NTREPID®

Online Law Enforcement

Stand-Alone Laptops Endanger Investigations

The internet plays a part in virtually all law enforcement investigations. Before gathering evidence or working undercover online, investigators will commonly connect to the internet on a dedicated laptop using their personal Wi-Fi. Unfortunately, this is an unsafe way to operate, introducing investigators to a number of risks: location leaks, content blocking, malware infections, and more.

Just as detectives wear plain clothes and drive unmarked cars, it's important for web-based law enforcement officers to prevent these risks by avoiding identity exposure.

Avoiding Identification

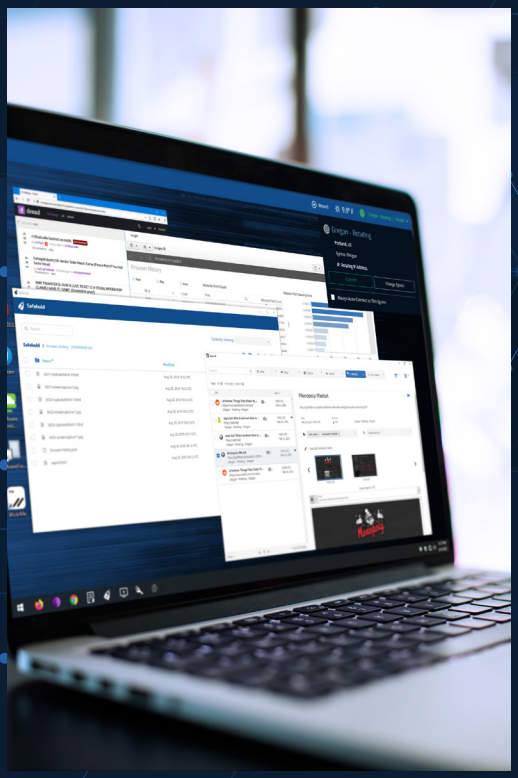
It's in the Details

When you're active online, your computer reveals many details about your identity. Websites can track your operating system, browser, plug-ins, language capabilities, and countless other identifiers to profile you, most often for digital marketing analyses. However, websites owned by bad actors may have other intentions. Some investigators will try to disguise their technical identifiers, thereby eliminating any trace of their digital fingerprint. But these fundamental identifiers are actually still discoverable. Complete non-attribution online does not exist.

Meanwhile, inconsistent settings and behaviors can cause an investigator to look even more suspicious. Investigators often try to alter their identities by tethering their stand-alone laptop to a Wi-Fi hotspot that is unaffiliated with their organization. While this method prevents sites from tracing investigators' activities back to their organization's network, it doesn't prevent sites from blocking content or displaying misinformation. Websites can restrict access to content when the user is originating from a certain region or organization. Similarly, websites might publish false information to users egressing from the site's host region.

As investigators gather online research about potential criminals, they often find themselves on equally nefarious websites, like those containing tracking malware. A stand-alone laptop can protect an organization's network as long as the investigator makes sure to never connect to the agency's network while using it. Furthermore, consistently using the same laptop across multiple investigations jeopardizes the investigator's mission. If the laptop has been unknowingly infected with tracking malware, bad actors could gain access to a host of identifying information. Discarding or reimaging the laptop after each use is the only way to ensure that anything malicious on the device is destroyed. Yet, this option is impractical, wasting valuable time and money.

To effectively protect their online investigations, law enforcement agents need a more robust, protective, and permanent solution than a stand-alone laptop. Only a properly designed managed attribution platform can address these issues, ensuring both safe and effective online activities.



Nfusion

A Managed Attribution Platform for Online Law Enforcement

Ntrepid's Nfusion provides a secure operational environment for law enforcement investigators. Nfusion minimizes the risks created by stand-alone laptops and eliminates the need for inconvenient addendums, like hotspot internet services. Nfusion also includes 24/7, year-round technical and operational support: a Network Operations Center (NOC) maintains our managed attribution products; account managers provide hands-on training and troubleshooting; and the Ntrepid Academy leads monthly webinars and custom training opportunities. By choosing to partner with Ntrepid, law enforcement agencies will gain both sophisticated technological solutions and a team of technical experts.

NTREPID®

Contact us to learn more about the full spectrum of Ntrepid solutions.

www.ntrepidcorp.com
1.800.921.2414
solutions@ntrepidcorp.com