THE JOURNALIST SURVIVAL GUIDE

ANANIMATEDVIDEOGUIDE

Lesson 13
How to Store and Share Encrypted Data

Samir Kassir eyes

Why This Matters
Hard drives are not very well protected by the operating system password mechanism - it is pretty easy to remove a hard disk from a laptop and access it from another computer, similar to how you would access any hard disk you use for back-up or storage. Furthermore, most smaller devices (USBs, laptops, etc.) can be easily misplaced or stolen. To help keep your confidential information safe, you may want to use encryption to secure your most sensitive data.

What is Encryption?
Encryption is a way of using clever mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

To someone who is trying to view an encrypted piece of data without a password or key to unlock this information, this data will appear to be a random series of letters, numbers, and other characters. Storing confidential data can be a risk for you and for the people you work with. Encryption reduces this risk but does not eliminate it. The first step to protecting sensitive information is to reduce how much of it you keep around. Unless you have a good reason to store a particular file, or a particular category of information within a file, you should simply delete it.

Truecrypt
Truecrypt is a tool in which you can create an encrypted storage container to hide all of your sensitive files. Truecrypt functions much like a locked safe for your data, and contains several important features to allow you to design your information security strategy. It offers the possibility of permanently encrypting the whole disk of your computer including all your files, all temporary files created during your work, all programs you have installed and all Windows operating system files. TrueCrypt supports encrypted volumes (sections on a device that can store files separately from the main system) on portable storage devices. It also provides ‹deniability› features, by making its encrypted storage volume appear like other files, such as movies, documents, and music files. You can learn more about Truecrypt here: *https://securityinabox.org/en/truecrypt_main*

GPG4USB
GPG4USB is a simple, lightweight and portable program that lets you encrypt and decrypt text messages and files. GPG4USB is based on public-key cryptography. In this method, each individual must generate her/his own personal key pair. The first key is known as the private (or secret) key. It is protected by a password or passphrase, guarded and never shared with anyone. The second key is known as the public key. This key can be shared with any of your correspondents - and your correspondents can share theirs with you. You can find out more about sharing keys here: *https://securityinabox.org/en/gpg4usb-keysimportexport*

Once you have a correspondent's public key you can begin sending encrypted emails to this person. Only she will be able to decrypt and read your emails, because she is the only person who has access to the matching private key. Similarly, if you send a copy of your own public key to your email contacts and keep the matching private key secret, only you will be able to read encrypted messages from those contacts.

Note: Be mindful that the original, unencrypted versions of your documents and files may still reside on your computer, so both your correspondent and yourself must remember to remove them from computers when necessary.
You can learn more about GPG4USB here: *https://securityinabox.org/en/gpg4usb_portable*

Pidgin with OTR
Pidgin is a free and open source Instant Messaging (IM) client that lets you organize and manage your different (IM) accounts through a single interface. Before you can start using Pidgin you must have an existing IM account, after which you will register that account to Pidgin. For instance, if you have an email account with Gmail, you can use their IM service GoogleTalk with Pidgin. The log-in details of your existing IM account are used to register and access your account through Pidgin.

Note: All users are encouraged to learn as much as possible about the privacy and security policies of their Instant Messaging Service Provider. A helpful resource is TOS-DR.

Off-the-Record (OTR) messaging is a plugin developed specifically for Pidgin. It offers the following privacy and security features:
- Authentication: You are assured the correspondent is who you think it is.
- Deniability: After the chat session is finished, messages cannot be identified as originating from either your correspondent or yourself.
- Encryption: No one else can access and read your instant messages.

You can learn more about Pidgin with OTR here: *https://securityinabox.org/en/pidgin_main*

Produced by:
The SKeyes Center for Media and Cultural Freedom at the Samir Kassir Foundation

The content of the video was prepared with the pro bono assistance of:
The ICT team at the National Democratic Institute

Executive producer: **Maroun Sfeir**
Storyboard creation and animation: **kook creative studio**

Video Consultant: **Andrew Codd**
Translation: **Nour El-Assaad**
Voice over - Arabic: **Rima Khaddaj**
Voice over - English: **Andrew Codd**
Sound recording: **Creative Impact**
Music: **"Mining by Moonlight" by Kevin MacLeod**

This project has been made possible thanks to the support of the **National Endowment for Democracy**.