The Basics of

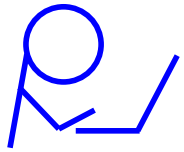
Data Security

Fabian M. Suchanek

based on “A practical guide to data security”

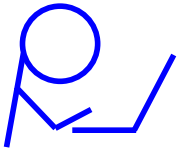
Data

work



study

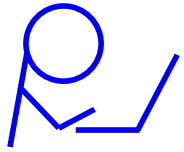
plan vacation



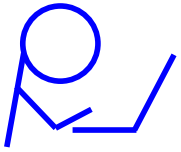
make photo album

watch movie

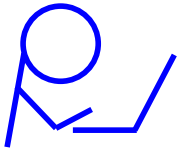
write letter



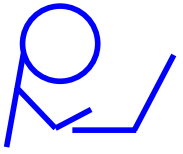
chat with friends



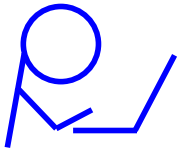
phone with friends



write a book

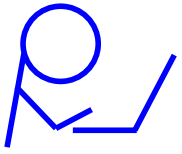


be creative

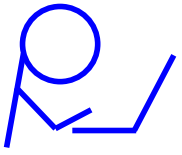


write diary

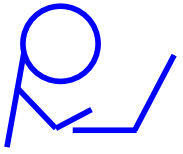
be politically active



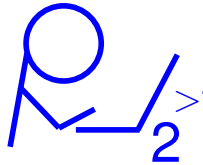
play games



learn language



listen to music



>toc

Overview

Protecting data against

- yourself
- hackers
- evil interlocutors
- companies
- governments

保护数据
·你自己
·黑客
·邪恶的对话者
·公司
·政府

Who is the biggest enemy to ur data?

hackers

病毒/勒索
viruses/ransomware

evil governments

big companies

数据泄露
data leaks

Who is the biggest enemy to ur data?

hackers

viruses/ransomware

evil governments

big companies

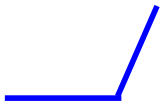
data leaks

you yourself

Backup your data!

All important data should live in at least 2 different places.

所有重要的数据应该至少存在在两个不同的地方。



+

some other place

... to protect against:

- theft
- loss
- hazards
- decay

...防止：盗窃
·失利
·危害
·衰减

Def: Ransomware

A ransomware is a malicious software program that makes your data unusable by encrypting it, and requests a ransom (=money) to decrypt it.

勒索软件是一种恶意软件程序，通过对数据进行加密而使数据无法使用，并请求赎金（=金钱）对其进行解密。

Cryptolocker: 325m USD paid

WannaCry: 150,000 USD paid, 4b USD in damages

Solution 1: Cloud Service

A cloud service automatically backs up your data. 云服务会自动备份您的数据。

(do not copy your data to the cloud service folder, move it there!)

Criteria for selecting a cloud service:

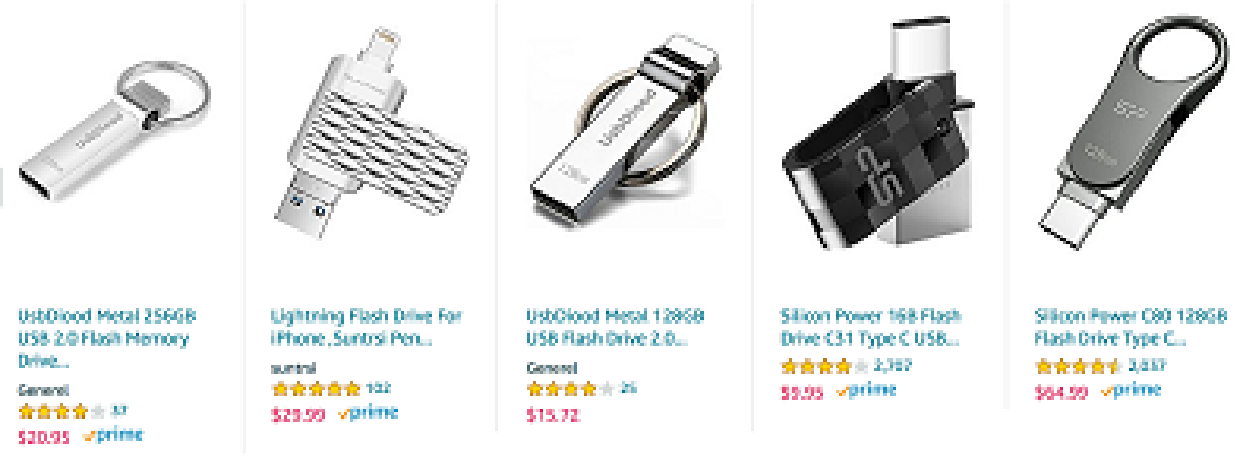
- can you go back in history? (“versioning”)
- can you undelete? (= protect against ransomware)
- two factor authentication (see later in this lecture)
- encryption (see later in this lecture)
- Web interface
- Is the client open-source?

选择云服务的标准：

- 你能回到历史吗？（“版本”）
- 你可以取消删除吗？（=防范勒索软件）
- 双因素身份验证（请参阅本讲座后面的内容）
- 加密（请参阅本讲座的后面部分）
- Web界面
- 客户是开源的吗？

Solution 2: USB key

Keep the data on a USB key that is physically stored in a different place.



Amazon

- store the USB key in a different place
- back up your data every few months

解决方案3：使用GIT或SVN等源代码管理系统，或Duplicity或Borg备份等远程加密备份系统。

Solution 3: Use a source control system such as GIT or SVN, >backup

or a remote encrypted backup system such as Duplicity or Borg backup.

Back up non-file data 备份非文件数据

- Pictures from your phone 您的手机里的图片
  通过安装云服务，或者将其复制到PC。 iPhone将自动备份到iCloud。

  Either by installing a cloud service, or by copying them to the PC.

  iPhones will automatically backup to iCloud.

•您的短信（在Android上：带有应用程序; 在iPhone上：iMessages（？））
- Your SMS (on Android: with an app; on iPhone: iMessages (?))

•您手机上的通讯录和日历（使用CalDav / CardDav）
- Your contacts and calendar on your phone (use CalDav/CardDav)
- Your emails

  Use, e.g., an email client on your computer.

  Otherwise, export your emails from your service provider.

  您的电子邮件
  使用电脑上的电子邮件客户端。
  否则，请从服务提供商处导出您的电子邮件。
- Your WhatsApp chats (stored only on your phone!)

  Tap the name of the contact, then choose “export”.

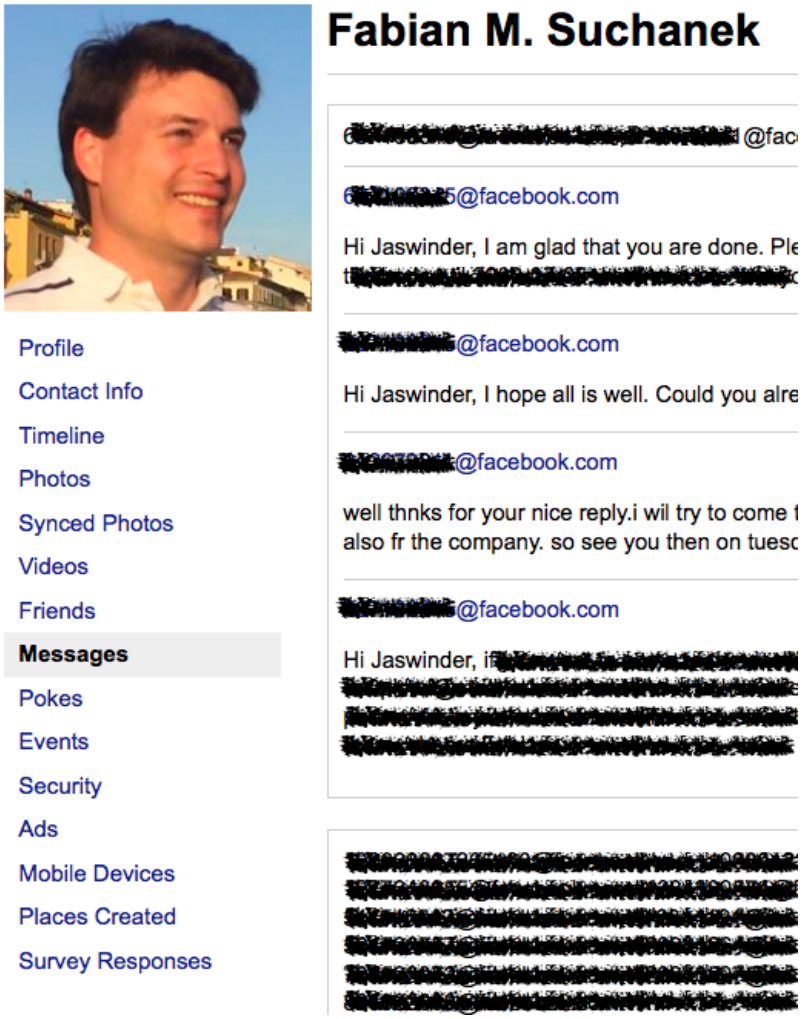
  Chats may also be backed up when you back up your phone.

  WhatsApp聊天（只存储在您的手机！）
  点击联系人的名称，然后选择“导出”。
  在备份手机时，聊天也可以备份。
- Data that you have stored in online services
  - Facebook
  - Google Drive
  - Trip planners

  •您存储在在线服务中的数据
  - Facebook
  - Google云端硬盘
  - 旅行计划
  - 在线论坛

Back up your Facebook

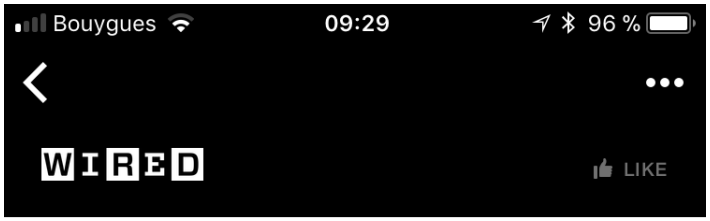
You can download your entire Facebook data into neat HTML files.



Google can do the same

>backup

Back up your Passwords



三个解决方案
1）设置备用电子邮件地址以重置在线服务的密码
2）把它写在一张纸上，存放在安全的地方
3）把密码放在一个文件中，用不同的密码加密，把文件给一个朋友，把密码给另一个朋友。

LONGFORM

比特币损失30000美元的史诗故事

‘I Forgot My PIN’: An Epic Tale of Losing $30,000 in Bitcoin

老将

A veteran tech journalist tries everything, including hypnosis, to recover a small fortune from a locked bitcoin device.

催眠

从锁定的比特币设备中收回一笔小小的财富

BY MARK FRAUENFELDER
29 OCTOBER 2017

The Trezor: January 4, 2016: 7.4 BTC = $3,000

In January 2016, I spent $3,000 to buy 7.4 bitcoins. At the time, it seemed an entirely worthwhile thing to do. I had recently started working as a research director at the Institute for the Future’s Blockchain Futures Lab, and I wanted

Three solutions:

1) set up an alternate email address
for resetting the password
of an online service

2) write it on a piece of paper
and store it in a secure place

3) put the password in a file,
encrypt it with a different password,
give the file to one friend,
and the password to another friend.

Overview

Protecting data against

- yourself
- hackers
- evil interlocutors
- companies
- governments

Protecting against hackers

防范黑客风险=事件发生概率×损害

risk = probability of the event × damage

low

high

如果黑客有权访问您的电子邮件，他们可以

If a hacker had access to your email, they could

- 阅读您曾经写过或收到过的所有电子邮件（银行，SO，EX，...）
- read all email you have ever written or received (bank, SO, ex,...)
- 查看附加到您发送或收到的电子邮件的所有图片
- see all pictures attached to emails that you sent or received
- 以您的名义发送电子邮件（例如发送给同事或客户）
- send emails in your name (e.g., to colleagues or clients)
- 在Facebook上发布你的名字的消息
- post messages in your name on Facebook
- 锁定您的Facebook帐户（通过更改密码）
- lock you out of your Facebook account (by changing the password)
- 锁定您的电子邮件帐户
- lock you out of your email account

文本

- 关闭您的电子邮件帐户，关闭您的Facebook帐户
- close your email account, close your Facebook account
- 弄乱你的博客
- mess up your blog
- 基本上掌握所有其他在线账户。
- gain hold of basically all other online accounts.

The main protection is your password.

Popular passwords are bad

Most popular passwords:

123456	abc123
password	admin
12345	121212
12345678	flower
football	passw0rd
qwerty	dragon
1234567890	sunshine
1234567	master
princess	hottie
1234	loveme
login	zaq1zaq1
welcome	password1
solo	

Time.com

A hacker can simply try out all of these passwords

Popular passwords

Common words are bad

- love
- Love
- love you
- ...

A hacker can simply try out all words from a dictionary ("dictionary attack")

- l0ve
- 1 l0ve y0u
- ...

Replacing letters by numerical counterparts is a known strategy => not safe

用数字替换字母是已知的策略=>不安全

2006年，55%的MySpace密码在8小时内被破解 9·11"袭击事件发生后，已故员工的密码被商业破解，以便使用他们的工作。

In 2006, 55% of MySpace passwords were crackable in 8 hours [Wikipedia]
After the September 11 attacks, the passwords of deceased employees were commercially cracked to allow using their work.

Def: Password strength

Def：密码强度

The number of possible passwords (combinations) of length n over k characters is n^k.

在k个字符上的长度为n的可能的密码（组合）的数目是n的k次方。

密码强度通常以“比特”的形式作为可能组合数量的二进制对数。

The password strength is often given “in bits” as the binary logarithm of the number of possible combinations.

Example: 10 letters a-z = 26^{10} combinations (0.1 quadrillions).

Password strength: $log_2(26^{10}) \approx 47$ bits

例如：10个字母a-z = 2610个组合（0.1 quadrillions）。 密码强度：log2（2610）≈47位

Short passwords are bad

combinations = characterstextasciicircum length

组合=字符文本ASCII周长

黑客可以简单地尝试所有的组合

A hacker can simply try out all combinations

Example: 10 digits = 10 billion combinations.

A PC can do 100m combinations per second

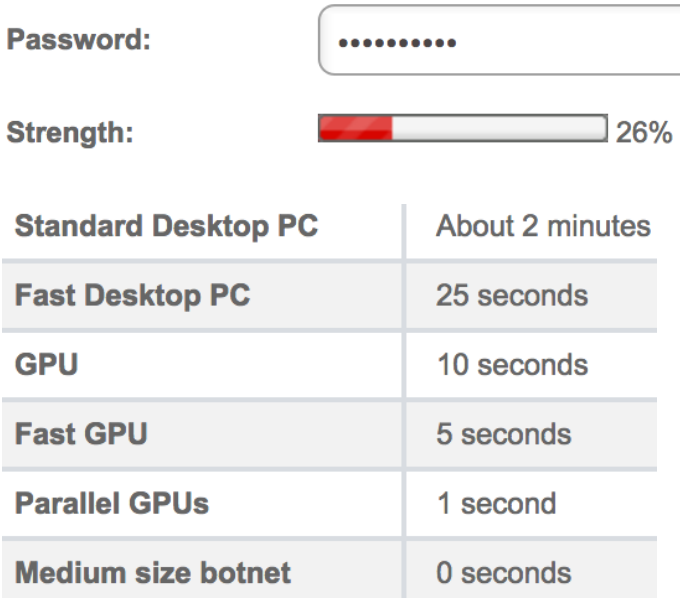
=> we need only 1.5 minutes to break it

例如：10位数字= 100亿个组合。

一台电脑每秒可以做100百万的组合=>我们只需要1.5分钟就可以打破它

Example: Uber sends out a 4 digit code to verify an account. Generate 1m account requests, verify 100 of them just by chance.

例如：Uber发送一个4位数的代码来验证一个账户。 生成100万个帐户请求，验证当中的100个只需要很短的时间。



Try it out!

(But not with your real password!)

Personal information is bad

Pet names

A notable date (wedding, b'date)

A family member's birthday

Your child's name

Another family member's name

Your birthplace

A favorite holiday

Your favorite sports team

According to Google

A hacker can find this information in social networks.

Security questions are bad

Security Questions.

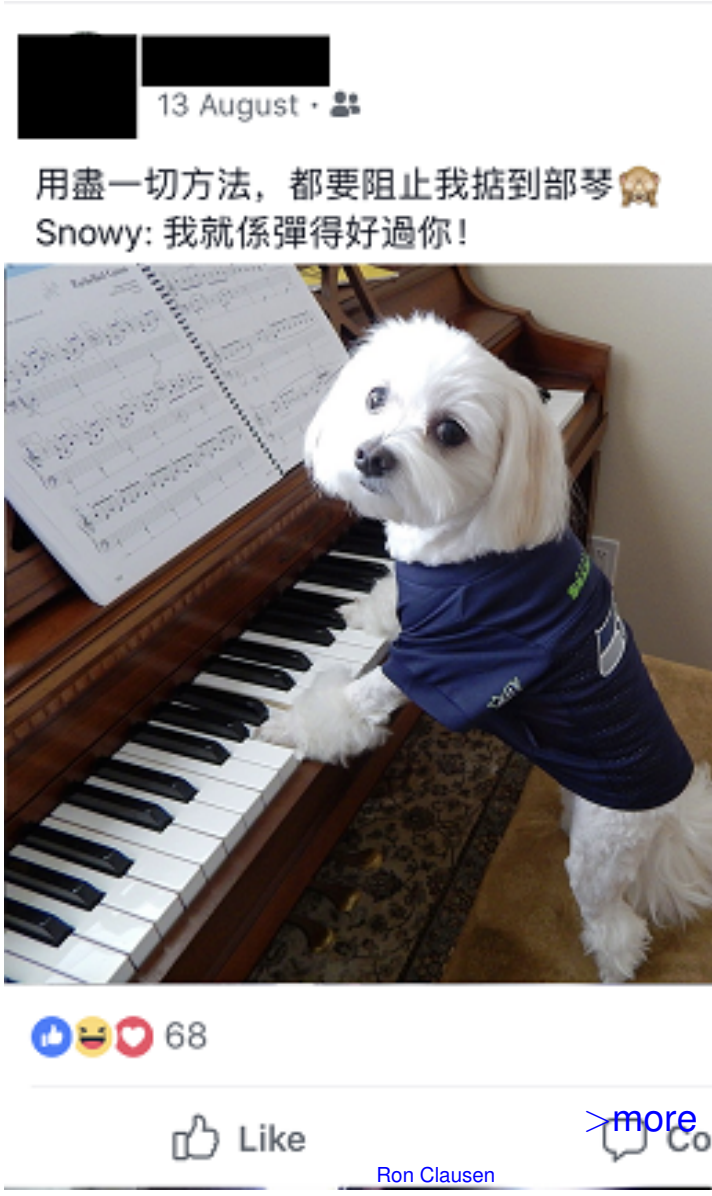
Select three security questions below. These questions will help us verify your identity should you forget your password.

Security Question	What was the name of your first pet? ▾
Security Question	What is your dream job? ▾
Security Question	In what city did your parents meet? ▾

A hacker can find this information in social networks.

40% of users fake the answers and then forget them. Most secure questions are also least memorized.

Research by Google



Ron Clausen

Difficult passwords are bad

"Your password must contain at maximum 5 letters,
and must contain a mammal that lives in the sea"

"你的密码最多必须包含5个字母，并且必须包含一个生活在海中的哺乳动物"

The more annoying passwords restrictions are,
the more likely users are to

- write the passwords down
- forget the passwords
- use simple variations of the same password

更令人讨厌的密码限制，用户越有可能
·写下密码
·忘记密码
·使用相同密码的简单变体

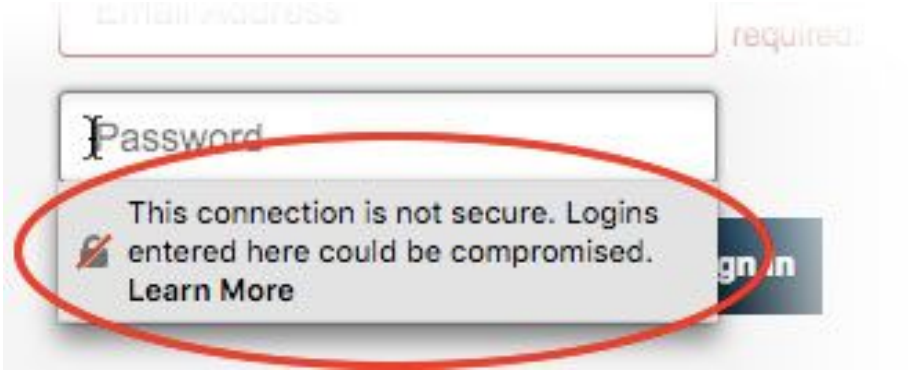
The same applies to passwords that have to be changed regularly.

这同样适用于必须定期更改的密码。

Using the same password is bad

If the password is compromised on one site

如果密码在一个网站上受到威胁



...it allows access to all the others:

Dropbox

amazon

Solution 1: First letter passwords

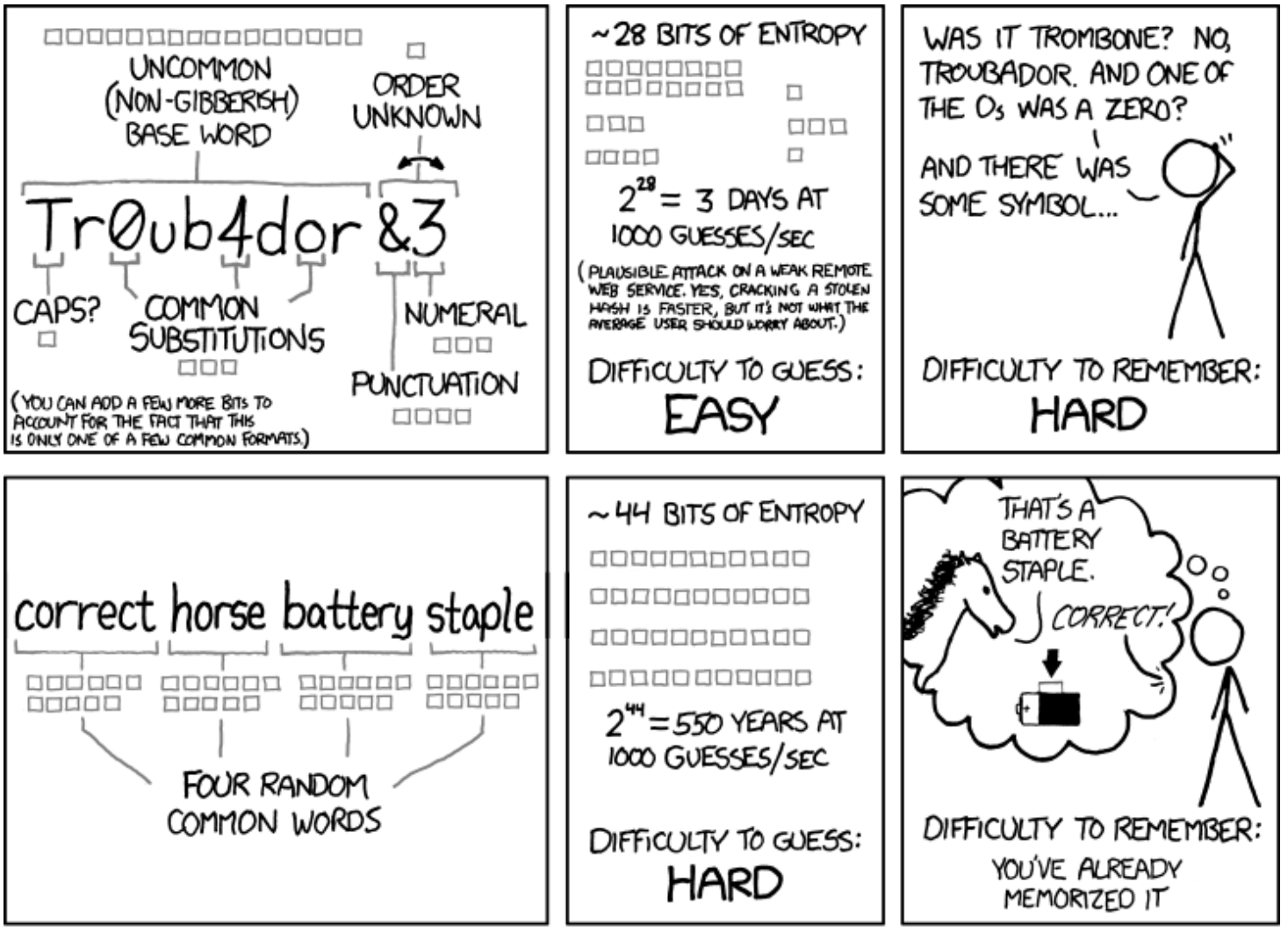
"How much money do I have?" -> "Hm$d1h?"

- easier to remember
- high entropy
- recommended strategy

·更容易记住
·高熵
·推荐策略

Solution 2: Diceware passwords

解决方案2：diceware密码



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

XKCD

Def: Diceware password

长度为n的diceware密码创建如下：

A diceware password of length n is created as follows:

1) Take a list of 6^5 words of some language,

   which are indexed $< 0, 0, 0, 0, 1 >, < 0, 0, 0, 0, 2 >, \ldots$

1）列出一些语言的65个单词，它们被索引为<0,0,0,0,1>，<0,0,0,0,2>

2) Repeat n times

   a) Roll a (physical) dice 5 times,

      obtaining numbers i_1, i_2, i_3, i_4, i_5

   b) Add to your password the word at index

      $< i_1, i_2, i_3, i_4, i_5 >$

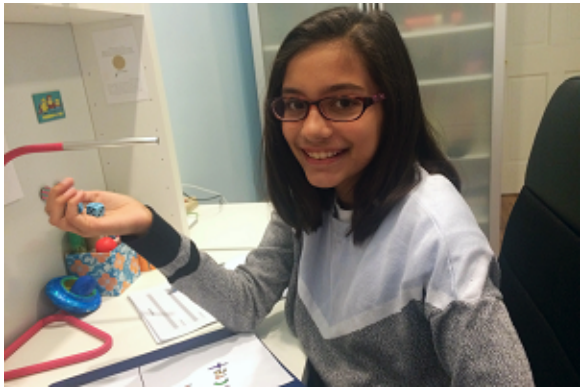
a）掷骰5次，得到数字i1，i2，i3，i4，i5

b）把在索引<i1，i2，i3，i4，i5>处的单词设置为你的密码...

43136 mulct
43141 mule
43142 mull
43143 multi
43144 mum
43145 mummy
43146 munch

EFF Diceware list

Or use a service:



Mira Modi's Diceware Service

combinations = $(6^5)^n$

Solution 3: Password managers (?)

Password managers contain one password per online service, and copy/paste it automatically into the login field.

密码管理器每个在线服务包含一个密码，并将其自动复制/粘贴到登录字段中。

LastPass •••|

KeePass

1Password

Caveats:

- what if you are in an internet café?
- what if the service gets hacked?
- what if the service leaks data?

注意事项：
·如果你在网吧?
·如果服务遭到黑客攻击?
·如果服务泄漏数据呢?

或者：使用随机密码并每次复制/粘贴。 您可以在线或使用密码生成密码

Alternatively: use a random password and copy/paste it each time.

You can generate the password online or with pwgen.

When a password is not enough

Mat Honan

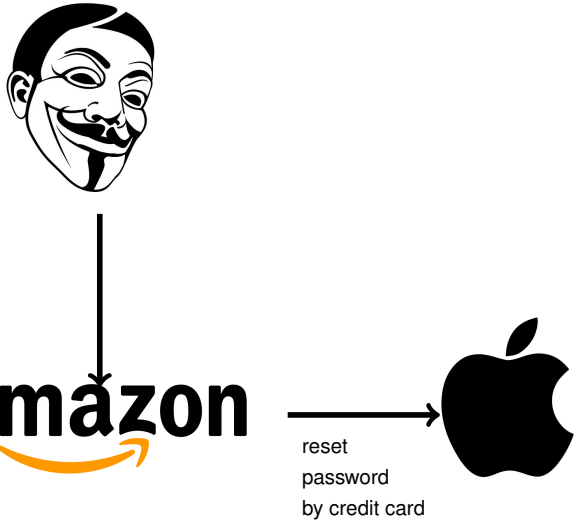
amazon

When a password is not enough

Mat Honan

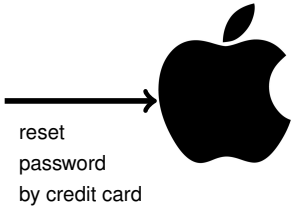
When a password is not enough

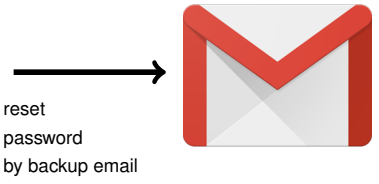
Mat Honan



When a password is not enough

Mat Honan





When a password is not enough

Mat Honan

amazon

reset
password
by credit card

reset
password
by backup email

reset
password
by backup email

When a password is not enough

Mat Honan

amazon

reset password by credit card

reset password by backup email

reset password by backup email

Two-factor authentication

您的数据至少应该有2个独立的障碍！

There should be at least 2 independent hurdles to your data!

Def: Two-Factor Authentication

Two Factor Authentication (2FA) method of access control that allows access only if two independent codes (“factors”) are entered.

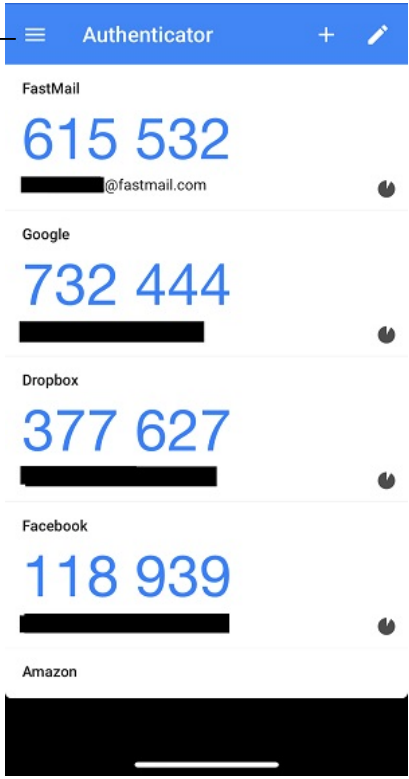
访问控制的双因素验证（2FA）方法，只有在输入两个独立的代码（“因素”）时才允许访问。

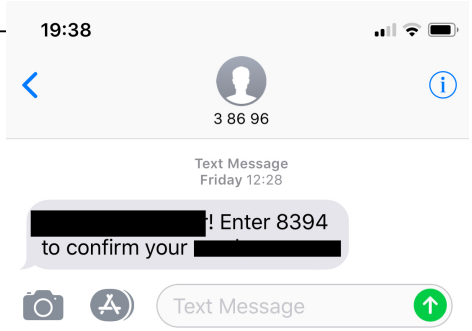
The first factor is usually a password.

第一个因素通常是一个密码。

The second factor can come

- from an app on your phone
- from a phone call
- from an SMS
- from a security key



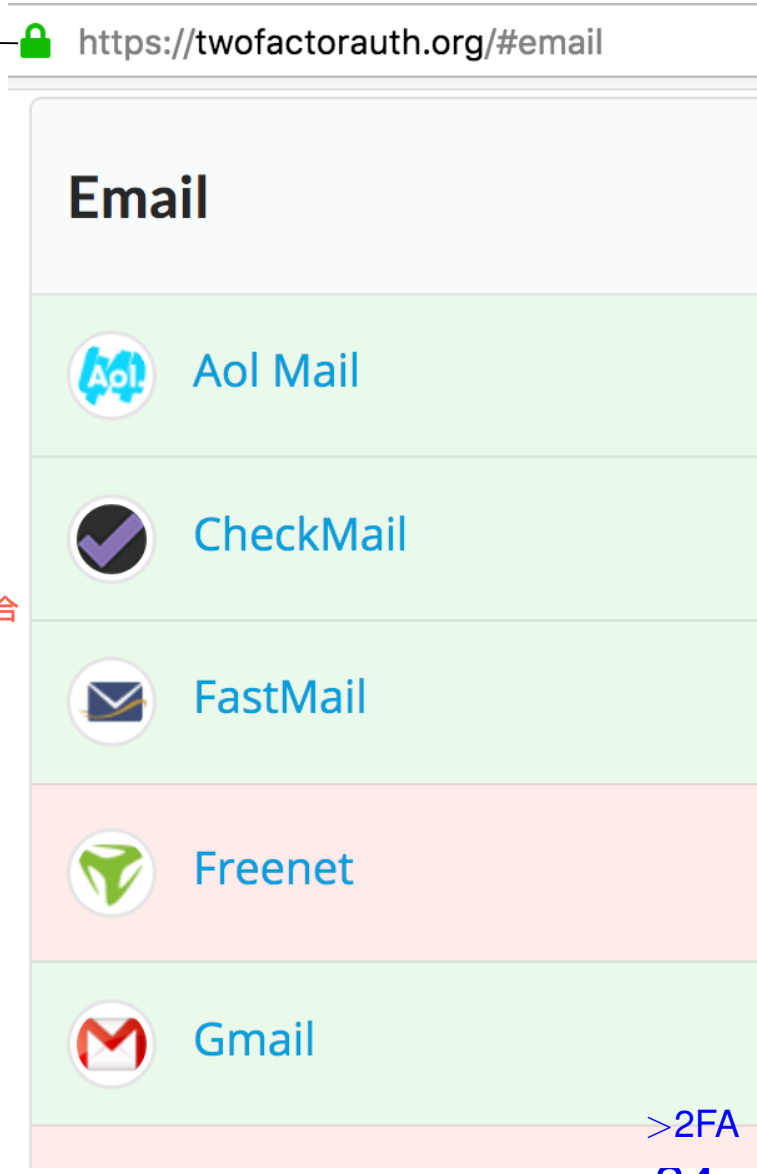


>2FA

Caveats with two factor authentication

- Not all services support 2FA
- SMS can be intercepted
- With Apple's two factor authentication, any linked device can generate codes => obtaining one device allows messing around with the others

并非所有的服务都支持2FA
•短信可以被拦截
•通过苹果的双因素认证，任何链接的设备都能生成代码=>获取一个设备允许与其他设备混合

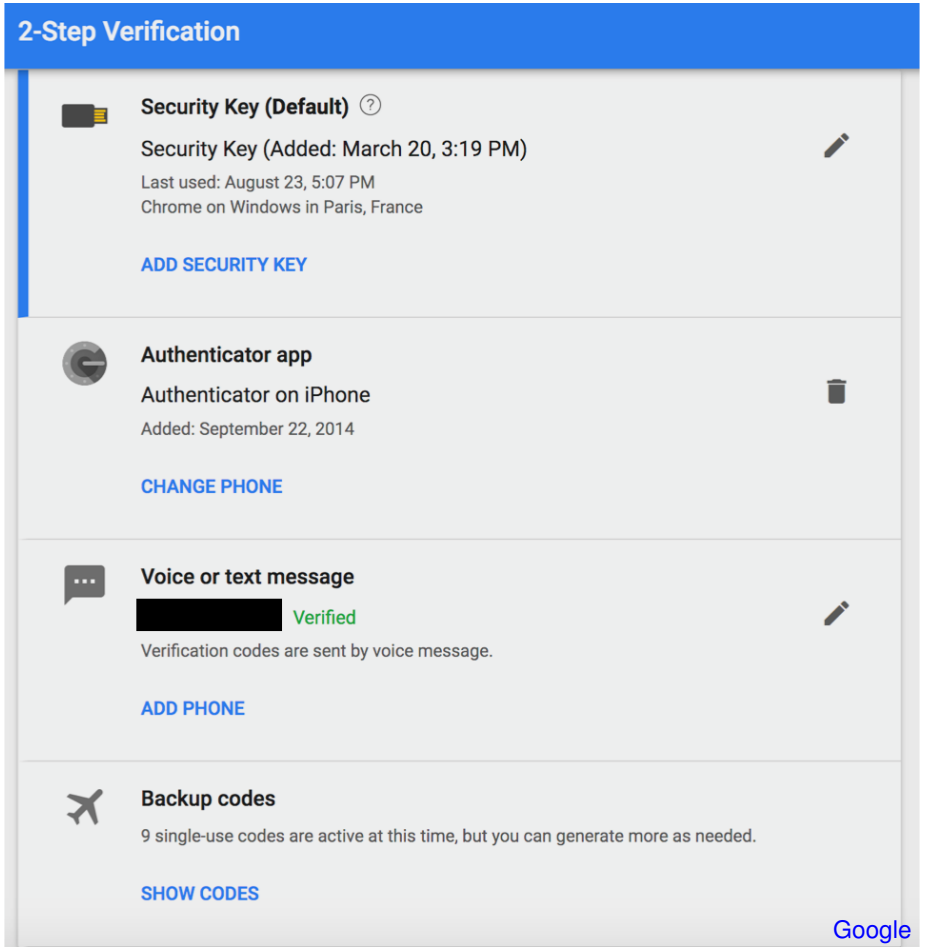


>2FA

Enable fall-back options! 启用回退选项！

Never enable 2FA without a fallback.
You risk getting locked out.

永远不要启用2FA若你没有后备。 你有可能被锁定。



穷人的堕落：用朋友的电话扫描2FA条码。

Poor man’s fall-back: scan the 2FA barcode with the phone of a friend.

Protect your devices

将两个障碍也添加到您的设备：拥有+密码

Add the two hurdles also to your devices: Possession + passcode

·在锁定屏幕上禁用通知。

- Disable notifications on the lock screen.

·在笔记本电脑上启用密码

考虑硬盘加密，否则代码是无用的。 Mac和Linux可以本地加密驱动器。

- Enable passcodes on your laptop

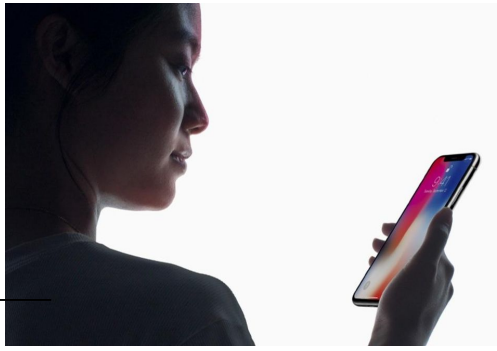
  Consider hard drive encryption, because otherwise the code is useless.

  Macs and Linux can encrypt the drive natively.

- Enable passcodes on your phone
  - passcode (cumbersome)
  - lock pattern (easy to copy)
  - fingerprint (great)
  - face id (can be exacted?)

在手机上启用密码
- 密码（繁琐）
- 锁定模式（易于复制）
- 指纹（很棒）
- 脸上的ID（可以被榨取？）

60% of people can reproduce the pattern after seeing it once in 1m distance



Apple

>2FA

Protect really sensitive data

Really sensitive data are

- embarrassing pictures of yourself or others
- files that contain passwords
- scans of your passport
- confidential information that you store for others

真正敏感的数据是
·自己或他人的尴尬照片
·包含密码的文件
·扫描您的护照
·您为其他人存储的机密信息
这样的数据可以用来让你难堪，模仿你，或勒索你。

Such data can be used to embarrass you, to impersonate you, or to blackmail you.

Wikipedia: Suicide of Amanda Todd
Wikipedia: Revenge Porn
Cyberbullying Research Center

Really sensitive data should never live outside protected spaces.

I.e., wherever it is, there should be 3+ hurdles to access it. Encrypt it (1,2).

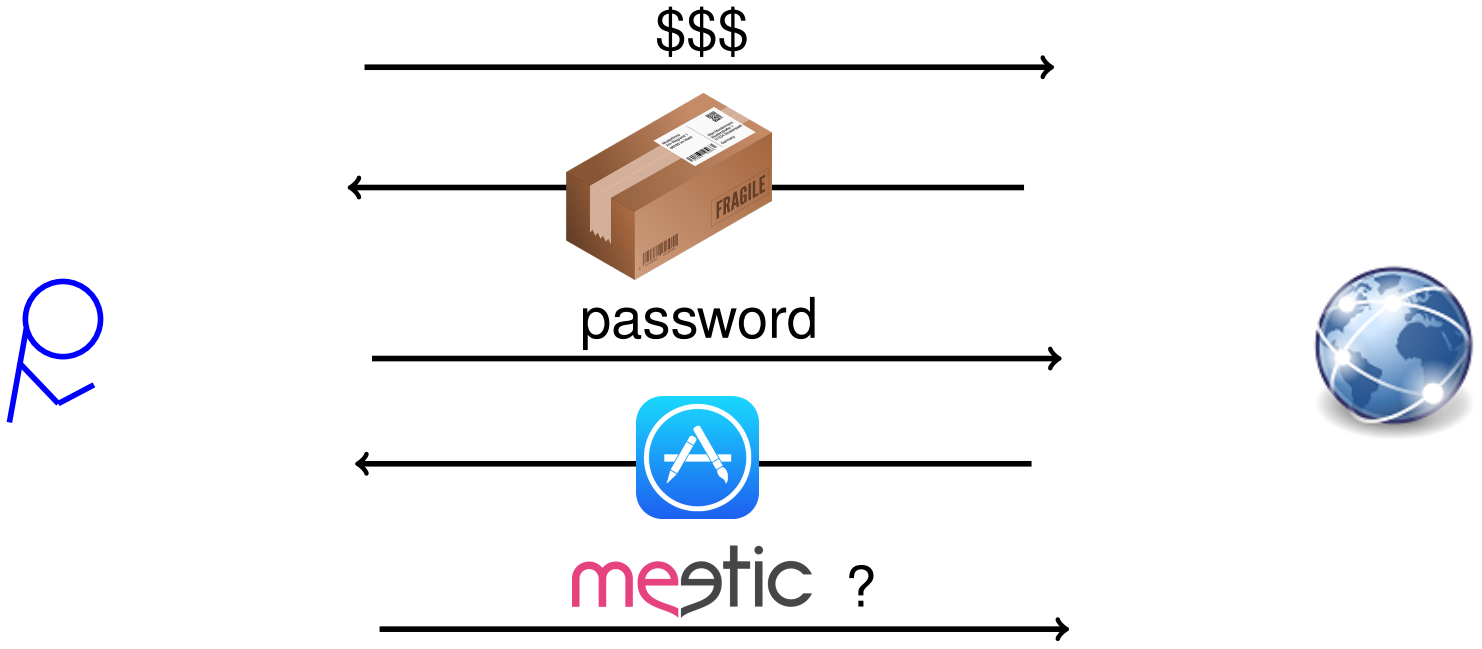
Overview

Protecting data against

- yourself
- hackers
- evil interlocutors
- companies
- governments

Interacting online

We exchange more than just clicks online.



If you're not talking to whom you think you talk, you're in trouble.

Any serious interaction on the Web should only happen if the identity of your partner has been confirmed by a trusted *third* party.

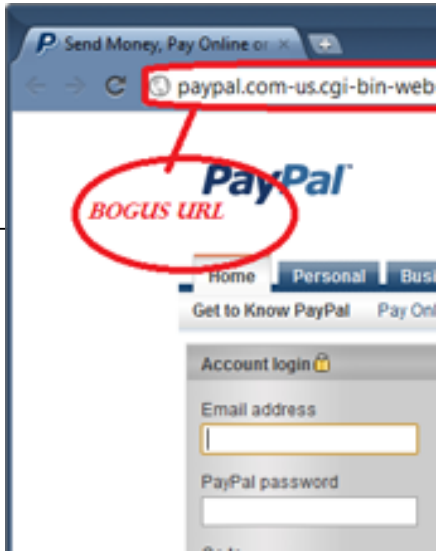
Extended Validation Certificates

扩展验证证书

You can be tricked into interacting with a bogus URL by:

- unreadable URLs
- homograph attacks

wikipedia.org



您可以通过以下方式欺骗与伪造的URL进行交互：

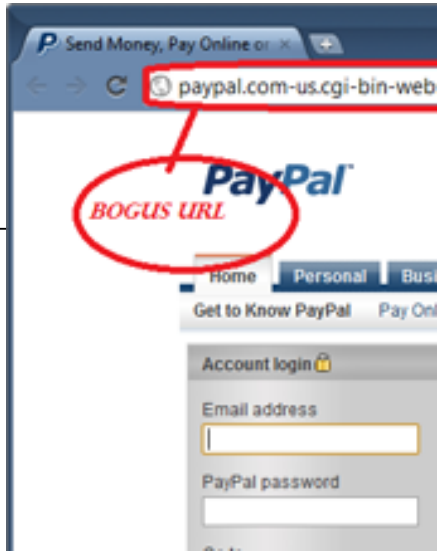
- 无法读取的网址
- 同形异义词攻击

Def: Extended Validation Certificate

You can be tricked into interacting with a bogus URL by:

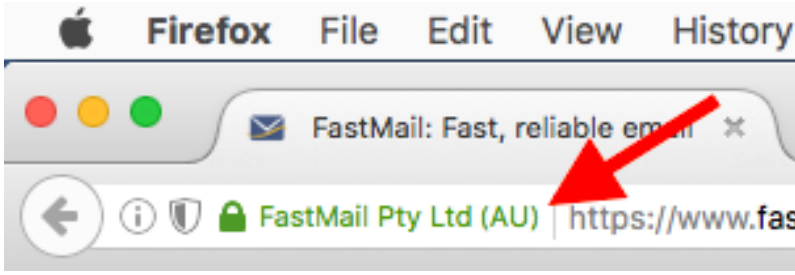
- unreadable URLs
- homograph attacks

wikipedia.org



扩展的验证证书意味着网页的身份已经被第三方确认。

An extended validation certificate means that the identity of the Web page has been confirmed by a third party.



Do not do banking without the EV certificate!

不要没有EV证书的银行业务！

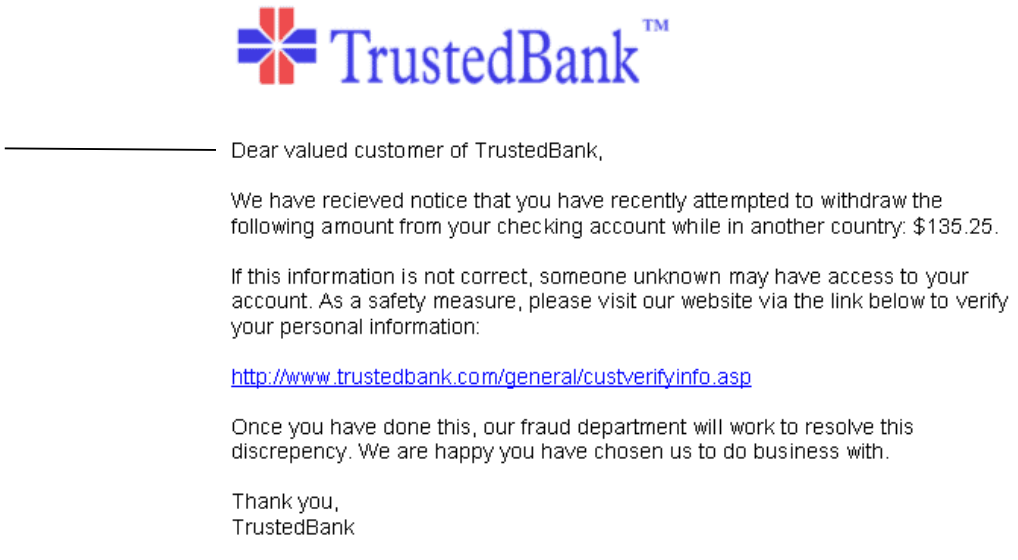
Def: Social Engineering

Social Engineering is the psychological manipulation of people into performing actions or divulging confidential information.

社会工程是对人们进行行为或泄露机密信息的心理操纵。

- Phishing (ask for password, pretending to be an authority)

钓鱼（要求输入密码，假装是权威）



- Vishing (phishing via automated phone message)

·钓鱼（通过自动电话信息进行钓鱼）

(real...)

- Baiting (leaving hardware around for others to pick it up)

诱饵（把硬件留给其他人捡起来）

(In a study, 98% of bait USB keys were picked up, and 45% called home [Wikipedia].)

（在一项研究中，98%的诱饵USB密钥被捡起，45%的人称为家庭[Wikipedia]。）

- Quid pro quo (attacker calling as help desk worker, offering help)

·Quid Pro（攻击者称为服务台工作人员，提供帮助）

>more

Watch out when downloading

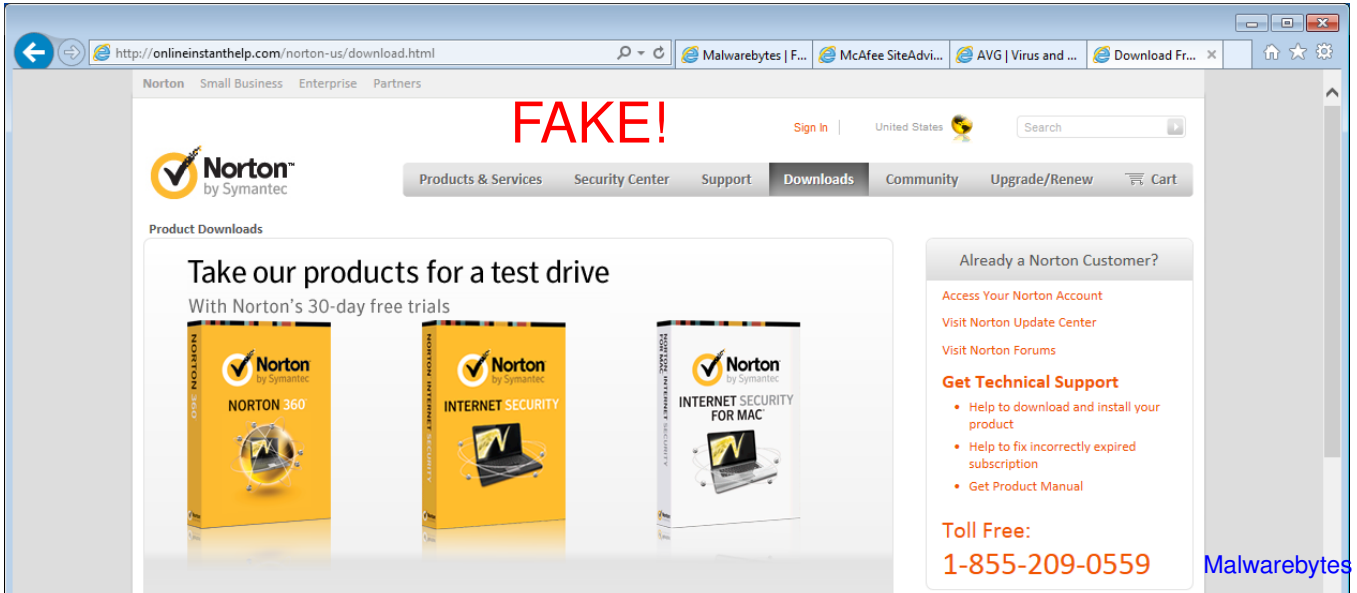
If you download bogus software, you may catch ad programs, keyloggers, viruses, or ransomware.

下载时请注意
如果您下载虚假软件，您可能会捕获广告程序，键盘记录器，病毒或勒索软件。
仅下载
•来自原始供应商（使用EV证书）
•如果由知名第三方（电脑杂志）推荐
•具有大量正面评级的iPhone应用程序

Download only

- from the original vendor (with EV certificate)
- if recommended by a reputed third party (computer magazine)
- iPhone apps that have a large number of positive ratings

>more



Malwarebytes

NakedSecurity

Do not trust online acquaintances

Do not send money to, send intimate pictures to, or meet in non-public places with online acquaintances.

不要相信在线的熟人
不要寄钱给亲密的照片，也不要在网上认识非公共场合。

Funny examples: 有趣的例子：

"On the Internet, nobody knows you're a dog."

Die PARTEI hacked AFD

Not so funny examples: News24

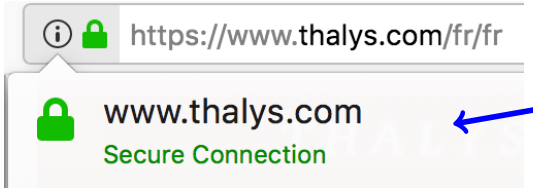
>more

Oh, and be careful

•不要点击随机广告
- Do not click on random advertisements

•不要打开来自未知发件人的电子邮件附件
- Do not open email attachments from unknown senders

•不要在没有HTTPS的情况下进行在线付款
- Do not make online payments without HTTPS



Does not verify identity,

but prevents evesdropping

- Do not buy from online shops, unless
  - they have an extended validation certificate
  - they are reputed (Amazon, Booking, etc.)
  - they are the official pages of brick-and-mortar shops (ask Google)

不要从网上商店购买，除非
- 他们有一个扩展的验证证书
- 他们被誉为（亚马逊，预订等）
- 它们是实体店铺的官方网页（问Google）

On a Mac: Install a virus scanner.

Everywhere: Keep all software updated.

On Windows 8+, the preconfigured virus scanner is generally enough.

Overview

Protecting data against

- yourself
- hackers
- evil interlocutors
- companies
- governments

What the big companies know

Your email provider, your social network and/or your search engine know

- your emails
- your Web searches
- your exact location (if logged in in Maps)
- the people you interact with
- what you like
- when you are online

您的电子邮件提供商，您的社交网络和/或您的搜索引擎知道
·您的电子邮件
·您的网页搜索
·您的确切位置（如果在地图上登录）·您与之互动的人
· 你喜欢什么
·当你在线

但是：公司提供高质量的免费服务作为回报！

BUT: The companies deliver a high-quality, free service in return!

What Facebook may know

your personality

type (better than your spouse)

substance use

field of study

impulsivity

political orientation

values

physical health

sensational interests

depression

gender

likely moving soon

age

receptivity to online insurance offers

“mother type”

education level

type of restaurants

relationship status

pain relief buyers

types of clothing

how much money will spend

balance on the credit card

wants to buy a car

type of vacation

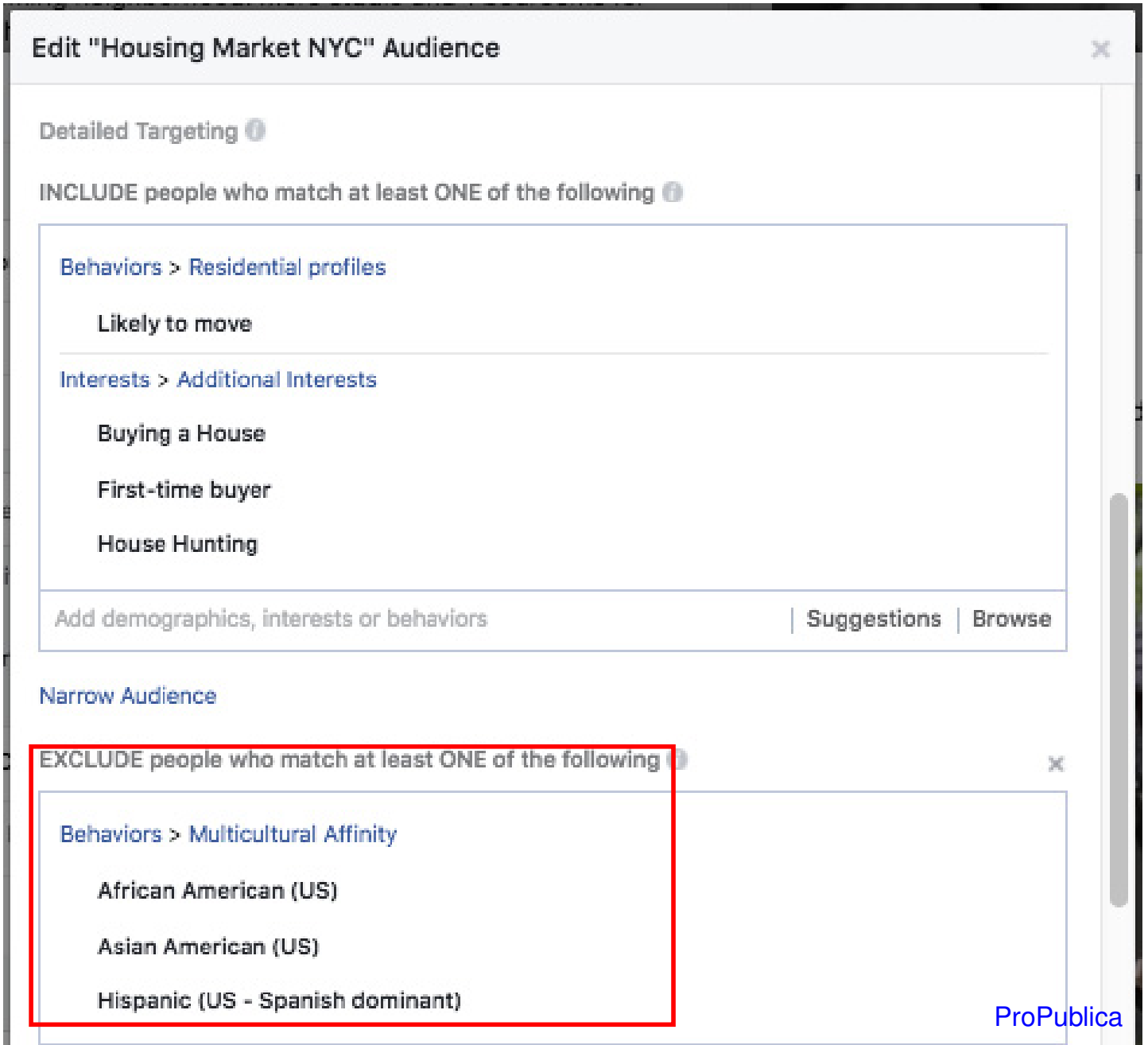
age of car

heavy buying of alcohol

purple = what advertisers can target

>more

Facebook allows targeting ads



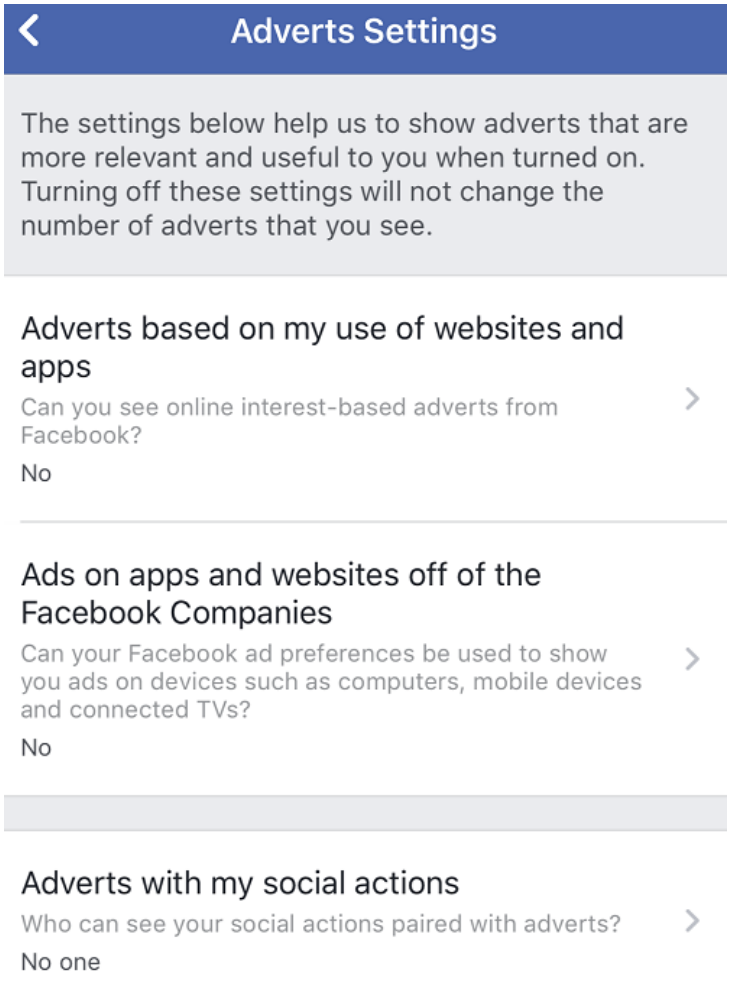
非政府组织ProPublica买了广告，要求排除非洲裔美国人，高中孩子们对轮椅坡道感兴趣的母亲，犹太人，来自阿根廷和西班牙语的外籍人士。

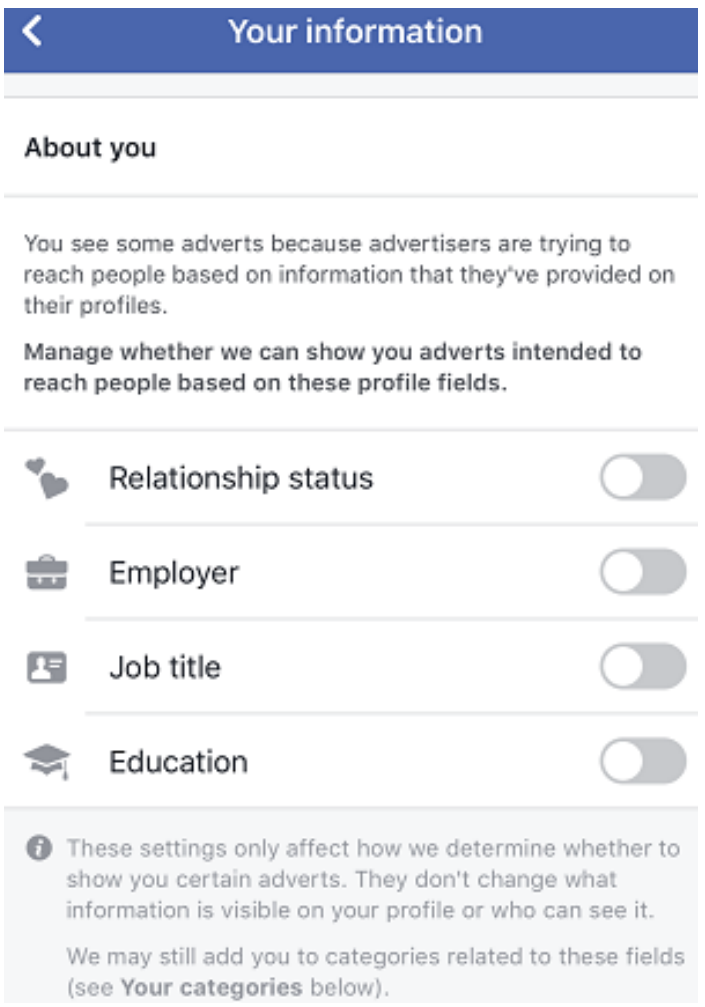
The NGO ProPublica bought ads and asked to exclude African Americans, mothers of high school kids people interested in wheelchair ramps, Jews, expats from Argentina and Spanish speakers.

ProPublica

>more

How Facebook puts ads





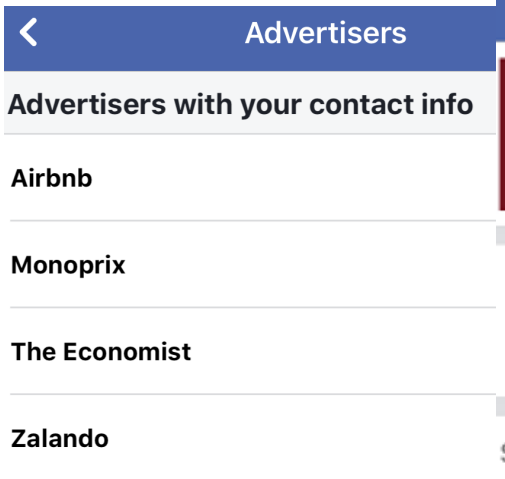
即使您不点击它们，Facebook“Like”按钮也会跟踪您。 即使你注销，他们的cookies仍然存在。

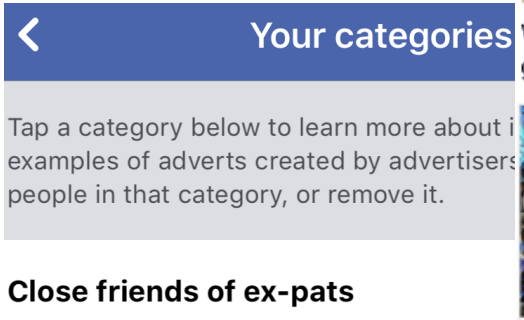
Facebook “Like” buttons trace you even if you don’t click them.

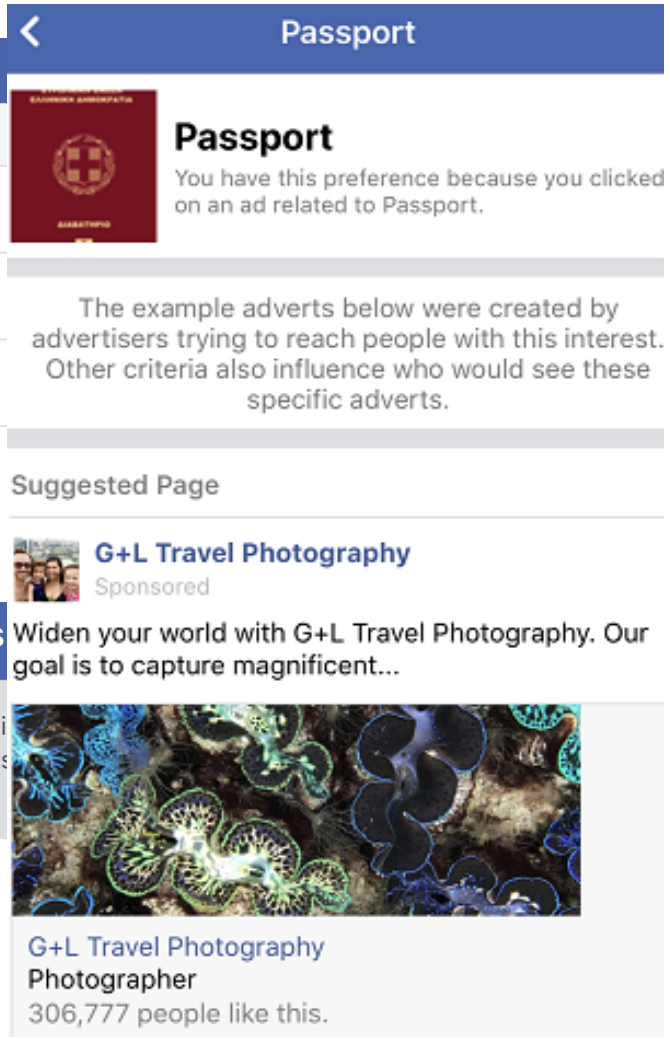
Even if you log out, their cookies remain.

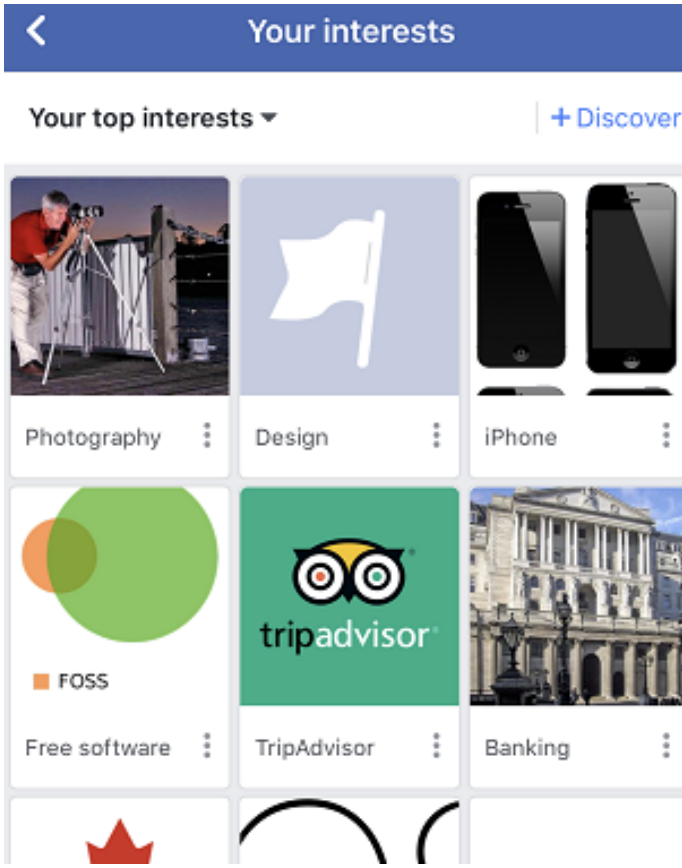
>more

How Facebook puts ads









Go check your privacy settings!

>more

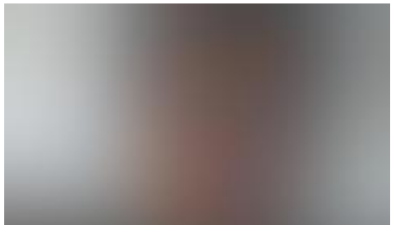
What WhatsApp knows

WhatsApp shares your phone number, contact list, and usage data with Facebook. The online time is also publicly available.

The messages themselves are private.

WhatsApp与Facebook分享您的电话号码，联系人列表和使用情况数据。 在线时间也是公开的。 消息本身是私人的。

Statistic for WhatsApp user: +316XXXXXXXX



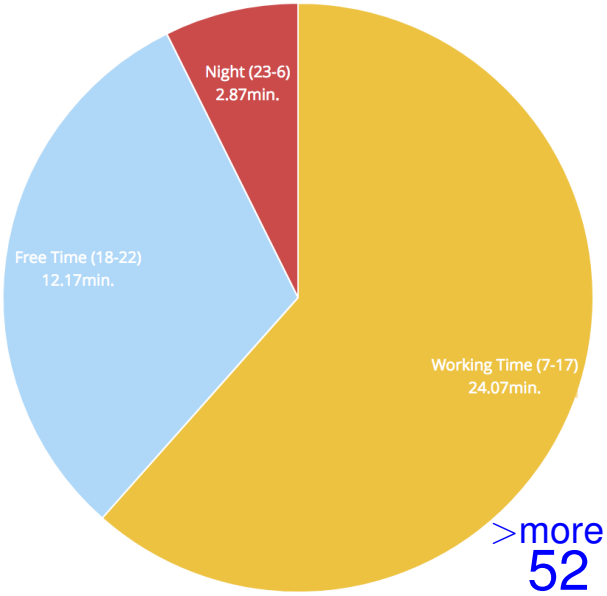
8362 connections 7 days 6:1:21 online
Ø 31.44 connections/day Ø 39:15min. online/day

Statusmessage:

Available

#Weekday	Avg. Online Time
Monday	48.63 min.
Tuesday	44.71 min.
Wednesday	49.92 min.
Thursday	39.15 min.
Friday	39.73 min.
Saturday	31.14 min.
Sunday	20.46 min.

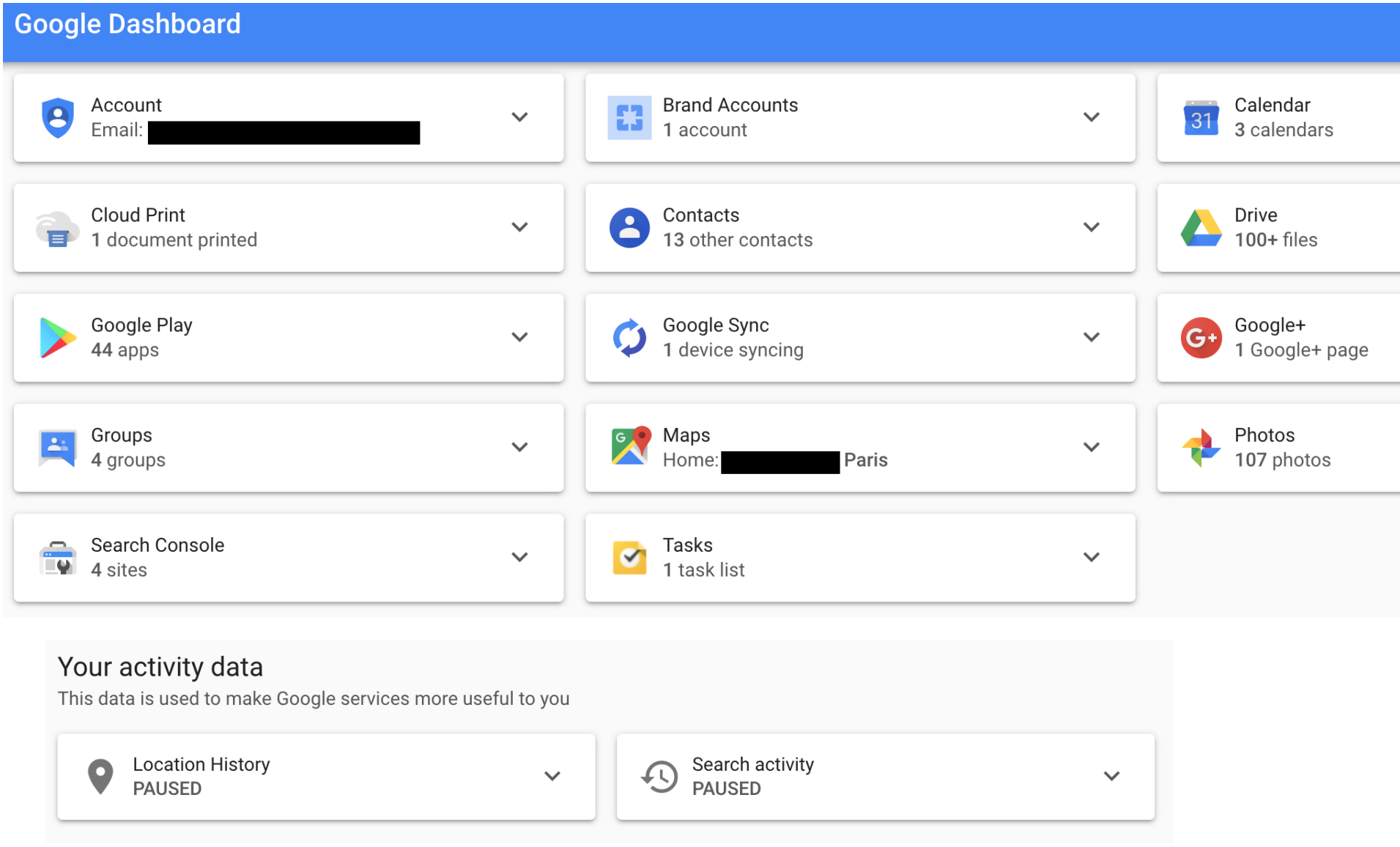
#Hour	Avg. Online Time	Avg. #Connections
0	0.74 min.	0.74
1	0.21 min.	0.25
2	0.05 min.	0.07
3	0.04 min.	0.05
4	0.1 min.	0.09



https://www.onlinestatusmonitor.com

>more

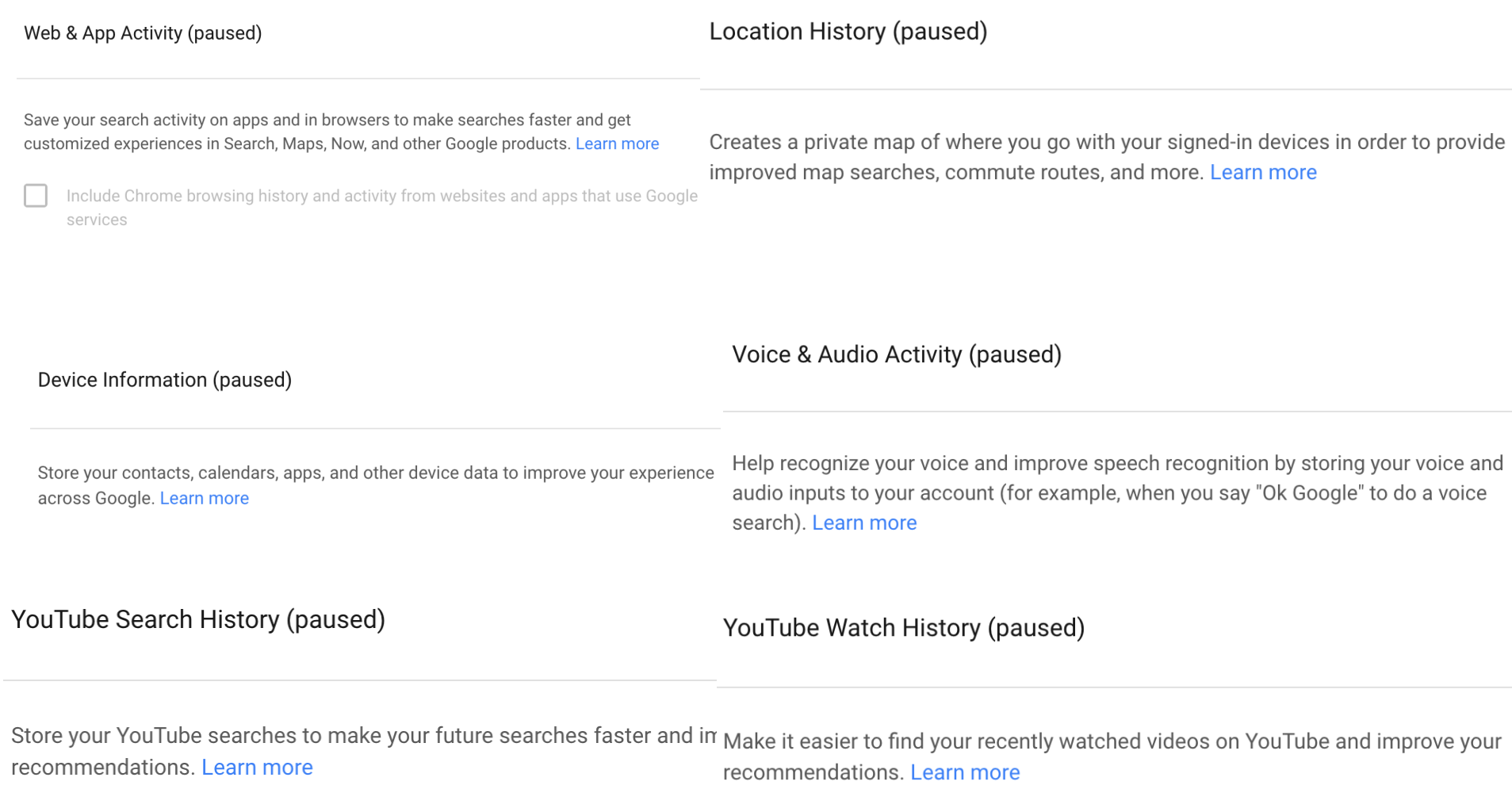
What Google knows



http://google.com/dashboard

>more

What Google knows



http://google.com/dashboard

Go check your privacy settings!

>more

Filter bubbles

Your service provider decides what you get to see.

It wants to keep you happy.

=> It may show you only what you like.

(think about Russia, Islam, Trump)

=> “intellectual isolation”, “echo chamber”,

“indoctrination with our own ideas”

=> reduced plurality, reinforced opinions, polarization

“You enter as a vegetarian, you leave as a vegan”

=> “threat to democracy” (Barack Obama)

Wikipedia: Filter bubble

过滤气泡
你的服务提供商决定你看到什么。
它想让你快乐。
=>它可能只显示你喜欢的东西。
（想想俄罗斯，伊斯兰教，特朗普）
>“智力隔离”，“回声室”，“用我们自己的想法灌输”
=>减少多元化，强化意见，两极分化“你作为一个素食者进入，你作为素食主义者离开”
>“对民主的威胁”（Barack Obama）

尝试一下：搜索一个有争议的话题，并将结果与朋友进行比较。

Try it out: search for a controversial topic,

and compare results with a friend.

>more

What it means if they know

服务提供商也可能知道您是否计划离婚
•有医疗问题
•有不寻常的性倾向
•未成年和怀孕
这个可以
•影响您看到的广告，即使Google明确表示不允许
•对服务提供者进行法院诉讼困难（勒索）。
可疑的服务提供商可能会将您的信息出售给数据经纪商，为其提供背景调查
•信用评分
•保险费用和保险索赔
看怀孕女儿的故事
•广告
•雇用决定

The service providers may also know if you are

- planning a divorce
- having a medical problem
- having an uncommon sexual preference
- under-age and pregnant

This can

- influence the ads you see, even if Google explicitly disallows it
- make court actions against the service providers difficult (blackmail).

Dubious services providers may sell your information to data brokers, feeding feeds background checks for

- credit scores
- insurance fees and insurance claims
- advertisements
- hiring decisions

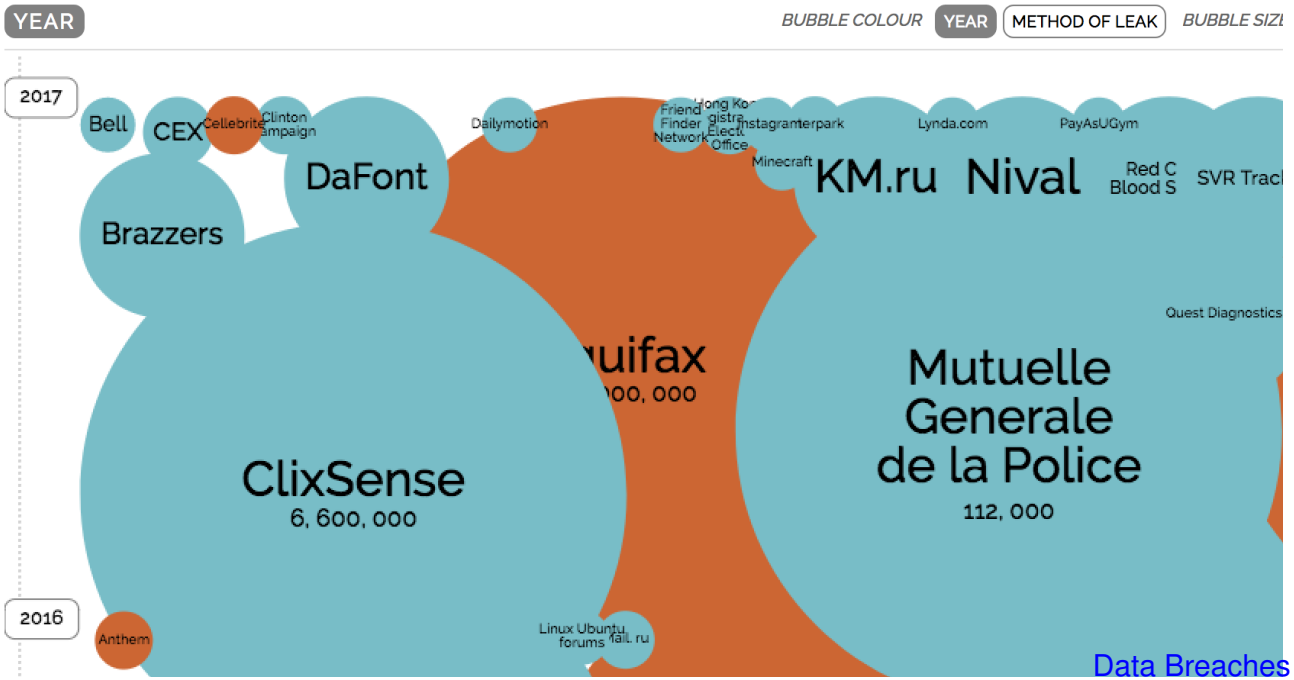
See story of pregnant daughter

>more

Leakage 泄漏

World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 10th Sep 2017)



In 2017, name, birthdates, home addresses, phones, religious affiliations, ethnicities &? political biases of 60% of the entire US population leaked to the public.

在2017年，姓名，生日，家庭住址，电话，宗教信仰，种族和？ 全美60%人口的政治偏见泄露给公众。

If such data is out

- somone can impersonate you
- someone can blackmail you
- your credibility suffers

如果这样的数据出来了
·有人可以冒充你
·有人可以勒索你
·你的信誉受损

>more

Give a chance to the small ones

Consider

·另类电子邮件提供商（您付费=>？他们不使用您的数据）

- alternative email providers (you pay =>? they don't use your data)

Criteria for choosing:

- two-factor authentication
- reputation
- Qualis rating

选择标准：
·双重身份验证
·信誉
·Qualis评级

Give a chance to the small ones

Consider

- alternative email providers (you pay =>? they don't use your data)
- alternative VOIP providers

WebRTC is a free protocol for voice and video calls over the Web, which works without creating an account or installing software.

=>? no sharing of data with NSA, less security flaws, no data collection

·另类电子邮件提供商（您付费=>? 他们不使用您的数据）
·另类VOIP提供商，WebRTC是一个通过网络进行语音和视频通话的免费协议，无需创建帐户或安装软件。
=>? 没有与NSA共享数据，安全漏洞少，没有数据收集

See here for a list

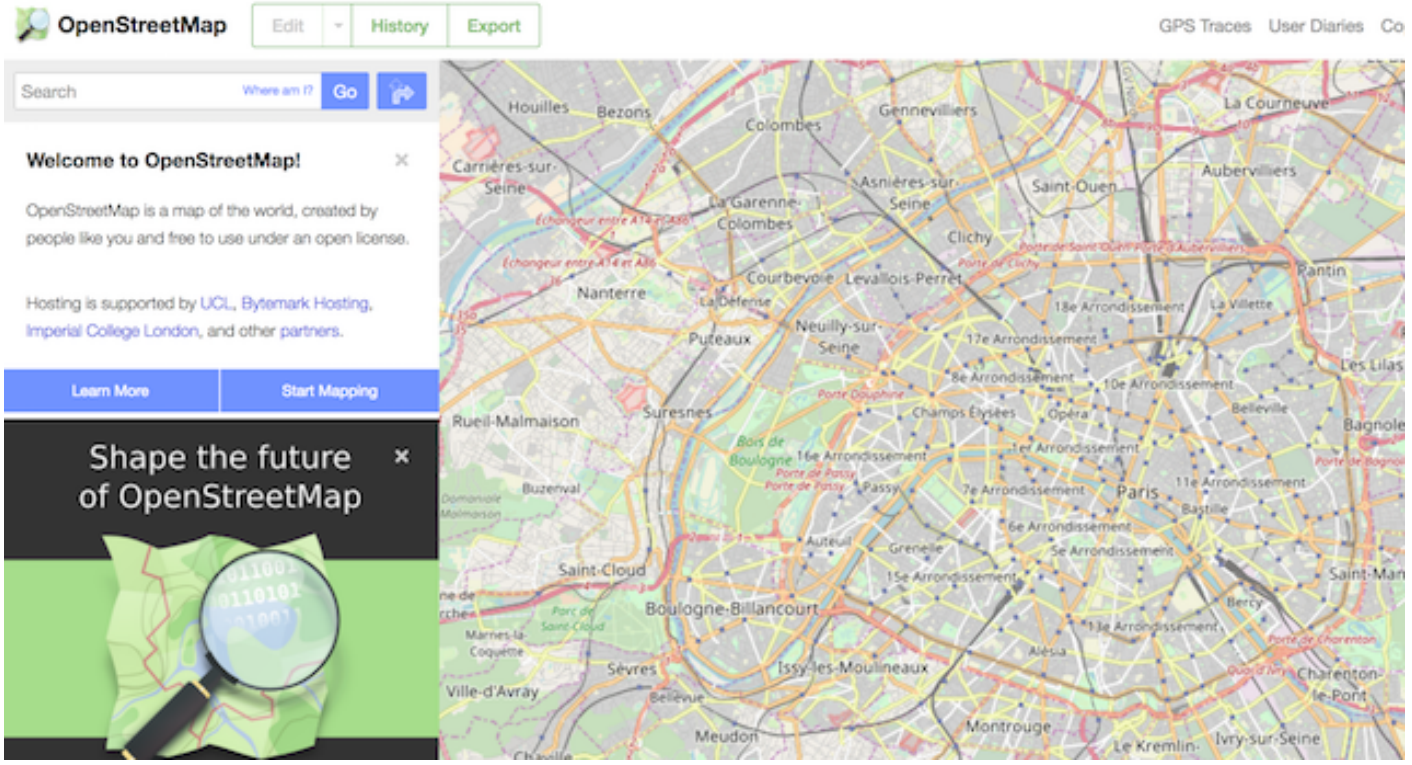
Give a chance to the small ones

Consider

- alternative email providers (you pay =>? they don't use your data)
- alternative VOIP providers
- alternatives to Map apps where you log in.

·另类电子邮件提供商（您付费=>？他们不使用您的数据）
·另类VOIP提供商
·登录的地图应用程序的替代方法。
OpenStreetMaps是一个协作开放地图项目。

OpenStreetMaps is a collaborative open map project.



There are apps for it

>more

Give a chance to the small ones

Consider

- alternative email providers (you pay =>? they don't use your data)
- alternative VOIP providers
- alternatives to Map apps where you log in.
- alternative search engines

>more

Give a chance to the small ones

Consider

- alternative email providers (you pay =>? they don't use your data)
- alternative VOIP providers
- alternatives to Map apps where you log in.
- alternative search engines
- alternative social networks (no...)
- alternative chat programs (no...)
- alternative browsers (no...; just check the privacy settings)

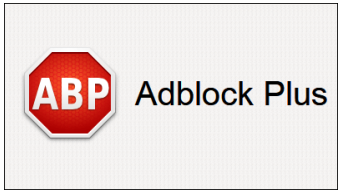
·替代电子邮件提供商（您付费=>？他们不使用您的数据）
·替代VOIP提供商
·登录的地图应用程序的替代方法。
·替代搜索引擎
·另类社交网络（不...）
·另类聊天程序（不...）
·替代浏览器（不... ...只是检查隐私设置）

Check your browser settings

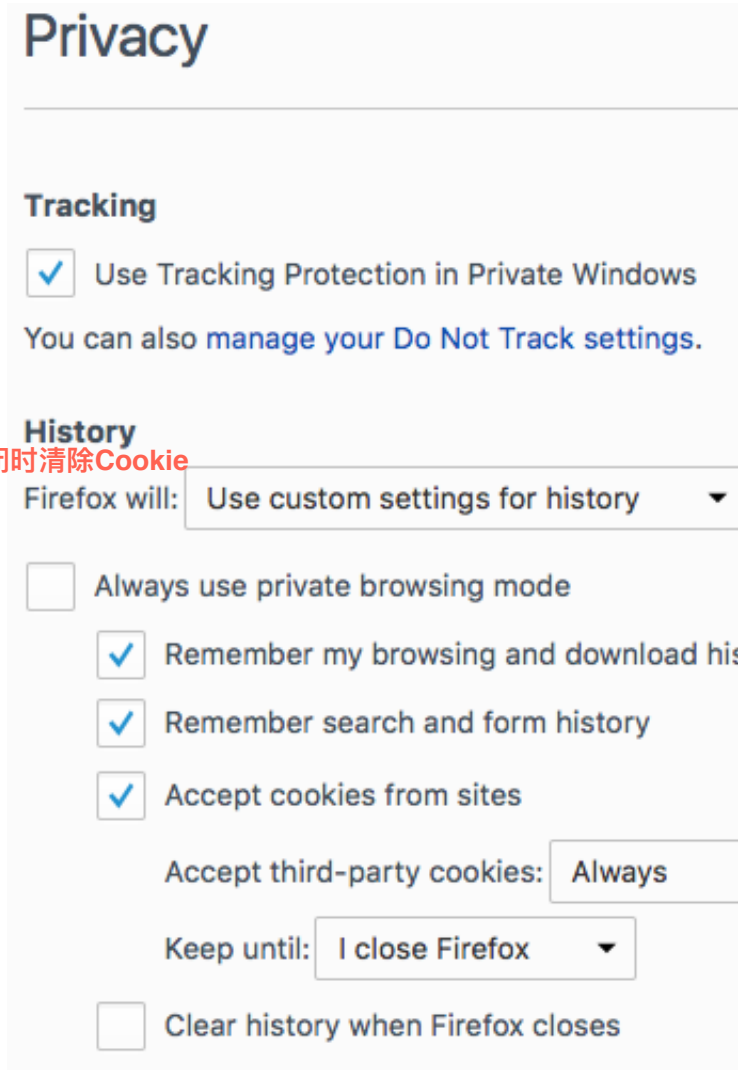
You can

- verify your browser privacy settings
  (in particular Web auto-completion)
- clear cookies upon closing
- remove toolbar plugins
- use privacy plugins

您可以
•验证您的浏览器隐私设置
（尤其是Web自动完成）•关闭时清除Cookie
•删除工具栏插件
•使用隐私插件



(has deal with advertisers)



Also check your phone settings.

Overview

Protecting data against

- yourself
- hackers
- evil interlocutors
- companies
- governments

Protecting against the government?

- if you are a political activist in a less democratic country
- if you want to guard against social scoring (in China, your social media interactions will determine your rights.)
- if you generally don't like the government spying on you

防止政府?
·如果你是一个不太民主的国家的政治活动家
·如果您想防范社交评分（在中国，您的社交媒体互动将决定您的权利）。
·如果你一般不喜欢政府监视你

Protecting against the government?

·如果你是不太民主的国家的政治活动家·如果你想防范社会打分（在中国，你的社交媒体互动将决定你的权利。）
·如果你一般不喜欢政府监视你

- if you are a political activist in a less democratic country
- if you want to guard against social scoring (in China, your social media interactions will determine your rights.)
- if you generally don't like the government spying on you

Government Surveillance: Last Week Tonight with John Oliver (HBO)

Last Week Tonight with John Oliver: Government Surveillance

If I had knowledge that the US government had a picture of my d*ck, I would be very p*ssed.

Protecting against the government?

- if you are a political activist in a less democratic country
- if you want to guard against social scoring (in China, your social media interactions will determine your rights.)
- if you generally don't like the government spying on you

Government Surveillance: Last Week Tonight with John Oliver (HBO)

Can they see my d*ck?

Yes. [...]
Anytime you have your picture on gmail [...], your junk ends up in the[ir] database.

Last Week Tonight with John Oliver: Government Surveillance

National Security Letters

NSA可以要求服务提供商在不告知客户的情况下翻转客户数据。

The NSA can request that a service provider turns over client data without telling the client about it.

Houston Division
1 Justice Park Drive
Houston, TX 77092
April 06, 2016

[redacted]
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
650-253-[redacted]

Dear [redacted]:

Pursuant to Title 18, United States Code (U.S.C.), Section 2709 (Section 201 of the Electronic Communications Privacy Act), to the extent you provide an electronic communication service as defined in 18 U.S.C. § 2510(15), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the name, address, length of service, and electronic communications transactional records for all services, as well as all accounts, provided to the individual(s) or identifier(s) listed below:

Account:	For Following Date(s) (YYYY-MM-DD):
[redacted]@gmail.com	From Inception to Present

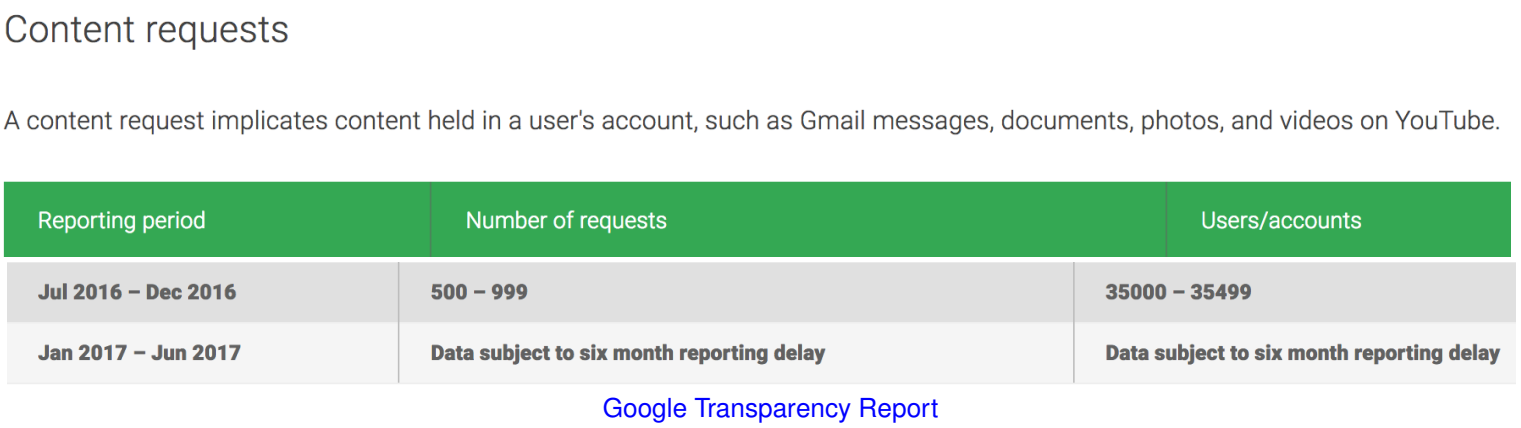
In accordance with 18 U.S.C. §§ 2709(c)(1)-(2), you, any officer, employee, or agent of yours are prohibited from disclosing this letter

NSL to Google

Content requests

The FISA Amendments Act, passed in 2008, authorizes the government to require US companies to provide information and the content of communications associated with the accounts of non-U.S. citizens or non-lawful permanent residents who are located outside the US.

2008年通过的FISA修正法案授权政府要求美国公司提供与美国以外的非美国公民或非合法永久居民账户相关的信息和通讯内容。



Content requests

A content request implicates content held in a user's account, such as Gmail messages, documents, photos, and videos on YouTube.

Reporting period	Number of requests	Users/accounts
Jul 2016 – Dec 2016	500 – 999	35000 – 35499
Jan 2017 – Jun 2017	Data subject to six month reporting delay	Data subject to six month reporting delay

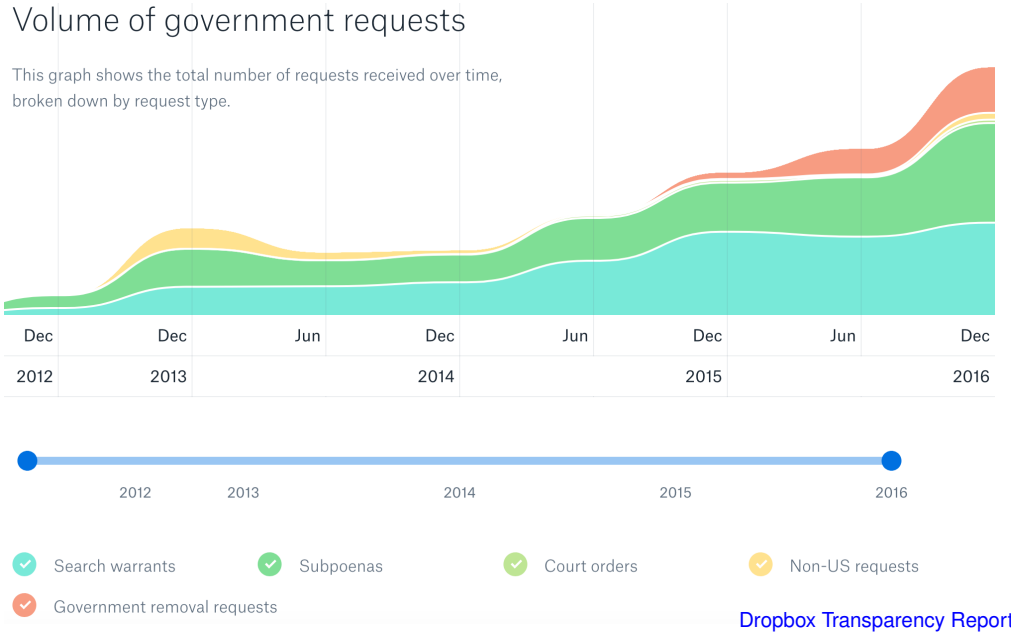
Google Transparency Report

Content requests

Dropbox guiding principles

- “Online services should be allowed to report the exact number of government data requests received”
- “Government data requests should be limited to specific people and investigations”
- “Governments should never install backdoors into online services or compromise infrastructure to obtain user data”

•“应允许在线服务报告收到的政府数据请求的确切数量”
•“政府数据请求应限于特定的人员和调查”
•“政府决不应该将后门安装到在线服务或妥协基础结构中以获取用户数据”



≈ 1000

Dropbox Transparency Report

Using government-style protection

You may also want to use this type of protection for

- personal problems you want to keep secret
- business secrets that the competition may not know
- activity that is (moral but) illegal in your country
- communication with whistle-blowers
- traits that are despised by society (e.g, being atheist in Bangladesh)
- activism against powerful or violent people

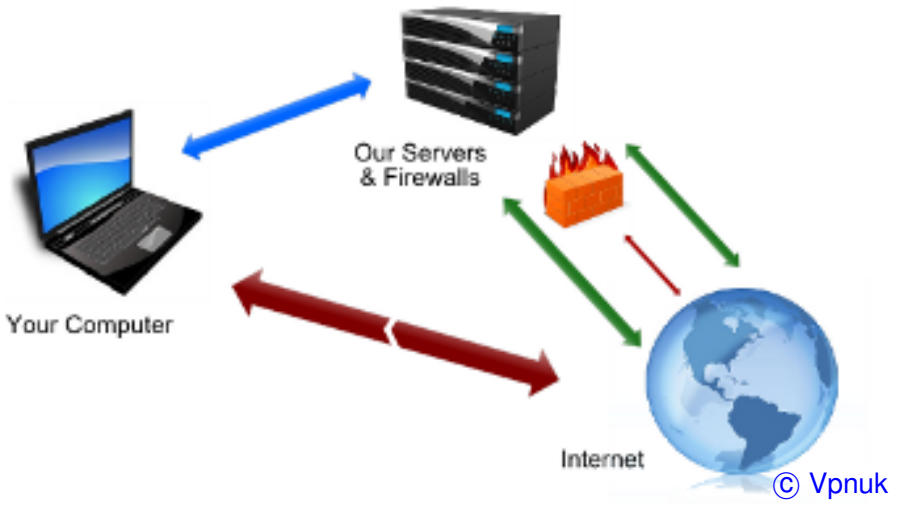
采用政府式的保护
您可能也想要使用这种类型的保护
•你想保密的个人问题
•竞争可能不知道的商业秘密
•在您的国家（道德但是）非法的活动
•与举报人沟通
•被社会所轻视的特征（例如在孟加拉国是无神论者）
•针对强大或暴力的人的激进主义

->email

Def: Virtual Private Networks

A Virtual Private Network (VPN) is a software that encapsulates your data from your computer to the Internet in a secure tunnel.

虚拟专用网络（VPN）是一种将数据从计算机封装到互联网的软件。



=> Nobody can see it's you who accesses the page

Useful if

如果有用
·您想要访问您所在国家/地区阻止的页面
·您想隐藏您正在访问的页面
·您正在使用无保护的无线网络

- you want to access a page that is blocked in your country
- you want to hide that you're accessing the page
- you are using an unprotected Wifi

Virtual Private Networks

A Virtual Provate Network (VPN) is a software that encapsulates your data from your computer to the Internet in a secure tunnel.

=> Nobody can see it's you who accesses the page

But:

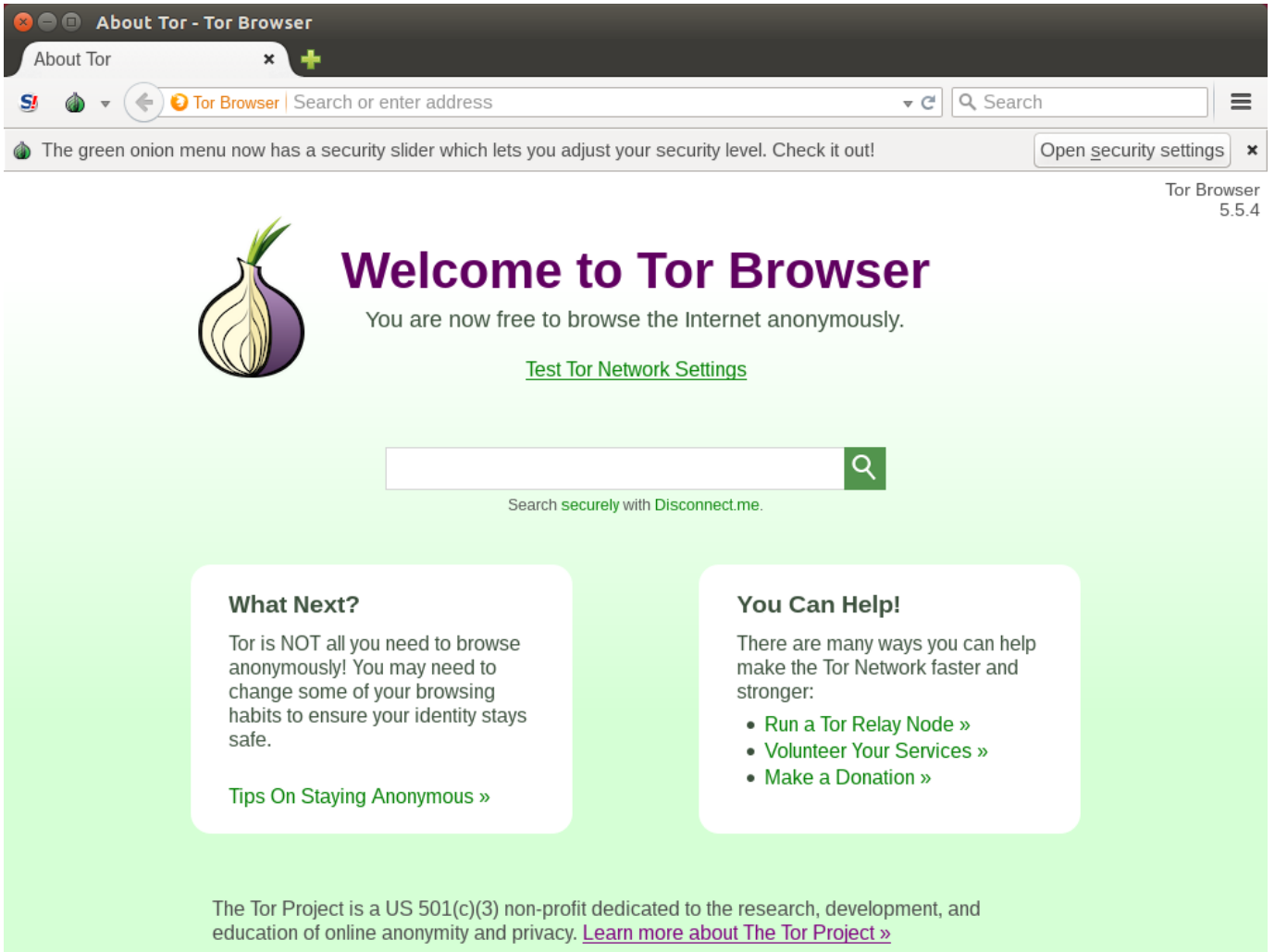
- the Internet access is usually slower
- VPNs are usually not for free
- some free VPNs sell your data for marketing purposes
- if you want to protect the data, not the visit, HTTPS is sufficient

但：
·互联网访问通常较慢
VPN通常不是免费的
·一些免费的VPN销售您的数据用于营销目的
·如果要保护数据，而不是访问，HTTPS就足够了

TOR

TOR浏览器通过分布式网络路由查询，从而阻止任何跟踪。

The TOR browser routes your queries through a distributed network, thus thwarting any tracking.



But: Due to the overhead, internet access via TOR is very slow.

->email

Def: End-to-end encrypted storage

An end-to-end encrypted cloud service encrypts your data on your device before uploading it into the cloud.

端到端的加密云服务在将您的设备上传到云中之前，会对您的数据进行加密。

- The service provider can't read it
- Nobody in the middle can read it
- The service provider cannot hand it to a government
- If the service provider is hacked, the data is of no use

·服务提供商无法读取它
·中间没有人可以阅读
·服务提供商无法将其交给政府
·如果服务提供商遭到黑客入侵，则数据是无用的

Disadvantages:

- usually less mainstream, more cumbersome providers
- usually no means to reset your password
- no added data services

缺点：
通常不太主流，更繁琐的提供商
·通常没有办法重置您的密码
·没有添加数据服务

Watch out for:

- two-factor authentication
- ability to undelete

->email

Phone, SMS, Chats

- the government can have access to the phone meta data
- SMS can be intercepted
- chats should be end-to-end encrypted

•政府可以访问手机元数据
•短信可以被拦截
•聊天应该是端对端的加密
端到端的加密聊天系统包括以下内容：

End-to-end encrypted chat systems include the following:

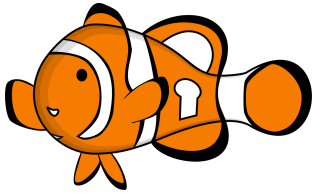
WhatsApp

Telegram

Signal Private Messenger

(recommended by Edward Snowden)

Single provider



OMEMO + XMPP

ChatSecure

Open to several providers

Email encryption

Solution 0: send encrypted cloud storage link (“share link”)

Advantage: works out of the box if you have such a cloud storage

Disadvantage: cumbersome for sender and recipient

解决方案0：发送加密的云存储链接（“共享链接”）
优点：如果您有这样的云存储，开箱即用
缺点：发件人和收件人麻烦

Solution 1: encrypted email services.

Advantage: easy to use

Disadvantage: provider dependency (works only inside 1 provider)

解决方案1：加密电子邮件服务
优点：易于使用
缺点：提供者依赖（仅在1提供者内部工作）

Solution 2: SMIME

Advantage: well implemented

Disadvantage: relies on central authority

解决方案2：SMIME
优势：实施得好
缺点：依靠中央权威

Solution 3: PGP

Advantage: provider-independent, decentralized

Disadvantage: cumbersome to use

解决方案3：PGP
优点：独立于供应商，分散
劣势：使用起来麻烦

RSA

RSA (Rivest-Shamir-Adleman) is a method for sending an encrypted message that works as follows (simplified):

1. Choose your public key pair n, e

RSA（Rivest-Shamir-Adleman）是一种发送加密消息的方法，其工作原理如下（简化）：
1.选择你的公钥对n，e

Public key:

$e = 7, n = 33$

Barack

RSA

RSA (Rivest-Shamir-Adleman) is a method for sending an encrypted message that works as follows (simplified):

1. Choose your public key pair n, e
2. Compute your private key d such that

$$\forall m : (m^{e \times d} mod n) = m mod n$$

计算你的私钥d

Public key:

$e = 7, n = 33$

Private key:

$d = 3$

Barack

RSA

RSA (Rivest-Shamir-Adleman) is a method for sending an encrypted message that works as follows (simplified):

1. Choose your public key pair n, e
2. Compute your private key d such that

   $\forall m : (m^{e \times d} mod n) = m mod n$
3. The sender encrypts a message m as $c = m^e mod n$

3.发送者将消息m加密为c = m^e mod n

Public key:

$e = 7, n = 33$

Private key:

$d = 3$

Angela

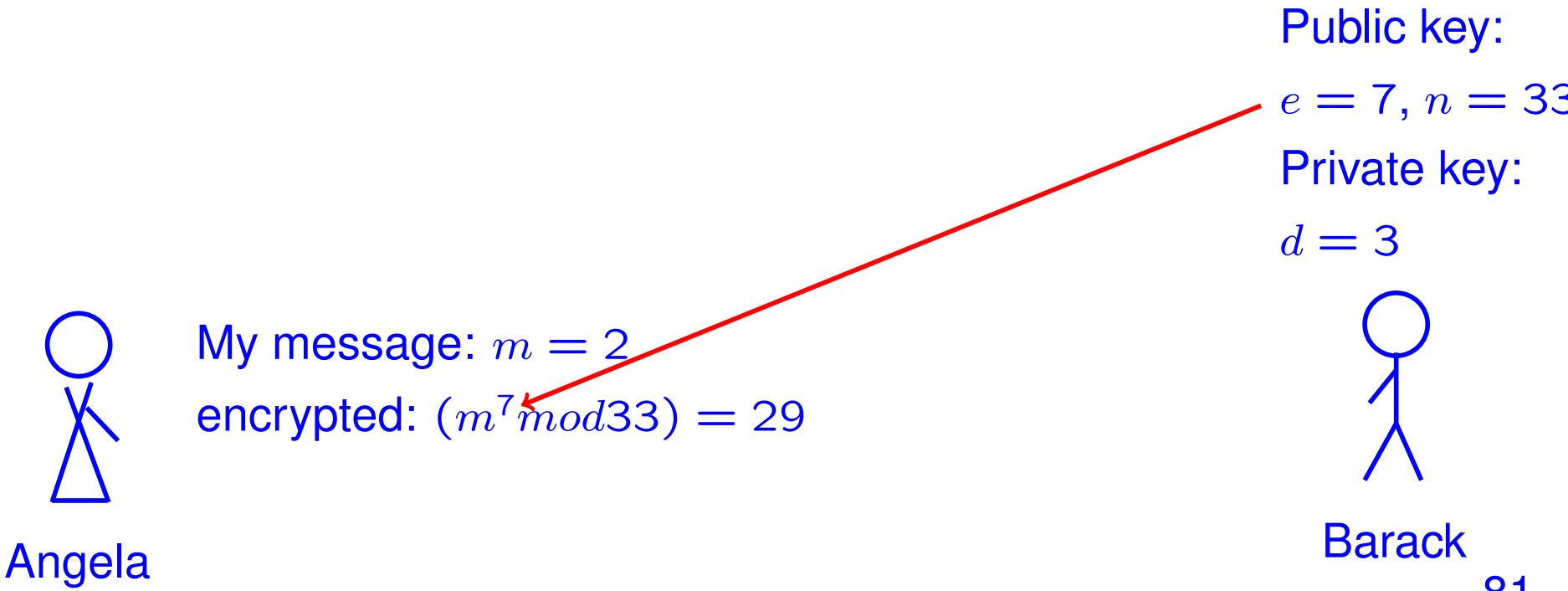
My message: $m = 2$

Barack

RSA

RSA (Rivest-Shamir-Adleman) is a method for sending an encrypted message that works as follows (simplified):

1. Choose your public key pair n, e
2. Compute your private key d such that
   $\forall m : (m^{e \times d} mod n) = m mod n$
3. The sender encrypts a message m as $c = m^e mod n$



RSA

RSA (Rivest-Shamir-Adleman) is a method for sending an encrypted message that works as follows (simplified):

1. Choose your public key pair n, e
2. Compute your private key d such that
   $\forall m : (m^{e \times d} mod n) = m mod n$
3. The sender encrypts a message m as $c = m^e mod n$
4. The encrypted message c is sent

4.加密的消息c被发送

Public key:

$e = 7, n = 33$

Private key:

$d = 3$

Angela

My message: $m = 2$

encrypted: $(m^7 mod 33) = 29$

29 received

Donald cannot understand 29

Barack

Def: RSA

RSA (Rivest-Shamir-Adleman) is a method for sending an encrypted message that works as follows (simplified):

1. Choose your public key pair n, e
2. Compute your private key d such that
   $\forall m : (m^{e \times d} mod n) = m mod n$
3. The sender encrypts a message m as $c = m^e mod n$
4. The encrypted message c is sent
5. You decrypt the message c as
   $c^d mod n = (m^e mod n)^d mod n = m^{e \times d} mod n = m$

Public key:

$e = 7, n = 33$

Private key:

$d = 3$

Angela

29 received,

compute

$(29^3 mod 33) = 2$

Barack

RSA in detail

RSA (Rivest-Shamir-Adleman) is a method for sending an encrypted message that works as follows:

1. Choose secret primes p, q, compute $n = p \times q$, compute $\phi(n) = (p-1) \times (q-1)$

   $p = 3, q = 11, n =$

   $\phi(n) = (3-1) \times (11-1$

2. Choose a prime number $e < \phi(n)$, publish e and n.

   $e =$

3. Compute your private key d such that

   $(e \times d) mod \phi(n) = 1.$

   By Euler's theorem, this implies

   $\forall m : (m^{e \times d} mod n) = m mod n$

   $d = 3$, because $((7 \times 3) mod 20) =$

   (d can be computed only by knowing the secret numbers p and q)

   $\forall m : (m^{7 \times 3} mod 33) = (m mod 33$

4. Encrypt m as $c = m^e mod n$, decrypt c as $c^d mod n = m^{e \times d} mod n = m$

Angela

My message: $m = 2$

encrypted: $(m^7 mod 33) = 29$

29 received, compute $(29^3 mod 33) = 2$

Barack

Def: PGP

PGP (Pretty Good Privacy) is an encryption program that implements RSA. The main advantage of PGP (and RSA) is that no shared secret password is needed. Sending a PGP message from Angela to Barack works as follows:

PGP（Pretty Good Privacy）是一个实现RSA的加密程序。PGP（和RSA）的主要优点是不需要共享密码。 从安吉拉发送PGP消息到Barack的工作如下：

Public key of the receiver

(available on a key server, on a Web page, or given in person)

Private key of the receiver

Angela

Message

Encrypted message

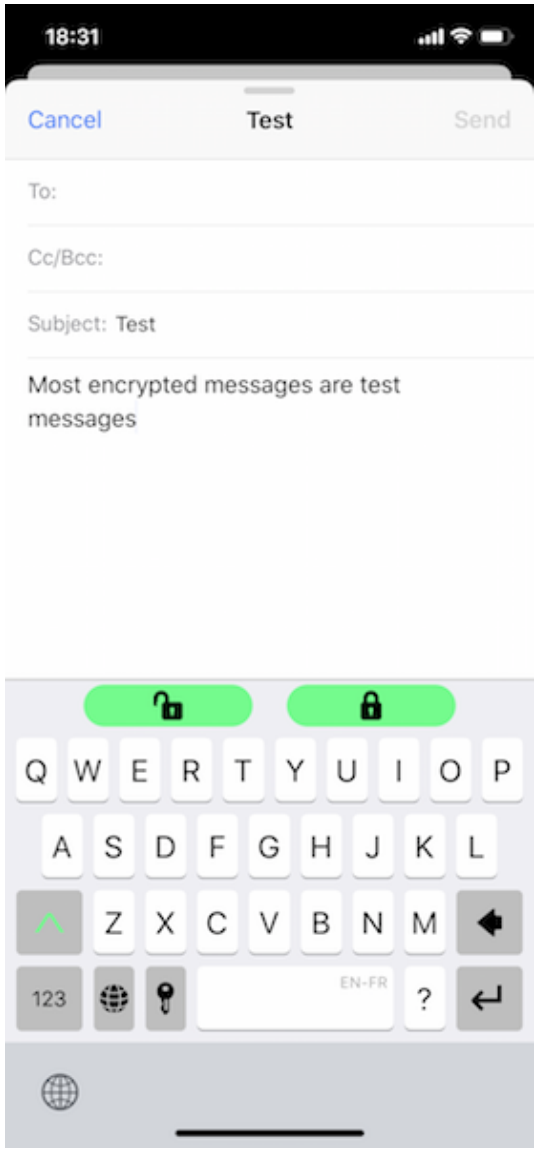
transmission

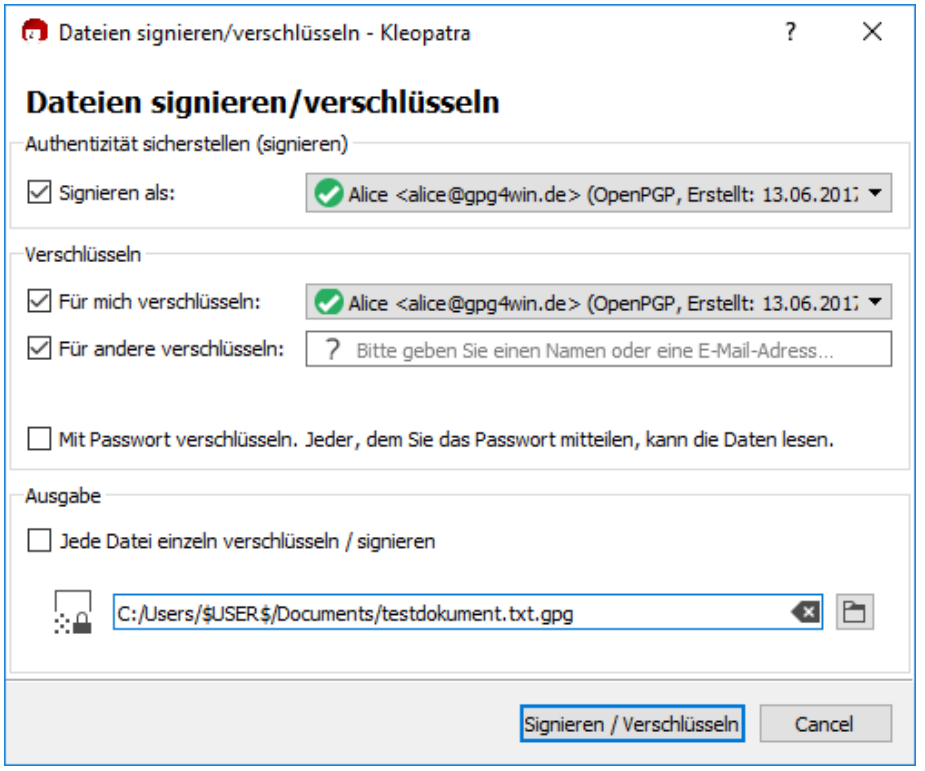
Encrypted message

Message

Barack

PGP encryption in practice

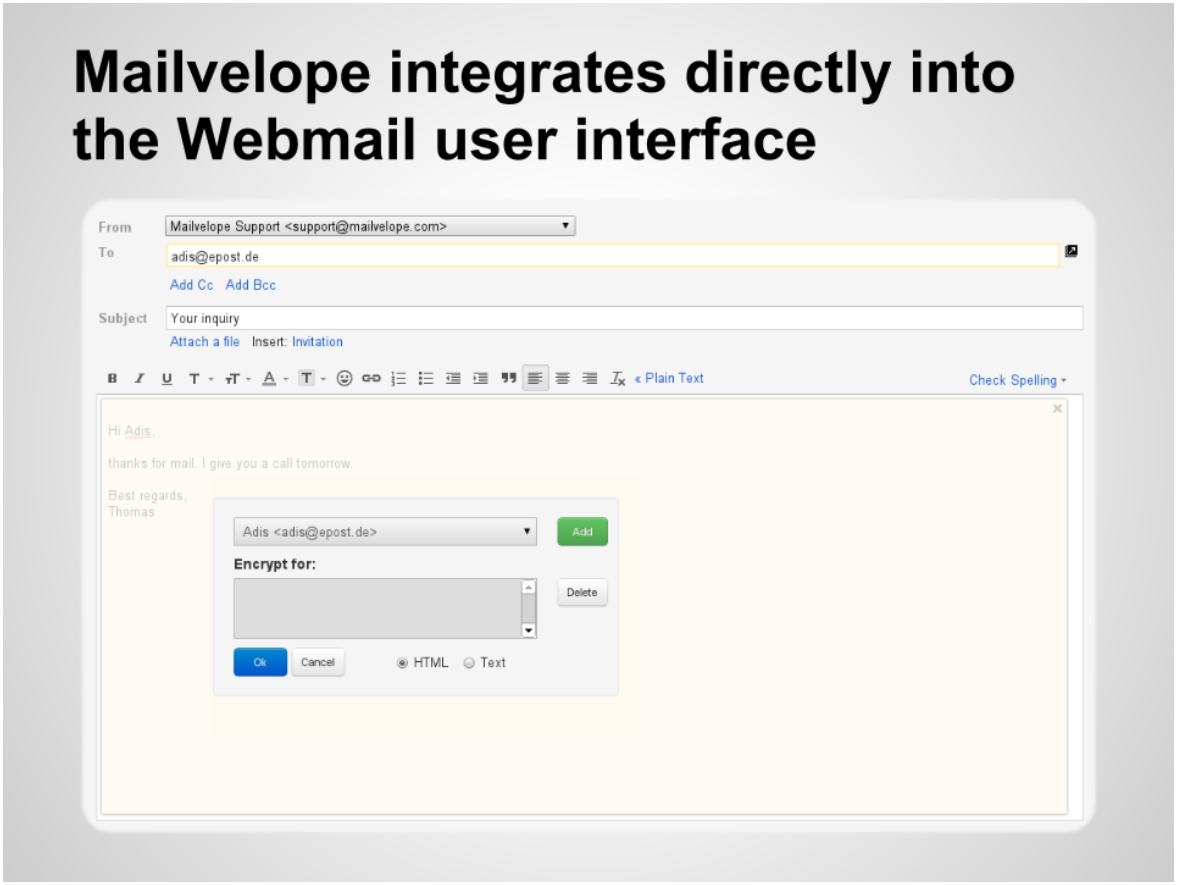




On a Windows machine,
e.g., with PGP4win

On a phone, e.g.,
with PGPeverywhere

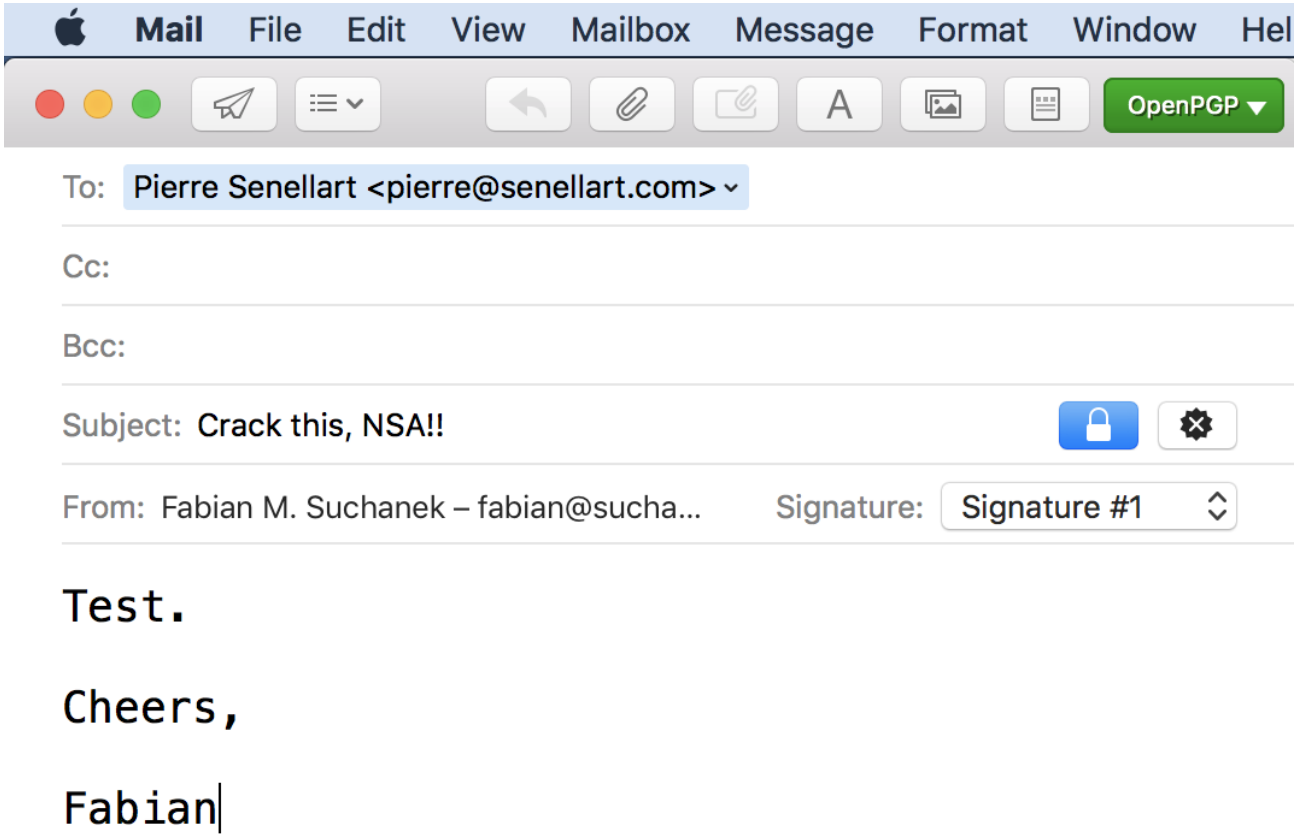
PGP encryption in practice



In a browser, e.g.

with Mailvelope

PGP encryption in practice



On a Mac, e.g., with GPGSuite

Happy encrypting :-)

Protecting data against

- yourself
- hackers
- evil interlocutors
- companies
- governments

Primitive Root

原始根

给定一个素数p，g是一个原始根模p，if ∀a ∈ {1, ..., p – 1} : ∃k : (gkmodp) = a.

Given a prime number p, g is a primitive root modulo p,

if $\forall a \in \{1, ..., p-1\} : \exists k : (g^k mod p) = a$.

(The definition extends to p that are not prime numbers.)

Example: $g = 3$ is a primitive root modulo $p = 7$, because

for any $a = 1...p-1$ I can choose k so that $(g^k mod p) = a$.

what I want to encode	what I send instead	How to get back to the original number
1	6	$3^6 = 729, (729 mod 7) = 1$
2	2	$3^2 = 9, (9 mod 7) = 2$
3	1	$3^1 = 3, (3 mod 7) = 3$
4	4	$3^4 = 81, (81 mod 7) = 4$
5	5	$3^5 = 243, (243 mod 7) = 5$
6	3	$3^3 = 27, (27 mod 7) = 6$