ANDROID SECURITY AND PERSONAL PRIVACY

OCTOBER 21, 2015

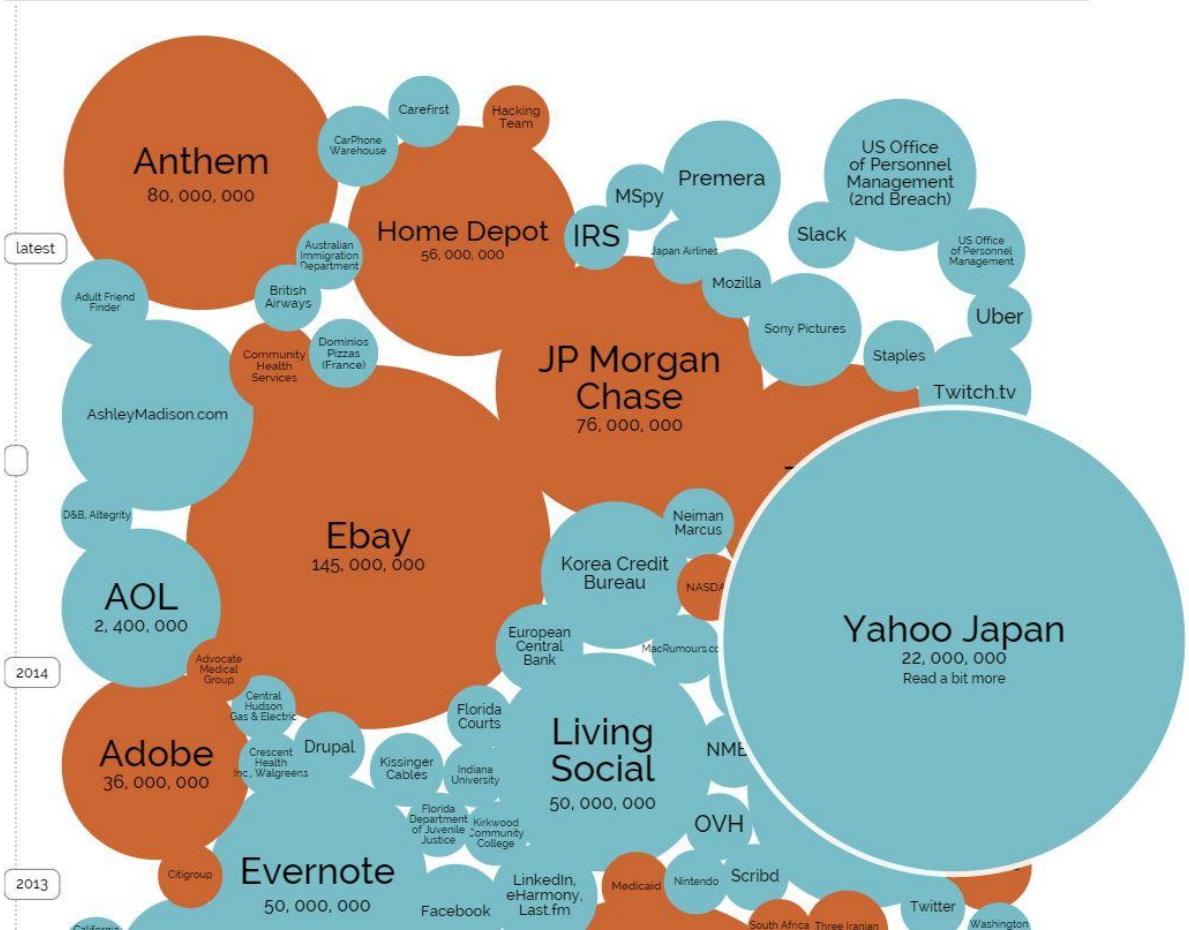
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 11th August 2015)

interesting story

YEAR | BUBBLE COLOUR: YEAR | METHOD OF LEAK | BUBBLE SIZE: NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



Tip 1: Use a Secure Lock Screen

This first tip is absolutely the most important Android security feature of them all. If your phone or tablet were to ever become lost or stolen, a secure lock screen would be the only barrier between a potential thief and all the passwords and sensitive data stored on your phone.

To set up a secure lock screen, head to your phone or tablet's main Settings menu, then go to Security and tap the "Screen lock" option. From here, choose either Pattern, PIN, Password, or on capable devices, the Fingerprint option.

Times Needed to Crack Passwords			
Number of Characters in Password	Total Number of Characters from Which Password is Selected		
	26 (lower case letters only - abc)	36 (lower case letters plus numbers - abc123)	52 (upper and lower case letters - AaBbCc)
5	1.98 minutes	10.1 minutes	1.06 hours
6	51.5 minutes	3.74 hours	13.7 days
7	22.3 hours	9.07 days	3.91 months
8	24.2 days	10.7 months	17.0 years
9	1.72 years	32.2 years	8.82 centuries
10	44.8 years	1.16 millennia	45.8 millennia
11	11.6 centuries	41.7 millennia	2,384 millennia
12	30.3 millennia	1,503 millennia	123,946 millennia

Attachment decoded: times_to_crack_passwords.jpg
=yend size=33645 crc32=fca8e983

Tip 2: Turn on Smart Lock Features

Google is aware that users tend to avoid setting up the secure lock screen because it complicates things a tiny bit, but knowing how important it is, they've added a new feature to Android 5.0 that will let you bypass the secure lock screen altogether in some cases.

The feature is called "Smart Lock," and the premise is simple—when your device is in a secure environment, you shouldn't have to be bothered by the secure lock screen.
Tap to Play Video

To set this feature up, head to the Security menu again, but this time choose the "Smart Lock" option (note that the secure lock screen must be enabled first). From here, you should see several options, and here's what they each do:

- Trusted devices: Bypass secure lock screen when connected to a known Bluetooth or NFC device.
- Trusted places: Bypass secure lock screen when device is in a preset location (home, work, etc.).
- Trusted face: Bypass secure lock screen when the front-facing camera on your device detects your face.
- Trusted voice: Bypass secure lock screen for "OK Google" voice search when user's voice is recognized.
- On-body detection: Bypass secure lock screen after passcode has been entered, where device has not been set down since.

Tip 3: Enable 2-Step Verification

Considering that Google and Android are almost synonymous these days, if someone were to ever gain access to your Google account, your device's security would be compromised. To combat this, you can add an extra layer of security to your Google account called 2-Step Verification that will require a second code to be entered after your password. The trick here is that this code will only be sent to your cell phone, meaning no one can get into your Google account without having physical access to your device.

To set up 2-Step Verification on your Google account, head to this link, then follow the simple prompts. As a head's up, this is probably better to do from a desktop or laptop.

Get codes via text message

Google can send verification codes to your cell phone via text message. Your carrier's standard messaging rates may apply.

Want a phone call instead?

Google can call your cell or landline phone with your verification code.

No connection, no problem

The Google Authenticator app for Android, iPhone, or BlackBerry can generate verification codes. It even works when your device has no phone or data connectivity.

Keep your account even more secure

Instead of using verification codes, you can insert a Security Key into your computer's USB port for even more protection against phishing.

Backup phone numbers

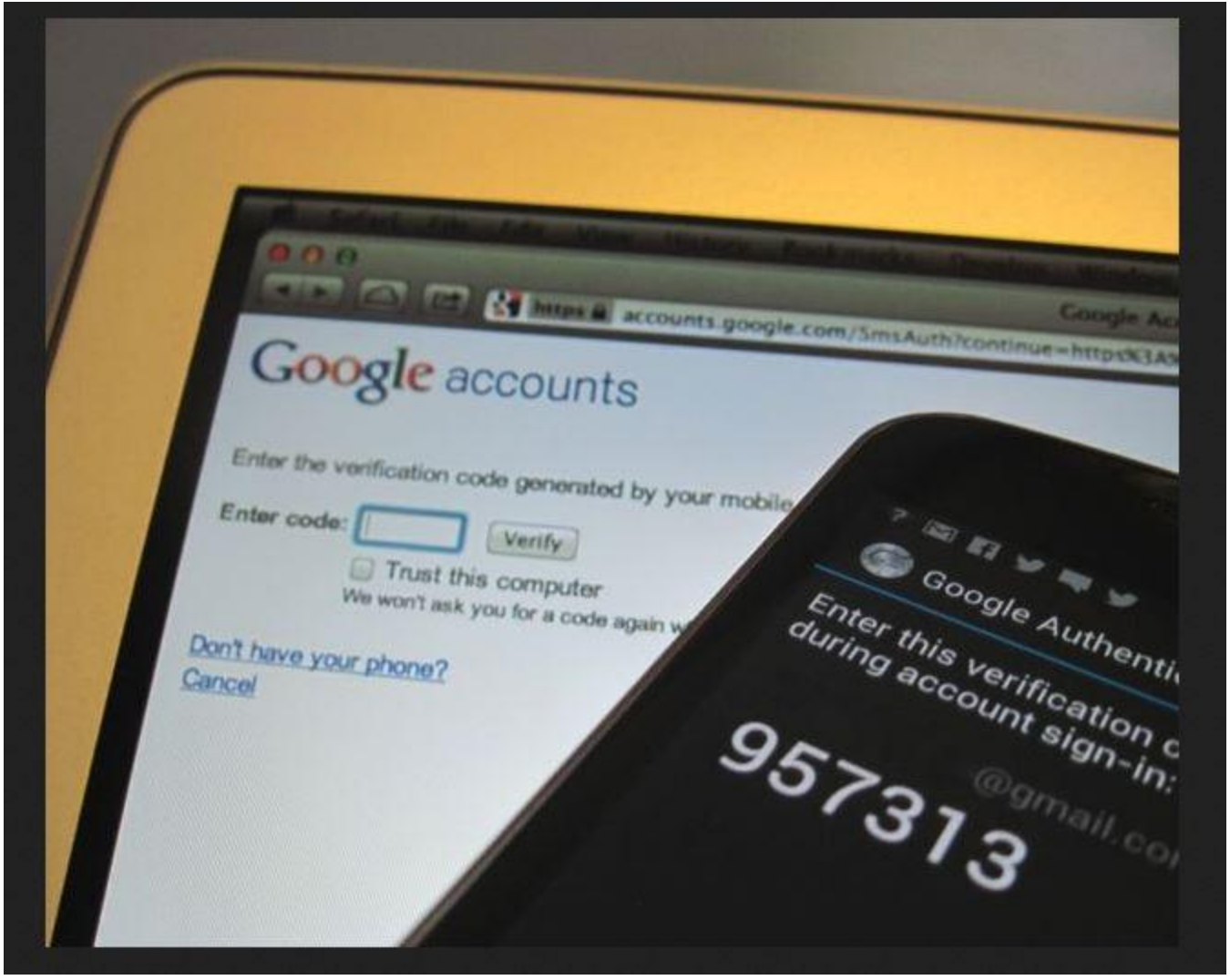
Add backup phone numbers so Google has another way to send you verification codes in case your main phone is unavailable.

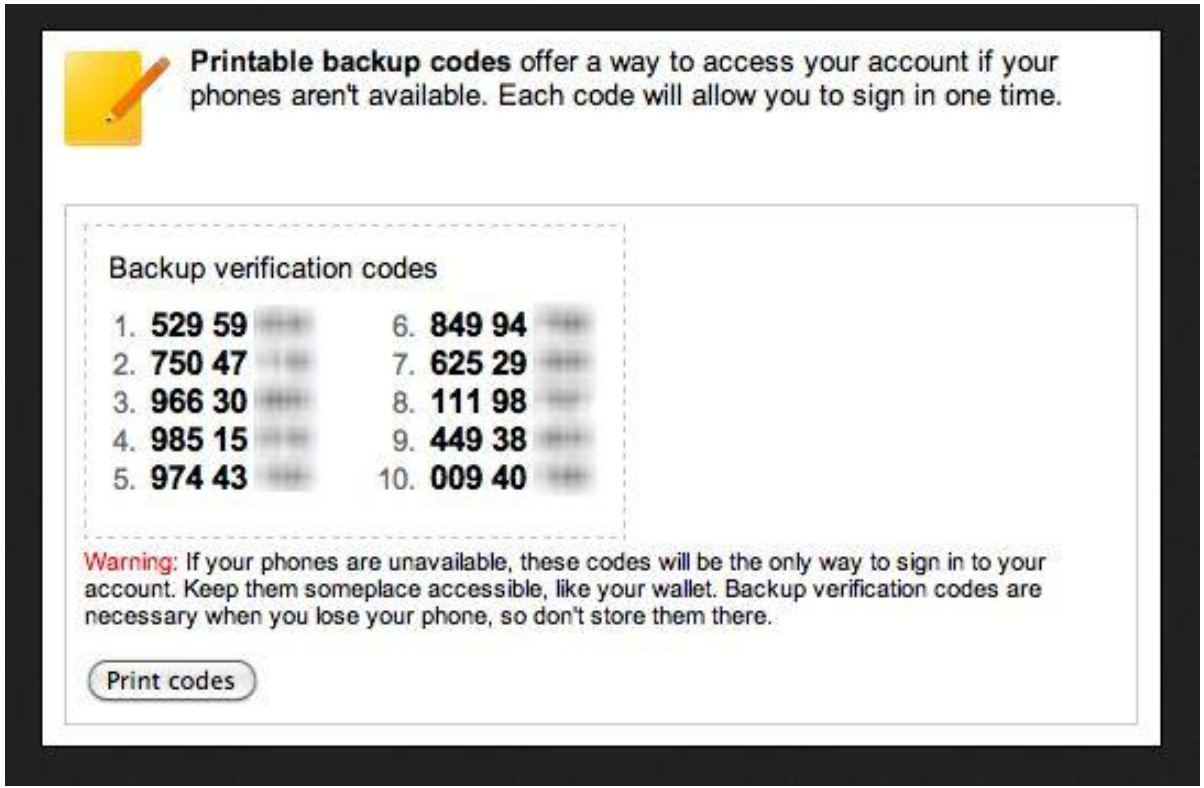
Backup codes

You can print or download one-time use backup codes for times when your phones are unavailable, such as when you travel.

Register your computers

During sign-in, you can choose not to use 2-Step Verification again on your computer. We'll still ask for codes or Security Key on other computers.


https accounts.google.com/SmsAuth?continue=https%3A%
Google accounts
Enter the verification code generated by your mobile
Enter code:
Verify
Trust this computer
We won't ask you for a code again w
Don't have your phone?
Cancel
Google Authenti
Enter this verification c
during account sign-in:
@gmail.co
957313


Printable backup codes offer a way to access your account if your phones aren't available. Each code will allow you to sign in one time.
Backup verification codes
1. 529 59
2. 750 47
3. 966 30
4. 985 15
5. 974 43
6. 849 94
7. 625 29
8. 111 98
9. 449 38
10. 009 40
Warning: If your phones are unavailable, these codes will be the only way to sign in to your account. Keep them someplace accessible, like your wallet. Backup verification codes are necessary when you lose your phone, so don't store them there.
Print codes

Tip 4: Set Up Android Device Manager

All modern Android phones and tablets have an awesome utility called Android Device Manager baked right in. This allows you to remotely lock, wipe, and locate your device should it ever fall into the wrong hands.

This feature should be enabled by default, but to be on the safe side, head to the Security menu again, then select the "Device administrators" option. From here, be sure to tick the box next to the Android Device Manager entry, then press "Activate" on the subsequent popup.

Tip 5: Make Sure "Verify Apps" Is Enabled

Android is now capable of scanning your device for malware automatically, and it does a wonderful job. This option is enabled by default in Android 5.0 and above, but for the folks on KitKat or lower, it's a great security service that should be manually enabled if it isn't already.

To begin, head to the Security menu in settings, then scroll down to the Device Administration section. From here, make sure that the "Verify app" option is ticked, and you'll be all set.

DEVICE ADMINISTRATION

Device administrators

View or turn off device administrators.

Verify apps

Block or warn before installing apps that may cause harm.

Notification access

Applications cannot read notifications.

Tip 6: Only Install Apps from Trusted Sources

Although Android is capable of scanning your apps to detect malware, you should never rely too heavily on an automated solution such as this. Instead, use the prophylactic approach of researching an app and its publisher before you install it.

At the very least, you should only install apps from trusted sources. Publishers like the Google Play Store and the Amazon Appstore can be trusted, but be weary when downloading APKs from random websites.

Tip 7: Uninstall Permission-Hungry Apps

Android uses what is known as a permission system to dole out access to certain parts of your device when apps request it. Unfortunately, until Android M is officially released, these permissions are handled in an all-or-nothing approach, and your only chance to deny an app access to the permissions it requests is by not installing it in the first place.

Some apps request way too many permissions, and this is a security risk in the sense that if an app has access to certain parts of your device, so does its developer. To see which apps on your phone are getting out of control with their permission requests, I'd suggest installing an app called Permission Friendly Apps. It scans your installed apps and rates them by how many permissions they've requested, where the higher the score, the bigger the security risk.

Tip 8: Use an Antivirus App

While Android scans for malware automatically and silently, an antivirus app can give you more peace of mind by actually showing you the results of its scans. There are many great antivirus options available. The majority of Android security apps are actually packages that include a host of other tools from housekeeping to remote lock or wipe. Here is a few of the more popular and top rated security apps that can also help find your lost Android device:

LOOKOUT MOBILE SECURITY

AVAST MOBILE SECURITY & ANTIVIRUS

AVIRA FREE ANDROID SECURITY

360 MOBILE SECURITY

BITDEFENDER MOBILE SECURITY & ANTIVIRUS

AVG ANTIVIRUS SECURITY

Tip 9: Encrypt Your Data

The word "encryption" might evoke feelings of technophobia in some, but it's an incredibly simple concept. Think of it like all of the data on your device being jumbled up to the point where it's meaningless to an outsider, but once a password has been entered, it all sorts itself out and falls back into place automatically.

With an Android device, encrypting your data is incredibly easy. Just head to the Security menu again, then choose the "Encrypt phone (or tablet)" option. From here, make sure your device is fully charged and connected to a charger, then press the "Encrypt Phone" button.Depending on how much data you have stored on your device, the process can take as long as an hour or more, so keep your phone plugged in and stay patient. When it's done, the data on your phone will be completely useless to an outsider, but all you have to do to decrypt it and render it useful again is enter the pattern, PIN, or password on your secure lock screen.

Tip 10: Don't Connect to Unknown Wi-Fi Networks

One of the biggest potential security risks to your phone or tablet is the network it's connected to. Traffic through this connection is generally trusted by default, so if you're not familiar with a Wi-Fi network, the best thing to do would be not connecting in the first place.

Public access points generally have some form of security that prevent the various devices connected to them from communicating with one another. But if you're not sure about a certain network's security measures, it would be best not to connect.

Tip 11: Use a Third-Party Web Browser

The internet browser on your device has the potential to be your biggest security hole. If you're using the stock browser that came preinstalled on your phone or tablet, the problem with these is that they don't generally receive updates until your entire device gets a firmware update.

Instead, consider downloading a third-party browser from the Play Store, which should receive prompt updates to block new security exploits that are discovered. One of the most secure and functional browsers available is Google's own Chrome, which is always updated with the latest security patches.

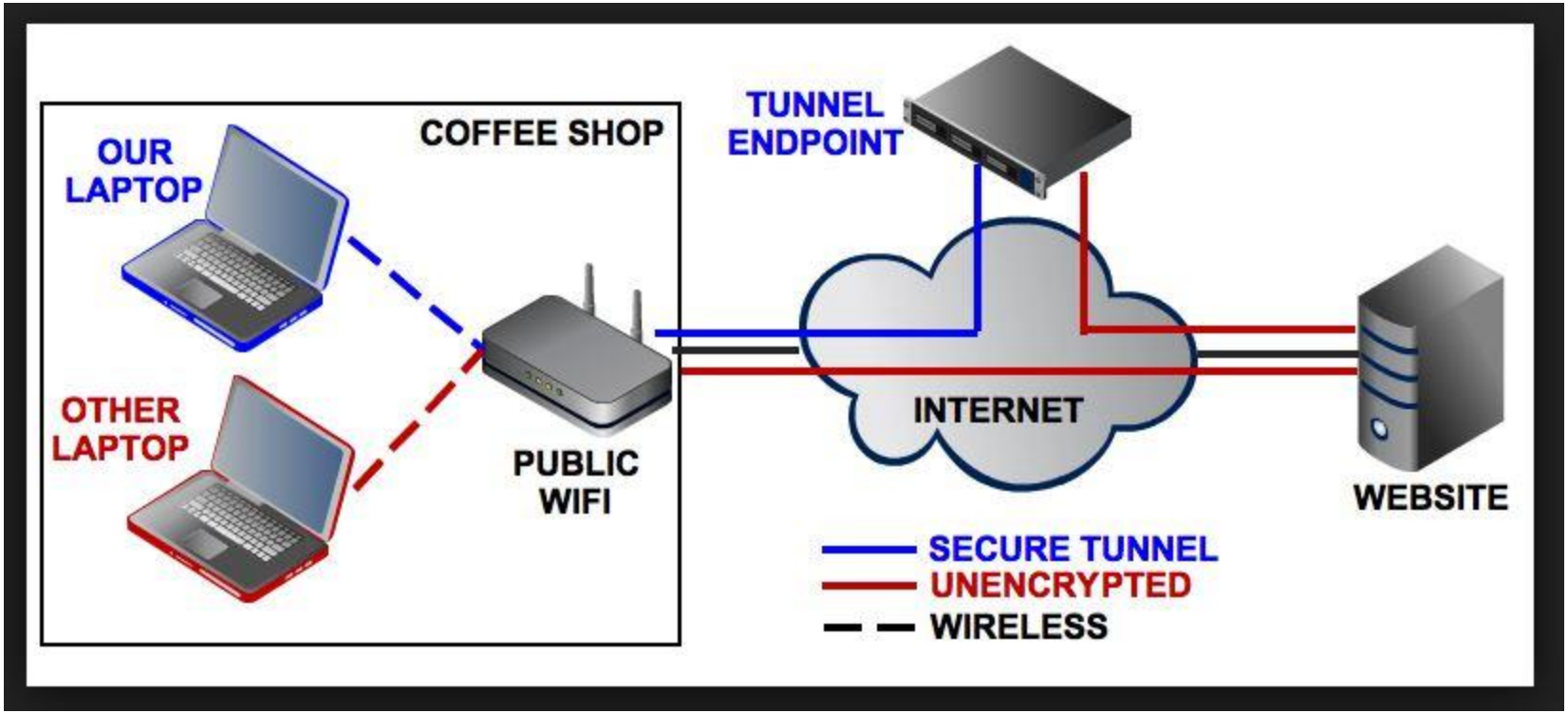
Tip 12: Keep Your Device Up to Date

Continuing on the topic of prompt updates being good for security, your phone or tablet will occasionally receive an over-the-air firmware update from the device manufacturer. Some users are reluctant to update their firmware for fear of change, but this is an important security measure as exploits and loopholes in the Android system are often patched in a firmware update. To see if your device has an update waiting on you right now, head to the "About phone" or "About tablet" menu in Settings. From here, tap "System updates" and install any available updates. Generally, though, you will receive a notification when a firmware update is ready.

Tip 13: Use a VPN Service to Encrypt Data Traffic

Every time you make a connection to any website, you're leaving a trail of breadcrumbs that can be traced right back to your smartphone. The site you connected to knows your IP address, your internet provider has records of the connection, and government agencies can gain access to this information with a simple subpoena.

The best way to shore up this vulnerability would be to use a Virtual Private Network (VPN) service that encrypts all data traffic, in which case the website never knows your IP, and your service provider only sees meaningless encrypted data.


COFFEE SHOP
OUR LAPTOP
OTHER LAPTOP
PUBLIC WIFI
TUNNEL ENDPOINT
INTERNET
WEBSITE
SECURE TUNNEL
UNENCRYPTED
WIRELESS

1. **Enhanced security**. When you connect to the network through a VPN, the data is kept secured and encrypted. In this way the information is away from hackers' eyes.
2. **Remote control**. In case of a company, the great advantage of having a VPN is that the information can be accessed remotely even from home or from any other place. That's why a VPN can increase productivity within a company.
3. **Share files**. A VPN service can be used if you have a group that needs to share files for a long period of time.
4. **Online anonymity**. Through a VPN you can browse the web in complete anonymity. Compared to hide IP software or web proxies, the advantage of a VPN service is that it allows you to access both web applications and websites in complete anonymity.
5. **Unblock websites & bypass filters**. VPNs are great for accessing blocked websites or for bypassing Internet filters. This is why there is an increased number of VPN services used in countries where Internet censorship is applied.
6. **Change IP address**. If you need an IP address from another country, then a VPN can provide you this.
7. **Better performance**. Bandwidth and efficiency of the network can be generally increased once a VPN solution is implemented.
8. **Reduce costs**. Once a VPN network is created, the maintenance cost is very low. More than that, if you opt for a service provider, the network setup and surveillance is no more a concern.

TECH WARS

In lawsuit over hacking, Uber probes IP address assigned to Lyft executive

1	ExpressVPN	30 Day Money Back Guarantee Unlimited Bandwidth, High Speed Servers Easy-to-use Apps for All Devices Read Review	78	5 Rate It! (7980)	Connect Now
2	IPVANISH VPN	Unlimited Bandwidth Fast VPN 7 Days Money Back Guarantee 100% Anonymous 0 logs Read Review	61	4.7 Rate It! (981)	Connect Now
3	IRONSOCKET	All-in-one package Major service overhaul in 2013 No logging of browsing activity Read Review	36	4.5 Rate It! (2475)	Connect Now
4	HIDE MY ASS!	Servers in 161 Countries 24/7 Customer Service IP switching can be scheduled by the user Read Review	161	4.3 Rate It! (4688)	Connect Now
5	purevpn	Dedicated IP for extra $2 /m. Servers in 87 Countries 5 simultaneous logins Read Review	87	4.2 Rate It! (3207)	Connect Now
6	vyprvpn by golden frog	700+ Servers, 200,000 IPs 24/7 Customer Support In-house built and managed servers Read Review	37	4.1 Rate It! (5327)	Connect Now
7	overplay	Offers Smart DNS Service Focused on online TV streaming Read Review	48	4 Rate It! (512)	Connect Now
8	STRONG VPN	99.9% Uptime Up to 2048 Bit encryption Automatic setup application Read Review	22	3.5 Rate It! (2120)	Connect Now

Tip 14: Block Access to Your Camera

If you've ever been concerned that someone may be spying on you, or that an app you've installed may be using its access to your camera module in a malicious way, you'll be happy to know that you can selectively disable all access to your camera. An app called CameraBlock can actually block access to your camera altogether at the press of a button. Once you've installed the app, head to your phone or tablet's main Settings menu, then search for and select the "Device administrators" menu. From here, enable the "Camera Block Free" option, then press "Activate" on the subsequent popup. At this point, just open Camera Block and press the shield icon to block access to your camera.

Tip 15: Use TextSecure for Encrypted Messaging

Hands down, the best way to prevent other parties from reading your text messages on Android is an app called TextSecure, which encrypts the messages and renders them useless to anyone who doesn't have your unique decryption key. Both parties will have to have TextSecure installed to take advantage of its encryption capabilities. Once you and your friend have installed the app and set it up, sending messages is just as easy as any other messaging app. For a walkthrough on getting started with secure text messaging, check out our full setup guide for TextSecure.

Tip 16: Use RedPhone for Encrypted Calls

The makers of TextSecure have another great app called **RedPhone**, which allows you to make encrypted phone calls without having to worry about someone listening in.

Once you've got the app installed, simply register your existing phone number so that all calls you make will use that number on the outbound caller ID. For fully encrypted phone calls, both parties will have to have RedPhone installed on their devices, but if you dial a number that isn't registered, the app will offer to send an install link to the other party.

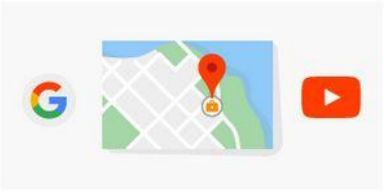
Completely Paranoid Tip: Get Rid of Google

Lastly, you might want to address the issue of Google being deeply integrated into Android. As you surely know, Google is an advertising company first and foremost, which means they like to collect usage data for targeted ads. If this makes you uncomfortable, be sure to check out our guide on removing Google from your Android experience, which should go a long way towards keeping your data private.

WWW.history.google.com

What data does Google collect?

Here are the main types of information we collect.



Things you do

When you use our services — for example, do a search on Google, get directions on Google Maps, or watch a video on YouTube — we collect basic information to make these services work. This can include:

- Things you search for
- Websites you visit
- Videos you watch
- Ads you click on or tap
- Your location
- Device information
- IP address and cookie data

Things that make you "you"

When you sign up for a Google Account, we keep the basic information you give us. This can include your:

- Name
- Email address and password
- Birthday
- Gender
- Phone number
- Country

If you have given us your billing information in order to make a purchase, we securely store it on our servers, just like we do with your basic information.

Things you create

If you are signed in with your Google Account, we store and protect what you create using our services, so you will always have your information when you need it. This can include:

- Emails you send and receive on Gmail
- Contacts you add
- Calendar events
- Photos and videos you upload
- Docs, Sheets, and Slides on Drive

RESOURCES:

http://drippler.com/drip/7-android-apps-helps-you-prevent-identity-theft-online

http://drippler.com/drip/android-security-13-must-know-tips-keeping-your-phone-secure

http://drippler.com/drip/how-improve-your-privacy-android-few-simple-steps

http://drippler.com/drip/how-maintain-your-privacy-android

http://www.greenbot.com/article/2919693/googles-essential-tips-for-keeping-your-android-devices-safe.html

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/