A Consumer Action Publication

# What's not to 'Like'?

## Protecting your privacy on social media

**YouTube, Instagram, Facebook, Twitter—these and other social media names are instantly recognizable to most "connected" consumers. In fact, using social media is one of the favorite pastimes of teens and adults alike.**

Sharing can be fun and rewarding, but there can be consequences if you aren't careful about what you reveal and to whom. Fortunately, there are many ways for social media users to limit what they share and protect their personal information. By exercising caution and being proactive, you can enjoy social media while maintaining as much privacy as you want.

## The importance of privacy

People share all sorts of things on social media. Some—say, a video of your pet doing something silly—could be shared with the whole world with no negative consequences. Others, like an announcement that you've won the lottery, can be risky. The first step in protecting yourself is being able to recognize the difference. See if you can recognize the risks in these messages shared openly on social media:

**Sarah, who lives in San Francisco, tweeted from Hawaii that she's having a great time on her weeklong vacation. (When Sarah returned home, she found that someone had broken into her apartment.)**

**Joe, who is hoping for a job promotion, posted a complaint about his employer—"The company I work for treats its employees like slaves!" (Joe's boss saw his post on a coworker's Facebook page—it doesn't look like there's a promotion in Joe's future.)**

**Ricardo loves getting birthday wishes, so he posted the month and date of his big day on his profile, along with the year he graduated from high school ("Class of '82"). (Ricardo became a victim of identity theft. Someone was able to figure out his full birth date and, along with his full name and other information gathered from his posts, used it to access one of his accounts.)**

**Janice, a 17-year-old high school senior who has just sent out her college applications, "Instagrammed" a photo of herself drinking beer at a friend's party. (Janice's top choice of schools checks applicants' social media activity and rejects students who engage in questionable behavior such as underage drinking.)**

**There's nothing wrong with sharing photos and videos, staying in touch with friends and family or promoting ideas or projects, but you have to first consider how any information you reveal could be used—particularly if it were to be seen by an unintended audience.**

## Choosing your audience

When you open a social media account, you typically have the option to change the preset (default) audience setting to match your preferences. In some cases, you can also adjust the setting for each individual item you post or share. Before you begin sharing, learn about the particular social network's privacy options and adjust them as needed.

While these settings can be very effective, do not allow them to give you a false sense of security. Just because you have limited your audience, it doesn't mean that something you share could not be seen by others. For example, you have no control over who sees the posts you add to others' profiles, and you cannot prevent others from copying and distributing something you've shared with them. It may also be possible to find your images, account profiles and content simply by searching for your name in an Internet search engine.

For this reason, it's always better to exercise *more* caution than less. Before you share anything, think about everyone who could potentially see it—employer, client, coworker, teacher, government agency, landlord, insurance company, grandparent—now or in the future.

Regardless of how limited your audience is, ***never*** share these things:

- Social Security number
- Mother's maiden name, full birth date (month, day and year) or other information that is routinely used to verify identity
- Personal address or phone number
- Your current (real-time) whereabouts or any other information that could be used to trace you
- Any information that reveals when your home is unoccupied or when you or your children are there alone

## Privacy dos and don'ts

**There are other important ways—in addition to limiting your audience—to protect yourself and your privacy online.**

**Here are 16 effective dos and don'ts:**

**Don't** feel like you have to fill in every field when creating your profile—it's all optional.

**Don't** accept requests or invitations from people you don't know in an attempt to rack up "friends" or "followers." And don't respond to messages from strangers.

**Don't** post information or photos—your new sports car, the interior of your home, etc.—or share travel plans that might make you more attractive to scam artists or thieves.

**Don't** respond to quizzes, games, coupon offers or other enticements that require you to enter personal information. Doing so opens you up to nuisance marketing efforts and even scams.

**Don't** click on unknown links, which could be

designed to infect your computer with a virus or data-stealing spyware.

**Do** set your computer and mobile devices to require a login password or PIN to start up or wake up.

**Do** create strong account passwords (a mix of at least eight numbers, letters and symbols) and change them regularly. Don't use the same password for all your accounts, or use your pet's or child's name if you share those details on social media. When given the option to choose security questions, do choose ones that nobody else is likely to know the answers to.

**Do** be sure to log out if you use a public computer to access your accounts. It's a good idea to log out even on your own personal computer and devices.

**Don't** let your browser save login information if prompted with that option, or check/uncheck the appropriate boxes in the Security, Passwords, Sync or AutoFill tabs of the browser's Settings or Preferences.

**Do** enable and update your security software (encryption, firewalls, antivirus/antispyware programs, etc.).

**Do** check the company's privacy policy before opening an account to find out how your personal information and/or the data on your device could be used.

**Don't** download an app unless it comes from a trusted source and you have checked user reviews and read the privacy policy.

**Do** read all notices from your social networks and

## Personalizing your privacy settings

Log in to your account and look for a section titled Privacy, Settings or Preferences, or use the Help feature to find and understand the network's features and tools. If you still need help, contact the social network's support staff via a link from the site or app, ask a question in the "Community" or "Forum" area, or do a web search of your question (example: "How do I use the privacy settings in [name of social network]?").

From here, you can adjust your settings to limit who can view your profile, contact you or see what you've shared. If necessary, take advantage of options to change the audience for each individual item you share, and block or "unfriend" someone to control your exposure. (Be aware that even if you have the option to go back and change the audience for an existing post or remove it entirely, it may be too late to keep it private.)

When in doubt, don't share!

## Controlling your apps

Generally speaking, apps—downloadable software that enhances the functionality of your smartphone or tablet—can access most of the information on your device, including contacts and messages. Some, but not all, apps will ask for your permission to access this information and/or your location.

To manage the settings for social media apps, look for Apps, Data Sharing or something similar in the social media website's Preferences, Settings or Help section. Then adjust the settings to match your comfort level. To control what an app collects and shares outside of social media, check the settings in the app itself. Read the app's privacy and data use policy, and then decide whether you are comfortable with it or need to uninstall the app and find a different one.

apps so that you don't miss any policy changes. If you're unhappy with a change, cancel your account and/or uninstall the app.

**Don't** allow apps to announce your location.

**Do** talk to your kids about how to be safe and responsible online (including warning about "sexting"), and do set strong privacy preferences on their accounts, take advantage of "parental controls" and routinely monitor your child's communications.

**Do** comply with your employer's social media policy, if it has one.

## About Consumer Action

*www.consumer-action.org*

Through multilingual consumer education materials, community outreach and issue-focused advocacy, Consumer Action empowers underrepresented consumers nationwide to assert their rights and financially prosper.

**Consumer advice and assistance:** Submit consumer complaints to: *www.consumer-action.org/hotline/complaint_form/* or 415-777-9635. Chinese, English and Spanish spoken

## Resources

Visit these links to learn more about how to protect your privacy and stay safe online:

StaySafeOnline.com [*https://www.staysafeonline.org*]

Privacy Rights Clearinghouse (social networking privacy) [*https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social*]

Google Safety Center [*https://www.google.com/safetycenter/*]

Online Safety Institute (good digital parenting) [*https://www.fosi.org/good-digital-parenting/*]

OnGuardOnline.gov (protect kids online) [*http://www.onguardonline.gov/topics/protecting-kids-online*]

Common Sense Media (responsible social media for youth) [*http://www.commonsensemedia.org/blog/talking-about-sexting*]

TRUSTe (privacy tips) [*https://www.truste.com/consumer-resources/personal-privacy-tips/*]

How to read a privacy policy [*http://oag.ca.gov/privacy/facts/online-privacy/privacy-policy*]

CNET (protecting your online reputation) [*http://www.cnet.com/how-to/how-to-manage-your-online-reputation-for-free/*]

CTIA-The Wireless Association (mobile device safety) [*http://www.ctia.org/your-wireless-life/consumer-tips/tips/how-to-erase-data-on-your-mobile-device*]

AARP (cyberproofing your phone) [*http://www.aarp.org/home-family/personal-technology/info-2014/cyberproof-stolen-phone-kirchheimer.html*]

Federal Trade Commission (FTC) (using public Wi-Fi safely) [*http://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks#Mobile*]

Apple (Mac) [*http://www.apple.com/support/osx/passwords/*] or PC [*http://pcsupport.about.com/od/tipstricks/ht/newxppassword.htm*] (how to set your system to require a login password or PIN to start or wake up)

ConnectSafely (creating strong passwords) [*http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/*]

PasswordsGenerator.net [*http://www.passwordsgenerator.net*]

PCMag.com ("best" free password managers) [*http://www.pcmag.com/article2/0,2817,2475964,00.asp*]

## About this guide

Consumer Action created this guide with a grant from the Rose Foundation.