Tips For Successful Social Media Investigations

Brought to you by

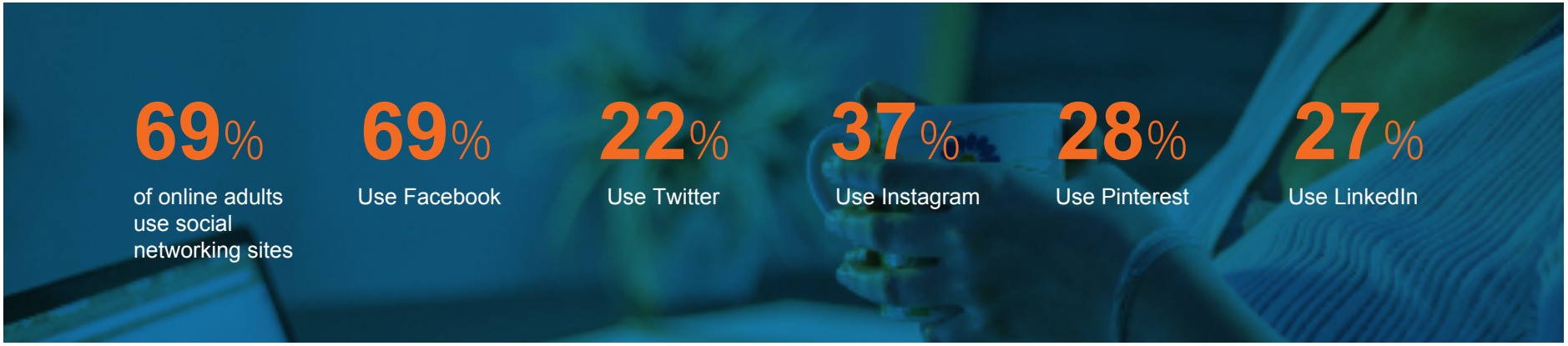
Case IQ

Contents

Tips on LinkedIn
See page 12

Introduction

Social media has become an integral part of everyday life for many North Americans. And it's not just teenagers who are signing in daily.



A small percentage of people enable maximum privacy settings on their social media accounts, creating a valuable repository of free information for investigators. By ignoring this rich resource investigators risk missing out on one of the most effective sources for gathering online intelligence and may miss critical evidence that can be used in an investigation.

This eBook outlines tactics for using social media to research subjects and gather evidence legally in the context of an investigation.

Preliminary Search

The first step in researching a subject online is to do a simple search using a search engine. The most common ones, Google, Bing and Yahoo, can provide a list of places, including social networks, where you can find more information about a person. You can also use more targeted search engines for social networks, such as Social Searcher, Pipl, Spokeo, Yasni and SocialSeeking.

The most effective searches are by:
Name
Nickname
Email address
Cell phone number

You can use Google's reverse image search to find places where a particular image has been used. It will reveal all the places where a photo has been posted on Facebook, Instagram or other social media networks and blogs.

When a preliminary search renders limited or no matches, it's time to dig in and search the networks one-by-one.

SEARCHING

Facebook

You will need an account

What you can find:

Even if you can't see someone's friends list, you may be able to see who has 'liked' their photos or posts, allowing you to view others in their network.

You may be able to see someone's political views, employer, family members, maiden name or nickname, causes they support, websites, groups they are part of, pages they like, birth date, anniversaries, education.

How to search:

You can search people by name and use filters to narrow the results. Type the name of the person you're trying to find in the search bar, then click "People" at the top to narrow your search to just individual profiles. You can also search by email address, but you will find only people whose personal information is public. You can search by URL using facebook.com/firstname.lastname or /firstname-lastname. If there are users with the same name, a number is assigned.

For accounts that are unsearchable, you can sometimes find people through the profiles of their family members and friends.

Privacy:

Privacy settings apply to each section of a Facebook profile. Some information may be public, while other sections may not be. Facebook won't display who is looking at your profile, but if you view someone's profile often enough, you may appear in their 'Discover People' suggestions.

Facebook's terms of service prohibit the creation of false profiles, however, many investigators set up one or two dummy Facebook accounts to use for investigations. Setting up a dummy email account will ensure that the Facebook accounts cannot be linked to you.

SEARCHING

Twitter

No account needed

What you can find:

You can see who a person is following and who is following them, their tweets and conversations. If other social media accounts are linked to the subject's Twitter account, photos, check-ins or Facebook statuses may also be visible on Twitter. This may help you find additional social media accounts for the person you are researching.

How to search:

Search by a person's name or Twitter handle. (A Twitter handle begins with @.)

You can also search with hashtags (#) to find content related to a topic or an event, as well as the people who are talking about those topics.

Privacy:

Most Twitter accounts are public, as Twitter is designed to be a public forum. Occasionally a subject may have set his or her account to private, meaning that you would need permission to see their information. Twitter users cannot see who has looked at their accounts.

SEARCHING

YouTube

No account needed

What you can find:

You can find videos posted on a subject or by a particular person and comments made about videos.

How to search:

YouTube is the second-largest search engine in the world and results can be voluminous. You can try searching by the person's name or by subject matter.

You can use advanced search operators to narrow results by type (videos, channels, playlists), subject category, video length, video quality or features. It's best if you know what you're looking for.

Privacy:

Users can set their accounts to private. Account holders cannot see who has looked at their accounts.

SEARCHING

Instagram

No account needed

What you can find:

You'll see photos, profile information if it's public, captions, hashtags and likes on photos and videos. Photos and hashtags can give clues about hobbies, friends, locations and affiliations.

How to search:

If you know the user name of the individual, type it in after the domain name (www.instagram.com/username). If you don't know the person's user name, try firstnamelastname.

The user name can sometimes be found on Facebook or Twitter. You can also use tools, such as Instagram for Chrome or Find-Gram to conduct more detailed searches.

Privacy:

Users can set their accounts to private. Account holders cannot see who has looked at their Instagram accounts.

SEARCHING

Pinterest

No account needed

What you can find:

Many people don’t restrict access to their Pinterest "boards" so this platform can give you some insight into who the person is and who is in their social circle. You can see who the subject follows and who follows them as well as their interests and hobbies.

In many cases, user accounts include links to their Facebook and Twitter accounts.

How to search:

If you know the user name of the individual, type it in after the domain name (www.pinterest.com/username). The user name can sometimes be pulled from Facebook or Twitter, as Pinterest uses the same user name depending on how the person set up the account.

Privacy:

Users can restrict access to their boards but not their Pinterest accounts. Users cannot see who has looked at their profiles.

SEARCHING

LinkedIn

You will need an account

What you can find:

You can see the subject's current employer and employment history, projects, groups, education and interests. To find out who is in the person's network, you can look at their connections, how they are connected to others, who they have recommended and who has recommended them.

How to search:

You can search users by name and use the advanced search to narrow down results by location, keywords, company, industry, schools, etc. Since LinkedIn is a site for professional networking, most people use their full name.

Privacy:

Most LinkedIn profiles are not protected. In your account settings, you can set your privacy controls and specify what others see when you've viewed their profile.

If you have a regular (free) account and want to remain anonymous when searching other profiles, you will not be able to see who has looked at your profile. Premium membership (paid) allows the account holder to see who has viewed their profile but remain anonymous, if desired. LinkedIn's Terms of Service prohibit the use of fake profiles and profile images.

Other Useful Networks

Flickr

Vine

Classmates.com

Imgur

For more search tips,
continue down.

Searching Anonymously

Investigators often need to keep their identities hidden while searching social media sites for information about the subjects in an investigation to avoid tipping off a suspect, jeopardizing the investigation or compromising the evidence. This can be a challenge.

Some social networks and online information sources either allow the subjects of searches to see who has been researching them, or provide clues that can identify the searcher. So, when anonymity is important, investigators need to take steps to keep their identities hidden.

Since the ability to search anonymously varies among social networks, it's important to know which ones reveal the searcher's identity and which don't. By setting your personal security settings to anonymous on LinkedIn, for example, your identity won't be revealed, even to those who have LinkedIn Premium (paid), although an account holder may receive some other clues about who has looked at their profile. See the privacy sections in the preceding pages to see which networks identify searchers.

Create a fake profile

Some investigators create alternate, unidentifiable account profiles on social media networks so that they can search anonymously. It's important to be aware that this is prohibited for some networks (such as Facebook), but not for others (such as Twitter). Check the terms of service for the social network before setting up a fake account.

If you do decide to set up a fake profile, be aware that you may not use someone else's photo or personal information to set up the account. It is illegal in some states to impersonate someone online, and certainly unethical.

For information on exceptions, see page 17.

Pretexting

Posing as a “friend” or creating a false profile to trick an account holder into granting access to private information on social media is known as “pretexting” and it can result in valuable evidence being disregarded. US bar associations have identified pretexting as unethical for both lawyers and investigators. But evidence acquired through pretexting is occasionally admissible.

Exceptions

In US civil litigation courts have ruled that “the admissibility of evidence is not affected by the means through which it was obtained,” the American Bar Association reports.

The National Association of Insurance Commissioners drafted legislation that would allow insurance fraud investigators to use pretexting tactics when “there is a reasonable basis for suspecting criminal activity.” The bill has been adopted by several states.

Legitimate Access to Private Accounts

If an investigator openly adds a subject as a friend to gain access to his or her profile information, and does so without creating a false profile or posing as an acquaintance, the evidence collected is often admissible.

An investigator may also simply request the protected content of a subject’s social media account to have it handed over voluntarily or by court order or subpoena. An investigator may also request disclosure from others who have authorized access to the content.

Preserving Social Media Evidence

Since social media is constantly changing, information on social networks can disappear as quickly as it appears, so it must be captured and preserved on discovery.

Screen Capture

The simplest preservation method is a screen capture, or screen-grab, which takes a picture of your screen. Remember to capture your computer's calendar and clock information in the picture to date- and time-stamp the evidence.

Screencast

Screencasts can be used to capture words, images and the interactivity between pages. This can be done alongside a webcast narration to record yourself describing what is on the screen. Again, remember to include your computer's date and time information in the screencast.

Facebook History

Facebook allows users to download their entire history, creating an electronic copy of their profile. This can be useful when the activity in question occurred months or years earlier and a search is necessary to find the relevant information. Sometimes subjects in investigations will willingly provide their Facebook histories. In other cases, an investigator may need to compel a subject to hand over the information.

Authenticating Social Media Evidence

Regardless of how they find evidence online, investigators are required to ensure content from social media is authentic before it can be presented as evidence.

Here are four ways to authenticate social media evidence:

- Ask the subject if he or she posted the photo or message. (Judges have ruled evidence from social media accounts inadmissible when attorneys have suggested their clients' accounts had been hacked.)

- Record the IP addresses from which a social media posts was created to verify who actually posted the content. Internet browsing history and witness testimony can also corroborate evidence.

- Email files or videos to yourself (or to others) to time-stamp the information. This is especially effective to corroborate the time that you made a screencast to preserve social media evidence.

- An affidavit, signed by a witness, attesting to the investigator's findings on social media sites can help to prove the authenticity of evidence.

Legal Considerations

Always check a social media network's terms of service before creating accounts specifically for investigations.

Lawyers and investigators can be fined and even incarcerated in some states for presenting evidence from investigations that used pretexting techniques. In California, for example, it's illegal to impersonate someone through or on an internet website.

Due to the ever-evolving nature of social media, laws surrounding online evidence gathering are constantly changing as courts attempt to keep up. Legal precedent for pretexting varies from state to state and from industry to industry.

The Gramm-Leach-Bliley Act and the Fair Debt Collection Act prohibit pretexting as a way to obtain personal financial information or for debt collection. But even when guidelines are unclear, investigators are discouraged from pretexting, since it is considered to be an unethical practice for obtaining evidence.

Case IQ™

Case IQ case management software simplifies the process of tracking and managing investigations, and gives you the reports you need to analyze results, demonstrate trends and prevent losses.

Get a free demo today.

Visit www.caseiq.com or call 1-800-465-6089