

# Data Protection and Security

Chris Wilson  
IT Security  
European Southern Observatory



A short presentation touching on some of the IT Security aspects of Data Protection, aiming to give some practical advice about how we as individuals can take an active role in securing our own data.

## Why Your Privacy is Important

“If you’re *not paying* for the product,  
then you *are* the product”



Why is privacy important?

You are probably already familiar with the phrase “if you’re not paying for the product, then you are the product”; it’s often used when talking about social media and other “big data” companies, but it’s been around for quite some time.

## Why Your Privacy is Important

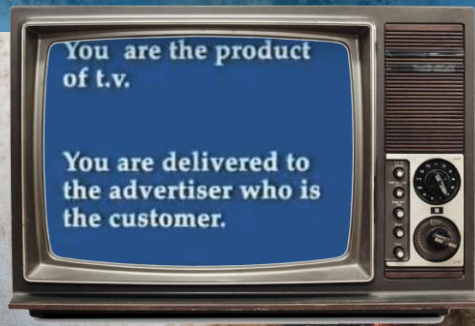
“If you’re *not paying* for the product,  
then you *are* the product”



The sentiment itself began as far back as the 70s, as a stark criticism of the overly commercialised/sponsored content offered by US television broadcasters; where many European governments had opted for license-based funding to maintain impartiality in the curation of content, commercially-driven content was generally embraced by the US as a way to reduce the cost of content creation, and the overall cost of TV ownership for private citizens.

## Why Your Privacy is Important

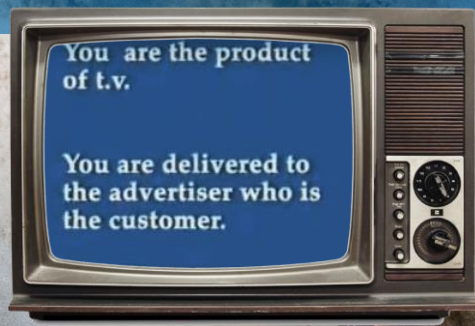
“If you’re *not* paying for the product,  
then you *are* the product”



By the mid-70s, commercials, “ads”, and other sponsored content had become prevalent that Artist Richard Serra created a video art piece called “Television Delivers People” (sample shown above) which used phrases like “the consumer becomes the consumed” and “you are the product of t.v” to raise attention to the issue.

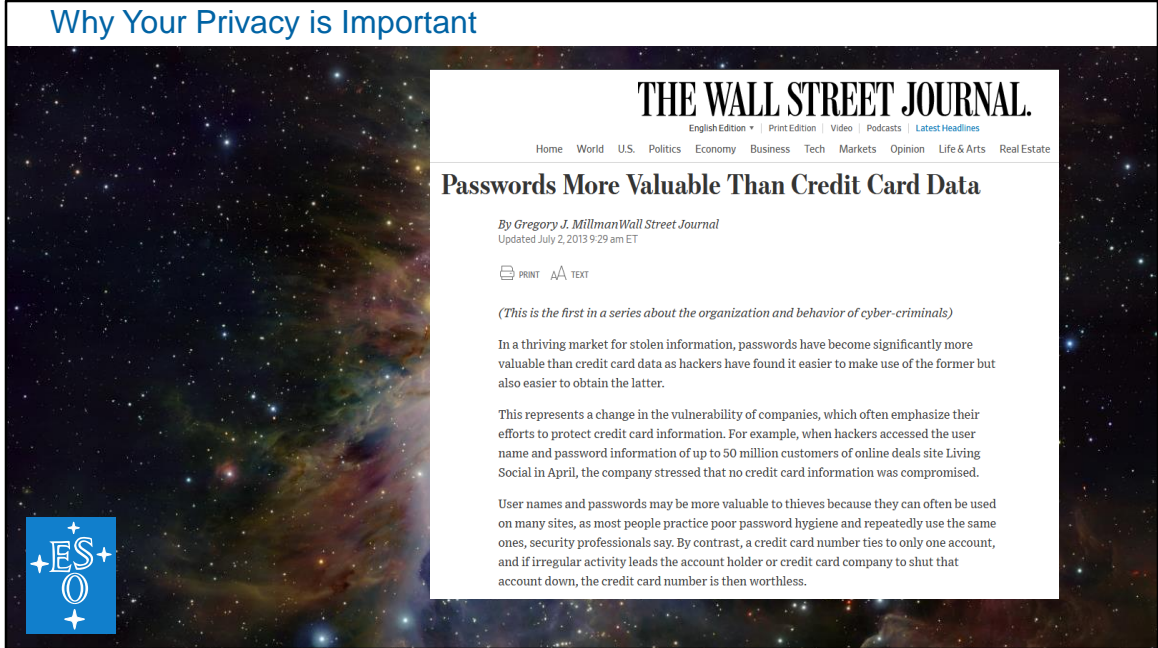
## Why Your Privacy is Important

“If you’re *not* paying for the product,  
then you *are* the product”



With the transition to internet-based commerce, this sentiment largely remains. The key difference now however, is that what was once intangible – the passive act of watching something and being influenced by it – the “product” we now provide has a more physical substance: data, which we inadvertently generate about what we do and how we act online. But this is just one example; the value and exploitability of information relating to, or about us, goes far beyond the use of free or ad-supported services targeted here.

## Why Your Privacy is Important



The screenshot shows a Wall Street Journal article from 2013. The article is titled "Passwords More Valuable Than Credit Card Data" and is written by Gregory J. Millman. It discusses how passwords have become more valuable than credit card data due to the ease of obtaining them and the fact that they can be used on multiple sites. The article is set against a background of a colorful nebula. In the bottom left corner of the screenshot, there is a blue square logo with the letters "ES" and "O" and some decorative elements.

**THE WALL STREET JOURNAL.**  
English Edition • Print Edition | Video | Podcasts | Latest Headlines  
Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate

### Passwords More Valuable Than Credit Card Data

By Gregory J. Millman/Wall Street Journal  
Updated July 2, 2013 9:29 am ET

PRINT TEXT

*(This is the first in a series about the organization and behavior of cyber-criminals.)*

In a thriving market for stolen information, passwords have become significantly more valuable than credit card data as hackers have found it easier to make use of the former but also easier to obtain the latter.

This represents a change in the vulnerability of companies, which often emphasize their efforts to protect credit card information. For example, when hackers accessed the user name and password information of up to 50 million customers of online deals site Living Social in April, the company stressed that no credit card information was compromised.

User names and passwords may be more valuable to thieves because they can often be used on many sites, as most people practice poor password hygiene and repeatedly use the same ones, security professionals say. By contrast, a credit card number ties to only one account, and if irregular activity leads the account holder or credit card company to shut that account down, the credit card number is then worthless.

For example: its fair to assume that credit card information is the most interesting type of data to a thief. And you'd be partially right; credit card fraud is still on the rise - in 2018 it amounted to \$28 billion worldwide (3 times more than in 2010). But the technologies and methods used to achieve that fraud are constantly changing.

This article from 2013 highlighted that despite it being easier (with modern cloning and skimming techniques) for criminals to steal card information, their net value on the black market was in steady decline due to a range of new security measures that were being implemented across the industry.

As a result, criminals realised it was less effort for them, to simply ask you for your Amazon password in a phishing E-mail, and sell it to someone who has the resources to coordinate a shopping spree at your expense, for instance.

Given that a large number of people use the same password for all online accounts, tricking someone to log in somewhere unimportant (like a hotel or news site) would have a higher chance of success, and still give them access to all your other accounts: one simple act, and they might get access to 10 or more different websites, each with different (or multiple) stored credit cards ready for them to use.

## Why Your Privacy is Important

**REUTERS**  
HEALTHCARE & PHARMA | SEPTEMBER 24, 2014 / 8:25 PM / UPDATED 6 YEARS AGO

### Your medical record is worth more to hackers than your credit card

By Caroline Humer, Jim Finkle | 6 MIN READ

NEW YORK/BOSTON (Reuters) - Your medical information is worth 10 times more than your credit card number on the black market.

**THE WALL STREET JOURNAL**  
English Edition | Print Edition | Video | Podcasts | Latest Headlines  
Home | World | U.S. | Politics | Economy | Business | Tech | Markets | Opinion | Life & Arts | Real Estate

### Passwords More Valuable Than Credit Card Data

By Gregory J. Millman/Wall Street Journal  
Updated July 2, 2013 9:29 am ET

PRINT | TEXT

*(This is the first in a series about the organization and behavior of cyber-criminals)*

In a thriving market for stolen information, passwords have become significantly more valuable than credit card data as hackers have found it easier to make use of the former but also easier to obtain the latter.

This represents a change in the vulnerability of companies, which often emphasize their efforts to protect credit card information. For example, when hackers accessed the user name and password information on the website of the company's Social in April, the company stressed the importance of the data.

User names and passwords may be more valuable than credit card numbers on many sites, as most people protect their credit card numbers more closely, security professionals say, and if irregular activity leads to the account being shut down, the credit card number is less useful.

There was an **80% INCREASE** in the number of people affected by **HEALTH DATA BREACHES** from 2017 to 2019.

Source: Varonis

A more unusual trend has been the rise in demand for health-related data: what value does an X-ray have to a hacker?

It turns out that, if it indicates you've got an illness that requires controlled, prescription medication or specialist equipment, it could allow someone to obtain a prescription to legally buy and then illegally resell those controlled items. If it shows you have excellent health, then it could allow someone to open up a new insurance policy against which to reclaim the costs for those fake prescriptions, in someone else's name.

Fueled by the heavily commercialised US medical system, the trend in medical-based identity theft has seemingly only been on the increase: the number of health-related data breaches rose by a reported 80% between 2017 and 2019 (according to publicly released breach disclosure reports).

## Why Your Privacy is Important

“So we should stop sharing our data with everyone right now...?”



So should we stop sharing our data with everyone, right now?

This is very much a personal choice which depends on the opportunities you personally stand to benefit from, as a result of sharing your information. There is arguably no right or wrong answer.



## Why Your Privacy is Important

“So we should stop sharing our data with everyone right now...?”



*Not really...* many opportunities and benefits of *secure data sharing* do outweigh the risks.

Personally, I don't think so: many opportunities and benefits of safe and secure data sharing do outweigh the associated risks. The big challenge, is *achieving safe and secure data sharing*.

In the big picture, these kinds of issue are the drivers behind the major changes to privacy law and regulation in recent years: to help establish a minimum baseline of protection for consumer rights and to make sure there's a financial incentive for companies to protect your data when its in your interests to provide it to them.

Principles like those shown all help to ensure the data that companies collect is constrained and limited to the scope for which it's needed, as overseen and endorsed by you; and that where companies don't protect the information entrusted to them, they are held accountable.

Now most of this is done behind the scenes on your behalf by a team of lawyers, data protection officers, IT security and technical specialists, so you might be thinking: what part do I play in all this?

# Why Your Privacy is Important

**Signal**  
'Data Linked To You'

- Contact Info
  - Email Address
  - Phone Number
- Search History
- Identifiers
  - Device ID

**iMessage**  
'Data Linked To You'

- Contact Info
  - Email Address
  - Phone Number
- Search History
- Identifiers
  - Device ID

**WhatsApp**  
'Data Linked To You'

**Analytics**

- Purchases
  - Purchase History
- Location
  - Course Location
- Contact Info
  - Course Location
- User Content
  - Other User Content
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data

**App Functionality**

- Purchases
  - Purchase History
- Financial Info
  - Payment Info
- Location
  - Course Location
- Contact Info
  - Email Address
  - Phone Number
- Contacts
  - Contacts
- User Content
  - Customer Support
  - Other User Content
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data

**Third-Party Advertising**

- Purchases
  - Purchase History
- Financial Info
  - Other Financial Info
- Location
  - Physical Location
  - Course Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Product or Video
  - Gameplay Content
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

**Health & Fitness**

- Purchases
  - Purchase History
- Financial Info
  - Payment Info
  - Other Financial Info
- Location
  - Physical Location
  - Course Location
- Contact Info
  - Physical Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Product or Video
  - Gameplay Content
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

**Product Personalisation**

- Purchases
  - Purchase History
- Financial Info
  - Payment Info
  - Other Financial Info
- Location
  - Physical Location
  - Course Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Product or Video
  - Gameplay Content
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

**App Functionality**

- Health & Fitness
  - Purchases
    - Purchase History
  - Financial Info
    - Payment Info
    - Other Financial Info
  - Location
    - Physical Location
    - Course Location
  - Contact Info
    - Physical Address
    - Name
    - Phone Number
    - Other User Contact Info
  - Contacts
    - Contacts
  - User Content
    - Product or Video
    - Gameplay Content
    - Customer Support
    - Other User Content
  - Search History
    - Search History
  - Browsing History
    - Browsing History
  - Identifiers
    - User ID
    - Device ID
  - Usage Data
    - Product Interaction
    - Advertising Data
    - Other Usage Data
  - Diagnostics
    - Crash Data
    - Performance Data
    - Other Diagnostic Data
  - Other Data
    - Other Data Types

**Other Purposes**

- Purchases
  - Purchase History
- Financial Info
  - Other Financial Info
- Location
  - Physical Location
  - Course Location
- Contact Info
  - Physical Address
  - Email Address
  - Name
  - Phone Number
  - Other User Contact Info
- Contacts
  - Contacts
- User Content
  - Product or Video
  - Gameplay Content
  - Customer Support
  - Other User Content
- Search History
  - Search History
- Browsing History
  - Browsing History
- Identifiers
  - User ID
  - Device ID
- Usage Data
  - Product Interaction
  - Advertising Data
  - Other Usage Data
- Diagnostics
  - Crash Data
  - Performance Data
  - Other Diagnostic Data
- Other Data
  - Other Data Types

**Forbes**  
Jan 3, 2021, 05:30am EST | 631,234 views  
**WhatsApp Beaten By Apple's New iMessage Privacy Update**  
Zak Doffman Contributor @Cybersecurity  
*I write about security and surveillance.*

**ESO**

As an example, this is an infographic produced recently by Forbes showing a simplified summary of the quantity and type of data some iOS messaging apps collect about their users. It was triggered by Apple's introduction of "privacy labels", which intend to show users what data individual apps collect, and how its used.

It is a great example of the principle of transparency: giving us as consumers, the information we need in order to make informed decisions about the types of service we want to use, and the data we'll be sharing in order to do it. But these types of initiatives only work if we as consumers take the time to understand and act upon the information given to us. In this case, just because Facebook Messenger collects more information about your use of its app, doesn't necessarily mean it is a risk for you as an individual – it depends upon your personal circumstances and preferences. The important thing is to be able to make an informed choice.

## Why Your Privacy is Important



So... what can I do to protect myself online?

Here are 5 quick ideas that might help.

## 1 Use E-mail Sub-addressing (RFC 5233)

my\_name@domain.com

my\_name+**subaddress**@domain.com



One of the easiest tricks is to use “e-mail sub addressing”. It’s a feature offered by some – but not all – E-mail providers that lets you create different sub-e-mail addresses for each of the services you use.

## 1 Use E-mail Sub-addressing (RFC 5233)

my\_name@domain.com

my\_name+**subaddress**@domain.com

Note: not always supported, and wildcard can differ by provider, i.e.:



Uses  
Plus (+)



Uses  
hyphen  
(-)

yahoo!mail

Sometimes described as “filtering”, “addressing”, “tagging” or “aliases”, overall support and implementation does vary, but most of the big vendors do allow ad-hoc usage.

Yahoo is a bit more complicated: you have to pre-configure the tag in your account first, then append it with a hyphen rather than a plus.

## 1 Use E-mail Sub-addressing (RFC 5233)

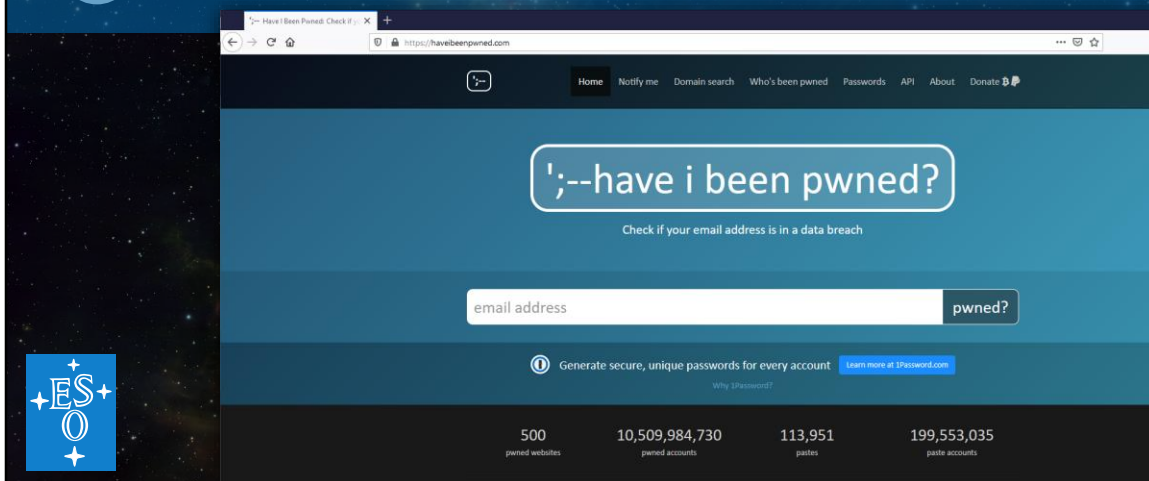
my\_name@domain.com  
my\_name+**subaddress**@domain.com

my\_email+**website**@gmail.com  
my\_email+**facebook**@outlook.com  
my\_email+**amazon**@mac.com  
my\_email-**netflix**@yahoo.com



Why is it useful? It lets you hand out a unique E-mail address to each service you subscribe to, in a way that ensures everything gets delivered to the same single inbox. This can help you organise your inbox with rules and filters (as originally intended), but it can also help you identify where emails come from: when you start receiving unsolicited messages from advertising agencies or spam robots, the alias/sub-address that they send the mail to, now shows you where they got your address. This can give a strong indication of which websites sell customer data to third parties (whether in accordance with their privacy policies or not), or which sites may have been hacked.

## 2 Notifications from haveibeenpwned.com



This can come in handy when you combine it with websites like haveibeenpwned.com

It sounds strange, but the word “pwned” is a reference to gamer culture: it originated as an over-eager misspelling of the word “own” and has now been embraced by opportunistic hackers (often called “script kiddies”) to embody the excitement and thrill of taking something from someone else: “I pwned you”.

The site itself is a free independent resource that lets you:

- 1 - check whether your e-mail address is linked to any passwords that have already been disclosed in known breaches;
- 2 – check whether a particular password has been seen in the wild before; and,
- 3 – receive automated notifications if your E-mail appears in any future data breaches.

If you use alias/sub-addresses for each online service, you can use it to pro-actively check whether specific websites have been compromised, giving you a heads’ up on what other data may have been accessed, or help you prioritise efforts to change passwords or enable more secure authentication.

### 3 Create Unique Passwords

“Passwords must be long,  
complex and unique...”



One of the safest ways to protect yourself, is to have a unique password for each website you use: separate passwords mean that if you get hacked once, you don't automatically get hacked everywhere.



### 3 Create Unique Passwords

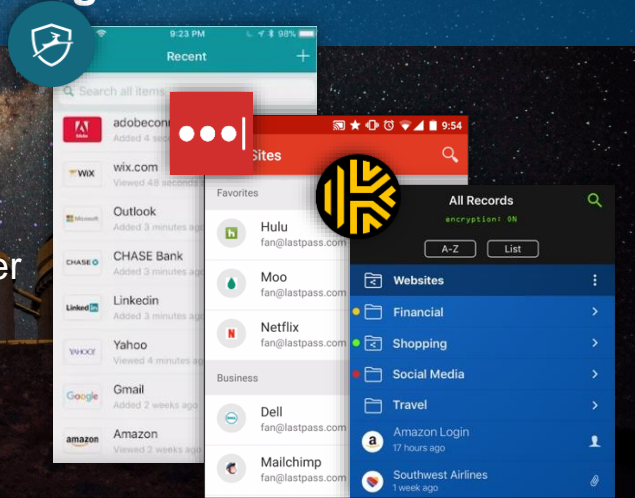


Now that's easy to say, but a completely different story trying to actually do it. We all have so many different accounts and services these days, creating a unique password for each one can sound like the impossible... there has to be a better way?

### 3a Use Password Manager

Cloud-synced examples:

- Dashlane
- LastPass
- Keeper Password Manager
- Many others



Password Managers.

This may seem counter intuitive – to put all my passwords in once place, which is protected by just one password – but the idea is that you only need to remember a single, strong and very unique password: the one used to access your password vault. And you only use that password in one place: your password vault.

Everything else is then managed by the manager: it will help you create the passwords, store them, and then insert them into the login process whenever its' needed through apps and browser plug-ins.

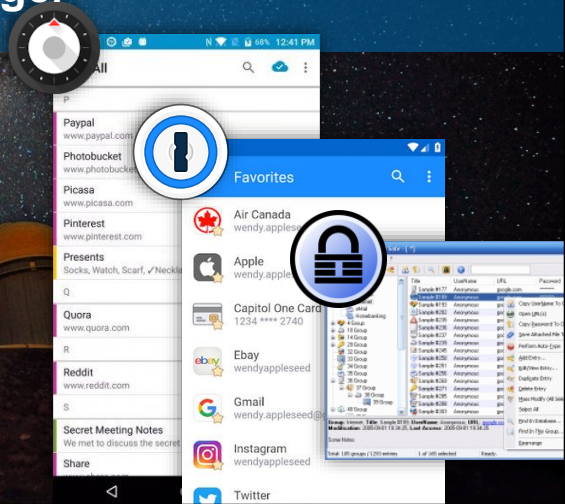
The only downside is that they're often not free, requiring a monthly subscription. But at around €40 per year, it is arguably a lot cheaper than the equivalent amount of your personal free time spent resetting passwords because you forgot them, or having to change them all because one website got hacked.

These are just some example cloud-based tools.

### 3a Use Password Manager

Non-cloud Examples:

- Blackberry Password Keeper
- 1Password
- KeyPass Password Manager
- Many others



If going to the cloud isn't an option, then there are some that support device-only, or local network-only protection; storing passwords in a password-encrypted file you can manage yourself.

The important thing to be aware of however, is that you need to control who has access to that file: if someone gets a copy of it, they have all the time in the world to try to guess the password and access its contents (the only thing protecting it is the password used to encrypt the data). It's therefore essential that you use a very strong, complex password – the more complex it is, the longer it will take to guess.

## 4 Enable Two-Factor Authentication

Protect your account with two of the following:

\*\*\* 🔒

Something you **know**  
(Password, PIN)



Something you **are**  
(Biometrics)



Something you **have**  
(Smartcard / Hardware)



For supported sites, visit [twofactorauth.org](https://twofactorauth.org)

The best way to reduce the risk of your passwords being disclosed is to enable two-factor authentication wherever you can. The idea is to require two pieces of information in order to log you in, rather than just one; requiring at least twice the effort for a criminal to gain access.

There are 3 possible factors:

- something you know – a shared secret like a Password or PIN;
- something you are – a unique attribute of your physical being, like a fingerprint, voice sample or IRIS scan;
- and something you have – an object or device known to be physically in your sole possession.

The most common approach is *something you know* and *something you have...* like a password and a verification code sent to a mobile phone via email or SMS; you may already be using it for your bank or credit card when you buy things online.

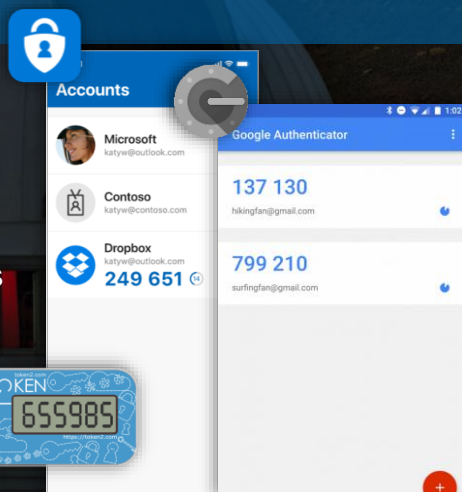
To see which of the services and websites support two factor authentication check out [twofactorauth.org](https://twofactorauth.org); they keep an active list of compatibility, with direct links to the relevant pages on each site showing you how to enable it for your account.

## 4 Enable Two-Factor Authentication

### Authenticator Apps:

- Microsoft Authenticator
- Google Authenticator
- Dedicated service application

Support for Temporary One Time Passwords (TOTP) and/or “Push” notifications.



While SMS and email are common forms of multi-factor authentication, they aren't necessarily the best: as standard features of most phones, any other software installed on your phone could theoretically get access to notifications generated by them (which could include verification codes). In fact, many phones are designed to share this information with other apps in order to make the user experience more engaging. As a result, malicious apps can exploit these features to forward verification codes to another device, allowing a criminal to authorise fraudulent activity without a user even knowing; thereby undermining the process.

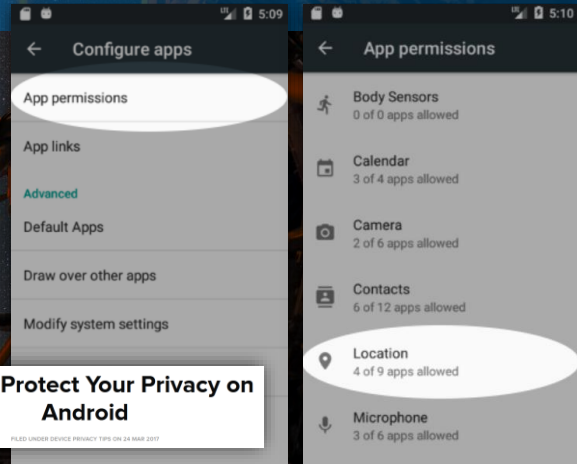
One way to avoid this is to use a dedicated Authenticator App designed with security in mind which supports software tokens such as Temporary One Time Passwords (TOTP). Microsoft and Google both provide generic Apps that can support multiple soft tokens at the same time. Many password managers also include this functionality within their standard apps, and there are a range of programmable hardware tokens, that can also be programmed via an app on your phone (or software on your computer) with some supporting up to 30 different accounts in the same physical token.

Other sites or services may provide their own dedicated apps that use “push notifications” instead. This is when a message is sent securely between the service and the App on your phone, requiring you to perform a task based on information shown across both screens. The main benefit of these is that they use encrypted communication between verified endpoints, preventing someone from listening in, and like the more general authenticators, are designed to deliberately prevent access to their data by any other app on a device.

## 5 Check App Permissions

Android:

- Permissions to be aware of:
  - Body Sensors
  - Calendar
  - Camera
  - Contacts
  - Location
  - Microphone
  - Phone (\$)
  - SMS (\$)
  - Storage



That being said, you should be aware of permissions when installing and updating Apps on your phone to avoid “information leakage”. Both Android and iOS have built-in features that allow you to review and control what permissions different apps have on your mobile devices.

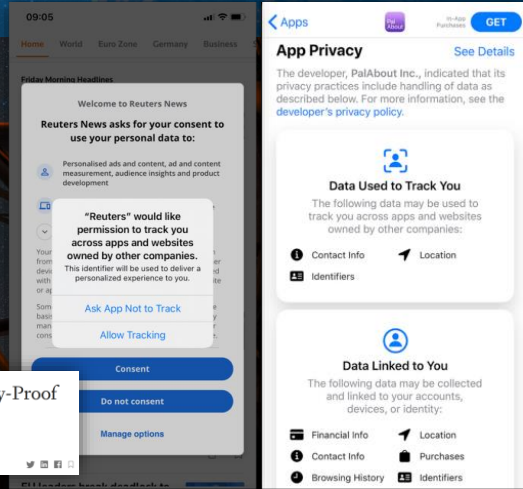
It is not always easy though: with permissions grouped into coarse headings like “Location” and “Storage”, it can be difficult to understand why certain features are needed by certain apps and in which circumstances. A simple example here is the requirement for “Location” access when an App tries to use Bluetooth (why do my wireless headphones need GPS?) In this case, it’s the prevalence of fixed devices that broadcast Bluetooth signals that are to blame: Smart lightbulbs and power sockets, even some WiFi routers broadcast Bluetooth device IDs these days, meaning Bluetooth can be used to determine your physical location.

This is arguably one of the main issues with course definitions like this; when an App only needs a permission for a one-off singular activity (i.e. to pair some headphones, or other Bluetooth device), we are unlikely to go back and disable it afterwards. But, it can be worth going back and having a look what your apps are doing. If you search online, there are plenty of guides on how to control how much data you share with the apps on your device and prevent over-sharing.

## 5 Check App Permissions

iOS

- Permissions; and, since December,
- Privacy Labels
  - Contact Info
  - Health & Fitness
  - Financial Info
  - Location
  - Sensitive Info
  - User Content
  - Browsing History
  - Search History
- Identifiers
- Purchases
- Usage Data
- Diagnostics
- Other Data



With the release of Privacy Labels, iOS gives a little more information here, forcing developers to disclose the types of data that are Used to Track You, Linked To You, and Not Linked To You. In practice there are 32 types of data grouped into 13 categories... giving iOS users a much more granular view on what information an app collects and uses. Accompanying Privacy Policies in the App Store should explain the reasoning behind this data use in a way that is easier for users to digest and understand, allowing you to take more control over what permissions are needed and when. It's worth taking the time to look over and turn off features that don't make sense for the type of App that has requested them... again online guides can help you here.

## Your Privacy is Important

We all have a part to play in the protection of information; especially our own.

### Top tips:

- 1 Use E-mail Sub Addressing
- 2 Check out [www.haveibeenpwned.com](http://www.haveibeenpwned.com)
- 3 Create Unique Passwords & Use a Password Manager
- 4 Enable Two-Factor Authentication
- 5 Check App Permissions



There's a lot more we can talk about: cookies preferences on websites; installing an adblocker in your browsers. But we're out of time for today.

Hopefully some of this has been useful, but the most important message, is that we all have a part to play when it comes to the protection of information – it's a shared responsibility, but when it comes to our personal data, the ultimate risk owner is us.

Stay alert, and stay safe.





[www.eso.org](http://www.eso.org)