CYBER SECURITY MANUAL

TABLE OF CONTENTS

ABOUT THIS MANUAL

There is a growing number of sex workers in our region who now use dating sites, escort sites, smartphone apps, and social media platforms for work and for activism.

The Internet can provide increased freedom, safety, and opportunities for sex workers. It can enable us to work for ourselves, to make informed decisions and to build community. It gives us a space to exchange sexual health and safety information, general advice, and support each other during crisis. However, it also brings new threats and challenges.

As internet use increases, stigma and violence remain very high, and we are also seeing it used as a weapon by clients, police, and the state. Blackmail, doxxing and digital attacks against sex workers are now unfortunately commonplace, with results that in some cases have even been life-threatening. In countries with authoritarian regimes where online surveillance is used against its citizens, the threat to both sex workers and activists is very real. There is a great need to come together and assess our shared experiences, risks and the measures we can take as a community to protect ourselves.

This guide is a summary of four online trainings run by SWAN during the summer of 2022, in which sex workers and activists had a chance to bring their questions to a consultant on digital security, share their experiences, needs, and problems with the goal to help improve their digital literacy, assess online risk levels and areas of vulnerability and learn some simple methods to protect themselves online.

In this manual you will find security tips for on the most commonly used online platforms, smartphone apps, and assets such as phones and computers. We hope it can be of use to you and your communities and that this resource will be a step towards more accessible online safety tools built by and for sex workers in our region.

ASSETS

STEP 1 Try to think what are the assets that you have

An asset is anything that you have and use in your private or work life. It includes devices (notebooks, computers, smartphones), documents (passport, driving licence, work contract) and accounts (e-mail accounts, messengers, banking services). Assets can make an endless list, and this list will be unique for each an everyone of you; only you can know which assets you have.

List all your assets on a piece of paper or in a Word document.

STEP 2 What can happen to your assets?

Try to think what negative events can take place in relation to each of your assets.

For example, your email account can be hacked, people can gain access to your correspondence or write something from your address. Notebook can be stolen, lost, broken, or you can simply spill water over it.

Go through the list of your assets and write all the possible negative events that can take place in relation to them. These events will be your risks.

STEP 3 How to prevent risks?

Try to answer the following questions for each of the risks you have identified:

- What can you do to prevent the risk? Which measures can be taken so that the risk would not take place or so that the risk is minimal?
- How can we mitigate the risk? What shall we do in advance so that in case the risk does take place the impact is minimal?
- What shall we do when risk will have happened? If the risk does take place, what shall we do right after it happens to minimize the harm?

STEP 4 Let's see an example

One of my assets is my Facebook account. What can possibly happen to it?

- I can lose access to my account if I forget my password.
- It can get hacked.
- It can get blocked due to a massive bot attack reporting my Facebook posts.

I will answer the questions above in relation to the risk "Facebook account was hacked".

- What can you do to prevent the risk? Which measures can be taken so that the risk would not take place or so that the risk is minimal?
    - I should protect my account. I can install two-factor authentication, and use complicated unique password.
- How can we mitigate the risk? What shall we do in advance so that in case the risk does take place the impact is minimal?
    - I should not have no important communications on Facebook.

- What shall we do when risk will have happened? If the risk does take place, what shall we do right after it happens to minimize the harm?
    - I should inform my friends that my account was hacked.
    - I should attempt to restore access to my account through technical support.
    - If you had some confidential correspondence on Facebook you should inform your communication partner about the incident using alternative communication channels. S/he might be able to delete your correspondence before the hacker reads it.

TYPES OF ATTACKS

STEP 1 Phishing

Phishing is something like finishing with a bait. You are the fish. The goal is to get your personal data, login names and passwords.

Phishing letters are usually attractive and emotional. I single out three types of the phishing letters:

1. Threat to your account

Such a letter contains explicit references to the threats to your account, and may look as follows: “Your account was hacked, if you want to protect it follow the link”.

The link usually takes you to a copy of the sight where you presumably have a hacked account, the URL of the website however will be different. Instead of google.com you may see an URL which looks something like google.com.this.site.is.real.novirusesthere.com. The domain name in this case is not google.com, but the "novirusthere", and all the things that precede it in the URL are subdomains, which you can manufacture on any site naming them any way you want.

Do not click on the link provided in such letters, go directly to the website which has the presumably hacked account of yours. Open your account, check the login history and security actions history. If something raises your suspicions, change your password. However, if upon having entered your presumably hacked account you see no notifications, my congratulations! You have just avoided a phishing attack.

2. You have won a million dollars!

The aim of such latter is normally to steal your money. In some cases, you might be asked to pay taxes, to put down a security payment or pay a commission -- it may come in many forms. If you haven't bought a lottery ticket, it is doubtful you could win it. So, let's not discuss these types of letters in any more detail.

3. Working email with an attachment

You may receive a credibly looking letter which has some sort of unpaid bill, a document or in fact anything, attached to it. The letter might look legitimate, but you most probably do not remember the sender. In this case, the attachment might contain a virus.

Scrutinize not just the icon of the attached file, but also its name. If the file has an extension .exe, .msi, .vbs, .reg, or .dll it might be harmful for your computer.

If the file looks realistic, try to preview it (Gmail, for example, will allow you to do that with almost all types of documents).

If you nonetheless need to download and open the file, and the file extension looks safe, try to put it through an antivirus first. One of the possible options is to use the online antivirus VirusTotal. Upload your file to this page, and it will be scanned by a number of antivirus programs.

STEP 2 Viruses

Viruses are one of the most common types of attacks. Many of you have faced them in one way or another. Viruses use different methods to harm your computer system. Some viruses encode your files, while the others take over control over your computer, yet others quietly spy on everything you do.

How do we contract a virus?

1. We can download it with an attachment to a letter. We have discussed this situation above.
2. We can get it in a messenger. While using messengers we should follow the same security guidelines like for an email.
3. We can install it together with a pirate software. Downloading pirate software, you are consenting to starting a virus which will hack the program you need. What will the hacker program do next? Will it just hack the software, or will it get installed in your system? I do not have an answer here, and for this reason I always recommend using only licenced software.
4. We can get a virus with a flash drive. You may find the drive on the street or receive it from a trusted person, but irrespective of where you got it from scan each flash drive that you connect to your computer with an antivirus. After you connect a flash drive to your computer, the operation system will offer you a number of options: to open the File Explorer, format the drive or autorun it. Never go for the autorun as the autorun programme might have a virus hidden in it. Open your flash drive using the File Explorer, and then research the files.

How can we protect ourselves from the viruses?

Install an antivirus and update it on the regular basis. Never use pirate antiviruses; if you do not feel like buying any of them, simply turn on the Windows Defender.

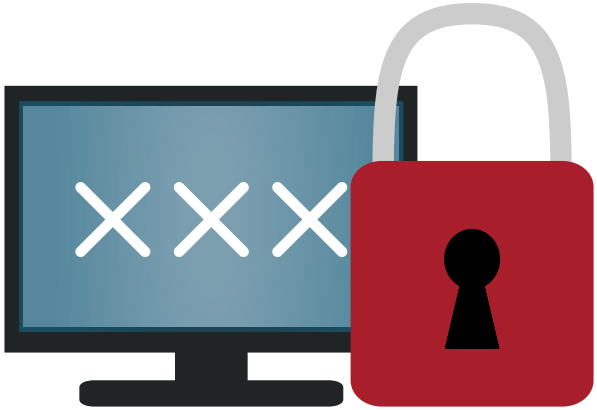
STEP 3 Remote attacks using zero-day vulnerability

Such attacks are normally targeted against concrete people and have very concrete goal. Civic activists, prominent politicians, celebrities -- many of them became victims of these attacks. Most probably, you will never face such attack. However, if you believe that you risk level is such that there can be direct attacks against you, you should seek a consultation of the cybersecurity specialist. One of the options is to approach the author of these guidelines Henry Demjanovich, his contacts are provided on the last page of the document.

ACCOUNTS' PROTECTION

STEP 1 Which accounts do we need to protect?

It makes sense to protect all of your accounts as much as you can. These include both personal and work accounts. It makes sense to separate your personal accounts from the work accounts and to come up with different passwords for them.



STEP 2 Password

Secure password has several characteristics:

- It is long (no less than 8 characters)
- It is varied (it includes upper-case and lower-case letter, numbers).
- It is unique (use different passwords for different websites).
- Can not be connected to you (never use your date of birth nickname, the nickname of your dog, etc. as password).

Currently, there is no need to change the passwords on the regular basis. The password should be changed only in case when it could be compromised, or someone could learn it.

STEP 3 Storing your passwords

You already know that you should use a unique password for each website you access, but it is almost impossible to memorize all your unique passwords. What shall we do in the case? We should use password manager.

If you use an iPhone, you might have come across the pre-installed password manager which offers to save passwords to applications and websites and can generate complicated passwords for registration.

If you prefer Android, then you should have seen Google Smart Lock.

Apart from that, all popular browsers offer you an option to have your password stored.

Finally, there are special password managers which allow to store all passwords in one application and access them from any device. I personally use BitWarden.

As you can see, there is a number of ways of storing your passwords, and you can go for either of them. Any of those methods is better than trying to memorize all your passwords.

If, however, you decided to opt for memorizing your passwords, try to use 2 or even better 3 different passwords:
1 main password for your personal life, personal email, and banking services 2 – for your work, working accounts and websites. 3 – for "garbage" websites where you need to register for one not very important action, for example for downloading an e-book.

STEP 4 Two-factor authentication

Many websites allow you to set a two-factor authentication. Sometimes it is also called a two-step verification. The first factor in this process is your password. The second factor can be something from the list below:

- Pop-up notification "You are entering your account, confirm your identity".
- One time SMS-code,
- OTP code from an application called Google Authenticator (or a similar application).
- USB-key (looks like a flash-drive)
- Back-up codes (those are generated as a second factor as soon as you have set up any other factor).

You can select any of the factors which looks most appealing to you, but before making a decision you should know their peculiarities.

Pop-up notifications will be available only on the smartphones where you have logged into you account. This method works with Google, Facebook, and some other accounts. The majority of websites and applications do not support this method.

SMS-code is a standard second factor supported by the majority of services. However, you have to understand that the SMS can be captured. And if the goal of the perpetrator is to hack your account specifically, especially if the perpetrator is the state, the SMS code will not protect you.

OTP-keys are perhaps the most wide-spread and reliable method of the two-factor authentication. You can use any of the multiple applications that are available for generating keys, just remember that the standard Google Authenticator does not allow you to back up

your access codes. It means, that if you delete the Google Authenticator from your phone by mistake or lose access to your phone, you will also lose access to your accounts. To avoid this, I use Aegis. This application allows to back up your codes, to protect the back-up copy with password, and the access to the codes is also reliably protected.

USB-key – is a great method entering your account. Microsoft suggests giving up passwords in favour of the USB-key. The key can be used both with your computer and your smartphone. There are also wireless NFC codes. The key is special because it exists in one physical copy, and to access your account one has to have it at hand. If your key is securely stored, nobody will be able to access your account even if they have password. But it also means that you will not be able to access your account either unless you have the key at hand.

Back-up codes are the last resort and can save you in a critical situation. Back-up codes should be printed out and stored in a safe place. At some point when you lose access to your second factor and you need to restore access to your account, they can save you.

Secure password and two-factor authentication are a crucial for the security of your accounts.

STEP 5 Passwordless accounts

Some websites and applications can be accessed without a password. You can access them using your Google or Facebook accounts. In this case, you can log in using virtually one button. The danger of such access is that you may unwillingly pass more information to the website than was requested. Scrutinize the list of accesses requested by the website if you use your Google or Facebook accounts. Normally, the website will receive your name, your e-mail, possibly you profile picture or even the date of birth. If the website requests more information, you might contemplate how reliable it is.

In general, using Google or Facebook accounts to access other websites is more secure than getting a password protected account for that website. Because this way you will have to protect only your Google or Facebook account, you do not need to protect all accounts on all websites.

PROTECTING YOUR NOTEBOOK

STEP 1 Setting up password

The password which protects access to your notebook will protect you from other people accessing your data for a short time the notebook is left unattended. If you leave your notebook unattended for 5 minutes, someone might access it and quickly look up some data, for example, your browsing history.

The password will not protect you in case your notebook gets stolen, or in case people have more time to gain access to your data.

STEP 2 Using BitLocker encoding

To protect all information on your notebook you can set up a BitLocker. BitLocker is accessible for Por versions of Windows 7,8, 8.1 and 10.

Older notebooks will require you to come up with a password that you will need to ender in addition to your system password. This is not needed for the newer notebooks.

While setting up the BitLocker, the system will offer you to save or print a back-up key. Save this key by all means. There might be a case when this key will help you to restore access to all your files.

STEP 3 Turning on Windows Defender

Recently, viruses do not attack regular users, but they still exist, and they are still dangerous. Windows Defender is a good antivirus built into the system. It will suffice to provide standard protection from the standard threats. In the majority of cases, it makes no sense to buy an antivirus or to use the free one; what is more none of them will be so deeply integrated into the system as the Defender.

STEP 4 Check privacy settings

Windows 10 provides a quality protection of our privacy. You can see which applications accessed your camera or your microphone. You can also easily learn if there is a program or an undetected virus spying on you. To do that go to Setting> Privacy and select Microphone or Camera in the menu on the left side. You will see all the Windows store applications which are allowed access to your camera and microphone. Below you will see all the applications (including those which did not come from the store) which accessed your camera or your microphone. If you notice something that should not be there, it is a good reason to approach a cybersecurity specialist for a consultation. It can be that someone one spying on you using your camera or your phone.

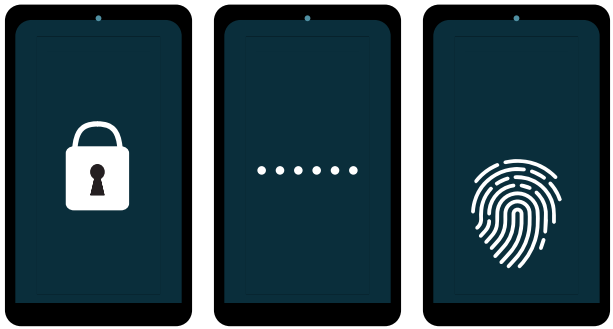
There are also things that are important to know about the work of your camera. If your notebook has an indicator for the camera being on, and this indicator is not broken (in other words, it is on when your camera is in use), you can be sure that nobody is spying on you. Currently there are no possibilities of accessing the notebook camera without turning the indicator on. It will always be on when you use your camera unless it breaks down completely.

PROTECTING YOUR SMARTPHONE

STEP 1 Setting up a sign-on password and PIN-code

Do not use patter lock for signing on, as this is the most insecure method of doing so. It can be snooped, guessed, or restored based on the finger trances on the screen. The majority of people use one out of 20-30 standard patterns that are easy to identify. Use a password or a PIN-code.

You can also use fingerprints for signing on. I do not recommend face recognition since some smartphones allow to use your photo to get around this protection.



STEP 2 Check privacy settings

The settings of your smartphone should have an option Privacy or something similar, depending on the system you are using. Here you can see which applications can access your camera, microphone, and geolocation. In some versions of the Android you can also see when the particular application accessed your camera and your mic last.

If you see some applications on the list that should not be there, delete them, and seek consultation of a specialist.

STEP 3 Use only licenced software from official sources

Always download applications only from the official application stores such as Play Market, App Galery, Galaxy Store, F-Droid. Never try search the application you need in Google using key words “download this application for free apk” because this is an almost 100% guarantee that you will download a harmful software to your smartphone.

We are talking about software, and not viruses. Very few viruses in the sense we use this word when talking about computers, exist for smartphones. Instead, you can install a harmful program which during the installation will demand access to everything it can reach, including your files, camera, microphone, calls and contacts. Such harmful programs can spy on you and show you unwanted advertising.

Downloading software from reliable sources only you will with hight probability protect yourself from harm.

STEP 4 Emergency factory reset

There are situations when you have to factory reset your smartphone and delete all the data stored on it. This can be done with the help of a program called Locker, which has to be installed from the F-Droid application store.

This program will ask you to give it administrator access, do that as otherwise it will not be able to completely reset your device to factor settings. Factory reset will take place after having mistakenly entered the PIN-code several times (the number of times can be selected when you set the program up). You can also turn on/off the notification that factory restore will take place when wrong PIN code is entered.

DATA PROTECTION

STEP 1 Protection from loss

In order not to lose access to your data, you have to regularly back up all the important information.

You can copy of important files to some external device regularly, for example one per week. You can use a flash-drive, an external hard drive or a cloud storage. It is important to do it regularly.

You can use special applications on your notebook or smartphone which allow to create a cloud folder on your hard drive. In this case, all you need to do is to save all your important files inside this cloud folder. Such a folder is stored on your computer, and all of the files are available without Internet access, but at the same times it is always synchronized with your cloud storage and all of the files are backed up automatically.

The best solution here is OneDrive integrated into Windows. You can use 5 gigabytes for free or purchase another 1000 gigabytes for a fee of 6 USD per month. OneDrive not only allows to create a cloud folder on your computer, but also to automatically synchronize the Documents, Desktop and Pictures folders.

You can also use any other cloud services starting from Google Drive and down to your own copy of the OneCloyd running on your own server or on the server of your organization.

STEP 2 Protection from theft and blackmailing

To protect your information from getting stolen, you should take measures to protect the devices on which it is stored.

If your information is stored on your notebook, protect your notebook, set up a sing on password and turn on BitLocker disk encoding.

If you store your data in a cloud storage, protect your cloud storage, use secure password, and set up two-factor authentication.

In case the data is on a flash drive, encode the flash-drive or the information on it. You can use BitLocker to encode the flash-drive (in this case you will be able to use this flash drive only with computers which have Windows as operational system). You can also use a special program called VeraCrypt to encode some files or you flash drive as a whole. In this case you will be able to access your files on any device that has this program installed.

It is important to remember that you have to encode not only files, but their back-up copies as well. At the same time, you do not have to encode your files before placing them into the cloud, it is enough to encode the cloud itself.

STEP 3 Data recovery

Not all data can be recovered. Sometimes the information is gone forever.

You can recover any data that was saved in the cloud storage such as Microsoft OneDrive or Google Drive. You can even recover the files that you have removed from your recycle bin -- you will get 14 to 120 days to do that, depending on the service you are using.

If you use HDD disks to store data, you will most probably be able to recover your data from them. You will not be however able to recover data from the SSD drive which is most probably installed in your notebook or computer.

Only the back-up copy of all important files can save you.

Always save all your important files at least in two places, but do not forget to protect each of them.

PROTECTING YOUR CORRESPONDENCE

STEP 1 Email

Most of you are using one the most popular email services which is Google Mail. Some of you are using other services as well, such as Yahoo, Hotmail, etc. Let's have a look at who can learn what about our letters.

All standard mail services encode your connection either to the browser or to a mail client. It means that all the letters that you send and receive can be seen only by you, your communication partner, and the mail service. Third person can access your e-mail either by hacking your account or by getting a court order to read your correspondence which your email service must comply with. You know how to protect your account, but how can we protect our correspondence from the email service?

There are two ways to do that. On the one hand, you can encode all mails on the client side, in other words, use encoded mail.

This is a time-consuming method; you communication with your partner will look as follows:

1. You and your communication partner generate private and public key for yourself. You can either use Mailvelope browser extension or you can generate the keys in the Mozilla Thunderbird. mail client.
2. You exchange your PUBLIC keys with your partners and import them into your mail clients (or into the Mailvelope browser extension).
3. When creating a letter, you will encode it.
4. You send the encoded letter.

In this case, if you enter your email account using any other device, the encoded correspondence will look like a meaningless set of symbols or as exchange of text files with meaningless set of symbols. Neither you (without having the key), nor the mail service or anyone else will be able to read your correspondence. However, some data will remain visible, such as the sender's and recipient's email addresses, some service information.

Alternatively, you can use any safe email service, for example Protonmail.

Such services perform all the encoding tasks behind the scenes, and thus simplify your life. It is important to remember, however, that having hacked your account in this mail services the perpetrator will see all your correspondence, unlike in the first method when s/he will see a set of meaningless symbols.

STEP 2 Messengers

Let's take a look at three most popular messenger: Telegram, WhatsApp, Signal.

Signal is one of the most protected messengers in the world, but it is also one of the least convenient messengers. It offers some basic functions, chat, calls, stickers, and smiles. You can also set up automatic deletion of your messages.

WhatsApp is technically similar to Signal, as both messengers use the same encoding algorithm. Both messengers treat your correspondence as your own private business, it is stored in your devices, but WhatsApp allows you to back-up your correspondence.

Telegram is a more convenient messenger, but is it similarly secure?

You can use secret chats in Telegram, in their essence they are similar to regular Signal or WhatsApp chats. These chats are stored only on your devices (more specifically, on the device which initiated the chat), and you can't get access to them even if you hack the account.

The functions of these three messengers should suffice to protect your security and privacy of your correspondence. It is important to understand, that messengers do not offer you anonymity -- they connect your profile to your mobile number.

There are messengers which do not require your phone number, however very few people use them, and it is doubtful that you will be able to persuade all people from your network to use them.

Each of the messengers mentioned above can be protected. You can set up pin code to sing on to the messenger on the specific device, or you can use two-factor authentication -- an additional password which will make it impossible to enter your account even if the perpetrator has your sim-card.

SOFTWARE

STEP 1 Smartphone software

To search for smartphone software, use the integrated application store (App Store, Play Market, App Gallery, Galaxy Store, etc.).

You can also use a free software store for Android called F-Droid.

STEP 2 Software for notebooks and computers

First of all, use the integrated application store (Windows Store, Mac app store), it is possible that they have the program you need.

If the standard application store does not have the needed software, go to the official website of the program developer. To find the official website google the program name without any additional words (for example, free download). One of the first search results will probably be the official website you are looking for. If you are not sure, look for the program in Wikipedia, and the Wikipedia will have a link to the official publisher's site.

If you have to pay for the program, there is normally a possibility to use a demo version with limited number of functions or full program but for a limited period of time.

Do not download applications from unverified sources as such applications may have hidden harmful functions and can infest your system with viruses.

STEP 3 Installing applications

Be vigilant when installing an application. Always go for custom installation wherever possible. During the installation read the messages appearing on the screen after each step. Frequently, you will see automatically checked boxes for installing additional garbage

programs. Always unchecked those boxes, do not agree to having all sorts of trash installed into your system. Unwanted applications, advertising banners and extraneous browsers can get into your system using these dirty tricks. This garbage programs will most probably have no viruses, but in and of themselves these additional applications are trash which slows your system and prevent you from using your computer efficiently.

STEP 4 Updating your software

To ensure the high level of security for your computer system, you should always update the system, applications, and programs. Security gaps are being constantly discovered in the operation systems and applications. Software publisher makes the necessary updates as soon as those vulnerabilities become known. All the corrections arrive to us in the form of the updates. Sometimes the updates contain new functions, sometimes they correct mistakes or have security patches. Always use the most current version of the system, applications, and drivers to reduce the risks of the abuse of software and hardware vulnerabilities.

SECURE INTERNET

STEP 1 Use trusted networks

Trusted are the networks which you have set up yourself or which have been set up for you. Your home and workplace networks can be considered trusted.

STEP 2 HTTPS Everywhere.

Surfing the Internet make sure that all the websites you work with support HTTPS protocol. To do that, pay attention to the address bar of your browser. The website address should have a lock sing next to it. This sign means that there is an encoded connection between you and website, and nobody apart from you and the server can see what exactly you do on the website, which data you are uploading or downloading.

You can install HTTPS Everywhere extension into your browser, and this extension will warn you if the website you are trying to access does not use the HTTPS protocol and thus is not safe.

It is important to understand, that the lock sign does not automatically mean that the website is great and safe. The lock means only that there is a secure connection between you and the website.

STEP 3 VPN

VPN is a virtual private network. When using a VPN, you create a sort of protective encoded tunnel between yourself and the VPN service. On the way between you and the VPN servers nobody will be able to capture your traffic or to learn where you are going. VPN conceals your destination -- that is the website or the server of an application you would like to access. It also conceals all the data that you transfer inside this tunnel: your messages, data, and files.

You can use VPN when you are using unknown networks, for example, in a hotel, a restaurant or on a city square. Nobody can capture or decode your traffic that goes through the VPN.

It is however important to understand that VPN has its limitations. It will not protect your from the threats on the side of your device, i.e. from viruses or harmful programs,nor from the threats originating from the website you are accessing. Some websites can be vulnerable to hacking and can be used to hack your device as well. VPN will not save you from it, only antivirus can help.

STEP 4 Be selective about the websites you are visiting

The majority of websites and web portals which have millions of users every day are safe for you. The threats can come from the little-known websites which you can come across by chance.

For example, you want to download an e-book. You google the title of the book and get to a website you see for the first time. Be vigilant as this website can endanger your security. It can have viruses. The viruses will be addressed by your antivirus, so this is not a huge reason for concern.

Frequently, however, the big green Download button will download some garbage to your computer. It can be some useless program, the main function of which is to show you advertising. Such programs are not detected by antiviruses as they are not viruses, strictly speaking. Scrutinize the extension of the file you are about to download. If you planned to download an e-book, but have downloaded an *.exe file, most probably this is not the book, but a harmful program.

AFTERWORD

Cybersecurity does not boil down to installing an antivirus. It is a constant, ongoing process. It is a process that should become your habit. No doubt, you can check all your accounts and devices, make sure they are protected, encode all the important data and back it up. However, the results will not be spectacular if this is done only once. False security feeling that results from security measures can lead to carelessness and open a security breach. You can start thinking that since you have set everything up, you are secure, and stop watching what you are doing. And it is exactly at this point that you can be attacked because this is when you are most vulnerable.

Security is a process that should be continuous and uninterrupted. You should develop safe behavioural habits, for example to always close the cover of your notebook when you leave it alone, look at the address bar when accessing a site, even if it is a site you have used before.

There is no such thing as absolute security. Good and evil, hackers and cybersecurity specialists will fight each other forever. New threats and new solutions appear every day. Keep an ear to the ground and be one step ahead! That's the only way to control your cybersecurity.

Written by: Henry Demjanovich, hnrdem@gmail.com, Telegram: @hnrdem


SWAN
SEX WORKERS' RIGHTS
ADVOCACY NETWORK