The 7 Deadly Sins of OSINT

OSINT investigations can range from simple, containing one target on one account, to the very complex, such as multiple targets spanning various platforms and locations. Likewise, a target of an OSINT investigation can take extreme measures to conceal their real identity, or they may unknowingly leave a large trail of breadcrumbs that lead an investigator straight to their doorstep.

In my experience, these breadcrumbs can often be grouped into just a handful of categories that encompass some of the most common mistakes users make which increase their vulnerability to OSINT-based techniques. Keep in mind that, in most cases, practicing good overall operational security (OPSEC) will mitigate many of the risks exploited by a good OSINT investigator. Curious to know just of many of these 7 Deadly OSINT Sins you are guilty of committing online?

Take a look at the full list and how to mitigate their effects below.

ENVY

I consider Envy to be the driving force behind many of the other OSINT sins: including Greed, Wrath, and Pride, though it might occasionally manifest on its own. Users that are envious of others, whether their achievements, social status, follower count, wealth, etc, may participate in riskier behavior that increases their OSINT attack surface in order to obtain validation or to increase their perceived worth in one of the aforementioned traits. This might occur by oversharing or posting more frequently to gain more followers or notoriety, or perhaps the user will attempt to discredit or attack one or more users that they consider “unworthy” of being in such a position.

Mitigation Methods: Take the time to unplug. Don’t let other’s successes reduce the validity of your own, life (and social media) isn’t a competition.

LUST

Even accounts that are locked down to outside users are not fully protected from OSINT practitioners. Exploiting the sin of Lust is often one of the ways to penetrate accounts otherwise closed to outsiders. Users may be quick to accept friend or connection requests from an account that is crafted to appear like an attractive member of the sex the target is interested in. A sock account can therefore be used to dupe a user into accepting a connection that allows an investigator to view all of their content. In many instances, users that restrict viewing of their accounts tend to be more open in sharing information to users that have been granted such access.

Mitigation Methods: Learn to spot sock-puppets and be wary of unusual and unsolicited connection requests, especially if your account is private or otherwise locked down. This is particularly true for those requests that that appear to be crafted as a perfect match to you.

GLUTTONY

Despite the number of relevant posts filling social media, Gluttony is perhaps the most under-exploited of the OSINT sins. It is often exhibited via a photo of a meal or a check-in to a restaurant. Depending on if the restaurant is tagged, or if the food is specialized, an investigator may be able to identify, at the very least, the chain in question. Any unique background information (signs, decor, tabletops, floor tiles) can assist in narrowing down locations to a specific instance of the restaurant chain. It may also be possible to establish a pattern of life for users that post numerous meals on social media. This can be done by averaging the times posted for each meal and might help narrow down a range of time zones a target might reside in.

Mitigation Methods: For those that must share photos of your meals, try to include as little information about the location you are in as possible. For especially higher-risk persons, staggering the times of posting your scheduled meals also makes it more difficult to fingerprint your time zones based on common patterns.

GREED

The OSINT sin of Greed is very similar to the real-world version and I often see it in giveaways of real or virtual items or currency. Search any social media site for “cash.app” or “gofundme”, etc and look at how many people are quick to share their link to those purporting to give away money in exchange for likes and shares of their post. While linking other accounts always posts a risk of an investigator finding the connection, these payment platforms are high-value targets for an investigator as they more often include a target’s real information rather than that of their social media handle. Similarly, users that share local giveaways might inadvertently be giving up location information as well. After all, do you really think a doughnut shop in New Jersey is going to ship the dozen doughnuts prize to someone in Indonesia?

Mitigation Methods: Don’t mix business and pleasure (accounts). Keep your cash transfer apps and fundraisers to your personal accounts or in private messages only.

SLOTH

In OSINT, Sloth can take many forms. However, it primarily occurs when a target reuses something due to laziness or lack of creativity such as passwords, photographs, usernames, biographical data, etc. Numerous tools and techniques exist for locating usernames on other platforms and basic Google Dorks allow investigators to find biographic data, headlines, images, and commonly used hashtags that a user shares across platforms. Additionally, tools like Dehashed enable the linking of accounts belonging to users with unique (to them) passwords that are reused on other platforms. Even a user which employs different usernames can therefore be linked if their accounts have shared passwords and both been involved in data breaches.

Mitigation Methods: Don't reuse passwords, ever. Treat accounts that share the same username, email, profile photo, etc as the same account, meaning that if you wouldn't share information on one account with that name then you shouldn't do so on any of them. Go back and remove any leaked data from old accounts that may use the same username or password to prevent historical information from being used against you in the future.

WRATH

Wrath is one of the more unusual sins and does not seem to occur as often as the others. Oftentimes, this OSINT information occurs as a result of an online argument that escalates to the point of driving another user to doxx your target. Although this can lead to more rapid results by leveraging such information found on places like Pastebin or Doxbin, or in the interaction between the users during the argument, be sure to verify such information as the results can vary wildly. At the very least, such occurrences may provide you with additional leads for branching out the investigation or for cross-referencing what you already assume you know about a target.

Mitigation Methods: Do not engage in heated arguments online, particularly with users that have knowledge of information that may be used against you. If possible, remove any information of yourself online to reduce the chance of others locating and combining it into a single source for others to find.

PRIDE

People like to share their accomplishments and success. For OSINT, I equate the sin of Pride to be oversharing, particularly when it involves identifiable material in the form of major life accomplishments. This can take many forms, with some of the most notable examples including a target sharing a photo of their newly awarded driver’s license (search the hashtag #gotmylicense), diploma (#classof####), certification (#gotcertified), workplace award (#workaward), etc. Oftentimes they fail to redact these images and their full name, state/province, country, license plate, workplace ID, etc are on full view. This makes it very easy for an investigator to unmask the user behind the social media account in record time.

Mitigation Methods: Double check your photos and posts before posting to be sure you have sanitized all personal information. Do not unnecessarily overshare, particularly things that make it easy to identify you or narrow down who you are.