Project Upskill II

Unseen Access

How Cybercriminals Intrude on Your Devices

and How to Stop Them

Al Williams

December 10, 2025

Why Project Upskill?

The Cybersecurity & Infrastructure Security Agency (CISA) collaborated with other US and International partners to create Project Upskill, cybersecurity guidance for high-risk communities.

Project Upskill provides users with simple steps to improve their cybersecurity.

Why Project Upskill?

While none of these steps will offer complete protection against cyber intrusions, this combination of best practices will make it harder to target high-risk individuals and organizations.

They will also limit opportunities for attackers that leverage common techniques such as ransomware or malware.

Why Project Upskill II?

Anyone over 55 who uses a computing device (iPhone, laptop, etc.) is at higher-risk due to data breaches revealing our ages.

The Willow Valley Computer Club's Project Upskill II extends CISA's Project Upskill to include illustrations, examples, additional material, suggestions, and recommendations.

After completing Project Upskill II, you should feel more confident that you can implement basic cybersecurity practices.

Our Recommendations

We all have personal threat models – lists of events we want to prevent or defend against, and a list of decisions of what to do if an event occurs.

None of us can physically see the threats to our computing devices and our personal information. We need advice.

CISA’s Project Upskill provides guidance but does not recommend any software or hardware.

Our Recommendations

The Computer Club makes recommendations for software apps and computing devices based on cybersecurity best practices.

Our recommendations are not requirements that you must follow.

Where we’ve been and where we’re going in the Project Upskill II series.

Goal for Presentation 1

We often focus on the visible risks to our data, like device security. However, hidden risks, such as overlooked privacy policies, can be just as damaging. Our first presentation shed light on this crucial area with suggested solutions.

Goals for Presentations 2, 3, and 4

To ensure the security of your personal data on your computing devices, we provided a layered security approach including:

implementing basic cybersecurity,
preventing account breaches, and
ensuring the protection of your stored data.

Goals for Presentations 5, 6, 7, and 8

To ensure the security of your personal data that isn’t on your computing devices, we provide ways to

protect your data in transit,
secure your home Wi-Fi,
manage your privacy and security online, and
use Virtual Private Networks (VPNs) appropriately.

Managing Your Privacy & Security Online – Presentation 7

Phones, laptops, smartwatches, and other mobile devices collect a staggering amount of information about their users.

While this information can be used to enhance products and services, and the sale of information can even allow companies to offer many apps for “free”, threat actors can also exploit these troves of information.

Source: Managing Your Privacy and Security Online, https://www.cisa.gov/audiences/high-risk-communities/projectupskill/module6, Retrieved April 19, 2025

Managing Your Privacy & Security Online – Road Map

Manage your online presence by understanding privacy policies

Limit your digital footprint to reduce the likelihood of a successful attack

Follow cybersecurity best practices to protect yourself from tracking

Source: Managing Your Privacy and Security Online, https://www.cisa.gov/audiences/high-risk-communities/projectupskill/module6, Retrieved April 19, 2025

Privacy Policies

We focused on privacy policies in the first presentation. The next few slides highlight that presentation.

When you agree to a privacy policy, you are agreeing that the organization may collect any information they list in the policy.

Google’s Privacy Policy

Google’s Privacy Policy

“The activity information we may collect include:

Terms you search for

Videos you watch

Views and interactions with content and ads

Voice and audio information

Purchase activity

People with whom you communicate or share content

Activity on third-party sites and apps that use our services”

Source: https://policies.google.com/privacy#infocollet Effective July 1, 2023

Google’s Privacy Policy

“We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.”

Source: https://policies.google.com/privacy#infocollect   Effective July 1, 2023

Google’s Privacy Policy

> “If you use our services to make and receive calls or send and receive messages, we may collect call and message log information like your phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages.”

Source: https://policies.google.com/privacy#infocollect Effective July 1, 2023

Google’s Privacy Policy

“We collect information about your location when you use our services, which helps us offer features like driving directions, search results for things near you, and ads based on your general location.”

Source: https://policies.google.com/privacy#infocollect Effective July 1, 2023

WhatsApp’s Privacy Policy

WhatsApp’s Privacy Policy

> “We collect device and connection-specific information when you install, access, or use our Services. This includes information such as hardware model, operating system information, battery level, signal strength, app version, browser information, mobile network, connection information (including phone number, mobile operator or ISP), language and time zone, IP address, device operations information, and identifiers…”

Source: https://www.whatsapp.com/legal/privacy-policy

WhatsApp Privacy Policy

> “We collect and use precise location information from your device with your permission when you choose to use location-related features… Even if you do not use our location-related features, we use IP addresses and other information like phone number area codes to estimate your general location (e.g., city and country).”

Source: https://www.whatsapp.com/legal/privacy-policy

Privacy Policies – How To Minimize Impact

Do not agree to objectionable privacy policies – don’t use the app or service

Do not install apps unless you definitely need them

Do remove apps that are no longer used

Do turn off location services for any app unless the service is needed

Managing Your Privacy & Security Online – Road Map

Limit your digital footprint to reduce the likelihood of a successful attack

Manage your online presence

Follow cybersecurity best practices to protect yourself from tracking

Source: Managing Your Privacy and Security Online, https://www.cisa.gov/audiences/high-risk-communities/projectupskill/module6, Retrieved April 19, 2025

Limit Your Digital Footprint – Advertising IDs

Your digital footprint is revealed using various technologies as well as privacy policies:

- Advertising IDs
- location data

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

Advertising IDs (Ad IDs)

Ad IDs play a central role in aggregating information about individuals.

In the USA, Ad IDs are 11-digit codes assigned to computing devices by Apple, Google, or Microsoft.

Ad IDs enable near-real-time location tracking.

Websites collect location data, and other identifying information, and broadcast that information to hundreds of ad networks that may wish to bid on showing their ad to a particular user.

Source: *The Global Surveillance Free-for-All in Mobile Ad Data*, https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data, Retrieved April 13, 2025

How Can the Ad ID Data be Used?

Data brokers compile the data into detailed user profiles.

The profiles can be used to deduce information about your interests, activities, and whereabouts.

Companies can learn about your favorite shopping venues, health status, hobbies, and other personal data – without you directly telling them.

Threat actors can send targeted phishing emails to you.

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

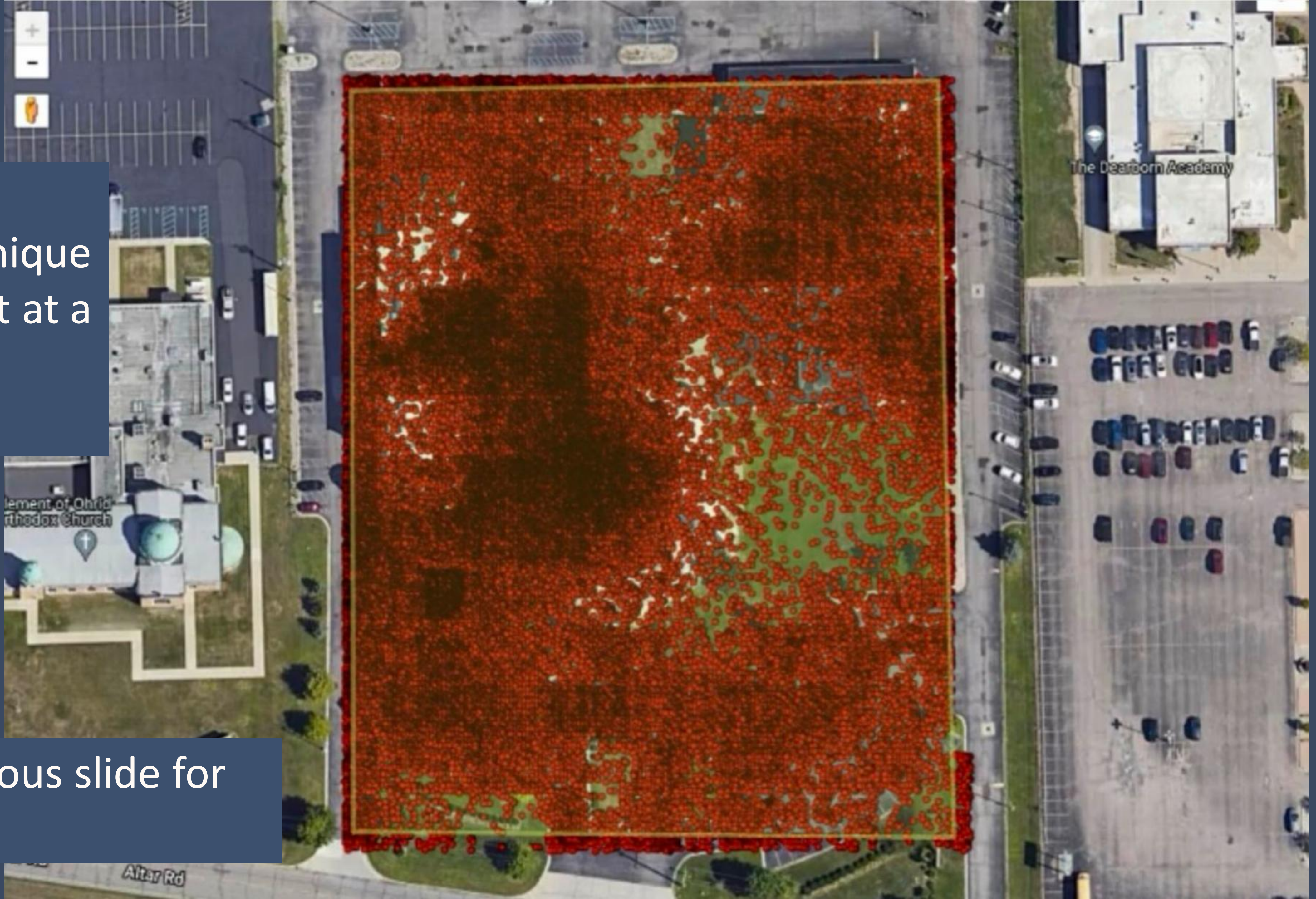
An Example of the Use of Ad IDs

The Global Surveillance Free-for-All in Mobile Ad Data article by Brian Krebs provides an excellent and comprehensive overview of an organization involved in surveillance and technologies being used.

Babel Street collects user information from data brokers and sells access, including people search services. Their LocateX platform allows customers to track individual cell phones using the phone's Mobile Advertising ID (MAID), a unique identifier in all Google Android and Apple mobile devices.

Source: *The Global Surveillance Free-for-All in Mobile Ad Data*, https://krebsonsecurity.com/2024/10/the-global-surveillance-free-for-all-in-mobile-ad-data, Retrieved April 13, 2025

Each red dot indicates a unique MAID present at a mosque in Dearborn, MI



See the previous slide for the source

Disable Your Device’s Ad ID – How-To’s

Windows: *https://support.microsoft.com/en-us/windows/general-privacy-settings-in-windows-7c7f6a09-cebd-5589-c376-7f505e5bf65a*

macOS and iOS:
Block personalized ads and location-based ads:
https://support.apple.com/en-us/HT202074
Manage tracking permissions: *https://support.apple.com/en-us/HT212025*

Android: *https://support.google.com/googleplay/android-developer/answer/6048248?hl=en*

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

Disable Ad ID on Windows – A Walkthrough

Go to *Start* > *Settings* > *Privacy & security* > *General*

Choose your preferred setting for *Let apps show me personalized ads by using my advertising ID.*

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025=

How To Manage Your Ad ID Information

You can request that any of your information, including Ad ID information, be removed from specific organization platforms, including data brokers. Sometimes, the organization may be legally obligated to honor your request.

Some companies and organizations can help you with data broker protection, *but be careful when selecting an organization – many will claim complete removal of your information. But it isn't easy to achieve because newly acquired information is constantly being added to data broker repositories*.

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

Ad IDs – Insight Summary

Most operating systems, including Windows, macOS, iOS, and Android, assign unique Ad IDs to devices to facilitate the collection of user data, including location data, your browser activity, and information your apps collect.

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

Limit Your Digital Footprint – Location Data

Your digital footprint is revealed using various technologies and privacy policies:

Advertising IDs

location data

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

Disable Location Tracking

You can disable location tracking in

- Windows
- iOS
- Android
- macOS

In Linux, each distribution has different approaches to controlling location tracking.

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

Disable Location Tracking

Windows

- You can disable location tracking
  - For all apps
  - For specific apps
- You can use Airplane Mode to temporarily turn on and off location services

Source: *How to Disable Location Tracking in Windows 11*, https://www.howtogeek.com/how-to-disable-location-tracking-on-windows-11/, Retrieved April 21, 2025

Disable Location Tracking

iOS

- You can disable location tracking
  - For specific apps
- You can allow an app to use Precise Location (as opposed to approximate location)
- You can use Airplane Mode to prevent your iPhone or apps from sharing the phone’s location

Source: *Turn Location Services and GPS on or off on your iPhone, iPad, or iPod touch*, https://support.apple.com/en-us/102647, Retrieved April 21, 2025

Disable Location Tracking

Android

Multiple options exist for controlling the phone’s location settings, as Google’s support documents describe.

Source: *Manage your Android device’s location settings*, https://support.google.com/android/answer/3467281?hl=en-419, Retrieved April 21, 2025

Source: *Manage location permissions for apps*, https://support.google.com/android/answer/6179507?hl=en-en, Retrieved April 21, 2025

Disable Location Tracking

macOS

- You can
  - Turn off Location Services
  - Specify which apps and system services can use Location Services

Source: *Control access to the location of your Mac*, https://support.apple.com/guide/mac-help/allow-apps-to-see-the-location-of-your-mac-mh35873/mac, Retrieved April 21, 2025

Disable Location Tracking

Linux

Each Linux distribution offers its specific capabilities and may not provide the ability to disable location tracking.

Limit Your Digital Footprint - Summary

Your digital footprint is revealed using various technologies and privacy policies:

Ad IDs

location data

Source: *Limit Your Digital Footprint*, https://www.cisa.gov/resources-tools/training/limiti-your-digital-footprint, Retrieved April 7, 2025

Managing Your Privacy & Security Online

Limit your digital footprint

Mange your online presence

Follow cybersecurity best practices to protect yourself from tracking

Source: Managing Your Privacy and Security Online, https://www.cisa.gov/audiences/high-risk-communities/projectupskill/module6, Retrieved April 19, 2025

Manage Your Online Presence

Threat actors target everyday citizens as well as those at higher risk using social engineering to achieve:

identity theft
account takeovers
doxxing (exposing private information on the Internet
installation of malware
unauthorized access to devices and data

Manage your social media accounts to minimize the likelihood of loss

Source: *Manage Your Online Presence*, https://www.cisa.gov/resources-tools/training/manage-your-online-presence, Retrieved April 19, 2025

Manage Your Social Media Accounts

Your social media usage can provide theat actors with enough context to create compelling spear-phising messages:

Interests
Photos – self posted and tagged
Relations – personal and professional
Hobbies
Online quizzes and games
Travel plans

Source: *Manage Your Online Presence*, https://www.cisa.gov/resources-tools/training/manage-your-online-presence, Retrieved April 19, 2025

Manage Your Social Media Accounts

Manage your social media accounts by being mindful of the information you're posting online

Fitness apps reveal not only fitness activity but also locations of your activity

Source: *Manage Your Online Presence*, https://www.cisa.gov/resources-tools/training/manage-your-online-presence, Retrieved April 19, 2025

Best Practices for Your Social Media Accounts

Make your social media account private

Do not make your birthdate, location, or other personal details available on your profile

Disable location sharing and do not use geo-location tags

Disable “tagging” settings or enable controls to approve or deny tags before a post is associated with your account

Source: *Manage Your Online Presence*, https://www.cisa.gov/resources-tools/training/manage-your-online-presence, Retrieved April 19, 2025

Best Practices for Your Social Media Accounts

Only add friends, followers, connections or contacts that you know and trust. Verify that the account actually belongs to the person you know and is not a false account that was created to gain closer access to you.

Vet any third-party app integrations to ensure they meet your cybersecurity requirements

Adjust settings for personalized ads to limit what information third parties receive about your account activity

Source: *Manage Your Online Presence*, https://www.cisa.gov/resources-tools/training/manage-your-online-presence, Retrieved April 19, 2025

USSOCOM Social Media Account Practices

The United States Special Operations Command (USSOCOM) provides *Social Media Smart Cards* that provide step-by-step social media guidance to its personnel. These individuals need a high degree of privacy to protect themselves and their families.

If you want even higher social media account protection, consider adopting some of their practices. The guidance is at *https://www.socom.mil/documents/ussocomsocialmediasmartcards.pdf*

Source: *Manage Your Online Presence*, https://www.cisa.gov/resources-tools/training/manage-your-online-presence, Retrieved April 19, 2025

Managing Your Privacy & Security Online

Limit your digital footprint

Mange your online presence

Follow cybersecurity best practices to protect yourself from tracking

Source: Managing Your Privacy and Security Online, https://www.cisa.gov/audiences/high-risk-communities/projectupskill/module6, Retrieved April 19, 2025

Follow Cybersecurity Best Practices to Protect Yourself

This is the seventh of eight presentations in the Project Upskill II series

The first presentation focused on privacy, and presentations 2-7 focused on cybersecurity.

These protections work together as a layered defense. To protect yourself effectively, you must put into practice the best practices presented throughout this series.

The following slides highlight key practices from the previous presentations.

Follow Cybersecurity Best Practices to Protect Yourself

Tracking technologies allow third parties to gather information about you.

Spyware is a class of tracking technologies that allows threat actors to track your location and communications, access the data on your device, and activate functions like the camera and microphone.

Source: *Follow Cybesecurity Best Practices to Protect Yourself from Tracking Technologies and Spyware*, https://www.cisa.gov/resources-tools/training/follow-cybersecurity-best-practices-protect-yourself-tracking-technologies-and-spyware, Retrieved April 19, 2025

Follow Cybersecurity Best Practices to Protect Yourself

Adware and cookies are two common tracking technologies.

Threat actors can use keyloggers, rootkits, stalkerware, and trojan horses to track you and access your devices, accounts, and data.

These technologies are often used to intimidate, silence, and suppress individuals and high-risk communities.

Source: *Follow Cybesecurity Best Practices to Protect Yourself from Tracking Technologies and Spyware*, https://www.cisa.gov/resources-tools/training/follow-cybersecurity-best-practices-protect-yourself-tracking-technologies-and-spyware, Retrieved April 19, 2025

Follow Cybersecurity Best Practices to Protect Yourself

Only download software from the maker of the software.

Reboot your computing devices at least weekly.

Put into practice all of the Project Upskill II guidance.

Source: *Follow Cybesecurity Best Practices to Protect Yourself from Tracking Technologies and Spyware*, https://www.cisa.gov/resources-tools/training/follow-cybersecurity-best-practices-protect-yourself-tracking-technologies-and-spyware, Retrieved April 19, 2025

Summary

Limit your digital footprint

Manage your online presence

Follow cybersecurity best practices to protect yourself from tracking

Source: Managing Your Privacy and Security Online, https://www.cisa.gov/audiences/high-risk-communities/projectupskill/module6, Retrieved April 19, 2025

Virtual Private Networks

December 17, Wednesday, 10 am

Cultural Center Education Room

Articles

For the latest cybersecurity information, these are accurate and reliable sources:

Ars Technica	arstechnica.com
Bleeping Computer	bleepingcomputer.com
CISA	cisa.gov
Forbes	forbes.com
Proton Blog	proton.me/blog
Proton VPN Blog	protonvpn.com/blog

Books

Beginner's Introduction to Privacy, Naomi Brockwell, (Independently Published, 2023)

Means of Control: How the Hidden Alliance of Tech and Government is Creating a New American Surveillance State, Bryon Tau, (Crown, 2024)

Your Face Belongs to Us: A Tale of AI, A Secretive Startup, and the End of Privacy, Kashmir Hill, (Crown, 2024)

Extreme Privacy: What It Takes To Disappear, 5th Edition, Michael Bazzell, (Independently Published, 2024)

Firewalls Don't Stop Dragons, 5th Edition, Carey Parker, (Apress, 2024)

YouTube Channels

David Bombal, [Cybersecurity, Privacy, IT] https://www.youtube.com/@davidbombal

Naomi Brockwell TV, [Privacy]
https://www.youtube.com/channel/UCSuHzQ3GrHSzoBbwrIq3LLA

PC Security Channel, [Cybersecurity, Malware]
https://www.youtube.com/channel/UCKGe7fZ_S788Jaspxg-_5Sg

Questions?