Identity Awareness, Protection, and Management

Constant Internet connectivity is increasingly becoming a necessity in today's fast-paced, interconnected world. Online services, devices, and networks increasingly share personal identity information—moving beyond the traditional name and date of birth to include behavioral patterns, purchasing history, and network of associates—to create the complex network that is your online identity.

Without knowing the common ways our data is collected, who is collecting it, and where it can end up, safeguarding our information becomes difficult. Fortunately, by following the recommendations presented in this guide, you can learn to better protect yourself, your friends, and your family online.

Your Total Online Identity: What Footprints Do You Leave?
# TABLE OF CONTENTS

1. FACEBOOK ........................................................................................................................ 4
2. FACEBOOK MOBILE ........................................................................................................... 6
3. TWITTER .............................................................................................................................. 8
4. LINKEDIN ........................................................................................................................... 10
5. GOOGLE+ .......................................................................................................................... 12
6. PHOTO SHARING SERVICES .............................................................................................. 14
7. ONLINE DATING SITES ...................................................................................................... 16
8. MOBILE DATING APPS ...................................................................................................... 18
9. SECURE CHAT APPS ......................................................................................................... 20
10. SMARTPHONES ................................................................................................................ 22
11. TRAVELING SAFELY WITH SMARTPHONES .................................................................. 24
12. SMARTPHONE EXIF REMOVAL ....................................................................................... 26
13. MOBILE WALLETS ............................................................................................................ 28
14. SECURING YOUR HOME WIRELESS NETWORK ............................................................. 30
15. ONLINE REGISTRATION .................................................................................................... 32
16. OPTING OUT OF PUBLIC RECORDS AND DATA AGGREGATORS .................................. 34
17. IDENTITY THEFT PREVENTION ....................................................................................... 36
18. KEEPING YOUR KIDS SAFE ONLINE .............................................................................. 38
19. VOICE OVER IP (VOIP) .................................................................................................... 40

## USEFUL LINKS AND RESOURCES

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityTheft.gov (by the FTC)</td>
<td><a href="https://www.identitytheft.gov/">https://www.identitytheft.gov/</a></td>
</tr>
<tr>
<td>Online Guardian</td>
<td><a href="http://www.onguardonline.gov/topics/social-networking-sites.aspx">http://www.onguardonline.gov/topics/social-networking-sites.aspx</a></td>
</tr>
<tr>
<td>Privacy Right Clearinghouse</td>
<td><a href="http://www.privacyrights.org/privacy-basics">http://www.privacyrights.org/privacy-basics</a></td>
</tr>
<tr>
<td>How to Disable Flash</td>
<td><a href="http://goo.gl/DQa6HJ">http://goo.gl/DQa6HJ</a></td>
</tr>
<tr>
<td>HTTPS Everywhere</td>
<td><a href="https://www.eff.org/https-everywhere">https://www.eff.org/https-everywhere</a></td>
</tr>
<tr>
<td>Securing Your Web Browser</td>
<td><a href="https://www.us-cert.gov/publications/securing-your-web-browser">https://www.us-cert.gov/publications/securing-your-web-browser</a></td>
</tr>
</tbody>
</table>

## 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.
FACEBOOK

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 that your family takes 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.
- Never post Smartphone photos and do not use your face as a profile photo; instead, use cartoons or avatars.
- Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.

MINIMIZING YOUR FACEBOOK PROFILE

Facebook provides shortcuts to their privacy settings that help to limit what others can see in your profile. Select Privacy Checkup to change your basic privacy setting. For more extensive settings, click See More Settings. From there, navigate through the pages of the settings toolbar to control how your personal information is shared with others.

1. Use the Privacy tab to declare which audiences can search for you, contact you, and see your posts. In general, it is best to limit the audiences to 'Friends' or 'Only Me'. The Use Activity Log selection can be used to review past posts individually and edit the audiences for each entry. The Limit Past Posts selection can be used to retroactively change the settings of all 'Public' posts to a 'Friends' only audience.

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

3. Followers can view your post from their personal News Feeds. It is even possible for followers to view the content you post without being an accepted Facebook friend. Set Who Can Follow Me to 'Friends' only.

4. The Security tab provides ways to protect your credentials and become aware of suspicious login attempts. Use Login Alerts and Where You're Logged In to monitor login activity and end inactive sessions.

5. Use the Ads tab to prevent Facebook from using your data for advertising. Set Third Party Sites and Ads & Friends fields to 'No One'.

6. Your Facebook contacts may be sharing your information with third-party apps without your knowledge. Navigate Apps > Apps Others Use and uncheck all data fields to prevent others from sharing your data.

Avoid linking third-party apps (e.g. Twitter) with your Facebook account. Data shared with other apps becomes subject to their terms and conditions which may result in unwanted data aggregation and dissemination.
FACEBOOK PROFILE PAGE

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. Within these tabs reside general audience settings. Use the guidelines below to maximize your security while interacting with these features.

ABOUT

Avoid entering personal data within the About section. This information is mostly optional and contains data fields including Work and Education, Places You’ve Lived, Contact and Basic Info, Family and Relationships, and Details About You. Use the audience settings to change the mandatory fields to ‘Friends’ or ‘Only Me’.

FRIENDS

Under the Friends Tab:

- Navigate Manage > Edit Privacy to change who can view your contacts. Limit your Friend List to ‘Only Me’.
- Navigate Manage > Manage Sections to control which data fields will appear on your timeline. Avoid sharing places on your timeline and use discretion when posting information regarding your personal interests.

VIEW ACTIVITY LOG

The View Activity Log tool displays the information that is posted to your timeline in a chronological order. 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 Settings > Download a Copy of your Facebook Data > And More. Select Start My Archive to view a personalized report of the data collected on you.

DEACTIVATING/DELETING YOUR FACEBOOK ACCOUNT

Deactivating an account removes your name and photos from things that you have shared. To deactivate your Facebook account, navigate to Settings > Security > Deactivate Your Account. Your account remains deactivated until your next login.

To delete your Facebook account, select Help from the triangle icon’s dropdown menu and select Visit the Help Center. Navigate Manage Your Account > Deactivating, Deleting & Memorializing Accounts > How Do I Permanently Delete My Account > Let Us Know. Verify that you wish to delete your account by clicking Delete My Account. Facebook will permanently remove most of your data within 90 days of submission.
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 about your activities, personal life, or professional life that you post and share.
• Ensure that your family takes similar precautions with their account; 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 other parties.

FACEBOOK MOBILE OVERVIEW

As of January 2015, Facebook Mobile hosted 745 million daily mobile active users who accounted for over 60% of all the mobile posts published to any online social networking service. Though privacy is still achievable, these mobile users place their personal identity data at a greater risk when compared to users logging in via desktop computer. This is in large part due to the fact that mobile devices provide Facebook with a means to access additional location information, contact lists, photos, and other personal data. Use the following recommendations to best protect yourself against over-sharing.

FACEBOOK MOBILE SETTINGS

Facebook Mobile’s general security settings closely resemble those of Facebook’s desktop application. Click More on the Facebook banner and select Settings. From there, navigate through the Security, Privacy, Timeline and Tagging, and Locations tabs to apply the settings shown below.

IPHONE SETTINGS

The iPhone’s security settings can help to further protect your personal data while you use the Facebook Mobile App. From the iPhone’s Settings icon, select Privacy and navigate through the Location Services, Photos, and Facebook tabs to disable all of the permissions, as seen below.

ANDROID SETTINGS

Android phones can be configured to protect your personal data while you access the Facebook Mobile App. Access the phone's general Settings feature and navigate through the Location Access and Apps tabs to limit the types of data that Facebook can retrieve from your mobile device.
Facebook Mobile allows you to post new statuses, upload photos, or check-in to locations, using the Update Status prompt. The icons highlighted on the update prompt are shortcuts for adding further information about you to each post. Four of these five 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 when posting to Facebook.

**Selecting Your Audience**

With every post, Facebook Mobile allows you to select the audience through the Share With prompt. For maximum privacy, select individual friends with whom you would like to share your post. Never make your posts available to the public.

**Tagging Friends**

Tagging friends in individual posts extends the reach of your profile and your contacts’ profiles. Limit the number of tags you post to your Facebook entries.

**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.

**Nearby Friends**

Nearby Friends allows you to share your location with friends. When activated, it 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.

**Nearby Places**

Nearby Places uses your GPS location to display local venues. When activated, the feature permits check-ins, provides a map to select locations, and shows other users’ reviews about the venue. Individual reviews link back to the poster’s Facebook profile. Avoid posting on these public threads.

**Cleaning up posts**

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

Avoid tagging friends in individual posts. Tagging friends in individual posts extends the reach of your profile and your contacts’ profiles. Limit the number of tags you post to your Facebook entries.

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

When this feature is enabled, Facebook builds a history of your precise location. You can view and manage this information from the Activity Log. 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.
TWITTER

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 that your family takes 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 other parties.

OVERVIEW

Twitter is a social networking and micro-blogging site that hosts more than 305 million monthly active users. The platform allows users to post text-based entries to their profiles and follow updates from other accounts. On average, Twitter users issue approximately 500 million entries per day from the web-based and mobile platforms combined. For most, Twitter is used as a source to discover breaking news coverages and staying 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 labelled 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 the account owner’s personal identity 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 140 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 used by multiple 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 post’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.
• More - Additional actions include Share via Direct Message, Copy Link to Tweet, Embed Tweet, Embed Video, Mute, Block, and Report.
Access Twitter’s settings by selecting the thumbnail image of your profile photo in the top banner of the webpage. From the dropdown menu, select Settings and locate the pages containing customizable security options: Security and Privacy, Account, Web Notifications. After configuring your settings, access Your Twitter Data to review the device and login histories to ensure that your account has not been accessed by unauthorized users.

SECURITY AND PRIVACY

Apply the settings shown below within the Security and Privacy tab to control how others can interact with your Twitter profile and your Tweets.

ACCOUNT SETTINGS

Account settings allow users to customize their Twitter handles and contact emails. Users can also request their Twitter archives which contain a transcript of all of their past Tweets or elect to deactivate their accounts.

NOTIFICATIONS

Email and web notifications alert users when others interact with their profiles or content. For maximum security, customize the notifications settings to receive as many alerts as possible.
LinkedIn Overview

LinkedIn is a professional networking service currently hosting more than 400 million users around the world. The site is primarily used by individuals looking to establish mutually beneficial professional relationships with companies, hiring managers, and other working professionals on the site. Users typically maintain profile pages outlining their professional and educational achievements, and establish networks with others who report similar backgrounds. Though the site offers valuable services, LinkedIn profiles tend to have high visibility, even to people who are not within the network. For this reason, it is essential to limit the exposure of your information. Follow the recommendations on this card to better protect your data while using LinkedIn.

LinkedIn Profile

A standard LinkedIn profile contains a user’s profile picture and current position or education level. The information supplied beyond these fields is largely optional and should be limited to maximize privacy. The colored tiles on the user’s profile page provide a means to include unique information.

Minimizing Public Profiles

By default, LinkedIn profiles can be discovered through public search engines. Due to the service’s high visibility, it is imperative to change your public profile privacy settings to adjust how your data is presented. The images below show how your data may appear to the public on your LinkedIn profile page.

Select Update your public profile settings to reveal the prompt shown to the right. This prompt controls how your LinkedIn data appears on public search engines such as Google, Yahoo!, or most notably, Bing. It is recommended that you make your public profile visible to no one in order to limit the reach of your data. If you wish to still remain visible to everyone, use the basic filters to uncheck sensitive data fields such as your picture and the details of your current position or educational programs.

Click the Privacy & Settings tab, shown in the image below, to reveal additional Account, Privacy, and Communication settings for your LinkedIn profile.
Apply the Privacy settings shown below to control how your data is displayed and to ensure that your information is visible only to the people you authorize.

**Who can see your connections**
Choose who can see your list of connections
- People will still be able to see connections who endorse you and connections they share with you. (Don’t want your endorsements visible? Just choose to opt out)

**How You Rank**
Choose whether or not to be included in this feature
- How You Rank shows how you compare to your connections and colleagues in terms of profile views. If you turn this feature off, others won’t see your or your standings in their "How You Rank" page. But you also won’t see your own rank or get tips on improving your visibility.

**Viewers of this profile also viewed**
Choose whether or not this feature appears when people view your profile
- Should we display "Viewers of this profile also viewed" box on your Profile page?

**Sharing profile edits**
Choose whether your network is notified about profile changes
- Should people know when you change your profile, make recommendations, or follow companies?

**Profile viewing options**
Choose whether you’re visible or viewing in private mode
- Select what others see when you’ve viewed their profile

**Representing your organization**
Choose if we can show your profile information on your employer’s page
- Hide my picture and profile information from showing up in this section of a job detail page?

**Sharing data with third parties**
Choose if we can share your basic profile data with third parties
- Should we share your basic profile and contact information with third party applications?

**ACCOUNT SETTINGS**
Apply the Account settings shown below to limit the amount of data you display and control who has access to your data.

**Authorized External Applications**
Listed here are external partner applications to which you have granted access to your LinkedIn profile and network data. If you remove that access here, they will no longer be able to access your LinkedIn data. To re-enable them in the future, go to the application and grant access again.

**Where you’re signed in**
See your active sessions, and sign out if you’d like
- You’re currently signed in to 2 sessions...

LinkedIn maintains an archive of each individual’s unique account activity. To request a copy of your archived data, select Account > Getting an archive of your data. In time, LinkedIn will provide you with a comprehensive report of your activities including account data, past posts, connections, and other network interactions. Review your data frequently to ensure that you are not over-sharing information. If you no longer plan to use the LinkedIn service, click Account > Closing your account and follow the subsequent prompts to unsubscribe from LinkedIn and officially close your account.
GOOGLE PLUS

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 or share about your activities, personal life, or professional life.
• Ensure that your family takes 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. Pictures of individuals should be taken at a distance or a severe angle.
• 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 other parties.

OVERVIEW

Google Plus is a social networking site visited by approximately 300 million monthly active users. Like other social networking sites, Google Plus provides a platform for its users to connect and share media. However, Google also uses these profiles to identify individuals interacting with other Google properties including YouTube, Gmail, Android services, and Google Search. These connections place users’ identity data at greater risks because a unique identity can be linked to other online activity. Follow the recommendations on this card to help limit the information you share through your Google Plus profile.

PROFILE INFORMATION

Google Plus profiles can be used to share personally identifiable information. Most data fields such as work history, education, and contact information are optional and should not be entered. Mandatory data fields, including gender and birthday, should be set to private. From your profile, select Edit Profile followed by the About Me icon to manage these fields.

FOLLOWERS

Your network consists of the people you follow and those who follow you. Your followers can see when you post content. Likewise, you are notified when posts appear from the people you follow. Your followers can be organized into subgroups referred to as “Circles” that help you control who can see your content. Select the People tab to manage your circles.

POSTING TO GOOGLE PLUS

Google Plus allows you to share photos, links, locations, and text entries with others in your circles. Once posted, the entries appear within your personal profile and become visible to others with whom you have given permission. Your followers can interact with the posts as seen in the examples below.

Viewers have the options to like, comment, or reshare individual posts. When they use one of these options, a clickable link to their profiles appears directly within the post. Limit your use of these features and use the View Activity option to review the actions taken with your posts.

• Likes - Posted entries appear with a “+1” embedded in the window. Clicking this icon will mark your endorsement of the content (Similar to Facebook’s “likes”).
• Comments - Users may leave comments on individual posts. These comments are visible to anyone who has access to the post.
• Reshares - Users may repost your content to their own profiles. It is important to note that both public and private posts can be reshared by their recipients and distributed to new audiences.

Select the What’s new with you? prompt on your Home page to post a new entry to your profile. Each post can include up to four different types of content: text, photos, links, and locations. Avoid sharing links to other social profiles, photos that clearly show your face, or any of your frequented locations, as these may lead to unintended dissemination of your personal identity data.

Use the icons (highlighted in the image to the left) to disable reshares and set the appropriate audience settings. Available audience settings include Circles, People, and Public.

<table>
<thead>
<tr>
<th>AUDIENCE</th>
<th>WHO CAN SEE YOUR POST?</th>
<th>PRIVACY STRENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Anyone</td>
<td>None</td>
</tr>
<tr>
<td>Circles</td>
<td>All of the individuals within the specified circles</td>
<td>Intermediate</td>
</tr>
<tr>
<td>People</td>
<td>Designated individuals from your followers list</td>
<td>Strong</td>
</tr>
</tbody>
</table>
PROFILE SETTINGS

Google offers extensive settings to secure your Google accounts. To locate the settings unique to your Google Plus profile, select Settings from the banner on the left side of your profile. Apply the following options to increase your profile’s security and limit the reach of your personal data.

Photos and Videos Shared on Google+
Show geo location by default on newly shared Google+ albums. You can change the setting per album by switching to classic G+ on desktop.
LEARN MORE

Allow viewers to download my photos and videos shared on Google+

Don’t feature my publicly-shared Google+ photos as background images on Google products & services
LEARN MORE

Profile
Show how many times your profile and content have been viewed.

Show your Google+ communities posts on your profile. LEARN MORE

Show these profile tabs to visitors (they’re always visible to you) LEARN MORE

Photos

Youtube/Videos

+1

Reviews

Help others discover my profile in search results. LEARN MORE

Who can see the “people in your circles” section on your profile: Your circles

Show people who have added you to circles

AUDIENCE

WHO CAN SEE YOUR PROFILE DATA?

PRIVACY STRENGTH

RECOMMENDATIONS

Public
Anyone
None
Not Recommended

Extended Circles
People in your circles plus individuals from their circles
Minimal
Not Recommended

Your Circles
All of the individuals within the approved circles
Intermediate
Minimum Setting

Custom
Designated individuals or circles from your followers list
Strong
Recommended

Only You
No one except for you
Maximum
Recommended

GENERAL SETTINGS

Navigate to the top of the Settings page to manage your General Settings. General settings allow you to control who can see the content you share. Use the settings shown below, and reference the table at the bottom of this section, to help determine how you will share your data.

Apps & Activities
You can control who sees your activity on Google+

MANAGE GOOGLE+ ACTIVITY

Public
Anyone

Extended Circles
People in your circles plus individuals from their circles

Your Circles
All of the individuals within the approved circles

Custom
Designated individuals or circles from your followers list

Only You
No one except for you

Location Sharing
Share your real-time location with people you choose. LEARN MORE

MANAGE LOCATION SHARING

Off
Never share your location.

Your location isn’t visible to anyone.

Account
DELETE YOUR GOOGLE+ PROFILE

When you share things with “Your Circles” you are sharing them with each of the groups checked in this section.
PHOTO SHARING SERVICES - DO'S AND DON'TS

- Only share photos with people you know and trust. Assume that ANYONE can see, copy, and forward photos you post and share online.
- Ensure that your family takes similar precautions with their photos; their privacy and sharing settings can expose your images 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 other 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.

PHOTO SHARING SERVICES OVERVIEW

Photo Sharing Services are online virtual photo albums that store, organize, and share your photos; many Social Networking Services (SNS) such as Facebook are also Photo Sharing Services. These services provide a convenient way to share photos, but can expose you to privacy risks if you do not take proper precautions. This Smart Card explains how you can change 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>facebook</td>
<td>Social Networking Site (SNS)</td>
<td>Public, Friends of Friends, Friends, Only Me</td>
<td>No</td>
<td>Can tag location to photos; geolocation suggestions</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>twitter</td>
<td>Social Networking Service (SNS)</td>
<td>Public, Private (requests to follow must be approved by the user)</td>
<td>No</td>
<td>Can tag location to photos; geolocation suggestions</td>
<td>Yes</td>
<td>If Public</td>
</tr>
<tr>
<td>Instagram</td>
<td>Share photos directly from mobile phones</td>
<td>Public, Private (requests to follow must be approved by the user)</td>
<td>No</td>
<td>Can tag location to photos; geolocation suggestions</td>
<td>No</td>
<td>If third-party apps enabled</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>Site dedicated to sharing and commenting on photos</td>
<td>Public, Private (images are only viewable with a direct URL), Albums can be set to Public, Hidden, or 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>

FACEBOOK

Facebook is an SNS with 1.59 billion active members who upload 700 million photos per day.

To maximize your privacy on Facebook, navigate to Settings > Privacy > Timeline and Tagging and make the following changes:

- Who can post on your timeline: Only Me
- Review posts tag you in before they appear on your timeline: On
- Who can see posts you've been tagged in on your timeline?: Only Me

TWITTER

Twitter is an SNS with 320 million active members. Users commonly Tweet photos of themselves and others. To maximize your privacy on Twitter, navigate to Settings > Security and privacy > Privacy and make the following change:

- Photo tagging: select Do not allow anyone to tag me in photos
Instagram is a site dedicated to sharing and commenting on photos. The site has more than 400 million active users. To maximize your privacy, make the following changes to your account settings:

1. Open the Instagram Mobile App on your Smartphone and then navigate to Settings > Account Basics and make the following changes:
   - Select Private Account

2. Now you can approve which followers can see your photos on Instagram.

Imgur allows users to share photos and photo albums and to automatically post photos to other sites such as Reddit and Facebook. The site has more than 150 million active users. By default, Imgur strips all EXIF data from the photos you upload. However, to maximize your privacy on Imgur, you need to make a few additional simple modifications to your account settings.

1. Navigate to Account > Settings and make the following changes:
   - Default Album Privacy: select Secret
   - Public vs Private Uploads: select Private

2. Use sites you visit to improve which recommendations and ads you see: select No
3. Use information from our partners to improve which recommendations and ads you see: select No

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 100 million active users. To maximize your privacy on Pinterest, make the following modifications to your account settings. Go to Settings > Account Basics and make the following changes:

2. In the Personalization section of the Account Basics Menu, make the following selections:
   - Use sites you visit to improve which recommendations and ads you see: select No
   - Use information from our partners to improve which recommendations and ads you see: select No

3. When you make a new Board in Pinterest, select the Secret Boards option to keep your Pins private.

Flickr is a site dedicated to sharing and editing photos. The site has more than 100 million active users. To maximize your privacy, go to Settings > Privacy & Permissions and make the following changes:

1. Who can download your images? - Only You
2. Allow others to share your stuff - No
3. Who can add you to a photo? - Only You
4. Who can print your photos - Only You
5. Allow your stuff to be added to a gallery - No
6. Hide your EXIF data - Yes
7. Show which application you used for uploading - No
8. Hide your stuff from public searches - Yes, on flickr and 3rd-party sites

In the subsection of the Privacy Settings, Who can see what on your profile, make the following additional changes:

1. Email address: Only You
2. IM names: Your friends and family
3. Real name: Your friends and family
4. Current city: Your friends and family

In the subsection of the Privacy Settings, Who can see what on your profile, make the following additional changes:

1. Email address: Only You
2. IM names: Your friends and family
3. Real name: Your friends and family
4. Current city: Your friends and family

When you make a new Board in Pinterest, select the Secret Boards option to keep your Pins private.
Online dating services are used by individuals looking to develop a personal or romantic interest with others on the site. While each service is unique, sites typically ask users to maintain a public profile containing photos and personal information about themselves. These profiles are often searchable through the site and at times may be pushed to other users who share common interests or locations. Should you elect to participate in online dating, use the recommendations on this card to protect your website-based online dating services. For additional information about mobile, app-based services such as Tinder, Bumble, Hinge, or Coffee Meets Bagel, please reference the Mobile Dating section on page 18.

Common Threats from Dating Sites

Online dating sites present a unique set of threats to users when compared to other social networking sites. Dating sites encourage interactions between unacquainted individuals, require an increased amount of personal information used to match compatible individuals, and have minimal ways of verifying the accuracy of users’ claims. Before participating in online dating, consider the following threats to your personal identity 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 accounts’ legitimacies.
- Matches may request personal contact information (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 the Proper Dating Site

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 required 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>Name, gender, sexual orientation, email, ZIP code, birthdate, relationship status, biography</td>
<td>Most registration information, optional lifestyle and dating preferences, photos</td>
<td>No questionnaires, Login with Facebook, Upload photos from Facebook</td>
<td>Free to join; ~ $21-$27/month to send messages and have invisible browsing, other features extra</td>
</tr>
<tr>
<td>OKCupid</td>
<td>Gender, sexual orientation, email, ZIP code, country, birthdate, biography, lifestyle questionnaire, photo</td>
<td>Most registration information, optional questionnaire answers</td>
<td>Optional questionnaire, Login with Facebook, Upload photos from Facebook, Connect Instagram feed and upload photos</td>
<td>Free to join and send messages; &quot;A-List&quot; membership (invisible browsing) ~ $10-$20/month</td>
</tr>
<tr>
<td>Plenty of Fish</td>
<td>Gender, sexual orientation, ZIP code, country, birthdate, ethnicity, physical description, personal questionnaires, biography, interests, face photo</td>
<td>Most registration information</td>
<td>Optional questionnaires, 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, face photo, birthdate, physical description, lifestyle questionnaire, face photo</td>
<td>Most registration information, biography, optional lifestyle and dating preferences</td>
<td>Optional questionnaire, Register with Facebook or Google; upload photos from Facebook</td>
<td>Free to join; $12-$20/month to send messages and see profile visitors</td>
</tr>
<tr>
<td>eHarmony</td>
<td>Name, gender, sexual preference, email, ZIP code, country, birthdate, relationship status, children, lifestyle questionnaire, occupation, face photo</td>
<td>All registration information, ethnicity, lifestyle Information</td>
<td>Mandatory Questionnaire, Login with Facebook, upload photos from Facebook</td>
<td>Free to Join; $12-$30/month to activate SecureCalls and see profile viewers</td>
</tr>
</tbody>
</table>

OVERVIEW

Online dating sites are designed to pair individuals based on common interests, values, lifetime achievements, and daily lifestyles. As a result, these sites require users to provide extensive personal information, allowing the services to collect targeted information about users’ lifestyles.

- 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 accounts’ legitimacies.
- Matches may request personal contact information (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.

On online dating services, users are often prompted to fill out questionnaires that collect personal, sensitive information. This data is used by the service to pair individuals based on common interests, values, lifetime achievements, and daily lifestyles. As a result, these sites require users to provide extensive personal information, allowing the services to collect targeted information about users’ lifestyles.

- 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 accounts’ legitimacies.
- Matches may request personal contact information (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 the Proper Dating Site

Selecting the proper dating site is crucial for protecting your personal identity data. Before registering an account, examine the types of data required by each online dating site, and choose the service that best fits your privacy needs.

Over the course of participating in online dating, consider the following threats to your personal identity 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 accounts’ legitimacies.
- Matches may request personal contact information (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.

On websites like Tinder, Bumble, Hinge, or Coffee Meets Bagel, please reference the Mobile Dating section on page 18.
REGISTRATION DATA

Protecting your identity data begins with registration. The example identity below displays the best ways to populate common dating site identity fields. Use the same principles in this example to register your account.

Name: Jennifer Vident (Use “Jen V.”)
- Do not provide your full name
Date of Birth: 3/23/1981 (Use “1/1/1981”)
- Supply a false date with your true birth year
Gender: Female
- True identification required for proper site use
Sexual Preference: Male / Female / Other
- True identification required for proper site use
Current Location: Hackensack, NJ (Use New York, NY)
Select a large metropolitan area / nearby zip code
Username: SightSeer889
- Usernames should not represent your true name
Photo: Use a photo that does not clearly show your face or distinguishable landmarks near your location

OKCUPID

OKCupid hosts ~2.9 million unique monthly visitors. Personal profiles display photos, registration information, and answers to free-text questions pertaining to the owners’ interests and daily activities.

Navigate Settings > General and activate the three Privacy options to help control who has access to your profile. The questionnaire is optional — submitted answers may be kept private using the lock icon shown below.

- A paid subscription known as the “A-List” is the most secure option. It allows you to browse profiles anonymously and hides your profile from everyone except those who you choose to like or message first.

ZOOKS

Zook hosts ~1.8 million unique monthly visitors. Dating profiles consist of the data entered during registration and free-text entries describing the owners’ dating preferences and personal background.

Free Zook accounts offer little to no user-controlled security settings. Options including account verification pose potential threats to privacy — verification requires linking phone numbers, videos, or social networks.

When profiles are visited, Zook identifies the visitor to the profile owner. Users can activate private browsing for 30 minutes by paying 30 Zook coins (Starting coin price: $5.95 for 60 coins, purchased within the profile).

MATCH.COM

Match.com hosts ~4.3 million unique monthly visitors. Free accounts display photos, information submitted during registration, interests, and the traits that users look for in their significant others.

Select Settings to toggle profile visibility. Turn the member spotlight off to prevent the profile from appearing in ads. Hidden profiles prevent others from seeing the account but also disable Match.com’s matching capability.

Private Mode is the optimal security setting — your profile is only visible to select people — and is available with a paid subscription. It permits matching, emailing, and displaying who is interested in or viewed the profile.

PLENTY OF FISH

Plenty of Fish hosts ~2.5 million unique monthly visitors. Profiles display the information submitted during registration and the traits that users look for in their 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.

EHARMONY

EHarmony hosts ~1.2 million unique monthly visitors. Profiles display registration information excluding photos and questionnaire responses. Other data includes free-text responses addressing the users’ interests.

Free EHarmony accounts offer little to no user-controlled privacy settings. Instead, the site determines which data can be seen by others and warns users what types of data may potentially be harmful to share.

Photos can only be seen by those who maintain paid accounts. Upgraded accounts also permit users to see who has viewed their profiles and initiate SecureCalls, phone calls without sharing personal phone numbers.
MOBILE DATING SITES - DO’S AND DON’TS

• Avoid using usernames and profile photos that appear on other social networking services.
• 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 potentially reveal your geographical location, such as a photo with a famous landmark in the background.
• Always read and take the time to understand the app’s Terms and Conditions before agreeing to register an account.

OVERVIEW

It is estimated that one out of every ten American adults actively uses mobile dating apps as their primary source for discovering 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 app-based online dating services. For additional information about the risks of Internet dating and more information on web-based services such as Match, Plenty of Fish, Zoosk, OkCupid, or EHarmony, please reference the Online Dating Smart Card.

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 passes on the profile. Regardless of the swiping direction, users’ 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>OPERATING SYSTEMS</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>iOS and Android</td>
<td>Facebook account info: Likes, photos, general info, and relationship interests</td>
<td>Name, photos, age, approximate location, gender, biography, work information, education information, Instagram photos</td>
<td>Location, Cellular Data, &amp; Push Notifications</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>iOS and Android</td>
<td>Facebook account info: Likes, photos, general info, and relationship interests</td>
<td>Name, photos, age, location, biography, work information, education information</td>
<td>Location, Cellular Data, Push Notifications, &amp; Photos</td>
<td>Free to join; No paid accounts available</td>
</tr>
<tr>
<td>Hinge</td>
<td>iOS and Android</td>
<td>Facebook account info: Likes, photos, general info, and relationship interests</td>
<td>Name, photos, age, location, biography, height, education information, work information, hometown, religion, interests, number of friends on Hinge, common Facebook friends, dating preferences</td>
<td>Location, Cellular Data &amp; Push Notifications</td>
<td>Free to join; No paid accounts available</td>
</tr>
<tr>
<td>Coffee Meets Bagel</td>
<td>iOS and Android</td>
<td>Facebook account info: Likes, photos, general info, and relationship interests</td>
<td>Photos, age, location, height, ethnicity, religion, occupation, employer, education information, mutual friends, biography, lifestyle, and dating preferences</td>
<td>Location, Cellular Data, Push Notifications, Contacts, &amp; Photos</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 an unlimited 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 Gear Icon > View Profile > Edit Info to change or delete the information displayed in your profile.

Settings: Navigate to Gear Icon > Discovery Settings to change your profiles’ visibility. Deactivating Show me in Discovery 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 open a conversation through the app. The match expires if a communication is not opened within the allotted time. Gender-based limitations do not apply for same-sex matches.

Profiles: Navigate to Gear Icon > Pencil Icon to change the information displayed in your profile.

Settings: Navigate to Gear Icon > Settings to enable notifications and set your profile’s visibility. Deactivating Public Profile hides your profile.

HINGE

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

Use: Users may swipe through an unlimited number of profiles per 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 other’s profiles or communicate through the app, without rematching.

Profiles: Select More > My Profile > Edit to change or delete the information displayed in your profile.

Settings: Select More > Preferences to enable notifications and change your location to the nearest metropolitan area. Profiles cannot be hidden.

COFFEE MEETS BAGEL

Coffee Meets Bagel matches people who are in similar social circles on Facebook. It also takes into account geolocation, education, physical attributes, and past swiping tendencies to suggest compatible matches.

Use: The app shows users around six compatible matches (“Bagels”) per day; these matches can be swiped anonymously. Twenty additional profiles appear under Give & Take; swiping on these profiles is not anonymous. Matches do not expire and there are no gender-based chat limitations.

Profiles: Select Profile > Edit Profile to change or delete the information displayed in your profile.

Settings: Select Profile > Settings to enable notifications and set your profile’s visibility. Deselecting Active membership hides your profile.
SECURE CHAT APPS

SECURE CHAT APPS - DO’S AND DON’TS

- Only establish and maintain contact with people you know and trust. Review your contacts often.
- Ensure that your contacts take similar security precautions as you. 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 member.
- Use all available PIN, password, and privacy protection options available. Change passwords every six months for enhanced 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 use the app.

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 security against eavesdropping by concealing the users’ identities or making the contents of the messages indecipherable to anyone except the intended receivers. As a result, using secure chat apps may potentially offer users two layers of security when the app is in use: anonymity and data security.

- **Anonymity**: Mobile applications do not connect personally identifying information to messages and often require zero or limited identity data to create an account. These apps often offer private or public messaging to pseudonymous profiles and messages that expire after an allotted time.
- **Data Security**: Mobile applications promote the protection of 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 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. Snapchat, but not the other three services, shares this information 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.

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>COMPATIBILITY</th>
<th>DESCRIPTION</th>
<th>IDENTITY DATA</th>
<th>SECURITY</th>
<th>LINKAGES</th>
</tr>
</thead>
</table>
| Snapchat | iPhone & Android | Temporary text/photo/video messages known as ‘Snaps’, money transfers (Square is the processor). US-based. | **Sign up**: Email address & birthday  
**Optional**: Phone number, debit card number, zip code | Potential for anonymity; Messages not encrypted end-to-end | Social Networks / Email: None  
Device / Internet: Address book, camera, microphone, location, cellular data, Wi-Fi |
| Telegram | iPhone, iPad, Android, Windows Phone, Mac, Windows PC, Linux Computers | Cloud-based messenger syncs across devices; Secure Chat feature with temporary text messages. Germany-based. | **Sign up**: Phone number  
**Optional**: Name & picture | Potential for anonymity; Encrypted messages | Social Networks / Email: None  
Device / Internet: Address book, cellular data, Wi-Fi |
| VSee | iPhone, iPad, Android, Mac, Windows PC | Text messages or video conferences; application file sharing on PC. US-based. | **Sign up**: Email address, first name, last name | Potential for anonymity; Encrypted messages & secure calls | Social Networks / Email: Gmail, Yahoo, MSN, AOL email contacts  
Device / Internet: Microphone, camera, address book, cellular data, Wi-Fi, LAN |
| KeyTone | iPhone & Android | Call/text/video messages over an Internet network. US-based. | **Sign up**: Phone number & email address | Encrypted messages & secure calls | Social Networks / Email: None  
Device / Internet: Address book, cellular data, Wi-Fi |
SNAPCHAT

Snapchat is used to send temporary photo/video messages (‘Snaps’) to other users. Snaps can only be viewed once by the intended recipients and are set to expire between 1 and 10 seconds. Snapchat also offers a chat feature where text messages can be sent to others. Chats are permanently erased when the recipient closes the chat window. Snapchat can also securely process payment transfers by way of the Snapcash feature.

Tap the **ghost** in the center of the camera page and then select the **gear** icon to adjust your privacy settings. Apply the following recommendations:

- Do not provide your real name in the **Name** or **Username** fields.
- Set who can **Send me Snaps** and **View My Story** to **My Friends**.
- Clear **Browser Data** and **Clear Conversations** after every use.
- Select **Manage** and disable both **Filters** and **Travel Mode**.
- If you elect to use Snapcash, turn on the security code (CVV) requirement and review transactions/receipts routinely.

TELEGRAM MESSENGER

Telegram is an app that primarily 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.

Tap the **Settings** icon and then select the **Privacy and Security** option. Apply the following recommendations to maximize security:

- Do not provide your real name or a profile photo.
- Set **Last Seen** to **Nobody**.
- Establish a secure **Passcode Lock** and **Two-Factor Authentication**.
- Review your active sessions routinely and close all unknown sessions.
- Set to **Delete My Account if away for 1 month**; accounts are free to make and there is no risk of losing contact information.

VSEE

VSee is a social messaging app used to establish secure conversations with other app users. VSee users can initiate video conferences with up to four people at a time and can send text messages protected with end-to-end encryption. Instant text messages are deleted when users choose to log out of their active sessions. Phone calls made within the app are also encrypted with end-to-end protection to prevent eavesdropping.

Tap the **blue icon** (three lines) in the top left corner of the screen. Proceed to **Settings** and apply the following selections to maximize your security:

- Disable **Stay Signed In**
- Disable **Auto Accept Calls**

Follow these basic instructions when using the app:

- VSee accounts are linked to email accounts; avoid using an email address linked to your true identity data.
- Delete the app’s history after each completed communication.
- Manually log out of your sessions when your conversations conclude.

KEYTONE

KeyTone is a social app designed to securely promote multiple forms of communication through the application. KeyTone users can share short video and audio messages, send text messages, and make secure VoIP phone calls to other app users. It employs standards-based protocols and cryptography for protecting data in transit, and offers in-app features such as ‘Ghost Mode’ to prevent over-the-shoulder eavesdropping.

Tap the **Settings** icon in the bottom right corner of the screen. Apply the following options to best secure your conversations through the app:

- Enable **Ghost Mode**
- Enable **2 Phase Call (SDES)** to improve encryption for phone calls.
- Enable **ICE** to prevent temporary storage of secure phone calls.

Follow these basic instructions when using the app:

- Manually delete your messages when your conversations conclude.
- Clear the app’s history after each completed communication.
SMARTPHONES

SMARTPHONES - DO’S AND DON’TS

- Always protect your device with a password, and run apps such as Android Lost and Find My iPhone to help you recover lost or stolen smartphones.
- Malicious emails and text messages can infect your smartphone with malware; run anti-virus software periodically on your device.
- The camera and microphone can be remotely activated; do not take a smartphone in situations where personal or legal matters are being discussed.
- As an extra precaution, remove the battery before discussing any sensitive information.
- When possible use VPN when accessing wireless networks, and turn off Bluetooth unless needed to prevent unwanted access to your device.
- Apps may gain real-time access to the data stored on your smartphone; review what data (e.g. location) the app collects before downloading.

PROTECTING YOUR SMARTPHONE FROM PHYSICAL ACCESS AND MALWARE RISKS

Use the following settings and recommendations to minimize inherent security risks posted by your smartphone and protect your personal data.

<table>
<thead>
<tr>
<th>RISK SCENARIO</th>
<th>IPHONE</th>
<th>ANDROID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMARTPHONE IS PHYSICALLY ACCESSED BY SOMEONE WITHOUT YOUR CONSENT</td>
<td>Navigate to Settings &gt; General &gt; Passcode Lock</td>
<td>Navigate to Settings &gt; Security &gt; Screen Lock</td>
</tr>
<tr>
<td>Use a complex password mixing letters + numbers</td>
<td>Block access</td>
<td>Uncheck</td>
</tr>
<tr>
<td>Optional setting</td>
<td></td>
<td>Always auto-lock your device</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SMARTPHONE IS LOST OR STOLEN</th>
<th>Install Find My Phone</th>
<th>Install Cerberus Anti Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capabilities:</td>
<td>- Remote lock</td>
<td>- Remote lock</td>
</tr>
<tr>
<td></td>
<td>- Erase data</td>
<td>- Erase data</td>
</tr>
<tr>
<td></td>
<td>- GPS locator</td>
<td>- Remote lock</td>
</tr>
<tr>
<td></td>
<td>- Sound alarm</td>
<td>- GPS locator</td>
</tr>
<tr>
<td></td>
<td>- Send text message to phone</td>
<td>- Scan for spyware, adware, and trojans</td>
</tr>
<tr>
<td></td>
<td>- Backup data through iCloud storage</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SMARTPHONE IS INFECTED WITH MALWARE</th>
<th>Install Lookout Mobile Security</th>
<th>Install Antivirus Security by AVG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phones are not readily susceptible to viruses. Use this app to prevent passing malware to contacts.</td>
<td>Capabilities:</td>
<td>Capabilities:</td>
</tr>
<tr>
<td>Capabilities:</td>
<td>- Scan for spyware, adware, and trojans</td>
<td>- App scanner</td>
</tr>
<tr>
<td></td>
<td>- Scan emails and PDF files before sending</td>
<td>- File scanner</td>
</tr>
</tbody>
</table>

RECOMMENDATIONS TO MINIMIZE PHYSICAL ACCESS AND MALWARE RISKS

- Updates for smartphones’ operating systems are sent out frequently. Install the updates immediately to maximize your protection.
- Jailbroken phones allow malicious apps to bypass vetting processes taken by the app stores. Never jailbreak your smartphones.
- Write down the serial number of your phone when it is purchased to help identify devices if lost or stolen.
- Avoid linking social networking services like Facebook and Twitter to your smartphones to prevent personal information aggregation.
- Change passwords on your phone frequently (approximately every 6 months) to maximize security.

Identity Awareness, Protection, and Management Guide
Smartphones communicate personal data across a variety of networks and apps in order to bring its complex functionalities to the user. Follow these steps to best protect your identity data in one of the following four common smartphone use case scenarios.

### USE CASE

#### IPHONE

##### CONNECTING TO WIRELESS NETWORKS

Information transmitted via public WiFi 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 (http://www.shrew.net) to encrypt your mobile activities.

Navigate to Settings > WiFi

- **Disable WiFi when not in use**

Navigate to Settings > General > VPN to enable and establish a VPN connection

- **Enable network permissions**

#### ANDROID

Navigate to Settings > WiFi to manage connections

- **Disable WiFi when not in use**

Navigate to Settings > More > Tethering & Portable Hotspot and disable Portable WiFi Hotspot

- **Uncheck**

Navigate to Settings > More > VPN to enable and establish a VPN connection

- **Enable network permissions**

#### CONNECTING VIA BLUETOOTH

Bluetooth involves the wireless communication of two devices within a close geographical proximity. When Bluetooth is enabled, hackers may be able to access the connection to your calendars, emails, messages, and photos without your knowledge. Avoid using Bluetooth and disable it when it is not being used.

Navigate to Settings > Bluetooth to disable services

- **Disable Bluetooth when not in use**

Navigate to Settings > Personal Hotspot to disable broadcasting your private Internet connection with others

- **Never share your Internet connection**

Navigate to Settings > More > NFC to manage Near Field Communications settings, which enable smartphones to transfer data by touching the devices together

- **Delete**

#### DATA RETAINING APPS

Downloaded apps frequently collect user's personal information to sell to third party data aggregators. Native applications such as Siri and Google Now will also collect data from users which may include name, email address, credit card numbers, contacts, and device information. These services also record and catalogue the audio during sessions. Avoid using these voice recording services.

Navigate to Settings > General > Siri

- **Disable Siri**

Navigate to Settings > Privacy to manage which specific data each app accesses from your phone

- **Turn OFF**

Navigate to Settings > Apps

- **Delete apps that use excessive # of personal data**

#### APPS USING REAL-TIME LOCATION

The majority of apps in the market 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 retain their location information inside their EXIF data. Be aware that your location is being shared when photos are uploaded from your smartphone to a SNS.

Navigate to Settings > Privacy > Location Services

- **Only grant access to apps that require a location function**

Navigate to Settings > Location Access

- **Disable all location services when not in use**

Navigate to Settings > Location Access

- **Uncheck both boxes when location services are not in use**
TRAVELING SAFELY 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 to protect you against the newest technical vulnerabilities
- Assume that all information on your device could be compromised while traveling in a foreign country; leave sensitive information off of your phone
- Use VPN to protect your phone when accessing WiFi 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

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

IPHONE

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

Go to Settings > About Phone > System Updates.

Your system is up to date.

Last checked for update at 12:19 PM.

Check for update

Check to see if your software is up-to-date; if not, your phone will prompt you to download 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

Use the Lookout app for iPhone. Go to Security to see if your phone has any malicious apps.

No malicious apps detected

Lookout checks your apps for malicious activity that can compromise the security of your device and personal information.

ANDROID

Use the Avast Antivirus Free app for Android. Click Scan Now to monitor for viruses.

Scan this device

Run your first scan

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

Go to Settings > General > Auto-Lock. Set the Auto-lock to 1 Minute.

Go to Settings > Touch ID & Passcode. Set Require Passcode to Immediately.

ANDROID

Go to Settings > Choose your password to enable password protection.

Go to Settings > Security > Automatically lock > Immediately.
DISABLE WIFI AND BLUETOOTH

Disable WiFi and Bluetooth on your smartphone when you are not using them; WiFi and bluetooth can render your smartphone vulnerable to malware.

**iPhone**

- **Settings > WiFi.** Turn Wi-Fi OFF
- **Settings > Bluetooth.** Turn Bluetooth OFF

**Android**

- **Settings > WiFi.** Turn Wi-Fi OFF
- **Settings > Bluetooth.** Turn Bluetooth OFF

USE VPN ON WIRELESS NETWORKS

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

**iPhone**

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

**Android**

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

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**

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

**Android**

- Use the Avast app to recover lost or stolen Android smartphones and wipe data remotely from the device.
EXIF REMOVAL - DO'S AND DON'TS

• Remove EXIF data before sharing or posting images, especially when images are captured in private homes or businesses.
• Whenever possible, use an EXIF viewer to verify that personal data is removed from photos, and prevent your phone from including geolocation data.
• Before uploading images, use 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 with no EXIF data, the content of images may contain identifying information, including associated persons and locations. Screen content with the assumption that anyone can see, copy, or forward photos that you post online.

EXIF DATA

EXIF (Exchangeable image File Format) 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+, 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, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod</td>
<td>Ability to reveal the exact location of private places, such as homes or offices. Some photosharing sites, including Google+ 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 particular device for 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, UniqueImageID, UserComment</td>
<td>Potentially reveals identifying information about those captured in the image by providing additional content regarding persons + locations.</td>
</tr>
</tbody>
</table>

Limiting EXIF data, especially geolocation information, before distributing image files can help protect your online 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 on a device running iOS 7 or Android Jelly Bean will create a new image containing no EXIF data. To take a screenshot on an iOS device, simultaneously press the lock and home buttons; with a Galaxy S3 or Note, press the power and home buttons simultaneously; with a Nexus 4, press the lock and the volume-down buttons simultaneously.
• Photos taken in airplane mode still contain geolocation data. To prevent this data capture, turn off location services/storage for your smartphone’s camera application, as shown below.
• Remember that uploading or sharing a lower quality image will still contain EXIF data. EXIF data and image quality have no correlation.

IOS (V. 6.0.1)

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 applications.
3. Return to the Settings app and navigate to Privacy > Photos.
4. Disable the permissions for other apps to access photos already stored in your device’s Camera Roll.

ANDROID (V. 4.3)

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

1. Open the camera app. A white camera symbol in the bottom right corner indicates the app is in camera mode.
2. Tap the white circle in the bottom right corner to bring up a cluster of options in the middle of the screen. Click settings symbol.
3. Click the location icon on the far left to disable location data.
4. When the location symbol appears with a line through it, then location data has been successfully disabled.
**EXIF REMOVAL SMARTPHONE APPS**

### TRASHEXIF FOR IOS

TrashEXIF is a free app that deletes EXIF information from image files stored on your iOS device.

1. Download the TrashEXIF app from the App Store.
2. Open the TrashEXIF app and select photo(s) which you want EXIF data removed.
3. Select Presets, then in the Removal Presets window, select Remove Location and Remove Device Information.
4. Return to the previous screen by clicking the name of the image in the upper-left.
5. Scroll down and click Remove Exif. This creates a copy of the image file(s) without EXIF and does not alter the original image file. The copy without EXIF data is displayed as most recent in your iPhone Photo app.

### PHOTOINFO ERASER FOR ANDROID

PhotoInfo Erase is a free app that deletes all EXIF data from image files stored on your Android device.

1. Download PhotoInfo Erase from the Play Store.
2. Open the PhotoInfo Eraser app and select Gallery.
3. Navigate your phone and select an image.
4. Select Tag Delete and press OK.
5. Click Gallery. A copy of your photo without EXIF data is now available in the PEraser folder.

### VIEWING AND REMOVING EXIF DATA ON OS X

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

1. Open the ImageOptim application.
2. Drag the photos 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 select Get Info. EXIF data is listed under More Info.

### VIEWING AND REMOVING EXIF DATA IN WINDOW 8

Use the Windows 8 OS 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 8 also allows system administrators to remove all EXIF data from the selected image by clicking the Remove Properties and Personal Information link.
MOBILE WALLETS

MOBILE WALLETS - DO'S AND DON'TS

- Utilize all available PIN, password, and fingerprint protection options.
- Turn on notifications, and regularly monitor transaction history for unauthorized payments.
- Only transfer money to people or merchants you know and trust.
- 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.

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 at the point-of-sale using a QR code or NFC chip (near field communication). You can pay selecting a specific card, account, or existing balance, if available.

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

RISKS OF USING MOBILE WALLETS

Consolidating multiple cards into a single app exposes you to an increased risk. 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 habits, activity, and finances.

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, as shown to the left.

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>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>Photo, phone number, email, debit card number</td>
<td>CVV requirement before transfer</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Apple Pay</td>
<td>iOS</td>
<td>User to merchant</td>
<td>Full name, billing address, shipping address, email, phone number</td>
<td>Fingerprint required for transactions</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Google Wallet</td>
<td>iOS, Android, browser</td>
<td>User to friend, User to merchant</td>
<td>Photo, full name, email, bank account, card numbers</td>
<td>PIN</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Venmo</td>
<td>iOS, Android, browser</td>
<td>User to friend</td>
<td>Photo, full name, email, about (optional), phone number, bank account, card numbers</td>
<td>PIN or fingerprint</td>
<td>Facebook (optional), internal social features</td>
<td>In-app contacts</td>
</tr>
<tr>
<td>LevelUp</td>
<td>iOS, Android, browser (limited)</td>
<td>User to merchant</td>
<td>Full name, email, birthday, gender, card numbers</td>
<td>PIN or fingerprint</td>
<td>Facebook (optional)</td>
<td>Private</td>
</tr>
<tr>
<td>PayPal</td>
<td>iOS, Android, browser</td>
<td>User to friend, User to merchant</td>
<td>Photo, full name, email, phone number, bank account, card numbers</td>
<td>Password</td>
<td>None</td>
<td>Private</td>
</tr>
</tbody>
</table>
Navigate to **Settings** in the upper left portion of the home screen:

- Add your **Email Address** to verify your account.
- Require **CVV Security Code Lock**.
- Enable **Push Notifications**.

Utilizing Cash’s Bluetooth-based Nearby option allows you to be seen by nearby users. This feature is not recommended.

An activity log is located in the upper right portion of the home screen. Monitor this section for unauthorized transactions.

### SQUARE CASH

### APPLE PAY - IPHONE ONLY

In the **Settings** > Passbook & Apple Pay menu, add credit or debit cards you wish to use with the service.

Note that an unauthorized user of your iPhone can view the last 4 digits of your cards, your billing address, shipping address, email address, and phone number.

To mitigate the risk of exposing personal information, enable PIN, password, or fingerprint protection for your iPhone’s lock screen. Use more than one of these options to ensure extra security and protection.

### GOOGLE WALLET

In the **Settings** menu:

- Turn on Notifications for Wallet Card purchases.
- Set PIN Timeout to ‘15 minutes.’
- Check Monthly statements for unauthorized transactions.
- Monitor the Transactions section of the sidebar for unusual activity.

**Note to Android users:** It is recommended you disable all location services by navigating to **Settings** > **Privacy** > **Location Services** and set Wallet location access to **Never**.

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

### VENMO

Navigate the dropdown menu to **Settings**:

- Under **Notifications**, enable push notifications for payment sent, trust charge received, and bank transfers to Venmo completed.
- Enable **Touch ID & Passcode** and turn on **Use Touch ID**.
- To limit social visibility, under **Privacy**, set audience for future transactions to **Private**.
- **Who can share transactions involving you?** to **Only Me**. Make all past transactions ‘Private.’
- Venmo provides an option to ‘trust’ friends and automatically pay their requests. Utilizing this feature is not recommended.

Monitor your transaction activity by clicking on the logo of a single person at the top of the home screen.

**iPhone users:** navigate to your phone’s **Settings** > **Privacy** > **Location Services** and set Venmo location access to **Never**.

### LEVELUP

Navigate to the **Settings** menu, found in the top left corner of the home screen:

- Monitor your transaction history under **Transaction History**.
- Enable PIN lock.
- iPhone users should utilize the Touch ID lock option.
- Do not connect your Facebook account to LevelUp.

**iPhone users:** navigate to your iPhone’s **Settings** > **Privacy** > **Location Services** and set LevelUp location access to **Never**.

### PAYPAL

Navigate to **Settings**:

- Upload an up-to-date **My Photo** to protect against fraud.
- Set a PIN under **Mobile Number and PIN**.
- Verify your phone number **Mobile Number and PIN**.
- Turn on all options under **Notifications**. Your account activity can also be monitored on the **Activity** home screen.
- Only enable Bluetooth when engaging in an in-store transaction.

**iPhone users:** navigate to your iPhone’s **Settings** > **Privacy** > **Location Services** and set PayPal location access to **Never**.
SECURING HOME WIRELESS NETWORK

- 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 device's firmware or periodically check for updates on the device's website.
- Limit the reach of your router's signal; position the router further towards the interior of your house and decrease the signal strength.
- Use an ethernet cable instead of a WiFi connection when possible; disable the wireless network when it will not be used for an extended time.
- Enable your router's firewall and strong encryption to block a number of 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.

WIRELESS NETWORKS OVERVIEW

Home wireless networks allow users to connect multiple devices to a single, remote Internet network. While wireless technology makes it easier for individuals 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.

To begin configuring your wireless network's security settings, you must first gain access to your router. Begin by launching any web browser and entering 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.

CHANGING ROUTER LOGIN SETTINGS

Routers often come preconfigured with a default username and password (e.g. Username = "Admin" and Password = "Password"). The first step toward securing your network should be to change these fields to more secure entries. Usernames should not represent your name, home address, or any other personal identity data. Passwords should be complex and different from the password used to access your network.

Insert image with login settings dialog box.

DISABLEING REMOTE ADMINISTRATION

Disable the remote administration of your wireless router to ensure that individuals cannot make changes to your router remotely. You can accomplish this by setting the remote management IP address to "0.0.0.0".

Insert image with remote management IP address configuration dialog box.

CREATING A NETWORK NAME AND PASSWORD

The Service Set Identifier (SSID) field is used to change the personalized name of your wireless network. Your wireless network name should not reveal any personally identifying information. Your network password — or Pre-Shared Key (PSK) — is the password that you use to connect to the Internet and it is distinct from the password that you use to login to your router. Your PSK password should also be long and complex.

Insert image with network name and password configuration dialog box.

DISABLING REMOTE ADMINISTRATION

Disable the remote administration of your wireless router to ensure that individuals cannot make changes to your router remotely. You can accomplish this by setting the remote management IP address to "0.0.0.0".

Insert image with remote management IP address configuration dialog box.

LIMITING ADMINISTRATIVE ACCESS

Add the Media Access Control (MAC) Addresses — unique individual identifiers assigned to computers and devices — for each computer and device you wish to have administrative access to your network.

Insert image with MAC address configuration dialog box.
Limit the number of MAC addresses you approve to maximize network security.

MAC Address Filter List

<table>
<thead>
<tr>
<th>MAC</th>
<th>Limit the number of MAC addresses you approve to maximize network security.</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0A:00:00:AA</td>
<td></td>
</tr>
<tr>
<td>00:0A:00:00:AB</td>
<td></td>
</tr>
<tr>
<td>00:0A:00:00:AC</td>
<td></td>
</tr>
<tr>
<td>00:0A:00:00:AD</td>
<td></td>
</tr>
<tr>
<td>00:0A:00:00:AE</td>
<td></td>
</tr>
<tr>
<td>00:0A:00:00:AF</td>
<td></td>
</tr>
</tbody>
</table>

What to do if you suspect your network has been compromised

Following the recommendations outlined in this card will significantly reduce your network’s chances of becoming compromised. However, it is wise to periodically check to see 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 it is determined 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 resecure 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 was able to gain access to your login credentials or other personal data.
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 other 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 during registration.
- Remove any identity data from your personal profile that was required during signup after completing the registration process.
- Change privacy settings to protect your identity information immediately after registering for an online profile.

IDENTITY ELEMENTS OF SNS ACCOUNTS

Your online identity is the aggregate of your online accounts and their associated personal identity data fields. Therefore, protecting your identity must begin as early as registering your online accounts. The identity data shown below is often required when registering social network accounts.

FIRST AND LAST NAME

First and last name are mandatory for almost all SNS accounts. In order to better protect yourself, use an alias or use the initial of your last name instead of its full version, especially if you have an uncommon last name.

DO NOT use the same password or username across multiple SNS accounts. Ensure that your passwords are complex and unique.

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, including your name, location, or birthday.

EMAIL ADDRESS

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

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. Only provide your true birth year.

LOCATION INFORMATION

Location information is required at varied levels of granularity depending on the service. It may include address, city, ZIP code, and/or country. During sign up, only provide the most generic location level required by the service or consider entering a nearby ZIP code or metropolitan area.

SOCIAL LOGIN

Services may allow users to sign up through a preexisting social network (e.g. Google Plus, Twitter, or Facebook). Avoid opting for this step unless the service requires it.

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 generic as possible (i.e. only provide the industry you work in). Avoid posting your employer and your work location.

RELATIONSHIPS/ ORIENTATION

Relationship statuses and sexual orientations are almost always optional data fields, except for online dating sites. Refrain from sharing this data with the service unless it is required.
IDENTITY INFORMATION REQUIRED DURING REGISTRATION BY SERVICES

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Outlook</th>
<th>Yahoo</th>
<th>Facebook</th>
<th>Twitter</th>
<th>Google Plus</th>
<th>LinkedIn</th>
<th>Pinterest</th>
<th>Instagram</th>
<th>Yelp</th>
</tr>
</thead>
<tbody>
<tr>
<td>First and last name</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Username</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Password</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Birthdate</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Email address</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Phone number</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Country</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company / Employment</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>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZIP code</td>
<td>X</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></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 a select 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.

First name
Last name
Email or mobile number

Account Confirmed
Your account has been confirmed. You can now use all of Facebook's features and connect with friends.

token is: 556584
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.
- 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 collecting public records information and extensive web indexing + 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

PRIVATEEYE, PEOPLEFINDERS, PUBLICRECORDSNOW, AND VEROMI

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


Complete the form, and mail it to the listed address.

Opt out of PeopleFinders and PublicRecordsNow by visiting: 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. Select No thanks, skip this step.

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.

INTERNATIONAL OPTING OUT INSTRUCTIONS

US SEARCH


Search for your name and click on the appropriate listing. Print the cover sheet and mail or fax with a copy of a state-issued ID or driver’s license to the listed address or fax number.

INTELIUS, PUBLIC RECORDS, ZABASEARCH, SPOCK, ISEARCH, DATECHECK, LOOKUP, PEOPLEFINDER, LOOKUPANYONE, PEOPLE LOOKUP, AND PHONESBOOK

Intelius owns, or is affiliated with, the following people search websites: Public Records, ZabaSearch, Spock, iSearch, DateCheck, Lookup, PeopleFinder, LookupAnyone, People Lookup, and PhonesBook. When you request removal of your records, also request removal from this network of sites. Opt out of Intelius online at http://intelius.com/optout.php. You can also fax your ID and a letter containing the information you want removed to 425-974-6194, using the following coversheet:

“As per your privacy policy, please remove my listing from Intelius, Spock, iSearch, ZabaSearch, Public Records, People Lookup, PhonesBook, DateCheck, LookupAnyone, and all other affiliated people search sites. Thank you for your help with this personal security issue.”

INSTANTCHECKMATE

To opt out of InstantCheckMate, follow the instructions at: www.instantcheckmate.com/optout

You can opt out by mail or online. You must include your full name, current address, email, and date of birth in order to opt out.

www.instantcheckmate.com

www.intelius.com

www.zabasearch.com

www.peoplesmart.com

www.peoplelookup.com

www.i-search.com

www.veromi.com

www.publicrecords.com

www.peoplelookup.com

www.phonesbook.com

www.lookupanyone.com
OPTING OUT INSTRUCTIONS CONTINUED...

**BEEN VERIFIED**

BeenVerified allows you to opt out at: beenverified.com/optout. Search for your listing, and claim it with the That's Me! button. Enter your email address. You must click the opt out link within the email sent to your account by the service.

www.beenverified.com/

**PEEKYOU**

Fill out the PeekYou opt-out form at: 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, fill in the CAPTCHA, and you’re all set. You’ll get an immediate 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.

www.peekyou.com

**SPOKEO**

To opt out of Spokeo, first find your listing, then visit Spokeo’s opt-out page: www.spokeo.com/opt_out/new.

Enter the URL of your listing and your email address. Go to your email, and click on the removal confirmation link.

www.spokeo.com

**WHITEPAGES**

Search for your information on Whitepages using your first name, last name, city, and state. Before deleting these records you must first register with the service. Click on your name in bold in the Filter by Age block. Copy the URL address at the top of your screen. Scroll down to the bottom of the screen and under Your Whitepages select Remove From Directory. On the Log In screen, select Sign up, and fill in your name, email address, and a new password. Select Create an account. You will be sent an email at the address you listed. Click the “Verify my email” link provided. Once you verify your email, you will then be taken to the Opt-out of Whitepages screen, paste the URL and click on Opt-out. If the information shown is correct, click on Remove this info from Whitepages. Select a reason from the drop down box and click on Next step. Verify the phone number, check the box, and click on Call now to verify. Answer the call and press 1.

www.whitepages.com

**US IDENTITY**

To opt out of US Identify, send a request to:

9450 SW Gemini Dr. Suite #29296
Beaverton, OR 97008-7105

In the request, write: “I would like all information for [Name] [Date of Birth] [Current City and State] removed from usidentify.com and all affiliated sites.” Be sure to include aliases, if applicable.

www.usidentify.com

**PIPL**

Search for your information on pipl using your first name, last name, city, and state. Go to www.pipl.com/directory/remove. Ignore the instruction to copy the page address, and enter the page address in the format shown. Add your email address and click SUBMIT. The next page will show any listings with your name or a name close to it. Click Remove for each item you want deleted. You will be sent one or more emails at the address you listed. You must click on the confirmation link provided in each email.

www.pipl.com

Identity Awareness, Protection, and Management Guide
IDENTITY THEFT PREVENTION

IDENTIFY THEFT PREVENTION - DO’S AND DON’TS
- Create unique passwords for each of your accounts to limit the chances of having multiple accounts compromised.
- Keep your computer up-to-date with the latest versions of your operating system and anti-virus software protection.
- Avoid sharing sensitive information such as credit card or Social Security numbers through text, email, 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. Every year, approximately 9.9 million incidents of identity theft are reported, equating to 19 individuals falling victim every minute. On average, each victim spends 30 to 60 hours and 50 to 500 dollars trying to resolve the issue. While the common conception is that identity thieves are online scammers, new evidence indicates that up to 50% of all reported cases involve theft from a neighbor, co-worker, or family member. Most identity theft cases can be resolved 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 assets at risk.

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

POSSIBLY HARMFUL
- Pets’ RFID Numbers
- Utility Account Numbers
- History of Residence
- Unsolicited Credit Offers

WHAT IS AT RISK?

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

FAKE WIFI NETWORKS
Fraudsters may establish fake WiFi hotspots to mimic public internet access points. Avoid communicating personal and financial information over public WiFi connections, and do not access any unsecured networks.

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 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 a 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@YYYY.ZZZ>
Reply-To: XXXXXX@YYYY.ZZZ>
Date: Mon, 23 Nov 2014 12:34:13 -0700
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 forfitur of funds. To see a summary or your account activity, open the attached documents or visit our Security Center.

*Data Source: Consumer Sentinel Network for total theft reports in 2014. Some reports contained multiple theft types.

AGE OF VICTIMS
- 19 and Under (6%)
- 20 to 39 (36%)
- 40 to 59 (38%)
- 60 and Over (20%)

*Presence of grammatical or spelling errors.
*Absence of a company logo within the email header.
*Non-descriptive senders or mismatched email addresses (e.g. the “From” and “Reply-To” addresses do not match).
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 leak of identity data during online activity.

### DATA PROTECTION AND RECOVERY SERVICE OFFERINGS

<table>
<thead>
<tr>
<th>Service</th>
<th>SSN</th>
<th>BANK ACCOUNT</th>
<th>CREDIT CARD NUMBERS</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 PER MONTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Guards</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Monthly</td>
<td>Up to $1 Million</td>
<td>$19.99</td>
</tr>
<tr>
<td>Identity Force</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Quarterly</td>
<td>Up to $1 Million</td>
<td>$18.95</td>
</tr>
<tr>
<td>Trusted ID</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Available</td>
<td>Up to $1 Million</td>
<td>$16.99</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 [www.annualcreditreport.com](http://www.annualcreditreport.com) to request free copies of your credit scores. Look for inconsistencies amongst 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.

**Create an Identity Theft Report:**

File an online complaint with the Federal Trade Commission (FTC) at [www.ftc.gov/complaint](http://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](http://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.

---

**Identity Awareness, Protection, and Management Guide**
KEEPING YOUR KIDS SAFE ONLINE

KEEPING YOUR KIDS SAFE ONLINE - 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 that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
• 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 don't use your face as a profile photo - use cartoons or avatars instead.
• Use secure browser settings when possible, and monitor your browsing history to ensure that you recognize all access points.

CHILD SAFETY ONLINE

A 2013 study reported that 96% of children above the age of 8 claimed to actively use the Internet, where kids are at risk of being exposed to cyber-bullying, coercion, pornography, drugs/alcohol, and violence. Dangers were not limited to the content that a child was subjected to, but also included the information that the child made available to the public through social networking services (SNS). The following web browser settings, add-ons, and software downloads are available to prevent and/or monitor a child’s activities online.

INTERNET EXPLORER SETTINGS

To view child safety options, navigate to Tools > Internet Options > Content. Click Parental Controls (Internet Explorer 9) or Family Safety (Internet Explorer 10) to customize settings for the different accounts registered on the computer.

Set up how Child will use the computer

Parental Controls:
- On, enforce current settings
- Off

Windows Settings

Time limits:
- Control when Child uses the computer

Games
- Control games by rating, content, or title

Allow and block specific programs
- Allow and block any programs on your computer

More Settings
- ContentWatch-Administrator Tools
  Provides access to ContentWatch-Administration

Current Settings:
- Child
- Standard user
- No Password

Web Restrictions:
- ContentWatch Filter

Time Limits:
- Time Limits: Off
- Game Ratings: Off
- Program Limits: Off

PARENTAL CONTROLS

Adjust how your children can use the computer. Allow or block specific programs, and set personalized restrictions based on game ratings.

PASSWORDS

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

TIME RESTRICTIONS

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

DOWNLOAD THE BLOCKSI EXTENSION FROM THE GOOGLE CHROME WEB STORE TO EMPLOY CHILD SAFETY SETTINGS FOR THE GOOGLE CHROME BROWSER.

ADVANCE CONTROL

Set a time frame of acceptable computer use for your child that permits an adult supervisor to be present.

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 CONTROL

Set a time frame of acceptable computer use for your child that permits an adult supervisor to be present.

STANDARD FIREFOX

Navigate to Firefox > Options > Privacy to prevent web tracking and Firefox > Options > Security to block sites with malicious content.

FOXFILTER FOR FIREFOX

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

SENSITIVITY SETTINGS

Always opt-out of website tracking

Examine URL (Web Address)

Examine Title (Title that appears in browser title bar)

Examine Meta Content (hidden keywords, description, etc. which are used for search engine placement)

Examine Body Content (visible content of the Web page)
A variety of free and paid software are available for monitoring your child’s online activities. The software listed below are effective in either preventing or monitoring content that your child tries to access.

**CAPABILITIES**

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

**NORTON FAMILY**

Register online with this service to monitor your child’s online activity. This service allows parents to track which websites children visit and prevent certain harmful content from being displayed on their monitors. Information reported to the parent includes websites visited, timestamps, searches conducted, and actions taken by the Norton Family security suite.

**Microsft Family Safety**

Download this free service from the Microsoft Windows website. The service provides basic content filters and reports of programs/websites accessed by each account.

Parents 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 prevent and monitor content from computer programs, instant messengers, SNS, and web browsing applications. It is installed onto the desktop and provides the most granular settings for filtering and reporting potentially harmful content.

Parents can respond to their child’s permission requests remotely from a mobile app or computer in real time. Additional settings include blocking 64 Bit applications, HTTPS 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 Family 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) - DO’S AND DON'TS

• Determine the features you need. VOIP services range from free smartphone apps to full-featured subscription enterprise systems.
• Check your bandwidth. You may need to upgrade your Internet connection to get the best use of bandwidth-heavy VOIP services.
• Keep a landline or cellphone active for times when Internet service is not available, power is out, or for calls to emergency services.
• Watch your wallet. Keep an eye out for hidden charges for licensing and support or free trials that may become long-term contracts.
• Ask about your VOIP provider’s disaster recovery plan in the event of a system failure.

WHAT IS VOIP?

Voice Over Internet Protocol, or 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, 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 WiFi.

BENEFITS OF VOIP

VOIP calls are much less expensive, 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.

CHOOSING THE RIGHT PROVIDER

• 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 companies?
• Is live support available 24 hours a day, seven days a week?

VOIP DISADVANTAGES

As with any data online, VOIP is vulnerable to hacking. Also, service providers may be able to access even encrypted messages and store them indefinitely. **VOIP IS NOT considered secure for the purposes of transmitting sensitive data.**

A poor Internet connection can result in low call quality, delayed messages, or buffering during video chats.

Some providers do not connect to 911 or information 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.

How VOIP Works

Using VOIP SECURELY

Password-protect your apps, and encrypt or erase sensitive information, including texts, call history and voicemail. But keep in mind even if a service offers encryption, some providers may include a “back door” to allow for lawful government surveillance of communications, i.e. during a criminal investigation. 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 can not 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?
• Be sure your WiFi network is password-protected and uses strong encryption (WPA2).
• Change default passwords on equipment and the remote-management interface.
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. Among the most popular services: Ooma: $129 equipment purchase. Service is free (except taxes and fees) and calls to other Ooma users are encrypted. Vonage: $9.99 a month. Unlimited domestic calls and mobile app. Via Talk: $15.75 a month. Unlimited domestic calls.

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>OPERATING SYSTEM</th>
<th>COST</th>
<th>BEST USES</th>
<th>SECURITY RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype</td>
<td>Windows, Mac, iOS, web, Android</td>
<td>Free to $13.99/month</td>
<td>Filesharing, screen sharing, document collaboration, video calls</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Google Voice</td>
<td>iOS, Android, web</td>
<td>Free</td>
<td>Encrypted one-to-one or group audio/video calls, livestreaming video</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Silent Circle</td>
<td>iOS, Android, Windows</td>
<td>$12.95 to $39.95/month</td>
<td>Anonymous, encrypted calls and messages, identity verification</td>
<td>★★★★★</td>
</tr>
<tr>
<td>FaceTime/iMessage</td>
<td>iOS, Mac</td>
<td>Free</td>
<td>Encrypted audio and video calls and messages, voice memos</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Blackberry</td>
<td>Blackberry, iOS, Android</td>
<td>$29.99/yr for BBM Protected</td>
<td>Secure messaging</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Crypto-cat</td>
<td>iOS, Mac, web</td>
<td>Free</td>
<td>Secure messaging, encrypted filesharing</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

* The rating is based on encryption protocols, code reviews, audits, and documentation as compiled by the Electronic Frontier Foundation in March 2015.

SKYPE

Navigate to Settings in the pull-out menu:

- Indicate who you want to be able to call or instant message you.
- Be sure "Allow Microsoft targeted ads" is not checked to keep your profile information (age, gender, or location) or app usage from being used to serve ads.

On the "My Profile" page, do not upload a picture or enter personal information, such as your name, birthday, city, gender, or bio.

HANGOUTS

Sign up for a Google Voice (GV) account at google.com/voice for a free number or port your existing number. Give GV number to contacts. Install Hangouts app. In main screen menu, choose "turn history off."

In Settings:

- Check "Incoming phone calls" and "Messages" for Hangouts to manage all calls, texts, and voicemail.
- Customize who can contact you directly and who needs an invite.

SILENT CIRCLE

On launch, swipe right and check "Start silent phone on boot."

In Settings, select "Encrypt Silent Text" and select a passphrase (14 characters is recommended).

Activate "Burn Notice" in a conversation to auto-delete messages. To verify users, confirm passphrase by phone and tick box.

FACETIMÉ

For security, be sure to enable two-factor authentication for FaceTime.

- Go to Settings > Messages and turn on iMessage. Then tap "Send & Receive" and sign in with your Apple ID and password.
- Go to Settings > FaceTime and turn on FaceTime. Follow the steps to sign in and link your phone number to your Apple ID.