

Заключение

1. Изучай программу - по одной. Не бери всё махом.
2. Привлекай знакомых. Создавай свой шифро круг.
3. Вырабатывай привычку шифроваться.

Теперь о пиратском

Всё выше описанное не причуды гиков и шифропанков, а реальность. Социальная, политическая, технологическая. Обеспечить сохранность своей информации, профилей, данных - дело самих граждан.

Шифроваться
- это привычка!

Последний довод

Вам нечего скрывать, но вы закрываете дверь своей квартиры. Тоже самое необходимо делать с информацией. Вы - честный человек, но не хотите, чтобы ваша информация (письма, файлы, пароли) читалась и использовалась другими.



-----BEGIN PGP MESSAGE-----
3CekWK6jfzjH37lusGk9aSA6el+qTLRNqfmX4r/
Vr4ArtGGb/dee88LuJN8HnYJf89PdOMK8Gedu
TalciVtrLA4UBDAMVyt
Nf0d4ruUx1jfk//kUze
CgaOS4Jlq08b7gm3v2Wr305Fh+vjkaFuYg5
aLv9Q3Qzt2S
wLciFAQwD
X466nL6FrQBCACNLrOPX3p02a9FPtxOEU
sPoXiz0KPBIZFGTYRmqFsr
F0ig8wbjw3uQsJ3wejjQ7Uf4ib6Hg9e+gXXzN
3W9iclub2aOFmis5OdR9UZZzWH6lzQW63bJ
vJ4VY8lou4xtVe5solZzBewyuXFug6VNw2nC
5cYF3UEKI3tVKyTreJ4hlArN1/UaSC6rILyRU
ebrl9ebHgmmb7ScCsvygf4dtPYTFRO89gRF
1LMnb/enEJT0dThsQrAdtgMjl4eGaxDuoDD
C6taY5FmtlXdN/uXV6JvsUSrkn1iJ6DO5cco
2czPdXmdx/tKGjXBM2/o8a0ukBqmXv8rf0dl
B9yB9NZvr/mTMmKz8PLZWWWVdgwNHXl
bq4pogbcidFOEaKEhitoBp0btbhT9JrVIMaF
cweK1KVXEqrXVKtboqLBxpoYZryT+4BvF1M
kdHPt09lyhOVfFnDaY1WN9POy77A5CzBN
9kttN77boKJ1EZrg4ce56rEvmuMocrSa3qSe
HzkVPfnah3pvKsM7QvZcmGHsNc0jhlyQ/Qj30
LeQVmf0To1ktOXOpdGONQXeu5enhYFYAcY
MwrpCYKvGXZmMwG3tKyKSyzH/PH7IZG2+cr
FNIPDIzg33cYWw9wfnYQG6tmKg4HfVSKPH0
ZfAYQiOGeroXfiVSS9MV0zSDh9JrdbIESBhJ+
UZ137d2uYxc2xe7/AFcWPmcyBMN2ZzNs4cY
uJvhXjxVPF3LCWПосвящаетсяumdLvtLCZMX
P6uxyXYkT3QMApq6HDVIDQ4Od7t8yx+yZKL
Н Дню безопасного интернета ghgvhghnynG
kjhkjkf_internetday.orgRKeSmkMBvgY+GrLvtzs
RW48cYqq/LYipTRwrj/KRCaRLSvxFDsAggyAF
Дню борьбы против массового надзораQgL
- thedaywefightback.org/ ncjbjcGKB7gfhjtGjlnds
Tol9n3fglmQcOCB7UY7fUSooTCCkTt4kWbcp
Дню открытых данных в Минске jklkjbl78k
bit.ly/1nka8MNQgInmmbg5/9VJl9kttN77boKJ1E
Zrg4ce56rEvmuMoLMnb/enEJT0dThsQrAdtgMj
l2aOFmis5OdR9UZZzWH6lz
-----END PGP MESSAGE-----

крипто
листовка
выпуск 1

Шифроваться - привычка

Файлы

Самое базовое - это защита файлов. Здесь помогают gpg-программы. Так что смело ищите что-то похожее. Например, **kleopatra**. Для linux это утилита **gpg**. Данная программа позволяет шифровать файл.

Сайт: gnupg.org

Папки

Если вы хотите шифровать целые папки и множество файлов, используйте **truecrypt**. Эта программа позволяет создавать контейнеры различных размеров, которые, как обычные диски, могут иметь свою структуру.

Сайт: truecrypt.org

Пароли

Итак. Файлы папки мы защитили, теперь самое время позаботиться о паролях. Если у вас один пароль на все сервисы, то срочно меняйте его. Если разные и хорошая память - можете пропустить этот абзац. Иначе используйте - **keepass**. Это программа хранит пароли в зашифрованном файле. Который защищён главным паролем, фразой или даже уникальным файлом.

Сайт: keepass.info



Текстовые чаты

Теперь мы перешли к общению. Ни для кого не секрет, что такие чаты как skype, icq могут прослушиваться провайдерами этих самых сервисов. Значит, самое время начинать шифровать сообщения на своём компе и пересылать их зашифрованными своим друзьям по чату. В этом помогут чат-клиенты с функциями OTR - out of record. Попробуйте для начала установить **pidgin** с такой функцией.

Если вы в сети с места работы, где нет возможности установить новую программу, но очень нужно пообщаться, используйте - **crypto.cat**. Это приложение к браузеру с шифрованием чата.

Сайт: pidgin.im +
otr.cypherpunks.ca

Голосовые чаты

Тоже самое делайте и с голосом. Ищите чаты, которые шифруют ваши сообщения. Хороший выбор - **mumble**. Также попробуйте jutsi.

Сайт: mumble.sourceforge.net

Почта

Теперь переходим к самому базовому средству общения - электронной почте. Этот сервис не используют, разве что 100% шифропанки. Хотя и им приходится грешить. Поэтому, если у вас есть почта, и вы постоянно поддерживаете связи с разными людьми, шифруйтесь. Попробуйте для начала связку программ **thunderbird + enigmail**. Они автоматизируют процесс шифрования, делая его удобнее.

Сайт: [mozilla.org/thunderbird +
enigmail.net](http://mozilla.org/thunderbird+enigmail.net)

Плагин для браузера

Завершаем материал простым плагином - **https everywhere**. Он обеспечивает автоматический поиск возможного соединения через протокол **https** с необходимым сайтом. Это не панацея. Но защищает слабые места на уровне передачи данных.

Сайт: eff.org/https-everywhere

