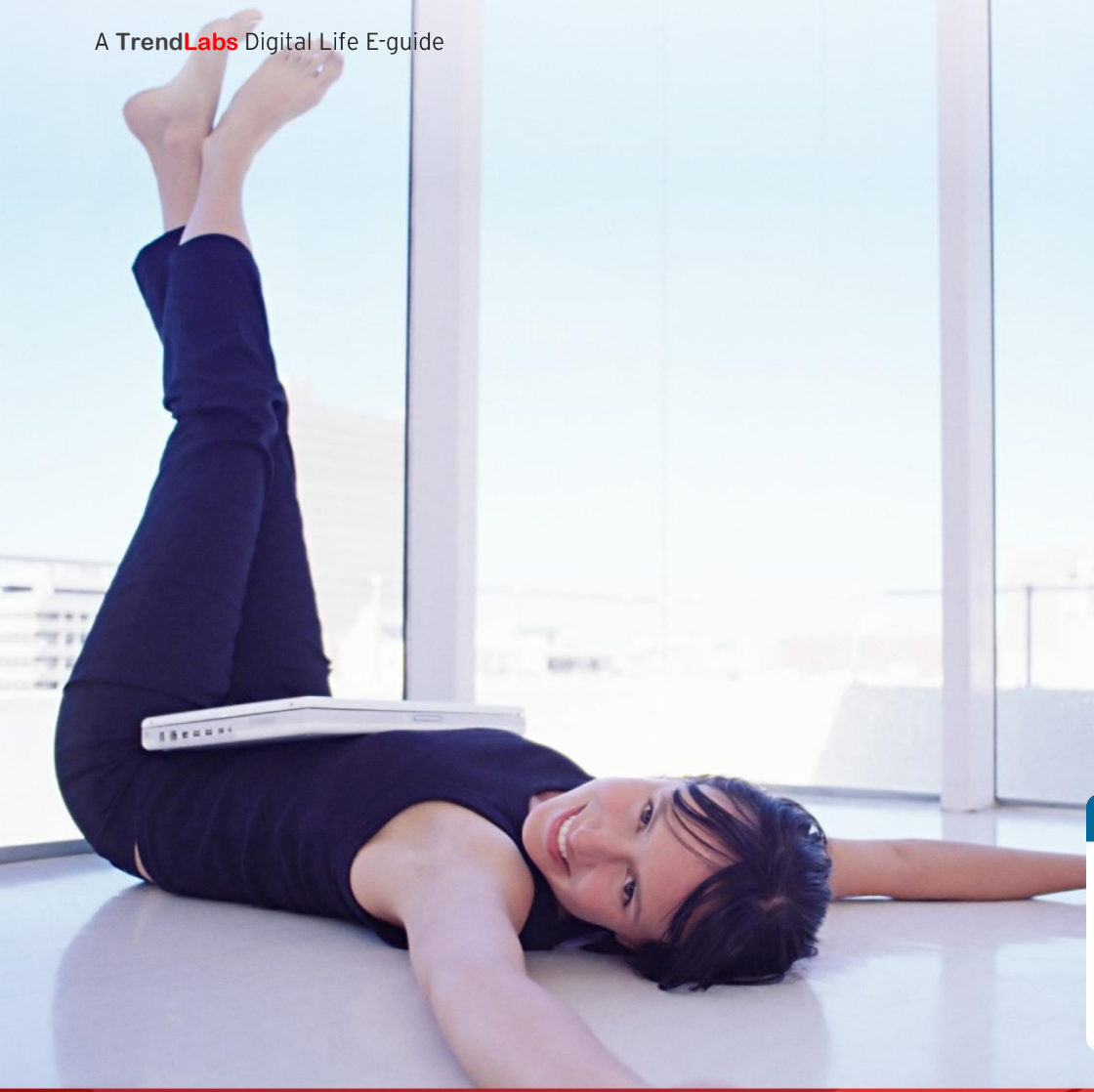
How to Manage Your Privacy Online

A **TrendLabs** Digital Life E-guide



Distributed by:

When you go shopping or banking online, you probably take great pains to make sure sensitive information (like your credit card details) remain private. But what about other details, like your daily plans or browsing habits?

When your private information goes public, malicious activities or bad guys aren't always behind it. You may not be aware that there are other ways for your information to go public.

What is Privacy for You?

There is no “one-size-fits-all” definition for privacy. Of course, there are things that everyone will agree on. For example, everyone will agree that seeing your credit card information go public is not a good thing. The same could probably be said for a home address.

But what about your favorite shoe brand? Or the last item you searched online? While some people might be squeamish about sharing with an advertising company the details of the last item they purchased, others wouldn’t even bat an eye.

It’s important to be aware of the different ways your private online information can be shared with others. That way, you can assess and decide on how much you are willing to share and adjust it accordingly.

Online Activity Tracked by Ad Networks

Have you ever seen an online ad with a product or brand that you searched *just* ten minutes ago? That's the result of customized advertising.

Online advertising or ad networks act as bridges between advertisers and the owners of the sites they wish their ads to appear in. These networks use a central server to deliver the right ads to the right site visitors and to monitor users across their entire network.

In order to deliver the ads, ad networks may allow third-party companies to observe users' online activities via their browsing history. Although matching users to online ads that may pique their interest may not be a problem to some, others may take this as a violation of privacy. What most sellers find convenient and useful may be construed as an invasion of privacy by the people they watch.

Keeping Your Browsing History Private

To protect your privacy, keep the following tips in mind:

• Regularly delete cookies. Cookies store site-related information that may be stolen for cybercriminal use. Take note that doing so will require you to reenter your user name and password every time you access a site.

• Consider private browsing. Opting for private browsing opens a new browser session that deletes its history and cookies as soon as you close the window. However, this doesn't guarantee anonymity while your browser window remains open, allowing advertisers to still track you down.

• Use the NAI's opt-out tool. This tool allows you to opt out of being "targeted" by customized ads. As an organization that promotes online advertising self-regulation, the Network Advertising Initiative (NAI) allows you to opt out of advertising promotions run by its member companies. As such, you will no longer be bothered by tailor-made ads from companies you choose to block.

Oversharing on Social Media

While ad networks have to guess what you're interested in based on your web preferences and usage patterns, social media sites have all the information they need as long as you feed it to them. Thanks to social media integration in multiple sites, social networking sites have easy access to your likes and dislikes.

Sharing anything and everything online can have a downside. Social media "mining" is becoming a standard industry practice, especially among insurance and human resource (HR) companies. People are combing through social media accounts for employment and legal purposes. So while that cheeky Facebook post might seem hilarious to your friends, your employer might see it differently.

Bad guys can also use social media mining to find out details about you. Once they do, they can use that information to hack accounts or perform identity theft.

Resetting Your Social Media Accounts

Consider what the Miranda Rights says—"What you say can and will be held against you"— and remember that it's best to think very carefully before you post anything online. Avoid sharing too much, especially if you haven't figured out how to fully configure your chosen social networking site's privacy settings yet.

You should also take note that configuring your social media accounts isn't a one-time event. Social networking sites are constantly adjusting and tweaking features and settings—including those for privacy.

You can use the digital life e-guide "How to Protect Your Privacy on Social Media" as a starting point for securing your accounts.

Information Tracked/Leaked By Apps

Mobile apps have become an indispensable part of everyday life, thanks largely to smartphone use. Unfortunately, apps have also become one way for your private data to go public.

Malicious apps created by cybercriminals can steal information stored on your mobile devices. The stolen information may then be sold in the criminal underground market or used for malicious schemes.

Meanwhile, many legitimate apps are powered by ads, meaning these are subject to the same privacy issues related to ad networks. Some apps even require information prior to installation such as your location and personal details such as age and sex. This information is then sent to their developers and third-party companies such as ad networks and marketers

Protecting Your Mobile Devices

You can secure your mobile device (and its data) by following some key safety habits:

- Scrutinize apps before downloading them. Bad guys are fond of mimicking legitimate apps to trick users into downloading malicious copycats.
- Check the permissions for each app. Permissions can be a good indicator if an app is requesting for more access than it requires.
- Install a security app that scans for malicious activity in your device. A security app that can also scan for potential privacy issues is even better.

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.

Enjoy your digital life safely

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