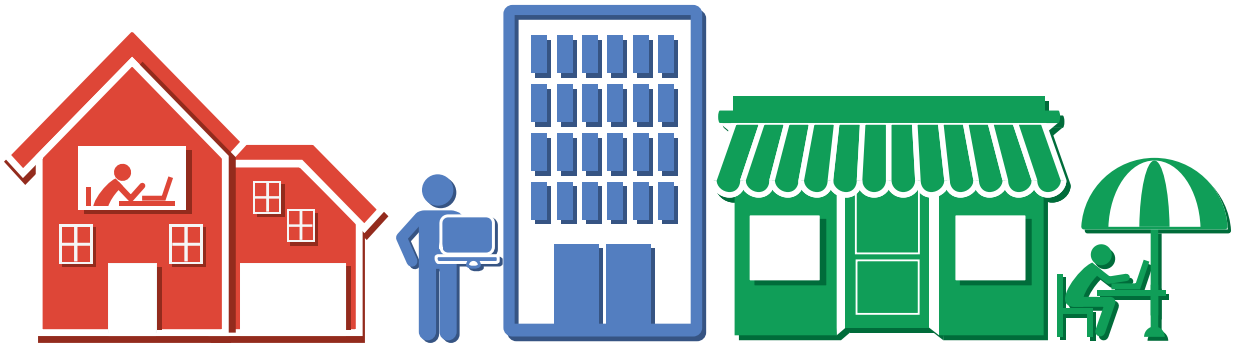
Google Safety Center

A guide to staying safe and secure online



Google

What's this booklet all about?

Google's Safety Center aims to help you, your family and your friends stay safe and secure on the Internet.

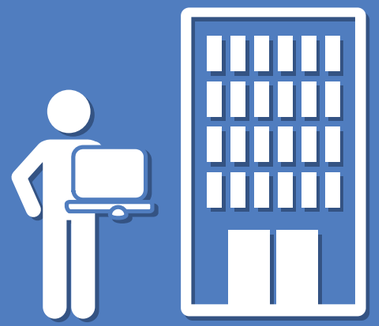
This booklet is designed to give you useful hints and tips that are easy to remember and put into action. We've included stickers with some of the key pieces of advice so you can put them on your computer or notebook to serve as helpful little reminders.

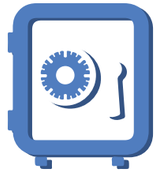
For in-depth information on all of the topics in this booklet and more, visit the Safety Center website at www.google.com/safetycenter.

Contents

How you can stay safe and secure online

Get off to a safe start. The Internet offers so many opportunities to explore, create and collaborate. To make the most of the web, you need to know how to keep yourself safe and secure. Whether you're a new Internet user or an expert, the advice and tools here can help you navigate the web safely and securely.





- Mix letters, numbers & symbols
- Use a different password for every website

Secure your passwords.

Passwords are the first line of defense against cybercriminals. It's crucial to pick strong passwords that are different for each of your important accounts, and it's good practice to update your passwords regularly. Follow these tips to create strong passwords and keep them secure.

1. Use a unique password for each of your important accounts, such as email and online banking.
2. Use a long password made up of numbers, letters and symbols.
3. Many services will send an email to you at a recovery email address if you need to reset your password, so make sure your recovery email address is up to date and linked to an account you can still access.

One idea is to think of a phrase that only you know, and relate it to a particular website to help you remember it. For your email account, you could start with a phrase such as "My friends Tom and Jasmine send me a funny email once a day," and then use numbers and letters to re-create it. "MfT&Jsmafe1ad" is a password with lots of variations. Then repeat this process for other sites.

- Don't respond to suspicious messages with personal information

Prevent identity theft.

Knowing the common tricks that criminals employ will help you protect yourself from online fraud and identity theft. Here are a few simple tips:

1. Don't reply if you see a suspicious email, an instant message or a webpage asking for your personal or financial information.
2. Never enter your password if you've arrived at a site by following a link in an email or a chat that you don't trust.
3. Don't send your password via email, and don't share it with others.

If you see a message from someone you know but it doesn't seem like it's from them, their account might have been compromised by a cybercriminal who is trying to get money or information from you. Be careful how you respond, or don't respond at all. Common tactics include asking you to urgently send them money, claiming to be stranded in another country or saying that their phone has been stolen so they cannot be called. The message might also tell you to click on a link to see a picture, an article or a video, which actually leads you to a site that might steal your information. Think before you click!

- Don’t respond to suspicious posts or emails
- Research online deals to avoid scams
- If it sounds too good to be true, it probably is

Avoid scams.

The web can be a great place, but not everyone online has good intentions. Here are three simple ways to avoid scammers and stay safe on the web:

1. Beware of strangers bearing gifts. If someone tells you you’re a winner and asks you to fill out a form with your personal information, don’t be tempted to start filling it out. Even if you don’t hit the Submit button, you might still be sending your information to scammers if you start putting your data into their forms.

2. Do your research. When shopping online, research the seller and be wary of suspiciously low prices, just as you would if you were buying something at a local store. Scrutinize online deals that seem too good to be true. No one wants to get tricked into buying fake goods.

3. When in doubt, play it safe. Do you just have a bad feeling about an ad or an offer? Trust your gut! Click on ads or buy products only from sites that are safe, reviewed and trusted.

- Log out of public or shared computers
- Set devices and screens to automatically lock

Lock your screen or device.

You should always lock your screen when you finish using your computer, laptop or phone. This step is especially important for phones or tablets, which are more likely to get misplaced and discovered by people you don’t want to access your information, as well as for home computers that are in shared spaces.For added security, you should also set your device to automatically lock when it goes to sleep.

- Secure your home router with a WPA2 password

Use secure networks.

It’s good to be extra-careful whenever you go online using a network you don’t know or trust, such as when you use the free WiFi at your local café. It's possible that the service provider is monitoring all traffic on their network, which could include your personal information.

When you connect through a public WiFi network, anyone in the vicinity can monitor the information passing between your computer and the WiFi hotspot if your connection is not encrypted. Avoid doing important activities such as banking or shopping over public networks.

If you use WiFi at home, make sure to secure your network so other people can’t use it. Secure it by setting up a password to protect your WiFi network—and just as with other passwords you choose, make sure that you pick a long, unique mix of numbers, letters and symbols so others can’t easily guess your password. Choose the WPA2 setting when you configure your network for stronger protection.

Finally, for an added layer of security, make sure you use a password to secure your router. Just follow the instructions provided by your Internet Service Provider or router manufacturer to set your own password for the router instead of using the router default password, which might be known to criminals. If criminals are able to access your router, they can change your settings and snoop on your online activity.

- Set up two-step verification for Google accounts
- Check settings before you share

Know your Google security and privacy tools.

With Google, you have a variety of tools that can help keep you safe and keep your information private and secure. Here is information about some of our most popular tools that help make Google work better for you.

Two-step verification

To bring even stronger levels of protection to your Google Account, we offer two-step verification to our users. This tool adds an extra layer of security by requiring not just a password, but also a verification code to sign in to a Google Account. Two-step verification lets Google make sure it's you by having you enter a code that's sent only to your phone—it's very unlikely that a remote attacker would get access to both that and your password.

Google account settings

On your Account settings page, you can see services and information associated with your Google Account and change your security and privacy settings.

YouTube privacy settings

Sometimes you might want to share your YouTube videos with just a small group of friends or even keep them to yourself. If so, you can choose to make your video either “unlisted” (hidden from search results, but viewable by people with the link) or “private” (viewable only by you) when you upload your video.

Know your Google security and privacy tools.

Manage the data stored in your Google Account.

Google Dashboard shows you what’s stored in your Google Account and provides an overview of some of your recent account activity. From one central location, you can easily view your data and activity and access your settings for services such as Blogger, Google Calendar, Google Docs, Google+ and more.

Manage your ads preferences.

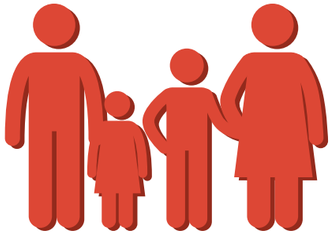
Ads help fund many of the free online services you love and use every day. With Google’s Ads Settings, you can understand how ads are selected for you, control your information that is used to select ads and block specific advertisers.

Manage who sees what you share.

Google+ circles help you manage your friends and contacts. You can put your friends in one circle, your family in another and your boss in a circle all alone—just like in real life. Then you can share relevant content, such as Google+ posts, YouTube videos, or Google Local Listing Ads, with the right people at any time you choose.

Make safety choices that fit your family

Lay the groundwork. As a parent or guardian, you know what feels right for your family and how your kids learn best. To help your family navigate through new technologies, gadgets and services in an ever-changing online world, you need to get practical advice. That’s why we continually talk to safety experts, parents, educators and communities around the world—to keep a pulse on what works. Together we can help nurture a community of responsible digital citizens.



Family safety basics

For busy parents, here are some quick suggestions for how to help keep your family safe online:

1 Talk with your family about online safety.

Be clear about your family's rules and expectations around technology, as well as consequences for inappropriate use. And most important, make sure your family feels comfortable enough to ask for guidance when they encounter tough decisions. This discussion can help your family feel safe when exploring the Internet on their own, and to know whom to turn to—you—when they have questions.

2 Use technology together.

It's a good way to teach online safety, and it creates opportunities for you to address online safety topics with your family as they come up.

3 Discuss online services and sites.

Talk with your family about what kinds of sites they like to visit and what is appropriate for each family member.

4 Protect passwords.

Help your family learn how to set secure passwords online. Remind your family not to give out their passwords, except maybe to trusted adults, such as a parent. Make sure they make a habit of signing out of their online accounts when they are on public computers at school, in a café or at the library.

5 Use privacy settings and sharing controls.

Many sites are available for sharing thoughts, photos, videos, status updates and more. Many of these services offer privacy settings and controls that help you decide who can see your content before you post it. Talk with your family about what they should and shouldn't share publicly. Help them respect the privacy of others by keeping personal details about family and friends private, and by not identifying people by name in publicly shared content.

6 Check age restrictions:

Many online services—including Google—have age limits restricting who can use their services. For example, you have to meet age requirements to have a Google Account, and some Google products are restricted to users 18 and older. Always check a website's terms of use before allowing your child to sign up for an account, and be clear with your children if you have family rules about which sites and services they can use.

7 Teach your family to communicate responsibly.

Here's a good rule of thumb: If you wouldn't say it to someone's face, don't text it, email it, instant message it or post it as a comment on someone's page. Talk about how what you say online might make other people feel, and come up with family guidelines about what kind of communication is appropriate.

8 Talk to other adults and experts.

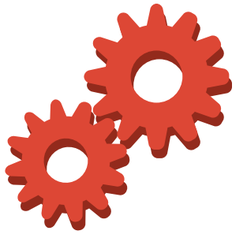
Open the conversation to your friends, extended family, teachers, coaches and counselors. Other parents and professionals who work with children can be a great resource to help you decide what feels right for your family, especially if you're dealing with an area of technology that you are unfamiliar with.

9 Protect your computer and identity.

Use antivirus software and update it regularly, unless you have a Chromebook, which doesn't need antivirus software. Talk with your family about the types of personal information—such as a Social Security number, a phone number or a home address—that should not be posted online. Teach your family not to accept files or to open email attachments from unknown people.

10 Keep it going.

Staying safe isn't a one-time thing—technology evolves, and so will the needs of your family. Make sure you keep up an ongoing dialogue. Re-establish your family's ground rules, check in on everyone's progress and set aside time to talk at regular intervals. The following tips from our partners address common issues that parents are concerned about.



Learn about easy-to-use safety tools.

Discover Google safety features designed to help control what your family sees online.

Get family-friendly results from Search.

By enabling Google SafeSearch, you can filter out most of the mature content that you or your family prefer to avoid. If an inappropriate result does sneak through, you can report it to Google. We're always working to improve our content filters, and this kind of feedback can help us make SafeSearch better for everyone.

Set a filter to keep inappropriate content out.

If you'd prefer not to see mature or age-restricted content as you browse YouTube, scroll to the bottom of any YouTube page and enable Safety Mode. Safety Mode helps filter out potentially objectionable content from search, related videos, playlists, shows and films.

Supervise users on shared Chromebooks.

You can't always be there to supervise your family's web activity. For the times you're not in the room with them, there's Supervised User for Google Chrome. When this feature is enabled, you can review a history of pages the user has visited, allow or block certain sites, and manage which websites your family member can view.

Limit access to approved apps and games.

Want to share your tablet without sharing all your stuff? On Android tablets running version 4.3 and higher, you can create restricted profiles to limit the access that other users have to features and content on your tablet.

Use app ratings to choose age-appropriate apps.

Just like at the movies, you can decide which Google Play apps are appropriate for your family by looking at the ratings: Everyone, Low Maturity, Medium Maturity, or High Maturity. You can filter apps by level, and also lock the filtering level with a simple PIN code (keeping other users from accidentally disabling the filter).

Discover Google safety tools designed to help your family monitor their online reputation.

Stop unwanted comments or tags.

If you'd rather not see someone's posts on Google+, you can block them by going to their profile and selecting Report/block [person's name]. You can also mute specific posts to no longer see them in your stream.

Control the chatter about your videos.

It's easy to moderate the comments on your YouTube channel. You can choose to delete comments, or to hold comments from certain people or with certain keywords from being published before you review them.

Block offensive YouTube users.

If someone is making comments that you don't like on your videos or channel, you can block them on YouTube. They will no longer be able to comment on your stuff or send you private messages.

Keep prying eyes off your device.

Not only is locking your screen an important part of protecting your account, it also makes sure that other people won't snoop around your phone if you happen to leave it out. You can select a PIN, password or a pattern to set a screen lock on your phone or tablet.

Report offensive content.

If someone makes an inappropriate comment or post on Google+, YouTube, or Blogger you can report it. Google has clear content policies that explain what is and isn't appropriate to do on these sites, so if you see content or behavior that violates our policies, you can flag it for review. We review flagged content around the clock, and we may remove content and limit or shut down accounts of users who violate our policies.

How Google helps protect you

The Internet is a great thing. But just like in the offline world, not everyone online has good intentions. Google takes your privacy and security very seriously. We invest millions of dollars each year and employ world-renowned experts in data security to protect your information. They focus on keeping you and your information safe and secure, and on staying one step ahead of cybercriminals.

Google works hard to help protect you from identity theft, personal fraud and online scams; to help protect your computer; and to make the Internet a safer place. We give you the tools and knowledge you need to keep yourself and your family safe online. And we're constantly investing and improving to fight on your behalf.

We're helping combat identity theft.

Google uses a variety of technologies to help protect you from online identity theft and make sure your Google Account stays safe and secure.

Two-step verification

To bring even stronger levels of protection to your Google Account, we offer two-step verification to our users. This tool adds an extra layer of security by requiring not just a password, but also a verification code to sign in to a Google Account. Two-step verification lets Google make sure it's you by having you enter a code that's sent only to your phone—it's very unlikely that a remote attacker would get access to both that and your password.

Encryption

Google takes many steps to keep your personal information safe from attackers and snoops. By default, we encrypt the Gmail connection between your computer and Google, which helps protect your Google activity from being snooped on by others. We also make this protection, known as session-wide SSL encryption, the default when you're signed into Google Drive and many other services.

We’re working to help keep your computer and device clean.

You can help protect your computer from malware, but Google also works hard to help protect you, too. We have hundreds of security experts working around the clock to help ensure that your data and devices are secure.

Helping you avoid malware

Just as Google searches the web for sites with the best answers to your questions, we also look for sites that appear to be harmful to users or have malware on them. Every day we identify and flag more than 10,000 of those unsafe sites, and we show warnings on as many as 14 million Google search results and 300,000 downloads, telling our users that there might be something suspicious going on behind a particular website or link.

Helping you keep your mobile device safe

Smartphones running Google’s Android software have similar protections in place to reduce the risk of damage. Android also requires that every app in the Google Play store list what kind of information the app wants to collect or access from your device, so you can decide whether you trust the app or not. We also automatically scan Google Play to block and remove harmful apps. For some Android phones, our Google Application Verifying Service will check for potentially harmful applications, no matter where you are installing them from.

We’re making the Internet safer for everyone.

Protecting users is a shared responsibility. We are all better off when everyone uses the best security technologies and techniques.

Sharing expertise and tools

Because your safety is important to us no matter what services or products you’re using, we share the information about the bad sites and links that we find with other companies, so that they can help protect their users as well. By working together and helping each other, the whole web is much safer.

Communicating with users and website owners

As we work to protect our users and their information, we sometimes discover and investigate unusual patterns of activity. Every day we identify and flag more than 10,000 of those unsafe sites. We also send messages every day to thousands of website owners whose sites we think might have been compromised by an attack, so they can clean up their sites.

Partnering with security organizations

Google is part of a number of organizations that work to help companies improve security for their users. For example, we partner with and helped found StopBadware.org to make the web safer by stopping, mitigating and cleaning up websites compromised by malware or other bad software.

STICKERS!

15 takeaway tips to help you stay safe and secure online. For more safety tips, visit www.google.com/safetycenter.

For partners and more resources, visit www.google.com/safetycenter.

For more information on how to stay safe online, visit **www.google.com/safetycenter**.

© 2014 Google Inc. All rights reserved, Google, the Google logo, Android, Blogger, Chromebook, Gmail, Google Calendar, Google Chrome, Google Dashboard, Google Docs, Google Drive, Google Local Listing Ads, Google Play, Google SafeSearch, Google+ and YouTube are trademarks or registered trademarks of Google Inc.
All other company and product names may be trademarks of the respective companies with which they are associated.