

media apps, look for “Apps,” “Data Sharing” or a similar term in the social media site’s Help menu, Preferences or Settings. To control what an app collects and shares outside of social media, check the settings in the app itself.

Control how much you share with the social network: Social media companies collect users’ personal data in order to send targeted advertising based on their online habits and purchases. Read the company’s “Privacy Policy” or “Data Use Policy” to learn how and when the site collects, uses and shares your personal information. It’s difficult to turn off this type of tracking and data collection, though new controls are starting to emerge that make it easier, such as the “Do Not Track” function available in some Web browsers.

Tips and reminders

Here are some tips and reminders that will help you enjoy social media while still protecting your privacy:

- Social media profiles are the first place many employers, college admissions officers, insurers, government agencies, customers and clients, landlords and others go to learn about you. Consider what your profile is communicating about you.
- Never publicly post your Social Security number, mother’s maiden name or other information that is routinely used to verify identity. Keep your address off social networks, and be very cautious about posting your phone number or an email address that could be used to trace you. If you post your birthday, do not display the year you were born.
- Create a strong account password (a mix of at least eight numbers, letters and symbols) and change it regularly. Don’t use the same password for all your accounts.

- Social media companies and app developers can change their privacy policies frequently, so read all notices these companies send you. Monitor your accounts and adjust your settings as needed.
- Don’t download an unfamiliar app until you’ve read user reviews and made sure the developer is legitimate.
- Some location-based apps track where you are and broadcast your whereabouts—even apps that don’t need that information to function. This information not only tells others where you are, but also that your home may be unoccupied.
- Participating in games and quizzes is likely to open up your personal information—and even that of your contacts—to use by a website or app.
- Understand and comply with your employer’s social media policy, if it has one. If it doesn’t, err on the side of caution when posting information.
- Don’t accept invitations to connect or friend requests from people you don’t know.
- If you post something to another person’s profile, you can’t control who else sees it.

Kids and social media

Though some social media sites prohibit use by children under 13, kids are still finding ways to use these services.

One of the best ways to protect kids on social media is to talk to them about how to be safe and responsible online.

Set strong privacy preferences on their accounts, take advantage of controls that allow parents to monitor or restrict their children’s contacts and network activity, and actively monitor your child’s communications.

Resources

How to Read a Privacy Policy

<http://oag.ca.gov/privacy/facts/online-privacy/privacy-policy>

This guide from the California Department of Justice Privacy Enforcement and Protection Unit helps consumers nationwide understand what to look for in a privacy policy.

OnGuardOnline.gov

www.onguardonline.gov

This federal government website helps consumers—including children and teens—be safe and secure online.

Consumer Action

www.consumer-action.org

Email: info@consumer-action.org

About this publication

 **Privacy Information**
A Consumer Action Project

This publication was funded by Consumer Action’s Privacy Information Project (www.privacy-information.org).

Privacy Information
www.privacy-information.org

A project of **Consumer Action**

Privacy and control for social media users

How much do you want to share?



Ever-evolving Internet-based communications tools allow users to share information, build online communities, expand professional networks and bring attention to key issues. Because sharing online can lead to unintended consequences, it's important to be aware of the risks and benefits of social media, as well as the information controls available to users.

Using social media has become a part of everyday life for people of all ages and backgrounds. Posting pictures, finding and staying in touch with friends and customers, sharing personal milestones, viewing résumés and broadcasting news and ideas are just some of the ways that more than a billion people and businesses around the world use social media.

Sharing can be fun, productive and rewarding. But social media users who don't exercise reasonable caution and take the time to learn the data-use policies of each site they post to may find they are sharing more than they mean to or are comfortable with. This is why many social networks offer ways to control how much you share and who you share it with.

Why privacy matters

Social media users need to understand who has access to their profile and how the information they share can be used, both by other users and by the social media company itself. Your personal information is routinely used to sell you new or enhanced services and shared with other businesses that would like you to use their products or services.

In the wrong hands, personal information such as your full name, birthday and/or year of birth, current location, travel plans, children's names and where you work could be used in invasive or criminal ways. Careless use of social media has the potential to expose you to unwelcome target marketing, cybercrimes like bogus emails, identity fraud

and cyberbullying, and even physical crimes such as stalking, burglary or assault.

The good news is that you can control much of what you share via social media.

To share or not to share?

There are two decisions to make when using social media: what to share and who to share it with. When determining what to share, think about how the information you reveal could be used. Here are a few things to consider:

Could someone (for example, an ex-spouse fighting for custody, a lender considering your loan application or a health insurer determining whether you qualify for coverage) use the information against you?

Sample post: Argh. I've started smoking again, pretty heavily.

Possible result: Health insurance company decides you are a higher risk and increases your premiums.

Could the information make you or a family member or friend vulnerable to identity fraud or some other crime?

Sample post: Can't wait for our weeklong vacation starting tomorrow!

Possible result: Thieves may see this as an opportunity to rob your home while you are away.

Would you want your current or a prospective employer to see your communications and photos, or the communications and photos of people you're connected to?

Sample post: My boss is such a pain! I'm tired of doing all the work and not getting any credit.

Possible result: Your employer may question whether you value your job.

Can you remove information, or "hide" it, if you want to in the future? (Even if you can, do you want to take the chance that a permanent record has been created online?)

What you want to share should influence your decisions about who to share with. For example, a photo that may be appropriate for sharing with friends and family may not be something to share with an employer, client, parent or child.

As you post, carefully consider restrictions on who will be allowed to see it. Should you share with your inner circle, acquaintances, friends-of-friends or "everybody"? Generally speaking, the wider your audience, the more thought you should give to what you reveal.

Privacy controls

Whether you're accessing your social media accounts via a computer, a smartphone, a tablet or other Web-enabled device, you have options regarding what information to share and the people you share it with. When you open an account with any social network, it comes with default (automatic) settings. The default settings are not the same for each network, and on some networks they may be set for less privacy than you would like. Before you post, adjust the privacy settings to match your comfort level.

The location and design of privacy settings and controls varies across social networks and devices. Your favorite social media sites viewed on your computer may look quite different when accessed via "apps" on your mobile device. But the user controls for posting information generally should be the same.

To access privacy controls, first log in to your account, then look for a tab or heading such as "Privacy," "Privacy Controls," "Privacy Settings," "Account Settings" or "Preferences." If you're having trouble finding it, use the site's "Help" feature. Here you'll find instructions on locating and using the network's features and tools.

If you still can't find what you're looking for in the Help section, contact the social network's Support staff via a link from the site or app, or ask a question in the "Community" or "Forum" area, where other users and, in some

cases, support staff can respond. Some networks also provide a guide on how to adjust their privacy settings, or you can use a search engine to find an online tutorial that guides you through the settings. Search for "How do I use the privacy settings in [name of social network]?" As always, be wary of any sites that appear bogus.

Follow these guidelines for navigating the privacy settings for your account:

Control who can find you: If you don't want everyone (the global public) to be able to find you or contact you, you can limit who can. Options on a few popular social networks include: "Change your profile photo & visibility," "Select who can send you invitations" and "Protect my Tweets."

Control who can view your profile and communications: Your audience—those who can see your profile and communications—can be huge (the public) or very, very small (just yourself), or something in between. To keep some people in and some people out, look for tools in the account settings such as blocking or "unfriending." You may be able to access controls when you post so you can specify a different audience for each individual communication. Even if you fail to make a choice before posting, you should be able to change the audience setting by "editing" existing posts.

Control how much you share with "apps": Apps are software applications and games designed for Web-enabled mobile devices. Many apps depend on the ability to retrieve and share users' personal information, such as contacts, calendars, emails, texts and even location.

Generally speaking, apps can access most of the information in your phone, including your list of contacts and your emails and texts, without your direct permission, but some apps will ask for your consent to access more sensitive information such as your location. To manage the settings for social