
Welcome to
IDENTITY MANAGEMENT
HIGHWAY
EXIT 1A
Identity
SECURITY
IDENTITY
Theft
SAFETY
#1
FORGERY
Merge Right
DETER • DETECT • DEFEND
AVOID
COMPROMISE
PROTECTION
LIKE
TWEET
FOLLOW
create
BLOG
content
Social
Media
SHARE
Caps
Shift
Alt

Contents

Version Date: 20150309

Identity Threats to Military and Veterans

20150111

According to the FTC, US military and veterans are twice as likely to suffer identity theft as the general public.

- Protect your personally identifiable information (PII)
- Older adults are more likely than the general population to be victims of white collar Internet fraud.
- 1.84 million Americans have been the victims of medical identity theft.
- The identities of 2.5 million deceased Americans are mis-used annually.
- Odds of being a victim of identity theft in a given year - 1 in 20.
- Odds of your child's personally identifiable information being misused before age 18 - 1 in 40.

Top Threats	Responses
Fake charity	Investigate charity before donating
Phone, email, letter phishing for PII	Never provide PII on phone or email; hang up if caller is suspicious; double check phone numbers with legitimate web site
Credit card theft	Shred documents with PII; check credit report frequently; credit freeze
Free membership; discounts	Nothing is free if traded for your PII
Fake survey with promised gift	Do not fill out survey or answer questions with PII

PII & Documents to Protect

- Name
- Birthdate
- Place of birth
- Mother's maiden name
- Vehicle registration, plate number
- Driver's license number
- Social Security Number
- Mailing and home addresses
- Email address
- Telephone number
- Credit card numbers
- Bank account numbers
- Medical insurance information
- Biometric attributes

Action to Take Online

- Avoid email scams
- Use strong passwords
- Use 2-factor authentication
- False answers to security questions
- Use secure websites
- No use of public WiFi
- Keep device's security software up-to-date
- Clear cookies and browser history frequently
- Understand privacy policies

Actions for the Physical World

♦ Be aware of your surroundings	♦ Use a locked mailbox
♦ Use checks sparingly	♦ Check financial statements often
♦ Invest in a home safe	♦ Read medical statements
♦ Shred documents and bills	♦ Request credit report annually
♦ Don't give out SSN	♦ Use credit instead of debit cards
♦ At ATMs look for skimmers & shoulder surfers	♦ Force photo ID check - write "See photo ID" in place of signature on credit cards

Resources:

Veteran's Administration hotline for vet victims of identity theft – (855) 578-5492

Identity Theft Resource Center

Federal Trade Commission tax fraud assistance

Internal Revenue Service identity theft assistance

Federal Bureau of Investigation reporting internet fraud

Source: Center for Identity, University of Texas - Austin

Facebook Smart Card

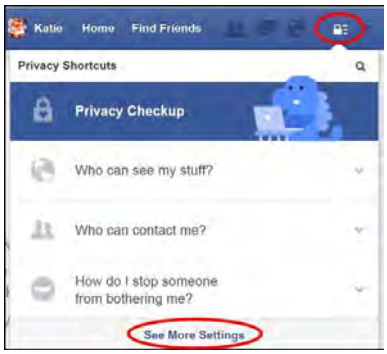
20141023

Minimizing Your Facebook Visibility

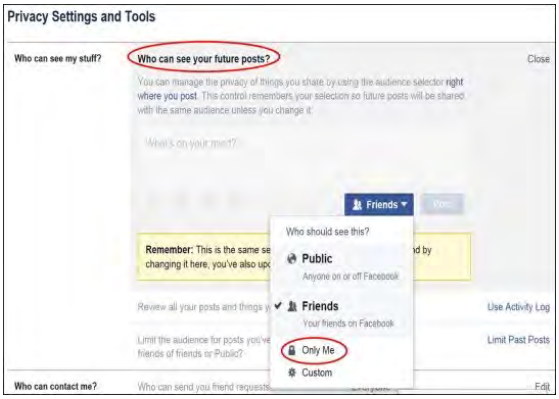
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; 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 don't 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.
- Do not login to or link third-party sites (e.g. Twitter, Bing) using your Facebook account. "Facebook Connect" shares your information, and your friends' information, with third party sites that may aggregate and misuse personal information. Also, use as few apps as possible, as most of them can access and share your personal data.

First, click on the *lock icon* in the upper right corner of your profile. Then click *See More Settings*.

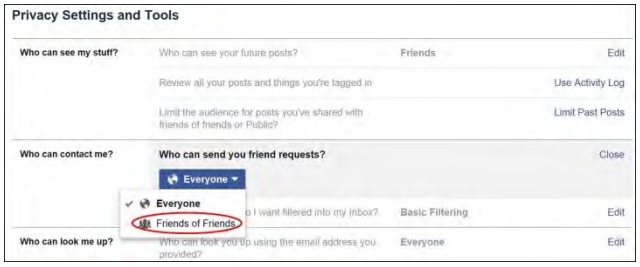
This brings you to the **Privacy Settings and Tools** menu. Now, you'll need to change **Who Can See My Future Posts?** to *Only Me*.



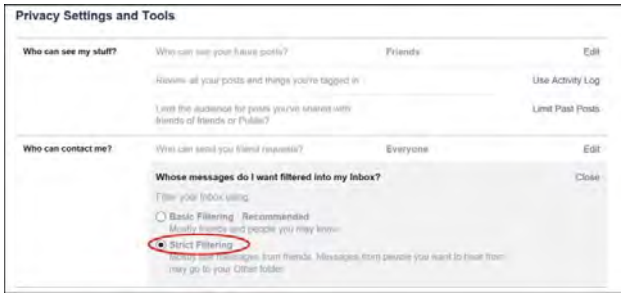
Next, you can change who can see your past posts by clicking *Limit Past Posts* and confirming the change. This will make it so your past posts are visible only to **your friends**, instead of the **public** or **friends of friends.**



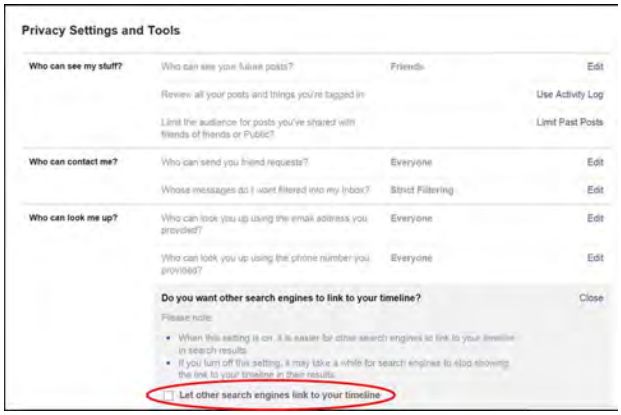
Next, switch **Who can send you friend requests** from *Everyone* to *Friends of Friends*. This will cut down on the number of random friend requests you receive.



To limit who can contact you privately via your inbox, change **Whose messages do I want filtered into my inbox** from *Basic* to *Strict* filtering.



This one's important. To prevent people who Google your name from being able to see a preview of your public Facebook Timeline, make sure you uncheck *Do you want other search engines to link to your Timeline?*



Facebook Smart Card

20141023

Next, click on *Timeline and Tagging Settings* to limit who can post to and see things on your Timeline. Make sure you change **Who can post on your timeline**, **Who can see posts you're tagged in on your timeline**, **Who can see what others post to your timeline**, and **When you're tagged in a post, who do you want to add to the audience if they can already see it** all to *Only Me*.

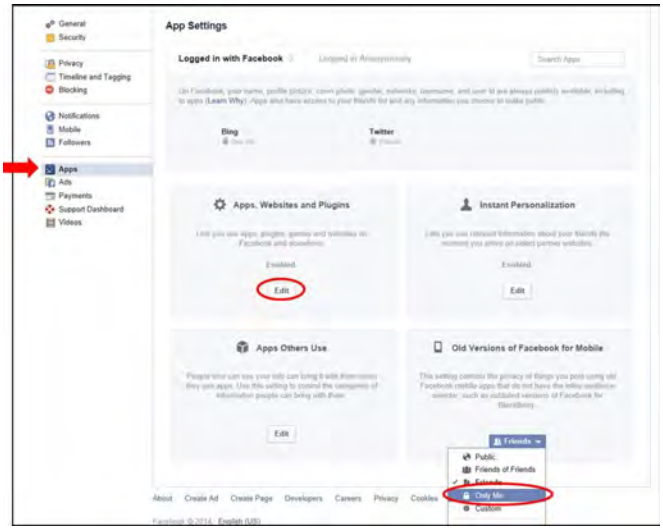
Now you'll want to give yourself a chance to review any posts or pictures you're tagged in. Change **Review posts that friends tag you in before they appear on your timeline** and **Review tags people add to your own posts before the tags appear on Facebook** both to *On*. Then change **Who sees tag suggestions when photos that look like you are uploaded** to *No one*.

Facebook also allows your followers, along with your friends, to see your public posts. To make sure your posts are visible only to your friends and not followers, change **Who can follow me** from *Everybody* to *Friends*.

Next, click on the *Ads* section on the left menu. This lets you choose if you want your name or social actions paired with an advertisement. For **Third-party sites**, select *No one*, and then **Save changes** to prevent this. Then do the same for **Ads and friends** below.

Next, click on the *Apps* menu to change what information of yours apps can see. To prevent them from seeing your information, change **Apps, Websites, and Plug-Ins** to *Disabled* from *Enabled*. This will also automatically update **Apps others use**, so your friends can't see your info if you've used the same app.

Lastly, you can control who sees your posts uploaded from old, outdated Facebook apps on old phones by changing the **Old versions of Facebook for mobile** to *Only Me*. After that, you're all set! You can now browse Facebook without broadcasting your every move.



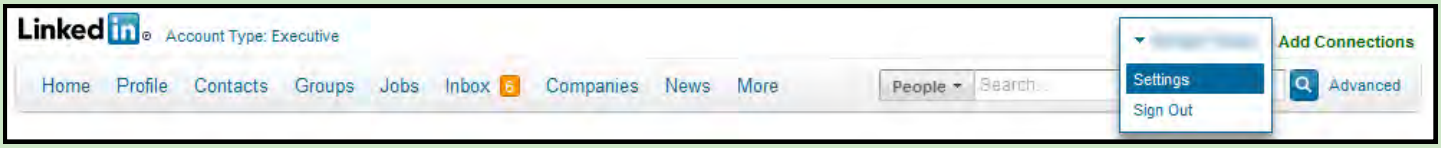
LinkedIn Smart Card

20141029

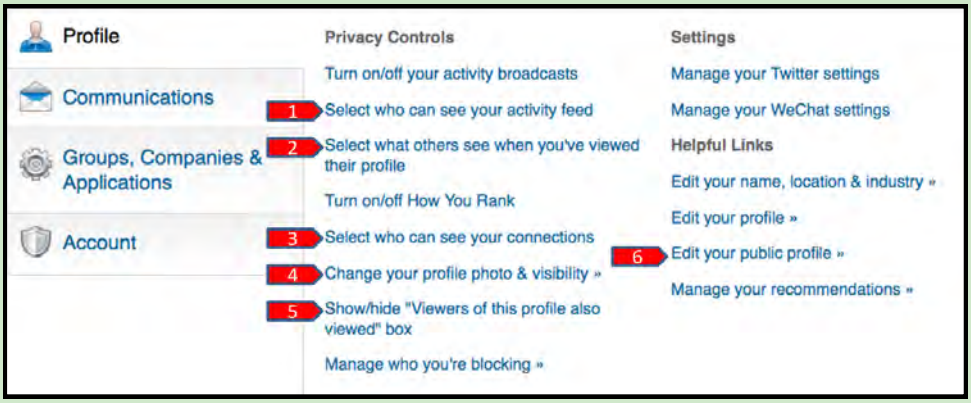
Social Networks - Do's and Don'ts

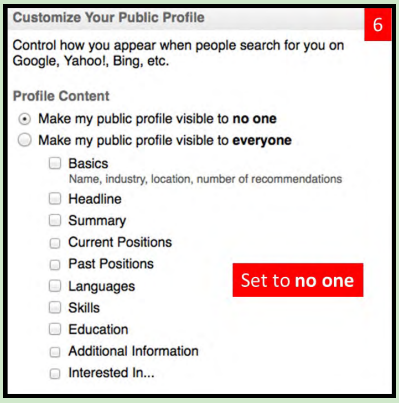
- Use an email account not associated with banking, finances, or other important contacts.
- Only establish and maintain connections with people you know and trust.
- Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life 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 your face. Select pictures that were taken at a distance, at an angle, or are otherwise concealed. Never post Smartphone photos, instead, use cartoons or avatars.

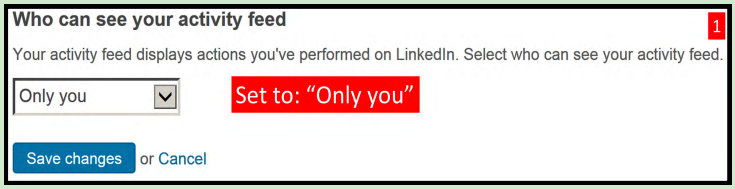
Managing Your LinkedIn Profile

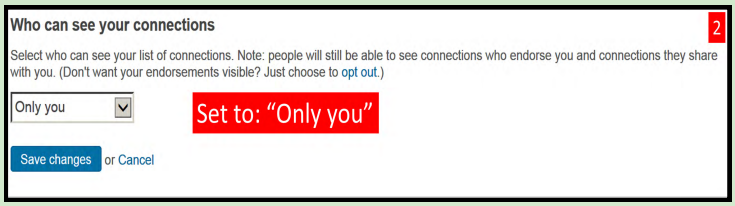


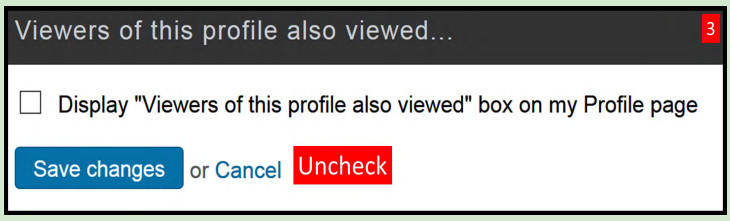
Apply the **Profile** settings shown below to ensure that your information is visible only to the people of your choosing.

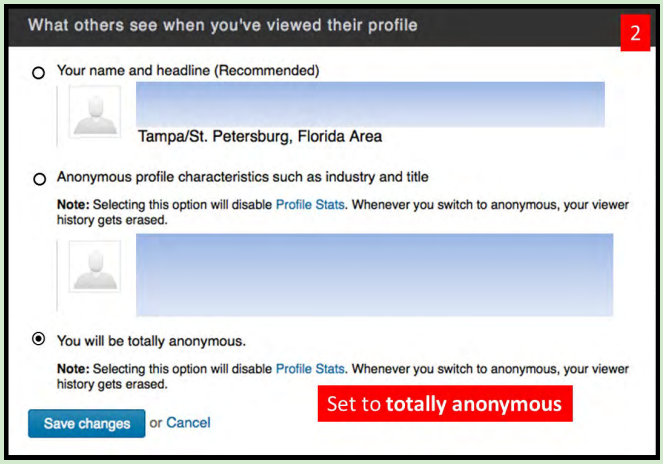


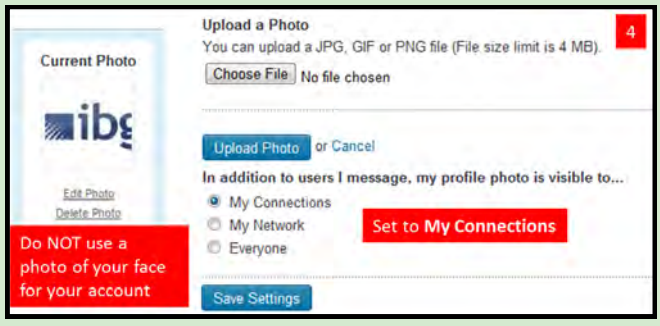












Terms of Use

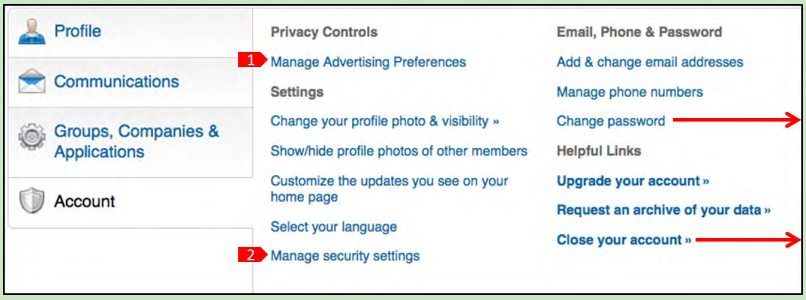
Unlike other social networking sites, LinkedIn's Terms of Service assure you that you retain full rights to content that you post on LinkedIn. Naturally, they cannot guarantee what others who see your content may do with it, but after you delete it, they do not retain it. While they won't alter the intent of your content, they reserve the right to format or translate it as necessary.

LinkedIn Smart Card

20141029

Account Settings

Apply the Account settings shown below to ensure that your information is shared in a limited fashion.

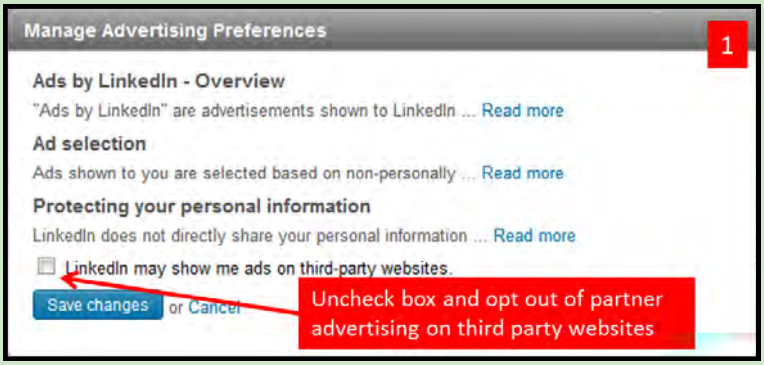


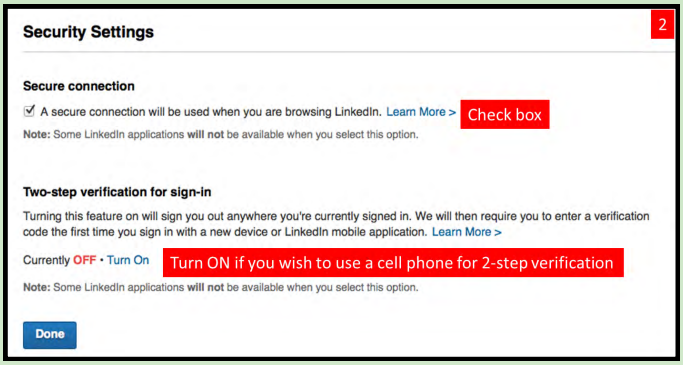
Passwords

Use complex passwords with capitals and numbers so hackers cannot access your account. Change password every 6 months.

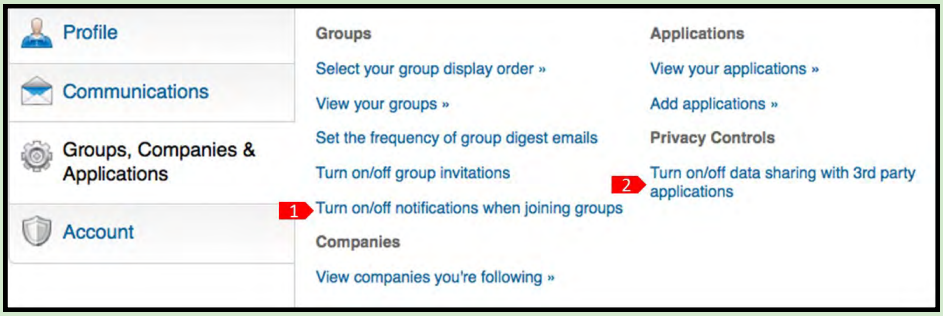
Closing Your LinkedIn Account

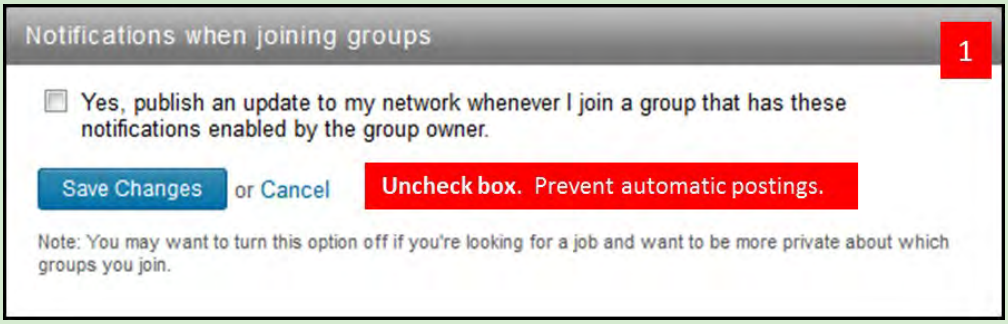
When you no longer want to use LinkedIn services, you can close your account by clicking on Close Your Account and confirm that you want to take that action.





Application Settings





Avoid using Twitter connect and the LinkedIn smartphone app to prevent accidentally sharing location data or personal information.

LinkedIn retrieves information about users on websites with LinkedIn Plug-In integration and reports comprehensive summaries of its users through the Bing search engine. Prevent sharing your activities on third-party websites with LinkedIn to protect your online identity.

Privacy Policy

You may delete imported contacts from address books. You may opt out of some site information collection. Site uses information about you to target ads. Site may use your location data to prevent fraud and security purposes. Your posts may be seen by advertisers unless in private groups. Plug-in impression data is de-personalized after 7 days. Site may review your InMails for support purposes but not advertising.

Useful Links

A parent's guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearing House	https://www.privacyrights.org/privacy-basics
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/social-networking.aspx

Twitter Smart Card

20140703

Social Networks—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 and friends take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you and your family that clearly show your face.
- 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. Instead, use avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Managing Your Twitter Account

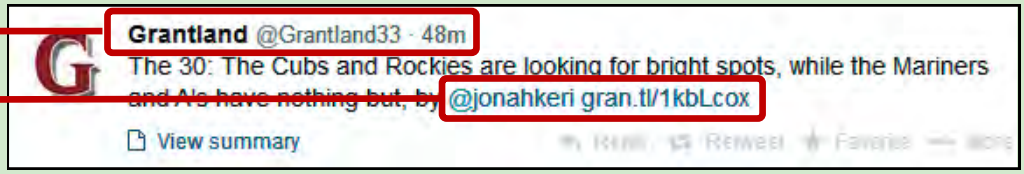
Twitter is a social networking and microblogging site whose users send and receive text-based posts online. As of October 2014, the site has approximately 271 million daily active users, generating 500 million Tweets and 2.1 billion search queries daily.

Following are people you subscribe to; **Followers** subscribe to your tweets; **Private Tweets** will only be visible to followers you approve

Tweets

"Tweets" are short text-based messages - up to 140 characters - that users post to Twitter. "Tweet" can refer to a post as well or to act of posting to Twitter. Tweets are public, indexed, and searchable unless protected by the user. Many users never Tweet, choosing only to follow persons or topics of interest.

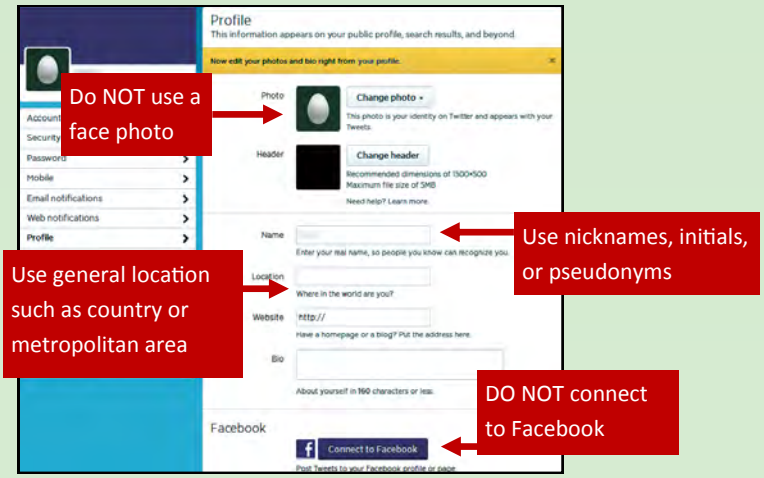
Mentions (@username) are used to tag a user in a Twitter update. When a public user mentions a private Twitter account, the link to the private account profile becomes public.



Hashtags (#topic) *are used to mark a keyword or topic in a Tweet. Posts that include a hashtag are categorized by topics in the Twitter search engine. Hashtagged words that become popular are Trending Topics (ex. #jan25, #egypt, #sxsw).*

Profile Settings

Apply the **Profile** settings shown below to ensure that your information is visible only to people of your choosing.



Twitter Best Practices

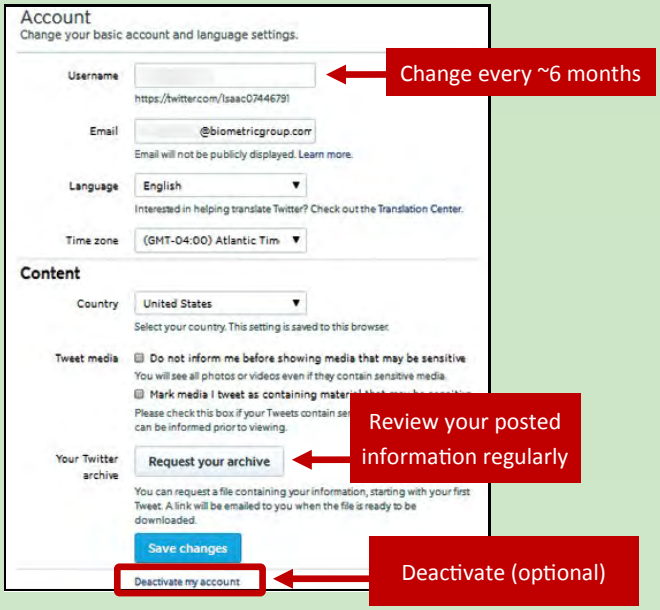
- Avoid using hashtags (#) in updates to prevent Twitter Search from indexing and associating your tweet with a topic.
- *Tweet responsibly*. Do not provide personal details regarding your whereabouts or activities in your post.
- Do **NOT** upload personal photos or websites.
- Do **NOT** allow Twitter to use your location on mobile devices.
- Change your Twitter **username** frequently to limit your account exposure.

Twitter Smart Card

20140703

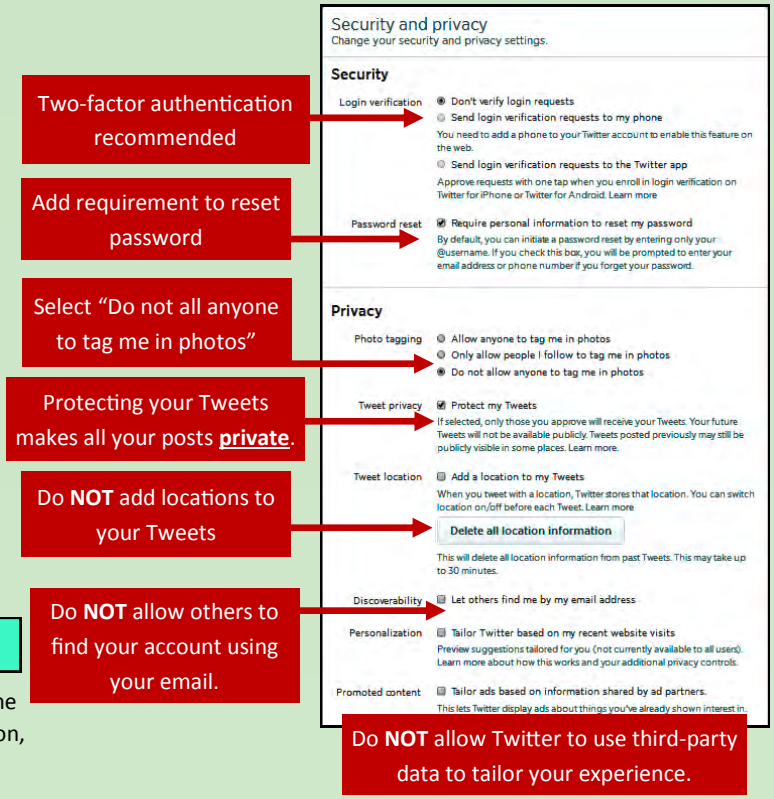
Account Settings

Apply the **Account** settings shown below to ensure that your information is shared in a limited fashion.



Security & Privacy Settings

Apply the **Security and Privacy** settings shown below to protect and reduce the visibility of your personal information.

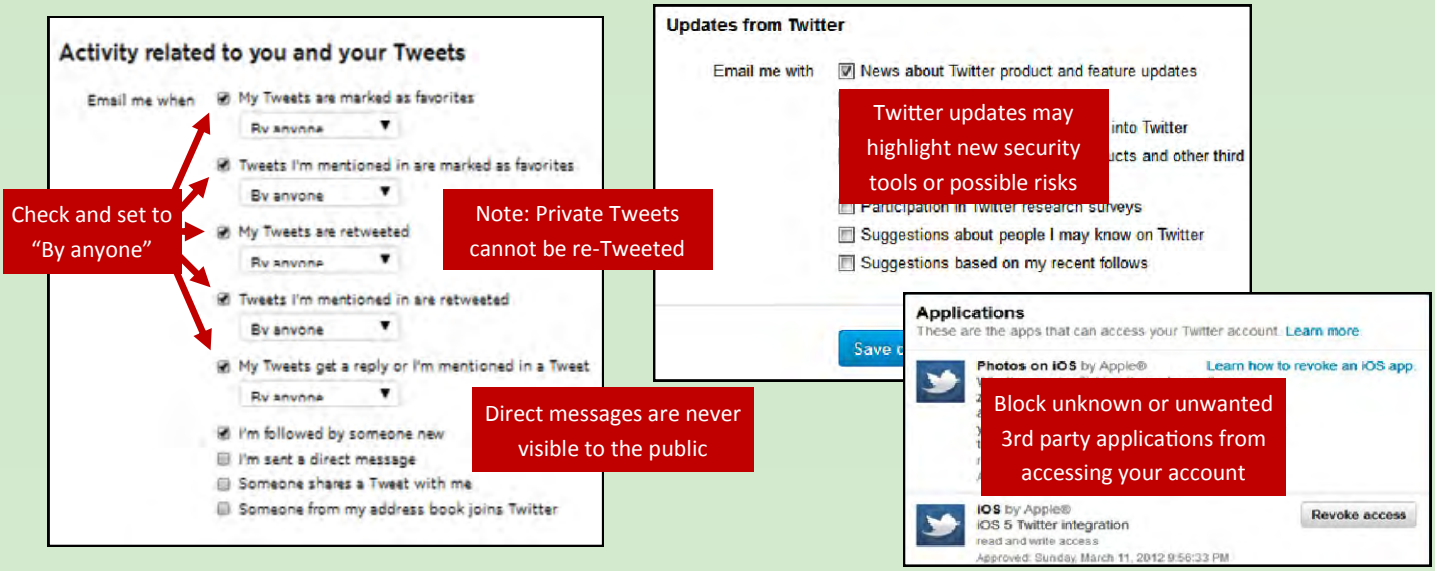


Deactivating / Deleting Your Twitter Account

To deactivate your account, go to **Settings**, and select **Account**. At the bottom of the page, click "**Deactivate my account**." After deactivation, the user can reactivate the account within **30 days**.

Notification & Application Settings

Maintain a small digital footprint by minimizing the number of notifications. Revoke access to unnecessary third applications.



Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	www.privacyrights.org/fs/fs18-cyb.htm
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/social-network
Online Guardian	www.onguardonline.gov/topics/social-networking-sites.aspx

Instagram Smart Card

20150304

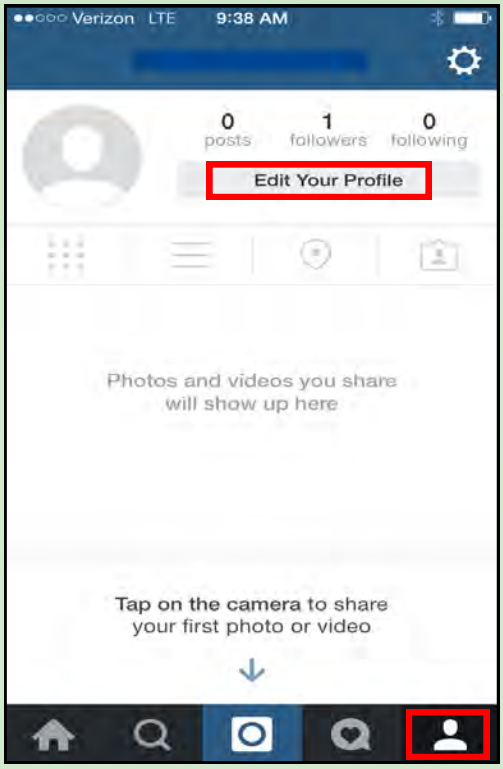
Do's and Don'ts

- Avoid using geo-location tags to prevent others from seeing your location.
- Only establish and maintain connections with people you know and trust. Understand that not everyone is who they say they are.
- There are privacy concerns when using your name and birthday when registering for "free" services such as apps and social media. It is not necessary to use your real name or birthday when registering for an account.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share. Assume that everything you post to your account is forever.
- Use caution when posting images of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities. Avoid full face photos.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.

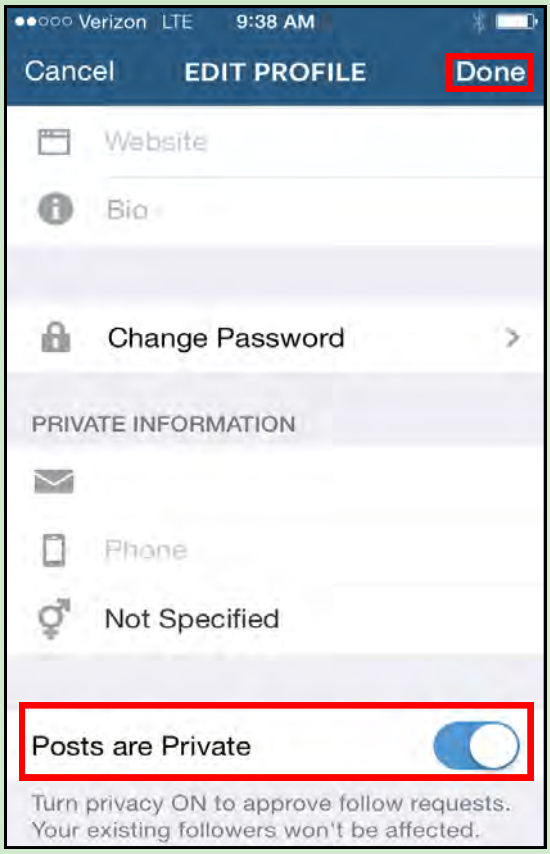
Managing Your Instagram Profile

Apply the **Profile** settings shown below to ensure that your information is visible only to the people of your choosing.

- Go to your profile by tapping 
- Tap **Edit Your Profile** next to your profile picture.



- **For iOS devices** Turn on the **Posts are Private** setting and then tap **Done**
- **For Android devices** Turn on the **Posts are Private** setting and then tap the check mark to save your changes
- **For Windows devices:** Turn on the **Posts are Private** setting by checking the box and then tap the check mark to save your changes

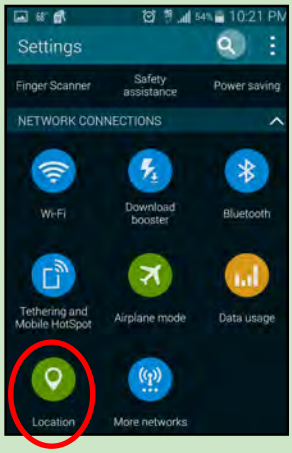


Things To Keep In Mind About Private Posts

- Private posts you share to social networks may be visible to the public depending on your privacy settings for that network. For example, a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your Twitter posts.
- Once you make your posts private, people will have to send you a follow request if they want to see your posts, your followers list or your following list.
- People can send a photo or video directly to you even if they're not following you.
- You'll see follow requests  in Activity, which you can then approve or ignore.

Instagram Smart Card

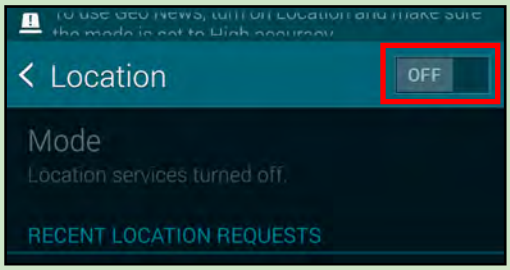
Geo-Location



Apply the device settings shown below to ensure that your location is not shared through Instagram photos.

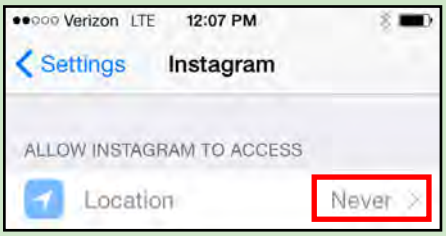
To adjust geolocation settings on Android:

- Open the **Settings** on your phone **> Location** > then slide the toggle switch to off



Location access to photos taken with Instagram can be disabled two different ways on iOS:

- Open the **Settings** on your phone and scroll down and tap on **Instagram** > **Location** and change to **Never**



- Open the **Settings** on your phone > Tap **Privacy** > **Location Services** > Tap on **Instagram** and change to **Never**

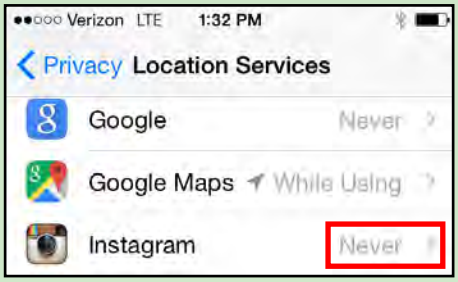


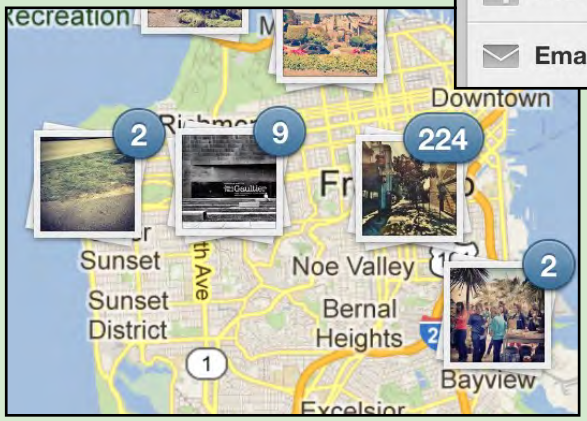
Photo Map

With Instagram Photo Map, you can showcase where you've taken your photos or explore where others have taken photos on a map. You can edit your map at any time and will always be able to opt into each and every photo you add to your map.

When you post a picture using Instagram, you will be asked to **Add to Photo Map**. Once you accept the photo map option you will also be asked to **Name This Location.**

By default, adding location or adding to your Photo Map is turned off for all photos you upload to Instagram. This means that no photos will appear on your Photo Map without your explicit permission.

Photo Map will allow your photos to be displayed on a map and can pose a threat to you and your family if not used smartly. If you chose to use Photo Map, be cautious of posting pictures of your home, work or other locations that could bring harm to your or your family if available to the public.



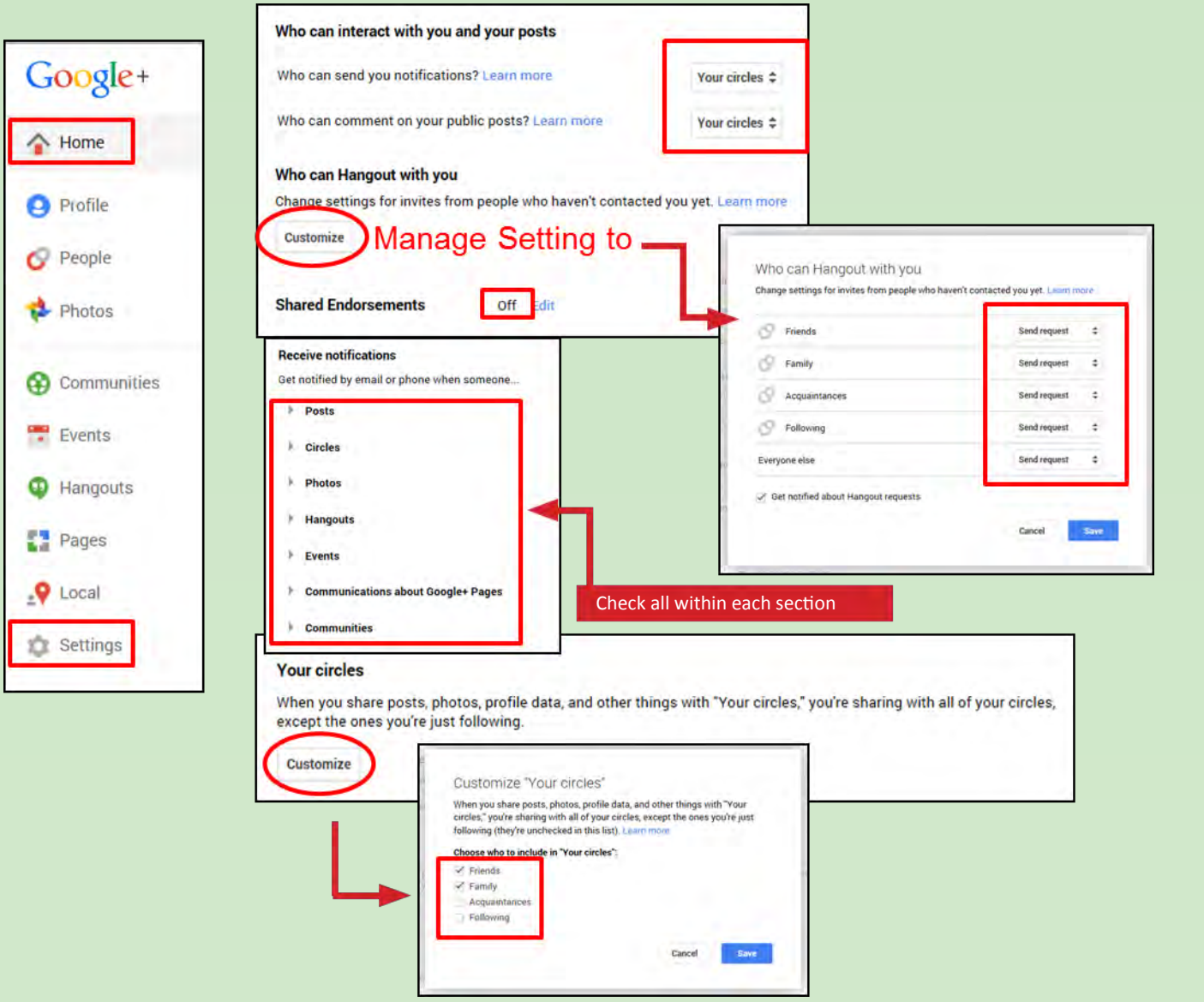
Google + Smart Card

20141023

Introduction

- Only put people in your circles that you know and trust.
- Use a separate Gmail for corresponding with trusted individuals within Google+; use another Gmail for personal business/affairs.
- Assume ALL information and images you share are viewable by the public, regardless of your settings.
- **PLEASE NOTE: Anyone can put you in their circle and you CANNOT remove yourself from their circle.**
- For maximum security, select settings "Only You" and "Your Circles" whenever given the selection. Also ensure your family takes similar precautions with their accounts. Their privacy and sharing settings could expose your personal data.
- DO NOT log in or link third party sites (e.g. Facebook, LinkedIn, Twitter) using your Google+ account. Third party sites may aggregate and misuse personal information.
- **DO NOT** add your mobile phone number and do not upload photos from your smartphone. Metadata can identify where you took the picture.
- Make your profile and cover picture a photo of something other than yourself.
- A good general rule is the less you share, the better.

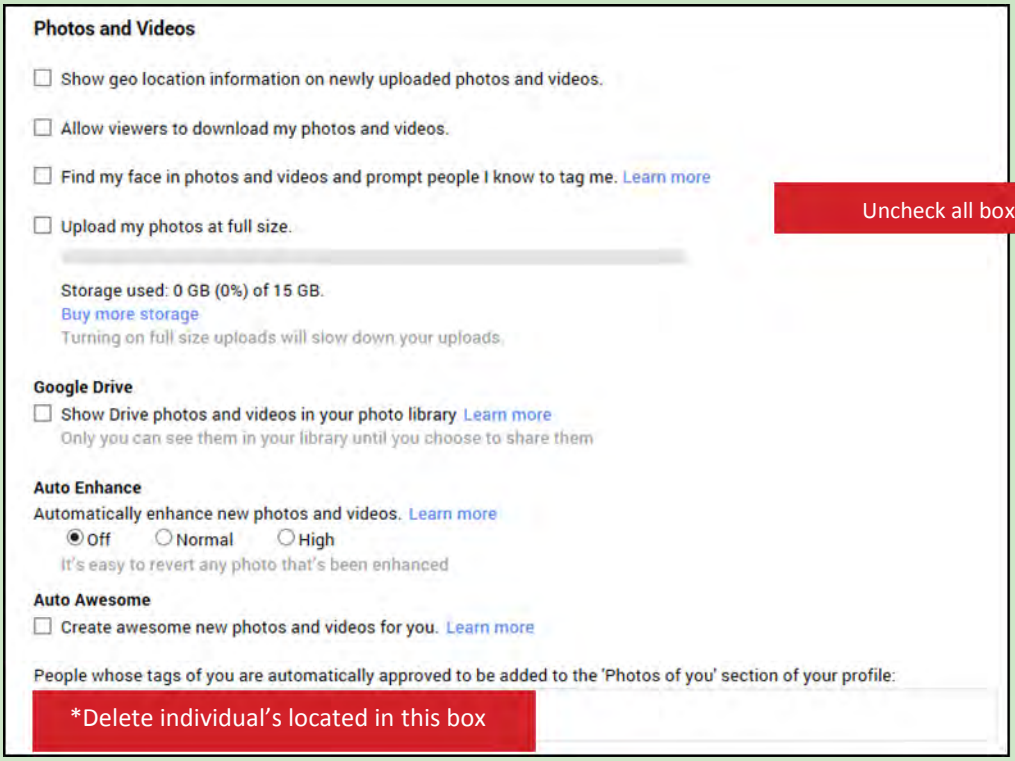
Account Settings



Google + Smart Card

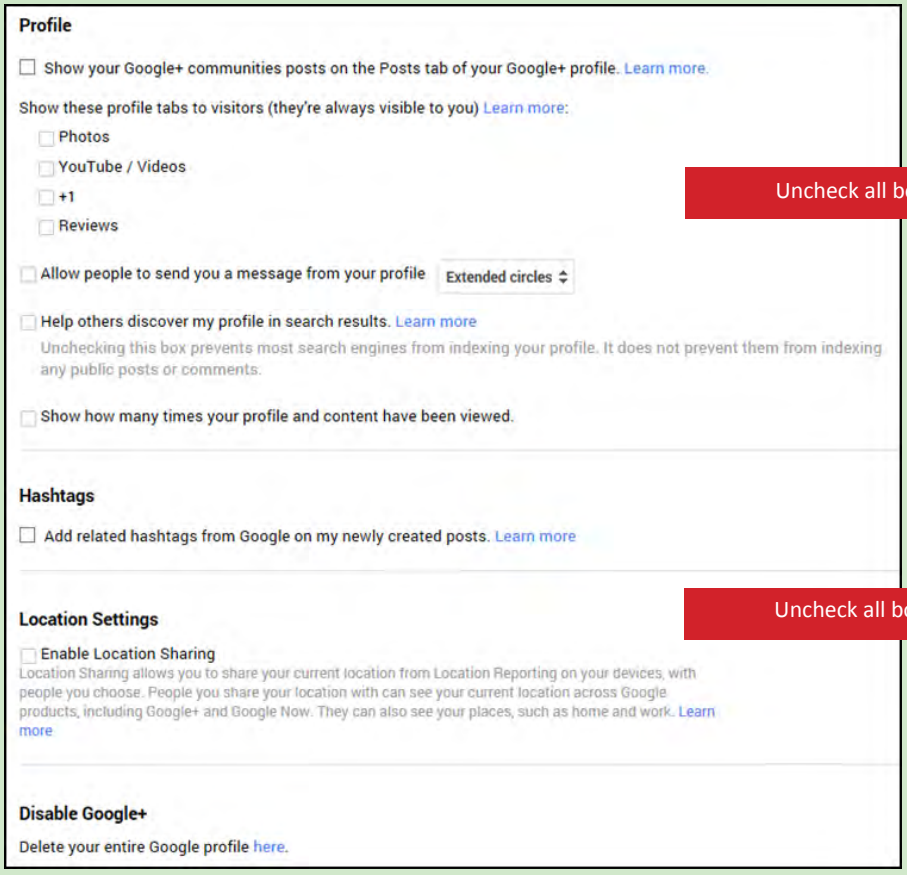
20141023

Photos and Videos



Uncheck all boxes in this section

Profile



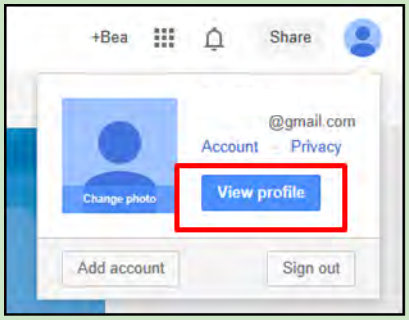
Uncheck all boxes in this section

Uncheck all boxes in this section

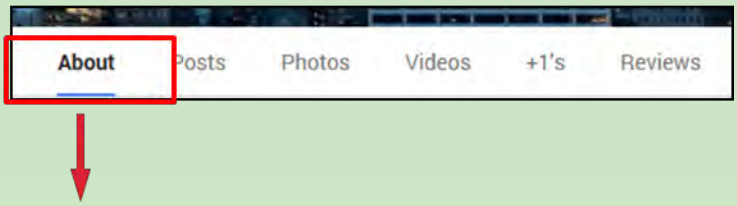
Google + Smart Card

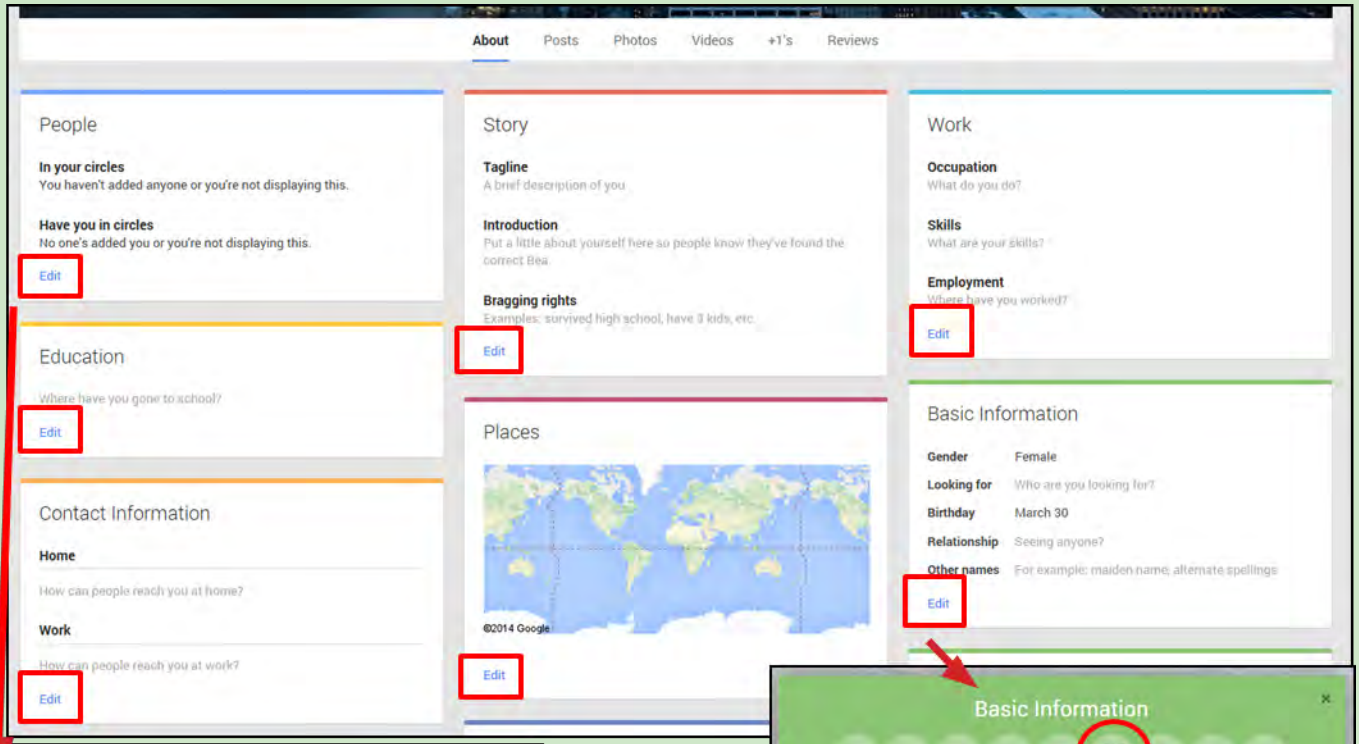
20141023

View Profile

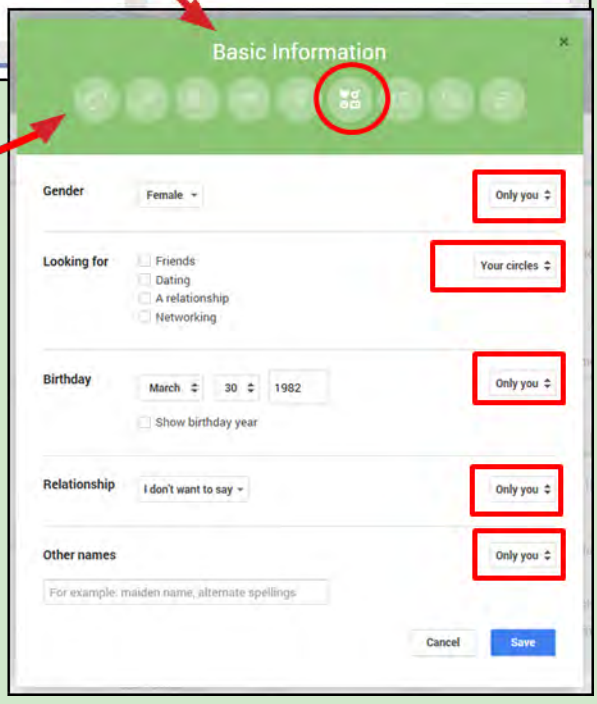


*Click on "View Profile" and then click "About" and "Edit" to change visibility of each individual box on your Google+ profile page





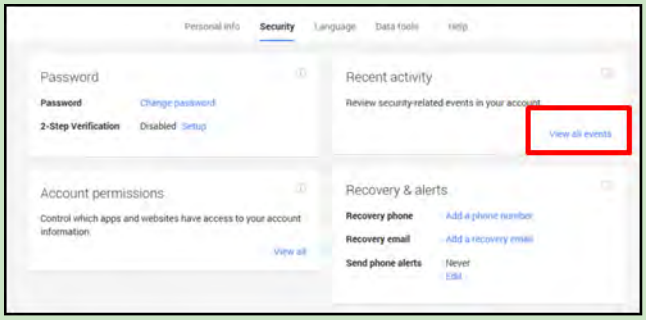
*Click on the individual circles to change the settings for each individual box

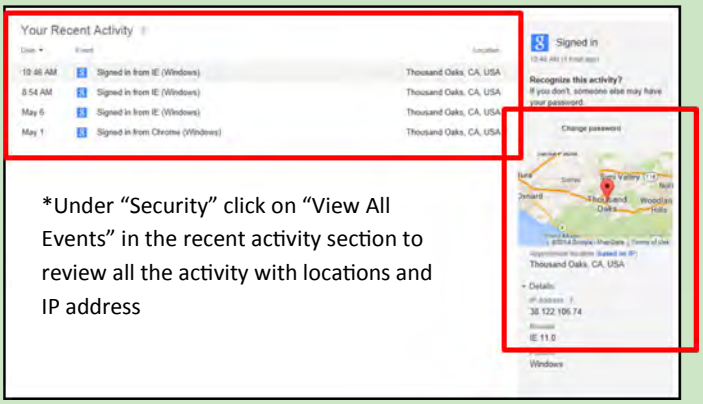


Google + Smart Card

20141023

Security

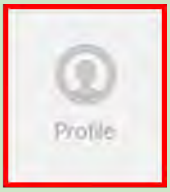


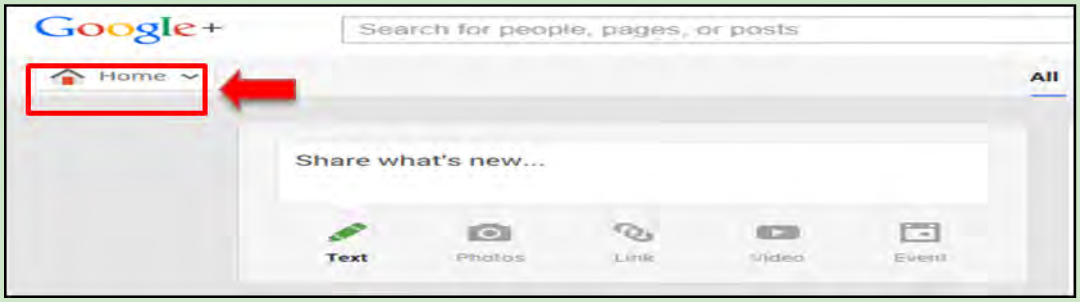


*Under “Security” click on “View All Events” in the recent activity section to review all the activity with locations and IP address

Post Deletion

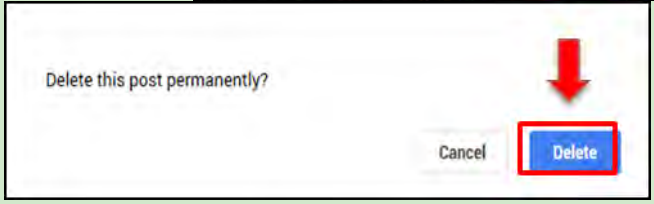
From the Google+ home page, select the “Home” tab in the upper left hand corner of the screen and select the “Profile” icon





The next screen will contain all the posts, photos, and videos you have posted to your Google+ profile.

To delete a post, click the arrow icon in the upper right hand corner of the individual post and select “Delete post”. You will then be prompted to confirm the request to delete



Opting Out of Public Records and Data Aggregators Best Practices Smart Card

20140703

Opting Out of Public Records and Data Aggregators—Best Practices

- 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 process 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.

What to Look For

Search for your name, names of family members, email addresses, phone numbers, home addresses, and social media usernames using Google. Once you have located information that you want removed, you should record your findings to facilitate the removal process. Please note, the information presented here about how to remove personal details from data aggregators is subject to change.

PrivateEye—Veromi—PeopleFinders—PublicRecordsNow

PrivateEye, Veromi, PeopleFinders, and PublicRecordsNow are all owned by the same parent company, Confi-Chek.com. You must opt out of each individually.

- Opt out of PrivateEye by completing the form at: **https://secure.privateeye.com/optout-form.pdf**
- Opt out of PeopleFinders and Public Records Now by visiting: **peoplefinders.com/manage/**
- Opt out of USA People Search by visiting: **usa-people-search.com/manage**
- Opt out of Veromi by visiting: **veromi.com/Help#26**

PrivateEye

Veromi

peoplefinders find anyone, anywhere

PublicRecordsNOW

MyLife

Call MyLife at (888) 704-1900 and press 2 to speak to an operator. Have the following inf ormation ready: name, age, date of birth, email, current address, and one previous address. Tell the representative that you want your listing removed and provide the information you want deleted. Be sure to specifically request your information is removed from Wink.com as well as MyLife.com. Once they confirm the removal, the listing will be off the site in 7-10 days.

mylife

http://www.mylife.com

US Search

Opt out of US Search by visiting http://www.ussearch.com/privacylock. Search for your name and click on the appropriate listing. Print the cover sheet and mail or fax a state issued ID or drivers license to the listed address or fax number.

http://www.ussearch.com

US SEARCH for PEOPLEDATA®

Intelius—Public Records—ZabaSearch—Spock—iSearch—PeopleLookUp—PhonesBook—DateCheck—LookUp—PeopleFinder—LookUpAnyone

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

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

INTELIUS Live in the know.™

PublicRecords.com If it's out there, it's in here

http://www.zabasearch.com
http://www.peoplelookup.com
http://www.lookupanyone.com
http://www.intelius.com
http://www.publicrecords.com
http://www.phonesbook.com
http://www.peoplesmart.com

Opting Out of Public Records and Data Aggregators Best Practices Smart Card

20140703

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.

http://www.beenverified.com/

Spokeo

To opt out of Spokeo, first find your listing. Now visit Spokeo's opt out page at http://spokeo.com/optout. Enter the URL of your listing and your email address. Go to your email and click on the removal confirmation link.

http://www.spokeo.com

US Identify

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.

http://www.usidentify.com/

PeekYou

To opt out of PeekYou, fill out the form at:
http://www.peekyou.com/about/contact/optout/index.php
select **Remove my entire listing** under **Actions**. 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 that it has been deleted.

http://www.peekyou.com

Whitepages

To opt out of Whitepages, search for your information using your first name, last name, city, and state. Before deleting these records you must first register with the service. To do this, click the listing containing your information, then click the "Claim and Edit" and login buttons. Once an account is created, sensitize the information using the **Edit** buttons . Additionally, check the box under "Hide" and hit the update button to finalize changes. Delete all information whenever possible.

http://www.whitepages.com

InstantCheckMate

To opt out of InstantCheckMate, follow the instructions at:
http://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.

http://www.instantcheckmate.com/

Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	https://www.privacyrights.org/privacy-basics
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/social-networking.aspx
Online Guardian	www.onguardonline.gov/topics/social-networking-sites.aspx

Opting Out of Search Engines & Other Databases Smart Card

Intelius

http://www.intelius.com

How do I remove my information from your database/reports?

The quickest and simplest way to have your information removed from our database and reports (also known as "opting out") is to send us a request via the Intelius Opt-Out online form (https://www.intelius.com/optout.php). Be sure to include your email address so that we can notify you both when your request is received and when we've completed your opt out.

You can also send us a request via fax or postal mail. In order to accurately identify your records, we need your request to include:

- Name
- Date of birth
- Address
- Proof of identity, consisting of either:
- Copy of a government-issued ID with any photo or ID number crossed out. Examples: driver's license, U.S. passport, U.S. military ID card, state-issued ID card, or employee ID card from a state agency.
- Notarized Identity Verification Form

Here is contact information for submitting your request:

Fax: (425) 974-6194

Mail: P.O. Box 4145, Bellevue, WA 98009-4145

Your information will be removed from our database within 7-14 days. For more details on how we protect your privacy, view our Privacy Policy.

People Look Up

http://www.peoplelookup.com/privacy

How to Remove your Information from the PeopleLookup.com Public Records Databases

Public records are available from the official public records custodian or repository to anyone who requests them. In order for any database of public records to be useful, the databases must contain all of the information in the public records offices. If you have a compelling privacy or security issue, you may wish to contact the official custodians of those public records that contain sensitive information about you, such as your county's land records office, to determine how to remove your information from the public record. (The process of having public records sealed typically requires a court order.) This process will ensure that the information is not available to the public, to us, or to any other public records information provider.

In addition to public records, personal information may be publicly or commercially available. Publicly available information consists of online and offline information that is generally available but is not maintained by a government agency, such as names, addresses and telephone numbers of individuals and businesses, professional licensing and trade organization information, press releases and newspaper articles and content from blogs or social networking sites. Commercial records consist of information that is maintained by enterprises and is available for purchase, such as marketing and telemarketing lists, phone connect and disconnect information, and business profile data.

As a courtesy we allow you to opt out your personal information from our Website. What this means is that your name as it appears in a particular record and the associated identifying information such as your address and phone number will be suppressed if you request this in the manner described below. However, please note that any time your identifying information appears in a public record or in a publicly or commercially available manner, in a way that is different from the particular record you opted out, it will again appear on our Website. For example, if your address or area code changes, your new information -- including other associated identifying information -- will again appear unless you opt out the new record. Similarly, if the way in which your name or address appears in a record differs from a record you opted out (e.g., "Michael" instead of "Mike," or "1212 Second AVE NE" instead of "1212-2nd Avenue Northeast"), we may include the differing record. Please also note that there may be more than one record on our Website associated with your personal information. Opting out one particular record will not opt out other record(s). Your opt out will apply from processing date forward; any report purchased prior to your opt out will still be available to the purchaser thereof in accordance with the terms of our service. In addition to this Website, there are many other companies offering public records search services, and your request that we opt out your information from this Website will not prevent your information from appearing on these other services.

Opting Out of Search Engines & Other Databases Smart Card

People Look Up (Cont)

In order for us to suppress or opt out your personal information from appearing on our Website, we need to verify your identity. To do this, we require faxed proof of identity. Proof of identity can be a state issued ID card or driver's license. If you are uploading, faxing, or mailing a copy of your driver's license, we require that you cross out the photo and the driver's license number. We only need to see the name, address and date of birth. We will only use this information to process your opt out request.

Submit your opt out request via fax to 425-974-6194 or via mail to: PeopleLookup.com Consumer Affairs PO Box 808 Bothell, WA 98041-0808. Allow 7-14 days to process your request. We will only process opt out requests received by fax, or mail and no request will be processed without complete information (i.e., name, address and date of birth). Requests for opt out will not be processed over the phone or via email.

US Search

http://ussearch.com/consumer/commerce/about/privacy.jsp

How to Block Display of your Profile on US Search Websites and in US Search Reports:

US Search obtains most of the information for our products and services from partners who generally obtain it from public records. We do not maintain or control those records, and cannot remove your name from any public records.

As a courtesy we offer individuals the ability to block certain records from appearing on the US Search websites, in US Search Reports, and in advertisements "powered by US Search" on third party website. The US Search Privacy Lock suppresses your name only as it appears in the particular record you block, and only suppresses information (e.g., address and phone number) that is associated with the record you block. If your identifying information appears in a different format in other public records, your name may still appear on our Website, in our reports, or in our advertisements. For example, if your name appears as "Mike" in some records and "Michael" in another, you will need to repeat the lock process for each record separately.

If your identifying information, such as your address or area code changes, you will need to opt out again to prevent your new information from appearing. In order for us to suppress or opt out your personal information from appearing on our Website, we need to verify your identity. To do this, we require you to send us proof of identity via postal mail or fax, which we will use only to process your opt-out request. Proof of identity can be a state issued ID card or driver's license. Please cross out everything but your name, address, and date of birth before sending us the proof of identity.

Requests for opt out will not be processed over the phone or via email. Subject to limited exceptions for elected officials and/or law enforcement officers, US Search does not process third party requests or requests submitted in any other manner.

US Search (Cont)

To learn how to block your profile from appearing on our websites, in our reports, or in our ads, please http://www.ussearch.com/consumer/ala/landing.do?did=590.

People Finder

http://www.peoplefinder.com/privacy/

How to Remove your Information from Our Database

Public records are available from the official public records custodian or repository to anyone who requests them. In order for any database of public records to be useful, the databases must contain all of the information in the public records offices. If you have a compelling privacy or security issue, you may wish to contact the official custodians of those public records that contain sensitive information about you, such as your county's land records office, to determine how to remove your information from the public record. (The process of having public records sealed typically requires a court order.) This process will ensure that the information is not available to the public, to us, or to any other public records information provider.

In addition to public records, personal information may be publicly or commercially available. Publicly available information consists of online and offline information that is generally available but is not maintained by a government agency, such as names, addresses and telephone numbers of individuals and businesses, professional licensing and trade organization information, press releases and newspaper articles and content from blogs or social networking sites. Commercial records consist of information that is maintained by enterprises and is available for purchase, such as marketing and telemarketing lists, phone connect and disconnect information, and business profile data. Submit your opt out request online http://www.peoplefinder.com/optout.php

Blackberry Privacy Settings Smart Card

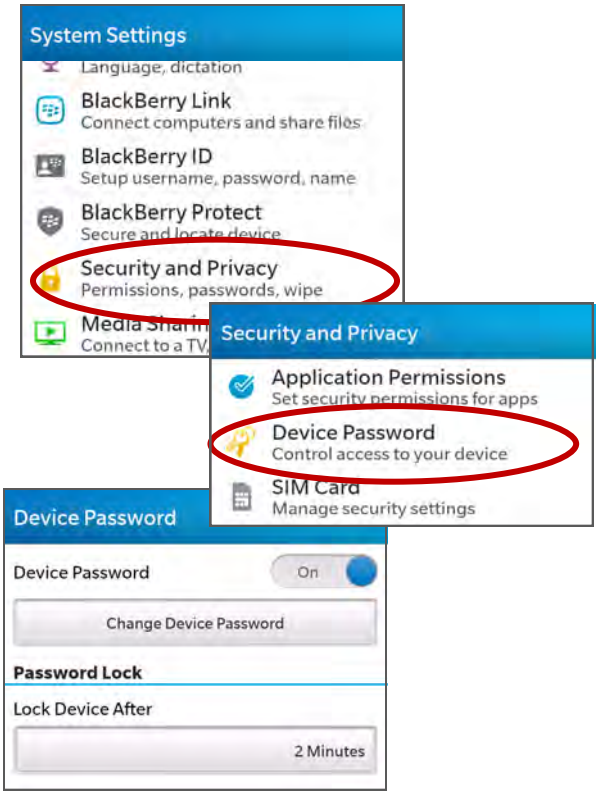
20150111

Managing your Blackberry Security Settings

There are a number of options you can set to help maximize the safety and security of your BlackBerry.

Enable Password Protection

From the Home screen, go to **Settings > Security and Privacy > Device Password.** Set Password to **On**. Enter your new password when prompted. Confirm password, and then exit to the main menu. Lock your phone by pressing and holding the power button to confirm that it has been password-protected.



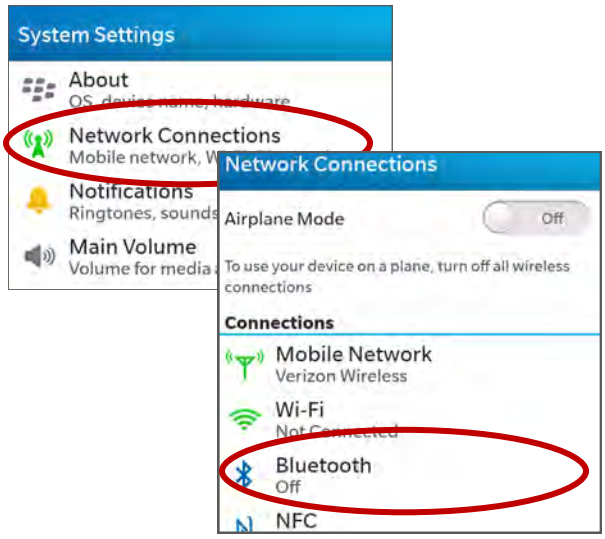
Enable Encryption

Also under **Settings > Security and Privacy > Encryption** and select **On. Scroll down and select On under Media Card Encryption. E**nter your new password when prompted.

Lock Down Bluetooth

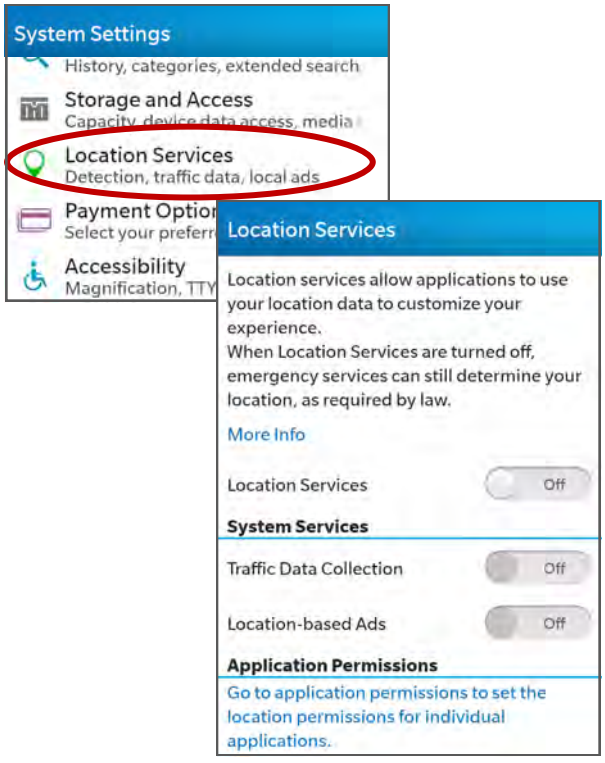
Bluetooth is set to on by default on Blackberries. In addition to wasting your battery, this leaves you open to Bluetooth-based attacks. We recommend turning Bluetooth off and enabling it on an as needed basis. To lock down Bluetooth:

Go to **Settings > Network Connections > Bluetooth** and select **Off.**



Disable Location Services

Almost all apps default to "allow" for location services, regardless of what the user selected during setup. To disable location services entirely, go to **Settings > Location Services** and select off. This will disable all Location capabilities on the phone.

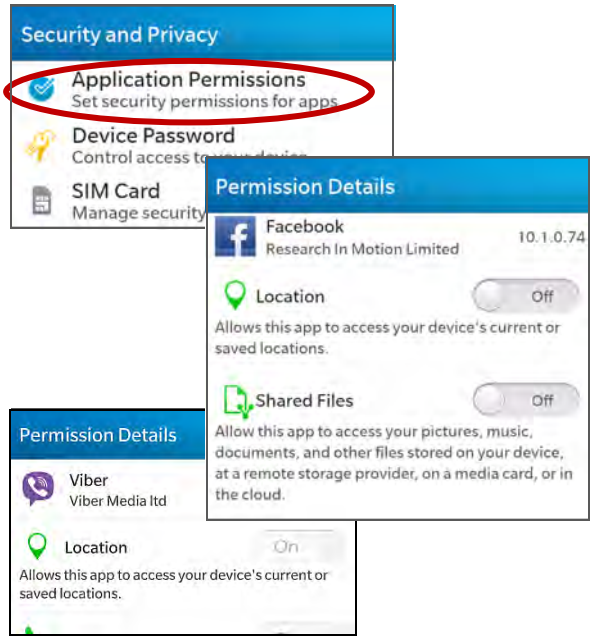


Blackberry Privacy Settings Smart Card

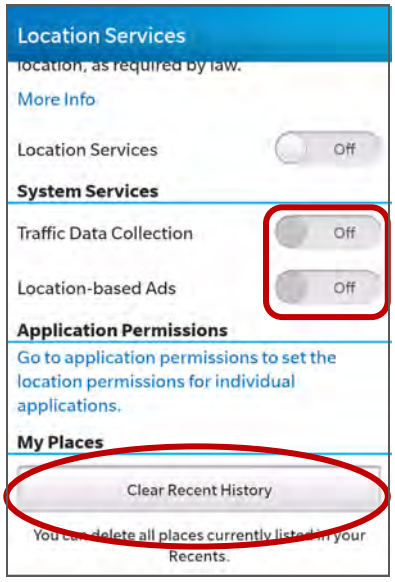
20150111

Geo-Tracking and Photo Tagging

Alternatively, you can choose which apps have location permissions. To do this, go to **Settings > Security and Privacy > Application Permissions** and select on or off for each individual application. Select on only when necessary, most commonly google maps or Uber type apps. Exit and save.



If you choose this route, we recommend leaving **Traffic Data Collection** and **Location-based Ads** on the overall Location Services set to off.



Once you've updated your location permissions, clear your recent location history (see above).

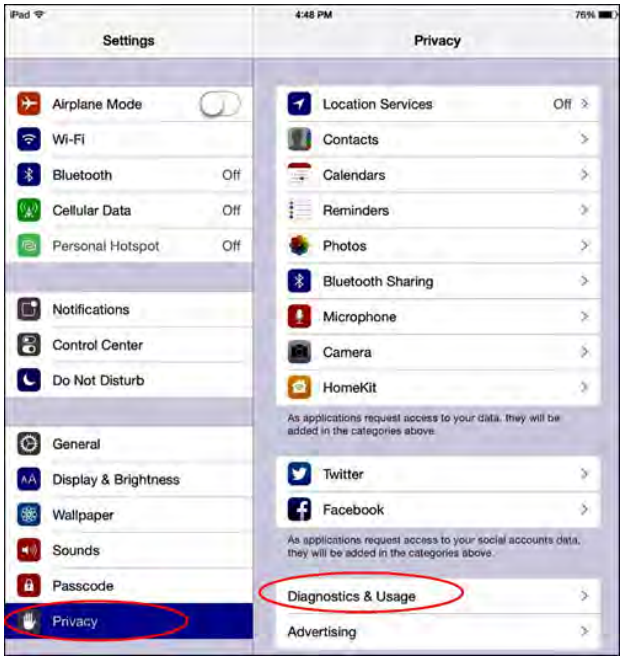
iOS8 Privacy Settings Smart Card

20141023

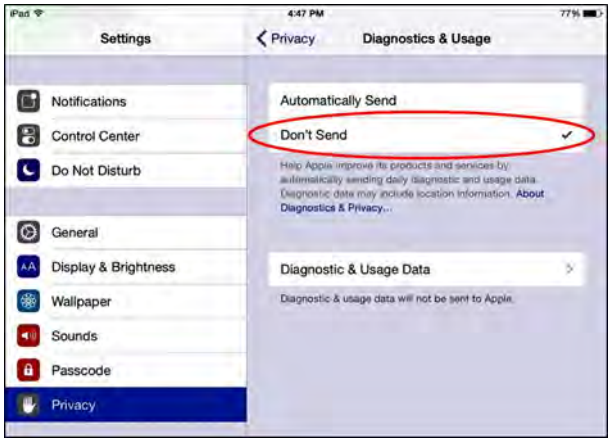
Diagnostics & Usage Data

Diagnostics and usage data enables a feature that gives Apple permission to track everything you do, to disable it in iOS 8:

Open up the Settings app and navigate to **Privacy** > **Diagnostics & Usage**.



Then tap on **Don't Send**.

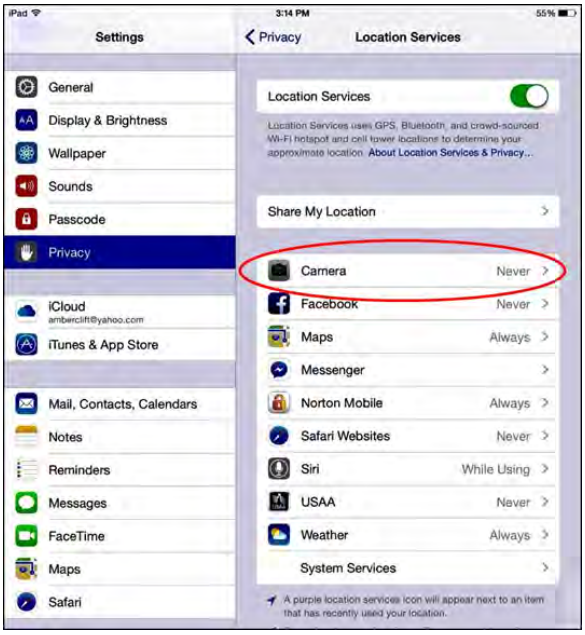


Geo-Located Photos

Whenever you take a photo, it records the location and saves that information inside of the photo's EXIF data. When you send that photo to someone else, they can see where you took it, in some cases, down to the specific street corner. If you post a picture that you took from your home, anyone that can view it can figure out where you live and more.

To disable your location from being shared in Message and Find my Friends, open the Settings app and navigate to **Privacy** > **Location Services**. Then navigate to **Share My Location** and click on the toggle to disable **Share My Location**.

Go back to **Location Services** to disable your location from being saved to photos. Click on **Camera** to change the settings.



Tap on **Never**.

Within the **Location Services** setting, decide which of your apps require location-based services and disable those that don't. Navigation and maps apps are examples of specialized apps that require location.

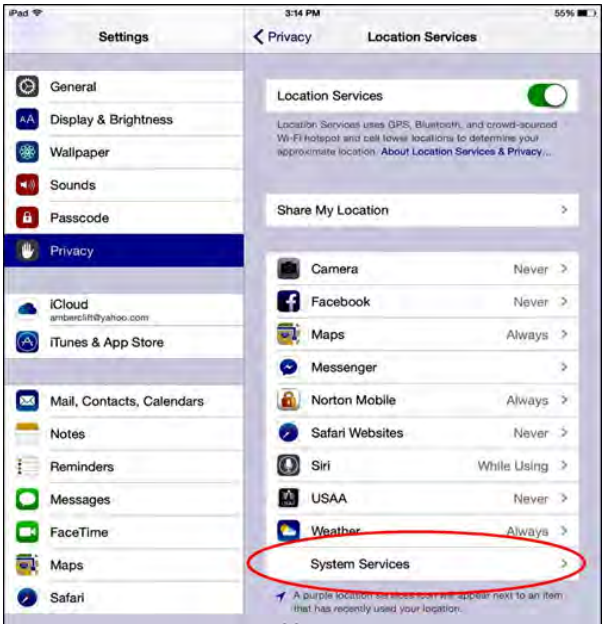
iOS8 Privacy Settings Smart Card

20141023

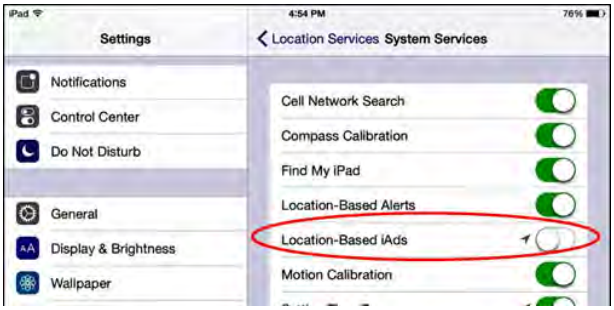
Location Based iAds

iAds has been around for a few years now, but not without its own controversy. Location-based iAds don't use your exact location and Apple doesn't give this info to advertisers. Most users prefer to disable iAds anyway. Here's how to do it:

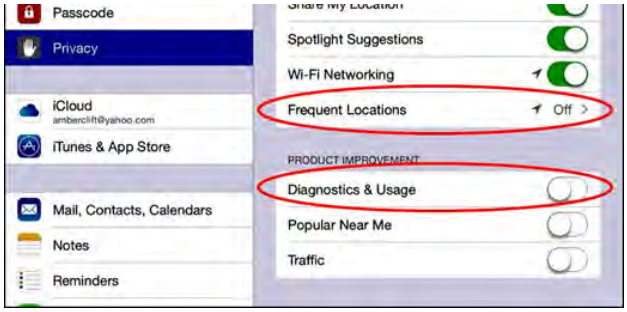
Open up the Settings app and navigate to **Privacy** > **Location Services** > **System Services**. You'll see a list of various toggles that you can turn off and on.



You'll see one that says Location-Based iAds. Go ahead and flip the toggle to the right until it's grayed out.



You should also to turn off **Diagnostics & Usage** (You'll have to do it here too), as well as tapping on **Frequent Locations** and turning that off as well.



Ad Tracking

Ads can track everything you do. Apple has a setting where you can turn this on or off. Open up the Settings app and navigate to **Privacy** > **Advertising**.

You'll want to make sure that you turn **ON Limit Ad Tracking**. In this instance "ON" is good. You'll also want to reset your advertising identifier while you're still on that page. Tap on **Reset Advertising Identifier** to start with a clean slate. Users who are concerned about having their usage habits tracked by advertisers can tap this button, which essentially makes them appear as a new user.

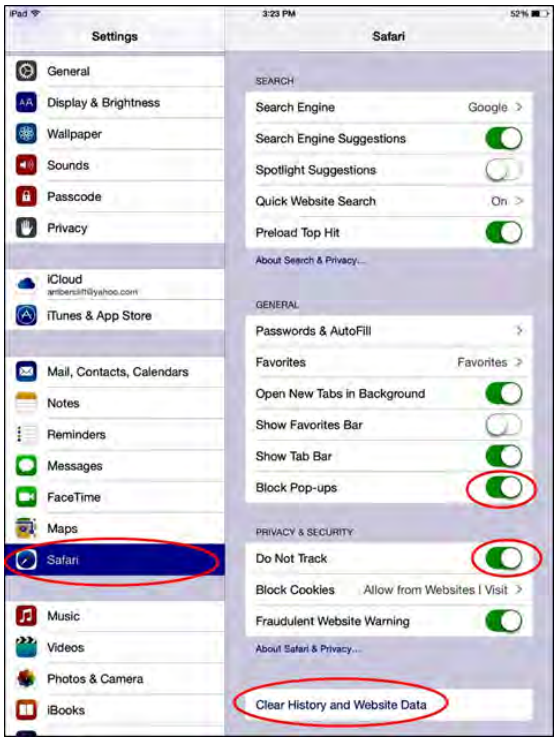
Safari's Do Not Track

Safari's Do Not Track is a universal web tracking opt-out initiative that allows users to prevent advertisers from tracking your browsing habits. The Safari mobile browser on iOS 8 allows you to opt-out to prevent your mobile web browsing history from being looked at by advertising eyes.

To opt-out, open the Settings app, scroll down and tap on **Safari**. Under the section titled **Privacy & Security**, turn on **Do Not Track**. It's also a good idea to enable **Block Pop-ups**. You can clear browser history here as well. It is a good idea to do this periodically.

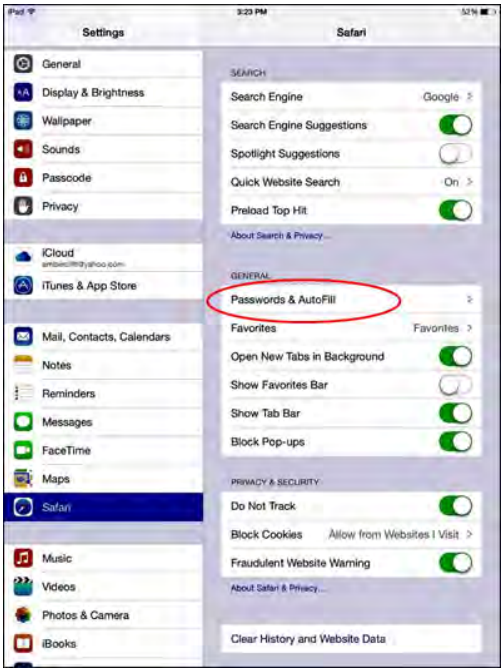
iOS8 Privacy Settings Smart Card

201410243



Passwords and AutoFill

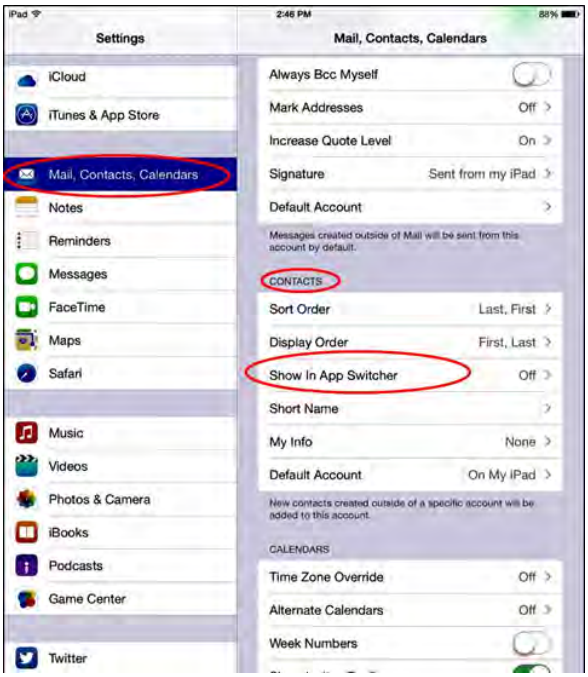
Lastly you will want to clear the auto fill to protect your passwords and credit card information. Open the Settings app, scroll down and tap on **Safari**. Under the section titled **General**, click on **Passwords & AutoFill**.



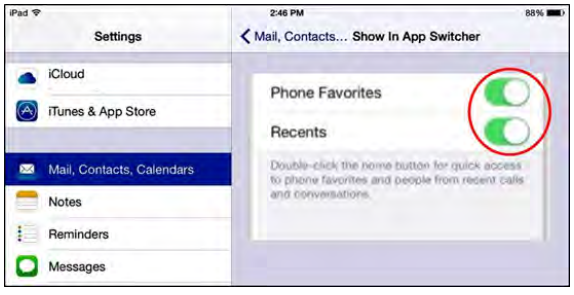
Then click on the toggle to disable **Use Contact Info, Names and Passwords** and **Credit Cards**. Be sure to check and delete any information you don't want saved by clicking on each option.

Prior to iOS 8, when you double-clicked your home button you would only see an array of app thumbnails, allowing you to quickly switch between apps. With iOS 8, avatars of your recent and favorite contacts will now show up as well.

To disable your contacts from displaying in the app switcher, launch the **Settings app.** Select "**Mail**, **Contacts**, **Calendar"** form the list of options.



Click the toggles to switch off **Phone Favorites** and **Recents** to disable avatars of your recent and favorite contacts from automatically displaying in the app switcher.



Smartphone Smart Card

201410243

Do's and Don'ts

- Smartphones are not impenetrable. Secure your smartphone with a password, and utilize apps such as *Find My iPhone* and *AndroidLost* to locate lost or stolen devices.
- All smartphones have cameras and microphones that can be remotely activated. Caution should be used when smartphone is near sensitive information.
- Bluetooth and wireless capable smartphones are convenient but easily exploitable by hackers. Use a VPN if possible and avoid public wireless networks, especially when accessing sensitive information.
- Prior to downloading apps on your smartphone, read the developers permissions. Many apps now require permission to access your camera, microphone, text messages, and phone contacts.
- Keep your locations services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked.
- If you have a google account, you can use your google credentials to login at maps.google.com/locationhistory to see your phones location history for the last year or more.

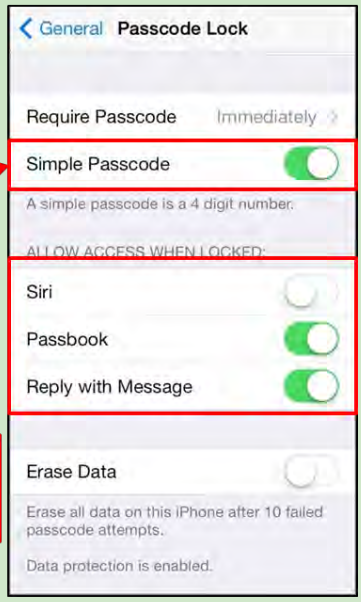
Physical Exploitation

The first line of defense in preventing unauthorized access to your data is to protect your smartphone with a passcode. Each operating system has different methods of security, both achieving the same goal. Always set your smartphone to require a passcode immediately and use an alpha-numeric passcode.

Android 4.4.4

Face Unlock is not secure; a picture of you will allow access to your phone.

iPhone 8.0.2



DISABLE Simple Passcode and secure device with a longer alpha-numeric passcode.

Turn these settings OFF; they allow anyone to access areas of your phone without a passcode.

Lost/Stolen Phone

In the U.S., it has been reported that over 100 cell phones are stolen or lost every minute. This fact alone proves it is necessary to keep your device secure and locked with a passcode. There are apps available for both Android and iPhone platforms that allow the user to manage their smartphones remotely in the event their phone is stolen or lost.

Android 4.4.4

Androidlost

- Wipe phone
- Lock phone
- Erase SD Card
- Locate by GPS or Network
- Email when SIM is charged
- Take picture
- Record sound from microphone
- Google.com/device

iPhone 8.0.2

Find My iPhone

- Wipe phone
- Lock phone
- Activate alarm
- Activate camera
- Locate by GPS or Network
- Backup data through iCloud

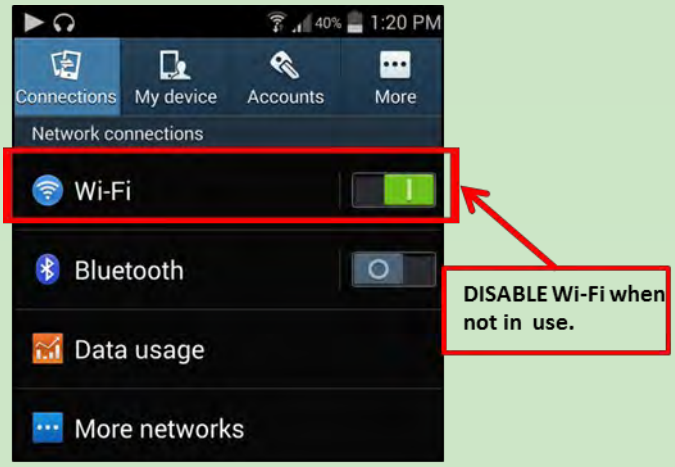
Smartphone Smart Card

201410243

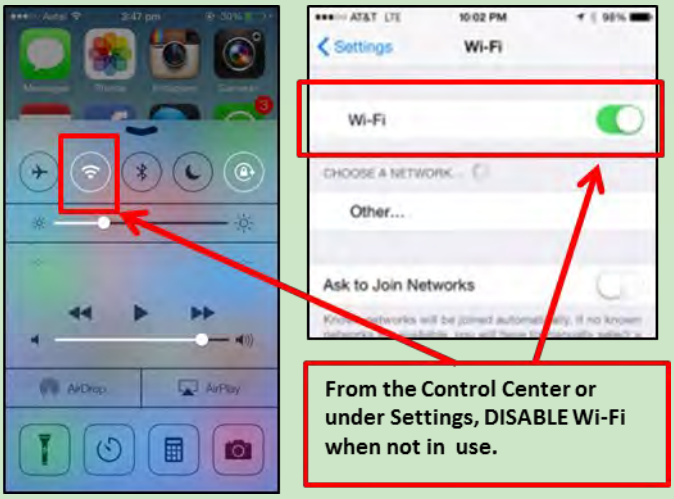
Wireless Networks

If possible, public Wi-Fi networks should be avoided due to the risk of interception by third parties. If public networks must be used, avoid logging into accounts that require passwords, as log-in credentials are easily exploited by hackers. Always use a VPN client to encrypt on-line transactions.

Android 4.4.4



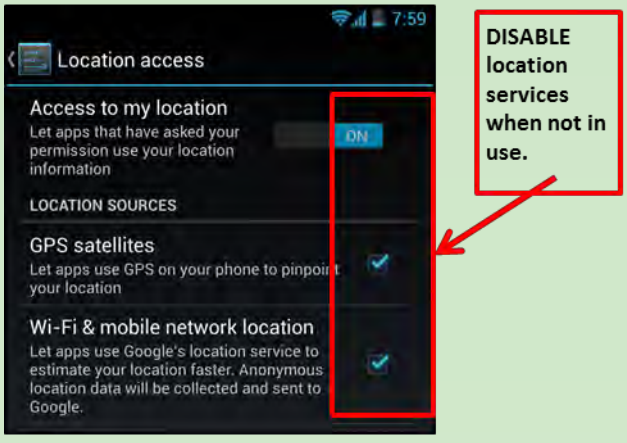
iPhone 8.0.2



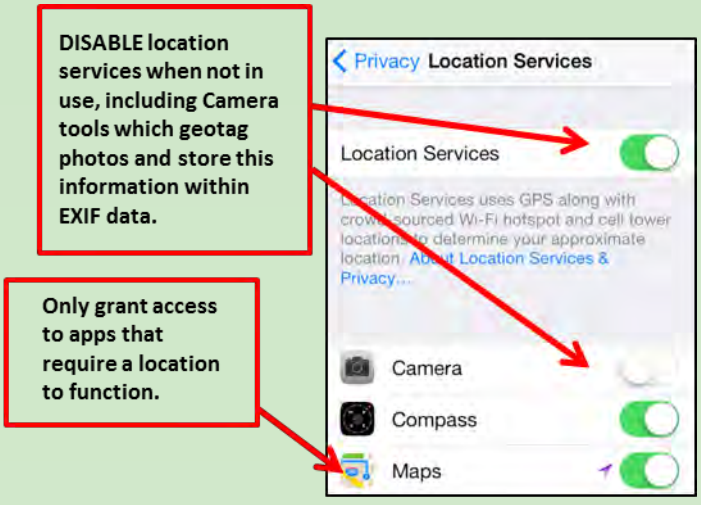
Location Tracking

Many applications will ask permission to use your current location. Users should avoid granting access when possible. Turn off all location services when they are not in use.

Android 4.4.4



iPhone 8.0.2



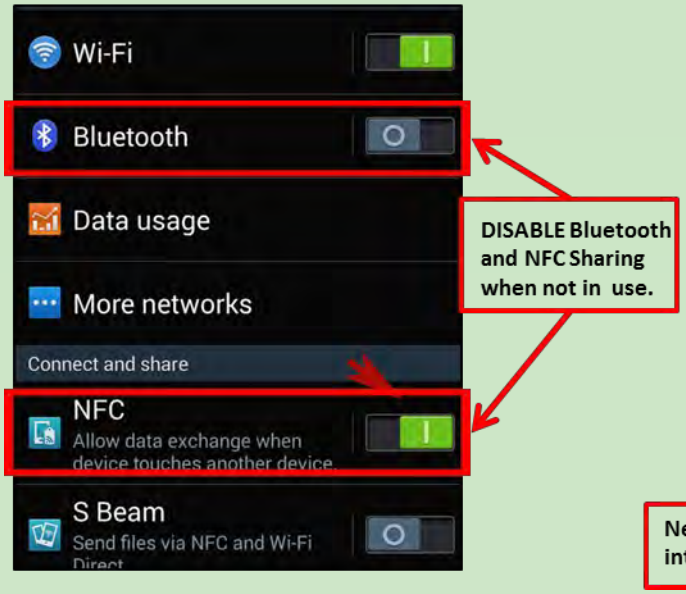
Smartphone Smart Card

201410243

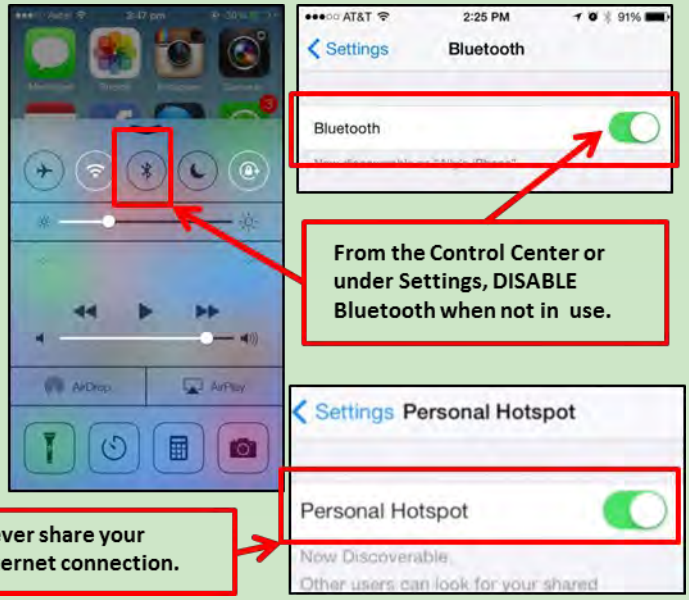
Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your smartphone, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes without you even knowing.

Android 4.4.4



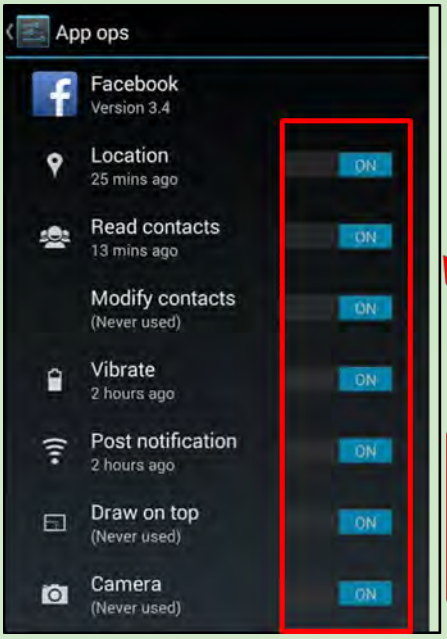
iPhone 8.0.2



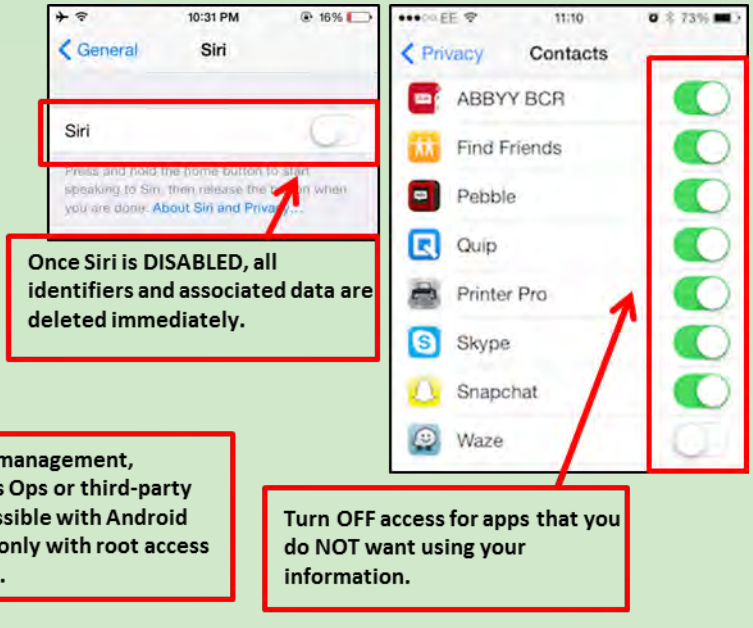
Data Retaining Applications

Downloaded applications often collect users' personal information (e.g. name, email addresses, contacts lists, credit card numbers, device information, etc.) and allow third parties to access this private and sensitive data. Even personal assistant applications, like Siri and Google Now, collect and retain user data. Siri voice clips are transferred to Apple's data farm and kept for up to two years. Google Now collects data from web searches, calendar appointments, photos, contacts, text messages, shopping habits, and book/movie/music choices. Review and manage applications to see what information is being collected and what permissions you have allowed.

Android 4.4.4



iPhone 8.0.2



Smartphone Exif Removal Smart Card

20140703_1200

Exif Removal - Do's and Don'ts

- Prevent your phone from including geolocation data when capturing images.
- Remove Exif data before sharing or posting images, especially images captured in private homes or businesses.
- Whenever possible, use an Exif viewer to verify Exif data has been removed.
- 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. Instagram, Flickr).
- Even with no Exif data, the content of images may contain identifying information, including 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.

Tag Category	Important Tags	Identity Implications
Geolocation	GPSLongitude, GPSLongitudeRef, GPSLatitude, GPSLatitudeRef, GPSDateStamp, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod	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.
Timestamps	ModifyDate, DateTimeOriginal, CreateDate	Creates a log of behavioral patterns and personal timelines.
Camera	Make, Model, Serial Number	A unique serial number identifies the particular device for an image or sets of images.
Authorship	Artist, Owner Name, Copyright	Links images with a name or organization.
Image Summary	ImageDescription, UniqueImageID, UserComment	Potentially reveals identifying information about the content of the images, such as captured persons or locations.

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 identifying Exif data in image files and 2) Removing existing Exif data from image files using an Exif removal application.

Prevent the Capture of Geolocation Data

iOS

If iOS location services are turned off, images captured with the native iPhone camera app will not contain geolocation Exif data.

1. Select the *Settings* app and navigate *Privacy >Location Services*.
2. Turn off location services altogether or for the iPhone's camera applications.
3. Return to the *Settings* app and navigate *Privacy >Photos*.
4. Disable the permissions for other apps to have access to the photos stored in the device's camera roll.

Android

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 the 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.

Prevent the Capture of Geolocation Data

- Taking a screenshot of a photo on a device running iOS 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 or google how to take a screenshot on your specific android.
- Photos taken in airplane mode contain geolocation data. Novetta recommends turning off location services/storage for your smartphone's camera application, as shown above.
- Remember that uploading or sharing a lower quality image will still contain Exif data. Exif data and image quality have no correlation.

Smartphone EXIF Removal Smart Card

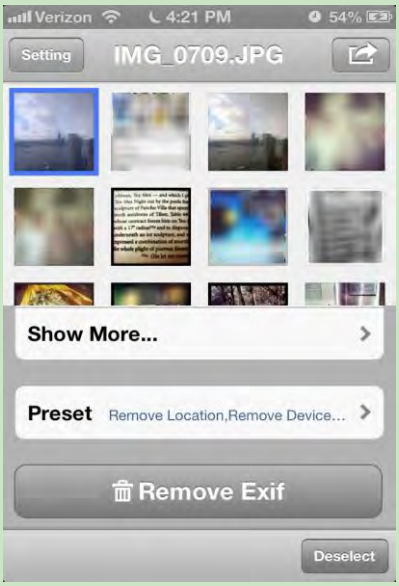
20140703_1200

Exif Removal Smartphone Apps

TrashExif for iOS

TrashExif is a free app that deletes geolocation and Camera 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 a photo(s) to clear of Exif data.
3. Select *Presets*, then in the *Removal Presets* [sic] 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 with No Exif is displayed as most recent in your iPhone Photo app.



PhotoInfo Eraser for Android

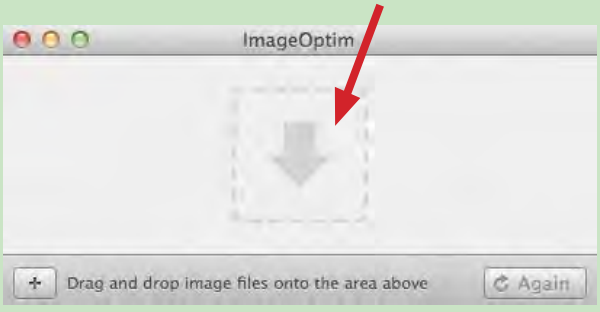
PhotoInfo Eraser is a free app that deletes all Exif data from image files stored on your Android device.

1. Download the PhotoInfo Eraser 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. Navigate *Gallery*. A copy of your photo with no EXIF is now available in the *PIEraser* folder.

Viewing and Removing EXIF Data in OS X

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

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.

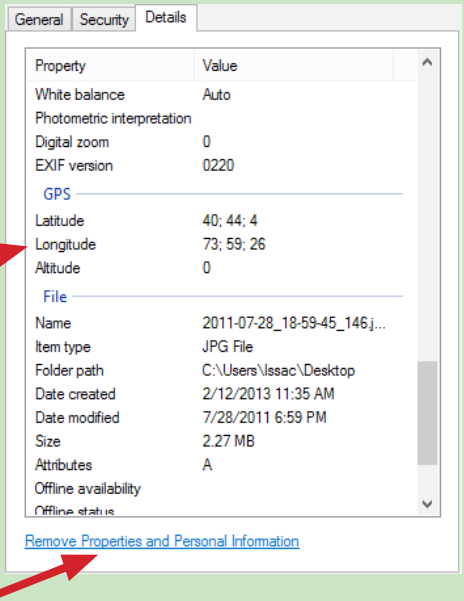


3. Check that the Exif data has been removed by right-clicking the image and select Get Info. Exif data is listed under More Info.

Viewing and Removing EXIF Data in Windows 8

Use the Windows 8 OS to verify EXIF data has been 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, is contained in the Details tab if it is included with the image.
4. Windows 8 also allows system administrators to remove all Exif data from the selected image file by clicking the *Remove Properties and Personal Information* link.



Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	www.privacyrights.org/fs/fs18-cyb.htm
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/social-network
Online Guardian	www.onguardonline.gov/topics/social-networking-sites.aspx

Traveling Safely With Smartphones

20141031

Traveling with Smartphones - Do's and Don'ts

- Consider pay-as-you go phone or replacing SIM card
- Disable GPS or location services services for most apps
- Assume that all information on your device could be compromised while traveling in a foreign country
- Do not allow apps to access Social Media
- Never store passwords or sensitive information on your smartphone
- Do not allow auto connect to WiFi
- Consider sanitizing emails prior to travel
- Examine all mobile devices for evidence of tampering upon your return
- Ensure you use complex passwords

To Do When Traveling

Ensure that your phone's software is up to date

- Use apps to ensure that the software on your smartphone is up to date.

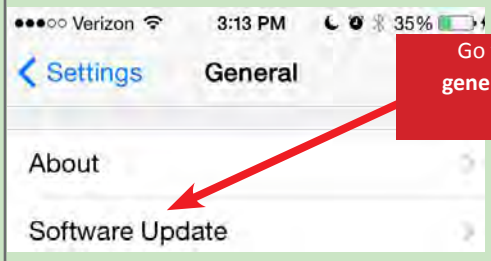
Protect your phone against Malware

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

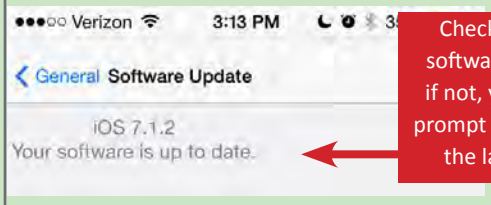
Set your phone to lock automatically

- In case you lose your device, you want your smartphone to lock automatically to prevent physical access.

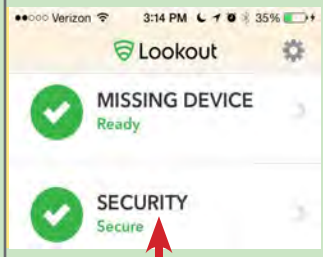
iPhone



Go to **Settings** > **general** > **Software Update**

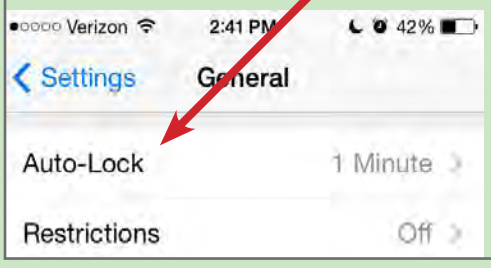


Check to see if your software is up to date; if not, your iPhone will prompt you to download the latest software



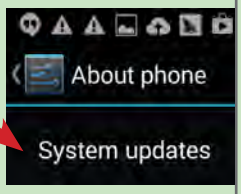
Use the Lookout app for iPhone Go to Security > Process Monitor to see if malicious processes are running on your iphone

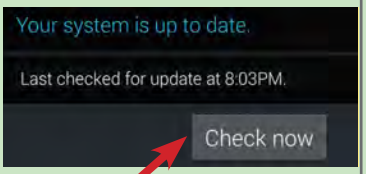
Go to settings > General > Auto-Lock
Set the Auto-Lock to 1 Minute



Android

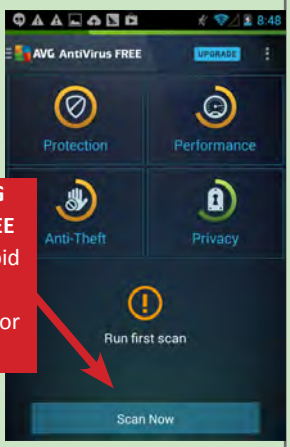
Go to **Settings** > **About Phone** > **System Updates**



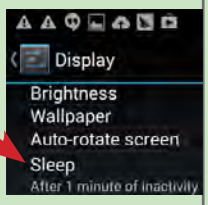


Check to see if your software is up to date; if not, your phone will prompt you to download the latest software

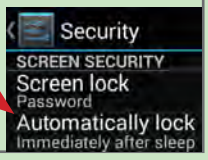
Use the **AVG Antivirus FREE** app for Android Click Scan Now to scan for viruses



Go to **Settings** > **Display > Sleep** Set the phone to sleep **after 1 minute**



Go to **Settings** > **Security** > Automatically Lock immediately



Traveling Safely With Smartphones

Traveling with Smartphones - Best Practices

- Assume that your phone may be scanned forensically when you enter a foreign country
- If possible, encrypt the data on your phone
- Consider installing a VPN on your device as more secure alternative to saving information locally

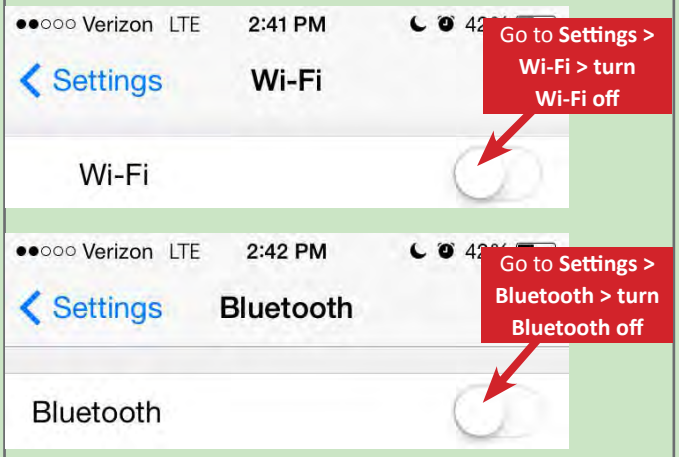
To Do When Traveling

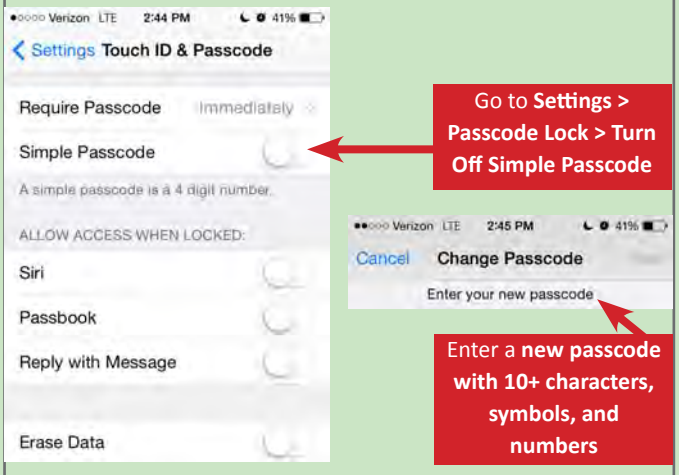
Disable Wi-Fi and Bluetooth
- Disable Wi-Fi and Bluetooth on your smartphone; Wi-Fi and Bluetooth can render your smartphone vulnerable to malware and hacking.

Use a 10+ character password or Screen Lock Pattern
- Short passwords are vulnerable to brute force attacks. Chose a password with a combination of letters, numbers, and symbols. If using a Screen Lock Pattern, choose a complicated pattern.

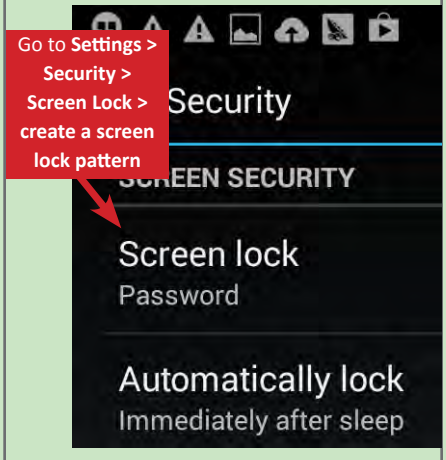
Recover lost or stolen smart-phones and wipe data
- Find my iPhone and Cerebus can locate lost devices and wipe data remotely from lost or stolen smartphones.

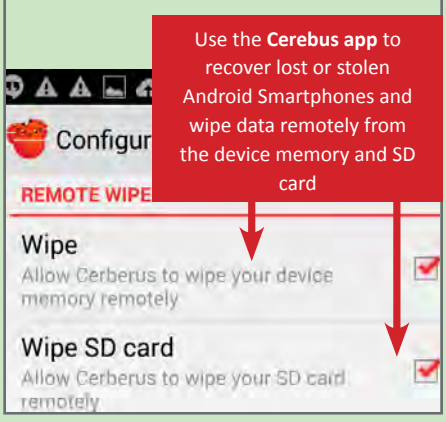
iPhone





Android





Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	www.privacyrights.org/fs/fs18-cyb.htm
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/social-network
Online Guardian	www.onguardonline.gov/topics/social-networking-sites.aspx

Photo Sharing Services Smartcard

20140614

Photo Sharing - 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.
- Ensure that your family takes similar precautions with their photos; their privacy and sharing settings can expose your images.
- Avoid posting or tagging images that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed.
- Do not use your face as a profile photo, and do NOT enable Location Services for your smart phone camera or photo sharing app.

Choosing the Right Photo Sharing Service

Choosing the right photo sharing service for your needs depends both on your intent and your audience. Key questions to ask are:

- Are you sharing photos primarily for yourself, your friends and family, or for public consumption?
- Are your contacts or viewers already using a specific service?
- How much control do you need to maintain over your images? Is the retention of Exif data problematic?

Your choice of photo sharing service determines the amount of control you retain over your images. All services allow you to remove images, but not all services allow for account deletion. Additionally, deleting your content or your account does not ensure removal from the internet.
Nine popular photo sharing services are described below. Default settings are in bold.

Service	Primary Use	Image Privacy Options	Keeps Exif?	Location Adding Options (non-Exif)	Allows Reposting?	Google Indexed?
flickr	Share photos within grouped user environments	Private, Contacts, Family, Friends, **Public**	**Yes,** No	Editable location, map based	**Yes**, No	If Public (can opt-out)
	Social Network	Only Me, Friends, Friends of Friends, **Public**	No	Free-form text, linked to Facebook page, map based	Yes	If Public
Instagram	Share photos from camera enabled mobile devices	Requests to follow must be approved, **Public**	No	GPS-based device location; Customizable location, text search	No	If third-party apps enabled
photobucket	Share photos publicly or privately	**Public**, Private (optional password protection)	**Yes,** No	None	Yes	If Public
	Social Network	Only You, **Circles**, Public	Yes	Editable location, map based	Yes	If Public
	RSS Feed	Requests to follow must be approved, **Public**	No	Non-editable GPS location for mobile; Text selection for website (city, state)	Yes	If Public
yfrog	Enhanced photo sharing in Twitter	**None**, based on Twitter	No	None	Yes	If Public
Pinterest	Share concepts and ideas using images	**Public**	Yes	None	Yes	Yes

Flickr - Allows detailed control over phone sharing

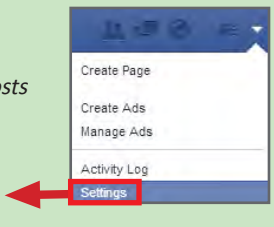
In upper right, go to *Camera* > *Settings* > *Privacy & Permissions*. Set as follows:

- Who can access your original image files? *Your friends and family or Only you*
- Allow others to share your stuff? *No*
- Who can add you to a photo? *Only You, edit* > *Remove me from all photos*
- Who can print your photos? *Only you*
- Allow your stuff to be added to a gallery? *No*
- Hide your Exif data? *Yes*
- Show which application you used for uploading? *No*
- Hide your stuff from public searches? *Check all three*
- Who can see what's on your profile? *Friends and family*
- Who will be able to see, comment on...? *Friends and family*
- Who will be able to see your stuff on a map? *Only you*
- Import Exif location data? *No*

Facebook - Compresses images & deletes Exif, increasing privacy

Go to *Triangle* > *Settings* > *Privacy*.

- Who can see your future posts? *Friends*
- Limit the audience for old posts...? *Limit Old Posts*



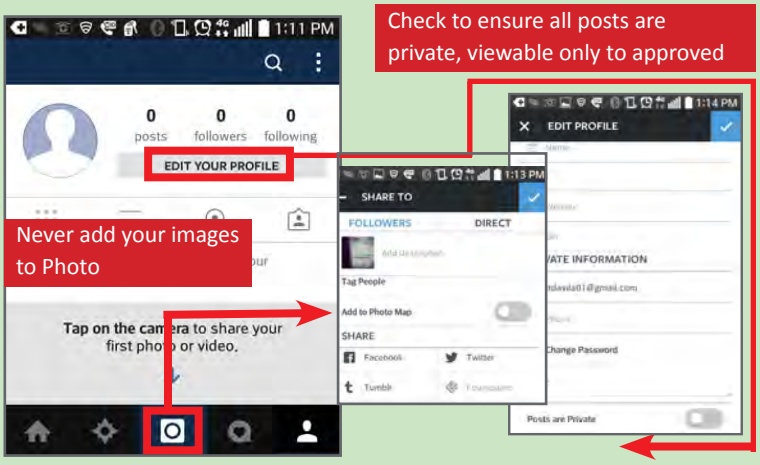
Then click *timeline and tagging*. Set as follows:

- Who can post on your timeline? *Friends*
- Review posts friends tag you in before they appear on your timeline? *Enabled*
- Who can see posts you've been tagged in on your timeline? *Friends*
- Who can see what others post on your timeline? *Friends*
- Review tags people add to your own posts on Facebook? *On*
- When you are tagged in a post, who do you want to add to the audience if they aren't already in it? *Only Me*
- Who sees tag suggestions when photos that look like you are uploaded? *No One*

Photo Sharing Services Smartcard

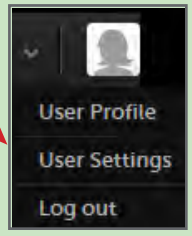
Instagram - Photos public by default, can be made private

Follow these pictographic instructions for Instagram on the iPhone:



Photobucket - Allows for password-protected sharing

In the upper right go to *User Settings*. On the *Albums* tab, uncheck all options listed under *Links* except *Link back to albums*.



Under *Privacy* set as follows:

- Allow others to follow me. *Uncheck*
- Allow comments in my albums. *Check*
- Show where my photos were taken. *Uncheck*
- Allow others to copy my photos & videos. *Uncheck*
- When I upload, permanently remove information about where my photos were taken. *Check*

Under Album Privacy, for each album choose to either:

- Make Private – Only you can view, or
- Password Protect – Anyone with the URL link and the password can view

Remember, choose unique passwords for each album

Google+ - Retains all Exif, multiple privacy settings

Navigate to *Google+ Dropdown Menu > Settings*.

Under *Photos* and *Videos*, set as follows:

- Show geolocation information... *Uncheck*
- Allow viewers to download my photos and videos.
- *Uncheck*
- Find my face in photos and videos... *Uncheck*
- People whose tags of you are automatically approved. *Groups and persons*

Under *Profile*, set as follows:

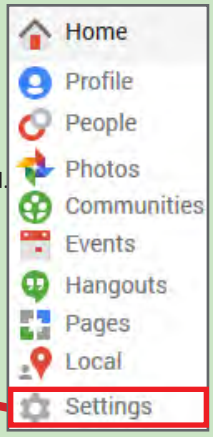
- Show these profile tabs to visitors. *Uncheck all*

Under *Hashtags*, set as follows:

- Add related hashtag from Google... *Uncheck*

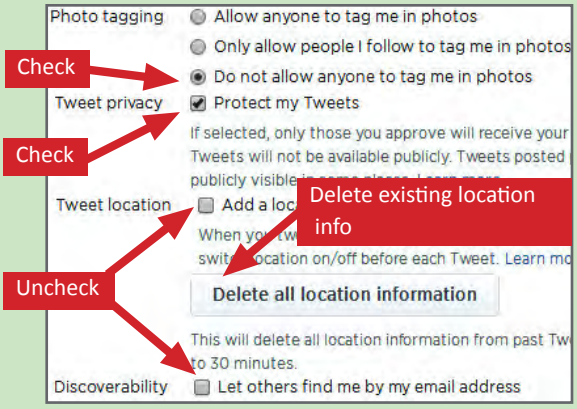
Under *Location settings*, set as follows:

- Enable location sharing. *Uncheck*



Twitter - Removes Exif, but minimal options to limit visibility

In the upper right, go to Settings > Privacy. Match your settings to those shown.



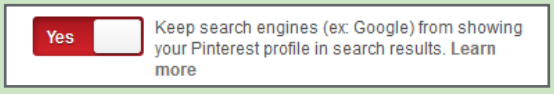
Yfrog Services - Removes Exif, privacy settings very limited

Yfrog can be used to post links to photos on Twitter and has also become its own social network called Yfrog Social. When using Yfrog with Twitter, go to *Settings* and disable photo tagging.

When using Yfrog Social navigate *Settings >> Account Info* and set the profile to *private*. Individual privacy settings can also be chosen for each picture and album during upload.

Pinterest - Retains Exif, privacy settings very limited

In the upper right go to *Settings* under the drop down menu. Under Basic Information turn *Search Privacy On*.



Useful Links

U.S. Army Social Media Roundup	http://dmna.ny.gov/members/geotagging.pdf
Washington State Web Wise	http://www.atg.wa.gov/InternetSafety/SharingOnline.aspx
Microsoft Safety & Security	http://www.microsoft.com/security/online-privacy/location-services.aspx
OnGuard Online	http://www.onguardonline.gov/articles/0033-heads

Online Registration Smart Card

20140703

Online Registration - Do's and Don'ts

Online services include sites that require users to register for personal profiles prior to using their functionality. Best practices include:

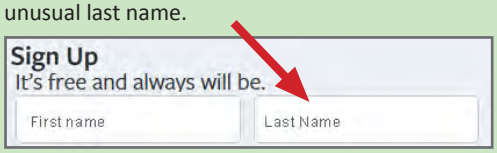
- Review the online service's terms of service to determine their data sharing policies with third party entities.
- Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- Never give online services access to your social security number or physical address.
- Turn down options to upload and share your existing contacts with the new social networking service during registration.
- Change privacy settings to protect your identity information immediately after registering for an online profile.

Identify Elements of Social Networking Site (SNS) Accounts

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

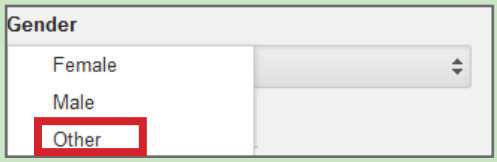
First and Last Name

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 unusual last name.



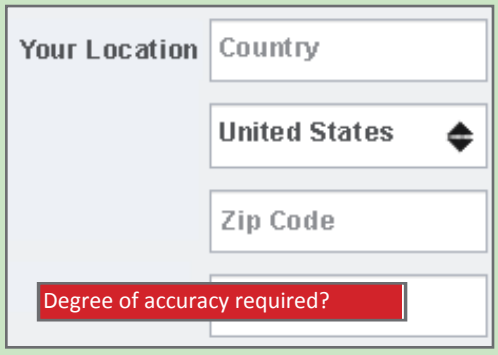
Gender

Gender is a common field to fill out on the registration page, used mostly for future content customization. Whenever possible, avoid making a distinction when signing up for your account.



Location: Address, Zip Code, Country

Location information is required at varied levels of granularity depending on the service. It may include address, zip code, and/or country.



Facebook Account

Many third party websites have adapted Facebook's authentication platform, Facebook Connect. Signing up with Facebook enables users to create new accounts by importing information that already exists on Facebook. Some sites require this process.

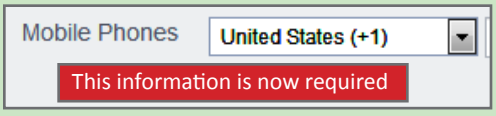
Username

Username is unique to each user account, unlike first and last name which can be shared across multiple users. **DO NOT** include personally identifiable information, such as last name or birthday, when making your username.

DO NOT use the same password across your SNS Accounts. Use unique passwords for each of your accounts.

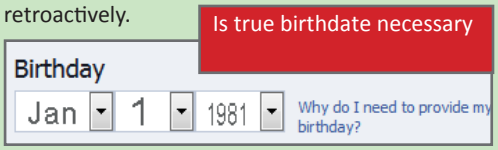
Mobile Phone Number

Registering for email accounts frequently requires a verifiable phone number. Refrain from using services that require phone numbers or opt to use an alternative method to verify accounts.



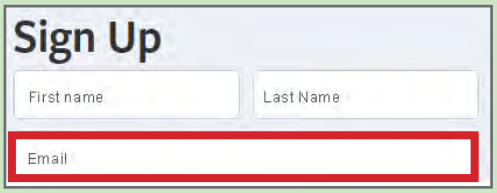
Birthday

Birthdays are used to verify the user's age and customize age-appropriate content for the user on the site. This information is sometimes published on the SNS profile and has to be removed retroactively.



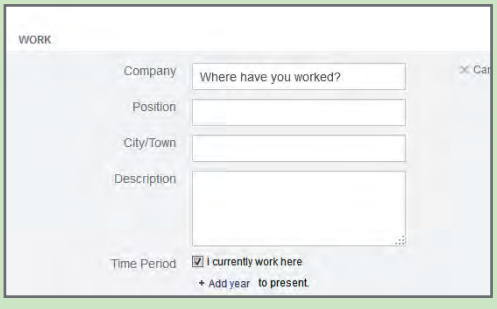
Email Address

Email is the 2nd most common requirement for creating a SNS account. It is used to **verify your account** during registration and often used as a credential during future log-ins.

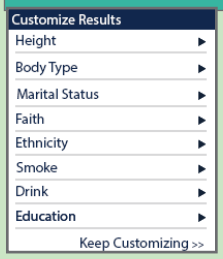


Company/Employment Information

Company and employment information are required for professionally-oriented SNS services, where the main purpose is to meet and build your network with other people in your field.



Sexual Orientation/Relationship Status



These fields are most often required in **online dating sites**, where the main purpose is to meet people.

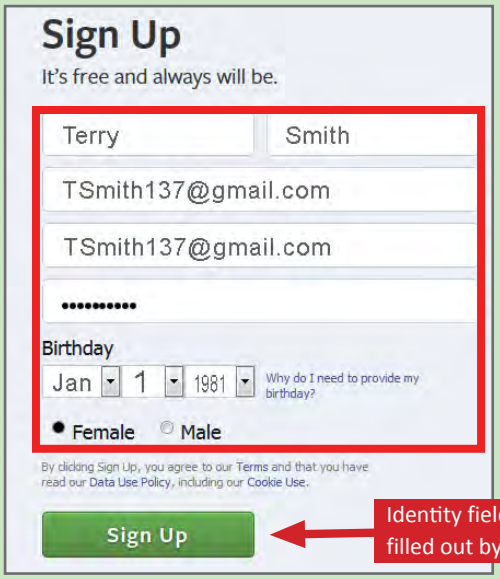
Online Registration Smart Card

Identity Information Required During Registration by Services

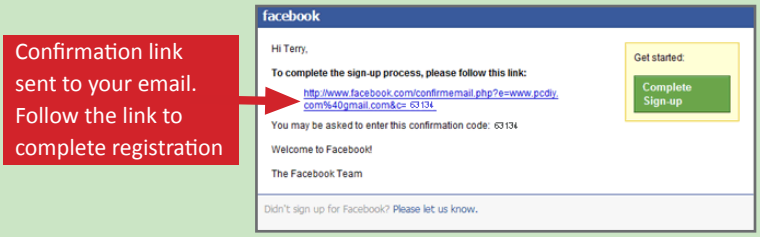
	LinkedIn	Facebook	Twitter	Google+	Yahoo	MSN	FourSquare	Pinterest	OkCupid
First and Last Name	x	x	x	x	x	x	x	x	
Username			x	x	x	x		x	x
Password	x	x	x	x	x	x	x	x	x
Birthday		x		x	x	x	x		x
Gender		x		x	x	x	x	x	x
Email Address	x	x	x	Or sign-up for a new Windows Live Account		x	x	x	x
Phone number				optional	x	optional			
Country	x			x		x			x
Company/ Employment Info	x								
Job Title	x								
Zip Code	x					x			x
Facebook Account	optional				optional		optional	optional	optional
Sexual Orientation									x
Relationship Status									x

Online Registration and Verification Process

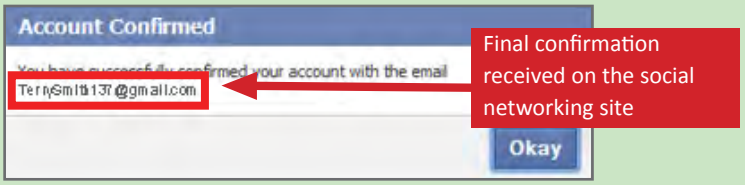
1 Enter required identity fields on the registration page.



2 Confirm your account via email. Avoid using mobile phone verification when possible to prevent sharing additional personal contact information.



3 Finish the confirmation process on the service website.



Useful Links

Microsoft Safety & Security	http://www.microsoft.com/security/default.aspx
A parent's Guide to Internet Safety	http://www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	https://www.privacyrights.org/privacy-basics
OnGuard Online	http://www.onguardonline.gov/topics/social-networking-sites.aspx

Anonymous Email Services Smart Card

20140826

Anonymous Email Services - Do's and Don'ts

- Always use a secure browser that anonymizes your IP address for accessing anonymous messages. Be sure your browser is updated regularly.
- Do not access more than one account in a single browser session, and never access named accounts, such as Google or Yahoo in the same session.
- Do not include personal details in your communication that could be used to identify you, such as your name, phone numbers, or addresses.
- Use public WiFi for additional anonymity and never repeat usernames or passwords.
- Remember, no set of tools can guarantee online anonymity.

Using an Anonymous Email Account

Anonymous email services can be used to send personal or work-related messages without leaving a trace of your identity. Truly anonymous email accounts require no personal information to register and retain little usage data. They should always be accessed and used **in conjunction with an anonymous IP address**.

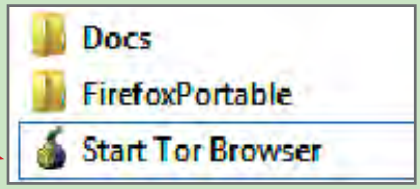
Using Tor to Anonymize Your IP Address

What is Tor?

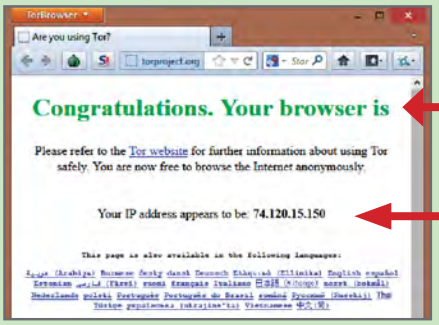
- Tor is a free, open source web browser that uses a volunteer network of servers and a layered encryption process to **anonymize your IP address**
- Before you access an email service, you must download and install Tor to protect your device's unique IP address
- Tor does not protect the information transferred between the Tor Network server and your destination site

1 Visit torproject.org and download the ***Tor Browser Bundle*** to your hard drive or a flash drive.

2 Open *browser.exe* in Windows Explorer, then open the new *Tor Browser* folder and double-click ***Start Tor Browser***.



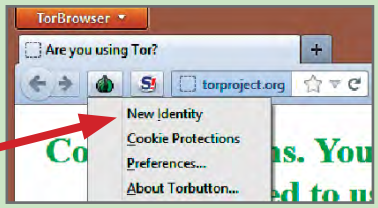
3 Make sure your Tor Browser is providing you with an anonymous IP address.



Your Tor Browser should display this message

Tor will display your device's IP address as it appears online

At times, you may have to change your Tor-generated IP address. You can renew a different IP address by going to ***Green Onion*** > ***New Identity*** in the top corner of the Top Browser.



Choosing the Right Anonymous Email Service

The following services can be used to send and receive messages anonymously or semi-anonymously. These two services specialize in security and privacy, have simple sign up processes requiring no personal information, and divulge account data only under rare circumstances, if ever. The right service for you will depend on the organization providing the service, frequency of your use, and the primary nature of your communications.

Service	Organization	Service Type	Data Retained by Service	Data Sharing Policy	Cost/ Payment Options	Suggested Frequency	Primary Use
Hushmail (hushmail.com)	Hush Communications Canada, Inc., Canada	Webmail	IP Address, purchase information*	No 3rd party sharing unless issued a court order	Premium/ Visa, MasterCard, Amex, Paypal, Money Order	Daily to Weekly Access	Scheduling in-person meetings, private correspondences, press communications
Cloak My (cloakmy.org)	Webmy.me Inc., California, USA	Message and chat	IP address, session cookies	No 3rd party sharing	Free	One-time correspondence	One-time messaging and chat, no account required

* *Name, account and domain, alternate email, billing address, credit card information, IP address of purchase, for accounts.*

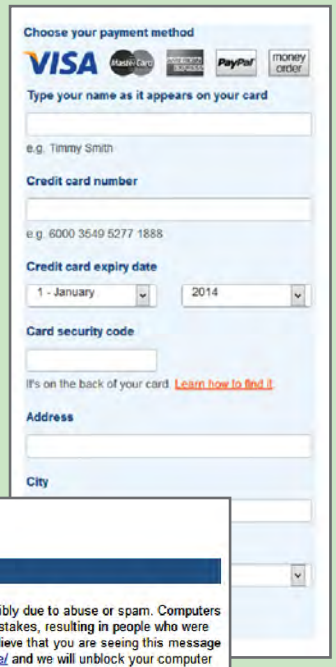
Anonymous Email Services Smart Card

Hushmail - Creating an Account and Using Tor

Hushmail is a traditional webmail service, similar to Gmail or Yahoo! Mail, that you can access through the Tor Browser. Unlike most webmail services, Hushmail does not collect personal information during registration. However, the service costs a minimum $34.99/year and requires payment methods that may expose your identity. To register for Hushmail:

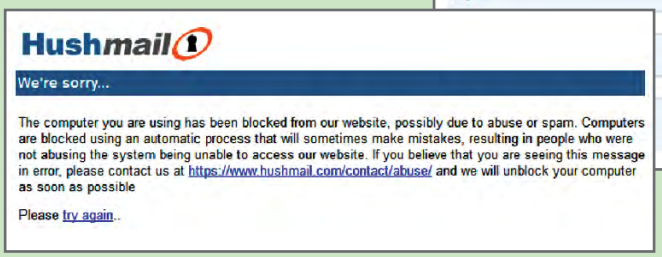
1 Fill out Hushmail's required registration information and create an account.

2 Hushmail requires you to purchase a subscription using Visa, Mastercard, American Express, Paypal, or a money order.



3 You can login to Hushmail's webmail client on the top right of the hushmail homepage to send and receive messages.

4 If you see the following message when attempting to sign in to your Hushmail account, you must use a new Tor Identity (see step 4 on the previous page).

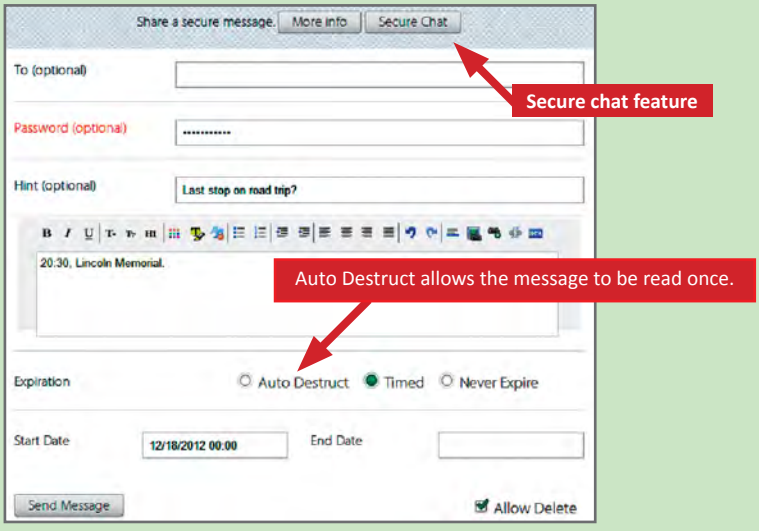


Cloak My - Sending Messages and Options

Cloakmy is a one-time message and chat service. Cloakmy is free, requires no personal information, and is accessible through Tor. However, Cloakmy does require you to provide your recipient with the unique URL outside of the service.

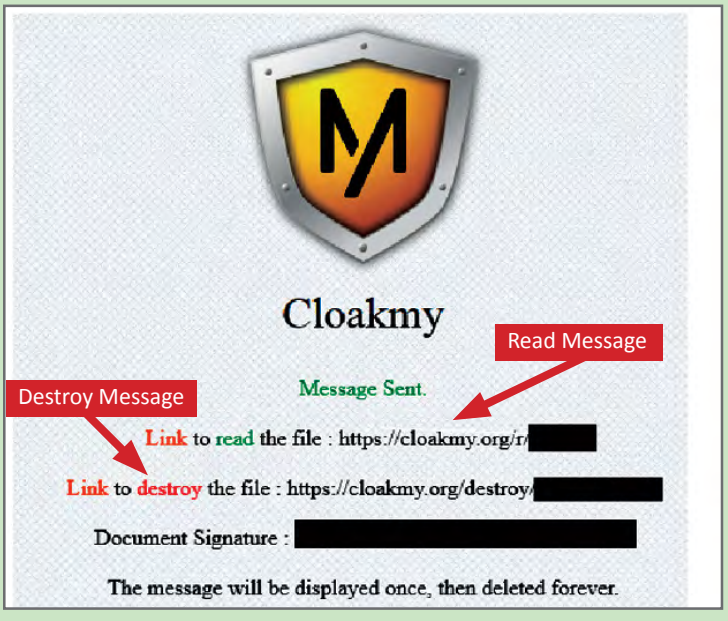
1 Enter the desired message. Supplemental information is optional.

2 Choose an expiration setting for the message.



3 After the message is sent, a unique URL location is created for the message.

4 You must distribute this URL to the recipient. **Only a user with this URL can view the message.**



Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	www.privacyrights.org/fs/fs18-cyb.htm
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/email.aspx
Online Guardian	www.onguardonline.gov/topics/social-networking-sites.aspx

Keeping Your Kids Safe Online

20140614

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 or your family that clearly show your face. 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, instead, use cartoons or avatars.
- 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 add-ons and software downloads are available to prevent and/or monitor a child's activities online.

Internet Explorer Browser 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.

Parental Controls

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

Passwords

Create a password for your child's account that only you and other adult supervisors know in order to ensure an adult presence.

Time Restrictions

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

Google Chrome Browser Settings

Download the Blocksi extension from the Google Chrome Web Store to employ child safety settings for the Google Chrome browser.

Advance Setup

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

Filters

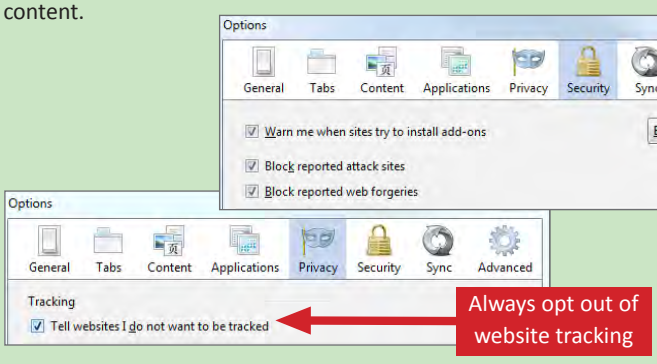
YouTube Filter - Filters individual YouTube channels and movies for content.
Content *Filtering* - Identifies suspect words in webpages to prevent access.
Black/White List - Allows users to add specific URL's to block or allow.

Time Control

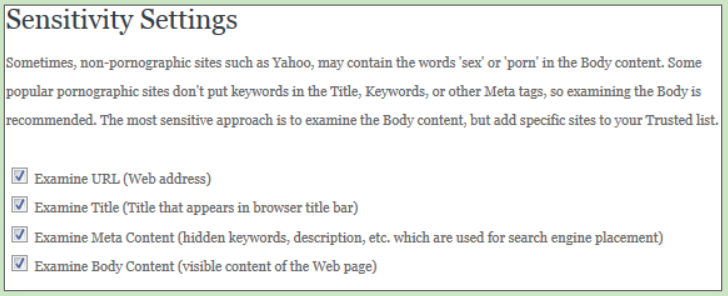
Set a time frame of acceptable computer use for your child that permits an adult supervisor to be present.

Firefox Browser Settings

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



Foxfilter for Firefox: To set parental controls, download the FoxFilter add-on. Once installed, users are allowed to set key words to block, permit acceptable sites, and set sensitivity settings.



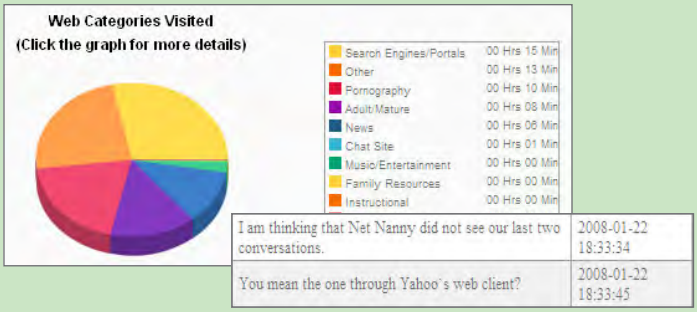
Keeping Your Kids Safe Online

Keeping Your Kids Safe Online - Do's and Don'ts

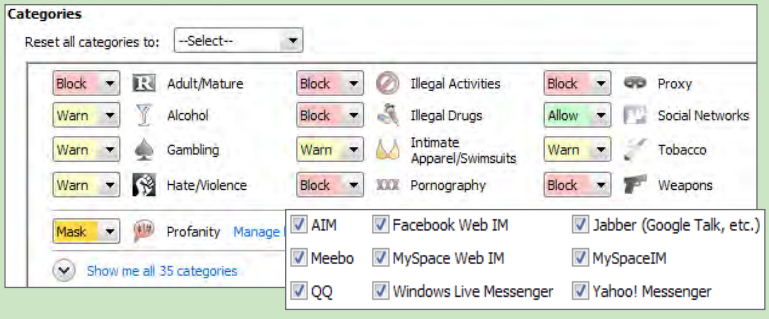
Service Capabilities	Software		
	Microsoft Family Safety	Net Nanny	Norton Family
Image Monitoring	Windows 8+	X	
SMS Message Monitoring		X	X
Contacts Monitoring	Windows 8+	X	X
Block Site Option	X	X	X
Allow Sites Option	X	X	X
Record User Activity	X	X	X
User Access Requests to Admin	X	X	X
Time Restrictions	X	X	X
Game Restrictions	X	X	
Paid Service		X	
Remote Access Notifications	X	X	X
Lock Safe Search	Windows 8+	X	

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.

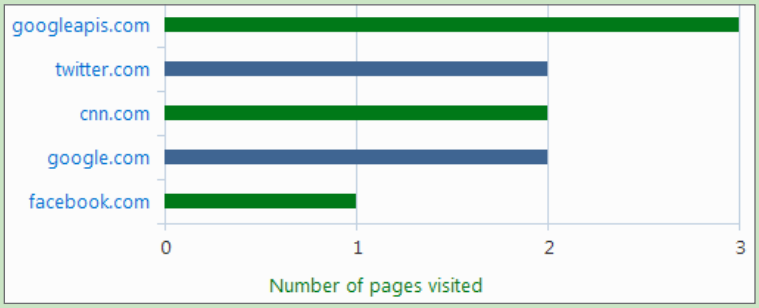


Overview

A variety of free and paid software packages are available for monitoring your child's online activities. The listed packages are effective in either preventing or monitoring content that your child tries to access.

Microsoft Family Safety

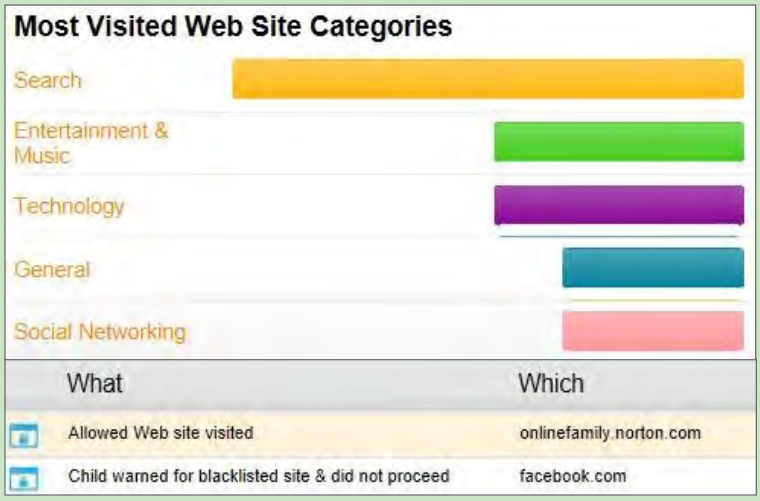
Download this free service from the Microsoft Windows website. The service provides basic content filters and reports of programs/websites accessed by each account.



Parents can set individualized settings for each account listed on the computer and can view their child's requests to access blocked content, each time they log in.

Norton Family

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



Norton Family also identifies the social networking profiles that their children maintain and allows the supervisors to see what information is being made public (name, age, profile picture, etc.). The service also prevents children from sharing personal information including phone numbers, Social Security numbers, and email addresses.

Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Privacy Rights Clearinghouse	www.privacyrights.org/fs/fs18-cyb.htm
Microsoft Safety and Security	www.microsoft.com/security/online-privacy/social-network
Online Guardian	www.onguardonline.gov/topics/social-networking-sites.aspx

Lock down Your Laptop Smart Card

Creating a Windows Login Password

Lock your laptop by making sure that your Windows user account is set up to require a password on log- in. A log- in password won't protect against an even semi competent hacker, but it could easily be enough to dissuade un-sophisticated criminals from snooping through your files after stealing your laptop.

In Windows 7, just hit **ctrl- alt - del** and select Change Password, the fourth option down. After that's set, head to the Power Options in the Control Pan-el, click **Require a password on wakeup** in the left- hand pane, and click the radio button next to **Require a password.**

In Windows 8, just search for "Users" to open up the Users menu in your PC Settings. Here you'll find options to both change your password and require users to log in when they wake the PC.

Encrypt Your Data

As mentioned above, a user account password won't protect your data from a determined snoop—they're easily cracked, or the thief can simply plug your hard drive into a different computer in order to access your files directly. If you travel and have any files on your computer that you simply don't want anyone else to see, you should use full disk encryption to keep them safe.

Because the strength of encryption is pretty much entirely dependent on the strength of your password, now would be a good time to talk about good password practices. You've probably heard it before, but a password can be easily cracked if it's too short or simple, or if you use the same one across multiple services. For the rest of your security measures to be effective, make sure you're following these three simple rules:

1. Use a password that's at least 12 characters, featuring a mix of lower case and upper case letters, as well as symbols and numbers.

2. Don't re- use passwords, especially for sensitive accounts, like your Windows logon, bank account and email account.

3. Change your password frequently. Every 6 months for important passwords, at the minimum. A free password manager like KeePass can make it a lot easier to follow the above rules. Again, make sure you choose a strong master password.

Bitlocker

Even without knowing your Windows password, intruders can easily gain access to files and passwords stored by Win-dows and other programs on your computer. They can do this by booting into their own operating system (Windows or Linux) from a special disc or USB flash drive. After doing so, they can access your hard drives just as you can when you're logged into Windows.

The only way to protect your data completely is by using encryption. You can encrypt select files, but to protect your system files and saved passwords, you must encrypt your entire hard drive. This operation takes more time and effort than encrypting select files does, but it offers more security--and it's great for laptops and netbooks that can easily go missing.

BitLocker offers protection for all of your personal files and documents, as well as for all of the system files and cached or saved passwords on your drive. Though Microsoft includes BitLocker with Windows Vista, Windows 7 Ultimate or Enterprise, and Windows 8 Pro or Enterprise, the feature isn't enabled by default. To activate it, you must manually enable it in the 'System and Security' Control Panel.

Lock down Your Laptop Smart Card

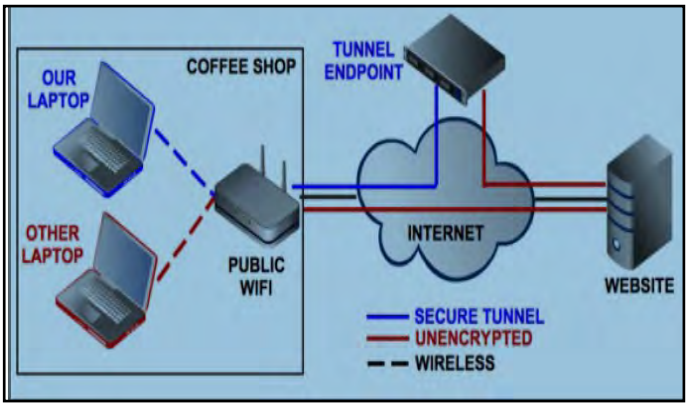
To support this simple encryption process, however, your computer must meet a few stringent software and hardware requirements. To start with, your drive must have two NTFS drive partitions: a system partition (which contains the files needed to start your computer), and an operating system partition (which you should have already, and which contains Windows and your personal files).

If the system partition is not already available, BitLocker may try to create it for you automatically, but sometimes it may not have enough available drive space to do so. In addition, your computer must have a motherboard with a compatible Trusted Platform Module (TPM) microchip, and the BIOS should be TCG (for Trusted Computing Group) compliant. Having a TPM microchip isn't mandatory, but without it the configuration and usability are more complicated.

If you don't understand the requirements, don't sweat it. To see whether your system meets them, simply open BitLocker: *Click Start, Control Panel, System and Security, BitLocker Drive Encryption, Turn on BitLocker.*

If your computer doesn't meet the requirements, it will let you know. If you get an error message about not having a TPM device, it's possible that your PC does have one that isn't enabled in the BIOS. Try checking your PC's BIOS setup menu at boot for any mention of TPM support. Otherwise, consider using a third-party encryption program, such as DiskCryptor, instead of using BitLocker.

Use a VPN on Unsecured Wi-Fi Networks



This diagram shows the difference between an unencrypted and a VPN-secured Internet connection.

Unsecured Wi- Fi networks present a major threat to your system's security on the road. You don't know who else is sharing the network, potentially intercepting and recording packets wirelessly sent by your computer. Basic HTTPS web security does a good job of protecting data sent across the internet, but you are essentially at the mercy of the receiving site's security protocols. If you're transferring sensitive data, the sensible solution is to always use a virtual private network.

With a VPN, traffic originating from your laptop is encrypted, then sent to a third party server, where it can safely be forwarded on to the World Wide Web at large, safe from prying eyes. There are lots of options for connecting to a VPN. Your company may provide one for you to use, or you can set up your own VPN server at home. For most people, the easiest option will be to use a web- based VPN, many of which offer a limited free service, and low-price monthly rates for heavier users.

Easy- to- use programs such as Firesheep make it easy for snoops to see what you're writing in your e- mail messages, posting to your Facebook page, or buying online. But with a VPN, you can surf the Web through that virtual tunnel, away from prying eyes, and your Internet traffic is encrypted. Whether you just want to access Wi- Fi networks on the road without potentially exposing your activities to nosy strangers, or whether you need to enable a team of remote employees to handle business securely on the Internet, you can find a VPN to fit your needs.

VPN for Beginners

Numerous VPN providers, including Banana VPN, Black Logic, LogMeIn Hamachi, and StrongVPN, have started offering their services for a fee, generally from $15 to $20 a month.

Is the privacy factor alone worth the effort? Yes, but VPNs offer other advantages as well. For example, if you're in Canada, ordinarily you can't watch a U.S. TV show on Hulu. But you can access the show if you use a VPN to obtain a U.S. IP (Internet Protocol) address.
Some VPN providers offer another benefit: anonymous Web browsing, which allows you to roam the Internet without being tracked. If your ISP blocks some applications, such as Skype or other VoIP (Voice over Internet Protocol) applications, you can use a VPN to get around the restrictions.

These VPN services may sound exactly like what you need. Beware, however: Not all services are created equal. If a service doesn't have enough VPN servers-- technically, VPN concentrators- - to support the number of customers, you may experience poor Internet speeds or be unable to make a connection at all. So, before subscribing to a VPN service, look into what its customers say about it. Better still, if the company offers a free test period, take advantage of it before paying money for a service that may not meet your needs.

Lock down Your Laptop Smart Card

20141029

VPN on Your Router

Besides paying $15 to $20 a month to a VPN subscription service, you might be able to install a VPN server into your router using open-source, alternative router firmware such as DD-WRT and OpenWRT. This firmware will allow you to use many, but not all, Wi-Fi routers and access points as VPN endpoints.

Before flashing your Wi- Fi hardware with any alternative firmware, make sure that it's supported. The last thing you want to do is to "brick" your wireless device--rendering it useless--just to set up a small VPN. Be sure to consult the DDWRT or the OpenWRT supported device lists. As these lists are all works in progress, check back often if you buy a brand-new router or access point. If you'd rather not take your hardware's life into your own hands, some routers, such as Buffalo Technology's WZR- HPG300NH AirStation Nfiniti Wireless-N High Power Router, come with DD-WRT already installed.

VPN Server Software

Some desktop operating systems, including Windows (from XP) and Mac OS X, include VPN server software. Granted, these are very simple VPNs, but they may be all you need. Of course, the Windows Server family comes with more- sophisticated VPN setups. If you're running all Windows 7 clients and Windows Server 2008 R2, you may also want to consider using DirectAccess, an advanced IPSec VPN that runs over IPv6 on ordinary IPv4- based LANs and the Internet.

If you don't choose to use DirectAccess but opt for Microsoft's older VPN technologies, Windows Server 2008 R2 has a helpful new feature: VPN Reconnect. Just as the name suggests, it will try to connect VPN sessions automatically if they're interrupted by a break in Internet connectivity. This function can be handy for users with spotty Wi- Fi connectivity, since they won't need to manually reconnect with the VPN after they reestablish a network connection. Most popular routers, such as the Linksys WRT160NL, make it easy for a VPN connection to work through the firewall.

Another way to add a VPN to your small network is to install VPN server software yourself. The best known of these is OpenVPN, which is open-source. It's available in versions for almost all popular desktop operating systems, including Linux, Mac OS X, and Windows. If setting up native OpenVPN sounds a little too technical for you, you can run it as a VMware or Windows Virtual Hard Disk OpenVPN virtual appliance. With this arrangement, you'll have a basic VPN up and running in minutes. But OpenVPN is far from the only VPN software out there. Other programs worth considering are NeoRouter and Tinc.

Sources

http://www.pcworld.com/article/2025897/a-road-warriors-guide-to-locking-down-your-laptop.html
http://www.pcworld.com/article/242617/how_to_use_bitlocker_to_encrypt_your_hard_drive.html
http://www.pcworld.com/article/236006/KeePass.html
http://www.pcworld.com/article/223044/vpns_for_beginners_to_experts.html
http://www.dd-wrt.com/wiki/index.php/Supported_Devices
http://wiki.openwrt.org/toh/start

Identity Theft Smart Card

201410243

What to do if your identity is stolen

The FTC has put together a great, step-by-step guide on what to do if you think your identity has been stolen. Here's where to start:

Take action immediately! Keep records of your conversations and all correspondence.

Flag Your Credit Reports. Contact the fraud department of the three major credit reporting agencies. Tell them you are an identity theft victim. Ask them to place a "fraud" alert in your file. An initial fraud alert is good for 90 days.

- Equifax 1-800-525-6285
- Experian 1-888-397-3742
- TransUnion 1-800-680-7289

Order Your Credit Reports. Each company's credit report about you is slightly different, so order a report from each company. They must give you a free copy of your report if it is inaccurate because of fraud. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact your creditors about any accounts that have been changed or opened fraudulently. Ask to speak with someone in the security or fraud department.

Create an Identity Theft Report and Report it to the Local Police. An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:

- File a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- Take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

These two documents comprise an Identity Theft Report.

For more information regarding identity theft, visit the following websites:

- Federal Trade Commission (FTC) http://www.consumer.ftc.gov/features/feature-0014-identity-theft
- FTC Identity Theft Online Complaint Form https://www.ftccomplaintassistant.gov/
- www.fraud.org (You can also call: 1-800-876-7060)

12 Practices to Avoid Identity Theft

1. Do not disclose your full nine-digit Social Security number

2. Avoid paper billing by requesting secure electronic statements instead

3. Lock your mailbox

4. Keep your information safe, both online and offline, shred documents containing personal information and password protect sensitive computer files

5. Use unique hard-to-guess passwords that include a combination of letters, numbers, and symbols

6. Avoid the same password across multiple accounts

7. Install and update antivirus, anti-malware, and security programs on all computers, tablets, and smart-phones

8. Don't disclose information commonly used to verify your identity on social network sites like, date of birth, city of birth, mother's maiden name, and name of high school

9. Avoid making purchases, paying bills, or sending sensitive information over unsecured WiFi networks

10. Disable Bluetooth on devices when not in use

11. Watch out for "phishing" scams

12. Fight "skimmers" by touching ATMs to see if all the parts are solid and not add-ons; cover the hand typing the password; look for suspicious holes or cameras

Securing Your Home Wireless Network

20140228

Securing Your Home Wireless Network— Do's and Don'ts

- When creating passwords for your networks devices, ensure that they are sufficiently long and complex by using uppercase letters, lower-case letters, numbers, and symbols. Consider a multi-password phrase that does not consist of dictionary-based words. An example of a satisfactorily long and complex password would be ILuvF00tb@77 from the phrase "I love football."
- Use a cable to directly access the internet for any computers that remain stationary.
- Turn off your wireless network when you will not be using it for an extended period of time.
- If you have guest access set up for your network, ensure that it is password protected.
- If possible, turn on automatic updates for your network device's firmware. If automatic updates are not offered, periodically check for firmware updates on the network devices' websites and manually download and install them.
- If your router is compromised or if you cannot remember the password, you can restore it to the default factory settings by pressing the reset button located on the back of the router.
- Position the router away from windows and further into the interior of your house to decrease the reach of the signal.

Glossary of Commonly Used Terms

Wireless Router - Physical hardware that allows users to connect their devices to a shared internet network.
Service Set Identifier (SSID) - The public name of a wireless network.
Wired Equivalent Privacy (WEP) - Older security algorithm for wireless networks that has numerous security flaws.
Wi-Fi Protected Access (WPA) - More recent security algorithm for wireless networks. Also has many security flaws.
Wi-Fi Protected Access II (WPAZ) - The most secure algorithm for wireless networks. Improved upon and replaced WPA.
Pre-shared key (PSK) - An authentication mechanism that mandates a password. Adds additional security to wireless networks.
Hypetext Transfer Protocol (HTTP) - Protocol for communication over a computer network.
Hypertext Transfer Protocol Secure (HTTPS) - Uses various encryption protocols to add additional security to HTTP.
Media Access Control (MAC) Address - A unique, individual identifier assigned to computers and devices.

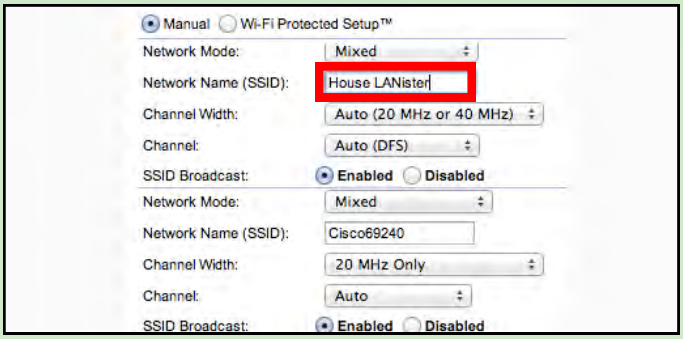
Access Your Router

To access your router, you must enter the appropriate IP address, username, and password. Most routers share similar log-in information

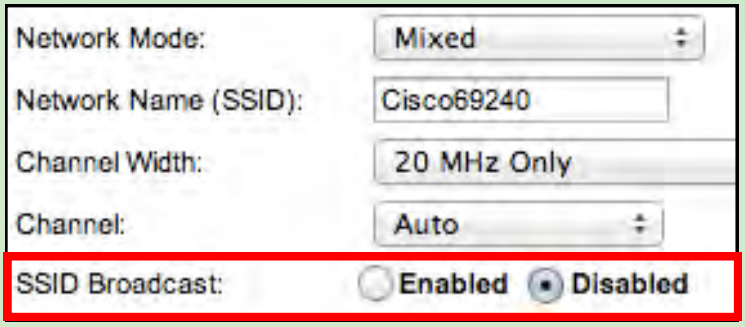
Router	IP Address	Username	Password
3Com	192.168.1.1	n/a	admin
Apple	192.168.1.1	admin	admin
Asus	192.168.1.1	admin	admin
Belkin	192.168.2.1	admin	n/a
Dell	192.168.1.1	n/a	admin
Linksys	192.168.0.1	admin	admin
Medialink	192.168.0.1	n/a	admin
Motorola	192.168.100.1	admin	motorola
Netgear	192.18.0.1	admin	password
TP-LINK	192.168.1.1	admin	admin
US Robotic	192.168.1.1	admin	admin

Choose a username that does not include you or your family's names and a password that is long and complex.

Creating a Unique SSID



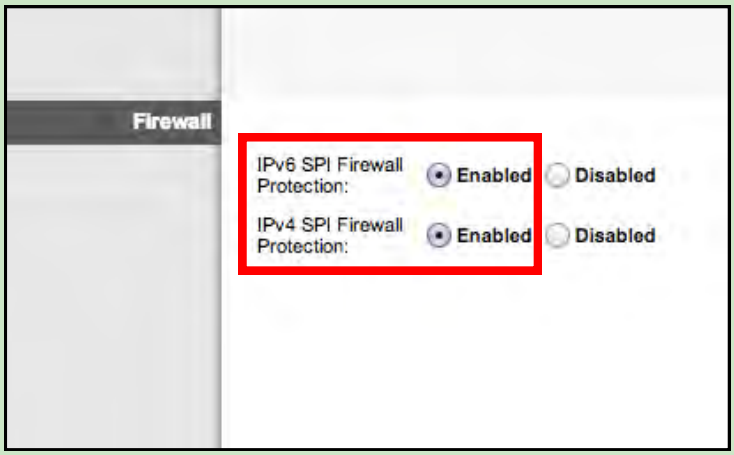
Disabling the SSID Broadcast



Securing Your Home Wireless Network

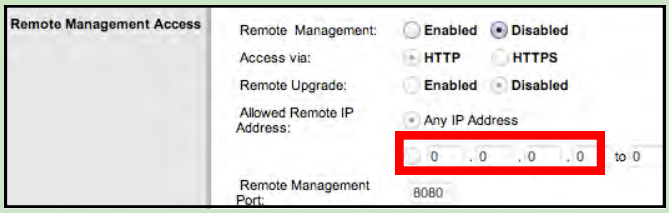
20140228

Router Firewall

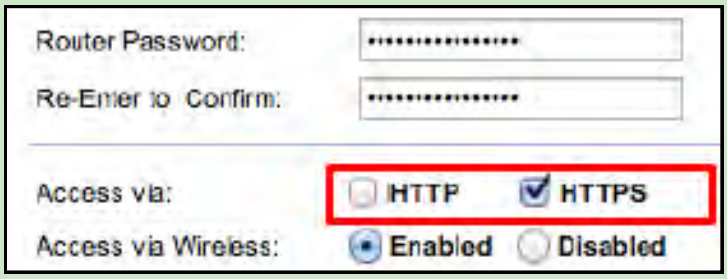


Remote Access

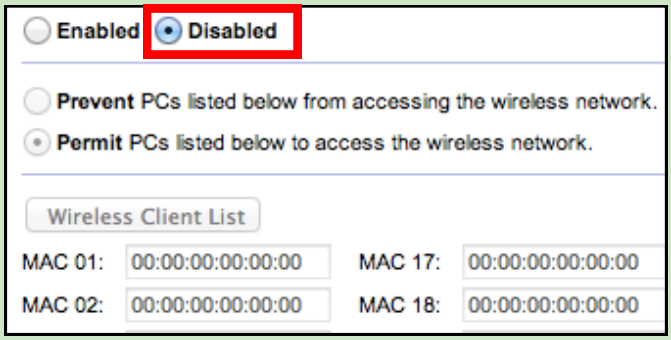
Check that the Remote Management IP Address is set to **0.0.0.0** in order to ensure that remote access is disabled.



Enabling HTTPS



Wireless MAC Filtering



Enable MAC address filtering to ensure that only approved computers and devices can connect to your router

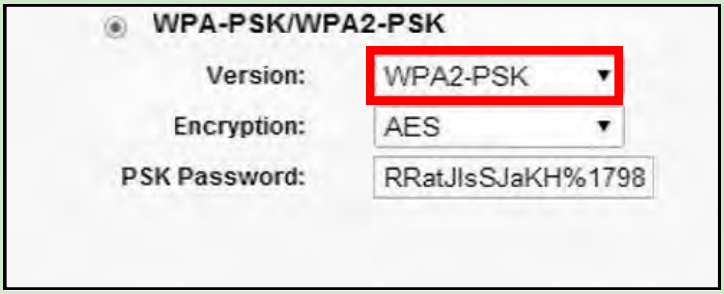
Adding MAC Addresses

Enter the Mac address and a brief description of the connected device.

Wireless MAC Filtering

Restricting administrative access through the web to specific devices. Add the MAC addresses of each computer and device you wish to add.

Encryption



Between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select WPA2-PSK and also AES for encryption. The PSK password should be long and complex, but different than the administrative router access password.

Useful Links

Practically Networked	http://www.practicallynetworked.com/support/wireless_secure.htm
Wi-Fi.org	www.wi-fi.org/discover-wi-fi/security
NIST	http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

Delete Cookies Smart Card

201410243

Introduction

Web cookies hide in your computer so that your browser and websites can track your browsing sessions and save certain useful information, such as account names and passwords, for later retrieval. Although cookies may seem harmless overall, they can threaten your privacy if an attacker tries to use them maliciously.

Because of that threat, most modern browsers make cookie storage easy to understand and control. They also make it simple to remove individual website cookies, or even to delete cookies from your computer entirely. Here's how you can perform the latter task in some of the most popular browsers.

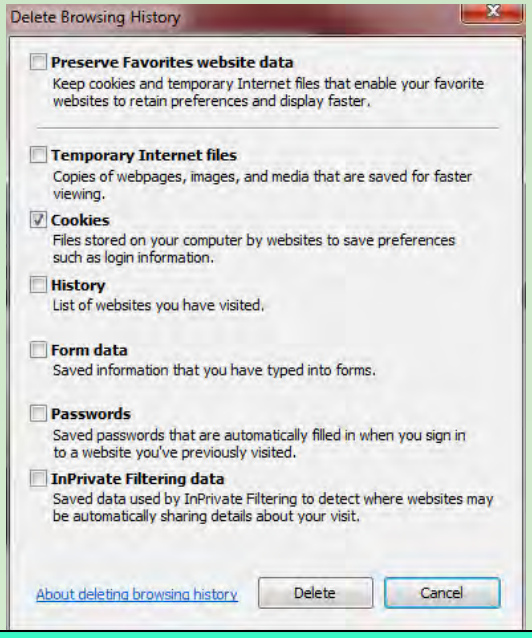
Delete Cookies in Internet Explorer

Note: *Much will depend upon your operating system and its version as to the precision of these instructions that are just one example from one version of IE on Windows OS.*

1. Upgrade to the latest version of Internet Explorer. Select the *Tools* menu from the Internet Explorer window, and click *Delete Browsing History*.

2. In the Delete Browsing History window, check the box next to *Cookies*. You can uncheck everything else if you want to remove only cookies.
From here you can choose which parts of your browsing history to erase.

3. Click *Delete* to remove all cookies stored in Internet Explorer.
Congratulations, you've successfully cleaned out your browser's cookie cabinet. Although cookie files pose a potential threat to privacy, don't forget that they can also improve your Web browsing by making it faster and more convenient.



Delete Cookies in Google Chrome

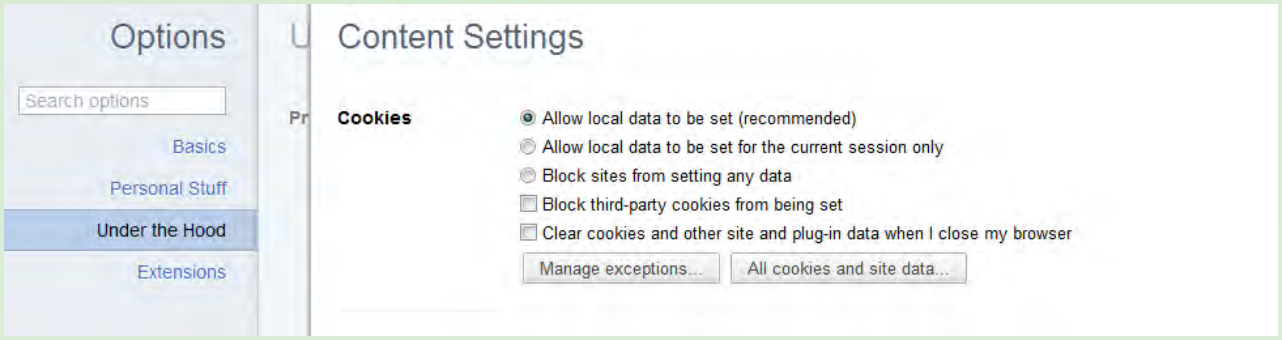
1. If you're running Google Chrome version 14 or higher, click the wrench button in the upper-right corner of the Chrome window. From there, select *Options*.

2. In the navigation pane of the Options page, click *Under the Hood.*

3. Under the Privacy section, click *Content Settings*.
Click the 'All cookies and site data' button in the Content Settings window.

4. Under the Cookies section, click *All cookies and site data*.

5. When the list of cookies appears, click the *Remove All* button to delete all cookies stored in Chrome.
Alternatively, you can navigate to the Cookies section of your Chrome browser and click the *Remove All* button to delete all cookies in one fell swoop.



Delete Cookies Smart Card

201410243

Delete Cookies in Firefox

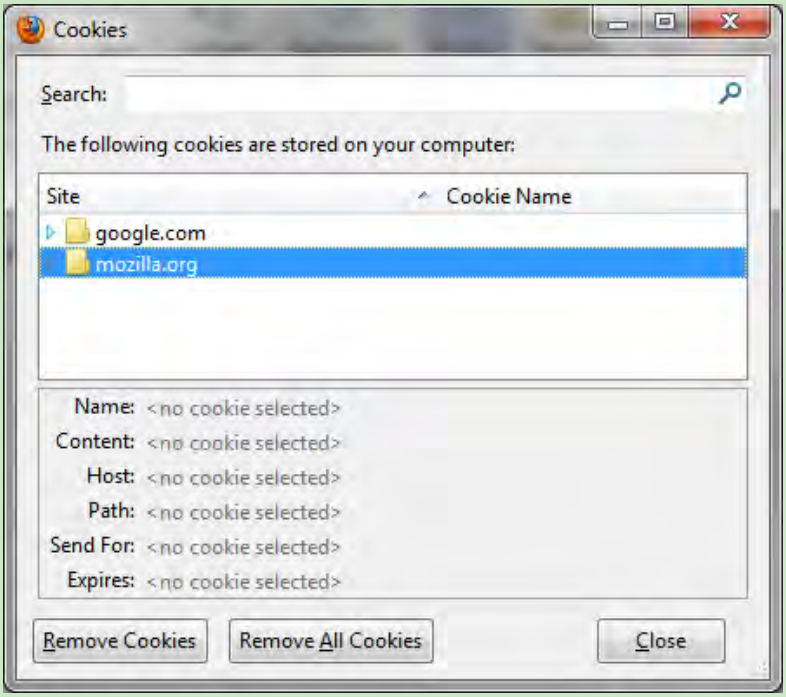
Note: *Screens and steps may vary depending upon the version of Firefox and the OS used. This is one example of a Firefox version with a Windows OS.*

1. Make sure you are running the latest version of Firefox browser, and the select *Tools* from the Firefox menu. From there, select *Options*.

2. Click the *Privacy* tab to bring up your user-privacy options.

3. Under the History section, click the *Remove Individual Cookies* link. Click the Remove All Cookies button to zap them.

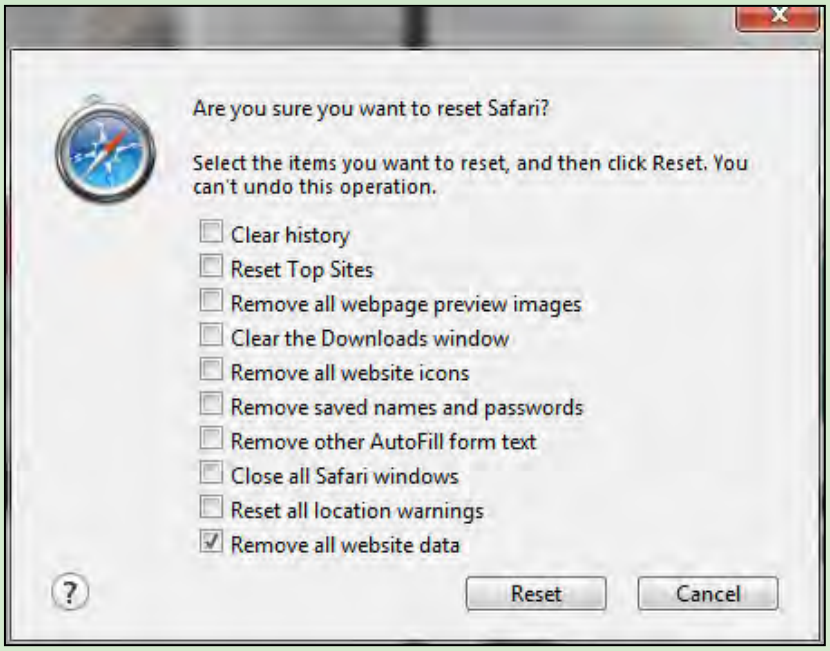
4. At the bottom of the Cookies window that appears, click the *Remove All Cookies* button to delete all cookies associated with your Firefox browser.



Delete Cookies in Safari

1. Confirm that you're running version 5 or later of Apple's Safari browser and then click the Gears menu in the upper-right corner of the Safari window. From there, select *Reset Safari.*

In this window, check the bottom box, 'Remove all website data'.



2. Check the bottom box, labeled *Remove all website data*. You can uncheck everything else if you want to remove only cookies.

3. Click the *Reset* button to eliminate all cookies associated with Safari.

Delete Browser History Smart Card

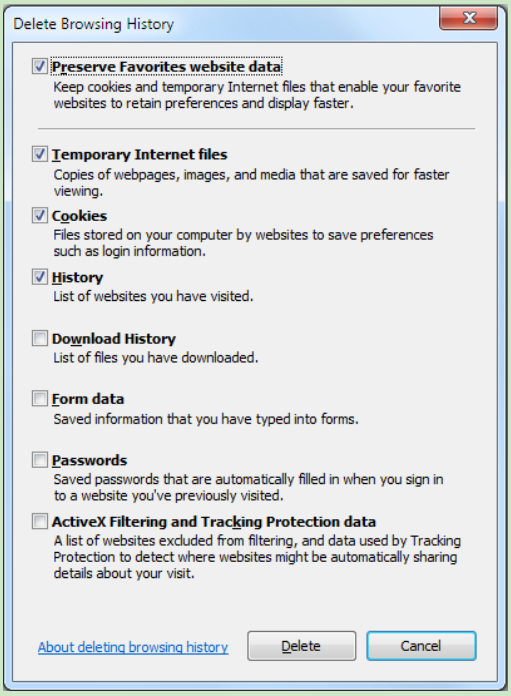
201410243

Introduction

Items such as browsing history, cache and cookies are saved on your browser while you surf the Web, utilized in a number of different ways to improve your browsing experience. These private data components, while offering conveniences such as faster load times and auto-populated forms, can also be sensitive in nature. Whether it be the password for your email account or the information for your favorite credit card, much of the data left behind at the end of your browsing session could potentially be harmful if found in the wrong hands. In addition to the inherent security risk, there are also privacy issues to consider.

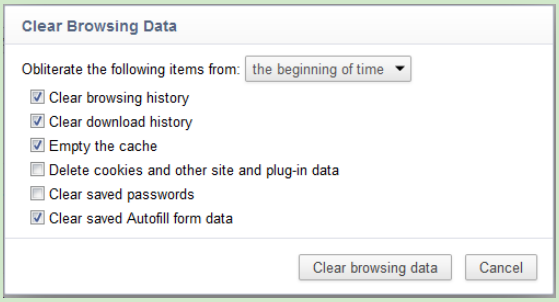
Delete Your Internet Explorer History

A useful keyboard shortcut for deleting your browsing history in Internet Explorer is *Ctrl-Shift-Delete*. If you press this combination of keys in a recent version of Explorer, you'll bring up a dialog box that lets you specify what you want to keep and what you want to purge. Simply check the boxes next to the history you want to remove and then click *Delete*.



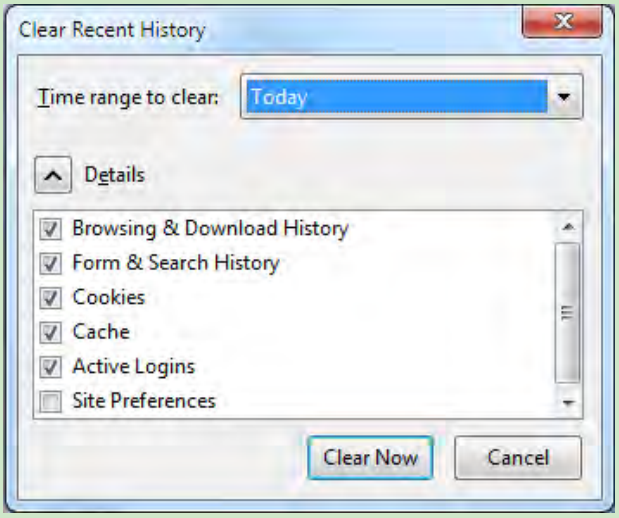
Delete Your Google Chrome History

Chrome users have access to the same slick keyboard shortcut as Internet Explorer users. Press *Ctrl-Shift-Delete* in Chrome, and you'll see Google's options for deleting your browser history. As with IE, simply check the boxes next to the history items you want to clear, but be sure to examine the options available to you in the drop-down menu at the top. This menu allows you to specify how much of your history you'd like to delete. You can choose to excise the past hour, day, week, or month--or you can obliterate everything since the beginning of time.



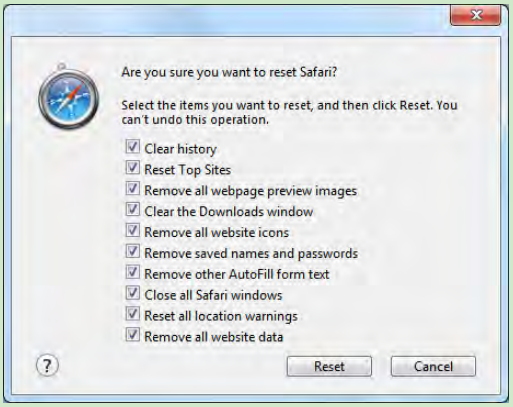
Delete Your Firefox History

Firefox fans, too, have access to the same keyboard shortcut for deleting browser history as IE and Chrome users: Press *Ctrl-Shift-Delete* to summon the history-clearing options that are available to you in Firefox. If you don't see a detailed list of what you can and can't delete, click the *Details* arrow to reveal the specifics. As with Chrome, you have the option of choosing a time range to clear. The options are a bit different, however. In Firefox, you can clear the last hour, the last 2 hours, the last 4 hours, the last full day, or your entire Firefox history.



Delete Your Safari History

Like most browsers, Safari has a ton of keyboard shortcuts, but it doesn't have one for deleting your browser history. Instead, click the gear icon in the upper-right corner, and select *Reset Safari*. In the resulting pop-up menu, check the items that you want to clear; then press the *Reset* button to purge your data.



Source: Jonathan Wylie, "How to Delete Your Browser History," PCWorld Dec 20, 2011; http://www.pcworld.com/article/246049/how_to_delete_your_browser_history.html

Delete Browser History Smart Card

201410243

Delete Your History on Android Devices

There are different browsers and even applications to consider, so here's a guide to doing so for three of the most popular Android browsers – Chrome, Firefox and Google Play Store.

Chrome Browser for Android

Chrome is the default web browser of the Android, so this is crucial for users of devices with the most recent updates (which are always recommended) and stock browser settings. With any tab open in the Chrome app, select the three square dots in the top right of the window and select *Settings*. Under the 'Advanced' heading choose *Privacy*, and then on the right side of the top bar you will see 'Clear Browsing Data'. Simply select this and choose what you wish to remove (history, cache, cookies, form data, saved passwords etc) and your web history is removed.

Alternatively, if you don't want the sites you browse to be stored in Chrome's history, simply go into *options* (the three squared dots) and select *New Incognito Tab*. Data won't be stored for the duration that this tab is in use.

Firefox Browser for Android

To remove your history in Firefox for Android, again select the three square dots in the top right, and choose *Settings*. Under the third division, named 'Privacy & Security' you will find *Clear Private Data*. From there, you can choose what you wish to delete and select *Clear Data*.

Google Play Store for Android

Browsers aren't the only applications which retain a history on an Android device. If you regularly search for apps in the Play Store, you may notice when you search for a new app that your previous searches remain. To remove these, choose the three square dots in the top right of the Play application, select *Settings* and under 'General' tap *Clear Search History*.

Google For Android

If you own an Android device, then you have a Google account. Any time you are logged on to that account, on any device that is connected to the internet, Google will store your search in case you want to revisit it later. If you didn't know that Google was doing this, or think you'd rather not have Google storing such data, you can clear the history and stop it storing future searches. To do this go to http://www.google.com/history and sign in to your account. Once in, choose the cog icon on the right and select *Settings*. Here you can clear your search history, and turn off your future 'Web History'.

Source:

Dave Kim on February 25, 2013; http://www.mobilesecurity.com/articles/384-how-to-clear-your-android-browsing-history

Clearing Safari's History

Open Settings. From your home screen (the default location), tap the Settings icon, open the Settings control panel. *If you don't see your Settings, swipe the screen, moving it to the left until you reach the Search page. Enter "settings" in the search field, and then tap on the Settings icon in the results.

Locate Safari. In the Settings control panel, search for Safari. It will be below all the built in apps. When you find it, tap the button to open the Safari control panel.

Locate the Clear History button. In the Safari control panel, scroll down to the Privacy section, and find the Clear History button, then tap it. Tap the Clear History button to erase your browsing history. You'll be asked to confirm that you wish to clear your history. Accept the confirmation. This removes only your browsing history—the specific web pages you've visited—but leaves intact everything else.

Choose additional options. You can clear cookies and data, as well. This is information used by websites that you visit to preserve such things as logins, auto-fill account info, and other automated functions.

Go private. For browsing without leaving a history, or cookies and data, enable Private Browsing. While this leaves no trace of your browsing activities, it will also not store passwords or other login data. *Note that when you disable Private Browsing, any pages you leave open will no longer be private.

*Note: iOS 5 or later: To clear other stored information from Safari, tap Advanced > Website Data > Remove All Website Data
**Note: With iOS 7 you may have to disable restrictions first. Go to settings > General > Restrictions > Disable restrictions. Then go to Safari and delete history. Then go back to restrictions and enable them.

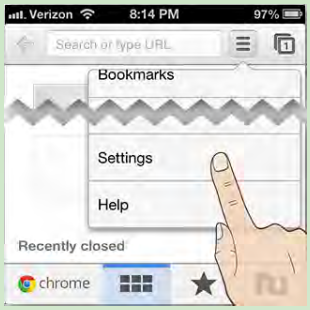
Delete Browser History Smart Card

201410243

Clearing Chrome's History

Launch Google Chrome. If you've downloaded it, but can't find the app, swipe the screen, moving it to the left until you reach the Search page. Enter "chrome" in the search field, then tap on the Chrome icon in the results.

Open the Settings panel. Tap the Chrome menu in the upper right: it looks like 3 short horizontal lines. Locate the Settings menu item at the bottom of the list, and tap it to open the Settings control panel.



Tap Privacy. In the Settings panel, locate the Privacy button, and tap it to open the Privacy control panel.

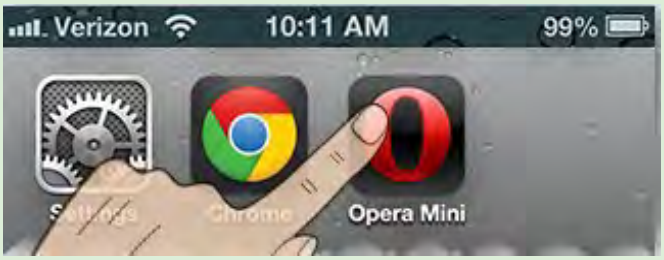
Clear Browsing History. It's located at the top of the page in the Clear Browsing Data section.

Accept the confirmation. From the popup confirmation dialog, tap the large red Clear Browsing History button. This will clear your entire browsing history for Google Chrome. •In the same section, you can also clear your cache, cookies and site data, or everything.

Browse "Incognito." For total history-free browsing, select "New Incognito* Tab" in the Chrome menu.

Clearing Opera's History

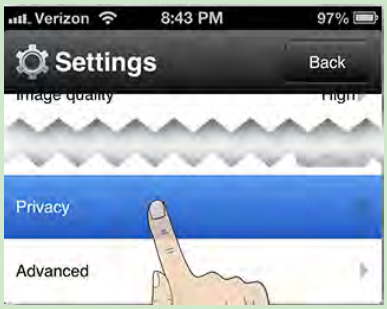
Launch Opera Mini. If you've downloaded it, but can't find the app, swipe the screen, moving it to the left until you reach the Search page. Enter "opera" in the search field, then tap on the Opera icon (a red O) in the results.



Clearing Opera's History (continued)

Launch Opera Mini. If you've downloaded it, but can't find the app, swipe the screen, moving it to the left until you reach the Search page. Enter "Opera" in the search field, then tap on the Opera icon (a red O) in the results.

Tap the Opera menu in the lower right. It is the Opera logo—the red O. A menu panel will pop up. Locate the settings option—a silver gear. Tap it to open the Settings control panel.



Tap Privacy. In the Settings panel, locate the Privacy button at the bottom of the screen. Tap it to open the Privacy control panel.

Tap Clear Browsing History. It's located at the top of the page in the Clear Browsing Data section.

Accept the confirmation. This will clear your entire browsing history for Opera Mini. In the same section, you can also clear your passwords and your cookies. As of this writing, Opera Mini has no provision for private or incognito browsing.

Source:

Serendipitee Combz, http://www.wikihow.com/Clear-History-on-an-iPhone

Additional Resources

20150110

Free Annual Credit Report https://www.annualcreditreport.com

The University of Texas Identity Center https://identity.utexas.edu/

Stay Safe Online https://www.staysafeonline.org/

On Guard Online http://www.onguardonline.gov/

Equifax: ID protection kit http://www.equifax.com/idtheftprotectionkit/

Federal Trade Commission: ID protection tips http://www.consumer.ftc.gov/topics/protecting-your-identity

IRS: ID Protection, Prevention, Detection and Victim Assistance http://www.irs.gov/Individuals/Identity-Protection

Netsmartz Workshop for Parents & Guardians http://www.netsmartz.org/netparents.htm http://www.netsmartz411.org/

FBI Parents Guide to Internet Safety http://www.fbi.gov/stats-services/publications/parent-guide https://sos.fb i.gov/

Online Safety Guidelines http://kids.getnetwise.org/safetyguide/

Network Advertising Initiative http://www.networkadvertising.org/choices/

Google Privacy http://www.google.com/intl/en/policies/privacy/tools/

Social Media Search http://iconosquare.com/instagram-search-tool http://web sta.me/search

http://Search.fb.com

http://Twilert.com

http://Search.twitter.com

http://Twazzup.com

For More information contact the Identity Management (IdM) Branch at:

Phone: 813-826-1256

Email: J3X-IDM.org@socom.mil

IdM NIPRNet portal at https://sof.socom.mil/sites/J3/J3X/IdM/Pages/IdM%20Trai ning.aspx

Identity Management

Biometrics

Behaviors

Community

Physical

Virtual

Records

Devices

Communications

Financial