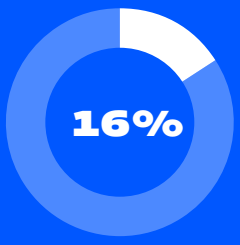
TAKE BACK CONTROL OF YOUR PERSONAL DATA

8 STEPS TO BETTER PROTECT YOUR PRIVACY ONLINE

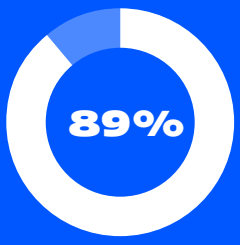
Americans have awakened to the reality that many of the apps on our devices are collecting substantial amounts of data about us every day, from the mundane to the highly sensitive.For some apps, data collection is just the first step in the process of commodifying that personal data—all out of sight from the consumer, who may believe the only thing that's going on is that she/he is playing a cool free game on their phone or tablet.

Data privacy is a fundamental right and one principle that flows from this is that consumers should be able to easily control the flow of their data through the digital ecosystem. For that right to have meaning, consumers must be able to understand the data flows and business models of any application or service they use and be able to make informed decisions about the collection, transfer, and use of their data. This means that service providers must explain in simple terms if and how data is going to be collected and used, and users should be given simple ways to control that data flow and use.

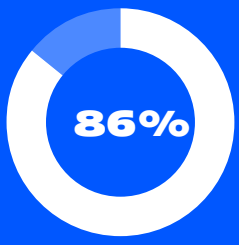
A consumer should not have to be a Chief Information Security Officer in order to manage their privacy. Unfortunately, according to a recent consumer survey commissioned by Trusted Future and conducted by the research firm AudienceNet, few Americans feel equipped to do so. Much work needs to be done, but as we drive to this more Trusted Future, there are actions that consumers can take today to better protect their privacy, and exercise additional control over their data.



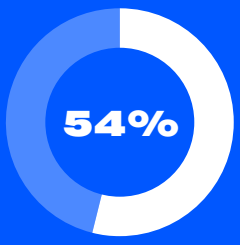
Felt very in control of their personal data.



Expressed concern about their data being shared with third parties.



Expressed concern about apps tracking their behavior across other apps, websites, and devices.



Have chosen not use use an app or program because of privacy concerns.

01

KEEP YOUR DEVICES SECURE BY PRACTICING GOOD CYBER HYGIENE. Taking steps to secure your device from hackers and fraudsters, is a base essential. If you are not secure, your data can be stolen, your devices tracked or features can be activated without your knowledge—all of which can undermine your privacy. For advice on how to keep your devices and accounts secure, review our **Nine Essential Steps to Keep Your Device Secure.**

02

PREVENT UNAUTHORIZED USERS FROM ACCESSING THE INFORMATION ON YOUR DEVICE IF IT IS LOST OR STOLEN.

Configure your device to require authentication before someone can access the device and its contents by using passcodes, strong passwords, face or fingerprint ID, or a physical dongle. Further protect your information from prying eyes if your device is lost or stolen by ensuring your device encrypts your data automatically and gives you the ability to remotely 'wipe' your device clean. By using all of these practices, you can reduce the risk that somebody will be able to access your data in a usable form if your device is lost or stolen.

03

UNDERSTAND HOW YOUR DATA WILL BE USED AND HANDLED BEFORE YOU "CLICK YES" OR "DOWNLOAD."

Before you download an app, review the privacy label for the app in the app store to be able to quickly see and compare what data it collects, and for what purposes. Alternatively, you can review the app's privacy policy. If it collects extraneous information unrelated to the purpose of the app, or if it is too vague about what data it collects, you can choose to use a different app. In addition, pay close attention to the permissions and app requests before granting an app permission to access certain data or functions (such as location, camera, microphone). Get comfortable saying "no" if a permission request seems unnecessarily invasive or just doesn't make sense.

04

BE CAREFUL WITH UNSOLICITED LINKS AND ONLY OBTAIN APPS FROM OFFICIAL APP STORES.

Cybercriminals have become more sophisticated about the use of social engineering to manipulate consumers into clicking on dangerous links via emails or text messages, some of which prompt users to download a malicious app containing malware. Devices that have been configured to "sideload" apps from unofficial app stores and third-party websites are much more vulnerable to "smishing" (use of SMS messaging as the vector to get you to download a malicious app) or other social engineering tricks (like web pages 'offering' free cool apps that, once downloaded, facilitate third party control of your device, its functions, and access to your data). Protect your device by only downloading apps from official app stores, such as Android's Google Play and Apple's App Store, which invest considerable resources into vetting apps.

05

CONDUCT A REGULAR "PRIVACY AUDIT" OF YOUR SOCIAL MEDIA ACCOUNTS, APPS, AND OTHER ACCOUNTS.

Periodically, reassess your existing data permissions and delete apps if you no longer use them. Do you still need that game you haven't played in months? Does it still make sense to let an app track your location "in the background"?

06

LIMIT THE INFORMATION YOU SHARE WITH THE WORLD.

In addition to being cautious about what data you share with apps, experts also advise that consumers should avoid "oversharing" on social media and adjust privacy settings to limit who can view your social media posts. Cybercriminals or other bad actors can use the information you share online to piece together details about your life, which can make it possible for them to answer security questions necessary to access your financial and other accounts (e.g. sharing about your upcoming high school reunion allows cybercriminals to identify your high school mascot).

07

TAKE STEPS TO BROWSE WITH MORE PRIVACY AND MORE SECURELY.

A billion-dollar industry has emerged in recent years centered on the collection and monetization of your browsing habits. Advertisers can sometimes use something called "third-party cookies" to learn about your interests as you visit different websites and then serve you targeted ads based on your browsing history. In addition to advertisers, bad actors can try to monitor your web activity to obtain passwords and account information. There are several ways to browse the Internet more anonymously:

- **Be aware of online tracking and what you can do to prevent it in web browsers and mobile phones.** Your browser settings can allow you to decide what type of cookies you want to allow. You can also turn on "private browsing" to reduce tracking. Similarly, some mobile phones now have settings that require an app developer to ask for your permission before they track your activity across apps and websites – limiting the data collected about you.

- **Choose browsers and search engines that limit tracking and data collection.** There are important differences between different browsers and search engines—while some are known to extensively track your browsing history, others limit the data that can be collected about users and block website ad trackers.

- **Avoid unsecured webpages.** Only visit websites that use HTTPS (check the beginning of the website's URL) to protect your browsing from prying eyes. Some leading browsers will also warn users when they are visiting websites that aren't secure.

08

ASK YOURSELF – "DO I TRUST THIS APP, DEVICE, OR COMPANY?"

Fundamentally, the biggest question to ask is whether you trust an app, site, device, or service and the company that is selling or running it. If you would not trust them to manage your private information or access to you, be hesitant, do research, and then make an informed decision.

"The Federal government needs the partnership of every American and every American company in these efforts. We must lock our digital doors — by encrypting our data and using multifactor authentication, for example—and we must build technology securely by design, enabling consumers to understand the risks in the technologies they buy."

PRESIDENT JOE BIDEN

TRUSTED RESOURCES FOR FURTHER READING

MAINTAINING PRIVACY ON YOUR DEVICE

Federal Trade Comission, *How to Protect your Phone and the Data on It* →

Cybersecurity & Infrastructure Security Agency
A How-To-Guide for Multi-Factor Authentication →
Security Tip: Securing Wireless Networks →

Military OneSource, *Top 4 Tips for Cell Phone Safety* →

Australia's eSafety Commissioner
Safe passwords →
Managing passwords →

New Zealand's Computer Emergency Response Team, *Using encryption to keep your data safe* →

European Union Agency for Cybersecurity, *What is Privacy and why it is important* →

PROTECTING YOUR PRIVACY WHEN USING APPS

Federal Trade Commission, *Tips to Protect Your Privacy on Apps* →

Cybersecurity & Infrastructure Security Agency, *Security Tip: Privacy and Mobile Device Apps* →

Australia's eSafety Commissioner, *Being safer with apps* →

PROTECTING YOUR PRIVACY ONLINE

Cybersecurity & Infrastructure Security Agency
- *Security Tip: Avoid Social Engineering and Phishing Attacks* →
- *Stop Ransomware* →

Federal Trade Commission, *How to Recognize and avoid phishing scams* →

Australia's eSafety Commissioner
- *Protecting your privacy online* →
- *Australia's eSafety Commissioner, Avoiding scams and tricks* →

Canadian Centre for Cyber Security, *Staying Cyber-Healthy During COVID-19* →

European Union Agency for Law Enforcement Cooperation (Europol)
- *Your life is online. Protect it!* →
- *Tips & Advice to Prevent Identity Theft Happening To You* →
- *Tips and advice to prevent identity theft happening to you* →

National Cybersecurity Alliance, *7 Tips to Manage Your Identity and Protect Your Privacy Online* →

USEFUL CYBER SAFETY TIPS

The New York Times, *How to Protect your Digital Privacy* →

CNET: *7 data privacy tips for your phone from digital security experts* →

National Network to End Domestic Violence: *Best Practices When Using Mobile Devices* →

Norton: *Good cyber hygiene habits to help stay safe online* →

TRUSTED FUTURE

TRUSTEDFUTURE.ORG