Ritu Gill

What are Sock Puppets in OSINT

Learn about Sock Puppets, the benefits of using them, and best practices for setting them up.

April 17, 2023

What are sock puppets?

Sock puppets, also known as research accounts, are online fictitious identities used to conceal the tru identity of the OSINT investigator and to gain access to information that requires an account to acces

Remember, you are responsible for reading and understanding the Terms of Service for the websites y use because creating fake accounts goes against some platforms' Terms of Service; however, this is nc usually illegal. It's equally important to check with your organization's policies to ensure you have permission to create and use sock puppets.

Purpose of Sock Puppets

OSINT investigators create sock puppets so they can access content on various sites, such as social media platforms, where content is only available with an account.

Sock puppets are also created to isolate OSINT research, ensuring a separation between the personal and work lives of OSINT investigators. It is essential to emphasize the importance of separating an OSINT investigator's real identity from their research accounts, otherwise known as practicing good Operational Security (OPSEC).

your personal vehicle? Most of you would hopefully answer "no"; you would not do that. The question to ask yourself is why you would use a personal Facebook account to research your subject. It's similar because your vehicle links to your real identity, just as your social media accounts link back to your real identity.

The Benefits of Sock Puppets

It is recommended that OSINT investigators avoid using their personal social media accounts for research purposes to uphold their privacy and security and ensure the investigation's integrity. Keeping personal and work accounts separate when conducting research is crucial for gathering information discretely and anonymously for good OPSEC.

What are the Sock Puppet Functions?

Most OSINT investigators will conduct passive research. That being said, it's important to understand the difference between passive versus active open-source research and collection because how sock accounts are set up will differ depending on the research type.

Passive means you do not engage with a target. However, your profile might still end up in these results of such things as "suggested friends" or "people to follow," so you may want to blend in a little. Choosing a name that blends into your target group is a good idea.

Active research means engaging with a target in some fashion, i.e., adding the target as a Facebook friend. Blending in with the target group is even more imperative for active research. If you are engaging with a target, you may want to create a couple of accounts on different platforms to make it look like you're a real person.

Best Practices for Sock Puppets

Creating research accounts is not easy, and often, trial and error wins the day.

There is no step-by-step process when setting up accounts, but these are some considerations before creating a research account; some points may seem basic but are equally important.

The best advice is to appear as any regular user who wants to create an account. There are several things to think about. For instance, a typical user would not hesitate when entering their email address and password.

- Name - Use fictional details when considering a name for your sock account. Avoid using your real identity. Consider what name would blend in with your target group because if you are suggested as a friend, you don't want your account to stand out.
- Email address – You have several email provider options (Mail.com, Gmail.com, Yandex.com, Outlook.com). Do not use a previously created email address – always start fresh and create a new email that has not been previously used.
- Phone verification – If you cannot bypass the phone verification, use a burner phone and SIM card to create accounts.
- Setting/Privacy settings - Immediately review and set the privacy settings for the platform and choose the most secure privacy settings that will allow people to see as little information as possible.
  If you're conducting passive research, you may want to keep the account completely locked down and do not need to leave the profile public.
  If you're doing active research, you must keep your account locked down until it appears to be that of a real person. Some considerations may include; are there enough Facebook friends, followers, and activity on the profile? Do you have a back story that fits well before you create your profile? Example: I assisted investigators with setting up a research account that was meant to be used for engaging a subject. I walked them through the process of creating an account. Once the account was up and live, it was important to have a backstory about why this user had a new account. The investigators mentioned that they wanted to keep the friends list open as that would be normal. I quickly noted that this was not a recommended action as it would not fit the backstory of who the investigator was playing. For instance, a male in his early 20s would easily have over 100 friends, so it did not make sense to have an open friends list until it was built up with at least 100 people.
- Profile photo - Use generic landscapes like mountains, beaches, etc. Avoid using someone else's identity. Sometimes it is helpful to use stock images and crop the photo so that any previously stored data is deleted before uploading, as social media platforms have algorithms that can detect the use of stock images and flag your account.
- Activity - Once your account is created, it's vital that you start interacting in a natural way, such as posting links, liking pages, etc. The main objective is to mimic how a real person would use a new account and convince the platform that you are a real person.

Learn more about OSITN by taking SEC497 Practical Open-Source Intelligence (OSINT)

Tags: Open-Source Intelligence (OSINT)

Related Content

Open-Source Intelligence (OSINT) December 20, 2024

SEC587: Advanced Open-Source Intelligence Course Update – What's New?

The escalating geopolitical activities of Russia and China have intensified the necessity for advanced OSINT techniques.

Blog

Security Awareness, Artificial Intelligence (AI), Digital Forensics, Incident Response & Threat Hunting, Cloud Security, Cyber Defense, Offensive Operations, Pen Testing, and Red Teaming, Industrial Control Systems Security, Open-Source Intelligence (OSINT)

December 10, 2024

Top SANS Summit Talks of 2024

This year, SANS hosted 13 Summits from OSINT, ICS, Ransomware, DFIR to HackFest. Here were the top-rated talks of the year.

Alison Kim

Blog

Open-Source Intelligence (OSINT) May 26, 2023

SANSがおすすめするサイバーセキュリティの仕事20選: テクニカルディレクター

テクニカルディレクターの主な業務や、

Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Your Email...

Select your country

By providing this information, you agree to the processing of your personal data by SANS as described in our Privacy Policy.

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Subscribe

Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Your Email...

Select your country

By providing this information, you agree to the processing of your personal data by SANS as described in our Privacy Policy.

- ☐ SANS NewsBites
- ☐ @Risk: Security Alert
- ☐ OUCH! Security Awareness

Courses

Certifications

Degree Programs

Cyber Ranges

Job Tools

Security Policy Project

Posters & Cheat Sheets

White Papers

Focus Areas

Cyber Defense

Cloud Security

Cybersecurity Leadership

Digital Forensics

Industrial Control Systems

Offensive Operations