στο Signal, και συγκέντρωσα μερικές προτάσεις προς διαμοιρασμό. Συνεχίζω να επιμένω πως τα κινητά τηλέφωνα κάνουν περισσότερη ζημιά παρά καλό στις ζωές μας και στα πράγματα που καλούμαστε να αντιμετωπίζουμε, επειδή είναι σημαντικό για εμένα να ακουστεί. Πρέπει να διατηρήσουμε και να χτίσουμε άλλους τρόπους οργάνωσης, ειδικά εκτός του διαδικτύου, και για την ποιότητα της ζωής μας και για το εγχείρημα της ασφάλειας. Ακόμα και αν συνεχίσουμε να χρησιμοποιούμε τα κινητά, είναι επικίνδυνο οι συζητήσεις μας να γίνονται συγκεντρωτικές. Αν οι σέρβερ του Signal έπεφταν σήμερα, ή του riseup.net, ή του Protonmail, φανταστείτε πόσο καταστροφικό θα ήταν αυτό για τα δίκτυά μας. Αν τα αναρχικά εξελιχθούν ποτέ σε μία μεγάλη απειλή για το κατεστημένο, θα έρθουν για εμάς και για τις υποδομές μας χωρίς έλεος, και δεν θα τους σταματήσουν οι “νομικές προστασίες” στις οποίες στηριζόμαστε. Καλώς ή κακώς, θεωρώ πως αυτό το σενάριο είναι πιθανό στην περίοδο που ζούμε, συνεπώς θα έπρεπε να είμαστε προετοιμασμένα για οτιδήποτε.

Τα άτομα της τεχνολογίας ανάμεσά μας πρέπει να συνεχίσουν να πειραματίζονται με άλλα πρωτόκολλα, λογισμικά και λειτουργικά συστήματα, και να τα μοιράζονται αν είναι χρήσιμα. Τα άτομα που δεν χρησιμοποιούν κινητά πρέπει να συνεχίσουν να μην τα χρησιμοποιούν και να βρουν άλλους τρόπους να ευημερούν εκτός διαδικτύου. Για τα υπόλοιπα από εμάς, ας ελαχιστοποιήσουμε το πόσο είμαστε εγκλωβισμένα από τα κινητά. Μαζί με την ιδιότητα της αντίστασης, πρέπει να χτίσουμε ζωές που αξίζει να ζούμε, με την ποιότητα των σχέσεων που πιθανά φίλα και συντρόφια βρίσκουν ακαταμάχητα συναρπαστική. Ίσως είναι η μόνη ελπίδα που έχουμε.

It feels so 80s" Or early 90s" To be political"
Where are my friends?"

Get off the internet!" (I'll meet you in the street)" Get off the internet!" (Destroy the right wing)"

This is repetitive"But nothing has changed"
Am I crazy?"
Where are my friends?"

(Le Tigre)

signalfails@riseup.net