Sicurezza per l'informatore/trice

Nel fornire informazioni sensibili, è necessario considerare i rischi per coloro che stanno divulgando informazioni su una terza parte. Tale terza parte può intraprendere azioni di ritorsione contro di voi o SwissLeaks. Rimanere anonimi durante tutto il processo di denuncia è un buon modo per proteggere se stessi e gli altri dalle minacce esterne.

Questo documento tratta i rischi connessi alla trasmissione di informazioni a SwissLeaks. È importante ridurre al minimo questi rischi.

Rischi sociali

Anche se il rischio di hackerare per scoprire la vostra identità è significativo, sono le persone che la circondano a costituire la più grande minaccia per il suo anonimato. Prima di inviare le informazioni, dovete considerare cosa accadrà dopo la divulgazione delle informazioni e le conseguenze nel caso in cui la fuga di notizie diventi pubblica.

Ponetevi le seguenti domande per valutare il vostro rischio: State agendo nell'interesse pubblico o con intento doloso? Le vostre azioni provocheranno una reazione violenta o legale da parte di un gruppo? Altre persone oltre a voi hanno accesso alle informazioni che state per fornire?
Quando queste informazioni arriveranno al pubblico, qualcuno vi farà domande in merito? Siete in grado di far fronte allo stress di un'indagine interna o esterna? Dovreste pensare a come rilasciare i documenti solo dopo aver riflettuto seriamente su questo tipo di domande.

Rischi digitali

L'uso del computer e di Internet lascia tracce. Tracce che possono essere lasciate sul proprio computer, sul computer del destinatario e nel frattempo su molti altri computer. Queste tracce e altre informazioni forensi potrebbero consentire a un investigatore di sapere dove vi trovate e chi siete.

Potete lasciare tracce quando:
● ricercate delle informazioni da trasmettere
● raccogliete delle informazioni da trasmettere
● leggete questo sito web
● ci trasmettete delle informazioni
● nello scambio di dati con i destinatari della vostra richiesta

Con gli strumenti e le conoscenze giuste potete ridurre al minimo il rischio di lasciare impronte digitali e di compromettere il vostro anonimato.

Protezione sociale

Quello che segue è un minimo di misure da adottare per proteggersi nelle interazioni sociali.
● Prima di trasmettere un contributo, non condividete le vostre intenzioni con nessuno.
● Assicuratevi che non vi siano sistemi di monitoraggio o osservatori nel luogo in cui raccogliete e trasmettete le informazioni.
● Cercate di fare in modo che le informazioni da voi fornite non vi identifichino se vi ha accesso una persona diversa dal destinatario previsto.
● Dopo aver trasmesso delle informazioni, non parlatene con nessuno.
● Dopo che la notizia della presentazione è diventata pubblica, fate attenzione a condividere la vostra opinione sulla notizia con chiunque.

Protezione tecnica

A causa della complessità tecnica dei moderni sistemi informatici e delle reti, è difficile essere completamente anonimi. Non è impossibile, ma è complicato. Dovete anche capire che nessuno comprende ogni dettaglio dei sistemi informatici e di rete. Tuttavia, se si attiene rigorosamente alle linee guida riportate di seguito, dovreste essere al sicuro.
● Al momento di raccogliere le informazioni da trasmettere, assicuratevi che non vengano lasciate tracce sui sistemi informatici in grado di identificarle (ad es.: raccogliete i file con una chiavetta USB). Una volta completata la trasmissione, distrugga e smaltisca la chiavetta USB.
● Dovete sapere che "cancellare un file" su quasi tutti i computer non elimina le tracce della presenza dei file da quel computer.
● Vi preghiamo di notare che i metadati possono essere inclusi in alcuni dei dati da lei inviati.
● Consideri la possibilità di rimuovere i metadati con uno strumento adatto a questo scopo.
● Le consigliamo di convertire i dati che ci invia in un formato standard come il PDF.
● Le informazioni devono essere inviate utilizzando il browser anonimo Tor.
● Non conservate copia delle informazioni da voi fornite.
● Non invii le informazioni dal computer fornito dal vostro datore di lavoro (utilizzate un computer diverso).
● Tenete la ricevuta che riceverete e distruggetela quando non vi servirà più.
● Non cercate le informazioni da voi fornite nei motori di ricerca o nei siti di notizie.

Abbastanza sicuro non significa che il vostro anonimato sia garantito. Questo significa che anche gli esperti di computer non dovrebbero essere in grado di determinare in seguito che voi siete stati la fonte della fuga.

Se desiderate capire meglio come operare in sicurezza in questo ambiente digitale

leggete le istruzioni create nell'ambito del progetto Security in a Box (link https://securityinabox.org/en/)