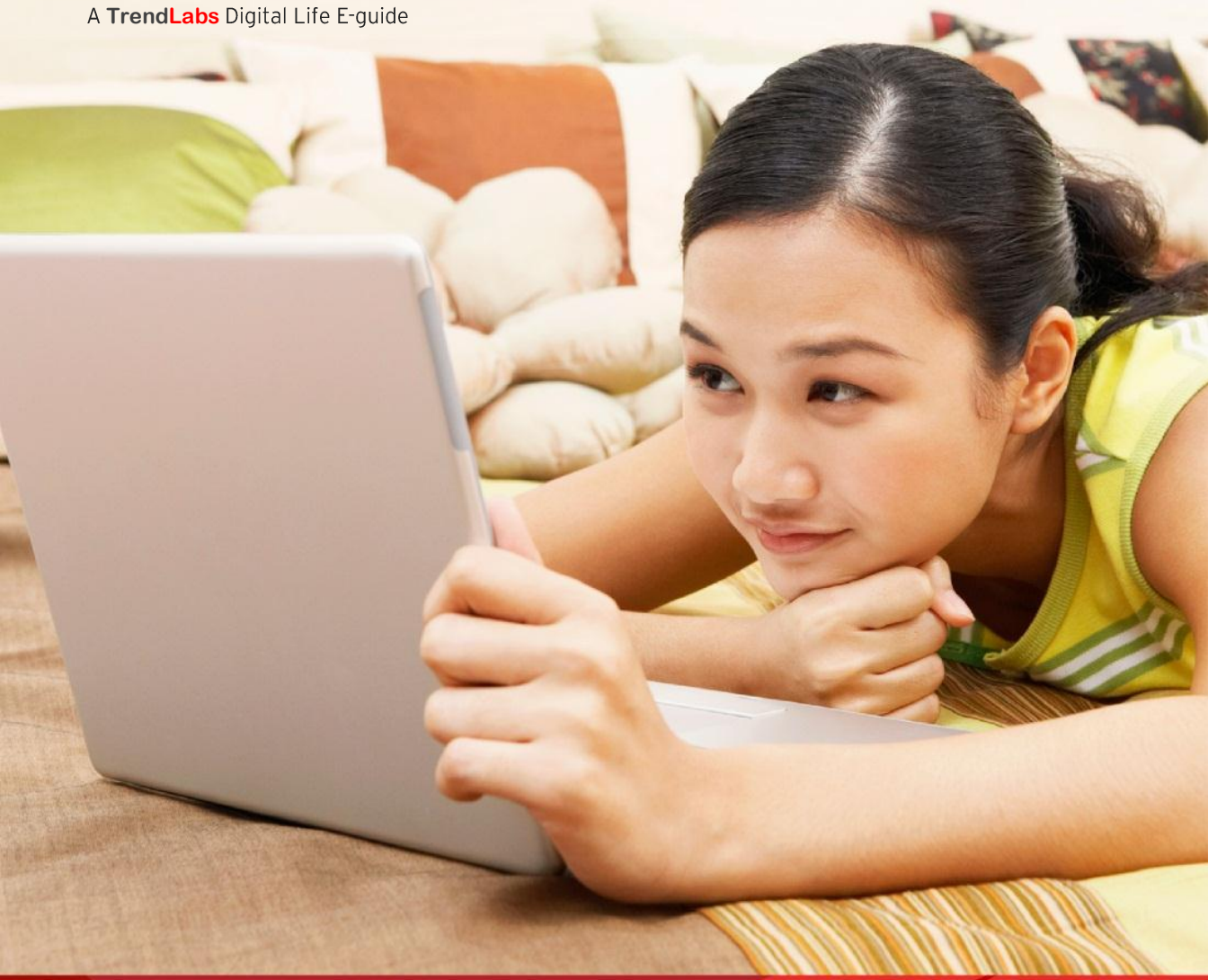
TREND MICRO™

Enjoy your digital life safely

How to Protect Your Privacy on Social Media

A **TrendLabs** Digital Life E-guide



How do you keep information private on social networking sites? According to a Trend Micro survey, only 38% know how to limit what they post online. This low figure shows that many users might be sharing more information than they originally intended.

Oversharing online might do damage to your reputation. For example, your family or employers might spot carelessly posted photos of yourself in compromising situations. Your details can also be used for identity theft, if cybercriminals utilize them to impersonate you. Identity theft has become so rampant that there was one identity fraud victim every three seconds in the US last year.

Relying on a site's privacy settings is just the start. While stricter account settings and tools can help you maintain privacy, there are other ways your personal information can leak out to the public. Knowing and addressing these potential privacy risks will help you protect your data.

Delivered Daily

Third-party apps, like horoscope or IQ test apps, may work on social networks but are not necessarily created by them. These apps often ask you for access to your information so they can personalize your user experience. If you're concerned about the amount of information an app is asking for, it may be best not to install it at all.

Social networking sites also have ads that appear as sponsored posts. Companies create deals with social networks that allow them to use any brand-related activity on the site, such as liking, as a sponsored post.

Check your app settings to avoid sharing too much information:

Facebook Control the visibility of app activities on your timeline and feed via the Apps section of your Privacy Settings. Also remove or manage the settings of each individual app. While you can't opt out of sponsored posts, you can adjust the privacy settings of these ads.

Google+ Manage app visibility or delete apps through the Apps and Activities section.

Twitter Revoke third-party apps from accessing your Twitter account through the Apps section.

The Fine Print

Privacy policies give you an idea of how much privacy social networks grant. You can find out: what they collect, how they collect information, who has access to that information, what in-place security measures they have, how long they will store your information, and how you can contact them, if you have any privacy concerns.

Most sites keep their privacy policies in locations that are easy to find. It's important to keep track of them because they can change anytime. You can also use a privacy scanner to quickly identity privacy settings that may leave your personal information vulnerable to identity theft, without having to read the fine print.

Check privacy policies and adjust settings to your comfort level::

Facebook Check the Facebook Data Use page to see how you can avoid divulging your Personally Identifiable Information (PII).

Google+ The site doesn't allow you to opt out of disclosing your PII. Read the Google+ Policies and Principles page and the Google Privacy Policy page.

Twitter See how you can withhold your PII on the Twitter Privacy Policy page.

NOTE: Law enforcement agencies can have full disclosure of your PII.

Tag, You're It

Getting tagged in a post might seem harmless, but it can also decrease your privacy. Your contacts will be able to see if you're tagged in a post or photo, even if they aren't connected to the original source. This can also be harmful to your reputation if you're tagged in an unflattering or sensitive photo or post.

Your location can also be revealed to contacts if a friend decides to tag where you are, allowing anyone to physically follow you. Removing tags or mentions may be difficult because some social networks do not have options to do so. Privacy scanners can help keep track of all your tags.

Keep tabs on all your tags and mentions:

Facebook Review tagged posts and photos before they're added to your timeline. You can also manually remove tags.

Google+ Approve or remove tags on images, or select a setting that automatically approves of tags from specific contacts.

Twitter Your contacts can automatically include your username in mentions and replies. But the visibility of these tweets varies, depending on your contacts' privacy settings. Setting accounts to "private" means that non-approved accounts will not be able to see or reply to tweets.

Friendly Sharing

Given how social networks work, your friends' privacy settings have a direct impact on your privacy. If your friends have less restrictive settings, it's possible for a wider audience to see your posts.

People can still share the information you post, even with strong privacy settings in place. Some social networks allow your contacts to copy and republish your original posts. Strangers can also see your private posts if a friend of yours tags them in. Remember that everything remains online and only post updates or photos you won't mind sharing with strangers.

Make sure your posts are only seen by your intended audience:

Facebook The existence of the "Friends of Friends" category means that the viewership of your posts and images extends to people you might not know.

Google+ You can share the list of people in your circles to the public, exposing those accounts to a larger audience.

Twitter Your account can be included in a Twitter list that can be shared publicly. Users will still need your approval to follow your account if it's set to private.

‘Til Deactivation Do Us Part

Some sites differentiate between account deactivation and deletion, so you could end up not erasing your account completely. If you have multiple accounts on the same site, you need to delete each one separately.

Deactivating or deleting your account doesn’t guarantee that all traces of it are permanently erased. Some of your cached profiles or posts might still appear on search engines. Your information could also remain stored in the site’s servers or databases.

Find out the steps to deleting or deactivating your accounts:

Facebook Deactivate or delete your account. Deactivation allows you to reactivate your account in the future. Permanently deleting your account removes all your personal information, except for your sent messages.

Google+ Deleting your Google+ account is more complicated since it’s connected to your other Google accounts. Account deletion removes all your contacts, comments, and posts.

Twitter Twitter waits 30 days before permanently deactivating your account. Even though your account has been deactivated, content might still be available on the site for a few days.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit www.trendmicro.com.

TREND MICRO™

Enjoy your digital life safely

Created by:
TrendLabs, The Global Technical Support & R&D Center of TREND MICRO