Online Security of Oppressed Groups of People

Mgr. Jan Vrba, MSc, DBA

Faculty of Administration and Economic Studies in Uherské Hradiště, Města Mayen 1536,
Uherské Hradiště, 686 01, Czech Republic, jan.vrba@fves.eu

Abstract

The research paper proposes the cost-effective ways how oppressed groups of people around the World can perceive their anonymity and be safe from possible imprisonment, oppression or violent attacks. This article is aimed as entry-level article to help oppressed group of people around the World such as journalists investigating human-trafficking cases, or any other person who is oppressed due to their gender, religion, political view or due to any other reasons. This article also serves as manual for oppressed group of people to know how they can protect themselves in a costs-effective way.

Keywords: Oppression, Online security, Manual, VPN.

1. Introduction

The main aim of the research paper is to investigate the possibilities of identity protection on internet in the real-world from the point of view of applicational settings and programs. By doing so, the following objectives are met:

- To create overview article on the topic of identity protection and identity hiding – explanations why, for who and other aspects,
- To draft real step-by-step manual of identity protection/hiding on internet including costs on how to (for casual computer/devices users) for oppressed group of people,

Please, note that the usage of TOR (The Onion Router) and similar apps in this article is limited due to its more-advance nature as well as due to its possible conflict with the general international laws since only using the TOR and similar apps/technologies may lead to police investigation as well as Police is able to track you even while using TOR.

In a fact, there is never a 100 % anonymous internet connection – every connection leaves certain tracks/marks and therefore is, in theory, trackable. Therefore, there is no need for TOR or similar Apps (Quora, 2022). Moreover, TOR or similar may not be available for certain oppressed group or people.

This article is an entry and introductory article for journalists, activists, oppressed group of people and others who needs to conceal, hide or protect their identity and actions on internet. **This article is written in a good will of providing the basic information for possible protection on internet for e.g. (please see the practical part of text with manual):**

- Journalists and activists writing about current problems and issues in countries in which it may lead to their imprisonment or even death penalty, or execution,
- Journalists and activists informing about topics such as slavery, human-trafficking and such as (who are in need of protection against human-trafficking rings),
- Other oppressed groups people who are oppressed or deprived due to their gender, political views, identity, race, or due to any other reason(s).

The main aim of this article is to assist the people such as journalists, underprivileged and oppressed groups of people in totalitarian states to reach the internet, data, information and to communicate safely without prosecution from the bodies which could do harm to them (e.g., mobs).

This article is not a manual for using the hidden/protected identity on internet to do fraud, illegal or criminal actions. Therefore, the Dark Net as well as TOR and similar apps are not mentioned in this article.

The article is written with the methodology of synthesis, literature review and real-action manual (including costs draft). To create the real manual for identity hiding/protection on internet, the following aspects are considered:

- **Reliability, reviews, real experience** – people need to stay in protected environment – if no, they may face prosecution, jail or execution.
- **Protection on the sufficient level** (not “low” and not “maximum” protection) – the protection should be sufficient to provide enough security/anonymousness,
- **Costs** – price of such as measurements which shall be kept reasonable and affordable – all measurements shall sum up to maximum of around USD 150 which is for people living in totalism-states already quite high price.

2. Literature Overview

One definition of oppression describes it as a system that maintains advantage and disadvantage based on social group memberships and acts on the individual, institutional, and cultural levels, both purposefully and accidentally. Oppression can be defined as a system that maintains advantage and disadvantage based on social group memberships (González-Scott, 2022).

There are basically five faces of oppression which oppressed people can meet. The first face is an exploitation which is a use of the efforts of other people to generate a profit while failing to provide them with adequate compensation (González-Scott, 2022).

Second face of oppression is marginalization which is **elegating or confining a group of people to a lower social standing** or outer limit or edge of society (González-Scott, 2022).

Third face of oppression stands for powerlessness since the victims do not have enough power to fight such an oppression (González-Scott, 2022).

Cultural imperialism is the fourth face of oppression. For instance, we can see cultural imperialism as **taking of culture by so-called ruling class and establishing it as the norm** (González-Scott, 2022).

The last face of oppression is a violence. Members of one group has to live in fear for their lives due to violence and attack from other groups or majority (González-Scott, 2022).

Oppressed Pedagogy, as mentioned by Alatise, Remi and Omobowale Ayokunle (2022) is important and the importance of receiving a good religious education cannot be emphasized. Education in many religious traditions has the potential to mold students' perspectives on modern social problems like poverty (Alatise, Remi, Omobowale, Ayokunle, 2022).

3. Basic Terms Definition

The basic terms definition chapter defines basic terms in understandable ways for readers and general publics. Terms for practical prat of this article are presented and explained.

Protection on internet, Cybersecurity Solutions

Solutions for Internet security must provide comprehensive protection against Internet-borne cyberthreats. Crucial capabilities include (Check Point, 2022):

- URL Filtering URL filtering allows an organization to restrict access to specific websites on company-owned devices. URL filtering can be used to restrict access to known dangerous websites and prevent employees from visiting sites that contain illegal or inappropriate content or have a negative impact on employee productivity (such as social media).
- Download Security Malicious content may be downloaded via a website or sent as an email attachment. A solution for Internet security should identify and block potentially harmful information en route to the user's device, before it enters the network or is downloaded into the user's system, therefore decreasing the hazard to the organization. Typically, a sandboxing strategy is used.
- Data Loss Prevention: Employees may purposefully or inadvertently leak corporate data via malicious websites, email, or insecure cloud-based data storage. Internet security solutions should monitor Internet traffic for sensitive and protected categories of data and prevent their exposure to the outside of the organization.
- Phishing Protection: Phishing attacks are among the most prevalent cyberattacks and can have a significant impact on the cyber and data security of an organization. Internet security solutions should include email scanning and anti-phishing methods to detect and prevent phishing emails from reaching their intended recipients' inboxes.
- Websites can execute scripts in the user's browser, which can exploit unpatched or zero-day browser vulnerabilities. Browser exploit protection facilitates the detection and prevention of the execution of this malicious code.
- Security against Zero-Day Attacks: Traditional signature-based defences protect against known weaknesses but are typically unaware of emerging attacks. An Internet security system's zero-day attack prevention function finds and stops new attacks.

VPN, Firewall and Antivirus system

VPN stands for "Virtual Private Network" and refers to the ability to create a secure network connection when utilizing public networks. VPNs encrypt your internet traffic and conceal your identity online. This makes it more difficult for unauthorized parties to follow your internet activities and steal your information. Real-time encryption is implemented. Your data transmissions over the internet will be encrypted and concealed from any prying eyes by using a virtual private network connection (VPN). Data that has not been encrypted can be read by anybody who has access to the network and has the motivation to do so. Cybercriminals and hackers will be unable to interpret this data if you use a virtual private network (VPN) (Kaspersky, 2022).

The only way to decode data that has been encrypted securely is to use the appropriate encryption key. In the absence of one, it would take a computer million and millions of years to break the code if it attempted to do so by brute force. Using a virtual private network, or VPN, allows you to disguise your online activities even when connected to a public network. To hide your location, virtual private network servers act simply as internet-based proxies on your behalf. It is not feasible to determine your specific location since the demographic location data comes from a server in a different country. Furthermore, the vast majority of VPN service providers do not log user behaviour in any way. On the other hand, certain service providers will monitor your actions but will not disclose this information to any outside parties. This indicates that any possible record of your user behaviour will remain permanently disguised, and it will not be able to be accessed (Kaspersky, 2022).

A firewall is a type of network security device that can monitor both incoming and outgoing network traffic and decide whether or not to allow certain types of traffic based on a set of security rules that have been preset. Firewalls have been the primary security measure for networks for more than 25 years now, making them the first line of protection. They serve as a barrier between internal networks that can be relied on, are managed, and are kept safe, and external networks that cannot be relied on, such as the Internet. There are many different forms of firewalls, including hardware, software, SaaS, public cloud, and private cloud (virtual) (Cisco, 2022).

Antivirus software is a type of application that shields computers against malicious software such as viruses, computer worms, spyware, botnets, rootkits, and keyloggers. Antivirus software falls under the category of applications. The purpose of scanning, identifying, and removing computer viruses is the primary focus of antivirus software. On the market nowadays, you may choose from a wide selection of different kinds and variants of anti-virus software. On the other hand, the primary objective of an antivirus program is to protect computers and remove viruses after they have been found. The vast majority of anti-virus programs provide users with the option to filter data either automatically or manually. The option for doing a fast scan can investigate data obtained from the Internet, DVDs that have been inserted into the computer, and files produced by software installers. The automatic scanning method might also do a full scan of the hard disk on a daily basis. You have the capability, thanks to the manual scanning system, to scan individual documents or the whole network at any point in time that you feel it necessary (Comodo Security, 2022).

Oppressed group of people

Oppressed group of people needs and seeks a special protection from criminals or governments or any other entities (e.g., majority of society). For instance, such an oppressed group of people may be one of the following:

- Journalists and activists writing about current problems and issues in countries in which it may lead to their imprisonment or even execution,
- Journalists and activists informing about topics such as slavery, human-trafficking and such as (who are in need of protection against human-trafficking rings),
- LGBT, LGBT+ and similar communities around the World,
- Other oppressed groups people who are oppressed or deprived due to their gender, political views, identity, race, or due to any other reason(s).

The life of oppressed people is usually connected with dangers such as criminal or violence attack on such people or their families and close friends. They can be also be a subjects of exploitation or revenge from Mafias or Criminal gangs. There are many dangers which oppressed group of people face in daily life.

The role of oppressed group of people in global (World) society is crucial because they for example are mostly the only witnesses of wrongdoing in certain countries or they are investigating and discovering serious crime such as human trafficking or drug trafficking. Of course, one can become oppressed also only by only living their lives such as in LGBT community.

4. Details on Methodology

The methodology consists of data research and research on the internet. Also, methodology of synthesis and literature overview is used.

1. The step-by-step approach include the following steps:
2. Internet research on available solutions, taking in account reliability, protection and costs,
3. Drafting and proposing the use of recommended solutions taking in account protection and costs,
4. Setting up a manual on how to protect yourself – what to look out for if you are an oppressed or endangered group as explained in the introductory part of this article.

Once again, it is necessary to underline that this is an introductory article which is not to be complex, but on the other hand easy to understand and in an outcome to help the endangered and oppressed group of people in today's World.

5. Practical Part on Identity protection/hiding and Practical Manual

From the point of view of security and anonymous protection in online World from being targeted by criminal gangs, human-trafficking rings, mafias or government, oppressed group of people shall use at least certain level of software measurements on their computers or mobile phones. The package of basic necessary level of measurements includes for instance:

1. VPN

- Secure VPN with kill-switch function turned on (this does not allow any inbound and outbound connection which does not go via VPN),
- The VPN shall be reliable and hosted in democratic country such as Japan, EU Countries or the USA,
- To enhance security the double VPN may be used, but it is not necessary in this case,

2. Antivirus, Firewall

- It is also necessary to use antivirus system and firewall from a reputable company such as AVAST, AVG or Kaspersky – especially is Android and Microsoft Windows systems are used,

3. **Internet Browser**

- It is recommended to use up-to-date and reliable internet browsers such as Firefox, Chrome or Opera,
- In special cases it is recommended to use TOR (The Onion Router), but this may be very complicated due to law problems in the U.S.A and possible police investigation,
- The setting shall be done as follows: turn off history, do not allow website to track you (via cookies and such as) and install third party security measurements and extensions such as AdBlock to enhance privacy,
- Also do not store any personal data, passwords and such as in the browser, it is also best to auto-delete history and all the data on the web browsers exit.

4. **Offline Settings of Computer**

- It is also necessary to prepare computer and store sensitive data such as data and information in a secure way and use security measurement such as VeraCrypt (formerly TrueCrypt),
- Use strong password to create password-protected containers and also protect the access to the computer itself by password or by physical key (e.g., YubiKey).

5. **Use of separate devices – separate personal (normal) life and working life**

- For instance, journalists or activists working on sensitive topics (human trafficking, drugs…) shall use separate devices (e.g., second mobile phone or second laptop) to access, store and investigate the data,
- The reason for such is that the sensitive activities are clearly separated from personal use not only on the level of software (e.g., VPN, web browsers) but also on the level of hardware (second device) therefore the chance of mix personal and working profiles and communication protocols is restricted.

Respecting the five main aspects mentioned above, the solution for the secure and cost-effective measurements is drafted below. The author of this article did the research based on real data – psychically buying and testing the following solution(s). Therefore, all the aspects are mirroring the real-life experience bearing in mind the fact of price factor of maximum USD 150. User friendliness and ease-to-use of the measurements is taken in account as well.

The following table proposes and sum up the one of the solutions for protection if the oppressed group of people needs to access the internet for their work, communication or life (e.g., access to Facebook).

Table: possible solutions for on-line protection and privacy.

Type	Name of solution	Total Costs (USD, approx.)	Notes
Mobile Phone	Xiaomi Redmi 9T, 4GB RAM, 64 GB ROM, Fingerprint, 48 MPx Camera	78 USD	Secondary Device
SIM Card	New SIM Card (pre-paid)	2 USD	Anonymous, for receiving login codes for communication apps such as Line…
VPN	Fast VPN	35 USD	Enable Kill-switch, available for MS Windows and Android, all solutions (VPN and Antivirus) can be installed on MacOS, Windows, Android
Antivirus and Firewall	Comodo Antivirus and Firewall	29 USD	
Web Browser	Google Chrome	0 USD Freeware	
Web Browsers Extensions		0 USD Freeware	To enhance anonymity and
Security System	VeraCrypt	0 USD Freeware	Available for Windows, to create password-encrypted containers, can be used on main computer
Total	**-**	**144 USD**	**-**

Source: author, tested in real life in September-November 2022.

6. Conclusion

This article is an entry and introductory article for journalists, activists, oppressed group of people and other who needs to conceal, hide or protect their identity and actions on internet. Please, note that the usage of TOR (The Onion Router) and similar apps in this article is limited due to its more-advance nature. Main aim of this article is to assist the people such as journalists, underprivileged and oppressed groups of people in totalitarian states to reach the internet safely. This article is not a manual for using the hidden/protected identity on internet to do fraud, illegal or criminal actions. Malicious content may be downloaded via a website or sent as an email attachment.

Internet security solutions should monitor Internet traffic for sensitive and protected categories of data. Your data transmissions over the internet will be encrypted and concealed from prying eyes by using a virtual private network connection. Using a virtual private network, or VPN, allows you to disguise your online activities even when connected to a public network. The vast majority of VPN service providers do not log user behaviour in any way. Certain service providers will monitor your actions but will not disclose this information to outside parties.

Antivirus software is a type of application that shields computers against malicious software such as viruses, computer worms, spyware, botnets, rootkits, and keyloggers. The purpose of scanning, identifying, and removing computer viruses is the primary focus of antivirus software. The life of oppressed people is usually connected with dangers such as criminal or violence attack on such people or their families and close friends. They can be also imprisoned by governments or are in a danger from point of view of exploitation or revenge from Mafias or Criminal gangs. There are many dangers which oppressed group of people face in daily life.

Turn off history, do not allow website to track you (via cookies and such as) and install third party security measurements and extensions such as AdBlock. Use strong password to create password-protected containers and also protect the access to the computer itself by password or by physical key (e.g., YubiKey). The following table proposes and sum up the one of the solutions for protection if the oppressed group of people needs to access the internet for their work, communication or life (e.g., access to Facebook). Price factor of maximum USD 150 is taken in account as well as user friendliness and ease-to-use.

For detailed recommendations, measurements and entry-level manual, please see the chapter “4 Practical Part on Identity protection/hiding and Practical Manual”.

References

- Alatise, R., & Omobowale, A. (2022). Informal Islamic Education in Lagos State: From Pedagogy of the Oppressed to the Oppressed Pedagogy. Journal Title, 7, 154-177.
- Cisco (2022). What Is a Firewall [Online]. [Accessed 4.11.2022]. Available from: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html.
- Comodo Security (2022). Webpage [Online]. [Accessed 4.11.2022]. Available from: https://antivirus.comodo.com/security/define-antivirus.php.
- González-Scott (2022). Tools for Social Change: The Five Faces of Oppression [Online]. [Accessed 4.11.2022]. Available from: https://educationalequity.org/blog/tools-social-change-five-faces-oppression.
- Check Point (2022). What Is Internet Security [Online]. [Accessed 4.11.2022]. Available from: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-internet-security.
- Kaspersky (2022). What is VPN? How It Works, Types of VPN [Online]. [Accessed 4.11.2022]. Available from: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn.
- Quora (2022). Can the police track you if you are using TOR [Online]. [Accessed 4.11.2022]. Available from: https://www.quora.com/Can-the-police-track-you-if-you-are-using-TOR.