IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISING OF THE COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS

EIGHTH EDITION, MARCH 2019

BROUGHT TO YOU BY:

U.S. DEPARTMENT OF DEFENSE
HOW TO USE THIS GUIDE

The Identity Awareness, Protection, and Management (IAPM) Guide is a comprehensive resource to help you protect your privacy and secure your identity data online.

The IAPM Guide is divided into two-page chapters detailing key privacy considerations on the most popular online services, mobile apps, and consumer devices available in the market today. Each chapter provides you with tools, recommendations, and step-by-step guides to implement settings that maximize your security. The guide is updated twice a year, in March and September.

While some of the chapters in the IAPM Guide deal with technical issues, they do not require a technical background to follow.

The US Department of Defense creates this guide as a public service, and hopes this guide will help readers keep their identities private and secure.
TABLE OF CONTENTS

1. OVERVIEW........................................................................................................................................... 2
2. FACEBOOK.......................................................................................................................................... 4
3. FACEBOOK MOBILE............................................................................................................................. 6
4. TWITTER............................................................................................................................................... 8
5. INSTAGRAM......................................................................................................................................... 10
6. LINKEDIN........................................................................................................................................... 12
7. PHOTO SHARING SERVICES.................................................................................................................. 14
8. ONLINE DATING SERVICES.................................................................................................................... 16
9. MOBILE DATING APPS.......................................................................................................................... 18
10. SECURE CHAT APPS............................................................................................................................ 20
11. SMARTPHONES................................................................................................................................ 22
12. TRAVELING SAFELY WITH SMARTPHONES....................................................................................... 24
13. EXIF DATA REMOVAL........................................................................................................................... 26
14. MOBILE WALLETS............................................................................................................................... 28
15. HEALTH APPS & FITNESS TRACKERS.................................................................................................. 30
16. SECURING YOUR HOME WIRELESS NETWORK.................................................................................. 32
17. ONLINE REGISTRATION........................................................................................................................ 34
18. OPTING OUT OF DATA AGGREGATORS................................................................................................ 36
19. IDENTITY THEFT PREVENTION............................................................................................................ 38
20. KEEPING YOUR KIDS SAFE ONLINE.................................................................................................... 40
21. VOICE OVER INTERNET PROTOCOL (VOIP)....................................................................................... 42
22. VIRTUAL PRIVATE NETWORK (VPN)................................................................................................... 44
23. WINDOWS 10..................................................................................................................................... 46

INDEX.................................................................................................................................................... 48

USEFUL LINKS AND RESOURCES

- Privacy Right Clearinghouse http://www.privacyrights.org/privacy-basics
- HTTPS Everywhere https://www.eff.org/https-everywhere
- Securing Your Web Browser https://www.us-cert.gov/publications/securing-your-web-browser

DISCLAIMER:

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this guide. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third-party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only.

Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government.

DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.
WHY IS IDENTITY PROTECTION A CONCERN?

YOUR DATA IS EVERYWHERE

Everything you do creates a stream of data

- **PERSONAL**
  - Name
  - Birthdate
  - Work, Education, and Address History
  - Family and Friends
  - Likes and Interests

- **FINANCIAL**
  - Credit Cards
  - Bank Accounts
  - Digital Wallets
  - Online Payments
  - Purchase history

- **BIOMETRIC**
  - Face Recognition
  - Voice Recognition
  - Fitness Tracker Data
  - Device Authentication
  - DNA Analysis

- **BEHAVIORAL**
  - Browsing history
  - Social Media
  - Relationships
  - Interactions with devices and sensors
  - Location tracking

YOUR DATA IS VALUABLE

- The 21st-century world is based on trading personal data, instead of money, for convenience or utility.
- Online companies collect your data to develop targeted ads and sell them. Digital advertising was worth $266 billion worldwide in 2018.¹
- On the criminal side, personal data is worth a lot of money. PII sells for $1-1,000 dollars each on the Dark Web, where criminals sell it in bulk.²

YOUR DATA IS UNPROTECTED

- The United States has no centralized, formal legal structure to protect your data.
- Companies can and do share data with each other, so you don’t know who might take over your data. 91% of users install mobile apps without reading the terms of service, which often allow for data sharing.³
- Biometric data is everywhere. Even a picture of your face can pose risks.
- Hacks are constant. Your data has probably already been stolen.

YOUR DATA CAN BE DANGEROUS

- Any piece of data alone can be innocuous, but tied to other sources, it becomes a three-dimensional image of you that can pose a threat. Advertising firms, public records companies, or criminals can link disparate information about you together.
- Identity theft can waste time and hurt consumers financially.
- Oversharing online can lead to personal embarrassment or professional consequences.
- Online behavior can reveal patterns of life that can lead to physical risk in the real world.

WHAT CAN YOU DO ABOUT IT?

EDUCATE YOURSELF

• 74% of people are unaware that Facebook develops profiles of users’ interests.¹
• Knowing the risks puts you ahead of most people.
• The IAPM Guide is a great start. Look at the Table of Contents page for more information sources.

REVIEW TERMS OF SERVICES, and stay up-to-date with privacy updates and changes.

PROTECT YOURSELF

• Use caution before agreeing to share your information. Think before you click.
• Learn how to tell the legitimate from the illegitimate.
• When in doubt, opt out.
• Threats to your identity constantly change. Monitor your credit and online accounts, and keep your software and devices up-to-date.

Be proactive about identity security. Only share PII with people or companies you trust.

41%
of online adults have shared the password to one of their online accounts with a friend or family member.⁵

39%
say that they use the same (or very similar) passwords for many of their online accounts.⁶

25%
admit that they often use passwords that are less secure than they’d like, because simpler passwords are easier to remember than more complex ones.⁷

STRIKE THE RIGHT BALANCE

DON’T PANIC!
Your identity and privacy can still be protected.

• Social media and apps are useful, but make sure you use them safely.
• Before using a product or sending your PII to someone, ask yourself if it is providing enough of a benefit to be worth the risk.
• If your identity has already been stolen, you still have time to react and recover.

¹ http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/
² http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
³ http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
⁴ http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
⁵ http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
⁶ http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
⁷ http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/
### SOCIAL NETWORK - DO’S AND DON’TS

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you, or your family, that clearly show faces. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Use secure browser settings when possible, and monitor your browsing history to ensure you recognize all access points.
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.

### MAXIMIZING YOUR FACEBOOK PRIVACY

Facebook provides shortcuts to privacy settings that limit what others can see in your profile.

Click on **Privacy Checkup** to change your basic privacy settings.

For more extensive and granular control, navigate to **Settings** from the top drop down menu. Click through each tab to control how your personal information is shared with others.

### RECOMMENDED SETTINGS

The (1) Security and Login, (2) Privacy, (3) Your Facebook Information, (4) Timeline and tagging, (5) Location, (6) Face Recognition, (7) Public Posts, (8) Ads, and (9) Apps and Websites tabs contain settings for concealing personal information. Use the settings displayed below to maximize your security online.

Facebook interactions (e.g., likes, posts) have been used to behaviorally profile individuals. Minimize the amount of personal information you share by limiting your interactions.

1. The **Security and Login** tab contains settings to protect your login credentials, monitor attempted and successful logins, and recover your account in the event of a lockout. Use **Where You’re Logged In** to monitor login activity and end inactive sessions, and turn ON alerts for unauthorized login under **Setting Up Extra Security > Get alerts**.

2. Use the **Privacy** tab to control which audiences can search for you, contact you, and see your posts. Under **Your Activity > Use Activity Log**, review past posts individually and limit the audiences for each entry. Use **Limit Past Posts** to retroactively change the settings of all “Public” posts to a “Friends” only audience.

3. Use the **Your Facebook Information** tab to view or download your data or delete your account. This tab contains shortcuts to your **Activity Log** and an informative **Managing Your Information** tab that guides you through common Facebook and Instagram data management questions and concerns.

4. **Timeline and Tagging** controls how others interact with your Timeline. Select **View As** to preview what others can see on your profile.

5. Facebook uses your device to obtain and store location data. The **Location** tab displays if your **Location History** is on. Use **View your location history > > Delete all location history** to remove stored data.

6. Use the **Face Recognition** tab and disable face recognition by setting to **No** as shown. This prevents Facebook from searching and matching your face against all photos and videos uploaded to its database.

7. Followers are people outside your “Friends” network who interact with content you share publicly. Your **Public Posts** are streamed on their News Feeds. To prevent this, set **Who Can Follow Me to Friends**. Restrict **Public Post and Public Profile** settings as shown.

---

Identity Awareness, Protection, and Management Guide
The Facebook profile page contains tabs that allow users to add information about themselves, view friend lists, and post text entries or photos to their profiles. General audience settings reside within these tabs. Use the guidelines below to maximize your security while interacting with these features.

**ABOUT**

Avoid entering personal data in the About section unless required by Facebook. This information is mostly optional and contains data fields including Work and Education, Places You've Lived, Contact and Basic Info, Family and Relationships, Details About You, and Life Events. Use audience settings to change the mandatory fields to Friends or Only Me.

**ACTIVITY LOG**

The Activity Log tool chronologically displays your Posts, Posts You’re Tagged in, and Others’ Posts To Your Timeline. Use the dropdown menu shown to delete or manage how individual posts appear on your Timeline.

**REVIEWING YOUR INFORMATION**

To review a comprehensive list of data collected by Facebook, navigate to Settings > Your Facebook Information > Access Your Information.

You can Download Your information entirely or by type or date range, in HTML or JSON format, and in high, medium, or low media quality.

**DEACTIVATING/DELETING YOUR FACEBOOK ACCOUNT**

Deactivating an account removes your name and photos from posts that you have shared. To deactivate your Facebook account, navigate to Settings > General > Manage Account then click on Deactivate your account. Your account remains deactivated until the next login. Some information may still be visible, such as your name in someone else's friend list and messages you have exchanged.

To delete your account, navigate to Settings > Your Facebook Information > Delete Your Account and Information, then click Delete Account. The deletion process begins 14 days after request submission, and Facebook will permanently remove most of your data within 90 days.
FACEBOOK MOBILE

SOCIAL NETWORK - DO’S AND DON’TS

• Only establish and maintain connections with people you know and trust. Review your connections often.
• Assume that ANYONE can see any information you post and share regarding your activities, whereabouts, and personal or professional life.
• Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
• Avoid posting or tagging images of yourself or family that clearly show faces. Select pictures taken at a distance, at an angle, or otherwise concealed.
• Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.
• Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.

OVERVIEW

Facebook reports 1.49 billion daily active global users in June 2018. Most users access the mobile app, as reflected by Facebook mobile’s advertising revenue, which accounted for 91% of Facebook’s overall advertising revenue for Q1 2018. Using Facebook’s mobile app (vs. website) places your identity at greater risk because smartphones provide to access additional personal data (e.g., location). Use the following recommendations to best protect yourself.

FACEBOOK MOBILE SETTINGS

Facebook Mobile settings closely resemble those of the website. Settings you implement carry across both the web and mobile app. From the 📞 icon in the navigation panel, select Settings & Privacy > Settings. Navigate tabs within the Security, Privacy, and Ads sections to implement settings shown below.

IPHONE SETTINGS

iPhones can be configured to control how your data is shared while you are using the Facebook app. From the iPhone’s Settings, scroll down to the Facebook tab to review and adjust Facebook’s access to your data, such as Location, Photos, Camera, and Microphone. Toggle OFF all permissions at all times unless required on a case-by-case basis.

ANDROID SETTINGS

Android phones can be configured to protect your personal data while you are using the Facebook app. Navigate to Settings > Apps > Facebook and scroll down to App Settings > Permissions to review and adjust Facebook’s access to your data. Toggle OFF all permissions unless required for a specific, limited-time use case (e.g., uploading a photo).
POSTING TO FACEBOOK

Facebook Mobile allows you to post a new status, upload photos, or check in to locations using the What's on your mind? prompt. The icons highlighted on the update prompt are shortcuts for adding further personal information to each post. Several shortcuts pose a significant risk to your privacy and should be used sparingly. Follow the guidelines outlined in this section to prevent over-sharing your information.

SELECTING YOUR PRIVACY

With every post, Facebook Mobile allows you to select the audience through the Select Privacy tab beneath your name. For maximum privacy, select Specific friends with whom you would like to share your post. Never make your posts available to the public.

ADD PHOTOS

Avoid posting photos to your Timeline. These photos can often be viewed from your contacts’ profile pages and can be saved without your knowledge or consent.

TAG FRIENDS

Tagging friends in individual posts extends the visibility of your post and profile to your friends’ networks. Limit the number of tags you add to your Facebook posts.

ADD LOCATION

Never disclose your location within a Facebook post. Doing so allows Facebook to keep records on your whereabouts and allows others to see when you are away from home.

LIVE VIDEO BROADCAST

Avoid posting live video broadcasts. Videos are hard to vet for potentially harmful data and can lead to legal repercussions if others believe a video compromises their privacy.

NEARBY FRIENDS - LOCATION SETTINGS

Nearby Friends allows you to share your location with friends. When activated, Facebook collects your location data, even while you are not using the app, and continually broadcasts your approximate locations to your friends. You also have the option to allow certain users to see your precise location for set periods of time. Do not turn on Nearby Friends.

LOCAL

Local uses your GPS location to display local venues. When activated, the feature permits check-ins, provides a map of your location, and suggests places to go based on where you and your friends have already been, or on situational needs such as dining. Avoid posting on these public threads.

When this feature is enabled, Facebook builds a history of your precise locations. You can view and manage this information from Settings > Location > View your Location History. In general, avoid giving Facebook permission to track your location.

To use this feature, you must have Location History enabled. This feature permits Facebook to track your precise location, even when the app is not in use. Avoid giving Facebook permission to track your location.
SOCIAL NETWORK - DO'S AND DON'TS

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information you post and share regarding your activities, whereabouts, and personal or professional life.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you, or your family, that clearly show faces. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.

OVERVIEW

Twitter is a social networking and micro-blogging site that hosts 326 million monthly active users, as of mid 2018. Twitter allows users to post text-based entries to their profiles and follow updates from other accounts. On average, Twitter users post approximately 500 million entries per day from both the website and its mobile app. For most, Twitter is used as a source to discover breaking news developments and stay up-to-date on current events or their friends’ recent whereabouts. Should you choose to maintain a Twitter account, use the recommendations in this card to enhance your privacy.

TWITTER PROFILES

Profile pages can be operated by a single individual, a group of individuals, or even large organizations. Regardless of who maintains the account, each individual profile is labeled with a unique username known as a Twitter Handle (e.g., @google). Handles allow other users to locate profiles and mention them in posts. In general, profile pages tend to contain some of the account owner’s personal data and display every Tweet posted by that user.

POSTING TO TWITTER

A Twitter entry is referred to as a “Tweet.” Tweets can be composed of photos, videos, links, polls, or short text entries, limited to 280 characters. Tweets are public, indexed, and searchable, unless protected by the user. Many users never Tweet, choosing only to follow persons or topics of interest.

Mentions (@username) are used to tag other users or accounts in a Twitter update. Tags create a link to the mentioned individual’s profile. When a public user mentions a private Twitter account, the link to the profile of the private account becomes visible to the public.

Hashtags (#topic) are used to highlight key topics in individual posts. When a hashtag is posted by numerous users across the network, the hashtag becomes a “trending topic” of conversation. Trending topics are advertised on Twitter and extend the reach of posts and profiles. Tweets with hashtags are searchable within the Twitter search engine.

When a Tweet is published, other Twitter users are able to interact with the post through the icons highlighted to the left. These icons permit actions including Replies, Retweets, Likes, and More.

- **Replies** - Replies are text responses to another user’s Tweet. The Reply prompt automatically mentions the author of the original Tweet within the text of the reply.
- **Retweets** - Retweets are used to forward other users’ Tweets to your personal followers. Retweets always retain a link back to the original poster’s profile page.
- **Likes** - Likes are used to show endorsement of another user’s post. A list of entries liked by a single user appears directly within that user’s Twitter profile page.
TWITTER SETTINGS

Access Twitter’s settings by selecting the thumbnail image of your profile photo in the top banner. From the dropdown menu, select Settings and privacy and navigate to pages containing customizable security options: Privacy and safety, Email notifications, and Account. After configuring your privacy settings, access your Twitter data tab to review device and login histories to ensure that your account has not been accessed by unauthorized users.

PRIVACY AND SAFETY

Apply the settings shown below in the Privacy and safety tab to control how others can interact with your Twitter profile and your Tweets. Save changes.

ACCOUNT SETTINGS

Account settings allow you to customize your Twitter handle and contact email. You can also request your Twitter archive which contains a transcript of all of your past Tweets and replies, or elect to Deactivate your account.

EMAIL NOTIFICATIONS SETTINGS

Email notifications alert you when others interact with your profile or content. For maximum security, customize the notifications settings to receive all alerts related to you and your account activities. Save changes.

In the Security section, use Set up login verification and check the box for Password reset verification to further secure your account.
**INSTAGRAM - DO’S AND DON’TS**

- Don’t connect your Instagram account with your other SNS profiles (e.g., Facebook, Twitter, Tumblr). It increases your account’s discoverability.
- Only accept follow requests from people you know and trust. Assume that ANYONE can see and forward photos you post, and save or forward copies.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images that clearly show your face. Select pictures of yourself taken at a distance, at an angle, or wearing sunglasses.
- Don’t embed your posts with hashtags (e.g., #foodie, #caturday), as hashtags increase your posts’ visibility and make them searchable by others.
- Remember that even if you restrict your data from public view, Instagram still has access to your data and may share it with third parties.

**INSTAGRAM OVERVIEW**

Instagram is a photo-sharing application that allows users to curate original content using pictures and videos. With 1 billion monthly active users as of June 2018, it is currently the second most popular social networking service (SNS) in the world, exceeded only by Facebook (which acquired Instagram in April 2012). Instagram functions primarily as a mobile platform. Its popularity stems from the ease with which users can take photos on the go and quickly upload, edit (using many pre-set digital filters), and post images.

In terms of privacy, Instagram accounts can be either public or private. Content posted on public Instagram accounts is indexed and can be searched and viewed by anyone, including non-Instagram members, via search engines such as Google. Posts made on private accounts are only shared with followers that have been approved by the account owner. It is recommended that you keep your personal Instagram account set to private at all times.

**INSTAGRAM MEDIA FORMATS**

<table>
<thead>
<tr>
<th>Media Format</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stories</td>
<td>Temporal video or photo posts that you share in real-time but which are not saved to your profile page. New stories are designated with a pink-purple circle around your profile page and are viewable for 24 hours.</td>
</tr>
<tr>
<td>Videos</td>
<td>Can be shared in a single post or as a video series. The best video formats are MP4 and MOV.</td>
</tr>
<tr>
<td>Photos</td>
<td>Can be shared in a single post or as a photo series. Instagram supports a maximum resolution of 1080x1080 pixels. Larger photos are automatically downsized during upload. The aspect ratio must be set between 1:91:1 (landscape) and 4:5 (portrait).</td>
</tr>
</tbody>
</table>

**ACCOUNT REGISTRATION - PRIVACY TIPS**

1. Sign up to see photos and videos from your friends.
   - **DO NOT** use your Facebook account for sign up or log in.

2. Name and Password
   - Add your name so friends can find you.
   - “Full Name” is NOT REQUIRED during registration. Do not share.
   - Choose a complex password and change it every 3 months.

3. Find People to Follow
   - Click on the “Find People to Follow” button to view recommended accounts to follow. You can choose to have your contacts periodically synced and stored on our servers. You pick which contacts to follow. Disconnect anytime to stop syncing.
To access your privacy settings, go to your Profile and tap the icon in the top-right corner of the screen. Apply the settings shown below to control how your photos and videos are shared, and to minimize the amount of personal information you share with Instagram and third parties.

**ACTIVITY STATUS**

toggle OFF “Show Activity Status” to prevent other users from seeing when you were last active on Instagram apps.

**STORY CONTROLS**

Block specific people from viewing your Instagram Stories by their usernames. Toggle OFF.

**PHOTOS & VIDEOS OF YOU**

Toggle OFF “Add Automatically” to review when others tag you in photos before they are added automatically to your Instagram profile.

**LINKED ACCOUNTS**

DO NOT link your other SNS accounts.

**CONTACTS SYNCING**

Toggle OFF everything.

**EMAIL AND SMS**

Clear Search History to delete your Instagram search history periodically.

**IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE**

From the Settings page, click on Help Center, then type in “delete my account” to pull up the Delete Your Account page. Follow the steps and confirm deletion by clicking “Permanently delete my account.” Once you delete your account, it can’t be reactivated and you can’t sign up again with the same username.
LinkedIn is a professional networking service with 590 million users worldwide. It is mainly used to connect employers who create job postings and job seekers who share their resumes and CVs. Users typically maintain profile pages outlining their professional and educational achievements, and establish networks with others who report similar interests and backgrounds. They can also share their areas of expertise, skills, personal interests, and hobbies. Since 2016, LinkedIn has been a subsidiary of Microsoft. Follow the recommended settings to limit the exposure of your personally identifiable information (PII) without foregoing LinkedIn’s many useful features.

**Social Network - Do’s and Don’ts**

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information you post and share regarding your activities, whereabouts, and personal or professional life.
- Ensure your family and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting images of you, or your family, that clearly show faces. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.

**Managing Your LinkedIn Presence**

Click on the Privacy tab under Settings & Privacy. Apply the settings shown below to ensure that your profile is visible only to the people of your choosing.

**Privacy Settings**

1. **Who Can See Your Last Name**
   - Select how your last name will appear to others. Your full name is always visible to your connections.
   - Abbreviate your last name

2. **Profile Viewing Options**
   - Set to “Private Mode” to ensure that your LinkedIn browsing history isn’t made visible to other members.

3. **Profile Editing**
   - Set your public profile visibility to “Off” unless you are actively seeking a job or are otherwise required to have a public professional web presence.
   - If your public profile is visible, make sure all the optional fields are checked OFF to prevent overexposure.

<table>
<thead>
<tr>
<th>Privacy Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who can see your email address</td>
<td>Set to “No”</td>
</tr>
<tr>
<td>Who can see your location on your profile</td>
<td>Set to “No”</td>
</tr>
<tr>
<td>Who can see your last name</td>
<td>Set to “Abbreviated”</td>
</tr>
<tr>
<td>Who can see your connections</td>
<td>Set to “No”</td>
</tr>
<tr>
<td>Who can see your activities with others</td>
<td>Set to “No”</td>
</tr>
<tr>
<td>Profile visibility off LinkedIn</td>
<td>Set to “No”</td>
</tr>
<tr>
<td>Profile visibility off Microsoft</td>
<td>Set to “No”</td>
</tr>
</tbody>
</table>

**Managing Your LinkedIn Presence**

LinkedIn is a professional networking service with 590 million users worldwide. It is mainly used to connect employers who create job postings and job seekers who share their resumes and CVs. Users typically maintain profile pages outlining their professional and educational achievements, and establish networks with others who report similar interests and backgrounds. They can also share their areas of expertise, skills, personal interests, and hobbies. Since 2016, LinkedIn has been a subsidiary of Microsoft. Follow the recommended settings to limit the exposure of your personally identifiable information (PII) without foregoing LinkedIn’s many useful features.
DATA COLLECTION, DATA PRIVACY, & ADS

Apply the Data Privacy and Advertising settings shown below to minimize the amount of information you share with LinkedIn and third parties. You can find these settings under Settings & Privacy > Privacy > How LinkedIn uses your data.

LinkedIn maintains an archive detailing each user’s unique account activity. Navigate to Settings & Privacy > Privacy > How LinkedIn uses your data > Download your data to receive a comprehensive report of your past activity and network information. Review your data frequently to ensure that you are not over-sharing information. Visit the Help Center to see the types of information LinkedIn collects.

REQUEST DATA ARCHIVE

Navigate to Settings & Privacy > Account > Partners and Third Parties > Permitted Services monthly and review which services and apps you’ve given access to your LinkedIn data. Remove permissions from services that you no longer use nor require.

LOGINS AND SECURITY SETTINGS

Navigate to Settings > Communications > LinkedIn messages and set Participate in research to No to prevent LinkedIn from using your activities for internal research purposes.

If you no longer plan to use the LinkedIn service, click Closing Your LinkedIn Account under Account settings and confirm your decision.
PHOTO SHARING SERVICES

PHOTO SHARING SERVICES - DO'S AND DON'TS

- Only share photos with people you know and trust. Assume that ANYONE can see, save a copy, and forward photos you post and share online.
- Ensure your family and friends take similar precautions with their photos; their privacy settings can expose you to unwanted parties.
- Avoid posting or tagging images that clearly show your face. Select pictures of yourself taken at a distance, at an angle, or wearing sunglasses.
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.
- Remove EXIF (Exchangeable Image File Format, or photo metadata) and location data from the photos you upload whenever possible.
- Limit the visibility of the photos to only your account or to accounts that you approve individually.

OVERVIEW

Photo sharing services (PSS) are online photo albums that store, organize, and share your digital photos; many social networking services (SNS) such as Facebook and Twitter also function as photo sharing services. PSS provide a convenient way to share photos, but can expose you to privacy risks if you do not take proper precautions. This chapter explains how you can control the security settings of six popular photo sharing services to protect your privacy.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>PRIMARY USE</th>
<th>PRIVACY OPTIONS?</th>
<th>EXIF?</th>
<th>LOCATION OPTIONS</th>
<th>ALLOW REPOSTING?</th>
<th>GOOGLE INDEXED?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapchat</td>
<td>Share temporary photo &amp; video messages known as “Snaps”</td>
<td>Everyone, My Friends, Custom</td>
<td>Yes</td>
<td>User location tracked by default; disabled with “Ghost Mode” feature</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>iOS Photos</td>
<td>Organize and share photos from Apple devices</td>
<td>Private (able to share album/images)</td>
<td>No</td>
<td>Locations on photos tracked by default; no option to remove info</td>
<td>No, but photos can be downloaded once shared</td>
<td>No</td>
</tr>
<tr>
<td>Google Photos</td>
<td>Automatically back up, organize, share photos from smartphones</td>
<td>Private (able to share albums/images and tag your Google contacts)</td>
<td>Yes</td>
<td>Can tag location to photos; geolocation tracking if enabled</td>
<td>No, but photos can be downloaded once shared</td>
<td>No, but the service is owned by Google</td>
</tr>
<tr>
<td>flickr</td>
<td>Share photos within grouped user environments</td>
<td>Public, Private, Contacts, Family, Friends</td>
<td>Yes</td>
<td>Can tag location to photos, can embed location in EXIF data</td>
<td>Yes</td>
<td>If Public (can opt out)</td>
</tr>
<tr>
<td>imgur</td>
<td>Share and comment on photos</td>
<td>Public, Hidden (images viewable with direct URL), Secret</td>
<td>No</td>
<td>None (can add location to photo description)</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>Pinterest</td>
<td>Share concepts and ideas using images</td>
<td>Public, Private (with Secret Boards)</td>
<td>No</td>
<td>None (can add location to photo description)</td>
<td>Yes</td>
<td>If Public (can opt out)</td>
</tr>
</tbody>
</table>

SNAPCHAT

Snapchat allows users to send temporary photo and video messages (“Snaps”) to one another. Snaps can only be viewed once by the intended recipient(s) and are set to expire within 1 and 10 seconds.

Tap your profile photo icon and then Settings > Who Can...:

- Set Contact Me to My Friends
- Limit View My Story to My Friends or Custom
- Tap See My Location. Turn on Ghost Mode and toggle OFF Allow friends to request my location
- Tap See Me in Quick Add and toggle OFF the box to avoid being recommended as connection to other users

Under Additional Services > Manage > Maps, toggle OFF Share Usage Data

IOS PHOTOS

iOS Photos is an intelligent photo organizer and sharing tool exclusively for Apple users. It is the default photo app on all iOS devices and comes pre-installed on Macs, iPhones, and iPads. It cannot be removed or uninstalled.

iCloud Photo Sharing is a feature allows users to create private albums from photos and share with their contacts. To share photos from your Apple device, navigate to Settings > Photos:

- Shared Albums: Toggle ON

When photos are shared with contacts who does not use iCloud, the app creates a link to a public website with the shared photos which anyone can see and access. Users can also post to SNS, messengers, and other photo sharing apps directly from iOS Photos.

iOS Photos doesn't provide a privacy control for managing location data in photos. If you are concerned, process your photos through EXIF removal tools (see pg. 26-27) before sharing them.
Google Photos, the default photo app on Android devices, is a photo sharing, storage, and organizational tool with more than 500 million active users. It seamlessly connects with Gmail to allow easy online photo sharing via albums and public URIs. In addition to location tagging, Google Photos uses face recognition to group similar faces and encourages photo organization by faces contained in the photos.

Make the following changes to your account settings to minimize the degree of personal data shared and collected by Google, and maximize your privacy. Open the Google Photos app on your smartphone or browser and navigate to:

- Go to **Account settings**

  - Under **Search privacy**, toggle **ON** Hide your profile from search engines
  - Under **Personalization**, toggle **OFF** the following selections:
    - Use sites you visit to improve which recommendations and ads you see: toggle OFF
    - Use information from our partners to improve which recommendations and ads you see: toggle OFF

  When you make a new Board in Pinterest, toggle the Secret boards option **ON** to keep your pins private.

Flickr, acquired by SmugMug in April 2018 and supporting 90 million monthly active users, offers free and paid accounts for photo sharing and editing. To maximize your privacy, click your avatar in the upper right corner and select **Settings** from the drop down menu. This takes you to the Account settings page.

Make the following changes under the **Privacy & Permissions** tab for Global settings and **Defaults for new uploads**:

When you make a new Board in Pinterest, toggle the Secret boards option **ON** to keep your pins private.

Imagur allows users to share photos or albums with anyone using a customized URL and easily post their photos to other sites such as Reddit and Facebook. Imagur has over 250 million MAU. By default, Imagur strips all EXIF data from the photos you upload. However, you still need to make a few modifications to your account settings to maximize privacy.

Hover over your username (top right) and select **Settings** from the drop down menu to make the following changes:

- When creating a new album, select Hidden to make albums accessible by URL only, or Secret so album is visible only to you
- Comment mentions: check this box to receive notifications when you are mentioned in a comment.
- Use the **Security** tab to review account activity sessions.

Pinterest is a site where users can upload, categorize, and share images called Pins on dedicated pages called Pin Boards. The site has more than 250 million monthly active users (MAU). To maximize your privacy on Pinterest, make the following modifications to your account settings. Go to:

  - Select **Hidden** or **Secret** to maximize privacy

  When you make a new Board in Pinterest, toggle the Secret boards option **ON** to keep your pins private.
ONLINE DATING SERVICES

ONLINE DATING SERVICES - DO’S AND DON’TS

- Do not link online dating profiles to your social networking or photo sharing services (e.g., Facebook and Instagram).
- Avoid using usernames and profile photos that appear on other social networking sites.
- Do not include information unique to you (e.g., last name or place of work) in your public profile data or messages.
- If possible, upgrade your account to a paid version; paid accounts often offer more control over who can see your profile and what data is visible.
- Always read and take the time to understand the site’s Terms and Conditions before agreeing to register an account.
- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.

OVERVIEW

Online dating services are used by individuals looking to develop a personal or romantic relationship with other users. While each service is unique, sites typically ask users to maintain a public profile containing photos of themselves and personal information. These profiles are often searchable through the site and, at times, may be pushed to users who share common interests or locations. Should you elect to participate in online dating, use the recommendations in this card to protect your web-based online dating profiles and associated personal data. For additional information about mobile-based services such as Tinder, Bumble, Hinge, or Coffee Meets Bagel, please reference the Mobile Dating Apps chapter.

COMMON THREATS FROM DATING SITES

Online dating sites present a unique set of threats to users in comparison to other social networking sites. Dating sites encourage interactions between unacquainted individuals, collect extensive personal information that is used to match compatible individuals, and have few methods of verifying the accuracy of users’ claims. Before participating in online dating, consider the following threats to your personal data:

- Sites use questionnaires to pair like-minded individuals, allowing the services to collect targeted information about users’ lifestyles.
- Most sites encourage users to connect a social network to their profiles or require them to supply face photos to help verify the account’s legitimacy.
- Matches may request personal contact information (e.g., phone number or SNS). Use the dating site’s chat feature as the only form of communication.
- Catfishing—a form of social engineering that uses a fake online persona to glean information from unsuspecting, real individuals—is common among online dating sites and can lead to identity theft, character defamation, and other general online scams.

SELECTING A DATING SITE

Online dating sites are designed to pair individuals with one another based on common interests, values, lifetime achievements, and daily lifestyles. As a result, users of these sites often find themselves divulging additional information that they may not feel comfortable sharing on other social networking services (e.g., Facebook). Prior to registering an account, examine the types of data collected by each online dating site and select the service that best fits your privacy needs. Five of the top dating sites and their respective data requirements are outlined in the following table:

<table>
<thead>
<tr>
<th>SITE</th>
<th>REGISTRATION INFORMATION</th>
<th>VISIBLE PROFILE INFORMATION</th>
<th>DATA SHARING OPTIONS</th>
<th>PRICING</th>
</tr>
</thead>
<tbody>
<tr>
<td>match</td>
<td>Gender, partner gender preference, age preference, ZIP code, email address, password, birthday, seriousness of relationship, height, body type, relationship status, have/ want kids, education, smoke, drink, ethnicities, religion, salary, interests</td>
<td>Most registration information, optional lifestyle and dating preferences, photos</td>
<td>Login with Facebook, upload photos from Facebook</td>
<td>Free to join; $21-$27/month to send messages and use the invisible browsing feature; other features available at cost</td>
</tr>
<tr>
<td>okcupid</td>
<td>First name, email address, birthday, location, gender, sexual orientation, biography, lifestyle questionnaire, photos</td>
<td>First name, most registration information, optional questionnaire answers</td>
<td>Login with Facebook, upload photos from Facebook, connect Instagram feed and upload photos</td>
<td>Free to join and send messages (“A-List Basic”). $25-$35/month for A-List Premium, which offers enhanced profile priority and messaging features.</td>
</tr>
<tr>
<td>PlentyOfFish</td>
<td>Gender, sexual orientation, ZIP code, email address, country, birthday, ethnicity, physical description, personal questionnaires, biography, interests, face photo</td>
<td>Most registration information</td>
<td>Upload photos from Facebook</td>
<td>Free to join, send messages, and hide profile; $6-$13/month to see extended profiles</td>
</tr>
<tr>
<td>zoosk</td>
<td>Gender, sexual orientation, ZIP code, email address, face photo, birthday, physical description, lifestyle questionnaire, face photo</td>
<td>Most registration information, biography, optional lifestyle and dating preferences</td>
<td>Register with Facebook or Google, upload photos from Facebook</td>
<td>One-time activation fee of $24.95 for paid memberships. 1 month: $29.95, 3 months: $19.95/month, 6 months: $14.98/month</td>
</tr>
<tr>
<td>eharmony</td>
<td>Name, gender, sexual preference, ZIP code, email address, children, city of residence, DOB, ethnicity, height</td>
<td>Occupation, ethnicity, height, education, college, language, religion, smoke/drink preferences, children, passionate about, similarities, hobbies, positive characteristics, what user is most thankful for</td>
<td>Optional login with Facebook</td>
<td>Free to join. Membership required for active engagement ($15.95-$54.95/month depending on plan and subscription length)</td>
</tr>
</tbody>
</table>
Plenty of Fish hosts 80 million registered members. Profiles display the information submitted during registration and the traits that users look for in significant others.

Select **Edit Profile** and elect to hide your profile from others. Hidden profiles do not appear in search results and, unlike other sites, do not lose matching or searching functionality as a result. Select **Upload Images** and set images to private so they can only be shared with individuals via private message.

Paid subscriptions do not offer significant security upgrades compared to free accounts. Subscriptions are designed to increase the reach of a profile.

Zoosk hosts 27 million registered members. Dating profiles consist of the data entered during registration and free-text entries describing the owners' dating preferences and personal background.

Free Zoosk accounts offer little to no privacy setting options. Zoosk provides multiple options to verify your account, including completing a photo verification and linking your number, Twitter, Facebook, or US military service records.

When others visit the profile, Zoosk identifies the visitor to the profile owner. Users can activate private browsing for 30 minutes by paying 30 Zoosk coins (starting coin price: $5.95 for 60 coins, purchased within the profile).
MOBILE DATING APPS

MOBILE DATING APPS - DO'S AND DON'TS

• Avoid using usernames and profile photos that also appear on other social networking services and profiles.
• Do not include information unique to you (e.g., last name or place of work) in your public profile data or messages.
• Install all app updates as soon as they become available. Check your app's privacy settings after each update to ensure maximum protection.
• Enable push notifications and alerts for your apps to help keep track of who is connecting with your profiles.
• Avoid posting images that may reveal your geographical location, such as a photo with a famous landmark in the background.
• Always read and take the time to understand the apps’ Terms and Conditions before agreeing to register an account.

OVERVIEW

It is estimated that one out of every three American adults have used online dating services and mobile dating apps to actively discover romantic connections. As these apps continue to gain traction, users’ identity data will be placed at a significantly higher privacy risk. Should you elect to participate in mobile dating, use the recommendations on this card to protect your personal and identity data. For additional information about the risks of online dating on web-based services such as Match, Plenty of Fish, Zoosk, OKCupid, or eHarmony, please reference the Online Dating Services chapter.

USING MOBILE DATING APPS

Matching: Mobile dating apps frequently employ a technique called “Swiping”—the motion of directing one's finger across a phone screen's surface—to help convey interest in other users’ profiles. Traditionally, swiping a profile to the right indicates interest, while swiping it to the left indicates disinterest in the profile. Regardless of the swiping direction, selections are typically kept secret until both individuals show a mutual interest in one another.

Communication: Each app provides a matches page where users can revisit their matches’ profiles or open a text dialogue with them through the app. Profiles and conversations remain accessible unless the app employs a time limit or a user manually unmatches the profiles.

SELECTING A DATING APP

In general, mobile dating apps offer little to no user-controlled privacy settings. As a result, users must show discretion when registering an account and should avoid sharing potentially harmful data. Prior to registering an account, examine the types of data required by each mobile dating app, and select the service that best fits your privacy needs. Four of the top mobile dating apps and their respective data requirements are outlined in the following table:

<table>
<thead>
<tr>
<th>DATING APP</th>
<th>REGISTRATION INFORMATION</th>
<th>VISIBLE PROFILE INFORMATION</th>
<th>APP PERMISSIONS</th>
<th>PRICING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tinder</td>
<td>Facebook account or phone number verification (provided through Account Kit, which is powered by Facebook)</td>
<td>Name, photos, age, approximate location, gender, biography, work information, education information, Instagram photos, Spotify account (top artists, favorite song)</td>
<td>Location, Cellular Data, Storage &amp; Push Notifications Access to Facebook Account</td>
<td>Free to join; up to $10 / month for an upgraded account (change location, rewind features, disable ads)</td>
</tr>
<tr>
<td>Bumble</td>
<td>Phone number verification or Facebook account info Likes, photos, general info, and relationship interests</td>
<td>Name, photos, age, location, biography, work information, education information</td>
<td>Camera, Location, Phone, Cellular Data, and Storage Access to Facebook Account</td>
<td>Free to join; enhanced features available at-cost</td>
</tr>
<tr>
<td>Hinge</td>
<td>Facebook or Instagram account info</td>
<td>Name, photos, age, location, biography, height, education information, work information, hometown, religion, interests, dating preferences</td>
<td>Location, Cellular Data &amp; Push Notifications Access to Facebook Account</td>
<td>Free to join; preferred membership with premium features available for $5-13/ month</td>
</tr>
<tr>
<td>Coffee Meets Bagel</td>
<td>Phone number verification or Facebook account info Relationship interests, gender, location</td>
<td>Passions, hobbies, height, ethnicity, religion, occupation, employer, education, photos</td>
<td>Location, Cellular Data, Push Notifications, Contacts, &amp; Photos Access to Facebook Account</td>
<td>Free to join; up to $25 can be spent on credits (“beans”) at a time to view more profiles in a day</td>
</tr>
</tbody>
</table>
TINDER

Tinder evaluates account users’ geolocations, mutual Facebook friends, and common interests to match individuals. It also monitors users’ viewing and swiping habits on the service to help predict more compatible matches.

Use: Users may swipe through a limited number of profiles per day. There are no gender-based limitations on who is able to initiate a chat conversation once matched. Matches do not expire and are stored in the app unless they are manually removed by one of the users.

Profiles: Navigate to Person Icon > Edit Info to change or delete the information displayed in your profile.

Settings: Navigate to Gear Icon > Discovery Settings to change your profile’s visibility. Deactivating Show me on Tinder hides your profile.

BUMBLE

Bumble uses geolocation and behavior metrics to pair individuals. The app measures the number of conversations started and the average length of conversations to match engaged users and incentivize others to participate.

Use: Users may swipe through an unlimited number of profiles per day. Once matched, women are given 24 hours to initiate a conversation. For same-sex connections or friendship settings, either person has 24 hours to make the first move. The match expires if no communication is established.

Profiles: Navigate to Edit Profile to change the information displayed in your profile.

Settings: Select Settings to enable notifications and set your profile’s visibility. Activate Snooze Mode when you are not actively searching or would like to hide your profile from public view.

HINGE

Hinge, acquired by Match Group in 2018, matches people who have mutual Facebook friends. The app factors in geolocation, common interests, and the types of profiles each user has liked in the past to suggest more attractive matches.

Use: Users may swipe through an unlimited number of profiles but are capped at sending 10 likes a day. There are no gender-based limitations on who is able to initiate chat conversations. Matches expire after 14 days; users can no longer view each others’ profiles or communicate through the app without rematching.

Profiles: Select Settings and click on the pencil below your profile image to change or delete the information displayed in your profile.

Settings: Select Settings > Account to enable notifications, log out of, and delete your account. Profiles cannot be hidden, or de-linked from Facebook or Instagram.

COFFEE MEETS BAGEL

Coffee Meets Bagel matches people based on profile criteria and linked Facebook data. It also takes into account geolocation, education, physical attributes, and past swiping tendencies to suggest compatible matches.

Use: The app shows users a limited number of compatible matches (“Bagels”) per day, which users swipe to match. Matches are directed to a chat room that is open for 7 days (time period can be extended with paid “beans”). Each day, users can record up to 8 seconds of video answering a “question of the day,” using this feature provides additional opportunities for matching.

Profiles: Navigate to My Profile to Edit Username, Edit My Profile, Manage Photos, and adjust Account Settings.

Settings: Select Account Settings to enable push notifications. Toggle OFF the Active membership status to hide your profile and prevent location sharing.
SECURE CHAT APPS

SECURE CHAT APPS - DO’S AND DON’TS

- Only establish and maintain contact with people you know and trust. Do not accept chat requests from unverified numbers or IDs.
- Do not send messages you do not want copied, screenshot, or re-posted by another user.
- Use all available PIN, password, and privacy protection options. Change passwords every three months to enhance security.
- Do not link your app to your social networking services (e.g., Facebook, Twitter), or permit the app to use your location.
- Provide the minimal amount of identity data required to register and use the app.
- Ensure that your contacts take similar security precautions. Review your contacts often.

WHAT ARE SECURE CHAT APPS?

Secure chat apps are designed to protect users’ electronic communications against surveillance from third parties. These apps can be downloaded from your device’s native provider (e.g., Android Play Store or iPhone App Store), and often only permit users to communicate with others who have previously downloaded the app. In general, secure chat apps afford users greater protection against eavesdropping by concealing the users’ identities or making the contents of the messages indecipherable to anyone except the intended recipient(s). As a result, using secure chat apps may potentially offer users two layers of security: anonymity and data security.

- **Anonymity**: Secure chat apps do not connect personally identifying information to messages and often require zero or limited identity data for account registration. They often offer private or public messaging to pseudonymous profiles and messages that expire after an allotted time.
- **Data Security**: Secure chat apps protect private messages and account information through specific message encryption methods, account settings, desktop support, or storing a limited collection of user data on the app provider’s servers.

VULNERABILITIES

As with any communication over the Internet or a cellular network, your personal data and messages are potentially at risk of being compromised. Though often anonymous and encrypted, secure messages and their senders’ identities are susceptible to the following vulnerabilities:

- App providers collect user content, contact lists, and usage information, and hold this information for an indefinite length of time. Some of this information may identify devices or users, and may be shared with affiliates and third parties.
- Messages not encrypted from end-to-end are susceptible to interception and decryption. Screenshots of communications also allow data leakage.
- App providers may elect to log user data for an indefinite amount of time. Data logging can allow the recovery of older communications.
- Some apps require a phone number for account registration. Minimize identity linkages by using a secondary or VOIP number, rather than your primary.

CHOOSING THE RIGHT SECURE CHAT APP

As a whole, secure chat apps afford users enhanced privacy. However, users may place themselves at unwanted risk if they do not take the time to research app capabilities and take proper precautions. Compare the capabilities of the four apps below to determine which may be best suited for your personal use.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>OS</th>
<th>DESCRIPTION</th>
<th>IDENTIFY DATA</th>
<th>SECURITY</th>
<th>LINKAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook Messenger</td>
<td>Android, iOS, Mac, Windows</td>
<td>Supports text/photo/video messages, voice/video calling, and sticker/audio/file exchange over the Internet or cellular networks. US-based. Optional encryption.</td>
<td>Sign up: Facebook Account OR Phone number/name/contacts Optional: Picture</td>
<td>Potential for anonymity: Optional end-to-end encryption Encryption Type: Open Whisper System's Signal Protocol</td>
<td>Social Network / Email: Facebook Device Permissions: Contacts, Phone, SMS</td>
</tr>
<tr>
<td>Telegram</td>
<td>Android, iOS, Linux, Mac, Windows</td>
<td>Cloud-based messenger supports text/photo/video messages, audio/file/sticker exchange. Syncs across devices; Secret Chat feature with temporary text messages. Based in Dubai (April 2018).</td>
<td>Sign up: Phone number, first name Optional: Last name, contacts, picture</td>
<td>Potential for anonymity: End-to-end encrypted messages (Secret chats) Encryption Type: MTProto with end-to-end encryption</td>
<td>Social Network / Email: None Device Permissions: Contacts, Storage</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>Android, iOS, Mac, Symbian, Windows</td>
<td>Supports encrypted test/photo/audio/video or audio/file/video exchange, and voice/video calling over the Internet and cellular networks. US-based.</td>
<td>Sign up: Phone number Optional: Name, picture</td>
<td>Potential for anonymity: End-to-end encrypted messages, secure calls Encryption Type: Open Whisper System's Signal Protocol</td>
<td>Social Network / Email: None Device Permissions: Contacts, Microphone, Storage</td>
</tr>
<tr>
<td>Signal</td>
<td>Android, iOS, Linux, Mac, Windows</td>
<td>Supports encrypted voice/video calls and texts/audio/photo/video message exchange over the Internet and cell networks. US-based.</td>
<td>Sign up: Phone number Optional: Name, picture</td>
<td>Potential for anonymity: End-to-end encrypted messages Encryption Type: Open Whisper System's Signal Protocol</td>
<td>Social Network / Email: None Device Permissions: Contacts, Phone, Storage</td>
</tr>
</tbody>
</table>
**FACEBOOK MESSENGER**

Facebook Messenger was originally developed as Facebook Chat in 2008 and become a standalone app in August 2011. It currently allows users to exchange messages, photos, videos, stickers, audio content, and files, as well as voice and video calls, using optional end-to-end encryption supported by Open Whisper System's Signal Protocol.

- Tap your profile photo to access settings. Under Profile > Active Status, turn OFF Show when you're active. To enable encrypted messaging, navigate to Preferences > Secret Conversations and turn ON Secret Conversations. When starting a new chat, toggle ON the Secret button (lock icon, upper right) prior to selecting the recipient. To use the expiring Conversations. When starting a new chat, turn ON navigate to turn OFF Show when you're active.
- Consider using a secondary phone number to create a Messenger account that is not linked to your Facebook account.
- Do not link Messenger with your SMS conversations or device contacts.
- Use Secret Conversations for all conversations, and periodically delete all conversations.

**WHATSAPP**

WhatsApp, owned by Facebook, is currently the most popular social messaging app, with 1.5 billion monthly active users. WhatsApp provides end-to-end encryption for messages, calls, and video chats, which ensures that no one, not even WhatsApp engineers, can intercept the communication method except for the sender and recipient. Group messaging can include up to 256 participants, while voice/video calls support up to 4 users. The Broadcast List option enables a user to send the same direct message to up to 256 recipients, rather than using Group Chat.

- Tap the Settings icon (bottom right) to apply the following changes to best maximize your security. Go to Settings > Account and apply the following options:
  - Under Privacy, set Who can see my personal info options to Nobody. Do not share your Status or Live location information.
  - Under Security, enable Show security notifications to view changes in contacts' security codes.
  - Enable Two-step verification to prevent outside access.
  - Periodically delete all conversations.

**TELEGRAM**

Telegram uses the cloud to synchronize messages across multiple devices. The app also offers a Secure Chat feature designed to prevent eavesdropping by employing end-to-end encryption and destroying messages after a set period of time. Secure chats, unlike standard Telegram messages, are stored locally on the device and cannot be forwarded to other devices or users.

- Consider using a secondary or VOIP phone number for registration. Do not provide your real name, a username, or a bio. Navigate to [upper left] > Settings > Privacy and Security and apply the following options:
  - Under Privacy, set Last Seen, Calls, and Peer-to-Peer Calls to Nobody. Set Groups to My Contacts, Save each change by tapping [upper right].
  - Under Security, establish a Passcode Lock and enable Two-Step Verification.
  - Under Advanced, set Delete my account if away for 6 months; accounts are free to make and there is no risk of losing contact information.
  - Under Contacts, disable Sync Contacts and Suggest Frequent Contacts.

**SIGNAL**

Signal supports end-to-end encrypted communication between users. In 2018, Signal rolled out a unique "Sealed Sender" feature that also encrypts message sender/recipient information. The app does not collect user metadata, nor does it store messages when you backup your device. Signal's encryption code is open-source and also used by companies like Facebook and Google. iPhone users can only contact those who have the app as well; Android users can contact anyone, but messages with non-Signal users are unencrypted.

- Consider using a secondary or VOIP number for account registration.

- Tap the icon and select Settings > Privacy. Apply the following options to best secure your conversations through the app:
  - Enable Screen Lock and set the inactivity timeout to 2 minutes.
  - Enable the Screen Security and Incognito keyboard features to limit opportunities for information collection.
  - Under Communication, enable Always relay calls to ensure communications do not reveal your IP address.
  - Manually delete your messages when your conversations are over.
  - Clear the app's history after each completed communication.
SMARTPHONES - DO’S AND DON’TS

- Protect your device with a strong alphanumeric password. Pattern locks can be strong but have a greater risk of being compromised.
- If available, enable hard-disk encryption on your device. iPhones and Android devices with recent OS upgrades may enable encryption by default.
- Limit accessing sensitive information from the lock screen, including call logs, emails, text messages, and voice assistant functions (Siri, Google Now).
- Malicious emails and texts can infect your phone with malware. Avoid messages with links from unknown parties; regularly run antivirus software.
- Cameras and microphones can be remotely activated; as a precaution, remove batteries before discussing any sensitive information.
- If available, restrict permissions to limit the personal data apps can access. Review what data (e.g., location) apps collect before downloading.

PROTECTING YOUR SMARTPHONE FROM PHYSICAL ACCESS AND MALWARE RISKS

Use these settings and recommendations to minimize security risks and protect your personal data. Feature availability can vary by OS version and device.

<table>
<thead>
<tr>
<th>RISK SCENARIO</th>
<th>IPHONE (V. 11.4.1)</th>
<th>ANDROID (V. 7.0)</th>
</tr>
</thead>
</table>
| SMARThONE IS PHYSICALLY ACCEssED BY sOMEBONE wITHOUT YOUR CONSENT | Install Find My Phone
  - Navigate to Settings > Touch ID & Passcode
  - Use BOTH Touch ID and passcode
  - Block access to phone data when locked
  - Turn ON Erase Data after 10 failed attempts | Install Find My Device
  - Navigate to Settings > Lock screen and security
  - Use a mix of PIN, pattern lock, or biometrics
  - Go to Settings > Display > Screen Timeout

<table>
<thead>
<tr>
<th>RECOMMENDATIONS TO MINIMIZE PHYSICAL ACCESS AND MALWARE RISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Immediately install smartphone operating system updates and security patches. Keep all apps updated to maximize protection.</td>
</tr>
<tr>
<td>- Never jailbreak or root smartphones. Jailbroken/rooted phones allow malicious apps to bypass device security protocols and alter device software.</td>
</tr>
<tr>
<td>- Only install apps from the official Apple or Google Play store. On Android, ensure Settings &gt; Lock screen &amp; security &gt; Unknown sources is turned OFF.</td>
</tr>
<tr>
<td>- Record IMEI number to identify device if lost/stolen. iPhone: Settings &gt; General &gt; About &gt; iPhone</td>
</tr>
<tr>
<td>- Wipe data on device before discarding, donating, recycling, or selling it. Transfer SIM card to new device or destroy it.</td>
</tr>
<tr>
<td>- Change passwords on your phone frequently (approximately every 3 months) to maximize security.</td>
</tr>
</tbody>
</table>

SMARTPHONES - DO’S AND DON’TS
Smartphones communicate personal data across a variety of networks and apps. Follow these steps to best protect your identity data in one of the following four common smartphone use case scenarios. Availability of suggested settings may vary by OS version and type of phone.

<table>
<thead>
<tr>
<th>USE CASE</th>
<th>IPHONE (V. 11.4.1)</th>
<th>ANDROID (V. 7.0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONNECTING TO WIRELESS NETWORKS</td>
<td>Information transmitted via public Wi-Fi networks can be intercepted by third parties. Avoid using public wireless networks when possible, and always use a VPN client, such as Shrew Soft VPN (<a href="http://www.shrew.net">http://www.shrew.net</a>) to encrypt your mobile activities.</td>
<td>Navigate to Settings &gt; Connections &gt; Wi-Fi to enable and establish a VPN connection. Select the gear icon to configure Wi-Fi (feature varies by Android model) and select Never under “Keep Wi-Fi on during sleep.”</td>
</tr>
<tr>
<td>CONNECTING VIA BLUETOOTH</td>
<td>Bluetooth involves the wireless communication of two devices within a close geographical proximity. When Bluetooth is enabled, hackers may be able to exploit the connection to access your calendars, emails, messages, and photos without your knowledge. Avoid using Bluetooth and disable it when not in use.</td>
<td>Navigate to Settings &gt; Connections &gt; Bluetooth to disable services. Navigate to Settings &gt; Connections &gt; NFC and payment to manage Near Field Communications, which enables smartphones to transfer data by touching the devices together.</td>
</tr>
<tr>
<td>DATA RETAINING APPS</td>
<td>Downloaded apps frequently collect personal information to sell to advertisers or third-party data aggregators. Native applications such as Siri and Google Now may also collect data from users, which may include device information or audio from the device. However, many devices allow users to restrict the personal information or permissions that apps can access. Set strict limits to protect personal information.</td>
<td>Navigate to Settings &gt; Apps &gt; &gt; App permissions. Restrict excessive requests for personal data. Navigate to Settings &gt; Apps &gt; Google &gt; Ads. Turn ON.</td>
</tr>
<tr>
<td>APPS USING REAL-TIME LOCATION</td>
<td>Many apps will ask permission to track your real-time location. Users should avoid granting permission to these apps when possible, and turn off all location tools when they are not in use. Additionally, pictures taken with smartphones may retain location information inside their EXIF data, and location will be shared along with the photos once they are uploaded to a website or SNS. One exception to this rule is with device locating apps for loss and theft such as “Find My iPhone” or “Find my device”.</td>
<td>Navigate to Settings &gt; Location. Disable all location services when not in use. Turn OFF Google location history. Turn OFF Google location sharing. Turn OFF Google Web and App Activity.</td>
</tr>
</tbody>
</table>
## TRAVELING WITH SMARTPHONES

**TRAVELING WITH SMARTPHONES - DO'S AND DON'TS**

- Bring a dedicated loaner device when you travel overseas; do not bring your personal smartphone.
- Make sure your device is running the latest software; this will help protect you against any new technical vulnerabilities.
- Assume that all information on your device can be compromised while traveling in a foreign country; leave sensitive information off of your phone.
- Use a VPN to protect your phone when accessing Wi-Fi networks in a foreign country.
- Use anti-virus services to ensure that your phone is protected from malware.
- Password-protect your device and set your phone to lock automatically when not in use.

## ENSURE THAT YOUR PHONE’S SOFTWARE IS UP-TO-DATE

Ensure that the software on your smartphone is up-to-date. This will offer you the latest protection against newly discovered technical vulnerabilities.

### iPhone (V. 11.4.1)

- Go to Settings > General > Software Update. Check to see if your software is up-to-date.
- If your software is not up-to-date, your iPhone will prompt you to download the latest software.

### Android (V. 7.0)

- Go to Settings > Software update > Check for updates
- Confirm current software is up-to-date. If not, follow Android prompts to download and install the latest software.

## PROTECT YOUR PHONE AGAINST MALWARE

Like a computer, your phone is vulnerable to malware and malicious apps. Use anti-virus apps to ensure that your phone is protected.

### iPhone (V. 11.4.1)

- Use the Lookout app for iPhone. Go to Security to see if your phone has any malicious apps.
- Lookout checks your apps for malicious activity that can compromise the security of your phone and personal information.

### Android (V. 7.0)

- Use the Avast Antivirus Free app for Android. Click Scan Now to monitor for viruses.
- Avast also offers the option to scan Wi-Fi networks for threats.

## SET YOUR PHONE TO LOCK AUTOMATICALLY AND SET A COMPLEX SCREENLOCK PASSWORD

In case you lose your device, you want your smartphone to lock automatically to prevent physical access. Use a complex password to protect your phone.

### iPhone (V. 11.4.1)

- Go to Settings > Touch ID & Passcode. Turn on all Touch ID options and set Require Passcode to immediately.
- Go to Settings > Display & Brightness > Auto-Lock. Set the Auto-lock to 30 seconds.

### Android (V. 7.0)

- Go to Settings > Lock screen and security > Screen lock type to enable password protection. Choose between pattern, PIN, password, and fingerprint.
- Go to Settings > Display > Screen timeout and select the shortest timeout option available.
DISABLE WI-FI AND BLUETOOTH

Disable Wi-Fi and Bluetooth on your smartphone when you are not using them; Wi-Fi and Bluetooth can render your smartphone vulnerable to malware.

**IPHONE (V. 11.4.1)**

Go to Settings > Wi-Fi. Turn Wi-Fi OFF.

Go to Settings > Bluetooth. Turn Bluetooth OFF.

**ANDROID (V. 7.0)**

Go to Settings > Connections > Wi-Fi. Turn Wi-Fi OFF.

Go to Settings > Connections > Bluetooth. Turn Bluetooth OFF.

USE VPN ON WIRELESS NETWORKS

Virtual Private Networks—or VPNs—allow you to extend a private network across a public network such as public Wi-Fi. Using a VPN will make it more difficult for malicious individuals to eavesdrop on your Internet traffic. Use a VPN service such as SurfEasy VPN or Avast SecureLine to protect yourself.

**IPHONE (V. 11.4.1)**

Use VPN services such as SurfEasy and Avast SecureLine VPN for iOS to protect yourself on Wi-Fi.

**ANDROID (V. 7.0)**

Use VPN services such as SurfEasy for Android to protect yourself on Wi-Fi.

RECOVER LOST OR STOLEN SMARTPHONE AND WIPE DATA

Find My iPhone and Avast can locate lost phones, wipe data remotely from lost phones, and provide contact information to return a lost device.

**IPHONE (V. 11.4.1)**

Use the Find My iPhone app to recover lost or stolen iPhone smartphones.

**ANDROID (V. 7.0)**

Use the Avast app to recover lost or stolen Android smartphones and wipe data remotely from the device.
EXIF DATA REMOVAL

EXIF REMOVAL - DO'S AND DON'TS

- Remove EXIF data before sharing images with people or posting them online, especially when images are captured in private homes or businesses.
- Use an EXIF viewer to verify that personal data has been removed from photos before sharing and prevent your phone from including location tags.
- Before uploading images, use available privacy settings to limit the audience to only you or close friends and family.
- Minimize the use of apps that automatically upload and share captured images (e.g., Google Photos, Flickr).
- Even without EXIF data, the image content may contain identifying information, such as associated persons or location histories. Screen content with the assumption that anyone can see, copy, or forward photos that you post online.

EXIF DATA

Exchangeable Image File Format (EXIF) is a standard format for storing and exchanging image metadata. Image metadata is included in a captured image file and provides a broad range of supplemental information. Some social networks and photo-sharing sites, such as Flickr, Google Photos, and Instagram, have features that share EXIF data alongside images. Others, including Facebook and Twitter, do not share EXIF data but may utilize the information internally. EXIF data is stored as tags, some of which reveal unique identifying information.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>IMPORTANT TAGS</th>
<th>IDENTITY IMPLICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geolocation</td>
<td>GPSLongitude, GPSLongitudeRef, GPSLatitude, GPSLatitudeRef, GPSDateStamp, GPSTime Stamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod</td>
<td>Ability to reveal the exact location of private places, such as homes or offices. Some photo sharing sites, including Google Photos and Flickr, publicly display image GPS coordinates on a map.</td>
</tr>
<tr>
<td>Timestamps</td>
<td>ModifyDate, DateTimeOriginal, CreateDate</td>
<td>Creates a log of behavioral patterns and personal timelines.</td>
</tr>
<tr>
<td>Camera</td>
<td>Make, Model, Serial Number</td>
<td>A unique serial number identifies the device used to capture an image or sets of images.</td>
</tr>
<tr>
<td>Authorship</td>
<td>Artist, Owner Name, Copyright</td>
<td>Links images with a name or organization.</td>
</tr>
<tr>
<td>Image Summary</td>
<td>ImageDescription, UniqImageID, UserComment</td>
<td>Potentially reveals identifying information about those captured in the image by providing additional content regarding persons and locations.</td>
</tr>
</tbody>
</table>

Limiting EXIF data, especially geolocation information, before distributing image files can help protect your identity from overexposure. This should be done in two stages: 1) preventing your smartphone from storing the identifying EXIF data in image files, and 2) removing existing EXIF data from image files using an EXIF removal application.

PREVENTING THE CAPTURE OF GEOLOCATION DATA

- Taking a screenshot of a photo from a phone running an operating system newer than iOS 7 or Android Jelly Bean will create a brand new image that contains no EXIF data. To take a screenshot on an iOS device, simultaneously press the lock and home buttons; with a Galaxy or Note, press the power and home buttons simultaneously, or swipe your hand from left to right across the screen; with a Google Pixel, simultaneously press and hold the lock and volume down buttons for 2 seconds.
- Turn off geolocation data capture using your smartphone's camera application [shown below]. Note that photos taken in airplane mode still contain geolocation data.
- When uploading or sharing photos, remember that EXIF data and image quality have no correlation. Lower quality images still contain EXIF data.

IOS (V. 12.1.3)

Turn off iOS location services to ensure images captured with the native iPhone camera app will not contain any geolocation EXIF data.

1. Select the Settings app and navigate to Privacy > Location Services.
2. Turn off location services altogether or for the iPhone's Camera application.
3. Return to the Settings app and navigate to Privacy > Photos.
4. Disable permissions for other apps to access photos already stored in your iPhone’s Camera Roll.

ANDROID (V. 9.0)

Turning off location storage in the Android Pie camera application prevents captured images from containing EXIF data.

1. Open the Camera app and select More
2. Tap the white gear icon to access Settings
3. Under General, toggle OFF Save location
EXIF REMOVAL SOFTWARE

EXIF Viewer LITE BY FLUNTRO

EXIF Viewer LITE is a free, iOS app where you can view, delete, and edit EXIF data of images stored on your Apple devices. The app can also remove or edit EXIF data on multiple photos at once. The full version of the EXIF Viewer is available for purchase at $2.99.

1. Download the EXIF Viewer Lite from the App Store.
2. Open the NoLocation app and select photo(s) to view all their available EXIF data. From here, you can:
   - Select Remove Location to quickly remove location data on your photos. Other EXIF data will be preserved.
   - Select Remove EXIF to strip all the available EXIF data from your photos.
   - Select Edit EXIF to change the EXIF data on your photo by editing its date, time, and location.
3. Finalize changes by approving the app to make changes to your photos.

VIEWING AND REMOVING EXIF DATA ON OS X

Use the ImageOptim application (available at http://imageoptim.com) to remove EXIF data on your OS X computer.

1. Open the ImageOptim application.
2. Drag the photos selected for EXIF removal into the application window and wait for a green check mark to appear next to the file name.
3. Check that the EXIF data has been removed by right-clicking the image and selecting Get Info. EXIF data is listed under More Info.

VIEWING AND REMOVING EXIF DATA IN WINDOWS

Use the Windows 10 operating system on your computer to verify EXIF data has been successfully removed.

1. Navigate to an image in File Explorer, right-click the image, and select Properties.
2. In the Properties window, select the Details tab.
3. Most EXIF data, including geolocation, can be located in the Details tab if they are embedded inside the image file.
4. Windows 10 also allows system administrators to remove all EXIF data from the selected image by clicking the Remove Properties and Personal Information link.

PHOTO EXIF EDITOR - METADATA EDITOR

Photo EXIF Editor - Metadata Editor is a free app that deletes all EXIF data from image files stored on your Android devices.

1. Download Photo EXIF Editor from the Play Store and allow media access permissions.
2. Open the Photo EXIF Editor app and select Photos.
3. Navigate your device gallery and select an image.
4. Tap the EXIF Erasure icon on the upper right corner, select all tags for removal, and tap the save icon. Scroll down to review EXIF data has been removed; you can make manual adjustments to certain fields if desired.
5. An EXIF-free image file with an updated date and time stamp will be saved in place of the original, which can then be shared using your Gallery or SNS apps.
MOBILE WALLETS

MOBILE WALLETS - DO’S AND DON’TS

- Use all available PIN, password, and biometric protection options.
- Turn on notifications and regularly monitor transaction history for unauthorized payments.
- Only transfer money to people or merchants you know and trust, and establish a maximum transaction limit to monitor large purchases and transfers.
- Do not link your mobile wallet application to a social networking service (e.g., Facebook, Twitter).
- Link a bank account only to cash-out; delete bank account information once the cash-out process has completed.
- Before signing up, always research if a mobile wallet service provider has a good or bad track record in handling users’ privacy and data.

WHAT ARE MOBILE WALLETS?

Mobile wallets allow you to link credit cards, debit cards, and bank accounts to complete one or both of the following transaction types:

- **User to friend**: Allows you to transfer money to friends using their email address or phone number. Money is stored in a balance within the mobile application. You can use this balance for further transfers or deposit it into your bank account.
- **User to merchant**: Allows you to pay for goods and services online or at the point-of-sale using a QR code or NFC chip (near field communication). You can pay by selecting a specific card, account, or existing balance, if available.

Most mobile wallets from different companies do not interact with each other; for example, you cannot transfer money from Google Wallet to a friend with Venmo. Given that different mobile wallets perform distinct functions, you may choose to maintain multiple wallets.

BENEFITS OF MOBILE WALLETS

Mobile wallets are primarily designed to provide convenience. They allow you to quickly settle debts with friends wherever you are, without cash or checks. Mobile wallets can also consolidate many credit cards, debit cards, bank accounts, loyalty cards, and gift cards into a single app on your mobile device.

On most smartphones, fingerprints can be used as a purchase authentication method, enhancing your security over a physical credit or debit card.

Consolidating multiple cards into a single app increases your risk exposure. Physically losing possession of your phone may allow an unauthorized user to make payments with any linked card or account. Unauthorized users will also have access to consolidated transaction logs, exposing a wide range of your financial habits and activities.

Most wallets are also accessible through a web browser. Although cards may physically be in your possession, unauthorized access to your online wallet account will expose your personal information and activity, and also put your money at risk for theft.

Some mobile wallets offer social features, such as an activity feed of friends’ transactions or the option to post transactions to Facebook. Without strict privacy settings, social features expose your activity and potentially even your whereabouts.

CHOOSING THE RIGHT MOBILE WALLET

You should consider the following questions when choosing a mobile wallet:

- What operating system do you have?
- Are you transacting with your friends or paying merchants?
- What security features do you require?
- Do you want social options? Do you want the ability to limit social options?

Six of the most popular mobile wallet services are outlined below.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>OS</th>
<th>TRANSACTION TYPE</th>
<th>REQUIRED IDENTITY DATA</th>
<th>SECURITY OPTIONS</th>
<th>SNS LINKS</th>
<th>DEFAULT VISIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Square Cash</td>
<td>iOS, Android</td>
<td>User to friend</td>
<td>Phone or email, full name, zip code, SCash (unique payment name)</td>
<td>PIN</td>
<td>None</td>
<td>$Cashtag (can be hidden)</td>
</tr>
<tr>
<td>Apple Pay</td>
<td>iOS</td>
<td>User to friend, User to merchant</td>
<td>Full name, billing address, shipping address, email, phone number, debit/credit card data</td>
<td>Fingerprint or face required for transactions</td>
<td>Send money directly to contacts using iMessages</td>
<td>None</td>
</tr>
<tr>
<td>Google Pay</td>
<td>iOS (in-store payments not supported), Android, browser</td>
<td>User to friend, User to merchant</td>
<td>Full name, email, bank account, debit/credit card data</td>
<td>PIN, fingerprint</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Venmo</td>
<td>iOS, Android, browser</td>
<td>User to friend, User to merchant</td>
<td>Full name, email, phone number, bank account or debit/credit card data</td>
<td>PIN, fingerprint</td>
<td>Facebook (optional), internal social features</td>
<td>Friends (can set to private)</td>
</tr>
<tr>
<td>PayPal</td>
<td>iOS, Android, browser</td>
<td>User to friend, User to merchant</td>
<td>Nationality, full name, email, address, phone number, bank account data or credit/debit card data</td>
<td>Password, fingerprint</td>
<td>None</td>
<td>Private</td>
</tr>
</tbody>
</table>
SQUARE CASH

Navigate to Settings in the upper left portion of the home screen:

- Require Security Lock to transfer funds.
- Under Personal, add your Email Address or Mobile Number for account verification.
- Under Notifications, enable push and email notifications.
- Under Privacy, toggle "Cash.me" to OFF.

Users can link cash to a custom Visa debit card available through the app, or purchase/sell Bitcoin to use in transactions. An activity log is located in the upper right portion of the home screen. Monitor this section for unauthorized transactions.

APPLE PAY - IPHONE ONLY

In the iPhone Settings > Wallet & Apple Pay menu, add/remove credit or debit cards you wish to use with Apple Pay:

- Toggle "Apple Pay Cash" ON to enable direct money transfers with your contacts.
- Turn OFF "Double-Click Home Button" to limit access to Apple Pay when your phone is locked.
- Turn OFF "Allow Payments on Mac" to minimize risks of an unauthorized person making a purchase on your computer.

Enable PIN, password, or fingerprint protection for your iPhone’s lock screen. Use more than one of these options to ensure extra security.

GOOGLE PAY

Navigate the dropdown menu to Settings:

- Under Security, turn ON "Require PIN".
- Set Auto-lock to 15 minutes.
- Enable Fingerprint/Touch ID.
- Under Notifications, turn ON notifications for payments.
- Check monthly statements for unauthorized transactions.
- Monitor the Transactions section of the sidebar for unusual activity.

iPhone users: Navigate to your phone’s Settings > Privacy > Location Services and set Wallet location access to Never.

Android users: Navigate to Google Pay Settings > Permissions to disable location tracking for Google Pay.

VENMO

Navigate the dropdown menu to Settings:

- Under Privacy, select Private.
- Under Notifications, enable push notifications for all Payments and Activity options.
- Review Remembered Devices to check for suspicious log-ons.
- Under Friends & Social, do not connect Facebook or Phone Contacts.

PAYPAL

Log in to PayPal using your browser and navigate to Settings:

- Use the Security tab to configure Security questions, Mobile PIN, and Security key options.
- Under the Notifications tab, configure email and/or text notifications for all account activities.
- Do not provide SSN or Passport numbers.
- Review account Activity routinely to monitor for suspicious activity.

Mobile: Under Settings > Login and Security, toggle OFF "Remember Me" to prevent account information from being accessed prior to login.

PayPal can now be linked with Google Pay.

MOBILE WALLETS - BEST PRACTICES

To protect yourself while using mobile wallets, use the following guidance:

- Avoid accessing mobile wallets on public Wi-Fi networks.
- Use privacy settings to restrict the social features of mobile wallets, so only you can see account activity.
- Turn ON transaction alerts to receive email or text notifications of any transaction.
- Only provide personal or financial information that is required for mobile wallet use.
- Restrict permissions to your device contacts and settings.
- Never send or receive money from strangers or unverified accounts.

Identity Awareness, Protection, and Management Guide
A fitness tracker (a.k.a. activity tracker) is a popular consumer device or application used for monitoring and recording a person's fitness-related metrics such as distance walked or run, calorie burn, heartbeat, and quality of sleep. It is usually a type of wearable biosensor, an electronic device worn on the body as an accessory, equipped with sensors that convert biological elements into a signal input. Fitness trackers have reached mainstream adoption worldwide, with user penetration hitting 11.7% of the US population in 2018. The most common fitness tracker form factor is a wristband worn on the body as an accessory, equipped with sensors that convert biological elements into a signal input. Fitness trackers have reached mainstream adoption worldwide, with user penetration hitting 11.7% of the US population in 2018. The most common fitness tracker form factor is a wristband intended to be worn all day to measure physical activity and body functions through the 24-hour cycle.

Most wearables are used for fitness, wellness, and sleep tracking. All fitness trackers come with an accompanying smartphone or desktop app that provide useful insights and metrics. Although physical sensors in most fitness trackers are similar, the algorithms that interpret outputs are unique to vendors. User health and fitness data is transmitted via a Bluetooth, Wi-Fi, or near-field communication (NFC) connection to a computing device. The type of fitness tracker you choose depends on your budget and comfort level with sharing physical and activity data with the technology provider. The privacy considerations for each service is outlined below.

### HOW PEOPLE TRACK HEALTH & FITNESS

Most users track and analyze their health and fitness data in one of the three following ways:

- **Native apps**: Native fitness-tracking apps are native to the smartphone’s operating system (OS). They are developed by smartphone manufacturers, and analyze movement and inputs from the smartphone. They are the least privacy-invasive and accurate of the options. Examples include Apple Health and Samsung Health.

- **Hardware-independent apps**: Hardware-independent fitness-tracking apps aggregate inputs from different fitness-tracking devices and smartphones to create a comprehensive profile of user’s health and activities. These apps are device- and hardware-independent. They rely on user input data as well as data linked from other physical trackers using custom application programming interfaces (APIs). Examples include Google Fit and MyFitnessPal.

- **Hardware-dependent apps**: Hardware dependent fitness-tracking apps accompany and analyze data from a specific brand of wearable fitness tracker. Hardware and the accompanying app are developed by the same company. They provide the most comprehensive and accurate monitoring of your health and fitness, as the accompanied hardware is expected to be worn by the user at all times. Examples of this are Fitbit and Garmin Connect.

The type of fitness tracker you choose depends on your budget and comfort level with sharing physical and activity data with the technology provider. The privacy considerations for each service is outlined below.

### HEALTH APPS & FITNESS TRACKERS - DO’S AND DON’TS

- Do not connect your SNS accounts with your health and fitness profiles and apps. Ensure any social features are turned off.
- Provide minimal registration data during device setup; only complete required fields, and use your initials or an anonymous username when possible.
- Only enable connections during device data transmission; ensure they are disconnected when not in use.
- Frequently review permissions granted in your health and fitness apps under privacy settings. Sometimes permissions change without user notice.
- Research how to request archives and delete your health and fitness data with the wearable manufacturer before beginning to use the device.
- Limit the number of Internet of Things (IoT) and smart devices connected to the fitness-tracking device.

### HEALTH & FITNESS APPS

<table>
<thead>
<tr>
<th>HEALTH &amp; FITNESS APP</th>
<th>OS</th>
<th>COST</th>
<th>FITNESS DATA INPUT SOURCES</th>
<th>THIRD-PARTY DATA SHARING</th>
<th>BUILT-IN SNS LINKS</th>
<th>IDENTITY DATA</th>
<th>DEFAULT SHARING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APPLE HEALTH</strong></td>
<td>iOS only</td>
<td>Free</td>
<td>iPhone, Apple Watch, third-party apps (e.g., FitBit)</td>
<td>Shares health and fitness data with other iOS apps</td>
<td>None</td>
<td>Name, birthdate, weight, height, emergency contacts</td>
<td>Private</td>
</tr>
<tr>
<td><strong>SAMSUNG HEALTH</strong></td>
<td>Android only</td>
<td>Free</td>
<td>Android devices; third-party fitness trackers, medical sensors, scales</td>
<td>Shares health and fitness data with partner apps</td>
<td>None</td>
<td>Email address, birthdate, gender, height, weight</td>
<td>Private</td>
</tr>
<tr>
<td><strong>GOOGLE FIT/WEAR OS</strong></td>
<td>Android, iOS</td>
<td>Free</td>
<td>Android devices, third-party apps and devices, Google Fit apps and devices</td>
<td>Shares health and fitness data with connected apps and devices</td>
<td>None</td>
<td>Email address, gender, height, weight, high-accuracy location</td>
<td>Private</td>
</tr>
<tr>
<td><strong>MYFITNESSPAL</strong></td>
<td>Android, iOS</td>
<td>Free, Premium at $9.99 per month</td>
<td>Compatible with many popular health apps (e.g., Garmin Connect, Fitbit, Strava, Glow)</td>
<td>Shares data with other health apps (e.g., Apple Health, Garmin Connect)</td>
<td>Facebook</td>
<td>Name, email address, profile photo, location, zip code, height, gender, weight, birthdate</td>
<td>Private</td>
</tr>
<tr>
<td><strong>FITBIT</strong></td>
<td>Android, iOS, Windows</td>
<td>Free app, hardware $50-260</td>
<td>Fitbit fitness trackers</td>
<td>Shares data with compatible third-party apps</td>
<td>None</td>
<td>Name, display name, birthdate, gender, height, weight, place</td>
<td>Varies by data type</td>
</tr>
<tr>
<td><strong>GARMIN</strong></td>
<td>Android, iOS, Windows</td>
<td>Free app, hardware $50-560</td>
<td>All Garmin fitness trackers and smart watches</td>
<td>Shares fitness data with any apps using Garmin Connect API</td>
<td>No direct link to SNS, can share activities as web links</td>
<td>Name, profile photo, location, gender, height, age, birthdate</td>
<td>“My Groups and Connections”</td>
</tr>
</tbody>
</table>
The Medical ID option shares personal data and is not required to access app features. Do not create one, or delete one if you already have one. If you already created Medical ID, navigate to the Medical ID tab at the bottom:

- Select Delete Medical ID at the bottom.
- If you wish to maintain Medical ID, toggle OFF Show When Locked.

Navigate the upper-right drop-down menu to Settings:
- Under General select Password > Set password to protect your Samsung Health data.
- Under Advanced, toggle OFF Together to keep your data private.

Navigate the upper-right profile icon to access your profile page. Do not add a photo or a Nickname.

To delete existing data: use Manage your data > Manage All Data or delete Activities and Location data.
- Manage activity tracking (steps and distance) by setting Track activity metrics to ON or OFF as needed.

Use the upper-right profile icon to access your profile page. Do not add a photo or a Nickname.

Navigate to the More tab > Settings > Sharing & Privacy. Implement data-protective settings suggested below. Do not link your Facebook account.

On your phone, navigate to Settings > Apps > Fit > Permissions, and toggle the Location permission OFF. Leaving location tracking enabled allows Google Fit to precisely map your daily activities, which may reveal sensitive information about your whereabouts.

Navigate the upper-right drop-down menu to Settings.
- Under General select Password > Set password to protect your Samsung Health data.
- Under Advanced, toggle OFF Together to keep your data private.

Toggle OFF

Unselect ALL

Set to "Only Me"

REVOKE ACCESS to all extra data sharing options

Navigate to the More tab > Settings > Profile & Privacy.
- Set privacy settings of your Garmin profile and activities to "Only Me."
- Toggle OFF all personal data shown on your profile.
- Navigate to Data, revoke access to all additional data sharing.

Use initials & general location

Review each category

Set to "Only Me"

Toggle OFF

Use the upper-right profile icon to access your profile page. Do not add a photo or a Nickname.

Navigate to the More tab > Settings > Sharing & Privacy. Implement data-protective settings suggested below. Do not link your Facebook account.

On your phone, navigate to Settings > Apps > Fit > Permissions, and toggle the Location permission OFF. Leaving location tracking enabled allows Google Fit to precisely map your daily activities, which may reveal sensitive information about your whereabouts.

- To delete existing data: use Manage your data > Manage All Data or delete Activities and Location data.
- Manage activity tracking (steps and distance) by setting Track activity metrics to ON or OFF as needed.
Securing Home Wi-Fi Network

Securing Home Wireless Network - Do's and Don'ts

- Use an ethernet cable instead of a Wi-Fi connection when possible; disable the wireless network when it won't be used for an extended period of time.
- Use the most up-to-date hardware and operating systems to maximize your connecting device's security options.
- Turn on automatic updates for your network devices' firmware or periodically check for updates on the network devices' websites.
- Determine whether you have a router and modem, a hybrid router-modem, or just a modem to best secure your network.
- Enable your device's firewall and implement strong encryption to block various techniques used by unauthorized individuals to access your network.
- Secure mobile devices that can access your home network; establish screen locks to ensure that stolen devices cannot reconnect to your network.

Overview

Home wireless networks allow users to connect multiple devices to a single, remote Internet network. While wireless technology makes it easier for users to access the Internet, it also opens the door to new security threats not present in hard-wired connections. Failure to take the proper precautions when configuring your home wireless network may leave your personal information and Internet traffic susceptible to unauthorized individuals. Use the recommendations outlined in this card to secure your home wireless network and better protect your privacy.

Wireless Network Basics

A home wireless network consists of a modem, a router, and a selection of personal electronic devices. Unlike Local Area Networks (LAN)—networks requiring all devices to be linked together via network cables—a home wireless network broadcasts radio waves from a router to allow wireless devices to communicate with one another. When the router receives communications from personal devices, the data is then passed through a hard-wired connection to the modem and onto the Internet service provider.

Depending on your particular Internet Service Provider (ISP), geolocation, and Internet package, you may not own all the hardware components of a home wireless network. Technology advancements enable some companies to sell router-modem hybrids, reducing the number of necessary devices. In other scenarios, some ISPs establish relationships with residential complexes so that everyone in a building must use their service and thus, don't provide routers.

If you have a router, you must first gain access to your router to initiate the necessary security settings. Launch any web browser and enter the default IP address of your wireless router into the URL bar. Next, enter the default username and password for your router into the prompt. If you are unaware of your default IP address, password, or username, reference http://www.routeripaddress.com to determine your router's specific details. Even without a router, you can use the information in this chapter to secure your home wireless network.

Preventing Third-Party Access to Your Wireless Network

Some ISPs, such as Comcast XFinity or Verizon FiOS, offer roaming Wi-Fi hotspot services, which allows users to access the Internet on their mobile devices at faster speeds than normally available. These services often use bandwidth from the in-home wireless networks of nearby subscribers. If your ISP offers this type of service, call the company directly to opt out.

What to Do If You Suspect Your Network Has Been Compromised

Following the recommendations outlined in this card will significantly reduce your home network’s chances of becoming compromised. However, it is wise to periodically check if there has been any unauthorized activity on your network. Within the router’s web interface, locate the section that identifies the devices connected to your network (e.g., Attached Devices, DHCP Clients Table, Connected Devices, etc.). If you see an unknown device accessing your network, end the connection, and consider contacting your Internet service provider to determine if your network was compromised. If you determine that your network was accessed unlawfully, immediately change the usernames and passwords to the wireless network and administrative login pages. Also remember to check and re-secure other online accounts including online banking, social media, and email accounts. If your network was compromised it is possible that the hacker may have been able to see your Internet traffic and gain access to your login credentials or other personal data.

Wireless Settings Overview

Follow these steps in order to secure your home wireless network and prevent third-party hackers, neighbors, and scammers from accessing your personal data. The settings in this card apply whether you have a router or not. For router-specific instructions, go to https://routersecurity.org/.

Changing Device/Account Login Settings

Whether you have a router or simply a modem, your ISP account comes with a default username and password setting, (e.g., Username = "Admin" and Password = "Password") so that anyone can login to their settings for the first time. Once you have logged into your device settings, by going through your ISP or reading your devices’ manual, change the defaults to enable additional security. Usernames should not represent your name, home address, or any other personal identity data. Passwords should be unique, alphanumeric combinations with at least 12 characters.
**Choosing Strong Encryption**

To maximize the security of your network, select WPA2-PSK (AES) as your primary security mode, if possible. WPA2 is the strongest form of encryption used to protect wireless networks, while AES is an encryption standard trusted by government organizations to protect sensitive information. The table below shows available encryption types and their associated strengths. Make sure to combine strong encryption protocols with the additional security of a password. This will make it less likely that outsiders can eavesdrop on your Internet activities.

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Privacy Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPA2-PSK (AES)</td>
<td>Maximum</td>
</tr>
<tr>
<td>WPA2-PSK (TKIP)</td>
<td>Minimal (older devices only)</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>Weak or None</td>
</tr>
<tr>
<td>WEP</td>
<td>Weak or None</td>
</tr>
</tbody>
</table>

**Encryption Privacy Strength**

**MAC Address Filtering**

MAC address filtering allows the administrator to create a list of approved devices that can access the network. Devices not on this list are denied access or have to request it from the administrator. MAC addresses are not discoverable through the settings; search for ways to retrieve your personal devices’ MAC addresses based on their operating systems.

**Setting Up a Firewall**

A firewall is a network security system that controls incoming and outgoing network traffic based upon predetermined security rules. The firewall can block a number of techniques commonly used by unauthorized individuals to compromise and access networks. Always enable firewall settings to secure your home network. Use the maximum security settings available whenever possible.
ONLINE REGISTRATION

ONLINE REGISTRATION - DO'S AND DON'TS

- Remember that even if you restrict your data from public view, the service still has access to your data and may share it with third parties.
- Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- Never give online services access to your Social Security Number or physical address.
- Do not upload or share your existing contacts with a social networking service (SNS) during registration.
- Remove any identity data from your personal profile that was required during sign-up after completing the registration process.
- Change privacy settings to protect your identity information immediately after registering for an online profile.

IDENTITY DATA IN SOCIAL NETWORKING SERVICE (SNS) ACCOUNTS

Online identity can be described as an aggregate of accounts and account-related activities associated with a single person. Common identity elements required by social networking services (SNS) in exchange for 1) creating accounts and 2) participating in their services and features are shown below.

FIRST AND LAST NAME

First and last names are mandatory for almost all SNS accounts. When possible, use your initial instead of your full last name, especially if it is uncommon.

USERNAME

Usernames are unique to each user account, and are used to identify specific individuals within a network. When making your username, do not include personally identifiable information (PII), such as your name, location, or birthday.

Do not use the same password or username across multiple SNS accounts. Ensure that your passwords are complex and unique. Include numbers and special characters.

BIRTHDAY

Birthdays are used to verify the user's age and customize age-appropriate content on the site. This information is sometimes published on the SNS profile and has to be removed retroactively. Don't share your full birthdate unless it's required.

EMAIL ADDRESS

Email accounts are ubiquitous in online registration. Consider creating a unique email address for each SNS account you register.

EMPLOYMENT INFORMATION

With the exception of professional-oriented SNS services, company and employment information are often optional data fields. When providing work information, try to be as generic as possible (i.e. only provide the industry you work in). Avoid posting your employer and your work location.

SOCIAL LOGIN

Services may allow users to sign up through preexisting SNS accounts (e.g., Google Plus, Twitter, or Facebook) by importing your existing data. Avoid using social login whenever possible.

MOBILE PHONE NUMBERS

Increasingly, accounts may ask to verify your identity using a phone number. Refrain from using services that require phone numbers or opt to use an alternative method to verify accounts.

RELATIONSHIPS/ORIENTATION

Relationship status and sexual orientation are almost always optional data fields, except for online dating sites. Refrain from sharing this data with the service unless it is required.
IDENTITY FIELDS DURING REGISTRATION, BY SERVICE

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Outlook</th>
<th>Yahoo</th>
<th>Facebook</th>
<th>Twitter</th>
<th>Google</th>
<th>LinkedIn</th>
<th>Pinterest</th>
<th>Instagram</th>
<th>Yelp</th>
</tr>
</thead>
<tbody>
<tr>
<td>First and last name</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Username</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Birthdate</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Optional</td>
<td>✓</td>
</tr>
<tr>
<td>Email address</td>
<td></td>
<td></td>
<td></td>
<td>Or Phone</td>
<td>Or Phone</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Or Phone</td>
</tr>
<tr>
<td>Phone number</td>
<td>Optional</td>
<td>✓</td>
<td>Or Email</td>
<td>Or Email</td>
<td>Optional</td>
<td>Or Email</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Job title</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ZIP code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Social Login</td>
<td>Optional</td>
<td></td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Interests</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ONLINE REGISTRATION AND VERIFICATION PROCESS

The data required during registration varies by service; review the mandatory personal fields prior to registering an account with the service. Also, be mindful that some services may wish to verify the legitimacy of your account via phone, email, or other identity verification techniques.

1. Enter required identity fields on the registration page. Avoid supplying more information than is required.

2. Consider using dual-factor authentication to add an additional layer of security to your account. Dual-factor authentication requires the user to verify an attempted login via email, text message, or an automatically generated code. When possible, use an application such as Authy or Okta that automatically generates a login code, instead of providing your phone number for dual-factor authentication.

3. Confirm your account via email, if possible. Avoid using mobile phones or other identity verification procedures in order to prevent further dissemination of your data.

4. Access your newly created account once it is confirmed. Review your populated personal identity data fields and remove any non-required personal information.

Sign Up
It’s free and always will be.

Follow the confirmation link sent to your email address to complete registration.

Account Confirmed
Your account has been confirmed. You can now use all of Facebook’s features and connect with friends.
OPTING OUT OF DATA AGGREGATORS

OPTING OUT OF DATA AGGREGATORS - DO’S AND DON’TS

- Conduct research to see what records each data aggregator has collected about you and your loved ones before opting out.
- Some data aggregators may have information about you and your family under multiple listings; you may need to repeat the removal processes described below for each listing.
- Have ALL the required information prepared before you begin the removal process.
- Follow ALL necessary steps to complete the removal process; you may need to mail or fax information to the aggregator.
- Encourage family members and cohabitants to remove their records from data aggregators as well.

DATA AGGREGATORS - HOW TO LOCATE YOUR INFORMATION ONLINE

Data and identity aggregators collect and catalogue information about individuals through a combination of public records collection and extensive web indexing and crawling. Search for your name, names of family members, email addresses, phone numbers, home addresses, and social media usernames and URLs using Google. Once you have located information that you want removed, record your findings to facilitate the removal process. Please note the information presented here, regarding how to remove personal details from data aggregators, is subject to change.

OPTING OUT INSTRUCTIONS BY SERVICE

OVERVIEW

Many data aggregators offer online opt out forms, while others require hard-copy forms to be mailed or faxed along with proof of identity. Online methods often require your email address; monitor your inbox and spam folder to ensure you receive opt-out email instructions and confirmations. Note the timeframe required for data removal, and check the aggregator site after that time has passed to ensure your information has been removed. Given the quantity of data aggregators, it may be helpful to create and update a tracking sheet to guide your removal processes.

PRIVATEEYE - PEOPLEFINDERS - PUBLICRECORDSNOW - VEROMI

PrivateEye, PeopleFinders, PublicRecordsNow, and Veromi are all owned by the same parent company: Confi-Chek.com.

Opt out of PrivateEye by visiting: https://www.privateeye.com/static/view/optout/
Complete the online form. After completion, you will be automatically redirected to PrivateEye partner sites.

Opt out of PeopleFinders and PublicRecordsNow by visiting: https://www.peoplefinders.com/manage
Enter your information and select Find My Listing. Find your record, and select This is me > opt out my info. Check all three boxes under Security Check, and select Continue.

Opt out of Veromi by visiting: veromi.net/Help
Under Privacy and Security select How do I remove myself from these records? and follow the instructions.

Opt out of PublicRecordsNOW by visiting: https://www.publicrecordsnow.com/static/view/optout/
Enter your information and select Opt out.

US SEARCH

Search for your name and select the appropriate listing to block. Print the cover sheet and mail or fax to the address/number provided with a copy of a state issued ID or drivers license.

NAME

www.ussearch.com

INTELIUS - PUBLIC RECORDS - ZABASEARCH - SPOCK - ISEARCH - DATECHECK - LOOKUP - LOOKUPANYONE - PEOPLE LOOKUP - PHONESBOOK

Intelius owns, or is affiliated with, the following people search websites: Public Records, Zabasearch, Spock, iSearch, DateCheck, LookUp, LookupAnyone, People Lookup, and PhonesBook. Instructions for opting out of each site vary. Visit the help section of each website and search for instructions under Privacy and Opt Out topics. Opt out of Intelius online at http://intelius.com/optout. Requests are usually completed within 72 hours.
### OPTING OUT INSTRUCTIONS CONTINUED...

#### BEEN VERIFIED

![BeenVerified Logo]

BeenVerified allows you to opt out at: [https://www.beenverified.com/f/optout/search](https://www.beenverified.com/f/optout/search).

Search for your name in ALL STATES, and click the listing(s) relevant to you. Enter your email address, complete the reCAPTCHA, and click **Send Verification Email**. Follow instructions in the verification email to complete de-registration.

#### PEEKYOU

![PeekYou Logo]

Fill out the PeekYou opt out form at: [www.peekyou.com/about/contact/optout/index.php](http://www.peekyou.com/about/contact/optout/index.php)

Under **Actions**, select **Remove my entire listing**. Paste the numbers at the end of your profile’s URL in the “UniqueID” field, and complete the CAPTCHA. You will receive an initial email confirming you’ve sent in your opt-out form and a second email in a few days or weeks to tell you it has been deleted.

#### SPOKEO

![Spokeo Logo]

To opt out of Spokeo, first find your listing, then visit Spokeo’s opt out page: [www.spokeo.com/opt_out/new](http://www.spokeo.com/opt_out/new).

Enter the URL of your listing, complete the CAPTCHA, and enter your email. Click **Remove This Listing**.

Your listing will be removed in 2-3 days.

#### WHITEPAGES

![Whitepages Logo]

First, locate your information on Whitepages by searching your name. Then visit [https://www.whitepages.com/suppression_requests](https://www.whitepages.com/suppression_requests). Enter the URL of the relevant profile(s) in the Opt-out form and click **Opt-out > Remove me > I just want to keep my information private**.

Verify your identity with a phone call; enter your phone number and you will immediately receive an automated call from Whitepages. Use your touchscreen to enter the 4 digit verification code provided via the opt out form. For further details, visit: [https://support.whitepages.com/hc/en-us/articles/115010106908-How-do-I-edit-or-remove-a-personal-listing-US-IDENTITY](https://support.whitepages.com/hc/en-us/articles/115010106908-How-do-I-edit-or-remove-a-personal-listing-US-IDENTITY)

#### US IDENTITY

![US Identify Logo]

First, search for your information on US Identify and identify the profile(s) relevant to you. Be sure to include aliases, if applicable.

To opt out of US Identify, visit [http://www.usidentify.com/company/contact.html](http://www.usidentify.com/company/contact.html). You may submit an opt-out email request to support@usidentify.com or contact customer service by phone at (855) 454-0394.

In an email request, write “I would like all information for [Name] [Date of Birth] [Current City and State] removed from usidentify.com and all affiliated sites.”

#### PIPL

![PIPL Logo]

Pipl is a people search engine and no longer offers a direct information removal option. Instead, Pipl recommends you remove your personal information from the source websites it lists under your name; once data is removed from the source website, it should no longer appear in Pipl results.

For further information, visit: [https://pipl.com/help/remove/](https://pipl.com/help/remove/)

#### INSTANTCHECKMATE

![InstantCheckMate Logo]

To opt out of InstantCheckMate, follow the instructions at: [www.instantcheckmate.com/optout](http://www.instantcheckmate.com/optout)

Select **Remove This Record**. Enter your email address, complete the reCAPTCHA and select **Send Confirmation Email**. Click **Confirm Opt Out** inside the email you receive, and InstantCheckMate will begin processing your opt out request, which can take 48 hours.
IDENTITY THEFT PREVENTION

IDENTITY THEFT PREVENTION - DO’S AND DON’TS

• Create a unique password for each of your accounts and devices to limit the risk of having multiple accounts compromised at once.
• Change your login passwords on a regular basis, and don’t store them in your email or cloud storage services, which a hacker can potentially access.
• Keep your computer up-to-date by installing the latest versions of the operating system and anti-virus software protection.
• Avoid sharing sensitive information such as credit card or Social Security numbers through texts, emails, or chats.
• Never use public networks to conduct online financial transactions. Remember to log out of personal accounts opened on public devices.
• Ensure that all communications involving online financial transactions are sent through an SSL encrypted connection ("https://").

IDENTITY THEFT - BACKGROUND

Identity theft is currently the fastest growing crime in America. In 2017, more than 16.7 million incidents of identity fraud were reported by individuals in the US. On average, each victim spends 100 to 200 hours over a six-month period trying to resolve an identity fraud issue. While the common conception is that identity thieves are online scammers, evidence indicates that up to 50% of all reported cases involve theft committed by a neighbor, co-worker, or family member. Most identity theft cases can be resolved with minimal long-term impacts if they are caught early.

TYPES OF IDENTITY THEFT AND WHAT’S AT RISK

Identity theft occurs when one individual fraudulently uses another’s personal information for financial or personal gain. Though the motives behind identity theft may differ, disseminating sensitive or potentially harmful information places your identity and financial assets at risk.

SENSITIVE DATA

- Social Security Number
- Driver’s License Number
- Credit Card Number
- Bank Account Number
- Birth Certificate
- Tax Information
- Employee Identification Number

POSSIBLY HARMFUL

- Pets’ RFID Numbers
- Utility Account Numbers
- Residential History
- Unsolicited Credit Offers

WHAT DOES IDENTITY THEFT LOOK LIKE?

IDENTITY THEFT TYPES

- Financial
- Insurance
- Medical
- Criminal
- Driver’s License
- Social Security
- Synthetic
- Child

AGE OF VICTIMS

- < 19 years: 4%
- 20 to 39 years: 29%
- 40 to 59 years: 32%
- 60+ years: 35%

FAKE WI-FI NETWORKS

Fraudsters may establish fake Wi-Fi hotspots to mimic public Internet access points. Avoid communicating personal and financial information over public Wi-Fi connections, and do not access any unsecured networks.

Do NOT use unsecured Wi-Fi Connections

SOCIAL MEDIA MINING

Sharing personal information may allow another individual to apply for a line of credit using your identity, or send targeted phishing scams. Avoid sharing home addresses and birth dates on social profiles, and never disclose any of the sensitive information listed above.

PHISHING SCAMS

Phishing scams are among the most popular techniques for acquiring personal information. The information gleaned from phishing scams can be used to open fraudulent accounts or assume control of existing accounts. The model below outlines the common identifiers of a phishing email.

1. Non-descriptive senders or mismatched email addresses (e.g., the “From” and “Reply-To” addresses do not match).
2. Unprofessional subject titles.
3. Phrases demanding the user to share personal information to prove their identity.
4. Threats to close accounts without compliance or immediate actions.
5. Absence of company logo within the email header.
6. Presence of grammatical or spelling errors.
7. Emails containing links to other pages or attachments may contain malicious scripts to install malware.

From: Payment Services <XXXXX@XXXX.XXX>
Reply-To: <XXXXXXX@XXXX.XXX>
Subject: Suspicious Account Activity!

This message is to inform you that your account has exhibited unusual activity within the past 24 hours and has since been locked for security purposes. In order to verify ownership of your account you must respond to this email with the following information:

Name:
Email:
Account Number:
Social Security Number:

Failure to verify your account information may result in forfeiture of funds. To see a summary of your account activity, open the attached documents or visit our Security Center.

*Source: Network for Identity Theft Types by # of Reports, Federal Trade Commission, Consumer Sentinel Network Data Book 2017 (March 2018)
My current activity is: reading

Signs of Identity Theft

Credit scores are susceptible to damage through identity theft. However, damages from identity theft can be reduced significantly if caught early. Bank statements should be checked weekly, while each of the three credit reports should be checked once per year. The following occurrences may indicate a stolen identity:

- Errors appearing on bank and credit card statements.
- Errors appearing on credit reports.
- Financial accounts flagged for suspicious activity.
- Debt collectors calling to inform about delinquent debts.
- Problems filing insurance claims.
- Fraud alerts activated on credit cards.

Identity Theft Protection Services

Select companies offer services to monitor customers’ credit scores and to protect their personal information online. Each company works with creditors to identify fraudulent activity and restore a customer’s reputation. Most packages also offer financial reimbursements for significant personal losses. Individuals should still follow best practice guides to prevent the compromise of identity data during online activity.

<table>
<thead>
<tr>
<th>DATA PROTECTION &amp; RECOVERY VENDOR</th>
<th>PRODUCT</th>
<th>SSN</th>
<th>BANK ACCOUNT</th>
<th>CREDIT CARD</th>
<th>MEDICAL FRAUD</th>
<th>PUBLIC &amp; COURT RECORDS</th>
<th>COMPUTER SECURITY OFFERINGS</th>
<th>CREDIT REPORTS</th>
<th>FINANCIAL COVERAGE</th>
<th>PRICE/MONTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premier</td>
<td></td>
<td>✔  ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Annually</td>
<td>Up to $1 Million</td>
<td>$24.99</td>
</tr>
<tr>
<td>UltraSecure + Credit</td>
<td></td>
<td>✔  ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Quarterly</td>
<td>Up to $1 Million</td>
<td>$23.95</td>
</tr>
<tr>
<td>Ultimate Plus</td>
<td></td>
<td>✔  ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>Annually</td>
<td>Up to $1 Million</td>
<td>$29.99</td>
</tr>
</tbody>
</table>

Resolving Identity Theft

Place an Initial Fraud Alert

Call one of the three credit report companies listed below and request that an initial fraud alert be placed on your credit scores. The alert lasts for 90 days and prevents any new lines of credit from being opened in your name without a form of verifiable identification. Placing an initial fraud alert entitles you to a free credit report from each of the three credit report companies. Also, consider freezing your credit to prevent creditors from accessing your credit reports. Credit freezes can be implemented for a fee (between $5.00 to $15.00) and are enabled by calling each of the three credit reporting agencies listed below. Credit freezes remain active until the individual who requested the credit freeze contacts the credit agencies and instructs them to unfreeze the reports.

Request Your Credit Scores

Use sites like www.annualcreditreport.com or www.creditkarma.com to request free copies of your credit scores. Look for inconsistencies within your credit reports and send letters to each of the three credit reporting companies explaining the misuses. Then, contact the fraud department of each business that reported a fraudulent transaction. Close any financial accounts that were opened without your permission or which show unauthorized activity.

Create an Identity Theft Report

File an online complaint with the Federal Trade Commission (FTC) at www.ftc.gov/complaint and a police report outlining the details of the theft. If the police are reluctant to file a report, present them with the FTC’s Memo to Law Enforcement, which is available at www.IdentityTheft.gov. Together these documents make up an identity theft report and can be used to remove transactions or obtain information about the accounts misused by an identity thief.
KEEPING YOUR KIDS SAFE ONLINE - DO'S AND DON'TS

• One family member’s unsecured privacy and sharing settings can expose personal data from the rest of the family.
• Ensure kids only establish and maintain connections with people you know and trust. Review their connections often.
• Assume that ANYONE can see any information kids post and share regarding their activities, whereabouts, and personal life.
• Avoid posting or tagging images of you and your family that clearly show your faces. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post smartphone photos and ensure kids don’t use their face as a profile photo; use cartoons or avatars instead.
• Use secure browser settings when possible, and monitor your child’s browsing history to ensure that you recognize all access points.

OVERVIEW

A 2016 study reported that 96% of children above the age of eight claimed to actively use the Internet, where kids are potentially exposed to cyber-bullying, influence operations, pornography, drugs/alcohol, and violence. Children are at risk not only from exposure to inappropriate content posted by others on the Internet, but also from exposing their personal information to strangers on social networking services (SNS). The following web browser settings, add-ons, and software downloads are available to restrict or monitor a child’s activities online.

MICROSOFT EDGE SETTINGS

To view child safety options, login to your Microsoft account upon opening the browser and click on Family Safety. From this page, you can register accounts for your children and customize their Internet browsing settings. The Family Safety settings can be only accessed with a Microsoft account.

GOOGLE CHROME SETTINGS

To ensure your child’s safety when using Google Chrome, download Blocksi from the Chrome Store to add child safety settings to the browser.

ADVANCE SETUP

 Allow, block, or warn users of certain content types. Select the > next to each filter category to set more granular restrictions.

FILTERS

 YouTube Filter - filters individual YouTube channels and videos for content.
 Content Filtering - identifies specific words in webpages to prevent access.
 Black/White List - allows users to add specific URLs to block or allow.

TIME RESTRICTIONS

Set a time frame of acceptable computer use for your child.

FACEBOOK SETTINGS

STANDARD FIREFOX: Select Tools > Options > Privacy & Security to block sites with malicious content. Under Tracking Protection > Use Tracking Protection to block known trackers, select Always. For Send websites a “Do Not Track” signal, select Always.

FOXFILTER FOR FIREFOX: To set parental controls, download the FoxFilter add-on. Once installed, users are allowed to set keywords to block or permit specific sites, and set sensitivity settings.

PARENTAL CONTROLS

Adjust how your children can use the computer. Allow or block specific programs and websites, and set personalized restrictions.

PASSWORDS

Create a username/password for your child’s account that only you know.

TIME RESTRICTIONS

Set a time frame of acceptable computer use for your child.
FAMILY SAFETY SERVICES
A variety of free and paid services are available for monitoring your children's online activities. The software options listed below are effective in either restricting or monitoring content that your child tries to access.

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>MICROSOFT FAMILY SAFETY</th>
<th>NET NANNY</th>
<th>NORTON SECURITY PREMIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image monitoring</td>
<td>Windows 8+</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SMS message monitoring</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Contacts monitoring</td>
<td>Windows 8+</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Block sites option</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Allow sites option</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Record user activity</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>User access requests to admin</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Time restrictions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Game restrictions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Paid service</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remote access notifications</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock safe search</td>
<td>Windows 8+</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

MICROSOFT FAMILY SAFETY
Activate this free service from your Microsoft/Outlook account. The service provides basic content filters and reports of programs/websites accessed by each account.

Adults can set individualized settings for each account and view their child's requests to access blocked content each time they log in.

NET NANNY
This service is available for download for $39.99 and can both restrict and monitor content from computer programs, instant messengers, SNSes, and web browsing applications. It is installed onto the desktop and provides the most granular settings for filtering and reporting potentially harmful content online.

Parents can respond to their child's permission requests remotely from a mobile app or computer in real time. Additional settings include blocking applications, Internet connections, proxy servers, blogs, and chat rooms. Net Nanny displays an extensive list of SNS and instant messengers as well as 35 categories of potentially harmful content to screen.

NORTON SECURITY PREMIUM
At a cost of $109.99/year, this comprehensive service offers online family monitoring features along with Norton Security protection. This service allows parents to track which websites children visit and prevent certain harmful content from being displayed on their monitors. Parents can use this tool to conduct web, time, search, social network, mobile app, text, and video supervision; review activity history; lock devices; and receive email alerts, on up to 10 devices.

Net Nanny also provides time-based Internet usage restriction capabilities for each user profile.

Norton Security Premium identifies SNS profiles that children maintain and allows supervisors to see what they are sharing with the public (name, age, profile picture, etc.). It also prevents children from sharing personal information including phone numbers, Social Security Numbers, and email addresses.
VOICE OVER INTERNET PROTOCOL (VOIP)

WHAT IS VOIP?

Voice Over Internet Protocol (VOIP) is a group of technologies that allow voice and video calls and multimedia messages to be delivered over the Internet to other VOIP users, or to users on legacy telephone networks anywhere in the world. Communications travel over broadband Internet connections via computer, Internet Protocol (IP) telephones, tablets, smartphones, specially-equipped analog telephones, and television sets, making VOIP an attractive, low-cost alternative to traditional telephone services. Popular VOIP services include Skype, FaceTime, Silent Circle, Google Hangouts, Viber, Vonage, and WhatsApp, but there are several types:

- **Business** - Multi-line packages that require special equipment or cloud services and substantially more bandwidth than a typical home connection. Advanced features such as private branch exchanges, automated attendants, and faxing are available.
- **Residential** - VOIP services provided through a DSL or cable modem, or a special VOIP router that provides more bandwidth for calls. These packages often use a combination of installed equipment and mobile apps.
- **Mobile** - Free or low-cost VOIP services available through smartphone apps. Calls and messages travel over a cellular data connection or Wi-Fi.

BENEFITS

VOIP calls are affordable, particularly since most services do not have long-distance fees and offer low per-minute rates for international calls. Some companies, such as Google, Apple, and Microsoft, offer free VOIP services.

Popular features include group video chat, file-sharing, mobile apps, voicemail transcription, call screening, call recording, and transferring calls or messages between devices.

VOIP can be used anywhere you can connect to the Internet. One number can ring multiple devices simultaneously. Users can also choose which calls go to which devices and at what times.

VOIP does not have geographic boundaries. Users can easily acquire local numbers in other states or countries.

Because of its extensibility and portability, it is easier for developers to create and implement new applications and technologies that can transmit data through VOIP.

EVALUATING PROVIDERS

- Which features are in the basic plan? Which require an additional fee?
- Is the service E911-compliant?
- Does the paid service provider itemize its fees? Does it breakdown its activation, licensing, equipment, support, per-minute rates, and any termination fees?
- Is special equipment required? Is it free?
- Can purchased equipment be used with other providers?
- Is live support available 24 hours a day, seven days a week?

DISADVANTAGES

A poor Internet connection can result in delayed messages, buffering, and low audio/image quality.

Some providers do not connect to 911 or emergency services, so a second phone line may be needed.

Not all devices are E911-compliant (Enhanced 911), meaning they do not automatically transmit a caller’s location to emergency operators.

VOIP hardware cannot be used without power and an Internet connection.

Security systems and other devices in your home may not work with VOIP.

VOIP is vulnerable to routine computer disruptions, including crashes and malware.

USING VOIP SECURELY

Password-protect your apps, and encrypt or erase sensitive information including texts, call history, and voicemail. Here are some tips and security-related questions to ask:

- Are all calls on the provider network encrypted? For calls to landline phones, the portion of calls carried on the legacy network is not encrypted.
- Are messages encrypted in transit and at rest, so even the provider cannot access them?
- Does the provider use firewalls, redundant servers, and 24/7 monitoring?
- How often does the provider test for system vulnerabilities? Are patches applied quickly?
- Can you use your own virtual private network (VPN) with the VOIP service?
- For residential service, can stolen equipment (routers, phones) be disabled remotely?
### CHOOSING A VOIP PROVIDER

<table>
<thead>
<tr>
<th>MOBILE SERVICE</th>
<th>OPERATING SYSTEM</th>
<th>COST</th>
<th>BEST USES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Skype</strong></td>
<td>Windows, Mac, iOS, web, Android</td>
<td>Free to $13.99/month</td>
<td>File sharing, screen sharing, document collaboration, video calls</td>
</tr>
<tr>
<td><strong>Google Hangouts</strong></td>
<td>iOS, Android, web</td>
<td>Free</td>
<td>Encrypted one-to-one or group audio/video calls, live streaming video, screen sharing (web)</td>
</tr>
<tr>
<td><strong>Silent Circle</strong></td>
<td>iOS, Android</td>
<td>$9.95/month</td>
<td>Anonymous, encrypted calls and messages, identity verification</td>
</tr>
<tr>
<td><strong>FaceTime</strong></td>
<td>iOS, Mac</td>
<td>Free</td>
<td>Encrypted audio calls, video calls, and messages; voice memos</td>
</tr>
<tr>
<td><strong>Viber</strong></td>
<td>iOS, Android, Windows, Linux</td>
<td>Free</td>
<td>Encrypted audio calls, video calls, and text messages; group chat up to 250 people</td>
</tr>
<tr>
<td><strong>Cryptocat</strong></td>
<td>Windows, iOS, Mac, Linux, web</td>
<td>Free</td>
<td>Secure messaging, encrypted file sharing</td>
</tr>
</tbody>
</table>

Residential VOIP services have similar cost savings to mobile apps but require more hardware, including a broadband modem and a telephone adapter or VOIP-ready telephone. A service contract may also be required.

Popular residential VOIP services include:

- **Ooma**: $79.99 equipment purchase. Service is free (except taxes and fees) and calls to other Ooma users are encrypted.
- **Via Talk**: $15.75 a month. Unlimited domestic calls.

### SKYPE

Under **Settings**, go to **Account & Profile > Your Skype Profile**:
- Under **Profile picture**, set visibility to **Contacts only**.
- Do not add your **Birthday**.

Under **Account & Profile > Manage > Your profile**:
- Do not provide optional personal data such as gender, location, or contact information.
- Uncheck boxes for **Appear in search results** and **Appear in suggestions**.

Under **Settings > Contacts**, toggle **"Sync your contacts"** to **OFF**.

### GOOGLE HANGOUTS

Sign up for a Google Voice (GV) account at [google.com/voice](http://google.com/voice) for a free number or port your existing number.

Install the Hangouts app and connect your GV number. In **Settings**:
- Toggle **"Answer on lock screen"** to **OFF**.
- Navigate to **Invitations > Customize invites** and select who can contact you directly and who needs an invite in order to establish a call.
- Turn **ON** invitation notifications.

### VIBER

Download and install the Viber app.
- Under **Settings > Privacy**, uncheck all boxes. Do not connect Viber to your Facebook or Twitter account.
- Under **Calls and messages**, uncheck boxes for Viber-in Calls and Receive Service Messages.
- Under **Media**, select **Delete Video and Voice messages**. Deselect both **Auto download options**.
- Under **General**, deselect **Show Viber status icon** and **Open links internally**.

### FACETIME

FaceTime is a built-in VOIP option for Apple users. FaceTime simply requires being logged in with your Apple ID to Mac, iPhone, or iPad.

Navigate to **Settings > FaceTime**:
- Turn **FaceTime ON**.
- Select if others can reach you on FaceTime by your phone number, email, or both. We recommend only enabling one of the two options.
- Toggle **"FaceTime Live Photos"** to **OFF**.
VIRTUAL PRIVATE NETWORK (VPN)

VIRTUAL PRIVATE NETWORKS - DO'S AND DON'TS

- Select a VPN provider that allows you to protect multiple devices; some services limit the number of devices you can run on a single private network.
- Review your VPN terms of service (ToS) thoroughly to ensure your web traffic, stored data, and personally identifiable information (PII) are protected.
- Monitor your Internet speeds after connecting to a VPN; overburdened VPN servers can slow connections.
- Enable the "kill switch" option of your VPN service; whenever you are disconnected from a server, Internet is also disconnected as a safeguard.
- Before making your selection, always research whether a VPN provider has a good or bad track record in handling user privacy.
- Remain vigilant once you have chosen a VPN service provider; be on the lookout for software upgrades and periodic changes in the ToS.

WHAT IS A VPN?

A virtual private network (VPN) is a private network that extends across a public network or the Internet, allowing users to surf the web privately, safe from outside view. When a VPN is activated, incoming web traffic is routed through a secure, remote server equipped with firewalls and data encryption tools.

For the average user, VPNs offer an added layer of identity protection by concealing network and location data and shielding PII from potential hackers and identity data brokers. While on a VPN, Internet traffic and session data are looped through a remote server with data encryption before reaching the requested website's server. Three common use cases for VPN technology are described below:

- **Business** – Companies use VPNs to allow access to intranet sites and secured files with off-site employees.
- **Residential** – More households are establishing VPNs at home to keep their family's PII, browsing history, Internet Protocol (IP) address, and location data secure from malware and malicious websites.
- **Mobile** – As increasing number of users access the web using their phones, mobile apps providing VPN access are becoming popular. However, VPN does not mask location or other session data from apps to which the user has previously permitted access.

CHOOSING THE RIGHT VPN SERVICE PROVIDER

The easiest way to establish and connect to a VPN from home is by using a reputable service provider. Your selection will depend on your specific usage requirements, physical location, and device type. These are some questions to consider before committing to one provider:

- Can the service be loaded onto multiple devices? Can the service be used on all devices simultaneously?
- Is the software or app compatible across different operating systems, if needed?
- Are there any data restrictions in place? Does the VPN service provider promise complete anonymity?
- What level of data encryption is offered? Does the service provider keep server logs?
- Where is the VPN provider located?

Most providers offer paid and free versions of their service. Be aware that the free option comes with limits such as bandwidth caps, the number of accessible servers, and the number of devices allowed per VPN. Compare the capabilities of four popular VPN service providers below to determine which product best suits your usage case and protection needs.

<table>
<thead>
<tr>
<th>SERVICES</th>
<th>COMPATIBILITY</th>
<th>COST</th>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
</table>
| **ExpressVPN** | iOS, Windows, Android, Linux, Blackberry, routers, browser extensions, media streaming devices | • $12.95 per month  
• 30-day money back guarantee | • Can run 3 devices simultaneously (with premium service)  
• VPN killswitch offered for Windows  
• Provides content unblocking | • Connection logs are retained  
• Limited simultaneous device connections |
| **ZenMate** | iOS, Windows, Android, Chrome, Firefox, Opera, routers | • Unlimited free browser add-on  
• $8.99 per month  
• 14-day money back guarantee | • Extremely streamlined and easy-to-use | • Limited traffic settings  
• Uses one security protocol (L2TP) |
| **IPVanish** | iOS, Windows, Android                             | • $10 per month  
• 7-day money back guarantee | • 2 simultaneous connections  
• Unlimited bandwidth  
• No VPN traffic logs | • No free trial  
• Limited device connections |
| **CyberGhost** | iOS, Windows, Android, Linux, Chrome OS, Raspberry Pi, routers | • Free limited service  
• $10.99 per month for full service  
• 30-day money back guarantee | • IP address shielding  
• Highly configurable  
• Unlimited bandwidth with premium subscription | • Full service requires a paid subscription  
• Server availability varies by country |
VPN BENEFITS

- The VPN tunnel, a private connection established between your device and the remote server, shields your PII from outside view.
- VPN services typically include: data encryption, IP address protection, ad blockers, and kill switches. Ad blockers remove unwanted advertisements, while a VPN kill switch automatically cuts your connection during service interruptions. These features ensure that your session is protected on both the browser and server level.
- VPNs shield PII in worst-case scenarios by encrypting user data, decreasing the risk of identity exposure against data theft and malicious attacks.
- VPN users can route web traffic through servers in other countries, which offer unique benefits, such as allowing users to view country-specific content that is normally blocked in their physical location.

VPN VULNERABILITIES

- VPNs can cause a reduction in Internet connection speed. The tunneling effect of most VPN services creates a lag in the connection.
- VPN service providers will have access to your username, password, session data, and some PII. Review your service's ToS frequently to ensure that the company is not sharing or selling your data with third-party partners and vendors.
- VPNs often use servers located in other countries; privacy laws vary among countries, so your data may be at greater risk when connecting to servers located in places with lenient privacy laws.
- Some VPN providers, especially free ones, come with monthly data caps. Make sure the plan you choose includes sufficient bandwidth for your needs.

HOW TO ESTABLISH AND CONNECT TO A VPN

Following VPN provider selection, set up and begin your protected browsing session. Using VPN software will require you to login each time you wish to make a connection. Most services require a basic username/password combination for authentication. Additional security features, like use of an alphanumeric authentication key, are used for account recovery or password resets. Some free trials may not require registration.

1. Create an account with your chosen VPN service provider.
2. Download and install the selected VPN program. If you are using a mobile device, locate the app in the App Store or Google Play Store.
3. Open the program on your device and sign in. VPNs can be run indefinitely, however if you logout of the program or shutdown your device, you will need to login again.
4. Choose your target server by country or region and establish a connection.
5. Once the connection has been established, allow the program to run in the background of your device. The VPN service dashboard gives you information about the new IP address, server location, and connection duration.
6. Disconnect from the chosen server when ready, removing the protection from your device. Login is required every time you want to reconnect to a VPN.
WINDOWS 10 - DO'S AND DON'TS

- Don't use Windows 10 without adjusting the default factory settings; they are set to maximize data collection across all Microsoft apps and programs.
- Review and adjust Cortana's default privacy setting before the first use to prevent Microsoft from collecting any gratuitous personal data.
- Don't approve any suggested system updates or "Express Settings" without reviewing the Terms of Service (ToS).
- Review data permissions of all apps installed on your computer every three months. Apps you never interact with can still access your Windows data and collect your user statistics and patterns for analysis.
- Ensure that your anti-virus software, VPN apps, and web browsers are up-to-date and functional.

OVERVIEW

Windows 10 comes with many new additions: a new browser, a varied login protocol, a digital assistant, and a list of default settings that collect and send usage data to Microsoft. These new user-friendly features create additional risks for your personally identifiable information (PII). The programs in Windows 10 are more interconnected than before and require new sets of user data and input to function, such as additional account fields, access to the lock screen, and the user's contacts list. This means Windows 10 is collecting and using personal data in new ways compared to its previous iterations. Follow the recommended settings in this chapter to avoid sharing an unnecessary amount of personal information with Microsoft.

CORTANA - WINDOWS’ INTELLIGENT PERSONAL ASSISTANT

Cortana is a voice-enabled intelligent personal assistant created by Microsoft. When used, Cortana is able to assist you in searching the web, creating alarms, managing your contacts, and writing emails and messages.

In order to function at full capacity, Cortana must access your Microsoft email address, geolocation data, microphone, calendar, and metadata, and connect with your computer settings. Using Cortana with the default factory settings will leave your PII exposed. If you choose to use Cortana, follow these recommended settings to maximize your privacy:

1. Access Cortana at the bottom left of your computer screen. It will appear as a search box or as the circle icon depending on your view settings.
2. From the Options menu, click on Start Menu > Settings > Cortana. Click through each entry on the settings bar to review the settings pertaining to Cortana.
3. We recommend that you disable Cortana during most normal usage scenarios. Enable Cortana only if you wish to access your microphone and use voice recognition as needed in special use cases.
4. Connecting your Windows-enabled devices allows you to share tasks, web browsers, and apps across multiple devices. It also syncs your data and exposes voice commands collected through Cortana. Set notifications to OFF.

5. After adjusting Cortana settings, go to Windows Settings > Privacy > App permissions to ensure that Cortana’s access to your data (including Location) is disabled.

Identity Awareness, Protection, and Management Guide
ADJUSTING WINDOWS 10 PRIVACY SETTING

Managing the privacy settings on Windows 10 is the only way to control what information is being collected, stored, and shared by Microsoft. The following steps will show you what Windows has access to and how you can maximize your data security.

1. Navigate to Windows 10’s privacy settings by Start Menu > Settings > Privacy.

2. Under the General heading, modify the options as shown below in order to secure your computer and PII.

3. Under Privacy > Speech, inking, & typing ensure speech services and typing suggestions are turned OFF to prevent the collection of voice, typing, and touch interface patterns.

4. Microsoft automatically enables numerous categories of app permissions, including access to your device camera, microphone, location, and your account information. Examine each category listed under Privacy > App permissions in detail. When in doubt, toggle OFF all access permissions that are not essential to your device usage. For example, turn OFF all general settings under Location and limit the number of apps that have access to your location data to only essentials (e.g., Maps).

5. Under Privacy > Diagnostics & feedback, opt to send only Basic device information to Microsoft. Toggle OFF Improve inking & typing recognition and Tailored experiences.

6. Under Activity history, deselect both boxes to prevent Windows from collecting your activities and syncing that data to the cloud. Toggle OFF Show activities from accounts. Scroll down and use Clear activity history to delete your data.
INDEX

ACCOUNT CLEAN UP

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXIF Data Removal</td>
<td>26</td>
</tr>
<tr>
<td>View Activity log</td>
<td>5</td>
</tr>
<tr>
<td>Health Apps &amp; Fitness Trackers</td>
<td></td>
</tr>
<tr>
<td>Apple Health</td>
<td>31</td>
</tr>
<tr>
<td>Google Fit</td>
<td>31</td>
</tr>
<tr>
<td>Mobile Dating Apps</td>
<td></td>
</tr>
<tr>
<td>Coffee Meets Bagel</td>
<td>19</td>
</tr>
<tr>
<td>Hinge</td>
<td>19</td>
</tr>
<tr>
<td>Mobile Wallets</td>
<td></td>
</tr>
<tr>
<td>Apple Pay - IPhone Only</td>
<td>29</td>
</tr>
<tr>
<td>Mobile Wallets - Dos and Don’ts</td>
<td>28</td>
</tr>
<tr>
<td>Online Registration</td>
<td>34-35</td>
</tr>
<tr>
<td>Opting Out of Data Aggregators</td>
<td>36-37</td>
</tr>
<tr>
<td>Secure Chat Apps</td>
<td></td>
</tr>
<tr>
<td>Signal</td>
<td>21</td>
</tr>
<tr>
<td>Telegram</td>
<td>21</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>21</td>
</tr>
<tr>
<td>Voice Over IP (VOIP)</td>
<td></td>
</tr>
<tr>
<td>Using VOIP Securely</td>
<td>42</td>
</tr>
<tr>
<td>Windows 10</td>
<td></td>
</tr>
<tr>
<td>Adjusting Window 10’s Privacy Setting</td>
<td>47</td>
</tr>
</tbody>
</table>

ACCOUNT DELETION

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>5</td>
</tr>
<tr>
<td>Deactivating/Deleting your Facebook account</td>
<td></td>
</tr>
<tr>
<td>Instagram</td>
<td>11</td>
</tr>
<tr>
<td>Deactivating your Instagram account</td>
<td></td>
</tr>
<tr>
<td>LinkedIn</td>
<td>13</td>
</tr>
<tr>
<td>Deleting your LinkedIn Account</td>
<td></td>
</tr>
<tr>
<td>Mobile Dating Apps</td>
<td></td>
</tr>
<tr>
<td>Instagram</td>
<td></td>
</tr>
<tr>
<td>Mobile Dating Apps</td>
<td></td>
</tr>
<tr>
<td>Bitcoin</td>
<td>19</td>
</tr>
<tr>
<td>Coffee Meets Bagel</td>
<td>19</td>
</tr>
<tr>
<td>Hinge</td>
<td>19</td>
</tr>
<tr>
<td>Tinder</td>
<td>21</td>
</tr>
<tr>
<td>Secure Chat Apps</td>
<td></td>
</tr>
<tr>
<td>Telegram</td>
<td>21</td>
</tr>
</tbody>
</table>

ACTIVITY HISTORY

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>4</td>
</tr>
<tr>
<td>Social Network - Dos and Don’ts</td>
<td></td>
</tr>
<tr>
<td>Facebook Mobile</td>
<td>6</td>
</tr>
<tr>
<td>Facebook Mobile Settings</td>
<td></td>
</tr>
<tr>
<td>Mobile Dating Apps</td>
<td></td>
</tr>
<tr>
<td>iOS (v 11.2.1)</td>
<td>26</td>
</tr>
<tr>
<td>Preventing the Capture of Geolocation Data</td>
<td>27</td>
</tr>
<tr>
<td>views and Removing EXIF Data on OS X</td>
<td></td>
</tr>
<tr>
<td>Facebook</td>
<td>6</td>
</tr>
<tr>
<td>iPhone Settings</td>
<td></td>
</tr>
<tr>
<td>Health Apps &amp; Fitness Trackers</td>
<td></td>
</tr>
<tr>
<td>Apple Health</td>
<td>31</td>
</tr>
<tr>
<td>The table</td>
<td>30</td>
</tr>
<tr>
<td>Instagram</td>
<td>11</td>
</tr>
<tr>
<td>Privacy Settings</td>
<td></td>
</tr>
<tr>
<td>Mobile Dating Apps</td>
<td></td>
</tr>
<tr>
<td>Selecting a Dating App</td>
<td>18</td>
</tr>
<tr>
<td>Mobile Wallets</td>
<td></td>
</tr>
<tr>
<td>Apple Pay - IPhone Only</td>
<td>29</td>
</tr>
<tr>
<td>Choosing the Right Mobile Wallet</td>
<td>28</td>
</tr>
<tr>
<td>Secure Chat Apps</td>
<td></td>
</tr>
<tr>
<td>Choosing the Right Secure Chat App</td>
<td>20</td>
</tr>
<tr>
<td>Signal</td>
<td>21</td>
</tr>
<tr>
<td>What are Secure Chat Apps?</td>
<td>20</td>
</tr>
<tr>
<td>Smartphones</td>
<td>22-23</td>
</tr>
<tr>
<td>Traveling with Smartphones</td>
<td>24-25</td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td></td>
</tr>
<tr>
<td>Choosing the Right VPN Service Provider</td>
<td>44</td>
</tr>
<tr>
<td>Voice Over IP (VOIP)</td>
<td></td>
</tr>
<tr>
<td>Benefits of VOIP</td>
<td>42</td>
</tr>
<tr>
<td>Choosing a VOIP Provider</td>
<td>43</td>
</tr>
<tr>
<td>FaceTime</td>
<td>43</td>
</tr>
</tbody>
</table>

C

CHILD SAFETY

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft Prevention</td>
<td>38</td>
</tr>
<tr>
<td>Age of Victims</td>
<td></td>
</tr>
<tr>
<td>ID Theft Types</td>
<td>38</td>
</tr>
<tr>
<td>Keeping Your Kids Safe Online</td>
<td>40-41</td>
</tr>
</tbody>
</table>

COMMUNICATING SECURELY

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft Prevention</td>
<td>38</td>
</tr>
<tr>
<td>Fake Wi-Fi Networks</td>
<td></td>
</tr>
<tr>
<td>Identity Theft Prevention - Dos and Don’ts</td>
<td>38</td>
</tr>
<tr>
<td>Phishing Scams</td>
<td>38</td>
</tr>
<tr>
<td>Keeping Your Kids Safe Online</td>
<td>40-41</td>
</tr>
<tr>
<td>Mobile Dating Apps</td>
<td></td>
</tr>
<tr>
<td>Hinge - Use</td>
<td>19</td>
</tr>
<tr>
<td>Mobile Dating Apps - Dos and Don’ts</td>
<td>18</td>
</tr>
<tr>
<td>Using Mobile Dating Apps - Communication</td>
<td>18</td>
</tr>
<tr>
<td>Secure Chat Apps</td>
<td>20-21</td>
</tr>
<tr>
<td>Voice Over IP (VOIP)</td>
<td></td>
</tr>
<tr>
<td>Choosing a VOIP provider</td>
<td>43</td>
</tr>
<tr>
<td>Disadvantages</td>
<td>42</td>
</tr>
<tr>
<td>Using VOIP Securely</td>
<td>42</td>
</tr>
</tbody>
</table>

CONNECTIONS & FOLLOWERS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>4</td>
</tr>
<tr>
<td>Social Network - Dos and Don’ts</td>
<td></td>
</tr>
<tr>
<td>Health Apps &amp; Fitness Trackers</td>
<td>31</td>
</tr>
<tr>
<td>Garmin Connect</td>
<td></td>
</tr>
<tr>
<td>MyFitnessPal</td>
<td>31</td>
</tr>
<tr>
<td>Samsung Health</td>
<td>31</td>
</tr>
<tr>
<td>The table</td>
<td>30</td>
</tr>
<tr>
<td>Instagram</td>
<td>10</td>
</tr>
<tr>
<td>Instagram Overview</td>
<td></td>
</tr>
<tr>
<td>Selecting a Dating App - Registration Info</td>
<td>18</td>
</tr>
<tr>
<td>Mobile Dating Apps</td>
<td></td>
</tr>
<tr>
<td>Choosing the Right Mobile Wallet</td>
<td>28</td>
</tr>
<tr>
<td>Mobile Wallets - Dos and Don’ts</td>
<td>28</td>
</tr>
<tr>
<td>Risks of Using Mobile Wallets</td>
<td>28</td>
</tr>
<tr>
<td>Venmo</td>
<td>29</td>
</tr>
<tr>
<td>Online Dating Services</td>
<td></td>
</tr>
<tr>
<td>Selecting a Dating Site - Data Sharing</td>
<td>16</td>
</tr>
<tr>
<td>Options</td>
<td></td>
</tr>
<tr>
<td>Online Registration</td>
<td></td>
</tr>
</tbody>
</table>
PAYMENTS

Mobile Wallets 28–29

PERMISSIONS

EXIF Data Removal (iOS v. 12.1.3) 26
Facebook Mobile Android Settings 6
Keeping Your Kids Safe Online Net Nanny 41
Mobile Dating Apps Selecting a Dating App 18
Mobile Wallets Google Pay 29
Mobile Wallets - Best Practices 29
Overview Your Data Is Everywhere 2
Photo Sharing Services Flicker 15
Smartphones Smartphones - Do's and Don'ts 22
Wireless Protection and App Security Settings 23

PHISHING

Phishing Prevention

PIN

Mobile Wallets 28–29
Secure Chat Apps Secure Chat Apps - Do's and Don'ts 20
Smartphones Protecting Your Smartphone from Physical Access and Malware Risks 22
Traveling Safely with Smartphones Set Your Phone to Lock Automatically and Set a Complex ScreenLock Password 24

R

RELOCATING

Identity Theft Prevention Social Media Mining 38
Online Registration 38

SHARING PHOTOS, VIDEOS, AND LIVE CONTENT

EXIF Data Removal 26–27
Facebook 4–5
Facebook Mobile 6–7
Instagram 10–11
Keeping Your Kids Safe Online 40–41
LinkedIn 12–13
Mobile Dating Apps 18–19
Online Dating Services 16–17
Online Registration 34–35
Photo Sharing Services 14–15
Secure Chat Apps 20–21
Twitter 8–9

TAGS

EXIF Data Removal
Android (v. 7.0) 26
EXIF Removal - Do's and Don'ts 26
Important Tags 26
Facebook Social Network - Do's and Don'ts 4
View Activity Log 5
Facebook Mobile Facebook Mobile Settings 6
Tag People 7
Instagram Instagram - Do's and Don'ts 10
Photos only 11
Keeping Your Kids Safe Online
Keeping Your Kids Safe Online - Do's and Don'ts 40
Photo Sharing Services 14–15
Twitter Posting to Twitter 8

THIRD-PARTY ACCESS

Health Apps & Fitness Trackers Fitbit 31
Third-party Data Sharing 30
LinkedIn Data Privacy and Advertising Settings 13
Online Registration Online Registration - Do's and Don'ts 34
Secure Chat Apps Vulnerabilities 20
What are Secure Chat Apps? 20
WhatsApp 21
Secure Home Wi-Fi Network Preventing Third Party Access to your Wireless Network 32
Smartphones Protecting Your Smartphone from Physical Access and Malware Risks 22
Wireless Protection and App Security Settings 23
Virtual Private Network (VPN) VPN Vulnerabilities 45

TRACKING

Facebook Mobile Local 7
Nearby Friends 7
Health Apps & Fitness Trackers 30–31
Keeping Your Kids Safe Online Firefox Settings 40
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOICE RECOGNITION</td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>Your Data Is Everywhere</td>
<td>2</td>
</tr>
<tr>
<td>Windows 10</td>
<td>46</td>
</tr>
<tr>
<td>Cortana - Windows' Intelligent Personal Assistant</td>
<td>46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>W I-FI</td>
<td></td>
</tr>
<tr>
<td>Health Apps &amp; Fitness Trackers</td>
<td>30</td>
</tr>
<tr>
<td>Overview</td>
<td>30</td>
</tr>
<tr>
<td>Identity Theft Prevention</td>
<td>38</td>
</tr>
<tr>
<td>Fake Wi-Fi Networks</td>
<td>38</td>
</tr>
<tr>
<td>Mobile Wallets</td>
<td></td>
</tr>
<tr>
<td>Mobile Wallets - Best Practices</td>
<td>29</td>
</tr>
<tr>
<td>Secure Chat Apps</td>
<td></td>
</tr>
<tr>
<td>Choosing the Right Secure Chat App</td>
<td>20</td>
</tr>
<tr>
<td>Securing Home Wi-Fi Network</td>
<td>32–33</td>
</tr>
<tr>
<td>Smartphones</td>
<td>23</td>
</tr>
<tr>
<td>Wireless Protection and App Security Settings</td>
<td>23</td>
</tr>
<tr>
<td>Traveling with Smartphones</td>
<td></td>
</tr>
<tr>
<td>Disable Wi-Fi and Bluetooth</td>
<td>25</td>
</tr>
<tr>
<td>Protecting Your Phone Against Malware - Android (v 7.0)</td>
<td>24</td>
</tr>
<tr>
<td>Traveling with Smartphones - Do's and Don'ts</td>
<td>24</td>
</tr>
<tr>
<td>Use VPN on Wireless Networks</td>
<td>25</td>
</tr>
<tr>
<td>Virtual Private Network (VPN)</td>
<td>44–45</td>
</tr>
<tr>
<td>Voice Over IP (VOIP)</td>
<td>42</td>
</tr>
<tr>
<td>What is VOIP?</td>
<td>42</td>
</tr>
</tbody>
</table>