AMITT

ADVERSARIAL Misinformation Influences tactics and technique

Attack, Defend, Safety, Secure, technique.

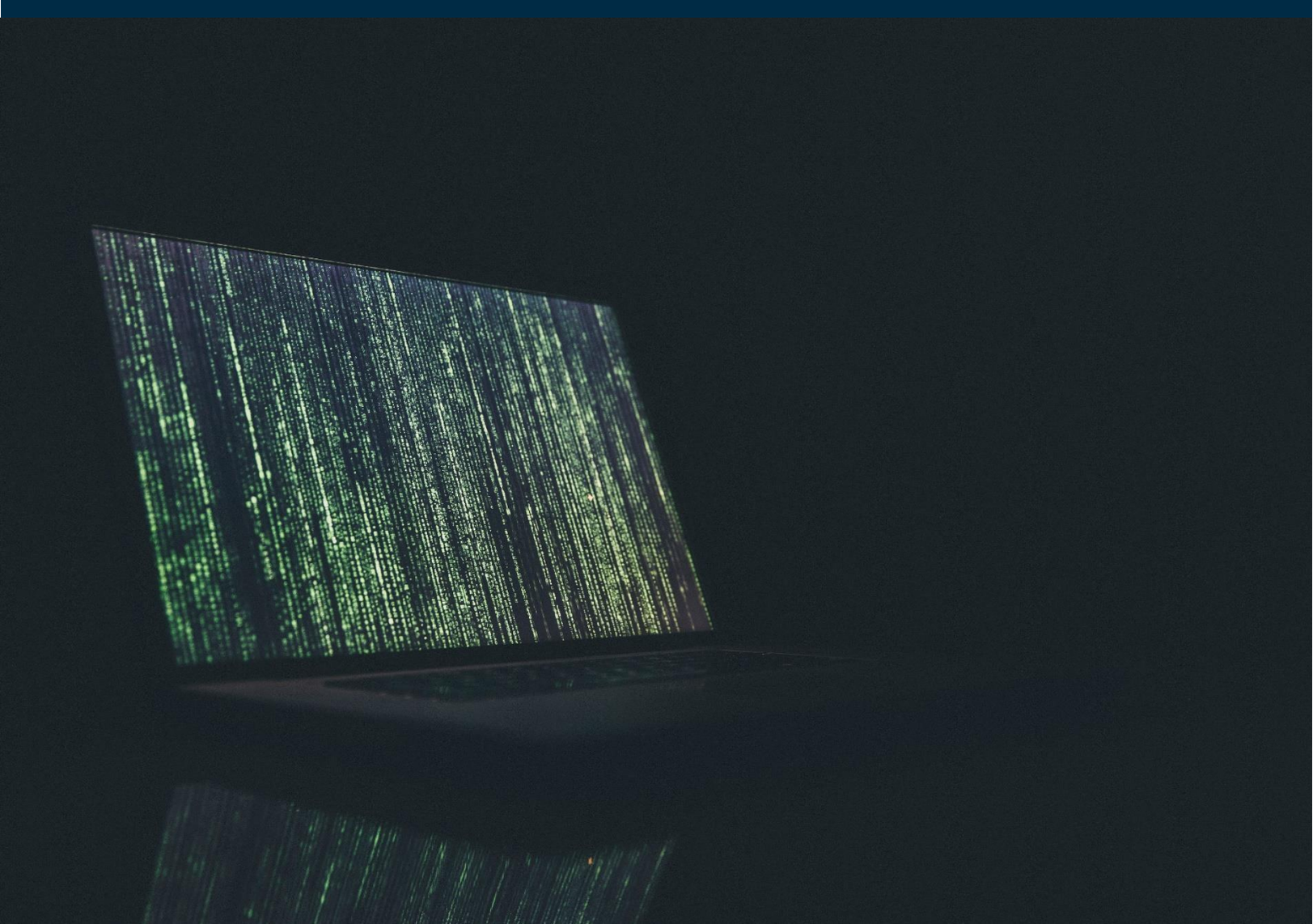


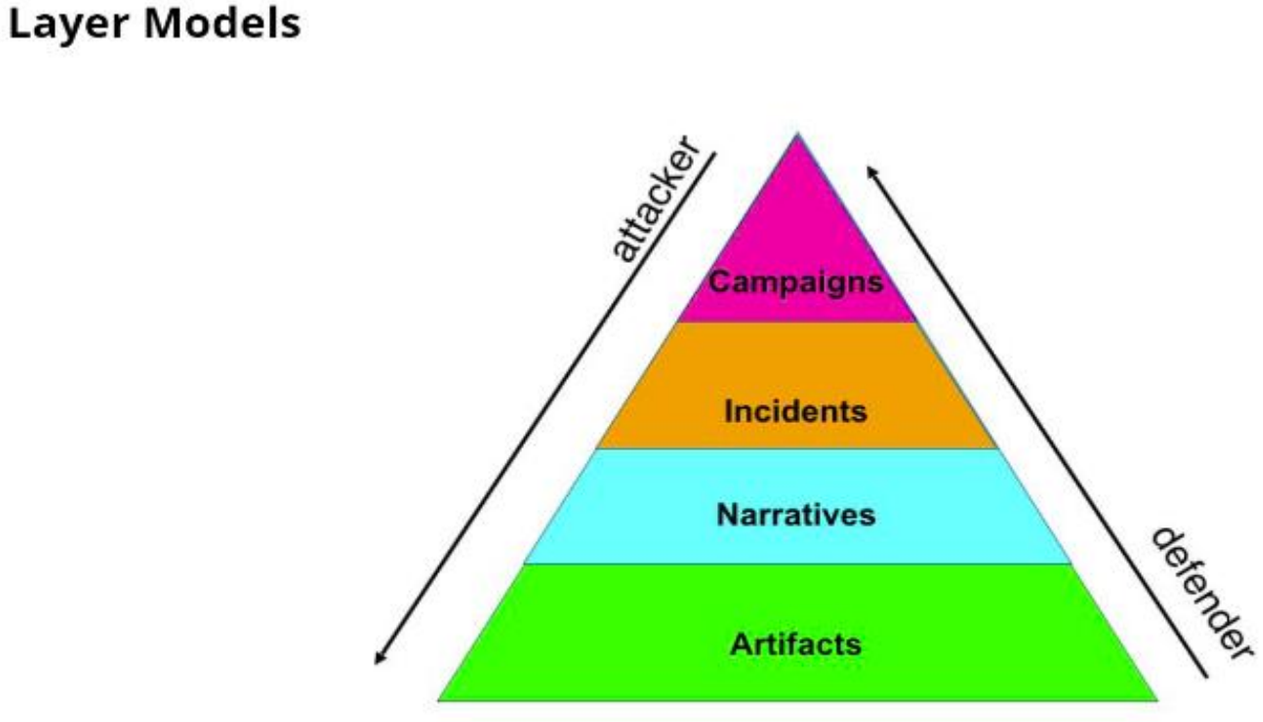
TABLE OF CONTENT

Introduction

In this section, we discuss a model that shares information about disinformation and discuss how attackers and defenders use the AMITT framework and Model to spread or mitigate the impact of disinformation on a target. How many actor models are involved in Power-motivated Disinformation? Also, discuss your safety and Mental health when you work to defend against disinformation. Security and safety are essential when we work on disinformation.

Disinformation Model

The model helps us share information about disinformation and helps us to create strategies for mitigating and defending against misinformation using tools and mechanisms.



Disinformation Pyramid

Disinformation Pyramid connects information operations, threat intelligence, OSINT Research, and data science of disinformation.

Attacker:

Start from the Top of the Pyramid and work their way down.

- **Campaign:** long-term disinformation operations. like geopolitics, nation-funded, and sometimes particular interest groups. Information operations often work on this level.
- **Incidents**: Short-term, Cyclic things, that happen over defined timespans that indicate teams or individuals.
- **Narratives:** Stories that we talk about ourselves and the world. A mixture of true and false

Introduction

information.

- **Artifacts: Incidents** and narratives show up online as artifacts. Social media accounts are used to spread disinformation.

Defender:

Start from the bottom of the Pyramid and work their way up.

- **Artifacts:** Analysts use images, website videos, etc. to link between them and collect info to understand what is happening.
- **Narratives:** Tagging information helps analysts to detect misinformation.
- **Incidents**: Analysts can recognize incidents through threat intelligence like TTPs, Threat actors, and other objects. OSINT research also happens on this level.
- **Campaign:** Information operations often work on this level by applying all information that collects on down layers.

Actor Model:

Three groups of people power-motivated misinformation. The attacker, Defender, and target people (population)

- **Red:** Attackers create incidents as part of long-term campaigns and use artifacts to spread in the form of narratives (memes or gist) and achieve their goals.
- **Blue:** Working back from artifacts to incident and campaign.
- **People**: Unintentionally the part of sharing misinformation or being a target of disinformation narratives.

Object Model

STIX is a data standard used to share information between threat intelligence and language to describe threat objects and the relationship between them. STIX translates well for information use it adds two objects for disinformation: narrative and incidents.

Behavior Model

TTPs are an important object that shares lots of information about disinformation. AMITT framework is designed to give responders a better way to rapidly describe, understand, communicate, and counter misinformation incidents. AMITT frameworks are used to break disinformation into components. The components include:

- Phase: High-level grouping of tactics. Ensure we could not miss anything including planning, preparation, execution, and evaluation.
- Tactics: Stages that someone running misinformation that likely to use.
- Techniques: Cultivate ignorant agents, This describes unwilling agents.
- Taks: Taks are things that we do, Technique defines how we do.

Social Media Object Models:

STIX gives artifacts object type of observed data and indicator. In this model, we talk about social media posts for each type of new platform like Twitter posts, Facebook posts, etc. but these found it difficult and confusing to work with speed.

OPSEC Foundation: Work Environment

Safety is important when we work on Disinformation Reasons are:

- Disinformation can be distressing material. Bad Images, hate speech, etc.
- Disinformation people are not always nice people operational security is important.
- Disinformation work also be separated from your day job.

Mental health

Disinformation includes difficult material like fear, emotions, disgust, and hate speech.

- Pace yourself
  - Talks with friends.
  - Eat chocolate.
  - Play with pets.
- Make disinformation something to go to
  - Don’t use a personal account.
  - Use incognito Mode.
  - Don’t always be passive, having some active account is useful too.

Operational security:

Operational security involves adopting measures to protect against threats, including both digital and physical aspects. By implementing threat-handling practices.

1. Threat Handling for Humans:
   - Implement security measures to protect against physical threats, social engineering, and phishing attacks.
   - Maintain awareness of potential threats and stay vigilant in detecting suspicious activities.
   - Regularly update passwords, enable multi-factor authentication, and secure personal devices.
2. Compartmentalization:
   - Separate and limit access to sensitive information based on a need-to-know basis.
   - Use strong access controls, such as role-based access control (RBAC), to restrict privileges.
   - Employ encryption and secure communication channels to protect sensitive data.
3. Foundations: Personal Security:
   - Protect personal information, such as social security numbers and financial details, by practicing good data hygiene.
   - Be cautious of sharing personal information online and use privacy settings on social media platforms.
   - Regularly monitor and review personal accounts for suspicious activities or signs of compromise.
   - Use 2FA, implement strong passwords, and mitigate surface attacks\.

OPSEC Foundation: Work Environment

.

1. Compartmentalization:
    - Separate work-related activities and information from personal life to maintain privacy and security. (Virtual Box, VM ware)
    - Limit access to sensitive work data based on a need-to-know basis, implementing access controls and encryption where necessary.
    - Avoid discussing work-related matters in public or insecure environments to prevent unauthorized access or leaks.
2. Cover Your Persona:
    - Maintain a professional online presence and be mindful of the information you share on public platforms.
    - Use separate email addresses, phone numbers, or social media accounts for work-related communication.
    - Be cautious of phishing attempts and social engineering attacks, verifying the authenticity of communication and requests.
3. Work Recipes: If This, That, Then:
    - Develop clear workflows and protocols for handling different situations and scenarios in the work environment.
    - Establish standard operating procedures (SOPs) that outline steps to follow in response to specific events or incidents.
    - Regularly review and update work recipes to adapt to evolving threats and circumstances.

App Basics

Weak passwords and strong passwords. Passwords Manager is the easiest way to create, store and implement secure passwords for all of your accounts.

Local and cloud-based password manager

Local: More secure, less efficient, harder to maintain, easier to lose everything if you forget or lose everything access to local.

Cloud-based: Easy to maintain, easier to use, accessible anywhere, and less secure.

Some options

- 1password
- LastPass
- keepassXC

Two-Factor Authentication (2FA):

- Enable two-factor authentication for your online accounts whenever possible.
- Use a trusted authenticator app or hardware token as the second factor to enhance security.
- Regularly review and manage your authorized devices and 2FA settings for each account.

Using a VPN (Virtual Private Network):

- Utilize a VPN service when connecting to public Wi-Fi networks or accessing the internet from untrusted locations.
- Choose a reputable VPN provider that offers strong encryption and does not log your browsing activities.
- Enable automatic VPN connection on your devices to ensure secure and private internet browsing.

Web Browser Extensions:

- Install reputable browser extensions for additional security and privacy features.
- Consider using ad blockers and script blockers to prevent malicious ads or scripts from running.
- Utilize password managers to generate and securely store complex passwords for your online accounts.
- Enable browser security features like safe browsing and phishing protection to detect and block suspicious websites.

Burner Email and Phone Number:

- Burner Email: Use a burner email address when signing up for online services or platforms that require an email address. A burner email is a temporary or disposable email address that helps protect your identity and privacy. It can be created using various services that offer temporary email addresses. Burner emails allow you to maintain anonymity and reduce the risk of spam or unwanted emails.
    - 33mail: Free option that might get flagged.
    - Proton Mail: free end-to-end encrypted mail.

- Burner Phone Number: Similarly, a burner phone number is a temporary or disposable phone number that you can use for specific purposes, such as online registrations or communication. Burner phone numbers can be obtained through virtual phone number services or mobile apps. They provide an additional layer of privacy, allowing you to keep your personal phone number private and avoid potential unsolicited calls or messages.
    - Free VOIP
    - Paid VOIP

Secure Communication:

- Encryption: Use strong encryption techniques to protect data during transmission.
- Secure messaging platforms: Use applications with end-to-end encryption for secure messaging.
- Virtual Private Networks (VPNs): Employ VPNs for secure and private network connections.
- Secure email: Utilize encrypted email services or encryption tools for secure email communication.
- Secure voice and video calls: Use encrypted communication applications for secure audio and video conversations.
- Digital signatures: Implement digital signatures to verify document authenticity and integrity.

End-to-end Encrypted email services include

- Proton mail
- Tutanota

Practical

Defense against disinformation by protecting yourself.

When you're working against disinformation first protect yourself by hiding your identity. Don't use a legitimate or personal account to research it that put yourself in danger. It is recommended that you use burner email, phone number, and VPN it helps you to hide your identity and save yourself. There are the following platforms where you get burner email and phone numbers.

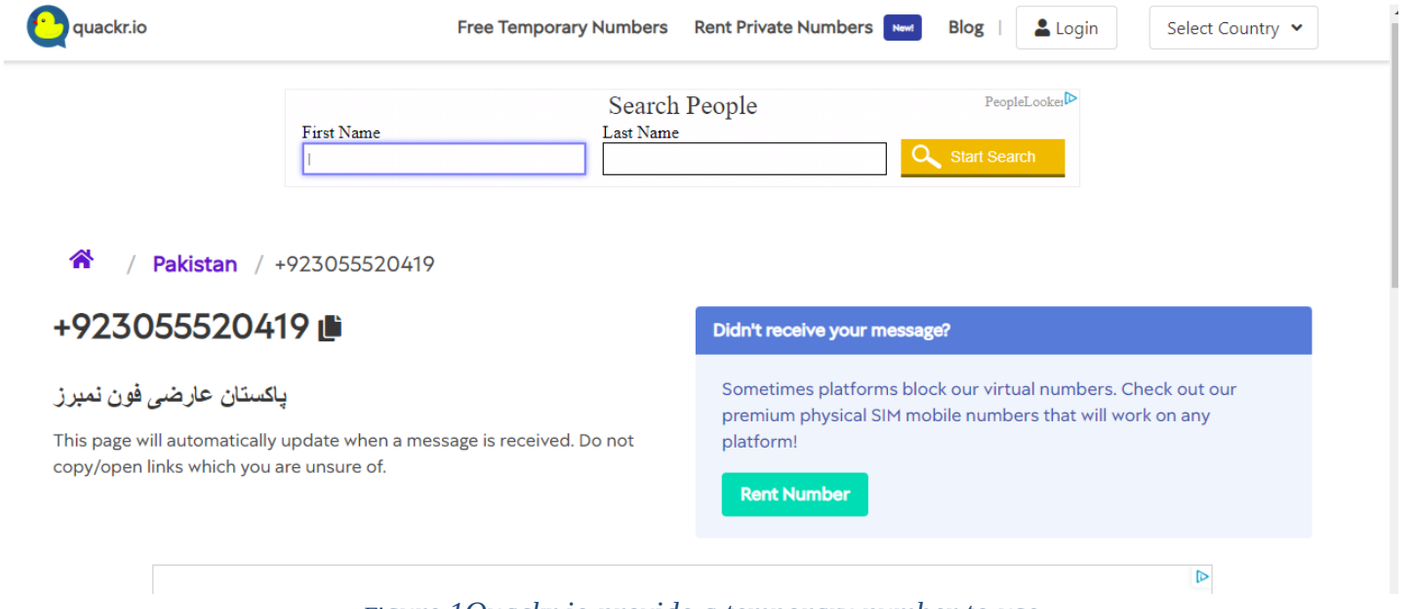


Figure 1Quackr.io provide a temporary number to use

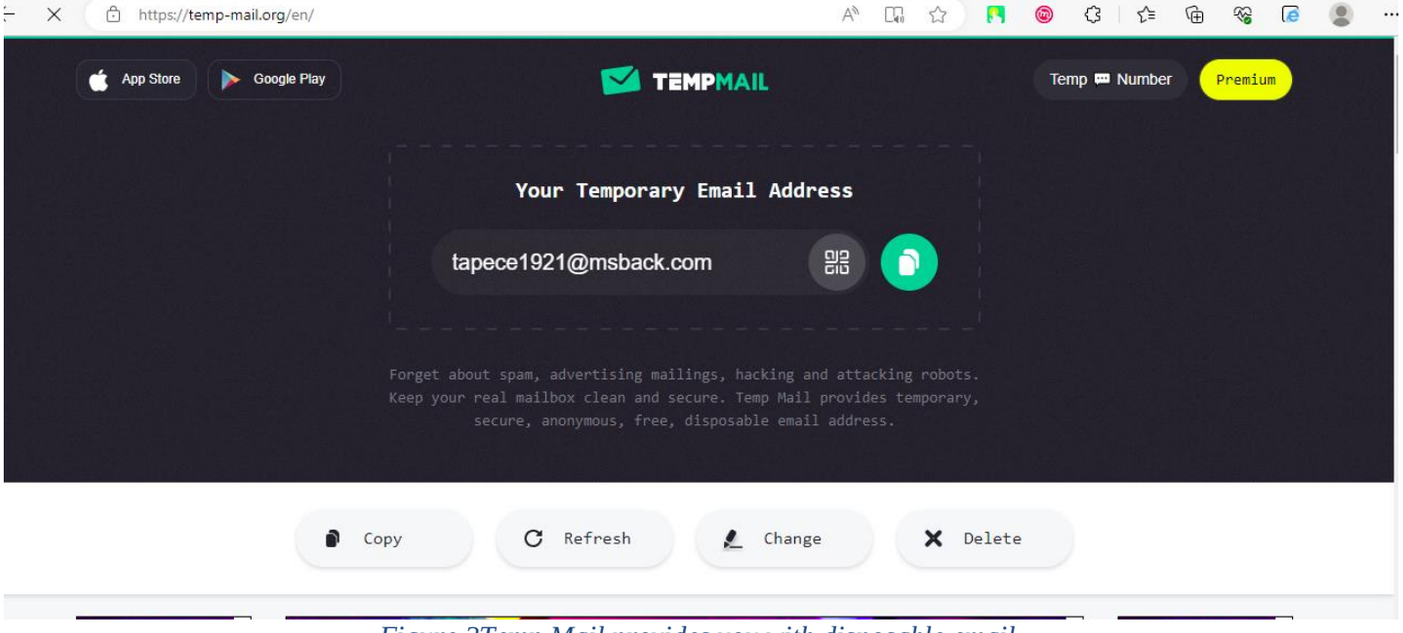


Figure 2Temp Mail provides you with disposable email.

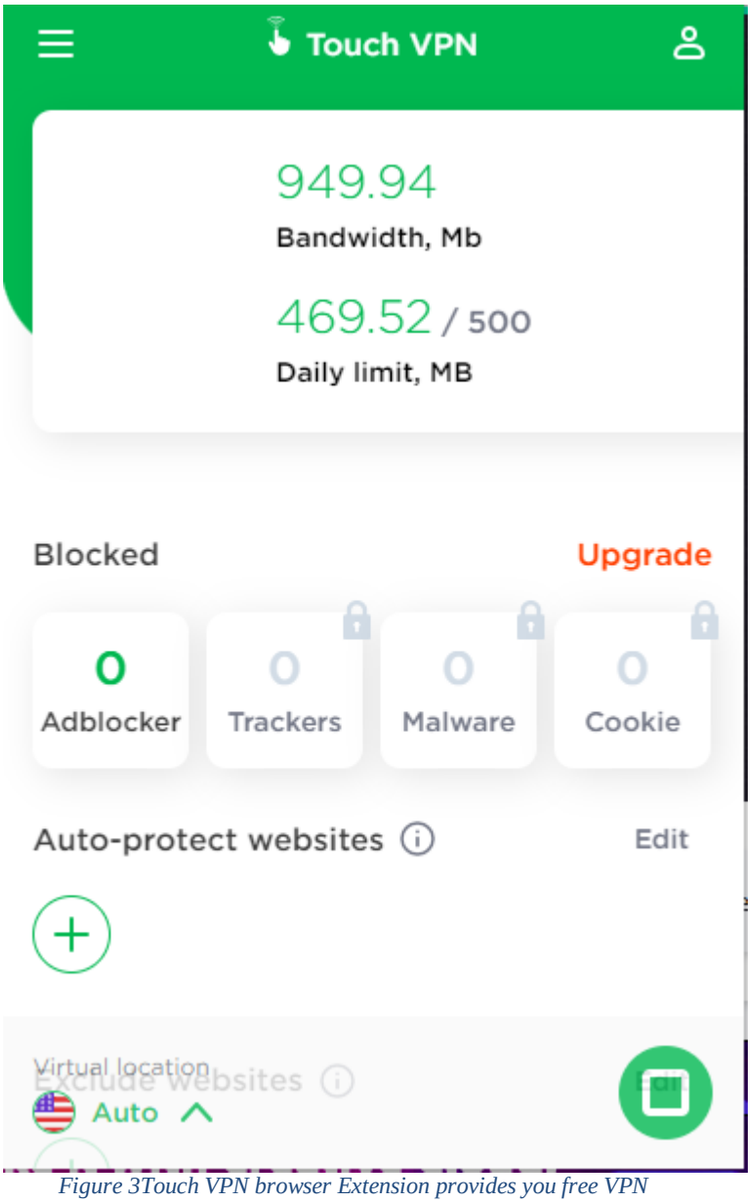
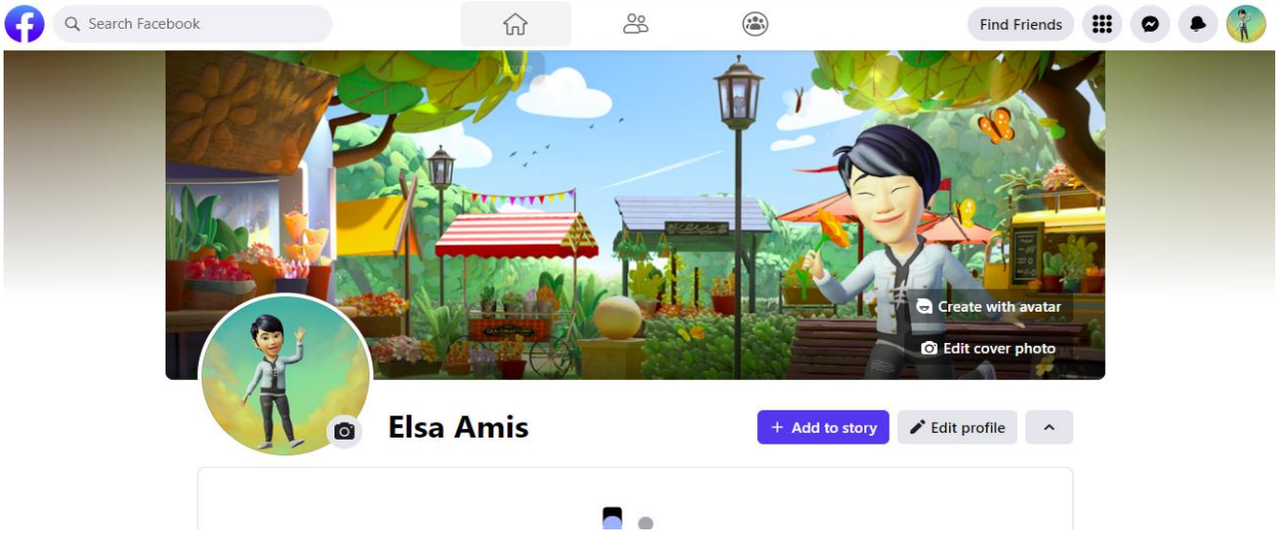


Figure 3Touch VPN browser Extension provides you free VPN

By using these platforms, you create fake social media accounts and do research against disinformation. You can use Google Fact check explorer to find false information and do research to find the campaign behind it using your fake identity.



Case Study

- A video is being shared on social media claiming it depicts a woman being forcefully converted to Islam.
- The post states that the video is from 'The Kerala Story' movie, portraying incidents of love jihad and forceful Islamic conversions.
- Reverse image search of the video's screenshots reveals that they were found in a BlogSpot article published in June 2021.
- The article reported that the video shows an exorcism in Bangladesh, which was misinterpreted as forceful Islamic conversions.
- Further searching on the internet reveals an extended version of the video published by various YouTube users in 2019.
- In 2019, a user on Twitter mentioned the video of a Hindu woman being forcefully converted to Islam, but another user, who speaks Bengali, clarified that it is an exorcism video.
- Bangladesh-based fact-checking site 'Rumor Scanner' published a fact-check article in January 2022, confirming that the video shows a Muslim priest performing an exorcism on a Muslim woman in Bangladesh.
- The priest mistakenly believed the possessor inside the woman was a non-Muslim and attempted to convert the supposed jinn to Islam.
- The Muslim priest taught the Kalima to the so-called jinn and took a statement of conversion from the possessed woman.

Claim: Video of a non-Muslim woman being forcefully converted to Islam

Fact: The video shared in the post shows old visuals of a peer or Muslim priest performing exorcism on a Muslim woman in Bangladesh. The video does not show the forceful Islamic conversion and it has nothing to do with India. Hence, the claim made in the post is **False.**

Conclusion

In the face of disinformation, prioritizing safety, mental health, secure communication, and operational security is crucial. Safeguarding our mental well-being by critically assessing information, seeking reliable sources, and fostering digital literacy empowers us to navigate the information landscape responsibly. Implementing secure communication practices such as encryption, VPNs, and digital signatures ensures the confidentiality and integrity of our conversations and data. Meanwhile, operational security measures like OPSEC and threat modeling protect against potential threats and vulnerabilities. By combining these efforts, we can combat disinformation effectively while safeguarding our safety, mental health, and privacy in the digital age.

Reference

1. documentation/BigBookOfDisinformationResponse/C04_disinformation_models.pdf at master · cogsec-collaborative/documentation · GitHub

2. Exorcism video from Bangladesh shared as visuals of a non-Muslim woman being forcefully converted to Islam - FACTLY