Signal

Safeguarding Your Online Identity

Operational Security and Privacy in the Age of Social Media

Contents

Disclaimer - This non-exhaustive document provides guidance and suggestions based on common operational security best practice online. This guide heavily relies on the readers abilities to self-assess exposures and implement the recommended security measures. As such, Signal Corporation takes no responsibility for the readers self-assessment of their vulnerabilities or implementation of the recommendations displayed in this educational document.

Safeguarding your Online Identity

This guide identifies common online vulnerabilities that can be exploited by a threat actor to reveal your personal information and presents a series of recommendations to mitigate them.

Introduction

In the age of social media, it is increasingly difficult to exist without a digital footprint - having an online presence is a social and often professional expectation or necessity. However, the information exposed by your online presence can present a critical vulnerability that a threat actor could exploit to learn your personal information and target you, resulting in harassment, social engineering attacks, doxing, physical intimidation, or even outright violence.

The following document is designed to educate the reader on the most common vulnerabilities that can be exploited to discover your personal information through publicly available information and open-source research techniques. This document also provides recommendations on how to mitigate these vulnerabilities and reduce the exposure of your personal information online.

These methods are designed to limit and deny a potential threat actor the ability to assess and exploit your exposed personal information and the vulnerabilities created by your online footprint. Implementing the recommendations will make your online presence harder to find, more difficult to verify, and minimize the value of any personal information that can be gleaned.

There is no “one size fits all” approach to online operational security (OPSEC) – the precautions you take should be in line with your own personal risk profile and tolerances. Not everyone needs to ‘disappear’ from online life, for most people it is enough to take some basic precautionary measures to ensure that you are maintaining a reasonable level of OPSEC.

Reading this guide, it is easy to become paranoid – that is not the purpose of this guide. Always remember that even for those with a high-risk profile, it is unlikely that you will ever be targeted by a threat actor. However, by the time you realise that you need good OPSEC, it is usually too late. As such, it is easier to proactively develop and practice good security habits ‘in case’, than it is to gamble and hope for the best.

If you struggle to understand how some seemingly minor pieces of personal information can be a security risk, remember that critical vulnerabilities are less about individual pieces of information being exposed, and more about the bigger picture that the individual pieces of information make.

Executive Summary

For those pressed for time, this page will highlight the key online vulnerabilities that can exploited by threat actors and provide a few simplified recommendations to mitigate them.

Please note that this summary is not exhaustive - if you are interested in improving your operational security or have a high threat profile, we strongly recommend working through the entire guide.

Common Vulnerabilities and Sources of Exposure

- Images and posts that can be used to infer personal information or patterns of life (i.e., frequently visited locations, daily schedule, and accessibility)
- Tags, interactions, images, and comments by friends/family.
- Content that you follow or interact with that suggests a connection.
- Obvious or repeated usernames.
- Person data aggregators.
- Publicly accessible files.
- Data breaches.

Quick Recommendations

- Review and tighten the privacy settings on all your online accounts.
- Be mindful of what personal information is revealed by the content and media you post online.
- Never publicly advertise (via geo-tag, interaction, post, photo, or video) your live location or intent to attend a location.
- Avoid posting information that can be used to infer your schedule/accessibility.
- Avoid posting identifiable photos of locations that you frequent (i.e., your residence)
- Make it difficult for people to identify your social media profile.
- Consider utilizing profile pictures and cover photos that are difficult to clearly identify as you (i.e., silhouetted photos) or simply leaving them blank.
- Consider utilizing a pseudonym or slightly altered/misspelt version of your name.
- Remember that you do not need to fill out all biographic 'about me' details on social media, leave your city of residence blank, and consider deleting information that is unnecessary.
- Do not reuse passwords and change them frequently.
- Talk to those close to you, educate them on operational security, and ask them to be mindful of what information they share online.

Recommendations

Usernames and Profile URL’s

Vulnerability: Utilising the same username (or obvious variants) across multiple platforms allows a threat actor to easily identify your online profiles. Script based username enumeration tools are free and commonly used within the OSINT community, allowing a threat actor to easily search across hundreds/thousands of websites for any accounts or URLS featuring a specific username. This is a particularly critical vulnerability for individuals that have a unique and/or easily identifiable name.

Self-assessment: Try searching for your own usernames and handles on WhatsMyName to get an idea of how username enumeration techniques work.

Please note that WhatsMyName is an imperfect username enumeration tool (particularly on mainstream social media platforms) – much more powerful script-based versions exist and are commonly used by moderately technically proficient threat actors alongside manual search techniques. Just because nothing was returned by WhatsMyName, does not mean a similar tool wouldn’t be able to find your profile.

Fix:

- Avoid utilising your full real name on online accounts where possible. Instead consider utilising a pseudonym or just going by your first name on social media profiles.
- Alternatively, purposefully misspelling your first or last name when selecting a username is a great way to add an obstacle to identification and username enumeration techniques.
- Avoid utilising the same username (or obvious variants) across multiple platforms.
- It is also best to avoid the most commonly used username/email formats and variations (i.e., John Smith, JohnSmith, John.Smith, John-Smith, John_Smith, JohnS, JSmith, John1990, JMSmith).
- Some platforms (i.e., Facebook and Linkedin) allow users to customise your profile URL. We recommend editing the default URL to add randomised characters, a pseudonym, or a misspelt version of your name. This technique provides the best defence against username enumeration discovery methods.

Privacy Settings

Vulnerability: Social media platforms often make it difficult to make your profile’s ‘private’. Securing your profiles often require selecting dozens of different sub-options across several different tabs and settings. As such, many people have a false sense of security thinking that they have secured their profile, whilst having left several key data-points exposed.

Fix:

- Review the privacy settings and similar menus (i.e., accessibility/audience/security) on all your online profiles and ensure that you max out all relevant privacy options. For example,
    - Hide your friends/followers list.
    - Hide the accounts/pages that you follow.
    - Hide mandatory biographical details (i.e., DOB) from public view.
    - Hide your public comments/replies.

    - Restrict the audience of your posts/content/interactions.
    - Restrict the audience of profile picture/cover photo to just friends.
    - Don't allow search engines to link your profile.
    - Don't allow users to look up your profile by phone number or email address.
    - Restrict other users' ability to tag you in content.

- Having a secured 'private' profile is all and well, however, your security is only as strong as those you allow in. Your friends and followers will still see everything you post, so we recommend reviewing your friend's/followers list and removing people as needed (especially those that you don't know).

- Remember that having a 'private' profile does not mean you should no longer implement good security practices. The rest of the information in this document remains highly important.

Public Profile Details

Vulnerability: Profile pictures, cover photos, personal biographies, and associated locations are all common features of most social media accounts. But, depending on the platform, these details are often still publicly accessible even when your profile is "private". As such, be mindful of what information may be publicly revealed by these details to a potential threat actor.

Self-assessment:

Firstly, log out of your social media (or utilise a different browser) and try searching for and viewing your social media profiles. Can they be accessed without logging into the site?

Secondly, try viewing your profile with a secondary account (that isn't friends/following you). What information is publicly viewable? To achieve this, you can easily buy a cheap/disposable SIM card to make a secondary 'burner' account with which to view your primary account. Alternatively, simply ask someone you trust (that you aren't friends on social media with, i.e., a co-worker) to quickly look at your social media profiles for you.

Consider the following questions – Can your profile easily be identified as you? Does it publicly reveal what city you live in? Who is pictured/tagged in your profile picture/cover photo? Do the images easily reveal your partner, children, or close friends? Do the comments or interactions on your profile/cover photo's reveal any critical personal details or relationships?

Fix:

- Not all information in the 'biography/about sections' needs to be filled out. Consider what fields are necessary and what you can simply delete/leave blank.
- Don't list what city you live in on your social media profile (or inadvertently indicate it via listing your employment or education institution)
- If possible, consider not having a profile picture or cover photo at all. Alternatively, consider utilising vague photos that are difficult to attribute/identify (i.e., A photo of you from behind, silhouetted at a random location).
- Avoid featuring or tagging your partner, children, friends, or family in profiles pictures and cover photos.

Media – Images & Video

Vulnerability: Most people do not consider how much information is revealed to an astute observer in the media that they post. For example, a simple selfie taken on your apartment's balcony could be used to verify and geo-locate your home address or a crumpled uniform on the bathroom floor may reveal your job or children's school. Being conscious of what is displayed (especially in the background) of your media is of key importance to securing your privacy.

Self-assessment: This vulnerability is difficult to self-assess due to personal bias but consider reviewing the media you have posted online for potential vulnerabilities. Make the media full screen and pay close attention to what is in the background, what information does this media give away?

Ask yourself whether someone could identify this location? Are there clearly recognisable landmarks, geographic features, shops, or streets signs in this picture? Could the information in this photo be combined with other pieces of exposed information to reveal something critical?

Remember, even if parts of an image may look blurry or hard to make out, a threat actor can utilise image manipulation techniques to enhance, reverse, or alter the colouration to clear things up.

Fix:

- It is best practice to not to post media at or of places that you frequent (i.e., your residence).
- Be mindful of what is captured in your media and displayed in the background.
- Delete any media that present a vulnerability.

Scheduling/Attendance

Vulnerability: From registering as 'going' to a large public Facebook event, through to your partner making a post about how they can't wait to go to a concert with you later that evening. From those gym selfies on Instagram about being on the 6 am grind, or that Tweet complaining about the constant traffic at a specific intersection you pass on your way home from work. Posts and interactions on social media can reveal or infer significant details about your schedule or intent to attend a location, that can in turn be used to establish "pattern of life" and assess your accessibility by a potential threat actor.

Self-assessment: As above, review the content on your online profiles.

Ask yourself: What do my posts say about my schedule and accessibility? Have I ever advertised my live location? Have I ever publicly announced my intent to be in a specific location?

Fix:

- Never share your live location in a social media post, especially while you are in a static location. If you want to make the post, rather save the photo, and post it after you have left the location.
- Don't publicly advertise your intent to attend a specific event or location online.
- Don't share information that reveals details about your routine.

Data Breaches and Passwords

Vulnerability: Email address and passwords are frequently exposed within data breaches online, potentially providing a threat actor with access to your online profiles and email accounts. This is a particularly critical vulnerability for individuals that regularly reuse the same password.

Self-assessment: Check whether your information has been exposed within a data breach.

To check, input your email addresses into the following sites:

- Have I been Pwned?
- Breach Directory
- Leak Peak

Fix:

- If your details have been exposed within a data breach, ensure that your password has since been changed and that you do not reuse that password (or any other obvious variants).
- It is recommended that you utilise a free service such as HaveIBeenPwned to subscribe to notification's alerting you to the next time your email address is included in a data breach.
- As a rule, avoid reusing the same password across different sites and regularly change your password. We recommend utilising a randomly generated passphrase and a password manager such as 1password to securely and practically store all your passwords.
- Lastly, make sure two factor authentication is activated on all your accounts, providing a final barrier to hostile account takeover.

Person Data Aggregators

Vulnerabilities:

Data aggregators are ubiquitous - collecting, buying, trading, and selling your personal data. Personal profiles containing an individual's name, residential address, phone number, email address, social media profiles, employment history, and many other details are aggregated and presented as a service for free/paid users (depending on the aggregator).

This is a particular vulnerability for people in the United States where there is a high concentration of data aggregators and weak privacy legislation surrounding personal information.

Self-assessment: To check your own exposure, try searching for yourself across the following websites. Please note that some of these websites are US centric and may not cover other localities.

Fix:

Utilise opt-out forms to have your personal information removed from the following major person data aggregation sites; PIPL, Spokeo, Radaris, Signalhire, PeopleDataLabs, PeekYou, IDCrawl, BeenVerified, Acxiom, PimEyes,

Review these sites periodically to ensure that your details haven't been reuploaded.

For a more comprehensive list of data aggregators and removal techniques, we recommend the following list compiled by Michael Bazzel.

Miscellaneous Search Engine Results

Vulnerability: Personal information is frequently exposed online even without your input.

For example, council permit requests, charity meeting minutes, club annual reports, media interviews, obituary listings, school yearbooks, crowdfunding sites, and sporting events are just a few of the common sources of exposed personal information we frequently encounter.

These are just a few examples of the numerous pieces of personal information that can be inadvertently exposed through no fault of your own. However, it is important to be aware of what information may be publicly available about you.

Self-assessment: Consider running the following Google searches and reviewing the results. Are any of them about you? Do any of them reveal any critical details? How can this information be used in conjunction with other exposed information to build a comprehensive picture of you as a person?

The list of searches below isn't exhaustive, but it does provide some of the advanced search engine techniques that a threat actor may try utilising. Feel free to try other combinations of queries as you search for information about yourself.

This template will utilise a fictional person, with a new search on each line. Simply substitute your own details and run the following example searches on both Google and Bing.

Details – Name: John Michael Smith. Email: johnsmith83@gmail.com. Associated Locations: 73 Smithers St. Northshore, Auckland,

Searches

- John Smith
- "John Smith"
- "John Michael Smith"
- ("John Smith" OR "John Michael Smith") AND (Auckland OR Northshore OR "73 Smithers")
- "johnsmith83@gmail.com"
- ("73 Smithers St" OR "73 Smithers Street")
- ("John Smith" OR "John Michael Smith") AND filetype:pdf
- ("John Smith" OR "John Michael Smith") AND filetype:doc
- ("John Smith" OR "John Michael Smith") AND Auckland filetype:pdf
- ("John Smith" OR "John Michael Smith") AND Auckland filetype:doc

Fix: Fixing website and search engine exposures can be difficulties with most of these issue only being able to be amended by reaching out to the original author, site admin, or search engine to have the result removed. Decide what information needs to be removed and request its removal.

This task is largely about being aware of what information is already available and exposed about you online and how it can be used in conjunction with other bits of information to build a cohesive picture of you.

Residence

Vulnerability: Photos and videos of your residence can provide a threat actor with an easy method to verify your residential address and conduct hostile reconnaissance (i.e., assessing its security and accessibility). Beyond content sourced from social media, the most common method of assessing a location involves viewing content on real-estate websites, Airbnb, and Google Street View.

This vulnerability is most relevant to individuals who either own a house or intend to stay at the same property for an extended period.

Real-estate sites often collate and publicly display property sales history, buyer/seller details, comprehensive video walk-throughs, image galleries, and in some cases even floor plans.

Like the media on real-estate websites, content on Google Street View can provide ample material to assess the security and accessibility of a property. Furthermore, street view can potentially reveal other details such as the colour and make of you or your family's car, which provides information that can later aid in identification.

Self-assessment:

- Google your residential address and review any relevant real-estate or Airbnb listings.
- Do the same with the aerial and street view media of your residence accessible on Google and Bing maps (ensuring to also look at historical images by selecting 'see more dates' while in street view mode.).
- Also search for your name/address in the White Pages to check if your residence/details is publicly listed.

Fix:

- If unwanted content is exposed on real estate sites, you may need to contact the relevant agent/website to have the content removed.
- If you are concerned by the content on Google Maps or have a high threat profile and need to maximise your defence against online hostile reconnaissance, you are able have your address blurred on mapping tools.

  1. Search up your address on Google Maps.
  2. Access and view your residence in 'street view' mode (by using the little yellow human icon) in the bottom right corner).
  3. Click 'report a problem' in the bottom right-hand corner.
  4. Tick 'request blurring' and select the reason as 'my home.'
  5. Provide additional details as needed, referencing being concerned about safety issues.

  The same process can then be repeated with Bing maps.

- If you are listed in the White Pages, you can opt-out and have the results removed here.
- If you advertise and rent your property out as an Airbnb, analyse the cost/benefit of doing so and consider how it may impact the properties security and potential accessibility.

Partners, Family, and Friends

Vulnerability: Once in the mindset, it's relatively easy to practice good operational security yourself, however, it is a lot more difficult to encourage your loved ones to also be mindful of what they share online. The greatest blind spot and weakness in an individual's OPSEC is usually those close to them.

For example, a child posting on social media about their football practice could result in a threat actor determining your accessibility to a reasonable level of confidence by determining the child's football team, their public set training schedule, and that a parent or guardian must be present at trainings.

This type of vulnerability is particularly salient to those individuals with a high-risk profile, that feel confident in their own operational security. It's all and well implementing all the techniques and practices discussed in this guide, but if a threat actor can simply look at your family's social media to reveal the desired information about you, then that is a significant vulnerability.

Self-assessment: By this stage you are aware of the most common vulnerabilities mentioned in this guide, we encourage you to now review the content on the profiles of those close to you with these vulnerabilities in mind. Take special notice of any posts, photos, and videos that mention, tag, or picture you.

What do these posts say about you? Has a friend posted your birthday cake tagging you, thus revealing a partial date of birth? Does the background of your child's Tik Tok dance montage inadvertently reveal the location of your house?

Also be aware, that those close to you (especially children) may have social media profiles you are not aware of. As such, educating them on the importance of good social media practice is vital.

Fix: Like everything in personal relationships, the best way to fix an issue is to talk honestly about it. Such a conversations may seem awkward and daunting, but in practice the conversation is relatively simple, and your loved ones will likely be understanding (in fact they may even appreciate you educating them on better personal online security).

If you are unable to disclose to them the nature of your work as an explainer or otherwise don't want to frighten your loved ones - it is usually enough to simply say, "I've been reading a few articles recently and I've been trying to get into some better privacy habits online, at some point would you have 5 minutes to have a chat and help me out?"

- Ask people to delete posts/images that reveal critical personal information about you.
- Ask people to refrain from publicly posting photos of you (or at least have them not tag you).
- Ask those closest to you to ensure their friend's lists are closed (especially if they also friend/follow your immediate family).
- In the future, consider changing your social media habits. Most interactions (i.e., liking a post) aren't 'needed'. Liking or commenting on public content provides an easy way to infer a link between you and another individual, it is better to limit this behaviour/practice if possible.

For more information, inquiries, or suggestions

support@signalpublicsafety.com