Privacy & Security Package

Commonwealth of Virginia

Virginia Fusion Center

MAY 17, 2018

(U) Personally identifiable information (PII) can be gleaned from social media accounts as well as public databases by anyone with access to the Internet. Proactive measures must be taken and maintained to ensure one's privacy. The following guidelines are intended to assist individuals with privatizing their identity, minimizing their publically available digital footprint, and remediating compromised information.

(U) There are numerous steps an individual can take to protect his/her privacy. While some apply to the law enforcement community at large, other, more extreme measures may be more appropriate for individuals with higher risk assignments. Privacy is a personal matter and each individual will have to decide what level of privacy meets his/her needs. Additionally, the steps listed in this document are for consideration only and not to be taken as recommendations. As always, follow your departmental policy.

(U) This package contains guidance on identifying your digital footprint in social media and in public databases; suggestions for limiting the amount of data you release and for removing personal information on the Internet.

(U) In addition, this packet contains recommendations on how to secure social media accounts, Windows machines, and Internet of Things devices.

Identifying your Digital Footprint

(U) The internet has become a necessary tool that touches on most aspects of everyday life. It is relied on to conduct business, perform personal transactions, and communicate with family and friends. As the internet and digital media evolves, users must find ways of defending themselves from attacks whether from hackers, scammers, stalkers or from a physical threat. Identifying what is known about you online is the first step in keeping yourself safe.

(U) To help determine how much of a digital footprint you currently have, review and answer the following questions.

(U) Social Media Footprint

1. (U) What social media accounts do you have? (Facebook, Twitter, LinkedIn, etc.)

   ____

   ____

2. (U) What email addresses do you have?
   a. (U) Check to see if your email has been breached by using the website: haveibeenpwned.com
   b. (U) If so, change your email password and consider using different user names and passwords for all accounts associated with that breached email account.
   c. **(U) It is recommended that everyone use different user names and passwords for each account regardless of a breach.

   ____

   ____

3. (U) What social media accounts do family members and associates have?
   a. What information is posted about you, your LEO affiliation, your spouse or ex-spouse, children, etc.?

   ____

   ____

4. (U) Who is sending you requests, do you know them?

   ____

   ____

(U) CAUTION

(U) Do not assume that deactivating your social media accounts is enough to protect you. Consider the following scenarios:

(U) It is Father's Day and your son posts a picture of you two together on your latest fishing trip and writes about how much he appreciates and loves you. He innocently adds how proud he is that you decided to dedicate your life to helping others by serving as a first responder.

(U) It is time for prom; you take photographs of your daughter and her date in the front yard. The photo is uploaded to Instagram and Facebook. In the background is a clear shot of your take-home police cruiser.

(U) You are called in to work a protest. Your spouse, worried about your safety and tired of your crazy hours, goes to social media and posts his/her fears and corresponding desire for the protests to stop so you will not have to be away from home.

(U) It is National Law Enforcement week and your cousin shows his appreciation by giving you a shout out on Twitter, subsequently revealing the fact that you work for the Virginia State Police.

(U) At the fall festival being held at the neighborhood clubhouse, Sean goes dressed as a firefighter. A photograph appears in the next community newsletter with the caption "Resident of Parkview, Sean Smith, dressed as his firefighter father Thomas Smith".

(U) Public Footprint

(U) Social media platforms are not the only entities storing your information. There are large marketing companies paying big dollars for your data. There are brokers that trade, share and sell any information they can get their hands on. See below:

(U) People & Telephone Search: Free websites that expose your home information.

(U) Public Data Brokers: Companies that sell your data for public use.

(U) Non-Public Data Brokers: Companies that sell your data for private use.

(U) Data Marketers: Companies that collect and sell your interests for targeted marketing.

(U) Ancestry Records: Services that display family information provided by users.

Again, perform detailed searches to determine what information is out there. To get a complete picture, conduct searches using different web browsers: Google, Bing, Yandex, Yahoo, etc.

(U) It is suggested you search using some of the most common search helpers (Booleans) like the examples below:

1. Use quotes to search for an exact phrase
   a. “Virginia State Police”
   b. “Trooper John Smith”
2. Use OR to search multiple terms
   a. “John Smith” OR “Johnny Smith” OR “Jonathan Smith”
   b. “Virginia officer” OR “Virginia police” OR “Virginia Trooper”
3. Use AND & NOT to narrow results
   a. “John Smith” AND “Virginia” (Will only give results for John Smith in Virginia)
   b. “John Smith” NOT “Florida” (Will eliminate results for John Smith in Florida)
4. Use SITE to see only results from a particular website
   a. Site:Facebook.com “John Smith”
   b. Site:Linkedin.com “John Ernest Smith”

(U) In addition, ask yourself the following questions:

1. (U) What professional and personal associations/organizations are you a member of and what methods of communication do you use when participating? (i.e. churches, civic organizations, homeowners organizations, work related organizations)? Have any of these organizations published any of your contact or personal information?

____

____

2. (U) What associations and affiliations do your family members and associates have? (i.e. schools, hobbies, churches, civic organizations)? Have these organizations published any personal or contact information for you or your family members?

____

____

3. (U) What online shopping places (i.e. Amazon, eBay, etc.), magazine/online subscriptions, and blogs have your personal information?

____

____

4. (U) What rewards programs/stores/memberships (gym, grocery, Costco/Kroger/Staples) currently have your personal information?

____

____

5. (U) What hobbies do you have? Do you participate in organizations related to these hobbies? Have these organizations published any information about you or your family?

____

____

(U) CAUTION

(U) Individuals should be aware that providing personal information to various organizations allows these organizations to post, sell, or include your data in newsletters, flyers, websites, rosters, etc. Individuals should identify who they have given their personal information to and attempt to remove any public references to themselves or their occupation.

(U) Additional help in conducting a complete digital self-assessment can be found at https://inteltechniques.com/menu.html. This website is maintained by Michael Bazzell, an expert on privacy and digital security. Bazzell spent 18 years as a government computer crime investigator. During the majority of that time, he was assigned to the Federal Bureau of Investigation’s (FBI) Cyber Crimes Task Force.

(U) Navigate to the site: https://inteltechniques.com/menu.html
-On the menu bar, select Tools
-Select OSINT links
(U) Perform self-searches using the various links.

(U) The Search Engines, Social Network & Forums, People Search Engines, and Public Records searches will be especially helpful in getting a complete picture of your online presence. Be sure to document your findings for removal purposes.

(U) Removing Data from the Internet

(U) After you have completed your digital footprint assessment and identified where your information resides, begin having your personal data removed or hidden. Although tedious, privacy can only be achieved by requesting data removal directly from the source of information. The below guidelines will assist you in that effort:

1. (U) Utilize Michael Bazzell's workbook "Hiding from the Internet" to opt out of online databases.
   a. Create a separate email account for this purpose. A free account can be created at Googe.com, GMX.com, or Protonmail.com.

2. (U) Make use of the tools found on https://inteltechniques.com and https://privacy-training.com.

3. (U) Ask professional / civic organizations to remove any information regarding your employment affiliation and personal information from their websites.

4. (U) If you find a page in a Google search result that displays personal information about you, such as your social security or credit card number, you can request immediate removal. Google will review your request and remove the information from their search results. This will not remove the information from the website that is displaying it, but it will take the link off of Google to make it more difficult to find. If any of the following three (3) scenarios occur, Google will usually comply with your request:

   If your *social security number* is visible, contact Google at: https://support.google.com/websearch/contact/government_number

   If your *bank account* or *credit card* number is visible, contact Google at, https://support.google.com/websearch/contact/bank_number

   If an image of your *handwritten signature* is visible, contact Google at, https://support.google.com/websearch/contact/image_of_handwritten_signature

5. (U) Is your private residence or business visible in Google Maps or Bing Maps? If so, you can have the images blurred. Simply type in your address, switch to street view, and the option to "report a problem" will appear at the bottom of your screen.

(U) CAUTION

(U) Unfortunately, sources differ in the ways in which you make the request and the ways in which they will honor the request.

(U) If you are unsuccessful after initially making a request for information removal, send the following by email or in writing:

> *"I have been unsuccessful in removing my personal information from your website. Per the information contained in your legal privacy policy, please remove the following details from your service".*
> *Name:* (State the name exactly how it appears on the source)
> *Address:* (State the address exactly how it appears on the source)*
> *Telephone number:* (Only if it appears on the source)**
> *Email address:* (Only if it appears on the source)**

* (U) If the source has a previous address listed, do not supply them with your current address.
** (U) If the source does not have your telephone number or email on file, do not supply them.

(U) There are some sources of data that are typically more difficult to have your information removed from. But, due to the dangerous nature of their work, members of the law enforcement community and other first responders may get special consideration when it comes to removing or hiding data. This is especially true for data held by non-public data brokers. To these sources, consider sending a written request on department letterhead* with the following:

> *"I am a full-time sworn law enforcement officer in the state of Virginia that is actively conducting investigations of violent subjects. This assignment has put me in immediate danger of physical harm. The attached letter from my supervisor confirms my position and assignment."*

> "*I am a member of the first responder community in the state of Virginia; the nature of my work often exposes me to violent subjects or situations. This assignment has put me in immediate danger of physical harm. The attached letter from my supervisor confirms my employment."*

(U) Always adhere to department policy concerning the use of department letterhead.

(U) Minimizing Internet Footprint

(U) Now that you have gone through the effort of having your data removed from the internet, you should form new habits that will assist you in limiting your digital footprint going forward. This will require you to check your online account settings for social media, web browsers, and other digital devices. You will need to routinely perform self-searches and exercise caution when sharing your information.

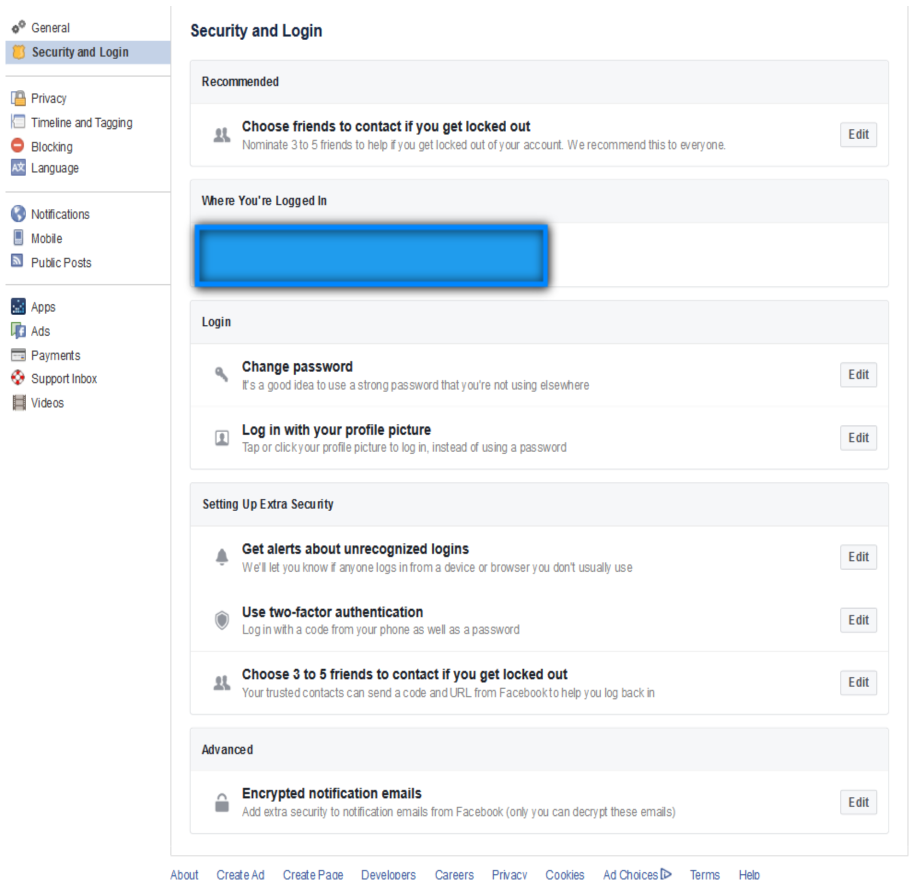
(U) In addition, you should consider creating alternate email accounts to use for non-personal business. Free accounts can be made at Google, GMX.com, or Protonmail.com. Try to create an extra layer of privacy by using one account for rewards programs, one for online shopping, and one for personal communications. Remember that you are not required to provide detailed information when opening an account.

(U) **Securing Your Social Media Accounts**

(U) Facebook:

(U) Facebook can be a great way to keep in touch with your family and friends. Unfortunately, you may also be giving access to more of your personal information than you realize. Below are some screen shots and security recommendations for maintaining the security of your Facebook account from outside, prying eyes.

> **(U) CAUTION**
>
> (U) Without notification, Facebook changes their setting configurations. You cannot adjust your settings and expect things to stay that way. It is extremely important to routinely check your settings.



Security and Login

Recommended

Choose friends to contact if you get locked out — Edit
Nominate 3 to 5 friends to help if you get locked out of your account. We recommend this to everyone.

Where You're Logged In

[redacted]

Login

Change password — Edit
It's a good idea to use a strong password that you're not using elsewhere

Log in with your profile picture — Edit
Tap or click your profile picture to log in, instead of using a password

Setting Up Extra Security

Get alerts about unrecognized logins — Edit
We'll let you know if anyone logs in from a device or browser you don't usually use

Use two-factor authentication — Edit
Log in with a code from your phone as well as a password

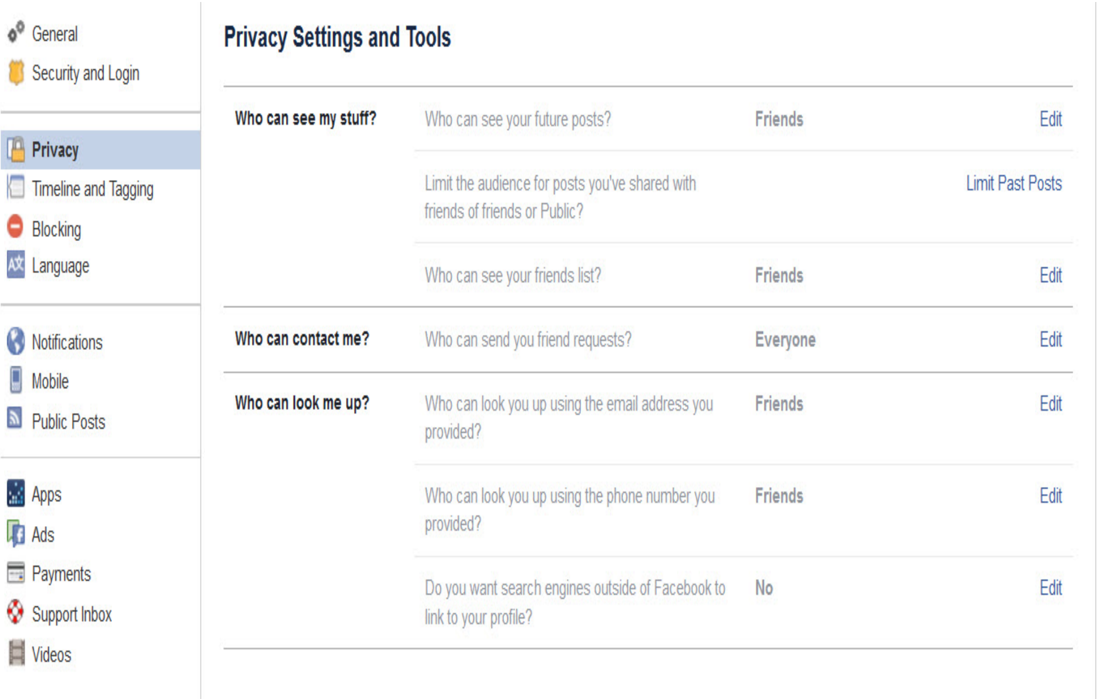
Choose 3 to 5 friends to contact if you get locked out — Edit
Your trusted contacts can send a code and URL from Facebook to help you log back in

Advanced

Encrypted notification emails — Edit
Add extra security to notification emails from Facebook (only you can decrypt these emails)

(U) Security and Login

(U) It is important to make sure your password is strong. The stronger your password, the harder it will be for your Facebook (and any other accounts) to be compromised by unauthorized access. Consider testing your password of choice at: howsecureismypassword.com. This is a great tool that will show you approximately how long it would take someone to crack your password. Two-factor authentication is also an excellent feature that will enhance the security of your account; however, we do not recommend using your real phone number as the second form of authentication.

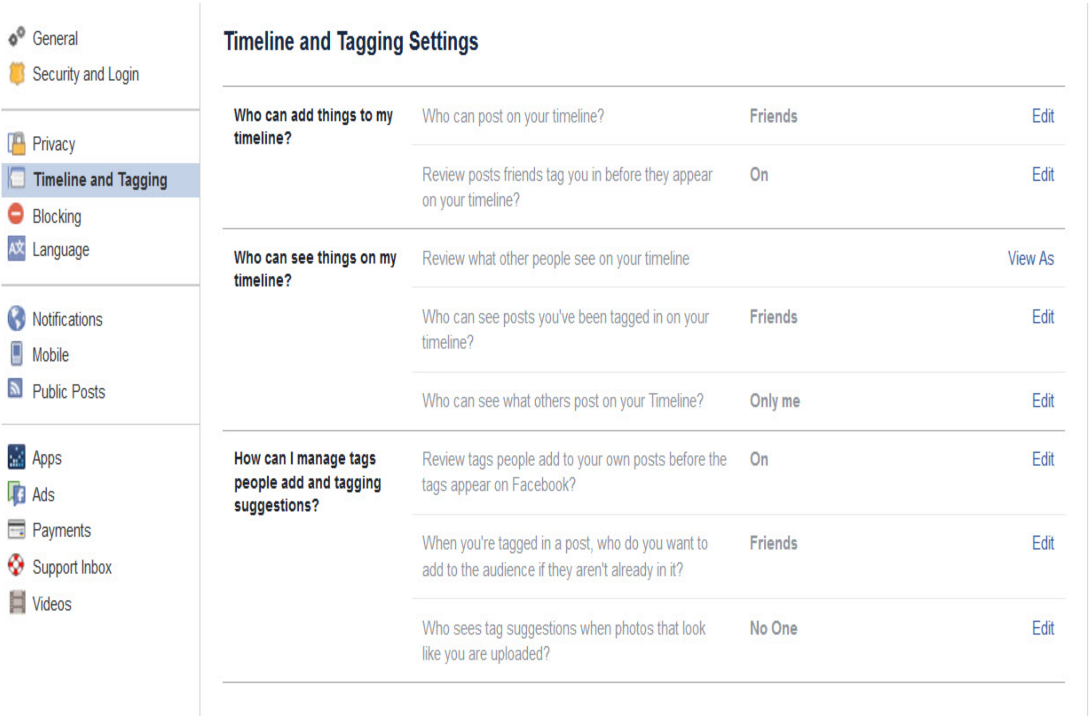


Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	Who can see your friends list?	Friends	Edit
Who can contact me?	Who can send you friend requests?	Everyone	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

(U) Privacy

(U) Facebook allows you control of who can see your information, who can contact you, and who can look you up. Be sure to choose wisely.

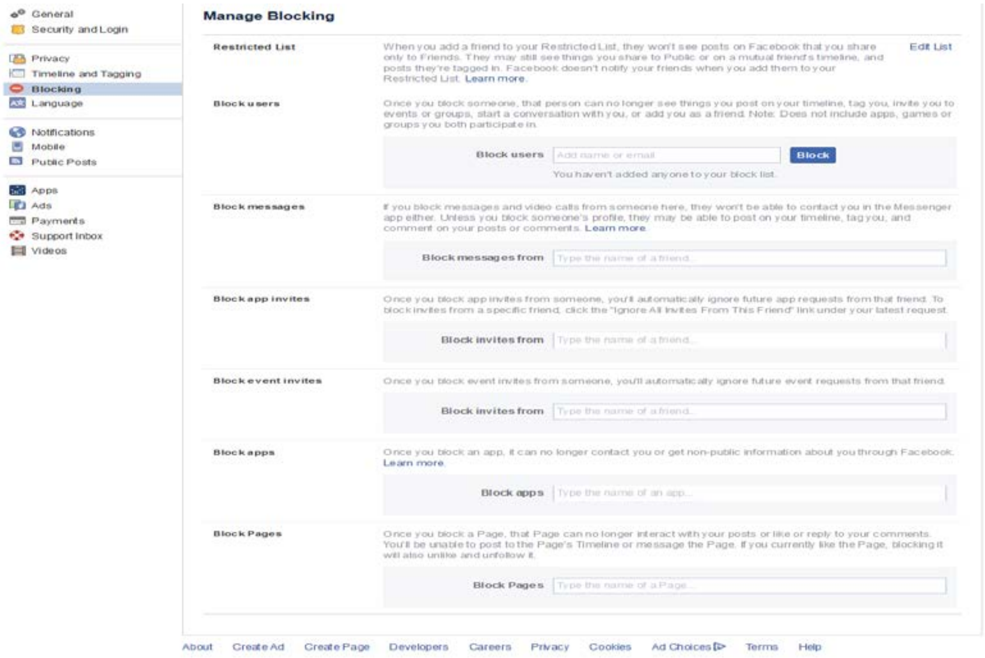


Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Friends	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Friends	Edit
	Who can see what others post on your Timeline?	Only me	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded?	No One	Edit

(U) Timeline and Tagging

(U) These options permit you to select who can add things to your timeline and who can tag you in their timeline. Requiring a review before people are allowed to post things about you is a safer option.



Manage Blocking

Restricted List When you add a friend to your Restricted List, they won't see posts on Facebook that you share only to Friends. They may still see things you share to Public or on a mutual friend's timeline, and posts they're tagged in. Facebook doesn't notify your friends when you add them to your Restricted List. Learn more. Edit List

Block users Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.

Block users: Add name or email

You haven't added anyone to your block list.

Block messages If you block messages and video calls from someone here, they won't be able to contact you in the Messenger app either. Unless you block someone's profile, they may be able to post on your timeline, tag you, and comment on your posts or comments. Learn more.

Block messages from: Type the name of a friend...

Block app invites Once you block app invites from someone, you'll automatically ignore future app requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request.

Block invites from: Type the name of a friend...

Block event invites Once you block event invites from someone, you'll automatically ignore future event requests from that friend.

Block invites from: Type the name of a friend...

Block apps Once you block an app, it can no longer contact you or get non-public information about you through Facebook. Learn more.

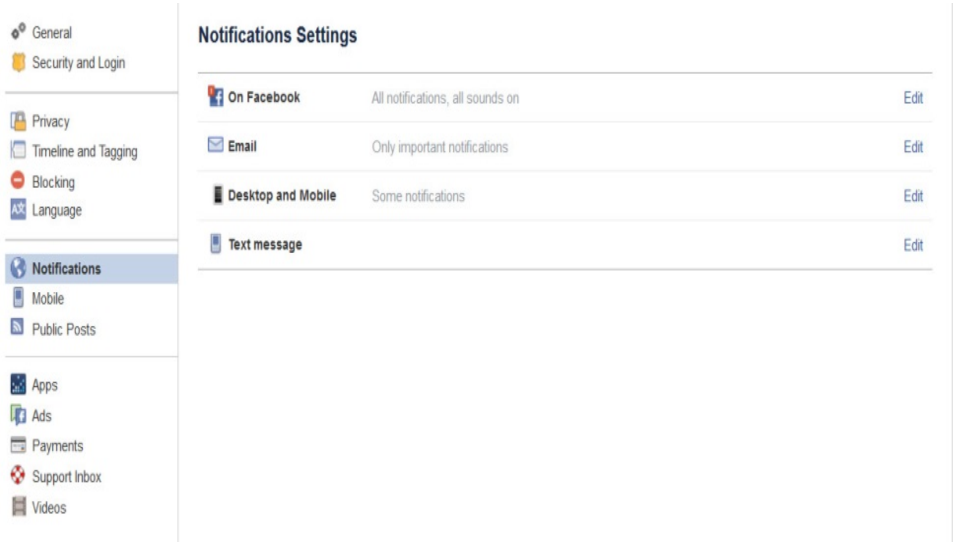
Block apps: Type the name of an app...

Block Pages Once you block a Page, that Page can no longer interact with your posts or like or reply to your comments. You'll be unable to post to the Page's Timeline or message the Page. If you currently like the Page, blocking it will also unlike and unfollow it.

Block Pages: Type the name of a Page...

(U) Blocking

(U) This setting allows you the ability to block users, messages, invites, event invites, apps, and pages. This is a great feature and should be considered for a safer experience.

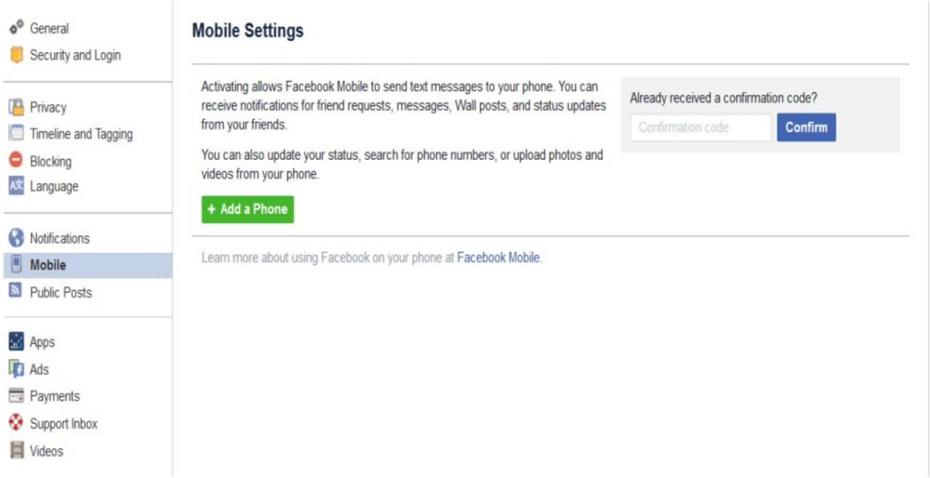


Notifications Settings

On Facebook	All notifications, all sounds on	Edit
Email	Only important notifications	Edit
Desktop and Mobile	Some notifications	Edit
Text message		Edit

(U) Notifications

(U) These settings are dependent on your personal preference, but should be checked to ensure you are only getting what you want.



Mobile Settings

Activating allows Facebook Mobile to send text messages to your phone. You can receive notifications for friend requests, messages, Wall posts, and status updates from your friends.

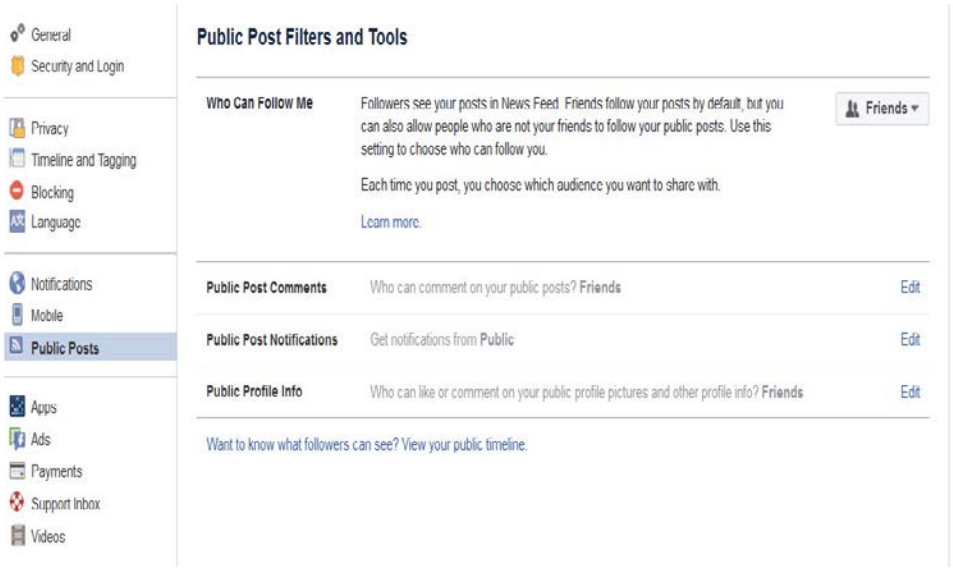
You can also update your status, search for phone numbers, or upload photos and videos from your phone.

Already received a confirmation code? Confirmation code

Learn more about using Facebook on your phone at Facebook Mobile.

(U) Mobile

(U) Adding your mobile telephone is not recommended.



Public Post Filters and Tools

Who Can Follow Me Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you.

Each time you post, you choose which audience you want to share with.

Learn more.

Public Post Comments Who can comment on your public posts? **Friends**

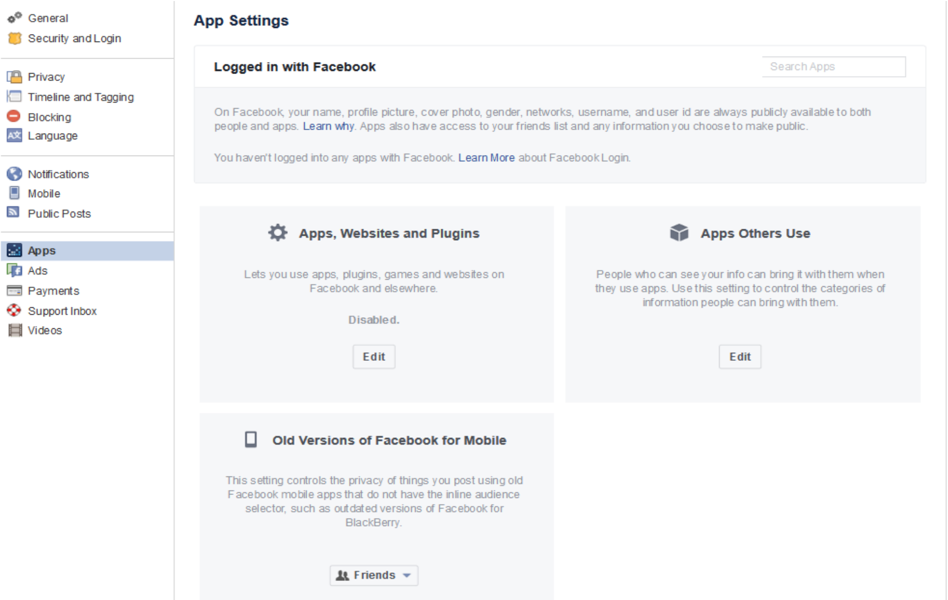
Public Post Notifications Get notifications from **Public**

Public Profile Info Who can like or comment on your public profile pictures and other profile info? **Friends**

Want to know what followers can see? View your public timeline.

(U) Public Posts

(U) Allowing your Facebook profile to be public is not recommended.



App Settings

Logged in with Facebook

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available to both people and apps. Learn why. Apps also have access to your friends list and any information you choose to make public.

You haven't logged into any apps with Facebook. Learn More about Facebook Login.

Apps, Websites and Plugins

Lets you use apps, plugins, games and websites on Facebook and elsewhere.

Disabled.

Apps Others Use

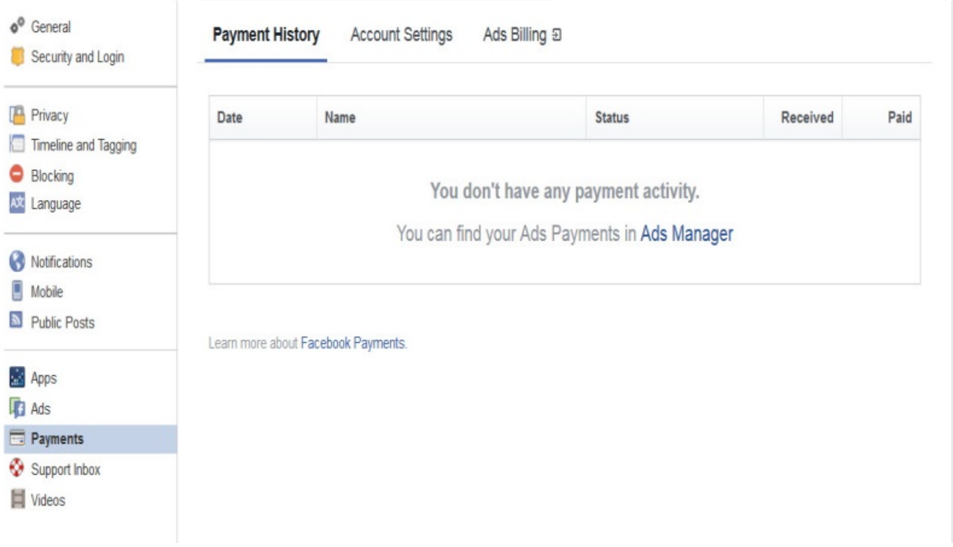
People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.

Old Versions of Facebook for Mobile

This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.

(U) Apps

(U) In order to maintain the security of the personal information you store on Facebook, it is important to disable the ability for Facebook to connect to other third-party sites and applications.



Date	Name	Status	Received	Paid

You don't have any payment activity.

You can find your Ads Payments in Ads Manager

Learn more about Facebook Payments.

(U) Payments

(U) Having personal credit/debit cards associated with Facebook is not recommended; however, the use of gift cards is acceptable as they cannot be connected to your personal information.

(U) Twitter:

1. (U) Change account settings to “require personal information to reset my password”.
2. (U) Utilize two-factor authentication by “checking verify login requests”.
3. (U) Check the option to protect your Tweets.

(U) LinkedIn:

(U) LinkedIn has robust security settings that need to be adjusted if you want your information to only be accessible to those you approve and not to the public. It is recommended that you visit your account settings and check them in detail, but below are a few suggestions:

1. (U) Visit the “Profile Settings” section under your account settings and control what parts of your profile are accessible to the public through public searches.
2. (U) Any actions you take in LinkedIn such as updating your experience, interacting with groups, or adding new connections can be seen by those you are connected to. Consider making your LinkedIn activity updates private.
3. (U) Keep in mind which apps you allow access to your LinkedIn profile and update settings where you deem necessary. It is usually recommended to turn off data sharing with third-party apps.
4. (U) As always, use a strong password to protect your account.

(U) Instagram:

(U) Instagram accounts can be set to private. This will prevent people you do not know from automatically following you through your account. In order for someone to follow you, they will need to send you an approval request. Be conscious of who you grant approval to. Again, use a strong password to protect your account.

(U) Securing Networks & Devices

(U) Windows Devices: *Be aware that Windows devices often "call home" to Microsoft and share your habits and computer data. There are certain settings you can make within the system to mitigate this.*

(U) Recommended Configurations

(U) (Windows 10, Windows 8)

1. Use Windows Defender (START) (SETTINGS)(UPDATE & SECURITY)(WINDOWS DEFENDER)
    a. Settings:
        i. Turn Real Time Protection On
        ii. Turn Cloud-based protection Off
        iii. Automatic Sample Submission Off
2. Firewall (SETTINGS)(SEARCH) Enter "Firewall"
    a. Settings:
        i. Check firewall status and ensure it is green
        ii. Firewall should be on for both public and private networks
3. Updates (SETTINGS)(UPDATES & SECURITY)(WINDOW UPDATES)
    a. Settings:
        i. Navigate to settings
        ii. Select Update security
        iii. Windows update
        iv. Turn on: " Available updates will install automatically"
4. Privacy (SETTINGS)(PRIVACY)(GENERAL)

    Consider selecting OFF for the following:

    a. Let apps use my advertising ID for experiences
    b. Turn on smart screen filter to check web content (URLs)
    c. Send Microsoft information about how I write to improve
    d. Let websites provide locally relevant content by language list
    e. Bluetooth (make sure off is selected until it is needed, then turn on)
    f. Let apps use my advertising ID for experiences (make sure off is selected)
    g. Turn on smart screen filter to check web content (URLs)
    h. Send Microsoft information about how I write to improve
    i. Let websites provide locally relevant content by language
    j. Location for this device
    k. Camera
    l. Microphone
    m. "Get to Know Me"
    n. Use autoplay for all media and devices

    o. Bluetooth (Select off until it is needed)

5. Additional setting considerations:
    a. Change option to enable showing hidden files or drives
    b. Uncheck “hide extensions for known file types”

(U) (Windows 7) The same settings are available as in Windows10 & Windows8

1. Install Microsoft Security Essentials.
2. Firewall (START) (CONTROL PANEL)(SYSTEM & SECURITY)(ACTION CENTER)(SECURITY)
3. Updates (START) (CONTROL PANEL)(SYSTEM & SECURITY)(ACTION CENTER)(SECURITY)
4. Privacy (START) (CONTROL PANEL)(NETWORK & INTERNET)(INTERNET OPTIONS)(PRIVACY)

(U) Internet of Things (IoT)

(U) The digital world is changing at an unprecedented rate. Consumers are purchasing vehicles that can park themselves, home controls that allow users to remotely turn their lights on and off, and refrigerators with televisions. With these added conveniences comes opportunity for exploitation. Be aware of the devices you are using and know exactly what they are capable of. Below are a sampling of specific devices and their possible hazards:

Nest Thermostat:

This device is aware of when you are home or away based on embedded sensors. (Forbes)

Alexa:

The microphone is always turned on; consider unplugging Alexa when it is not in use. (Naked Security)

PS3:

Capable of internet connectivity
A social network platform with many different community groups
Easy to employ anonymization, hiding one's identity
The microphone and camera have the potential of always being turned on
Easy to target children.

Visio Smart TV:

Capable of internet connectivity and the microphone has the potential of always being turned on and listening. (CNET)

(U) CAUTION

(U) When digital devices are purchased, they are automatically configured with default passwords. These passwords are typically not very strong and are easy to guess. These default passwords should be changed to something stronger immediately. It is also a good practice to use a different password for each device.

Test the strength of your password at: *howsecureismypassword.com*

(U) Fortunately, many resources are available that offer recommendations and instructions for the safe use of these appliances. Find additional information at:

https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips

https://www.symantec.com/solutions/internet-of-things https://www.networkworld.com/.../internet-of-things/how-to-improve-iot-security.htm

https://www.gao.gov/products/GAO-17-668

(U) For home wireless networks:

https://heimdalsecurity.com/blog/home-wireless-network-security/

(U) **Conclusion**

(U) The information available online is staggering. In a perfect world, maintaining privacy would not be necessary, unfortunately we do not live in a perfect world. Individuals must take control of their data to the extent they are able. The first step is discovering exactly what the internet says about you. You cannot begin to fix the problem without knowing the extent of the problem. If you are not happy with what you find, begin the process of having the data removed.

(U) But simply removing the data is not enough; this is not a one-time exercise. To maintain online privacy, you will have to put effort into it. You will need to change your habits, think more about information you share, examine your various security settings, and develop a plan for continuous monitoring. Electronic devices and the internet are not going away, but we do have some control over how we are affected by them.

Sources

Although other sourcing was used, the information contained in this product was primarily derived from the works of Michael Bazzell through his book: "*The Complete Privacy & Security Desk Reference"*, his websites: inteltechniques.com and privacy-training.com, and his online courses.

Bazzell, M., & Carroll, J. (2016).*The Complete Privacy & Security*: Desk Reference., Vol. One: LEIU / IALEIA Edition.

CNET. *How to make sure your Vizio smart TV isn't spying on you*. Retrieved November 3, 2017 from: https://www.cnet.com/how-to/disable-vizio-smart-tv-spying.

FORBES. *How hackers could use a Nest thermostat as an entry point into your home*. Retrieved October 26, 2017 from: https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#73b62c843986.

Google Support (2017). *My bank number appears in the search results - Google Search Help*. Retrieved November 2, 2017 from: https://support.google.com/websearch/contact/bank_number.

Google Support (2017). *My handwritten signature appears in the search results - Google Search Help*. Retrieved November 2, 2017 from: https://support.google.com/websearch/contact/image_of_handwritten_signature.

Google Support (2017). *My social security or government ID number appears in the search results - Google Search Help*. Retrieved November 2, 2017 from: https://support.google.com/websearch/contact/government_number.

OSINT Training by Michael Bazzell | *Open Source Intelligence Techniques*. Retrieved October 30, 2017 from: http://inteltechniques.com.

Privacy & Digital Security by Michael Bazzell: *Online & Privacy Training Courses*. Retrieved October 30, 2017 from: https://privacy-training.com.

SOPHOS: *Know the risks of Amazon Alexa and Google Home*. Retrieved November 3, 2017 from: https://nakedsecurity.sophos.com/2017/01/27/data-privacy-day-know-the-risks-of-amazon-alexa-and-google-home.