Comment éviter que son téléphone ne serve la répression de tou·tes

Quelques conseils relativement simples à mettre en oeuvre pour contrer les méthodes les plus courantes des Forces De l'Ordre (FDO) liées au téléphone.

En cas de risque de saisie physique du téléphone

- Chiffre ton téléphone (ou vérifies qu'il est chiffré par défaut) et configure un mot de passe de plusieurs lettres et symboles. Ça n'empêchera probablement pas les FDO de consulter le contenu de ton téléphone, mais ça réduit grandement le risque qu'ils se servent de ton téléphone pour usurper ton identité ou qu'ils y installent un logiciel espion.
- Idéalement, plus tu prends de risque (aller en manif'action est plus "risqué" en ce sens que de tracter pour la CGT devant son entreprise) et plus ça vaut le coup de ne pas avoir de téléphone sur toi ou d'avoir un téléphone le plus vide possible (mais qui peut utiliser Signal pour ne pas utiliser le réseau GSM), soit parce qu'il est dédié à ces activités soit parce que tu le remets à zéro avant chacun de ces activités et qui soit effaçable à distance.
- Dans tous les cas, il est conseillé de sauvegarder régulièrement tes données personnelles pour ne pas avoir peur de les perdre en cas de sasie et pour résister aux pressions des FDO.
- Briefe ton ou ta proche qui sera prévenu·e si tu es placé·e en garde-à-vue pour qu'iel puisse effacer à distance tout ton téléphone (il faut avoir configuré une application comme FindMyDevice) et désactiver le plus vite possible tes applications sensibles (comme Signal et tes mails). À défaut, occupes-t-en dès que tu sors de garde-à-vue ou que tu as de nouveau accès à un ordinateur car si les FDO conservent ton téléphone ils peuvent continuer à s'en servir après la fin de la GAV, de la perquisition ou du contrôle.
- Si les FDO mettent la main sur ton téléphone puis te le rendent, réinitialise-le à zéro pour supprimer la plupart des potentiels logiciels espions qu'ils y auraient installés.

Comment éviter que son téléphone ne serve la répression de tou·tes

Quelques conseils relativement simples à mettre en oeuvre pour contrer les méthodes les plus courantes des Forces De l'Ordre (FDO) liées au téléphone.

En cas de risque de saisie physique du téléphone

- Chiffre ton téléphone (ou vérifies qu'il est chiffré par défaut) et configure un mot de passe de plusieurs lettres et symboles. Ça n'empêchera probablement pas les FDO de consulter le contenu de ton téléphone, mais ça réduit grandement le risque qu'ils se servent de ton téléphone pour usurper ton identité ou qu'ils y installent un logiciel espion.
- Idéalement, plus tu prends de risque (aller en manif'action est plus "risqué" en ce sens que de tracter pour la CGT devant son entreprise) et plus ça vaut le coup de ne pas avoir de téléphone sur toi ou d'avoir un téléphone le plus vide possible (mais qui peut utiliser Signal pour ne pas utiliser le réseau GSM), soit parce qu'il est dédié à ces activités soit parce que tu le remets à zéro avant chacun de ces activités et qui soit effaçable à distance.
- Dans tous les cas, il est conseillé de sauvegarder régulièrement tes données personnelles pour ne pas avoir peur de les perdre en cas de sasie et pour résister aux pressions des FDO.
- Briefe ton ou ta proche qui sera prévenu·e si tu es placé·e en garde-à-vue pour qu'iel puisse effacer à distance tout ton téléphone (il faut avoir configuré une application comme FindMyDevice) et désactiver le plus vite possible tes applications sensibles (comme Signal et tes mails). À défaut, occupes-t-en dès que tu sors de garde-à-vue ou que tu as de nouveau accès à un ordinateur car si les FDO conservent ton téléphone ils peuvent continuer à s'en servir après la fin de la GAV, de la perquisition ou du contrôle.
- Si les FDO mettent la main sur ton téléphone puis te le rendent, réinitialise-le à zéro pour supprimer la plupart des potentiels logiciels espions qu'ils y auraient installés.

À distance sans risque de saisie du téléphone

- Garde ton téléphone à jour, c'est à dire ne repousse jamais une proposition automatique de mettre à jour un logiciel ou le "système" de ton téléphone pour éviter aux FDO de pouvoir exploiter certaines brèches de sécurité.
- Idéalement, plus tu prends de risque (aller en manif'action est plus "risqué" en ce sens que de tracter pour la CGT devant son entreprise) et plus ça vaut le coup de ne pas avoir de téléphone sur toi ou de mettre son téléphone en mode avion ou de retirer la batterie pour éviter que la position de ta carte SIM ne soit enregistrée par les antennes relais. Dans ce cas, évite d'adopter un comportement trop stéréotypé ou trop identique à celui de tes camarades (ne pas éteindre le téléphone au même endroit ni au même moment par exemple).
- Utilise le moins possible les SMS et les appels par le réseau GSM, qui sont très facilement accessibles par les FDO. Utilise plutôt une application de messagerie chiffrée de bout en bout et open source avec une bonne réputation, comme Signal. Pas uniquement pour les conversations sensibles mais tout le temps afin de brouiller les pistes et de ne pas alimenter la surveillance de masse.
- Utilise le moins possible les GAFAM ou à défaut les isoler dans une application Shelter car les FDO peuvent accéder à toutes les données récoltées par les applications commerciales (comme l'historique des positions Google Maps ou les photos partagées sur Messenger).
- Utilise le plus possible un VPN pour tes activités en ligne et le navigateur Tor pour tes activités les plus sensibles.
- Met en place une stratégie personnelle de cloisonnement en ligne et dans la vraie vie, c'est à dire ne donne pas la même identité partout et encore moins la vraie. Continue avec tes camarades à faire attention à ne pas communiquer d'informations sensibles à l'oral en présence d'inconnus ou dans des lieux potentiellement surveillées (comme la plupart des locaux militants publics).
- Evite quoi qu'il en soit de communiquer des informations directement incriminantes même en utilisant les meilleurs applications car les services de renseignement les plus poussés auront toujours une longueur d'avance technologique, même s'ils ne déploient leurs plus gros moyens que pour les enquêtes les plus poussées.

→ Pour des conseils plus poussés, des situations plus spécifiques ou encore pour comprendre ce qui justifie les conseils donnés dans ce tract, la version complète de ce document est sur paris-luttes.info et sur rajcollective.noblogs.org.

À distance sans risque de saisie du téléphone

- Garde ton téléphone à jour, c'est à dire ne repousse jamais une proposition automatique de mettre à jour un logiciel ou le "système" de ton téléphone pour éviter aux FDO de pouvoir exploiter certaines brèches de sécurité.
- Idéalement, plus tu prends de risque (aller en manif'action est plus "risqué" en ce sens que de tracter pour la CGT devant son entreprise) et plus ça vaut le coup de ne pas avoir de téléphone sur toi ou de mettre son téléphone en mode avion ou de retirer la batterie pour éviter que la position de ta carte SIM ne soit enregistrée par les antennes relais. Dans ce cas, évite d'adopter un comportement trop stéréotypé ou trop identique à celui de tes camarades (ne pas éteindre le téléphone au même endroit ni au même moment par exemple).
- Utilise le moins possible les SMS et les appels par le réseau GSM, qui sont très facilement accessibles par les FDO. Utilise plutôt une application de messagerie chiffrée de bout en bout et open source avec une bonne réputation, comme Signal. Pas uniquement pour les conversations sensibles mais tout le temps afin de brouiller les pistes et de ne pas alimenter la surveillance de masse.
- Utilise le moins possible les GAFAM ou à défaut les isoler dans une application Shelter car les FDO peuvent accéder à toutes les données récoltées par les applications commerciales (comme l'historique des positions Google Maps ou les photos partagées sur Messenger).
- Utilise le plus possible un VPN pour tes activités en ligne et le navigateur Tor pour tes activités les plus sensibles.
- Met en place une stratégie personnelle de cloisonnement en ligne et dans la vraie vie, c'est à dire ne donne pas la même identité partout et encore moins la vraie. Continue avec tes camarades à faire attention à ne pas communiquer d'informations sensibles à l'oral en présence d'inconnus ou dans des lieux potentiellement surveillées (comme la plupart des locaux militants publics).
- Evite quoi qu'il en soit de communiquer des informations directement incriminantes même en utilisant les meilleurs applications car les services de renseignement les plus poussés auront toujours une longueur d'avance technologique, même s'ils ne déploient leurs plus gros moyens que pour les enquêtes les plus poussées.

→ Pour des conseils plus poussés, des situations plus spécifiques ou encore pour comprendre ce qui justifie les conseils donnés dans ce tract, la version complète de ce document est sur paris-luttes.info et sur rajcollective.noblogs.org.