Online Investigations: 5 Mistakes Putting You at Risk

Online sources can yield great intelligence, but they can also be quite perilous. When visiting sketchy websites, you risk exposing your systems to malware infections, or making yourself and your org a target for attack. To protect sensitive data and organizations' networks, IT security teams often have a policy of blocking access to certain websites.

What happens when you need to visit those sites, or go undercover to browse the dark web? There might be a process that allows for exceptions or dedicated infrastructure that's reserved for such risky operations. But with online investigations, time is always of an essence, and you need to get access to all types of content or risk the mission.

Another important consideration is chain of custody (i.e., how information is collected, safeguarded, analyzed, shared, etc.). When you collect information online, how do you store it safely and securely? How do you collaborate and share with your team? And how do you make sure it's correctly labeled and properly documented?

At Authentic8, we deal with these types of questions daily. We've identified the top online investigation mistakes to address immediately.

1. 'Just' Looking It Up Online

With so much information available online, it's very tempting to quickly access the sites that you need, including social media or online directories, using your regular computer and browser. You already have the tools, and it's easy to locate people online with just a few clicks — find their phone numbers, addresses, known affiliates, figure out what they are doing, who they are hanging out with, which hobbies they are pursuing, etc. — the whole pattern of life analysis. The internet offers readily available sources — free and commercial — for background checks, criminal records, family trees, and just about everything else.

But while you are investigating your suspects, they might (and likely are) looking back at you. Even if you have created a "burner" profile to disguise yourself, and use incognito mode or VPN to browse the web, your computer leaves behind a trail of breadcrumbs that can easily lead a target back to you. Any search, however small or quick, needs to be approached with care to ensure that you protect yourself and your organization.

READ: What is Managed Attribution, and How Does It Improve Online Investigation?

2. Ignoring OSINT Tools and Techniques

If you are not familiar with the term, OSINT stands for Open Source Intelligence — basically collecting evidence from publicly available sources. The term was initially coined by the military, but at this point, organizations in both private and public sectors have embraced the art of OSINT, with many having designated specialists, tools and techniques.

As an online investigator, you can help protect your mission, your organization and yourself by learning and implementing OSINT tools. Authentic8 offers OSINT Academy, an online, self-paced training course for online investigators. Additionally, there are many great resources, like www.osinttechniques.com (not affiliated with Authentic8), that can help you find the right investigative tools for any type of research.

DOWNLOAD: Open and Dark Web Research: Tips and Techniques Booklet

3. Underestimating the Bounty of Social Media

It's mind boggling that in 2021, the world population is about 7.8 billion, and of that seven billion, there are 3.8 billion active social media users, with on average eight social media profiles each. And they spend about 144 minutes per day scrolling, posting, and watching all types of content on social media sites.

Take TikTok for example: the platform literally exploded in popularity among young people, and it didn't go unnoticed among bad actors. You can easily find ads for illicit merchandise specifically targeted at kids and young adults, and having tools that can help identify the people behind these ads can be extremely helpful to analysts.

READ: How to Quickly Investigate on TikTok

There are many specialized tools — third party and managed by social media companies themselves — that can help you conduct searches on social media.

- https://www.social-searcher.com/, an engine that allows you to monitor all mentions of a name, keyword, or phrase across 11 different social media platforms.
- https://socialbearing.com can give researchers a full profile and tweet analysis — what is someone looking at, which words do they use the most, are they sharing links in their profiles. You can even find out which OS someone is using when posting on Twitter, Instagram or TikTok, which, of course, can be really useful information.

When looking at images, certain browser plug-ins and extensions can make an investigator's job easier and help get results faster: Exif data plug-in, for example, helps analyze images and collect specific information, including when, where and on which device the image was taken.

4. Overlooking Your Own Online Fingerprint

You know how Facebook and other sites can "suggest friends" to you? They use a sophisticated algorithm based on the information they already have about your location, sites you visit, places you shop, people you talk to, profiles you look into, and so on. Things like super cookies follow you around the internet and share information between companies to build a complete profile, which, of course, can also be used by your adversary to figure out who you are.

If you haven't yet, check the "privacy settings" on any website you visit — you will be astounded how much information is being collected and shared across platforms. That's how social media and other internet platforms make money. But this is also something that investigators need to be very vigilant about — because once a target suspects that they are being watched, they can retaliate in an endless variety of ways, and/or move their operation underground, delaying the investigation and erasing valuable evidence.

Creating fake profiles is not a good alternative either. First, it doesn't disguise your identity — your browser fingerprint can still give you away; and also, in light of recent political events, sites like Facebook have started to really crack down on fake and spoofed social media accounts, even when they are used by journalists or good-faith analysts.

5. Thinking 'Dirty' Networks & Separate Infrastructure Will Keep Your Anonymous

To be good, effective investigators, you need to collect accurate information, while protecting your investigations, your organization and yourself.

Some organizations try to accomplish this by installing and maintaining a separate "dirty" network for browsing sketchy sites and downloading files. But separate infrastructures are not only costly to install and maintain, they also don't provide complete anonymity, and make it difficult to share evidence with other researchers and maintain a chain of custody.

A better approach is to use managed attribution services — a technology that allows you to use the same computer that you use day-to-day, but through access to a web-based service, which customizes and cloaks how you appear to external parties. You can actually modify your location, your device type, your web browser, your time zone and any of that other information that websites and services use to fingerprint and identify you.

With a cloud-based browser, all your activity is completely isolated from your actual workstation, preventing any malware infections from spreading through your network. It looks and feels like a regular browser, but your organization is completely protected, evidence is securely stored, and chain of custody is preserved.

READ: What VPNs and Incognito Mode Still Give Away in Your Online Identity

Contact us to learn how Authentic8 Silo for Research helps online investigators stay secure and anonymous.

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com