HEI GETT NACH DRU GESCHAFFT!!!

Anonymt surfen

Software	Erklärung	Link
Tor	Tor ass eng Software déi et erméiglecht sech anonym a sécher am Internet kennen ze bewegen. Tor gëtt ënnert anerem (awer net nëmmen) vu Journalisten, Whistleblower an Leit aus repressiven Staaten genotzt fir kennen weiderhin an engem onzenséiert Internet kennen deel ze huelen. Tor verschlësselt är Internet Verbindung an schéckt är Verbindung duerch divers aner Server am Tor Netzwierk. Dofir ass et onméiglech erauszefannen wien genee wat um Internet gemaach huet. Tor ass fräi a gratis. Tor gëtt vun fräiwëllegen bedriwwen déi hier Serverkapazitéiten zur Verfügung stellen, domatt dir sécher um Internet kennt surfen. Hei am Land gëtt et sou eng ASBL déi sech "Frënn vun der Ënn" nennt. Se ass ugewisen op all Don an giffen sech iwwert eng kleng Spend vill freeën. Fir Tor kenne ze benotzen ass et am einfachsten sech den "Tor Browser Bundle" erof ze lueden.	Download
VPN	Eng aner Méiglechkeet anonym a sécher am Internet kennen ze surfen ass, eng VPN ze benotzen. Dir musst iech dat esou virstellen, datt wann dir Facebook wëllt opruffen, är Kommunikatioun een Ëmwee iwwert en aneren Server mécht an deen alles weiderleet. Wichteg gëtt eng VPN virun allem wann een an engem ëffentlechen Hotspot ass ewéi zB HotCity an der Stad. VPN’s kaschten awer an der Regel bëssen Geld.	Eng Lescht vun Ubidder

Alternativen

Chat a Videotelephonie

Gewinnten Software	Alternativ	Erklärung	Link
WhatsApp Facebook Chat ICQ SnapChat	XMPP Jabber Pidgin TorMessenger Ricochet	XMPP oder einfach Jabber genannt, ass e Protokoll wat et erlaabt souguer mat aneren Messenger (ewéi ICQ asw) ze kommunizéieren an dat sécher. Et ass virun allem gratis, kann vu jidderengem benotzt ginn an et ass komplett dezentraliséiert. Dat heescht, wien den néidegen savoir-faire huet, dee kann op sengem eegenen Server, Jabber zur Verfügung stellen. Wisou ass Dezentraliséierung gutt? Stellt iech elo mol fir vun haut op muer fält de Server vun ICQ, SnapChat asw aus. Dann ginn déi Servicer net méi. Beim Jabber ass et ni méiglech ee Service komplett ze blockéieren, well ganz vill Leit een eegenen Jabber Server zur Verfügung stellen. Nieft XMPP ginn et och nach komplett dezentral Messenger. Als gutt Beispill dengt hei Ricochet!	Download Pidgin Download TorMessenger Jabber Account erstellen Download Ricochet
Skype	Jitsi	Jitsi ass eng Alternativ zu Skype a baséiert op XMPP. Dermadder ass et méiglech sécher ze chatten an Videotelephonie ze bedreiwen. Och Konferenzschaltungen mat méi Leit sinn méiglech. Jitsi leeft mëttlerweil Skype a villen Firmen de Rang of, well et komplett gratis ass a fräi ass.	Download

Browser

Gewinnten Software	Alternativ	Erklärung	Link
Internet Explorer	Firefox	Mozilla Firefox ass een oppen Browser deen och gratis ass. En hält sech un International Webstandards an Fehler ginn innerhal kierzester Zäit gefléckt. Net esou beim Internet Explorer wou eng Secherheetslück mol mei wei 5 Joer kann existeieren.	Download
Internet Explorer	Chromium	Chromium ass e Fork vum Google Browser Chrome. Well Chrome open source ass, kann dësen Fork existéieren. Wat ass den Ënnerscheed zwëschent Chrome a Chromium? Am Chromium goufen all déi sougenannten "Call-Back" Prozeduren erausgeholl an nach méi Wäert op Privatsphär geluecht.	Download

Suchmaschinnen

Gewinnten Software	Alternativ	Erklärung	Link
Google	DuckDuckGo	Google ass eng grouss Boite déi probéiert mät ären Daten Suen ze maachen. Allkéiers wann dir eppes sicht, dann gëtt dat vun Google gespäichert an et gëtt e Profil iwwert iech ugeluecht. Wien net well, datt Google weess, dat dir am Internet no enger neier Schaff sicht, oder Erwuesenenspillsachen wëllt kafen, dann muss een Sichmaschinn wiesselen. DuckDuckGo ass do ganz fir bei an respektéiert är Privatsphär.	Ukucken
Google	StartPage	Wien Google trotzdem bei sichen net mëssen well, deen soll StartPage als Mëttelsmann benotzen. Hei gitt dir är Sichufroo u StartPage an déi leeden et dann weider u Google. De Virdeel dovunner ass, datt Google net méi zouuerdnen kann vu wou a vu weem déi Ufro komm ass. StartPage gouf 2008 och mam EU Datenschutzgütesiegel ausgezeechent!	Ukucken

Operating System

Gewinnten Software	Alternativ	Erklärung	Link
Windows	Linux	Linux ass een alternatiivt Betribssystem dat haut well immens vill am Gebrauch ass, zemol op Plaze wou een et net giff mengen. Sou lafen zum Beispill Lifter, Android Smartphones, Automate vun all Zort a vill méi op Linux. Linux ass als oppen Alternativ entwéckelt ginn an et gëtt och vill méi Wäert op Sécherheet geluecht. Och gëtt et net nëmmen eng Zort vu Linux mä eng helle Wull un verschiddenen Distributiounen déi fir verschidden Zilgruppe konzipéiert goufen. Sou ginn et extra Distributiounen, déi op Schoulen zougeschnidde sinn, oder fir Leit déi Musek/Filmer entwéckelen. Fir den Ufänger, dee grad reicht op Linux wiesselt, empfehle mir Ubuntu oder Linux Mint.	Ukucken

Gewinnten Software	Alternativ	Erklärung	Link
Windows	BSD	Nieft Linux ginn et och nach Betribssystemer aus der BSD Rei. Des Betribssystemer baséieren op UNIX. BSD ass awer näischt fir Ufänger déi grad den Entschloss gefaasst hunn vun Windows ze wiesselen. Well hei gëtt een dann an d'kaalt Waasser gehäit. Mä vläit ass dat jo déi beschten Aart a Weis ze léieren? :) Déi zwee bekanntsten Derivater a wuel di mat der gréisster Community am Réck sinn FreeBSD an OpenBSD.	Ukucken

The cypherpunk movement

> A cypherpunk is an activist advocating widespread use of strong cryptography as a route to social and political change. Originally communicating through the Cypherpunks electronic mailing list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since the late 1980s.

Manifesto

```
A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age.
Privacy is not secrecy.  A private matter is something one doesn't
want the whole world to know, but a secret matter is something one
doesn't want anybody to know. Privacy is the power to selectively
reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of
their interaction.  Each party can speak about their own memory of
this; how could anyone prevent it?  One could pass laws against it,
```

```
but the freedom of speech, even more than privacy, is fundamental to
an open society; we seek not to restrict any speech at all.  If many
parties speak together in the same forum, each can speak to all the
others and aggregate together knowledge about individuals and other
parties.  The power of electronic communications has enabled such
group speech, and it will not go away merely because we might want it
to.

Since we desire privacy, we must ensure that each party to a
transaction have knowledge only of that which is directly necessary
for that transaction.  Since any information can be spoken of, we
must ensure that we reveal as little as possible.  In most cases
personal identity is not salient. When I purchase a magazine at a
store and hand cash to the clerk, there is no need to know who I am.
When I ask my electronic mail provider to send and receive messages,
my provider need not know to whom I am speaking or what I am saying
or what others are saying to me;  my provider only need know how to
get the message there and how much I owe them in fees.  When my
identity is revealed by the underlying mechanism of the transaction,
I have no privacy.  I cannot here selectively reveal myself; I must
_always_ reveal myself.

Therefore, privacy in an open society requires anonymous transaction
systems.  Until now, cash has been the primary such system.  An
anonymous transaction system is not a secret transaction system.  An
anonymous system empowers individuals to reveal their identity when
desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography.  If I say
something, I want it heard only by those for whom I intend it.  If
the content of my speech is available to the world, I have no
privacy.  To encrypt is to indicate the desire for privacy, and to
encrypt with weak cryptography is to indicate not too much desire for
privacy.  Furthermore, to reveal one's identity with assurance when
the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless
organizations to grant us privacy out of their beneficence.  It is to
their advantage to speak of us, and  we should expect that they will
speak.  To try to prevent their speech is to fight against the
realities of information. Information does not just want to be free,
it longs to be free.  Information expands to fill the available
storage space.  Information is Rumor's younger, stronger cousin;
Information is fleeter of foot, has more eyes, knows more, and
understands less than Rumor.

We must defend our own privacy if we expect to have any.  We must
come together and create systems which allow anonymous transactions
to take place.  People have been defending their own privacy for
centuries with whispers, darkness, envelopes, closed doors, secret
```

```
handshakes, and couriers.  The technologies of the past did not allow
for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems.  We
are defending our privacy with cryptography, with anonymous mail
forwarding systems, with digital signatures, and with electronic
money.

Cypherpunks write code.  We know that someone has to write software
to defend privacy, and since we can't get privacy unless we all do,
we're going to write it. We publish our code so that our fellow
Cypherpunks may practice and play with it. Our code is free for all
to use, worldwide.  We don't much care if you don't approve of the
software we write.  We know that software can't be destroyed and that
a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is
fundamentally a private act.  The act of encryption, in fact, removes
information from the public realm.  Even laws against cryptography
reach only so far as a nation's border and the arm of its violence.
Cryptography will ineluctably spread over the whole globe, and with
it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract.
People must come and together deploy these systems for the common
good.  Privacy only extends so far as the cooperation of one's
fellows in society.  We the Cypherpunks seek your questions and your
concerns and hope we may engage you so that we do not deceive
ourselves.  We will not, however, be moved out of our course because
some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for
privacy.  Let us proceed together apace.

Onward.

Eric Hughes


9 March 1993
```

Projects

Open DNS Server

Censorship free DNS server!
95.141.34.162

DNSCrypt Server

While having a free DNS server is cool, why not doing encrypted DNS requests as well?
85.93.216.115:5678
Provider public key:

```
5FF6:5A49:9C19:6B39:7DAF:4758:4070:7092:5ABA:B334:5E6C:B46A:FA4B:7771:5ADA:2EC8
```

.bit domains

The DNS server does also resolve .bit domains!

Keyserver DNS Round Robin

We offer a small DNS Round Robin for keyserver we trust.

keyserver.cypherpunk.lu

Crypto Partys

We are organizing Crypto Partys on a regular base.

Besides we write code.

- Glous. Commandline nopaste service with burn-after-reading and GPG encryption
- FISHY. This is a Xchat Twofish Encrypter. HowTo is documented in the script itself.
- Twofish Crypter. Encrypts your files with Twofish!
- Vigenere Cipher - Perl module. Crypt::Vigenere::Square is my implimentation of the Vigenere Cipher.
- QRScan - PGP encrypted letters
- ICMP Data Transporter

Support

And if another projects fits into the Ideology of the cypherpunk movement, you can be sure that we support it!

Like Frenn vun der Enn