

SECURE YOUR IDENTITY

We all perform many actions online on a daily basis which increases the amount of data we leave behind that can be used against us. Securing your identity means being aware of the locations your data lives, being aware of the data's vulnerabilities, and learning how you can begin to implement some very simple changes to ensure your identity remains protected. Here are some great tips, let's get started.

PASSPHRASES REALLY ARE EVERYTHING!

Good Passphrases are the Best Defense!¹⁸

A "passphrase" is a long phrase used as a password, which is stronger than a secular word password. The increased length can allow for a greater number of possibilities, a passphrases made of randomly-chosen words can be both easy to remember and hard for someone else to guess, which is what we want.

Computers are now fast enough to quickly guess passwords shorter than ten or so characters—and sometimes quite a few more. That means short passwords of any kind, even totally random ones like nQ\m=8*x, or !s7e&nUY, or gaG5^bG, may be too weak, especially for settings where an attacker is able to quickly try an unlimited number of guesses. This is not necessarily true for an online account, where the speed and quantity of guesses will be limited, but it could be true in other cases (for instance, if someone gets ahold of your device and is trying to crack its encryption password).

¹⁸ <https://securityinabox.org/en/guide/passwords>
& <https://www.eff.org/dice>

To learn how to make a good passphrase we are going to follow the wonderfully easy workflow set up by our friends at the Electronic Frontier Foundation:

Step 1: Roll five dice all at once. Note the faces that come up without looking at the wordlist yet. (On our dice, the EFF logo is equivalent to rolling a one.)

Step 2: Your results might look like this reading left to right: 4, 3, 4, 6, 3. Write those numbers down.

Step 3: Open [EFF's Long Wordlist \[.txt\]](#) to find the corresponding word next to 43463.

Step 4: You will find the word "panoramic." This is the first word in your passphrase, so write it down.

Step 5: Repeat steps 1-4 five more times to come up with a total of SIX words.

When you are done, your passphrase may look something like this:

panoramic nectar precut smith banana handclap

Step 6: Come up with your own mnemonic to remember your phrase. It might be a story, scenario, or sentence that you will be able to remember and that can remind you of the particular words you chose, in order. For example:

The panoramic view, as I tasted the nectar of a precut granny smith apple and banana, deserved a handclap.



43453	pandemic
43454	pang
43455	panhandle
43456	panic
43461	panning
43462	panorama
43463	panoramic
43464	panther
43465	pantomime
43466	pantry
43511	pants
43512	pantyhose
43513	paparazzi
43514	papaya
43515	paper

Once you have made your passphrase please make sure of the following:

KEEP IT SECRET

Do not share your passphrase with anyone unless it is absolutely necessary. And, if you must share a passphrase with a friend, family member or colleague, you should change it to a temporary passphrase first, share that one, then change it back when they are done using it. Often, there are alternatives to sharing a passphrase such as creating a separate account for each individual who needs access.

MAKE IT UNIQUE

Avoid using the same passphrase for more than one account. That way if one passphrase is compromised hackers won't be able to exploit the rest of your accounts because you used your password for all of your online services. A good way to keep track of many unique and complex passwords is to use a password managers like Keepass X, Last Pass and 1pass.

KEEP IT FRESH

Change your passphrase on a regular basis, preferably at least once every three to six months based on your risk assessment. Some people get quite attached to a particular passphrase and never change it. This is a bad idea. The longer you keep one password, the more opportunity others have to figure it out. Also, if someone is able to use your stolen password to access your information and services without you knowing about it, they will continue to do so until you change the password.¹⁹

¹⁹ <https://securityinabox.org/en/lgbti-mena/passwords>

PASSPHRASE MANAGER

These days we have accounts with a lot of companies. Emails, Social media accounts, online bank accounts and so on. One of the most important things you can do is not use one password for all accounts but generate different passwords for each of your individual accounts.²⁰

NOW, YOU MIGHT BE SAYING WHHA???????

But hear us out. This is actually a good thing. After all, your bank information is likely linked to many of your accounts, as well as your purchase history, media browsing habits, and a slew of other private information that you'd prefer protected. But if you're the kind of person who constantly forgets and resets passwords and usernames, or worse, recycles the same password you've been using for the past seven years, it's time for a password management tool. If a hacker discovers your password on a list they can then use it to access every tool in your life!

Passphrase managers actually become invaluable once you take the first step—they are an incredibly powerful improvement to your security, while also being very usable.

Passphrase managers store all your passwords, generate strong ones for you, and in general, the only password you have to remember is the one to open your password manager. So, make it a strong one.



²⁰ <http://lifehacker.com/5529133/five-best-password-managers>

LASTPASS

LastPass saves your passwords and gives you secure access from every computer and mobile device. You only have to remember one password—your **LastPass**²¹ master password. Save all your usernames and passwords to LastPass, and it will auto login to your sites and sync your passwords everywhere you need them.

The benefit of LastPass is that it is super easy to use across all your platforms. The problem is that its ease of use comes with the caveat that LastPass is a corporation and your information is in their cloud. So balance its ease with your vulnerability and make your decisions for its use based on that. In general Last Pass is better then no Password Manager so please consider it

THIS IS A LASTPASS VAULT.

It's where you can add, view, manage, and delete items that you've saved to LastPass.

The screenshot shows the LastPass vault interface. On the left is a sidebar with a dark background containing:

- Collapse button
- Sites (selected)
- Secure Notes
- Form Fills
- Sharing Center (highlighted with a blue dot)
- Security Challenge
- Emergency Access
- Account Settings
- More Options

The main area has a red header with "LastPass" and a search bar. Below it is a "Sites" section with a "Favorites (6)" dropdown. It lists:

- Airbnb (AirBnB fan@lastpass.com)
- amazon.com (Amazon fan@lastpass.com)
- Evernote (Evernote fan@lastpass.com)
- facebook (Facebook fan@lastpass.com)
- Bank of America (Bank of America fan@lastpass.com)
- mint (mint fan@lastpass.com)
- YNAB (YNAB fan@lastpass.com)

Below the sites is a "Read Only + Shared Folder" section. At the bottom right is a "Save" button with a plus sign.

Folders
Drag and drop logins into folders to keep them organized.

Search
Easily search for any item stored in the vault.

Sync
Your account is synced and available everywhere you need it.

Sharing Center
Share passwords with family and friends that need access to an account.

Sites
LastPass keeps your data secure while helping you login to all your web accounts.

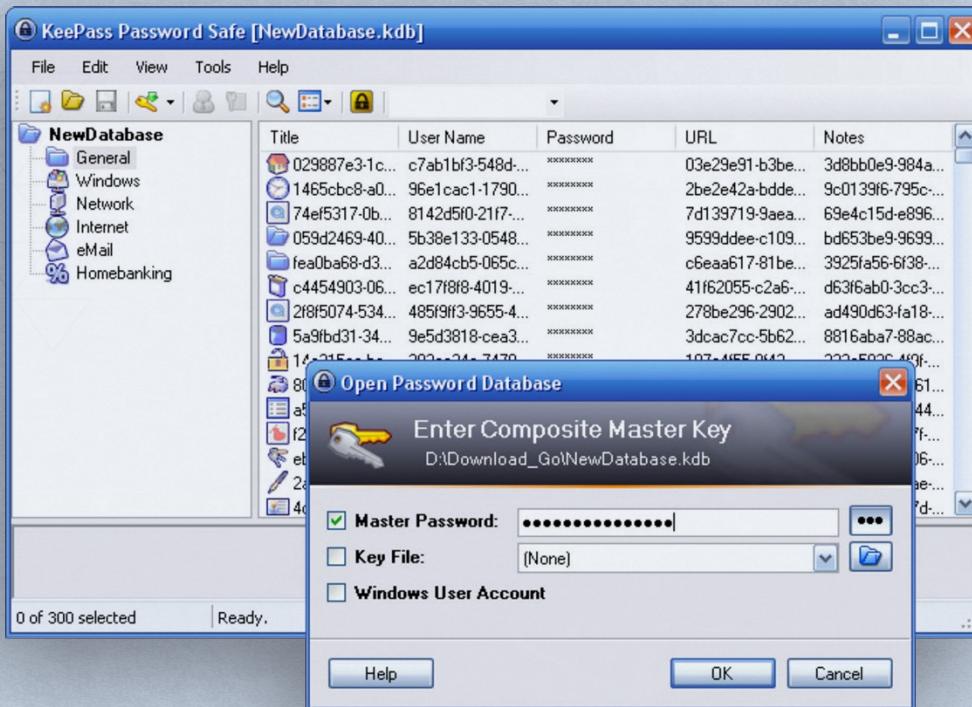
Save
Save new sites, notes, and profiles as you go.

²¹ <https://lastpass.com/how-it-works/>

KEEPASS X

KeePassX²² Password Safe is another free, open source, lightweight, and easy-to-use password manager for Windows, Linux, and Mac OS X, with ports for Android, iPhone/iPad and other mobile devices. You can download it for PC's or Mac's [here](#).

The benefits of KeePassX is that it is open source and is part of constellation of applications built by developers to support software independence. The challenges with KeePassX is the interface is confusing for beginners and there is not an easy way to sync KeePassX between your phone and your computer. That said, if you are willing to do a little work KeePassX can be one of your safest and most important autonomously implement password management solutions you could use.



²² <https://www.keepassx.org>

1PASSWORD

Like other password managers, 1Password enables you to sync your passwords across all of your devices using the same password vault. It is available for iOS, macOS, Android, and Windows.

When you first download the app from the App Store, you have to create an account. Same situation, one password will unlock all of your other passwords. It's all you need to unlock your confidential world on both desktop and mobile. **So make it good, and don't forget it.**

That will bring you into a dashboard where all your login information is stored. Here you can view and manage all the current user names and passwords you've saved.



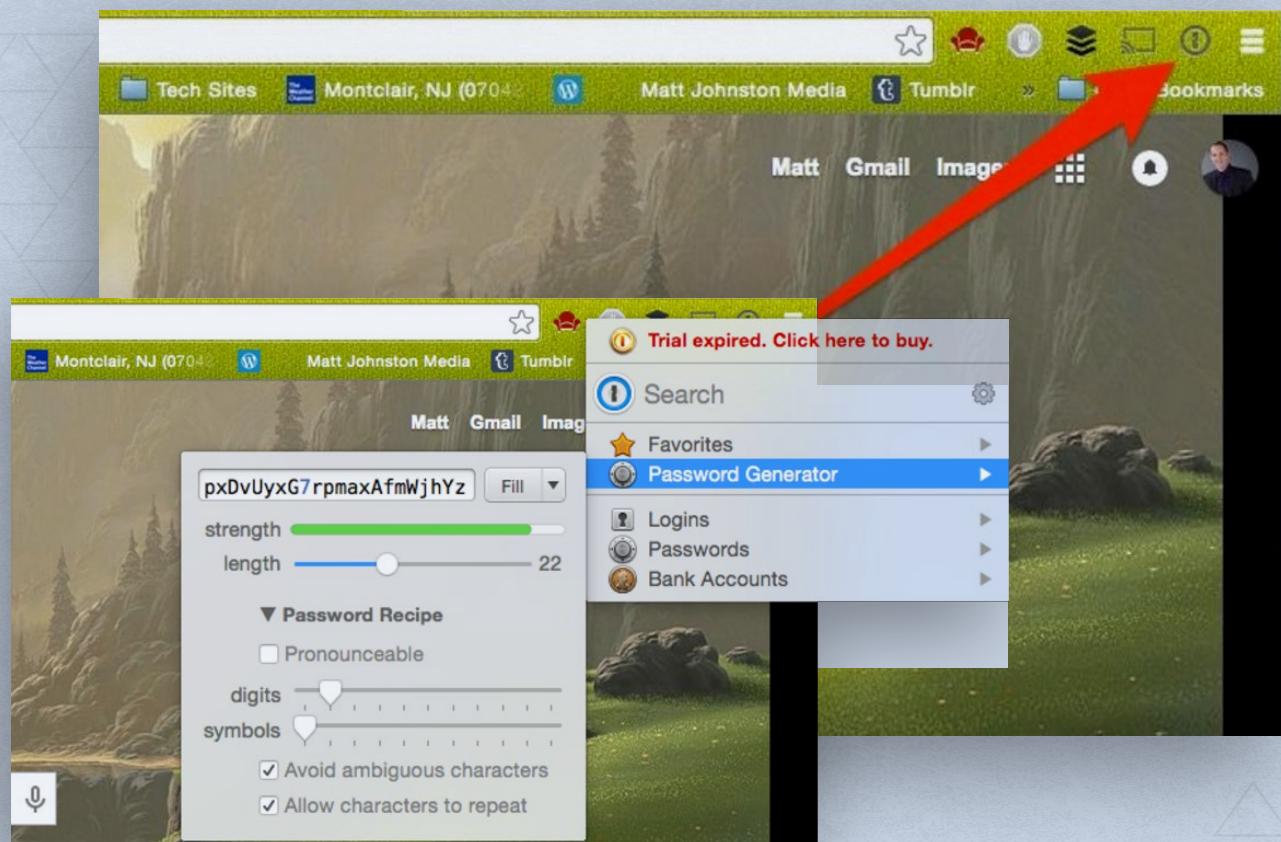
A screenshot of the 1Password desktop application. On the left, a sidebar lists categories: All Items (80), Favorites, Categories (Logins, Secure Notes, Credit Cards, Identities, Passwords, Bank Accounts), and Security Audit. The main pane shows a search bar and a list of items. The list includes: Amazon (with a shopping cart icon), AP Exchange (with a red AP logo), AP Images (with a red AP logo), Apple (with an Apple logo), Battle, Bccls, Best Buy (with a blue Citi logo), Best Buy (with a yellow Best Buy logo), Business Insider (with a blue BI logo). To the right, a detailed view of an Amazon login entry is shown. It includes: a thumbnail of the Amazon logo, the title "Amazon", a star icon, and a lock icon. Below this are fields for "username" (redacted), "password" (redacted), "strength" (green bar), and "website" (redacted). At the bottom, there are "show web form details", "last modified" (Mar 27, 2015 at 11:25 AM), and "created" (Mar 25, 2015 at 6:38 AM).

The secret to easily managing Login's is in a browser extension. You can get one for Chrome, Safari, Firefox or Opera.

Every time you're on a website where you need to input login information, you click this handy extension and tell it to fill in the information for you. The extension knows what site you're on and automatically fills in the blank fields.

The extension is also a hub for your whole password experience. In the drop down that opens, you can copy and paste passwords, view login information, and make complicated and hard-to-guess new passwords for all the sites you use.

Now there is no need to remember any passwords, just the one that gets you into the 1Password app.



The 1Password app has its own built-in browser that can take advantage of saved passwords, credit card information and more, but with the addition of Extensions in iOS 8, MobileSafari can use this information as well.

- ✓ If on a page with a login or other input field, simply tap the Share icon, then the iPassword icon. The app will ask for your master password, then it will fill in the requested information, just as it does on the Mac.

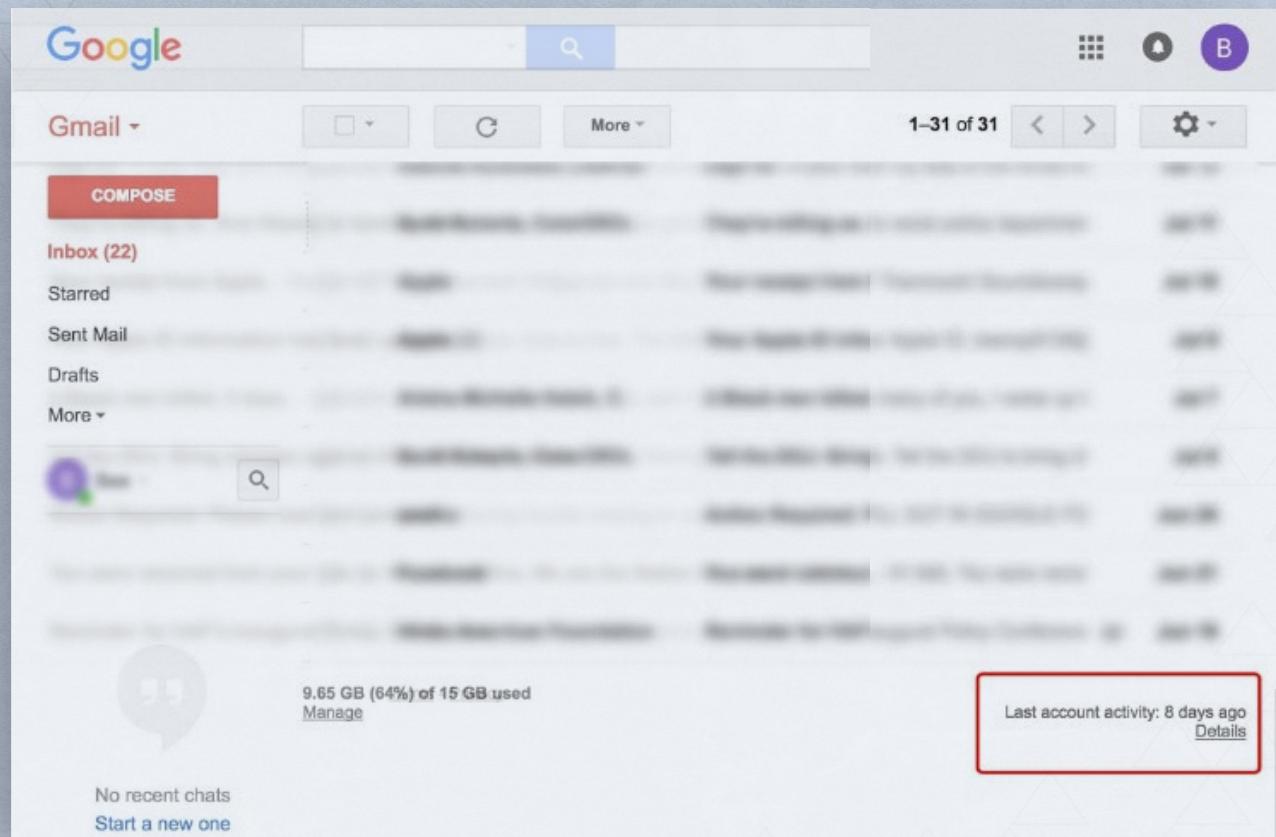
Apps also exist for Androids that work similarly. We recommend you sync your data across devices on a secure wi-fi network.



SECURE YOUR GMAIL

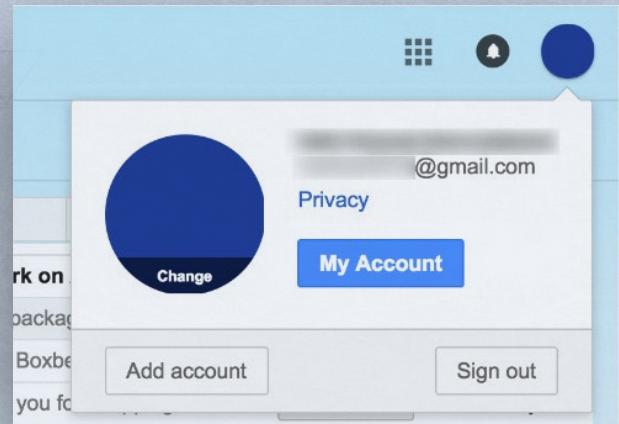
Google's Gmail is one of the most used web email apps in the world. This section helps us learn how to secure Gmail and how to identify if you are currently vulnerable. First, let's see whether your account has already been compromised.

- ✓ To check for signs of a hack, look at the bottom right hand side. It will tell you when the last activity on your account took place. Make sure the dates and times align with your use.
- ✓ Additionally, you can click on “**Details**” below to view a list of all the activity on your account.



✓ To set your account security for gmail and your google accounts in general, click on your profile picture on the top of your gmail screen and click on “My Account”

✓ You will be taken to a master settings page. Here you can make sure your basic settings are set to protect you. First, do an overall security check by clicking on “Get Started” under the “Security Check Up” option.



GOOGLE SECURITY CHECK UP

My Account

SERVICES WORK BETTER FOR YOU.

Sign-in & security

Control your password and account-access settings.

[Signing in to Google](#)
[Device activity & notifications](#)
[Connected apps & sites](#)

Security Checkup
Protect your account in just a few minutes by reviewing your security settings and activity.
[GET STARTED](#)
Last checkup: Yesterday, 9:06 PM

Find your phone
Whether you forgot where you left it or it was stolen, a few steps may help secure your phone or tablet.
[GET STARTED](#)

Personal info & privacy

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

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

Privacy Checkup
Take this quick checkup to review important privacy settings and adjust them to your preference.
[GET STARTED](#)
Last checkup: March 27, 3:22 PM

My Activity
Discover and control the data that's created when you use Google services
[GO TO MY ACTIVITY](#)

Account preferences

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

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

Check that your **recovery phone** or **email** are accurate and up-to-date. This will be useful in case you lose your passwords and entry into your account or if suspicious activity is detected on your account and Google wants to alert you.

← Security Checkup

Time for your Security Checkup

Protect your Google Account by reviewing these important settings.
You're only a few minutes away from better online security!



Check your recovery information

Help us get in touch with you if there's unusual activity in your account or you accidentally get locked out. Don't worry, we'll only use this info if we need to reach you about your account.

Recovery phone [Edit](#)
Recovery email [Edit](#)

[Done](#)

- ✓ Next, you can check that any recent changes made to the account settings were in fact made by you from a location you recognize.

Check your recent security events

Now, let's review your recent security events (like changing your password or adding a recovery email). Let us know if anything looks suspicious or unfamiliar, and we'll work together to ensure no one else has access to your account. [Learn more.](#)

A screenshot of the Google Account Security Events page. It shows a single event: "Changed recovery email" from "Brazil - Yesterday, 9:05 PM". Below the event list are two buttons: "Looks good" (highlighted in blue) and "Something looks wrong".

- ✓ Check that the devices from which you access your account look normal.

Check your connected devices

Next, please review the devices connected to your Google Account. Let us know if any of these devices look unfamiliar to you, and we'll work together to ensure no one else has access to your account. [Learn more.](#)

A screenshot of the Google Account Connected Devices page. It lists three devices: "Mac" (Brazil, CURRENT DEVICE), "United States - November 17, 9:42 PM" (status unknown), and "Windows" (USA - November 12, 10:15 PM, NEW). Each device entry has a dropdown arrow to its right.

- ✓ Check that the apps you have allowed access to your gmail account are there as you specified. We strongly recommend you do not allow access to random apps that are less secure as they can compromise your security and gather data about you.

Check your account permissions

Now let's review the apps, websites, and devices connected to your Google Account. Make sure you recognize, use and trust them all, or remove the ones you don't. [Learn more.](#)

A screenshot of the Google Account Account Permissions page. It shows two apps with access: "DocHub - Sign & Edit PDFs" (Has access to Google Drive, basic account info) and "Email Scheduler" (Has some account access, including Gmail, Google Docs, Google Sheets). Each app entry includes a "Remove" button.

- ✓ Lastly, check your 2-step verification settings and make sure you have your backup codes. To see more on this, read the section in this chapter called ***Two Factor Authentication for Gmail***

Check your 2-Step Verification settings

2-Step Verification adds an extra layer of security to your account. Please make sure your 2-Step Verification settings are up to date. [Learn more.](#)

Verify by



Text message to [REDACTED]

Backup options	Added on	Details
Backup phone	Oct 6, 2015	[REDACTED]
Backup codes	Oct 6, 2015	10 codes left

To update your settings please visit the [2-Step Verification](#) page.

[Done](#)

PRIVACY CHECK-UP

Now, back in your accounts page you can also perform a Privacy Check up.

The screenshot shows the 'My Account' page with three main sections:

- Sign-in & security**: Control your password and account-access settings. Includes links for Signing in to Google, Device activity & notifications, and Connected apps & sites. A 'Security Checkup' section with a 'GET STARTED' button is present.
- Personal info & privacy**: Manage your visibility settings and the data we use to personalize your experience. Includes links for Your personal info, Manage your Google activity, Ads Settings, and Control your content. A 'Privacy Checkup' section with a 'GET STARTED' button is present.
- Account preferences**: Set language, accessibility, and other settings that help you use Google. Includes links for Language & Input Tools, Accessibility, Your Google Drive storage, Family group, and Delete your account or services.

- ✓ Click on it and choose settings that minimize your exposure to the internet in general

The screenshot shows the 'Privacy Checkup' interface with the following steps:

1. Control what others see about you
2. Help people connect with you
3. Manage what you share on YouTube
4. Personalize your Google experience
5. Make ads more relevant to you



For example, uncheck the following suggestions so that only people you give your phone number to can contact you.

← Privacy Checkup

1. Help people connect with you

Let people with your phone number find and connect with you on Google services, such as video chats.



Help people who have your number connect with you across Google services. [Learn more](#)

Also help them find your name, photo, and other information that you've made visible on Google. [Learn more](#)

Help people who have your number connect with you across Google services. [Learn more](#)

Also help them find your name, photo, and other information that you've made visible on Google. [Learn more](#)

[EDIT YOUR PHONE NUMBERS](#)

[NEXT](#)

✓ 2. YouTube settings reviewed

Google can collect information on you to send you “**personalized ads**”. This means that you may get ads that relate to your recent emails. For example, if you wrote to your mom about difficulties you were having with your health, Google may start showing you ads for relevant pharmaceuticals. We strongly recommend you turn this service off and protect your daily information.

✓ To do this you need to toggle the “**Opt Out**”, switch to the “**OFF**” position.

Control your Google ads

You can control the ads that are delivered to you based on your Google Account, across devices, by editing these settings. These ads are more likely to be useful and relevant to you.

Ads based on your interests

Improve your ad experience when you are signed in to Google sites

OFF

With Ads based on your interests ON	With Ads based on your interests OFF
<ul style="list-style-type: none">The ads you see will be delivered based on your prior search queries, the videos you've watched on YouTube, as well as other information associated with your account, such as your age range or genderOn some Google sites like YouTube, you will see ads related to your interests, which you can edit at any time by visiting this pageYou can block some ads that you don't want to see	<ul style="list-style-type: none">You will still see ads and they may be based on your general location (such as city or state)Ads will not be based on data Google has associated with your Google Account, and so may be less relevantYou will no longer be able to edit your interestsAll the advertising interests associated with your Google Account will be deleted

We recommend you get an **IBA Opt Out Extension** for your Google Chrome. This tells Google, you have opted out of being tracked for ads throughout your browser experience.

- ✓ To install this go to **Chrome → Windows → Extensions**. Scroll to the bottom of the page and click on “**Get more Extensions**”. Search for Google Opt out and Install.

The screenshot shows the extension page for "IBA Opt-out (by Google)" on the Chrome Web Store. The page includes a puzzle piece icon, the extension name, its developer (chrome.google.com), a 4-star rating from 1097 reviews, and a "Social & Communication" category. It also shows 465,905 users installed and a green "ADDED TO CHROME" button. Below the header, there are tabs for "OVERVIEW", "REVIEWS", and "RELATED". The main content area features a blog post titled "10 Tips for Green Gardening" by "GOINGGREEN" on May 23, 2009, at 7:02 AM. The post discusses 10 tips for green gardening, mentioning organic and safe yard work, and how it can save money. To the right of the post are several promotional cards for related products:

- Energy Efficient**: Energy Efficient Controls: savings potential of approx. 70%. siemens.com/Sirius
- Solar Energy System**: Search Thousands of Catalogs for Solar Energy System. www.globalspec.com
- Juno & Jove**: Organic Style. Sustainable Fashion. Clothing and Accessories. www.JunoAndJove.com
- Burda Garden Heating**: Radiant Heaters for Cosy Hours in Your Garden. More Information Here! www.Burdawtg.de/Garden_Heater

On the right side of the page, there are sections for "By Google" (with a G+ icon) and "Compatible with your device" (with a checkmark icon). A large text block explains the extension's purpose: "Opt out of Google's interest-based ads as you browse the web with Chrome." Below this, a list of benefits includes stopping interest-based ads on partner websites, a one-time install, and persistence even after clearing cookies. There are also links for "Report Abuse" and "Additional Information" with details like version 1.5, last updated August 12, 2013, size 11.33KB, and language English.

TWO FACTOR AUTHENTICATION FOR GMAIL (2FA)

Because passwords can be phished, guessed, cracked, or acquired in other ways (like Keyloggers), you may want to consider adding another barrier to your accounts through two-factor authentication.

2FA as it's commonly abbreviated, adds an extra step to your basic log-in procedure. On your frequently visited accounts you typically enter your username and password once, and then you're done. This is categorized as a single factor of authentication. When you enable 2FA, it asks for two factors of authentication.²³ This factor can be code or even a physical dongle connected to your device.

A common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it. Including those two elements makes it more difficult for someone to access the user's bank account because they would have to have the physical item in their possession and also know the PIN.²⁴

Almost all online accounts and platforms now offer two-factor authentication. You can learn more and slowly implement 2FA by going to <https://www.turnon2fa.com>. You'll find tutorials for almost every platform you can think of and some you would even be surprised by. In either case you can never go wrong with 2FA so add it when you can!



NOTE: We will cover two factor authorization for Twitter and Facebook in the social networking section that follows.

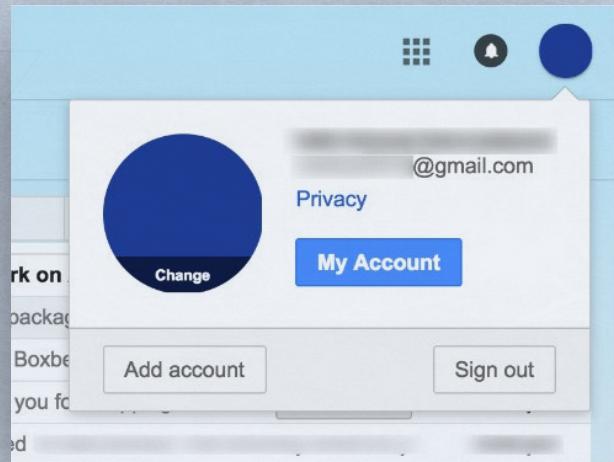
²³ <http://gizmodo.com/its-time-to-enable-two-step-authentication-on-everythin-1646242605>

²⁴ <http://searchsecurity.techtarget.com/definition/two-factor-authentication>

Most people only have—their password—to protect their account. With 2-Step Verification, if someone hacks your password, they will still need your phone or Security Key to get in.

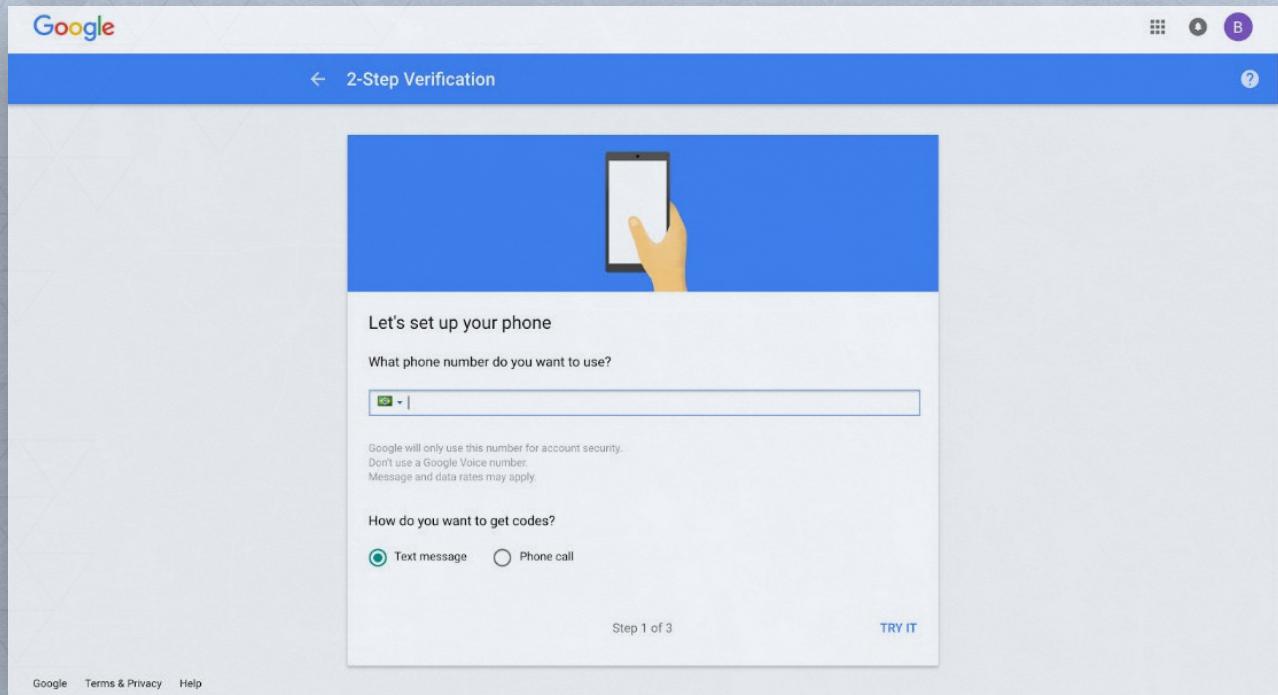
If turned on, signing in to your account will work a little differently:

- ✓ Whenever you sign-in to Google, you'll enter your password as usual.
- ✓ You will be asked for something else. Then, a code will be sent to your phone via text, voice call, or our mobile app.
- ✓ To set up 2FA on your gmail account, go to your profile pic/icon on the top right and click on “**My Account**.”, click on **Sign in and Security**. Then click to turn 2FA on.



The screenshot shows the 'Sign-in & security' page of the Google My Account settings. The left sidebar has links like 'Welcome', 'Sign-in & security' (which is selected and highlighted with a red border), 'Personal info & privacy', 'Account preferences', 'About Google', 'Privacy Policy', and 'Help and Feedback'. The main content area is titled 'Signing in to Google' and includes sections for password strength, sign-in methods, and 2-step verification. The '2-Step Verification' section is specifically highlighted with a red border around its 'Off' status.

Google will ask you for your phone number to send you the verification codes. Once you enter the phone number, you will receive a **text with the secret code**.





In the page that follows, **enter the code** you received via text

Google

2-Step Verification

Confirm that it works

Google just sent a text message with a verification code to [REDACTED]
Enter the code

Didnt get it? Resend

BACK Step 2 of 3 NEXT

Google Terms & Privacy Help

Google

2-Step Verification

It worked! Turn on 2-Step Verification?

Now that you've seen how it works, do you want to turn on 2-Step Verification for your Google Account

Step 3 of 3 TURN ON

Google Terms & Privacy Help



It's a good idea to set up backup codes to access your account when you don't have your phone at hand. When you click on backup codes, a list of codes comes up. Save these codes somewhere for future use.

The screenshot shows the '2-Step Verification' settings page. At the top, it says '2-Step Verification is ON since Nov 20, 2016' with a 'TURN OFF' button. Below this, under 'Your second step', there is a section for 'Voice or text message (Default)' which is set to send verification codes via text message. There is also a link to learn more about this step. Further down, there is a section for 'Set up alternative second step' with a note to set up at least one backup option. A 'Backup codes' section is visible, featuring a printer icon and a 'SET UP' button. At the bottom, there is a 'Google prompt' section.

The screenshot shows the '2-Step Verification' settings page with a modal window titled 'Save your backup codes'. The modal contains a list of 16 backup codes, each preceded by a checkbox. Below the list is a 'Google' logo. At the bottom of the modal, there is a note stating: 'You can only use each backup code once.' and 'These codes were generated on: Nov 20, 2016.' There are three buttons at the bottom of the modal: 'GET NEW CODES', 'DOWNLOAD', and 'PRINT'. In the background, the main settings page shows the 'Your second step' section with a note to set up at least one backup option.

That's it! Your 2FA has been set up!

If you set up 2-Step Verification using SMS text message or Voice call and also want to be able to generate codes using an Android, iPhone, or Blackberry, you can use the Google Authenticator app to receive codes even if you don't have an Internet connection or mobile service. Go to this [link](#), to set it up.



WARNING: 2FA can really protect your account from being hacked or stolen but bear in mind that setting up 2FA requires that you provide personal information, like your phone number, other email addresses etc, that will make these accounts increasingly traceable to you. In addition, many users find 2FA cumbersome because every time they login, it's a 2-step process. All factors considered, it is up to you to make the best decision on 2FA based on your situation and your needs.

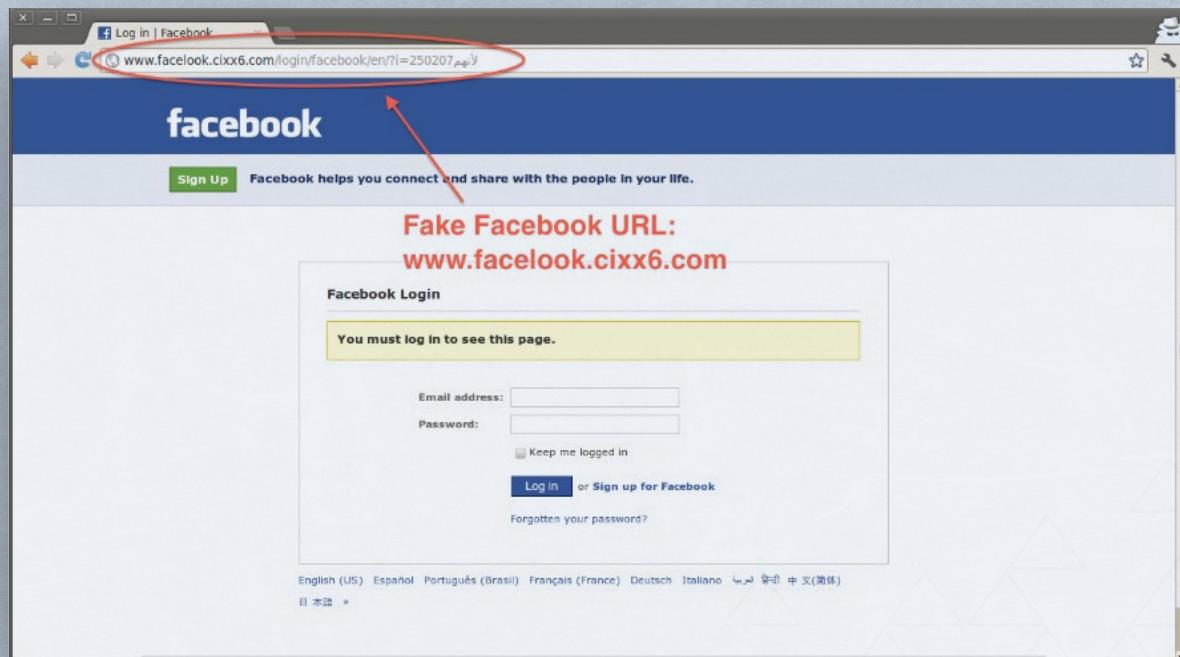
PROTECT YOURSELF FROM PHISHING

When an attacker sends an email or link that looks innocent, but is actually malicious, it's called **phishing**. Phishing attacks are a common way that users get infected with malware ("Malicious Software")—programs that hide on your computer and can be used to remotely control it, steal information, or spy on you.²⁵

The vast majority of malware is criminal, aimed at obtaining banking information or login credentials for email or social media accounts. But malware is also used by state actors. State intelligence agencies use malware to carry out covert actions against other states' computer systems, such as Flame and Stuxnet. States and state-supporting actors also use malware to spy on activists, journalists, and dissidents.²⁶

HOW CAN YOU IDENTIFY PHISHING SCHEMES?

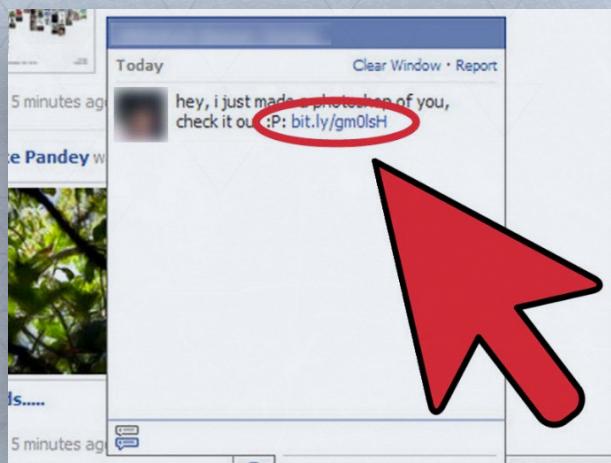
The message contains a mismatched URL, or a misleading domain name.



²⁵ <https://ssd.eff.org/en/module/how-avoid-phishing-attacks>

²⁶ <https://www.eff.org/issues/state-sponsored-malware>

The message is coming from your friend, but doesn't sound like your friend



The message asks for personal information like banking information

From U.S.Bank <...@Lehigh.EDU>☆
Subject Irregular Activities Verification.!
To Recipients <...@lehigh.edu>☆
12:24 AM
Other Actions ▾

usbank
All of us serving you™

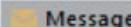
Note: This is a service message regarding Your Online Account please read.

Dear valued Customer :
This is a service message alert regarding the irregular activities we noticed on your account.
Please find Attached. Download the attached file and fill in all the requested information to complete the verification process to prevent your account from being blocked.

Your online account will be fully restored once the verification process is completed.
Thank you for being a valued customer.
©2014 U.S. Bank . All Rights reserved.

A screenshot of an email from U.S. Bank. The subject is 'Irregular Activities Verification!'. The email body starts with 'Dear valued Customer :'. It informs the recipient about irregular activities on their account and asks them to download an attached file for verification. The email ends with a copyright notice for 2014 U.S. Bank.

You are asked to send money to cover expenses

 Wed 1/14/2015 10:09 AM
Patrick Tan
RE: Request
To Benny Czarny
 Message  fw9_2013.pdf (115 KB)

Payee info: name, address, phone number
Completed Form W9 (if new domestic vendor)
Payee bank info:

- Bank name
- Bank address
- ABA/routing number
- Payee account number
- IBAN and/or SWIFT code (if international)

Amount of the wire payment

From: Benny Czarny [<mailto:benny@opswat.com>]
Sent: Wednesday, January 14, 2015 9:56 AM
To: Patrick Tan
Subject: Request

Hello Patrick,

Hope your day is going well. I will need you to make a wire transfer for me today. What would you need to get it done?

Thanks
Benny Czarny

DEALING WITH PHISHING

The best way to protect yourself from phishing attacks is to never click on any links or open any attachments sent to your email: this is unrealistic for most people. So here are some ways to deal.

Be alert. If something about a website doesn't feel right to you, it may not be:

- Check with the friend/family/bank/organization, over phone or another channel, to see if they actually did send you the files that were sent to you.
- If you have to frequently send and receive files for work consider sending the files through secure servers like Google Drive or Dropbox.

Antivirus software are programs that help protect your computer against most viruses, malware, worms, Trojan horses, and other unwanted invaders that can make your computer “sick” by performing malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers. We recommend that you use anti-virus software on your computer and on your messages. Note, installed software will not be useful if you do not update it regularly! Updates, keep the anti-virus on the lookout for the latest types of threats online.

We recommend Malwarebytes, Anti-Malware, Kaspersky labs and SOPHOS security, along with Windows Defender. These platforms are popular and used by many which keeps them efficient and more up-to-date than others.



TIPS: Another tool that is useful to know of is VirusTotal is a free online service that analyzes files and URLs enabling the identification of viruses, games, and other kinds of malicious content detected by antivirus engines and website scanners. Any user can select a file from their PC or email using their browser and send it to VirusTotal. However, it is important to note that VirusTotal is not a substitute for any antivirus/security software installed since it only scans individual files/URLs on demand.

Malwarebytes

For Home

ADVANCED MALWARE PROTECTION

Our next-gen technology protects businesses from attacks and remediates damage that other security solutions miss.

CONTACT US LEARN MORE

Need to remove malware immediately? [DOWNLOAD](#)

virus total

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected Choose File

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

[Scan it!](#)

[Blog](#) | [Twitter](#) | [contact@virus-total.com](#) | [Google groups](#) | [ToS](#) | [Privacy policy](#)

SO AGAIN NEVER OPEN ATTACHMENTS DIRECTLY ALWAYS OPEN IN GOOGLE DRIVE OR DOWNLOAD AND THEN SCAN IN VIRUS TOTAL

HAVE YOU BEEN COMPROMISED?

Everyday in the news, we hear about big corporations or websites getting hacked and being the bearers of bad news to their users informing them that their personal information has been stolen by hackers. These data breaches can include your name, passwords, government ID number, email address, date of birth, mother's maiden name, or any other piece of data you hand over to a website. Data from these breaches are posted on the internet for hackers of all types to see. These data leaks are often the source of bigger political hacks that can compromise movements.

One way to check to see when and where your data has been compromised is by using <http://haveibeenpwned.com> which is a service that catalogs data breaches as well as pastes (a type of publishing that is often used tech nerds and hackers). Be sure to change your passwords on these sites if you come up on a search.

The screenshot shows the Have I Been Pwned? website interface. At the top, there is a large blue header with the text '';--have i been pwned?' in white. Below the header, a sub-header reads 'Check if you have an account that has been compromised in a data breach'. A search bar contains the email address '@hotmail.com'. To the right of the search bar is a button labeled 'pwned?'. The main content area is red and displays the message 'Oh no — pwned on 1 site!'. Below this, a smaller message says 'Are you creating strong, unique passwords on all sites?'. There are social media sharing icons for Facebook and Twitter. In the bottom left corner of the red area, there is a logo for Adobe, consisting of a stylized red 'A' shape. To the right of the logo, the word 'Adobe' is written in white. At the very bottom of the red area, there is a detailed paragraph about the Adobe breach: 'The big one. In October 2013, 153 million accounts were breached with each containing an internal ID, username, email, **encrypted password** and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.'

COMBAT TROLLING BY FINDING YOUR DATA ONLINE

It is important to know where your personal data is online. By searching your information on the list of sites we have collected you can find and clear your presence on public data lists.



NOTE: While this is a painful and often shocking process for some, starting now can help reduce your footprint on the net.

This can be crucial for when Trolls, stalkers, and worse try to bully our folks for speaking out, a common strategy they use is Doxxing. In Doxxing your personal information including addresses, phone numbers, work information and family members are exposed on public platforms so that it opens you up to physical harassment and intimidation offline.

We want to stop tactics that might open up you and your loved ones to attacks. Limiting data is a crucial harm reduction strategy in a time when we are increasingly being seen as the target.

Please check yourself out and begin your data reduction journey with a visit to these sites:

Spokeo (to remove listing: http://www.spokeo.com/opt_out/new)

Anywho.com (to remove listing: <http://www.anywho.com/help/privacy>)

INTELIUS (to remove listing: <https://www.intelius.com/optout.php>)

Whitepages (to remove listing: <https://support.whitepages.com/hc/en-us/articles/203263794-Remove-my-listing-from-Whitepages->)

Finally, there is a more comprehensive list at Trollbusters at this link <https://yoursosteam.wordpress.com/2015/08/30/remove-your-mailing-address-from-data-broker-sites/>

