ONLINE SECURITY 101

one world platform

Page intentionally left blanc

ONLINE SECURITY 101

One World Platform
Sarajevo, Bosna i Hercegovina

https://oneworldplatform.net
https://zenskaposla.ba

info@oneworldplatform.net

Authors: Valida Hromadžić and Tina Lukežić
Graphic design and DTP: Denis Šparavalo Shpary

The handbook is part of the project "Strengthening of Online Security of Safe Houses" which was implemented by the Foundation "One World Platform" (OWP) in the period July-December 2017, with the financial support of the "Association for Progressive Communications" (APC).

one world platform

APC

Page intentionally left blanc

In 1993, the United Nations General Assembly adopted the Declaration on the Elimination of Violence Against Women (A / RES / 48/104). The Declaration defines violence against women as

"any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life."

What is Online Violence Against Women?

When we talk about online violence against women, or violence related to technologies, i.e. ICTs (Information and Communication Technologies), it includes acts of gender-based violence that have been committed, abetted or aggravated, in part or fully, by the use of ICTs, such as phones, the Internet, social media platforms and email. Technology-related violence against women is part of the same continuum as violence against women in the physical (offline) space.

In the physical space, in the streets and in homes, girls and women are faced with certain risks. In the online space, they are faced with online harassment, cyber stalking, invasion of privacy, with blackmail threats, viral "rape videos", which is specific to young girls, distributing of 'sex videos' that force survivors to relive the trauma of sexual assaults every time they are published online, via mobile phones, or distributed in other ways.

Cyber Stalking includes, but is not limited to:

- Harassment, humiliation and disgrace of the person concerned
- • Disturbing of family, friends and employers of the person in question for the purpose of their isolation
- Tactics to intimidate the person concerned
- Takeover of another person's identity
- Tracking a person (e.g. using Facebook/Viber notifications to find out the person's location, using tracking software, activating the GPS/location of the person which is to be followed)

Online violence against women is not a new form of violence, but the channel of violence is new. Violence against women, which is technology-related violates women's right to self-determination and bodily integrity. This causes mental and emotional damage, intensifies prejudices, harms reputation, causes economic losses, and creates obstacles to public participation, and can lead to sexual and other forms of physical violence.

ICTs have a variety of features that make them an appropriate tool for abuse. As abuse is done from a distance, the identification and the possibility to take action against the abuser/disturber becomes much more difficult.

Today, every person by only using a mobile phone can download and publish pictures and videos of another person, and they can replicate it countless times at no cost.

In most cases, people do not know what to do in order to protect themselves from such violations of rights. Telecommunication companies, Internet providers and developers must protect customer privacy and security. Governments must provide laws and policies in response to this relatively new form of violence against women.

How non-physical violence can be harmful?

Psychological violence is recognized as a form of violence and is clearly defined within international law as a violation of human rights. Damage caused by technology-related violence involves emotional and psychological damage, personal reputation damage, physical damage, and invasion of privacy, loss of identity, movement restriction, censorship as well as property loss. These forms of violence affect the ability of a woman to move freely without fear of being watched.

By mapping cases of online violence in the "Take Back the Tech!" online map (a project that is implemented by the "Association for Progressive Communications") it is evident that 3 categories of women are most exposed to online violence:

- Women in an intimate relationship whose partner had become abusive;
- Women who survived physical assault - often from intimate partner abuse or rape;
- Women in public life, i.e. those whose public profiles are involved in public communication (e.g. writers, researchers, activists and artists).

Use of technology and domestic violence

Like all forms of violence against women, online violence is also being carried out by people who know survivor. When it comes to violence against women that is connected to technologies and which is done in the context of domestic violence, women are exposed to physical beating and/or sexual abuse, followed by an insult, intimidation, or violence SMS, phone calls or emails. In some other cases, after the end of an intimate relationship, private and intimate photos, and women's videos are being published on the internet for the purpose of revenge and intimidation. In some cases, violence begins online and is transmitted to physical space. For example, a woman is initially threatened by a mobile phone, an act of violence that escalates into rape over time.

What is 'revenge porn'?

'Revenge porn' is a gross violation of a woman's privacy. These are cases where private and sexually explicit videos and photographic images are publicly disclosed without explicit permission and consent of the person being shot. These videos and photos are placed on different websites for the purposes of extortion, blackmail and/or humiliation. This term describes an act of violence and should not to be conflated with pornographic content. In cases of 'revenge porn' it is revenge (mostly to women) because of refusal of marriage proposal or termination of the relationship for any reason.

Violence against women and social media platforms

The most common forms of violence against women taking place in social media platforms are:

- Creation of false profiles of women, often to be defamed, discredited and with the aim of ruining reputation
- Spreading private and/or sexually explicit photos/videos with the aim of causing harm and/or blackmail
- Pages, comments, posts, and the like that are directed towards gender-based hatred (misogynistic slurs, death threats, threats of sexual violence, etc.)
- Publishing personal information about women, including names, addresses, phone numbers, and email addresses without the consent of women.

Strategies for protection of your online privacy

Protection of personal data on a computer

We store a lot of information on computers and phones about who we are and what we are doing. It does not hurt to be aware of a few things that can protect your personal information on the computer/phone which you are using.

Think first what or who you are protecting and from what. Answers may range from random virus attacks to the spyware (basically annoying programs that show up on your computer without your permission and gather information from it) to people who have physical access to your computer. Below are some of the concrete steps to address these and other potential threats.

Protecting your data, identity and computer

- Create a guest-user profile on your computer and allow other people to use the computer with that user profile. In this way you keep other people away from your files and data
- Protect folders and documents containing sensitive information with password
- Always be careful when giving your personal information (e.g. your name, address, phone number, etc.) when using the Internet
- Websites generally have privacy agreements if they search for your personal information. Read these agreements and find out how they intend to use your information in cases where they share them with a third party, etc.
- Always have a trusted antivirus program installed. One which regularly updates its databases so that it can track the latest viruses that infect the Internet. Set your computer to check your computer on a daily basis
- Make sure that the anti-virus automatically checks for incoming mails and downloads
- Never open attachments unless you are completely sure that the document is not infected
- When using a USB drive that is used on another computer, run an anti-virus program on it to make sure it is 'clean'.

Identity Theft – Phishing

Where is your personal account information being stolen?

Have you ever 'lost' your Yahoo! email account? Have you ever wondered how someone succeeds in getting your contact information that should be password protected?

One of the methods is known as “phishing”. This is when you are asked to provide confidential information such as passwords or other account details through fake emails or instant messaging or even by phone.

Sometimes such email can look very convincing with official logos and internet addresses or URLs that seem to be authentic, but in fact contains little differences that will lead you to the phishing website. For example, deliberately misplaced words that can be overlooked, or placing text with a valid URL address, but a real active link leads you to something else, etc. When you find yourself on such fake sites, any details you submit are stored by fraudster(s). In Yahoo!'s example, your actual friend’s account can be “phished” and then his stolen identity used to contact other people in his list and thus spread of the fraudulent data collection continues.

- Usually, the aim of identity theft is directed at financial risk and loss, where bank data are inadvertently sent to fraudulent sites, etc. However, through violation of personal communications and privacy rights, 'phishing' can also cause great damage to social relationships from online to offline area and can result in emotional and psychological trauma.

Basic tips for online chat

- Do not use the "automatically remember your password" option. If you use this option, it means that everyone who uses your computer will be able to log on to your communication service (or social platform) using your username and password.
- If you decide to activate the option to archive your online conversations, be sure to keep the archive on your disk so that you can delete it if necessary or move it to another (safer) storage device.

Smartphones

- Consider locking your phone with a password as a way to keep all your data in the phone private in case you lose your phone or it gets stolen.

- If you get disturbing messages, do not delete them. They can be an important proof if you have to provide documentation to the police or the provider of telephone services. If you receive disturbing phone calls, make sure your phone has the ability to record calls to have a digital record of someone who disturbs you.

Passwords/codes

This can be a tedious job, but good practice of making secure passwords/codes is essential for maintaining secure devices and data. You can install software to create strong passwords/codes and keep all passwords/codes in one convenient and secure database.

For this purpose, a good and tested tool is KeePass (KeePassX) (https://www.keepassx.org/) that works on all operating systems. There is also a variant for mobile phones Keepass2Android (https://play.google.com/store/apps/details?id=keepass2android.keepass2android&hl=en)

Digital security is needed for all people who use the Internet and share their data. It is vitally important that individuals, who share their information online, save their data and identity. A few basic tips for protection of online data:

- When using any of the digital platforms, make sure that you fully understand the terms of use, in order to understand the implications of creating and sharing content in the space
- If possible, use an anonymous email address when creating and setting up your account or profile
- Do not share personal information in the digital space that would not make you feel comfortable if they were followed or they appear in other locations if your account or website were hacked
- Report any harassment to site administrators and continue to make sure that they do something about it

Services and their settings

About Gmail settings

While using Google services, e.g. search through Google, search through Google Maps, or watch videos via YouTube, Google collects data that may include:

- Terms you search for
- Websites you visit
- Videos you watch
- Ads you click on
- Your location
- Device information
- IP address and cookie data

Google and the content you create

If you are signed in with your Google Account, Google stores and protects what you create by using Google services. This includes:

- Terms you search for
- Websites you visit
- Videos you watch
- Ads you click on
- Your location
- Device information
- IP address and cookie data

When you create a Google account, Google keeps your basic data that you give them. This can include your:

- Name
- Email address and password
- Date of birth
- Gender
- Phone number
- Country

In the "My Account" section (myaccount.google.com) you can find the tools/ settings where you can manage your privacy and information. In Activity Controls, you can adjust which data Google collects about you, including

Search, YouTube, and location related activities.

In the "Ads Settings" section, you can adjust the settings that control the ads that are displayed to you, and which are shown in accordance with your interests and terms you have searched for.

Facebook settings

Get to know the personal profile settings of Facebook. Click on “▼” in the top right corner (next to the question mark).
In the "Security & Login" section, you have the insight and overview of the devices you are signed in to on Facebook. If you do not recognize any of the listed devices, be sure to take the steps to remove that device.

In the "Login" section, you have the options to change the password.
In the "Setting Up Extra Security" subsection, you can set the settings so that you receive alerts on unknown logins to your account/profile. Make sure this option is turned on.

Here, you also have the option of using double authentication.
In the "Privacy" section, you can control who can see your future postings, how others can find you and get in touch with you.

In the “Blocking” section, you can control blocking whether it is the case of people/users, messages, apps, events, and pages.

Instagram settings

Instagram is one of the easiest applications to use. In order to protect your privacy and personal information, the basic step you have to perform is to choose a private profile option. Private profile on Instagram means that no one can access your profile or published content (which includes your photos and 'stories' i.e. stories that are deleted after 24 hours) unless you have accepted him/her as your friend. Of course, we recommend that you accept as your friends only those persons who you know personally. Also, it is advisable not to insert your full name or surname as Instagram name, but to figure out a nickname. If you want to be completely protected, it's preferable not to post an image with the location shown at the time you are at that location, but a few hours after you have left. Other personal information such as your address, phone number, your business address, and the like should not be disclosed publicly through published images, videos, and comments.

When you create your own Instagram profile, find, next to the profile editing option, and press the round button for all the settings. Among other things, you'll find account settings, the second one in a row, where you can choose a private account option, have a view of the photos of other users in which you are shown, view of the publications for which you have clicked the "like" button, and the list of those Instagram users who you have decided to block.

Internet Browsing

The Internet and WorldWideWeb are not the same. The Internet is a massive network of networks, a network infrastructure. It connects millions of computers globally, making a network in which every computer can communicate with another computer, as long as both are connected to the Internet. WorldWideWeb is a way of accessing information over the Internet.

Whether you are searching the Internet on a private, business or other computer, it would be good to take into account how safe a certain search engine is, how it collects information about you and how much of your activity it tracks.

For starters, check your browser's security through Panopticklick (https://panopticlick.eff.org/).

Regardless of the browser you use, check the default settings.

For Chrome:
> Settings > Show Advanced Settings
> Privacy > Send "Do Not Track" request with your browser traffic

For Firefox:
Tools > Options > Privacy & Security > Tracking Protection. In this section of the settings, choose the options that you think suits you:

- Always
- Only in private window
- Never

That is, send websites a "Do Not Track" signal that you don’t want to be tracked, depending on the version.

- Only when using Tracking Protection
- Always

Malwares and antiviruses

Malware is an abbreviation of malicious software designed to harm the computer system (e.g. data erasure). Modern malwares are designed to go unnoticed while performing undesirable actions in the background of the system (steal of sensitive data, allowing remote control over user's remote computer for the purpose of using that computer to perform further malicious attacks). Malwares exploits the gaps in the programmes/software itself. In essence, malwares exploit the failures in the user operating system or programs they use. Below are some of the most common types of malware.

a. A Trojan horse is a file that looks like an ordinary file (.jpg, .doc) but is actually a program that contains a malicious code or a code that causes damage. It is often used to create a "backdoor" so that the perpetrator of this malicious action can infiltrate into a computer, tablet or smart phone and launch additional remote operations. Most Trojans are supposed to take control over someone's computer, steal data, and put other malicious programs on the victim's computer. Such actions can cause different types of damage: interception of protected data, it can record i.e. record typing on the keyboard so that inserted codes can be used to steal personal information, download of other malicious programs, and launch of DoS (Denial-of-Service) attacks. Trojans do not have the ability to replicate and infiltrate other files, nor can they be self-replicated. Trojans must be activated by the user (often by opening corrupt e-mail attachments or by downloading files, so that they are triggered due to the user's negligence. Some types of Trojans, as previously mentioned, create a "back door", others intercept Skype and other VoIP (Voice over Internet Protocol) calls, capture audio or video calls that are forwarded to the attacker.

b. Viruses are a type of malicious software, designed to spread from one computer to another (just like flu viruses), causing damage to files and other programs. These are computer codes that self-replicate and modify other legitimate files and programs. They are often located in .exe files (files that run the program installer) in order to insert a code that allows further replication. It is exactly the self-replication that separates viruses from other malicious software. Viruses can be on the computer for some time, without doing any damage, until the moment the user starts or opens the file. Once your computer is infected with a virus, other computers on the same network may be infected. It can also be spread by clicking an attachment or sharing a USB drive with other people/computers so that it has the ability to spread via USB drives, Bluetooth, wireless network, 3G network, or through fake websites and links. As mentioned, its aim is to steal passwords or data, data you insert with keyboard, file corruption, spamming of your email contacts, or even taking control of your computer. Even your mobile devices can be infected with a virus. If you let's say download applications that are not from proven sources, or from verified creators. Viruses can be hidden in content attachments that are shared via social networks, such as funny photos, greeting cards, or audio and video files.

c. Worms are similar to viruses. They spread from one computer to another, however, the worm can be self-replicated and expanded into countless copies even though it was not activated by the user. Unlike viruses, worm does not need a program on which to "lock" and activate and duplicate. Once a worm enters a computer system, usually through a network connection or a downloaded file, it can be copied and spread through a network or Internet connection, by further infecting inadequately protected computers. As each copy of a worm can be further self-replicated, the speed with which it continues to spread is very fast. Worms exploit a large amount of system memory or bandwidth. Worm can be 'embedded' in a page and in such way infect the user, i.e. computer. Worms can, among other things, erase the files, open and close communication ports in order to hinder the traffic.

Antivirus software

Antiviruses are software that try to prevent malicious software (malwares) from taking over your device, i.e. they try to protect you from them. Viruses are the most widespread form of malware. Today's antivirus software warns you when you try to download suspicious files from external sources, and check the files on your computer and compare them with what the malware should look like.

An antivirus program can detect those malwares that are basically similar to examples which the antivirus program developer's have already analyzed. Some advanced malwares can attack or bypass an antivirus program.

Among recomended free antivirus softwares are Avast, Bitdefender and Avira

Some of the common terms:

ISP — Internet Service Provider

An Internet Service Provider is a company providing Internet access and usage services to its users.

Internet service providers can be organized in various forms, as a commercial, private or non-profit organization.

IP Address

The IP address is a unique address that identifies the device on the Internet or on a local network. It allows the system to be recognized by other systems over the Internet protocol. There are two primary types of IP address formats used today - IPv4 and IPv6.

IP - Internet Protocol

The Internet Protocol provides a standard set of rules for sending and receiving data over the Internet. This enables devices operating on different platforms to communicate with each other as long as they are connected to the Internet.

The Internet Protocol also provides basic instructions for "packet" transfer between devices. The Internet Protocol does not establish a connection and does not define packet management between devices. These aspects are managed by the "Transmission Control Protocol", which works in co-operation with the Internet Protocol on data transfer between systems on the Internet. Because of this, connections between systems connected to the Internet are often called "TCP/IP" connections.

Metapodaci (metadata)

Metadata is information that is created when you make a phone call or when you create an email:

- Phone numbers and locations of the caller and the recipient of the call
- Call time and call duration
- Serial numbers of phones

- Email addresses
- Time and location to which the email was sent
- Subject line

Metadata is also included in photos, videos, pdf and word documents and include:

- The time and date when the document was created
- The username of the person who created and edited the document
- Information about the device that created the document, photo, or video

Cookies

‘Cookie is a piece of information in the form of a very small text file that is stored on a user's hard drive. In some search engines, a cookie is a small file, and in some, like Firefox, all cookies are stored in one file.

It is created by the web servers (the computer that manages the web page). The information that the cookie contains is determined by the server and the server uses them whenever a user visits the site. Cookie can be viewed as a kind of ID card that tells the website when the user has returned to the page.

Cookies often store your browser settings, such as your choice of language or location. Also, cookies can store a wide range of information that includes information through which the user can be identified (such as name, home address, email address, or phone number).

The purpose of the cookie is to speed up the interaction between the user and the web site and to allow the web pages to follow the surfing habits of the user and to accordingly create profiles for marketing purposes.

To manage cookies, visit your browser settings.
For Chrome (chrome://settings/content/cookies).
For Firefox (about:preferences#privacy).
For Opera (Menu-Settings-Privacy and Security).

New private/incognito window

Chrome - New incognito window
A new incognito window prevents Chrome from keeping track of what you are visiting and downloading.

Note: You are still very visible on the web, only Chrome in this case “does not record” what you visit and download. The people with whom you share your computer in this case will not be able to track your activity through the search engine, but the bookmarks and downloads will be saved. Chrome claims that the following information will not be saved: your search history, cookies and site data, as well as the information you entered in certain fields or forms. Your activities may still be visible to the websites you visit, your employer or school, and your internet service provider.

Firefox - New private window
This option allows you to search without saving information about which pages you are visiting.

As with Chrome, this search option does not make you anonymous, it only prevents Firefox from keeping track of what you are visiting and downloading.

Sources used and adapted for making this material:

https://tacticaltech.org/

https://securityinabox.org/en/

https://www.genderit.org/onlinevaw/faq/

https://www.takebackthetech.net/know-more

https://techterms.com/

https://www.aboutcookies.org/

https://www.eff.org/

https://panopticlick.eff.org/

https://us.norton.com/

https://www.kaspersky.com/

https://myaccount.google.com

https://privacy.google.com

Feminist Principles of the Internet 2.0

Preamble of the feminist Internet works towards empowering more women and queer persons - in all our diversities – in order to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy. It contributes to the integration of our different realities, contexts and specificities - including age, disabilities, sexualities, gender identities and expressions, socioeconomic locations, political and religious beliefs, ethnic origins, and racial markers. The following key principles are critical towards realising a feminist internet.

Access

1. **Access to the internet** — A feminist internet aims at enabling more women and queer persons to enjoy universal, acceptable, affordable, unconditional, open, meaningful and equal access to the internet.
2. **Access to information** — We support and protect unrestricted access to information relevant to women and queer persons, particularly information on sexual and reproductive health and rights, pleasure, safe abortion, access to justice, and LGBTIQ issues. This includes diversity in languages, abilities, interests and contexts.
3. **Usage of technology** — Women and queer persons have the right to code, design, adapt and sustainably use ICTs and reclaim technology as a platform for creativity and expression, as well as to challenge the cultures of sexism and discrimination in all spaces.

Movements and public participation

4. **Resistance** — The internet is a space where social norms are negotiated, performed and imposed, often as an extension of other spaces shaped by patriarchy and heteronormativity. Our struggle for a feminist internet is one that forms part of a continuum of our resistance in other spaces, public, private and in-between.
5. **Transformative space** — The internet is a transformative political space. It facilitates development of new forms of citizenship that enable individuals to claim, construct and express selves, genders and sexualities. This includes connecting across territories, demanding accountability and transparency, and creating opportunities for sustained feminist movement building.
6. **Decision making in internet governance** — We believe in challenging and provoking the patriarchal spaces and processes that control internet governance, as well as putting more feminists and queers at the decision-making

forums. We want to democratise policy making affecting the internet as well as diffuse ownership of and power in global and local networks.

Economy

7. **Alternative economies** — We are committed to interrogating the capitalist logic that drives technology towards further privatisation, profit and corporate control. We work to create alternative forms of economic power that are grounded in the principles of cooperation, solidarity, commons, environmental sustainability, and openness.
8. **Free and open source code** — We are committed to creating and experimenting with them, including digital safety and security, and using tools, platforms and free and open source software (FLOSS). Promoting, disseminating, and sharing knowledge about the use of FLOSS is a central element of our praxis.

Expression

9. **Amplifying feminist discourse** — We claim the power of the internet to amplify women's narratives and lived realities. There is a need to resist the state, the religious right and other extremist forces that monopolise discourses of moral and morality, while silencing feminist voices and persecuting women's human rights defenders.
10. **Freedom of expression** — We defend the right to sexual expression as a freedom of expression issue of no less importance than political or religious expression. We strongly object to the efforts of state and non-state actors to control, surveil, regulate and restrict feminist and queer expression on the internet through technology, legislation or violence. We recognise this as part of the larger political project of moral policing, censorship, and hierarchisation of citizenship and rights.
11. **Pornography and "harmful content"** — We recognise that the issue of online pornography has to do with agency, consent, power and labour. We reject simple causal linkages made between consumption of pornographic content and violence against women. We also reject the use of the umbrella term "harmful content" to label expression on female and transgender sexuality. We support reclaiming and creating alternative erotic content that resists the mainstream patriarchal gaze and locates women and queer persons' desires at the centre. We support the acquisition of control over alternative erotic content and its creation in a way that is opposed to the dominant patriarchal view and which places women and queer persons' desires at the centre.

Agency

12. **Consent** — We call on the need to build an ethics and politics of consent into the culture, design, policies and terms of service of internet platforms. Women's agency lies in their ability to make informed decisions on what aspects of their public or private lives to share online.
13. **Privacy and data** — We support the right to privacy and to full control over personal data and information online at all levels. We reject practices by states and private companies to use data for profit and to manipulate behaviour online. Monitoring and surveillance are tools which patriarchy used through history in order to control and restrict women's bodies, speech and activism. We pay equal attention to surveillance practices by individuals, the private sector, the state and non-state actors.
14. **Children and youth** — We call for the inclusion of the voices and experiences of young people in the decisions made about safety and security online and promote their safety, privacy, and access to information. We recognise children's right to healthy emotional and sexual development, which includes the right to privacy and access to positive information about sex, gender and sexuality at critical times in their lives.
15. **Anonymity** — We defend the right to be anonymous and reject all claims to restrict anonymity online. Anonymity enables our freedom of expression online, particularly when it comes to breaking taboos of sexuality and heteronormativity, experimenting with gender identity, and enabling safety for women and queer persons affected by discrimination
16. **Memory** — We have the right to exercise and retain control over our personal history and memory on the internet. This includes being able to access all our personal data and information online, and to be able to exercise control over this data, including knowing who has access to it and under what conditions, and the ability to delete it forever.
17. **Online violence** — We call on all internet stakeholders, including internet users, policy makers and the private sector, to address the issue of online harassment and technology-related violence. The attacks, threats, intimidation and policing experienced by women and queers are real, harmful and alarming, and are part of the broader issue of gender-based violence. It is our collective responsibility to address and end this forever.

Page intentionally left blanc

Contents