CRYPTO PARTY

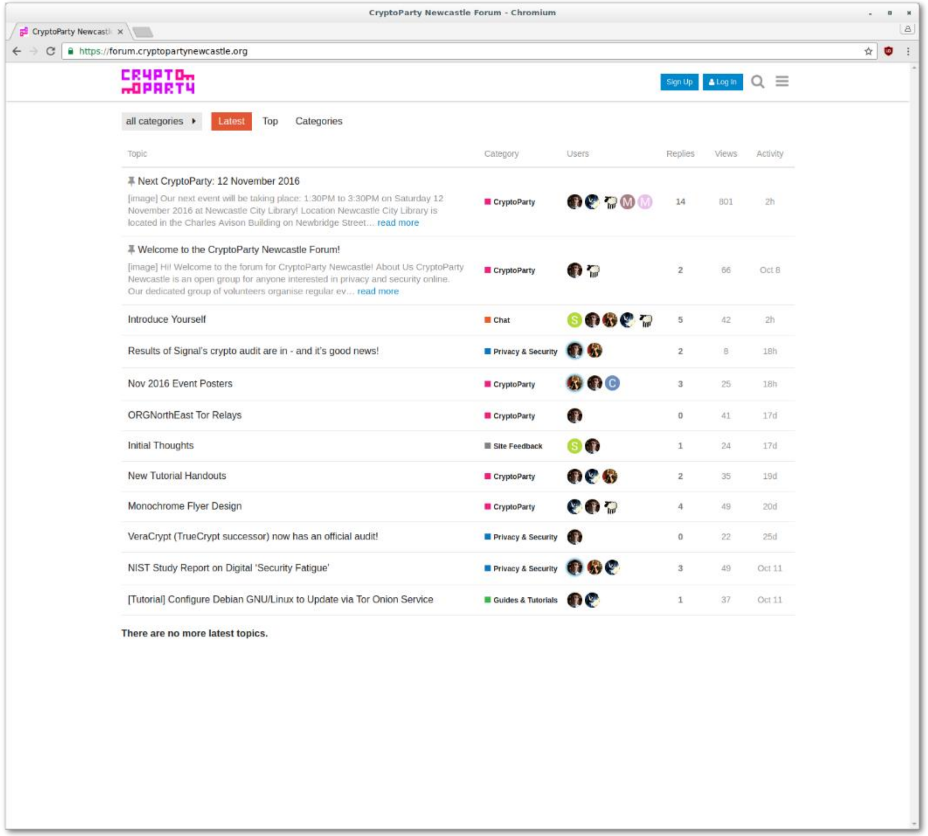
cryptopartynewcastle.org

Topics

- Tor Browser (and TAILS)
- Signal Private Messenger
- Full Disk Encryption
- PGP
- KeePass

CryptoParty Newcastle Forum

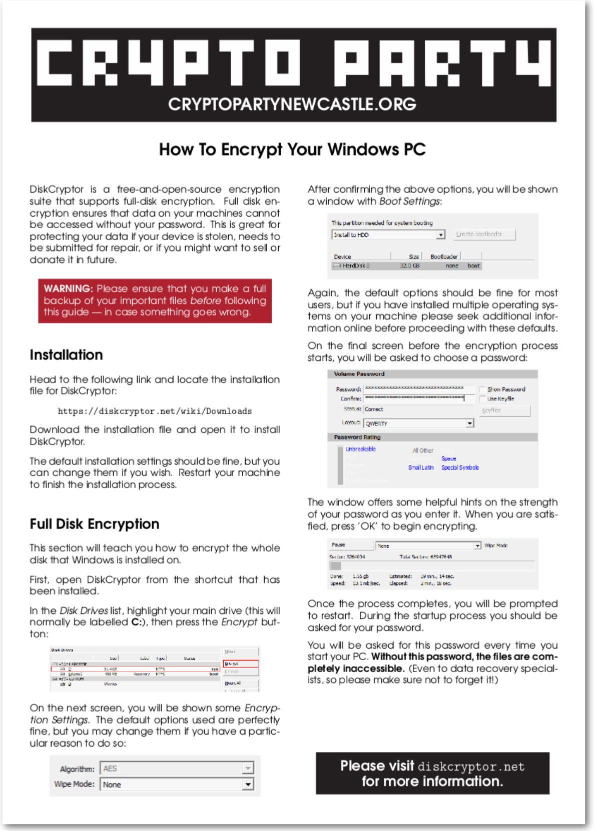
cryptopartynewcastle.org



Topic	Category	Users	Replies	Views	Activity
Next CryptoParty: 12 November 2016 [image] Our next event will be taking place: 1:30PM to 3:30PM on Saturday 12 November 2016 at Newcastle City Library! Location Newcastle City Library is located in the Charles Avison Building on Newbridge Street… read more	CryptoParty	M M	14	801	2h
Welcome to the CryptoParty Newcastle Forum! [image] Hi! Welcome to the forum for CryptoParty Newcastle! About Us CryptoParty Newcastle is an open group for anyone interested in privacy and security online. Our dedicated group of volunteers organise regular ev… read more	CryptoParty		2	66	Oct 8
Introduce Yourself	Chat	S	5	42	2h
Results of Signal's crypto audit are in - and it's good news!	Privacy & Security		2	8	18h
Nov 2016 Event Posters	CryptoParty	C	3	25	18h
ORGNorthEast Tor Relays	CryptoParty		0	41	17d
Initial Thoughts	Site Feedback	S	1	24	17d
New Tutorial Handouts	CryptoParty		2	35	19d
Monochrome Flyer Design	CryptoParty		4	49	20d
VeraCrypt (TrueCrypt successor) now has an official audit!	Privacy & Security		0	22	25d
NIST Study Report on Digital 'Security Fatigue'	Privacy & Security		3	49	Oct 11
[Tutorial] Configure Debian GNU/Linux to Update via Tor Onion Service	Guides & Tutorials		1	37	Oct 11

There are no more latest topics.

Handouts



CRYPTO PARTY
CRYPTOPARTYNEWCASTLE.ORG

How To Encrypt Your Windows PC

DiskCryptor is a free-and-open-source encryption suite that supports full-disk encryption. Full disk encryption ensures that data on your machines cannot be accessed without your password. This is great for protecting your data if your device is stolen, needs to be submitted for repair, or if you might want to sell or donate it in future.

WARNING: Please ensure that you make a full backup of your important files *before* following this guide — in case something goes wrong.

Installation

Head to the following link and locate the installation file for DiskCryptor:

`https://diskcryptor.net/wiki/Downloads`

Download the installation file and open it to install DiskCryptor.

The default installation settings should be fine, but you can change them if you wish. Restart your machine to finish the installation process.

Full Disk Encryption

This section will teach you how to encrypt the whole disk that Windows is installed on.

First, open DiskCryptor from the shortcut that has been installed.

In the *Disk Drives* list, highlight your main drive (this will normally be labelled **C:**), then press the *Encrypt* button:

On the next screen, you will be shown some *Encryption Settings*. The default options used are perfectly fine, but you may change them if you have a particular reason to do so:

Algorithm: AES
Wipe Mode: None

After confirming the above options, you will be shown a window with *Boot Settings*:

This partition needed for system booting
Install to HDD

Device	Size	Bootloader	
HardDisk 0	32.0 GB	none	boot

Again, the default options should be fine for most users, but if you have installed multiple operating systems on your machine please seek additional information online before proceeding with these defaults.

On the final screen before the encryption process starts, you will be asked to choose a password:

Volume Password
Status: Correct
Layout: QWERTY
Password Rating: Unbreakable

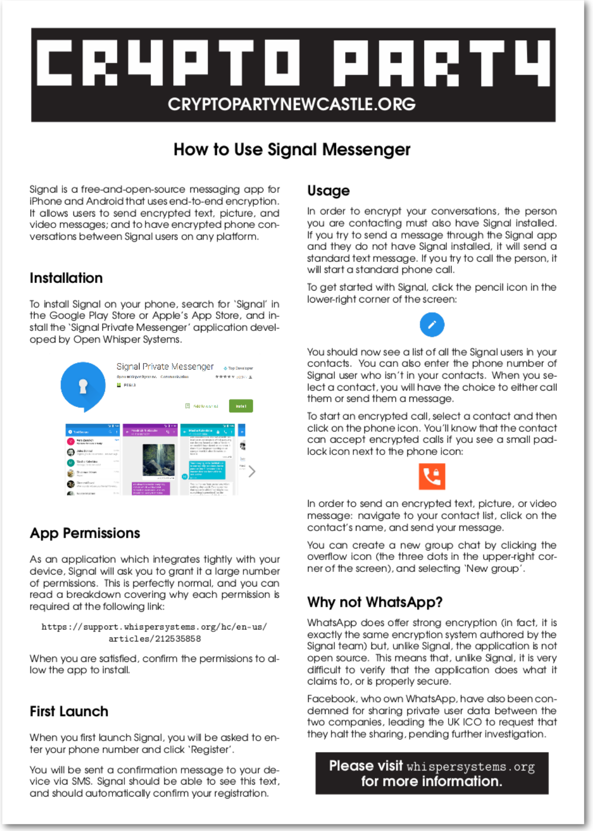
The window offers some helpful hints on the strength of your password as you enter it. When you are satisfied, press 'OK' to begin encrypting.

Wipe Mode: None
Sector: 3264004 Total Sectors: 65947648
Done: 1.55 gb Estimated: 39 min., 14 sec.
Speed: 13.1 mb/sec. Elapsed: 2 min., 18 sec.

Once the process completes, you will be prompted to restart. During the startup process you should be asked for your password.

You will be asked for this password every time you start your PC. **Without this password, the files are completely inaccessible.** (Even to data recovery specialists, so please make sure not to forget it!)

Please visit `diskcryptor.net` **for more information.**



CRYPTO PARTY
CRYPTOPARTYNEWCASTLE.ORG

How to Use Signal Messenger

Signal is a free-and-open-source messaging app for iPhone and Android that uses end-to-end encryption. It allows users to send encrypted text, picture, and video messages; and to have encrypted phone conversations between Signal users on any platform.

Installation

To install Signal on your phone, search for 'Signal' in the Google Play Store or Apple's App Store, and install the 'Signal Private Messenger' application developed by Open Whisper Systems.

App Permissions

As an application which integrates tightly with your device, Signal will ask you to grant it a large number of permissions. This is perfectly normal, and you can read a breakdown covering why each permission is required at the following link:

`https://support.whispersystems.org/hc/en-us/articles/212535858`

When you are satisfied, confirm the permissions to allow the app to install.

First Launch

When you first launch Signal, you will be asked to enter your phone number and click 'Register'.

You will be sent a confirmation message to your device via SMS. Signal should be able to see this text, and should automatically confirm your registration.

Usage

In order to encrypt your conversations, the person you are contacting must also have Signal installed. If you try to send a message through the Signal app and they do not have Signal installed, it will send a standard text message. If you try to call the person, it will start a standard phone call.

To get started with Signal, click the pencil icon in the lower-right corner of the screen:

You should now see a list of all the Signal users in your contacts. You can also enter the phone number of Signal user who isn't in your contacts. When you select a contact, you will have the choice to either call them or send them a message.

To start an encrypted call, select a contact and then click on the phone icon. You'll know that the contact can accept encrypted calls if you see a small padlock icon next to the phone icon:

In order to send an encrypted text, picture, or video message: navigate to your contact list, click on the contact's name, and send your message.

You can create a new group chat by clicking the overflow icon (the three dots in the upper-right corner of the screen), and selecting 'New group'.

Why not WhatsApp?

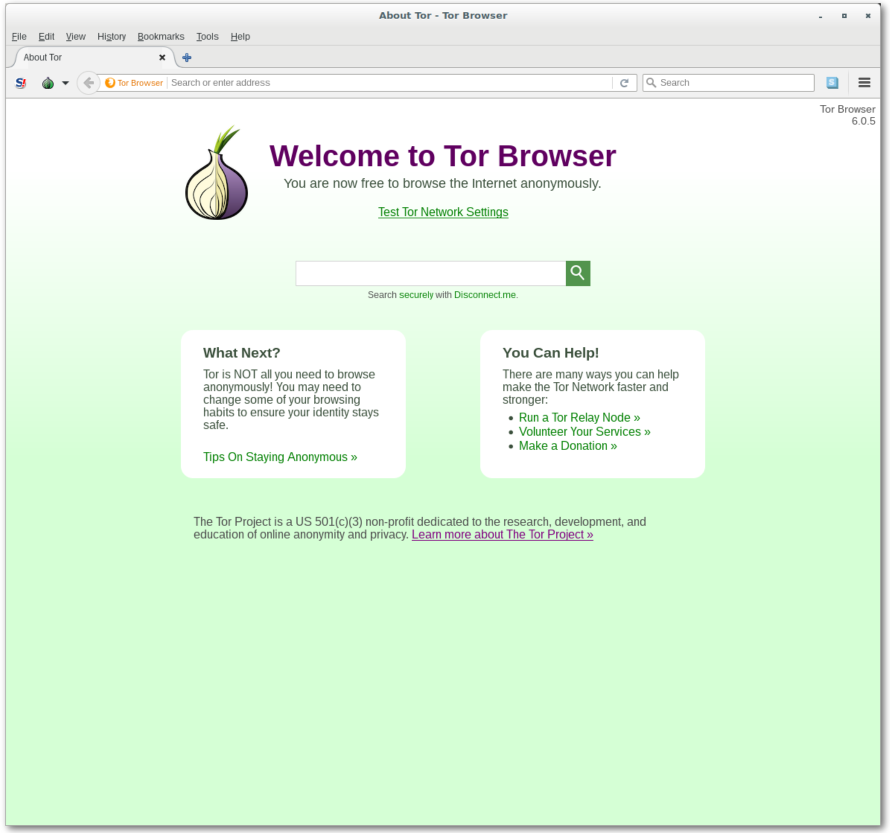
WhatsApp does offer strong encryption (in fact, it is exactly the same encryption system authored by the Signal team) but, unlike Signal, the application is not open source. This means that, unlike Signal, it is very difficult to verify that the application does what it claims to, or is properly secure.

Facebook, who own WhatsApp, have also been condemned for sharing private user data between the two companies, leading the UK ICO to request that they halt the sharing, pending further investigation.

Please visit `whispersystems.org` **for more information.**

Tor Browser

- A web browser that helps to defend your internet activity against surveillance.
- Your connections are routed through multiple servers and countries before reaching their destination.
- All connections are encrypted so that they cannot be read when in transit.
- Maintain privacy, anonymity, and security.
- Can be used instead of, or alongside, your current browser.



Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

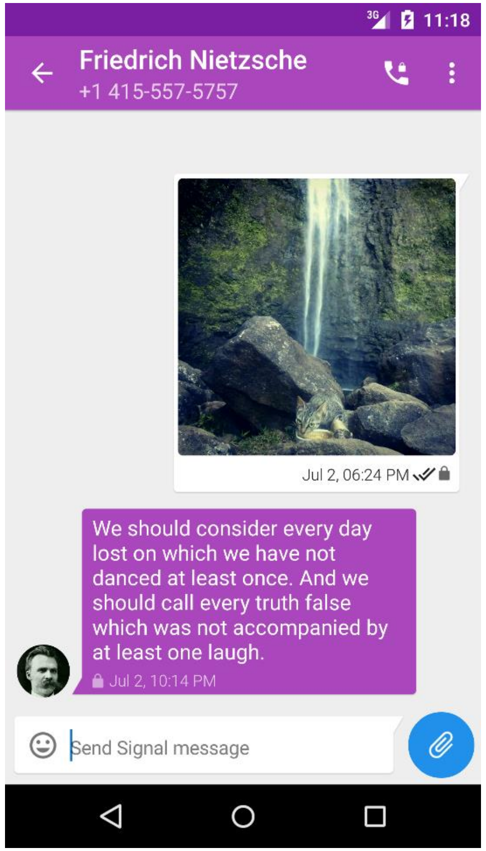
You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

Signal Private Messenger



Friedrich Nietzsche
+1 415-557-5757

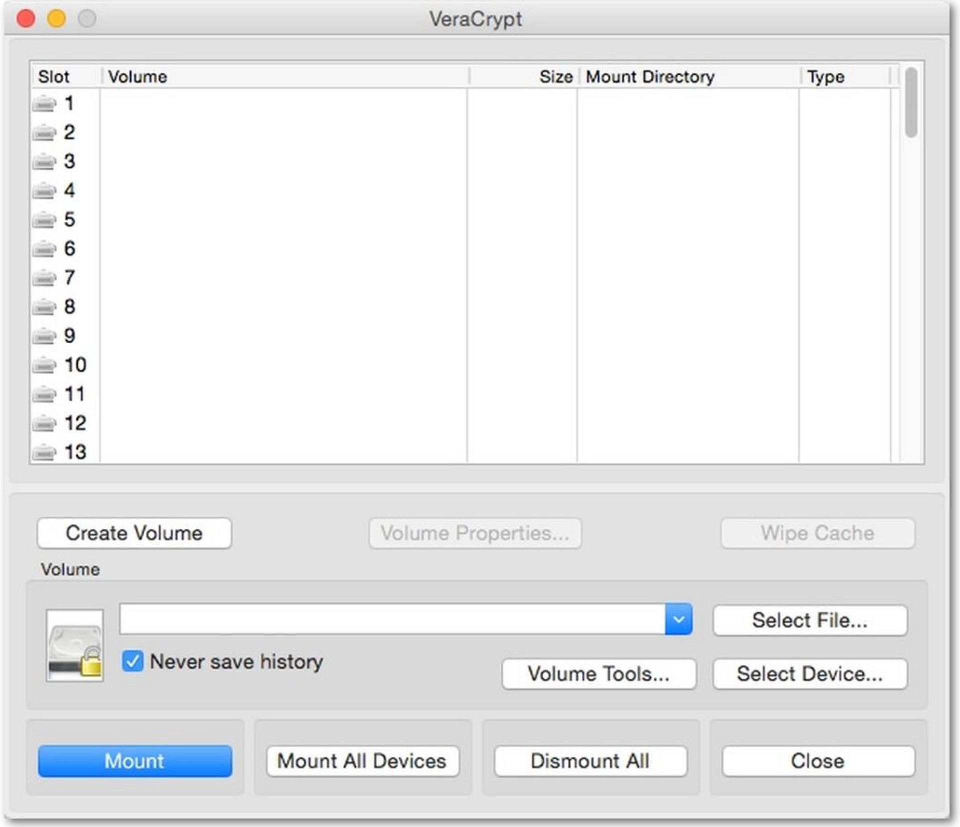
Jul 2, 06:24 PM

We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.
Jul 2, 10:14 PM

- Secure, encrypted and simple instant messaging app for Android and iOS.
- Supports text, picture and video messages as well as voice conversations.
- Supports group messaging.
- Can be used between Signal users on any supported platform.
- Fully free and open source – unlike most other encrypted messaging apps!
- Recently received a crypto & security audit.

Full Disk Encryption

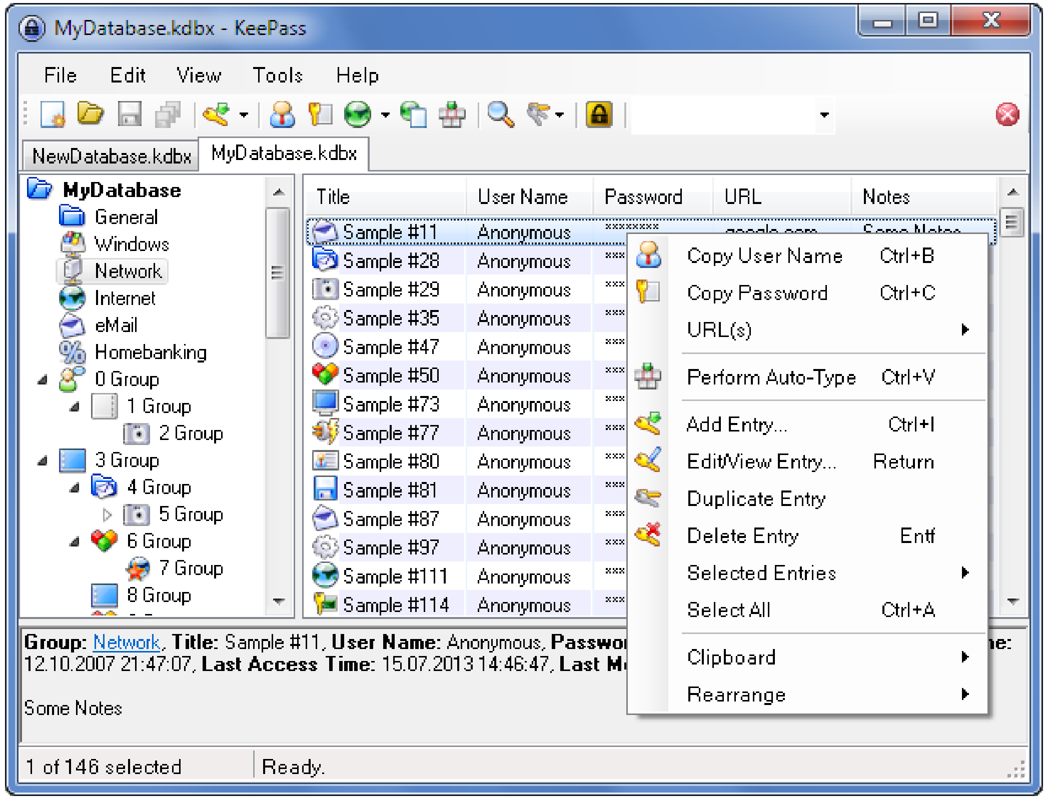
- Most people store a lot of personal information on a PC/laptop.
- Cache and temporary files tell a surprisingly detailed story about your life and everything you do on the machine.
- Ensure that none of the data on your computer is readable without knowledge of your encryption password.
- Nobody can read your data in the case of theft, or if you need to send away your machine for repair.



Slot	Volume	Size	Mount Directory	Type
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

☑ Never save history

KeePass



Title	User Name	Password	URL	Notes
Sample #11	Anonymous	********	google.com	Some Notes
Sample #28	Anonymous	***		
Sample #29	Anonymous	***		
Sample #35	Anonymous	***		
Sample #47	Anonymous	***		
Sample #50	Anonymous	***		
Sample #73	Anonymous	***		
Sample #77	Anonymous	***		
Sample #80	Anonymous	***		
Sample #81	Anonymous	***		
Sample #87	Anonymous	***		
Sample #97	Anonymous	***		
Sample #111	Anonymous	***		
Sample #114	Anonymous	***		

Group: Network, **Title:** Sample #11, **User Name:** Anonymous, **Passwo**
12.10.2007 21:47:07, **Last Access Time:** 15.07.2013 14:46:47, **Last M**

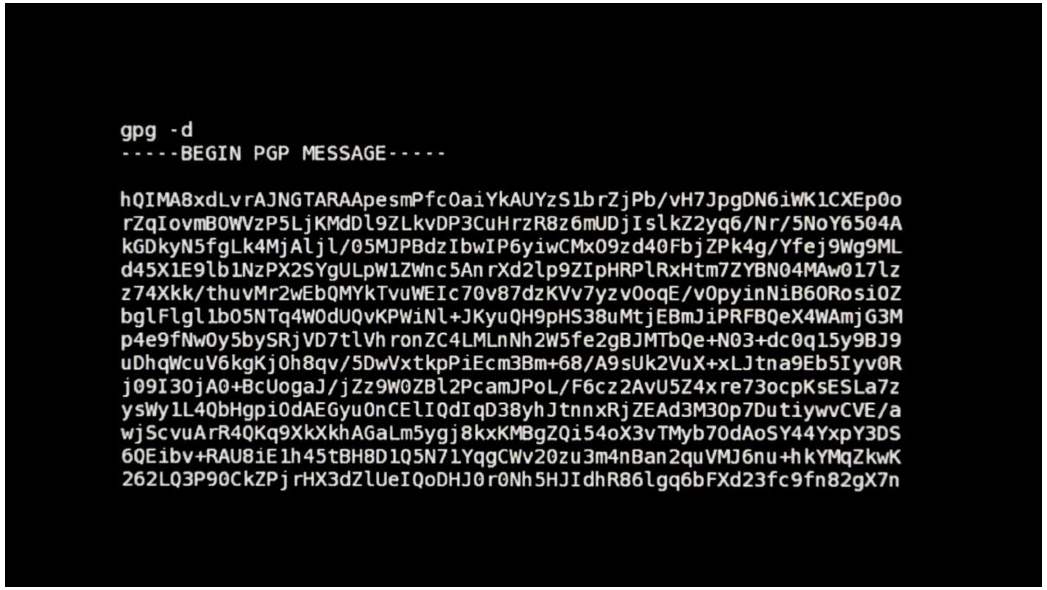
Some Notes

1 of 146 selected
Ready.

- A secure, encrypted password manager.
- Free and open source software –supports Windows, macOS, and Linux.
- Allows you to securely store all your passwords in an encrypted database.
- Features an automatic password generator to generate long, random passwords for you.
- ‘Auto-Type’ feature will handle ‘typing’ in passwords to sites for you.
- Don’t suffer like *Yahoo!* or *LinkedIn* users!

PGP

- A method of encrypting email so that it cannot be read in transit.
- Not quite as easy or flexible as something like Signal, but still gets a lot of use.
- Requires both participants to have set up PGP and have public keys available.
- Worthwhile setting up if email is your preferred method of communication.



```
gpg -d
-----BEGIN PGP MESSAGE-----

hQIMA8xdLvrAJNGTARAApesmPfcOaiYkAUYzS1brZjPb/vH7JpgDN6iWK1CXEp0o
rZqIovmBOWVzP5LjKMdDl9ZLkvDP3CuHrzR8z6mUDjIslkZ2yq6/Nr/5NoY6504A
kGDkyN5fgLk4MjAljl/05MJPBdzIbwIP6yiwCMxO9zd40FbjZPk4g/Yfej9Wg9ML
d45X1E9lb1NzPX2SYgULpW1ZWnc5AnrXd2lp9ZIpHRPlRxHtm7ZYBN04MAw017lz
z74Xkk/thuvMr2wEbQMYkTvuWEIc70v87dzKVv7yzvOoqE/vOpyinNiB6ORosiOZ
bglFlgl1bO5NTq4WOdUQvKPWiNl+JKyuQH9pHS38uMtjEBmJiPRFBQeX4WAmjG3M
p4e9fNwOy5bySRjVD7tlVhronZC4LMLnNh2W5fe2gBJMTbQe+N03+dc0ql5y9BJ9
uDhqWcuV6kgKjOh8qv/5DwVxtkpPiEcm3Bm+68/A9sUk2VuX+xLJtna9Eb5Iyv0R
j09I3OjA0+BcUogaJ/jZz9W0ZBl2PcamJPoL/F6cz2AvU5Z4xre73ocpKsESLa7z
ysWy1L4QbHgpiOdAEGyuOnCElIQdIqD38yhJtnnxRjZEAd3M3Op7DutiywvCVE/a
wjScvuArR4QKq9XkXkhAGaLm5ygj8kxKMBgZQi54oX3vTMyb7OdAoSY44YxpY3DS
6QEibv+RAU8iE1h45tBH8D1Q5N71YqgCWv20zu3m4nBan2quVMJ6nu+hkYMqZkwK
262LQ3P90CkZPjrHX3dZlUeIQoDHJ0r0Nh5HJIdhR86lgq6bFXd23fc9fn82gX7n
```

Citizenfour (2014)

CRYPTO PARTY

cryptopartynewcastle.org