

2 Factor Authentication

By Ron Brown



**Virtual Technology
Conference
Saturday, 02/10/18
@ 1 PM ET**

**Conference Description
& Registration Links go to**

apcug2.org/category/virtual-tech-conference

WHAT WILL THE ATTACKER DO TO YOUR ACCOUNT?



- Once they access your account they will turn off notifications and change your Password
- Ransack your InBox for stuff like Bitcoin Wallet
- Copy compromising pictures
- Copy Contact List
- Install a filter to mask their actions
- Look for Financial information, Passwords, Personal information
- Delete all your email, contact list, and Gdrive

Bitcoin's Prices Slide 9% To \$9,000 On Arun Jaitley's Warning Against Cryptocurrencies



Three major banks confirm that they won't allow cryptocurrency transactions with their credit cards

Bank of America, JP Morgan Chase and Citigroup won't let you buy Bitcoin on credit
By Andrew Liptak on February 4, 2018 5:40 pm



What the Coincheck hack means for the future of blockchain security

MIT Technology Review
Feb 1, 2018

The plunder of [more than \\$500 million worth of digital coins](#) from the Japanese cryptocurrency exchange Coincheck last week has added to a growing perception that cryptocurrencies are particularly vulnerable to hackers.



Security

Good news, everyone: Ransomware declining. Bad news: Miscreants are turning to crypto-mining on infected PCs

Screw asking for digi-coins. Craft 'em on 500,000 computers

By [Iain Thomson](#) in [San Francisco](#) 1 Feb 2018 at 00:13

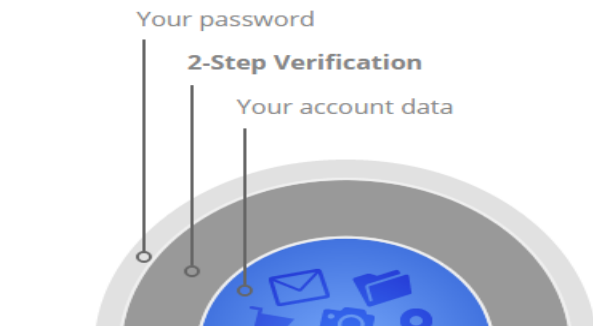
21



SHARE ▼




For the past few years, ransomware has been a bane of computer users. These software nasties infect PCs, scramble files, and demand payment in cryptocurrency to restore the documents.



An extra layer of security

Most people only have one layer – their password – to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone or Security Key to get into your account.



Sign in will require something you know and something you have

With 2-Step Verification, you'll protect your account with something you know (your password) and something you have (your phone or Security Key).



Two-factor authentication (or 2FA) is one of the biggest-bang-for-your-buck ways to improve the security of your online accounts

Extra Security to your online accounts on top of your Password

Your site will request something you know to log in (Password) and something you have your phone or usb security key



1. 2FA is unique to every account
2. Setup process is different
3. Often confusing terminology
4. Recommend start with one account- Google

One million account logins and passwords are stolen every month, says Google



Google has delved into the darker parts of the internet as part of a year-long research project analysing how cybercriminals manage to hijack user accounts by obtaining passwords and login codes.

In collaboration with the University of California, Berkeley, Google's research examined three common ways hackers manage to hijack accounts between March 2016 and March 2017

Phishing and keylogging – were used by cybercriminals to steal up to a staggering 250,000 account logins every week, Google found.

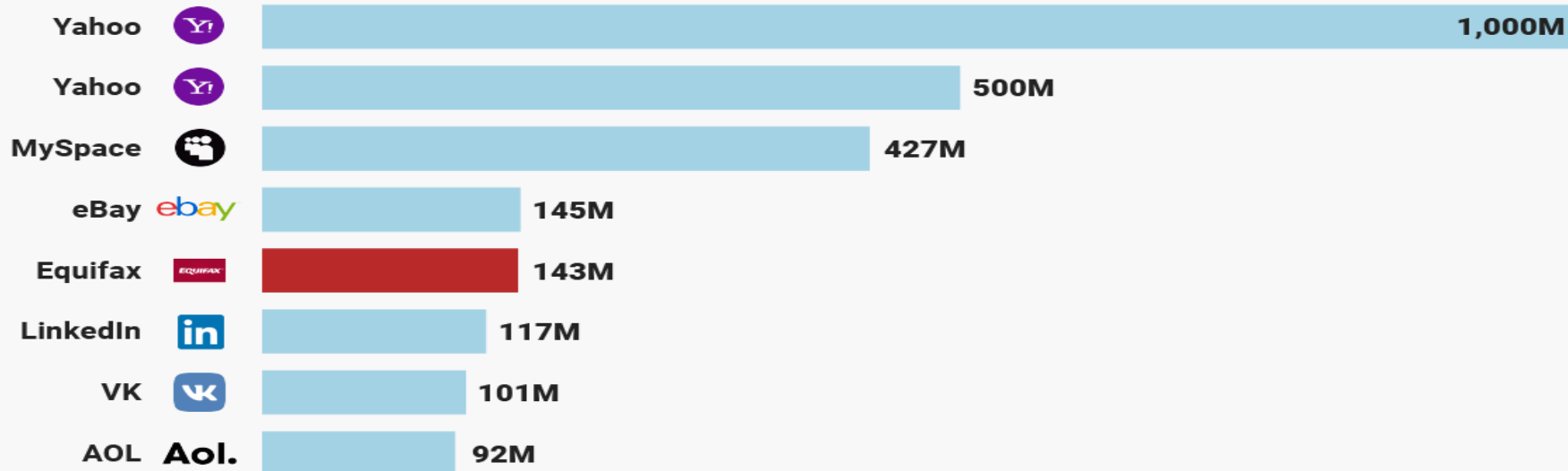


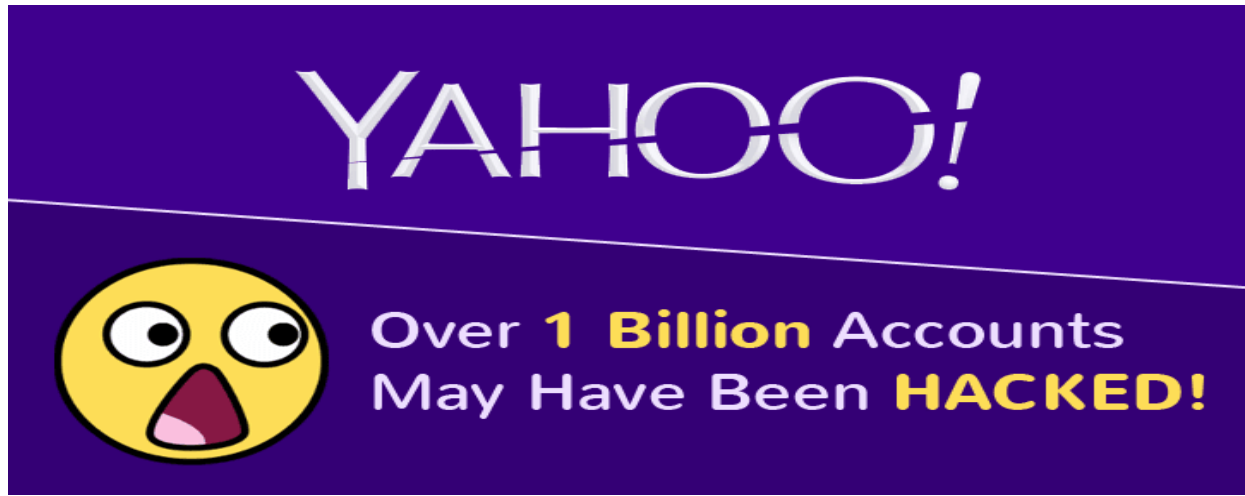


Delayed reporting for 6 weeks
CEO-CFO-Director sold all shares
CEO got 20M Bonus when fired



LATEST EQUIFAX HACK COULD BE THE WORST TO DATE





Yahoo's Marissa Mayer Subpoenaed to Testify Before Senate, Says Report

Verizon bought Yahoo for \$4.48 billion in June 2017

Marissa Mayer- 5 Years with Yahoo and left with a 23M severance package

Verizon reduced its acquisition offer by \$350 million following the disclosure of the breaches, purchasing the site for \$4.48 billion in cash.



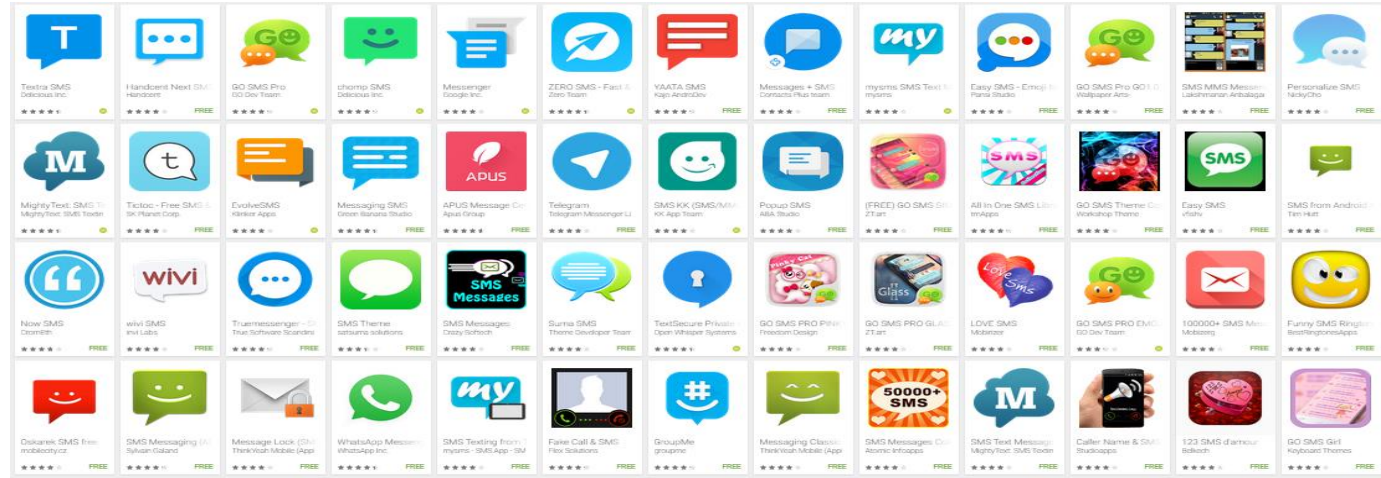
Microsoft sees no reason to increase its bid for Yahoo, two months after it made a \$44.6 billion offer to buy the Internet company, people familiar with Microsoft's plans said on Monday. (2010)

TWO CONCEPTS YOU NEED TO KNOW

1. SMS TEXT VS TEXT
MESSAGING

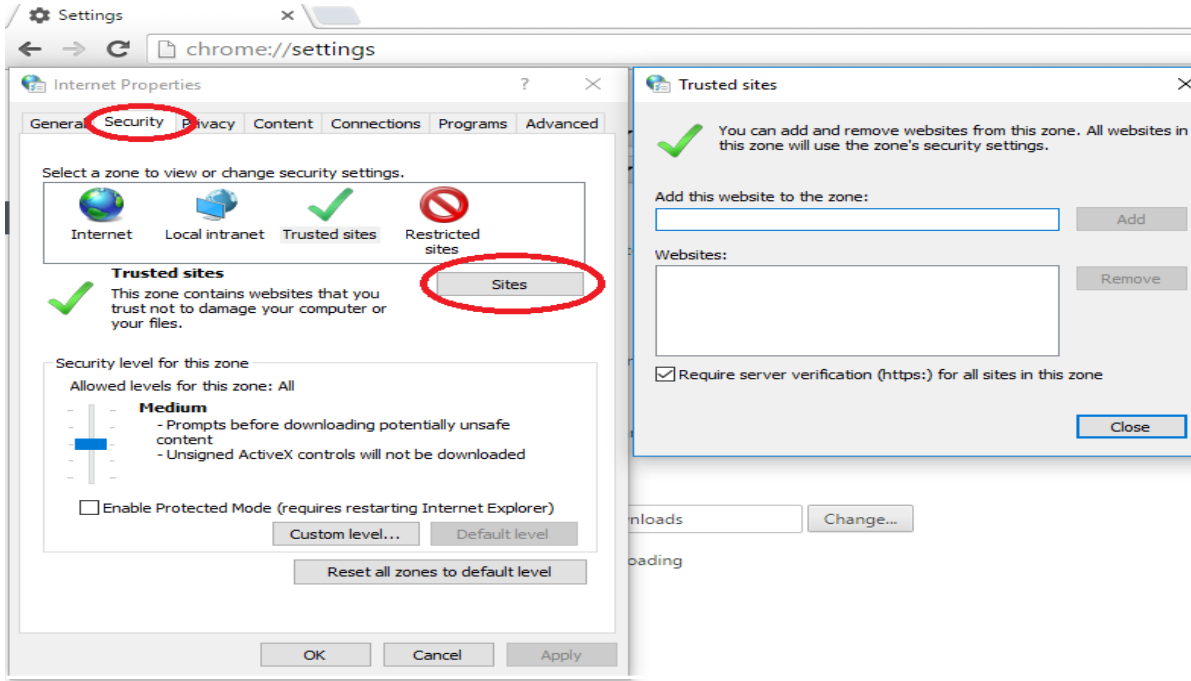
2. TRUSTED SITES





TEXT MESSAGING APPS

Trusted Sites



Google
Microsoft
Facebook
Your Bank
Last Pass

Browser
Cookies
C Cleaner

The Trick to get your Password



Why are Passwords so insecure?

Byron's Story





Passwords should be changed every 3 months

They should be complicated with upper and lower case

They should be 8 characters or more

PASSWORDS

The Guy Who Invented Those Annoying Password Rules Now Regrets Wasting Your Time



The man in question is Bill Burr, a former manager at the National Institute of Standards and Technology (NIST).

In 2003, Burr drafted an eight-page guide on how to create secure passwords creatively called the “NIST Special Publication 800-63. Appendix A.” This became the document that would go on to more or less dictate password requirements on everything from email accounts to login pages to your online banking portal. All those rules about using uppercase letters and special characters and numbers—those are all because of Bill.

“Much of what I did I now regret,” Bill Burr told The Wall Street Journal

This is why the latest set of NIST guidelines recommends that people create long passphrases rather than gobbledygook words like the ones Bill thought were secure.



SplashData has published its seventh annual "worst passwords" report, compiled from more than 5 million passwords leaked during the year, and there are some notable additions to the list.

In anticipation of last weekend's premiere of Star Wars: The Last Jedi, many fans have clearly decided to express their excitement by making "starwars" one of their passwords.

It joins the list at number 16, sandwiched between old favourite "abc123" and another new entry, "12312".

Worst Passwords of 2017

123456 (rank unchanged since 2016 list)
password (unchanged)
12345678 (up 1)
qwerty (Up 2)
12345 (Down 2)
123456789 (New)
letmein (New)
1234567 (Unchanged)
football (Down 4)
iloveyou (New)
admin (Up 4)
welcome (Unchanged)
monkey (New)
login (Down 3)
abc123 (Down 1)
starwars (New)
123123 (New)
dragon (Up 1)
passw0rd (Down 1)
master (Up 1)
hello (New)
freedom (New)
whatever (New)
qazwsx (New)

Still require strong PW

Passwords should withstand 100 guesses

it shouldn't be tied to any public information about you or your family.

Use a phrase

Go long

The new NIST guidelines suggest allowing users to create passwords up to 64 characters in length

Don't change your password until you have to

Choose something memorable

Get creative with characters

Use two-factor identification

5 2FA

- SMS 2FA --- SIMPLE
- Authenticator APP --- SUPER SIMPLE
- Google Prompt (Push 2FA) --- The SIMPLEST
- Authenticator Dongle
- Google Advanced Protection Program

Vip's, Politicians, Celebrities

Must use Fido U2F YubiKey






Cost \$18-\$25

Limited Apps

Four Main types of 2FA in common use by consumer Web Sites

Some Sites offer more than one option.

Twofactorauth.org to check sites

 BMO Bank of Montreal	Tell them to support 2FA on Twitter					
 BMO Harris Bank	Tell them to support 2FA on Twitter Tell them to support 2FA on Facebook					
 Boeing Employee Credit Union		✓				
 BoFI Federal Bank	Link	✓	✓			
 Capital One	Link	✓		✓		✓

SMS 2FA

Enable SMS 2FA - Provide SMS Phone number

Next time you log in with your username and password, you'll also be asked to enter a short code (typically 5-6 digits) that gets texted to your phone.

this is a very popular option for sites to implement, since many people have an SMS-capable phone number and it doesn't require installing an app.

It provides a significant step up in account security relative to just a username and password.



Disadvantages of SMS 2FA

- Don't want to give out phone number- (one more piece of personal info)
- Attackers using phone number takeovers could get access to your account without even knowing your account
- Can't log in if your phone is dead or can not connect to a network
- Trick phone company to assign # to different SIM Card
- International Travel
- Don't own Smart Phone



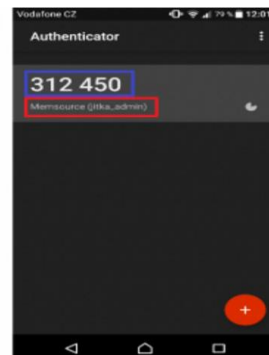
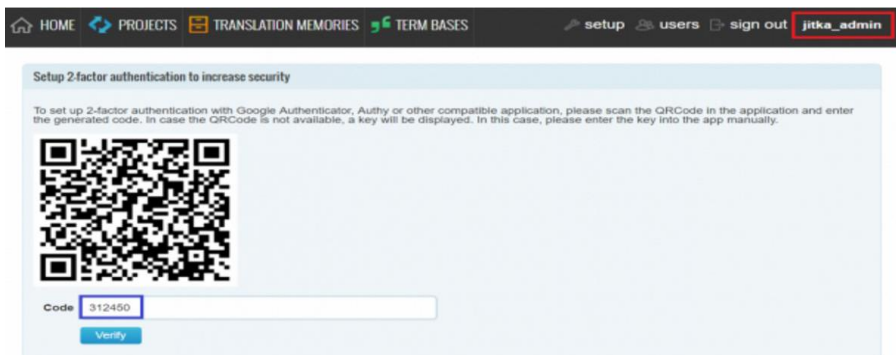
Authenticator APP= Time based one time PW

- Another phone-based option for 2FA is to use an application that generates codes locally based on a secret key
- Google Authenticator is a very popular application for this
- If a site offers this style of 2FA, it will show you a QR code containing the secret key. You can scan that QR code into your application.
- If you have multiple phones you can scan it multiple times
- you can also save the image to a safe place or print it out if you need a backup



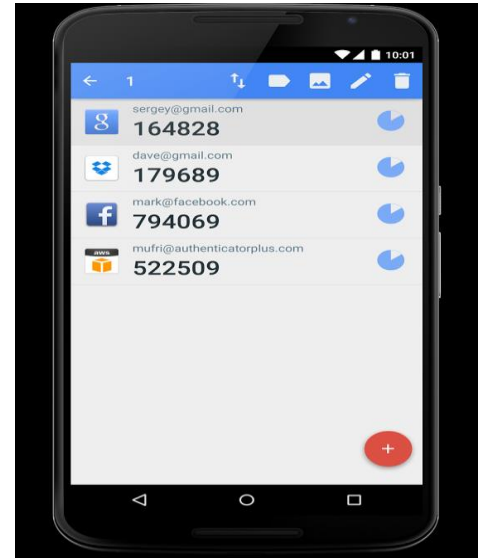
Authenticator App

- Once you've scanned such a QR code, your application will produce a new 6-digit code every 30 seconds.
- Similar to SMS 2FA, you'll have to enter one of these codes in addition to your username and password in order to log in.
- this style of 2FA improves on SMS 2FA because you can use it even when your phone is not connected to a mobile network
- the secret key is stored physically on your phone



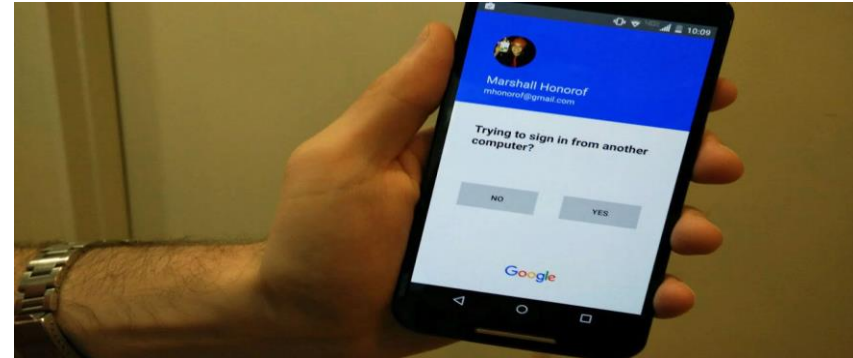
Disadvantages to Authenticator App

- If your phone dies or gets stolen, and you don't have printed backup codes or a saved copy of the original QR code, you can lose access to your account
- For this reason, many sites will encourage you to enable SMS 2FA as a backup
- if you log in frequently on different computers, it can be inconvenient to unlock your phone, open an app, and type in the code each time



Google Prompt (Push 2FA)

- Google Prompt method, can send a prompt to one of your devices during login
- This prompt will indicate that someone (possibly you) is trying to log in, and an estimated location for the login attempt. You can then approve or deny the attempt.



Push Based 2FA Improves in Authenticator Apps in Two Ways

acknowledging the prompt is slightly more convenient than typing in a code, and it is somewhat more resistant to phishing

this requires that you pay close attention to a subtle security indicator, IP address

Disadvantages of push based 2FA

It's not Standardized

can't consolidate all your push-based credentials in a single app

it requires a working data connection on your phone

while Authenticator apps don't require any connection

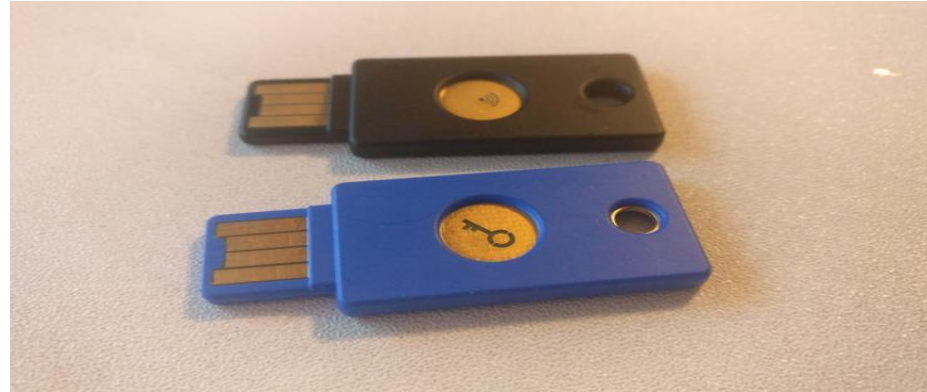


FIDO U2F / Security Keys

- Universal Second Factor (U2F) is a relatively new style of 2FA, typically using small USB, NFC or Bluetooth Low Energy (BTLE) devices often called “security keys.”
- Like push-based 2FA, this means you don’t have to type any codes.
- U2F is also well-designed from a privacy perspective



Where do I buy Security Keys?



USB security key with Bluetooth connectivity from
Feitian
standard USB key from
Yubico

GOOGLE'S 'ADVANCED PROTECTION' LOCKS DOWN ACCOUNTS LIKE NEVER BEFORE



Logging in from a desktop will
require a special USB key
(\$20)



Accessing your data from a mobile device
will similarly require a Bluetooth dongle
(\$25)

October 17-2017 – Google
Advanced Protection

Makes it harder than ever for hackers to
break into your sensitive data on Gmail,
Google Drive, YouTube or any other
Google property.

The opt-in, ultra-secure mode is
intended for truly high-risk users,
including those who face the threat of
state-sponsored, highly resourced
cyberespionage





Welcome, Ronald Brown

Control, protect and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy and decide how your information can make Google services work better for you.

Sign-in & security >

Control your password and Google Account access.

[Signing in to Google](#)
[Device activity & security events](#)
[Apps with account access](#)

Personal info & privacy >

Manage your visibility settings and the data we use to personalise your experience.

[Your personal info](#)
[Manage your Google activity](#)
[Ads Settings](#)
[Control your content](#)

Account preferences >

Set language, accessibility, and other settings that help you use Google.

[Language & Input Tools](#)
[Accessibility](#)
[Your Google Drive storage](#)
[Delete your account or services](#)

Signing in to Google

Control your password and account access, along with backup options if you get locked out of your account.

Make sure that you choose a strong password

A strong password contains a mix of numbers, letters and symbols. It is hard to guess, does not resemble a real word, and is only used for this account.

Password & sign-in method

Your password protects your account. You can also add a second layer of protection with 2-Step Verification, which sends a single-use code to your phone for you to enter when you sign in. So even if someone manages to steal your password, it is not enough to get into your account.

Note: To change these settings, you will need to confirm your password.

Password	Last changed: 24 February, 05:44	>
----------	----------------------------------	---

2-Step Verification	On since: 22 July, 11:39	>
---------------------	--------------------------	---

App passwords	None	>
---------------	------	---

Google account PIN	Last changed: 25 January, 19:45	>
--------------------	---------------------------------	---

Your second step

After entering your password, you'll be asked for a second verification step. [Find out more](#)



Google prompt (Default) ⓘ

Samsung Galaxy Tab4 10.1

Added: 1 August, 15:56

Motorola Moto G(4) Plus

Added: 1 August, 15:56

[ADD PHONE](#)



Authenticator app

Authenticator on Android

Added: 22 July, 11:39

[CHANGE PHONE](#)



Voice or text message

[\(602\) 730-6314](#) Verified

Verification codes are sent by text message.

[ADD PHONE](#)



Backup codes

10 single-use codes are active at this time, but you can generate more as needed.

[SHOW CODES](#)



Two-Factor Authentication Backup Codes

ⓘ If you lose access to your authentication device, you can use one of these backup codes to login to your account. Each code may be used only once. Make a copy of these codes, and store it somewhere safe.

860218724	958717631
363816342	915196351
039118211	007597330
705566718	462807066
820836406	295210480

[Print Codes](#)

[Copy Codes](#)

Set up alternative second step

Set up at least one backup option so that you can sign in even if your other second steps aren't available.



Security Key

A Security Key is a small physical device used for signing in. It plugs into your computer's USB port. [Find out more](#)

[ADD SECURITY KEY](#)

Devices that do not need a second step

You can skip the second step on devices that you trust, such as your own computer.



Devices you trust

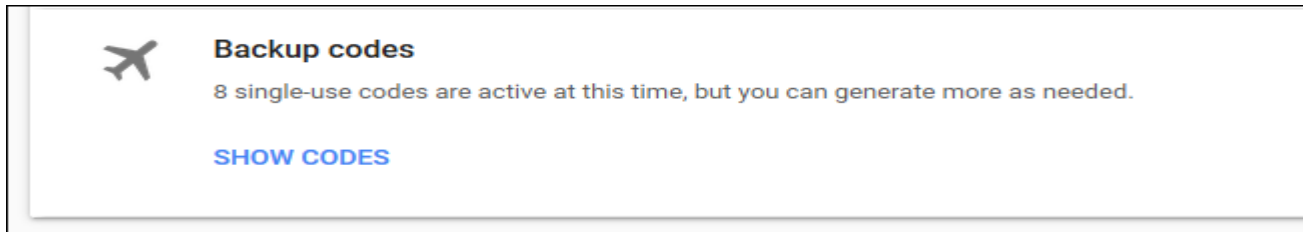
Revoke trusted status from your devices that skip 2-Step Verification.

[REVOKE ALL](#)

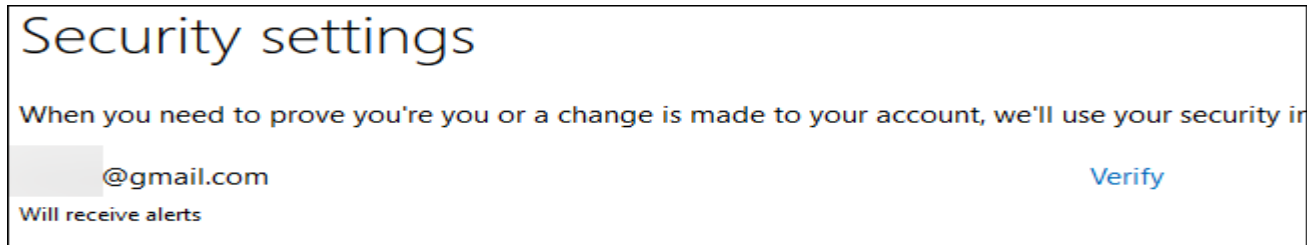
How to Avoid Getting Locked Out When Using Two-Factor Authentication

What happens if you lose or reset your phone? If you don't plan your recovery method ahead of time, you could permanently lose access to your accounts.

Print Your Backup Codes and Store Them Securely



Ensure You Have a Linked Email Address



All four major US carriers team up to create a better 2-factor auth solution

+4,578



Mobile Authentication
Taskforce

Better solution than SMS
Text for 2018

Who's using 2FA?

Less than 1 in 10 Gmail users enable two-factor authentication

Usenix Enigma It has been nearly seven years since Google introduced two-factor authentication for Gmail accounts, but virtually no one is using it.



In a presentation at Usenix's Enigma 2018 security conference in California, Google software engineer Grzegorz Milka today revealed that, right now, less than 10 per cent of active Google accounts use two-step authentication to lock down their

services.
12 per cent of Americans have a password manager to protect their accounts, according to a 2016 Pew study.

Google has tried to make the whole process easier to use, but it seems netizens just can't handle it. More than 10 per cent of those trying to use the defense mechanism had problems just inputting an access code sent via SMS.

2 Factor Authentication
Ron Brown – Silvercomctc
69janeplace@gmail.com

Questions?



An International
Association of Technology
& Computer User Groups