



THE ART OF DIGITAL SECURITY FOR PAKISTANI WOMEN

2nd Edition

THE ART OF DIGITAL SECURITY FOR PAKISTANI WOMEN



Digital**Rights**Foundation
"KNOW YOUR RIGHTS"

COPYRIGHT INFORMATION

This guidebook is available under the Creative Commons
Attribution-ShareAlike (CC BY-SA) license.

Disclaimer:

Every effort has been made to ensure the accuracy of the contents of this publication. The authors or the organization do not accept any responsibility of any omission as it is not deliberate. Nevertheless, we will appreciate provision of accurate information to improve our work. The views expressed in this publication do not necessarily represent the views of the Friedrich-Naumann-Stiftung für die Freiheit.

A project of



Digital**Rights**Foundation
"KNOW YOUR RIGHTS"

with the support of

Friedrich Naumann
STIFTUNG **FÜR DIE FREIHEIT**

CONTENT

1. Introduction	1
2. Digital Shadows	2
3. Secure your devices	4
4. Backup your data	6
5. Secure Password	8
6. Securing Online Accounts	10
7. Browser Security	15
8. Social Media and Anonymity	17
9. Cyber Harassment and Safe Spaces	19
10. Reporting Cyber Harassment	24
11. How to Create Hamara Internet	27

ABOUT DIGITAL RIGHTS FOUNDATION

Digital Rights Foundation is a research based advocacy organisation based in Pakistan focusing on information and communication technology to support human rights, democratic processes, and better digital governance. DRF opposes any and all sorts of online censorship and violations both on ground and online. We firmly believe that freedom of speech and open access to online content is critically important for development of the socio-economic infrastructure of the country.

www.digitalrightsfoundation.pk

ABOUT HAMARA INTERNET

Hamara Internet, literally meaning “Our Internet” is a pioneer campaign by Digital Rights Foundation that seeks to acknowledge the increasing trends of online violence and technology related abuse against women. Hamara Internet project aims to build a movement to promote a free and secure digital environment where women can participate in the digital world freely. Through awareness-raising sessions, digital security training, research, and dissemination of digital security kits, it aims to build women’s capacity so that they can take back the online spaces that belong to them, and reduce the digital gender gap that prevails in Pakistan, Hamara Internet project envisions the internet that is a space truly shared by all.

ACKNOWLEDGEMENTS

This guidebook would not have been possible had we not joined forces with Friedrich-Naumann-Stiftung für die Freiheit- Pakistan (FNF Pakistan). With their absolute support, we were able to create this resource for female students, which we hope will help them in not only staying safe and secure online, but also in reclaiming online spaces.

Authors:

Nabiha Meher Shaikh
Ghausia Rashid Salam
Luavut Zahid

Editors:

Nighat Dad
Adnan Ahmad
Ushbah Al-Ain

Translation:

Ali Kamran Khan

Design:

Iffra Khalid

Second Edition Credits

Seerat Khan
Hyra Basit
Shmyla Khan
Hija Kamran



WHY THIS GUIDE BOOK?

There are many digital security guides and manuals available online free-of-cost. However we realised there was a need for one for Pakistanis, especially Pakistani women. The challenges we face are different than the challenges faced by people in other parts of the world. Our cultural realities differ and the solutions we require also differ from the ones advocated online. For example, for women in some cultures, putting their picture on Facebook is not a security risk, but for girls in Pakistan (some of whom end up never using their own pictures publicly) this could very well be the case.

Women have reported how a simple profile picture of just their face will be taken and doctored using photo manipulation software. Their faces were superimposed on intimate pictures of others, and which in turn used to blackmail these women. Many were unable to ask their families for help, nor could they approach law enforcement even though they had done nothing wrong. The reason for this is that in Pakistani culture, family honour is intrinsically connected to women's bodies which is why this kind of blackmail is able to happen in the first place.

Complaints from Pakistani women have driven this initiative. In the absence of proper laws, we realised that only is there impunity for harassment online, but that no comprehensive guide for solutions that can work for Pakistani women existed. The tools used for digital security are the same as used elsewhere, but we have included Pakistani cultural context. We have also included tips for creating an internet culture where we no longer have to face these challenges.

INTRODUCTION

Noted journalist Jahanzaib Haque once highlighted that around 70-85% of all online users in Pakistan are male. Combine that with the fact that during the period of August 2014-August 2015 Pakistan's Federal Investigation Agency said that of the 3,027 cases of cybercrime that were reported, around 45% were related to cyber harassment on social media against women.

What is needed in Pakistan is the inclusion of more women in online spaces, more safety in digital places, and an online culture that is not hostile to women. This book is going to help you ensure that you learn how to stay safe online so that you do not limit your online experience.

We know plenty of girls who have stopped using Facebook because their profile picture was stolen, or added restrictions to their WhatsApp settings after they received unwanted messages. And this is not okay.

Women both young and old are using the internet and other digital tools for all kinds of things. From shopping through Facebook pages to coordinating assignments on WhatsApp. Sometimes when they see danger in these digital spaces many opt to stop using these services all together. Concern for safety and security online leaves them separated from all the good things the online world has to offer.

With this manual we aim to teach you the art of staying safe and secure online!

Before we begin, here's the most important tip: You do not need to be an engineering student, have a computer science background, or be a techie in order to set up digital security. Even if you are not tech-savvy ensuring online security and privacy is basic and requires no special skills or knowledge. So do not be afraid of digital security being too 'technical,' be more afraid of what could happen if your information is compromised or added restrictions to their WhatsApp settings after they received unwanted messages.

DIGITAL SECURITY SHADOW

Everything you do online leaves a digital data trace behind, a hint of who you are. This information is collected by websites, and collectively, these traces can be used to identify, track or even commodify you. This is your digital shadow; a profile of who you are. This information is collected by companies that stand to make huge profits from selling your information to advertisers. The companies that do so are not small unknown entities with limited reach, but include large legitimate corporations such as Facebook. The privacy policies we all agree to ensure that we are giving companies permission to store information such as our credit card information, Wi-Fi details, our location our viewing habit etc. that in turn are sold to other companies. We think we are using online products, but in reality, we become the products and the companies are the consumers.

It is important to know about your digital shadow because this information can be used by others as well, and not just large companies. If someone can trace you, they can potentially use the information to harass you. Women have reported that their ex-husbands have been using their digital traces to locate them.

HOW CAN YOU FIND YOUR DIGITAL SHADOW?

Doxxing is when information about a person is released online with malicious intent. One doesn't have to be hacked to be doxxed. Your information can be easily found using your digital shadow.

To see just how easily your information is available online, try self doxxing: Remember searching for your name on Google will not show you enough details about your online information.
<https://immersion.media.mit.edu/>

Use a search engine like DuckDuckGo,
which protects your privacy

Search for all your usernames on active
profiles as well as inactive/past online
profiles to see what is online

Search for all email addresses to see where
your email has been posted or possibly
misused

Search for your phone number(s), including
land lines and mobile phones, to do a reverse
phone lookup to see what information
related to your number is online

Search for your home and office addresses and do a reverse address lookup to see where your address, property records, etc. can be found online

Do a reverse image lookup on your public pictures, such as Facebook cover photos or profile pictures, to see if they have been used anywhere else.

Now that you've figured out what your digital shadow is and how it can be easily discovered, think about why knowing about your digital shadow is important.

To learn more about how digital **shadows work**, visit Tactical Technology Collective's online resource, myshadow.org & <https://immersion.media.mit.edu/>



SECURE YOUR DEVICES

Let's start with securing your devices. One simply mistake is to leave your device unsecured, without a password or passcode as your device becomes more vulnerable when you leave it

MAKE THIS A RULE

Put a password or code on every single device you own. It is yours and it has your data in it. It is your property and if it gets stolen, you don't only lose the device but also all the data in it.

Sarah's brother used to check her phone regularly. He would yell at her if she didn't give him access to her phone. He would go through her messages and pictures. Sarah is not alone. Women in Pakistan often have to share their passwords or codes with their family members. If they don't, the information is sometimes obtained forcefully. Sarah knows she has a right to privacy, but fears what will happen if she asserts her self too much. She knows that her brother is subjecting her to social surveillance and she is not alone. Her friends also have to keep their devices open or share their codes with their family members. Most of them struggle with trying to demand their right to privacy and the repercussions of demanding this right.

ARTICLE 14

Inviolability of dignity of man, etc.
(i) The dignity of man and, subject to law, the privacy of home, shall be inviolable.

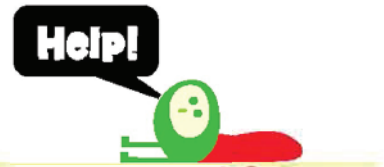
Sarah starts to talk to her about her right to privacy. She starts a conversation at home about privacy and trust. She knows it will take some time before she gets her rights and often gets frustrated when she is not able to convince her brother. However, she reminds herself that she is negotiating her rights and eventually, her brother starts to trust her instead of controlling her.

RUNNING AN ANTIVIRUS CHECK-UP ON YOUR COMPUTER REGULARLY

A virus is a malicious code or program which can infect your computer, and hijack your computer's functionality by erasing, modifying, or tracking data. Trojan is an example of virus that can install itself on your computer through online downloads, such as websites offering free music or videos, as well as emails, particularly spam emails. This is why you should never click any links sent by unknown senders. Remember, viruses can also be disguised in the form of pictures, videos, audio, greeting cards, so always think twice before forwarding that funny mass email.

An anti-virus should always be active and updated to the latest version to protect your web-browsing. Beyond regular protection, remember to run a regular full system scan to ensure your machine is safe from viruses. Always install known anti-virus software such as:

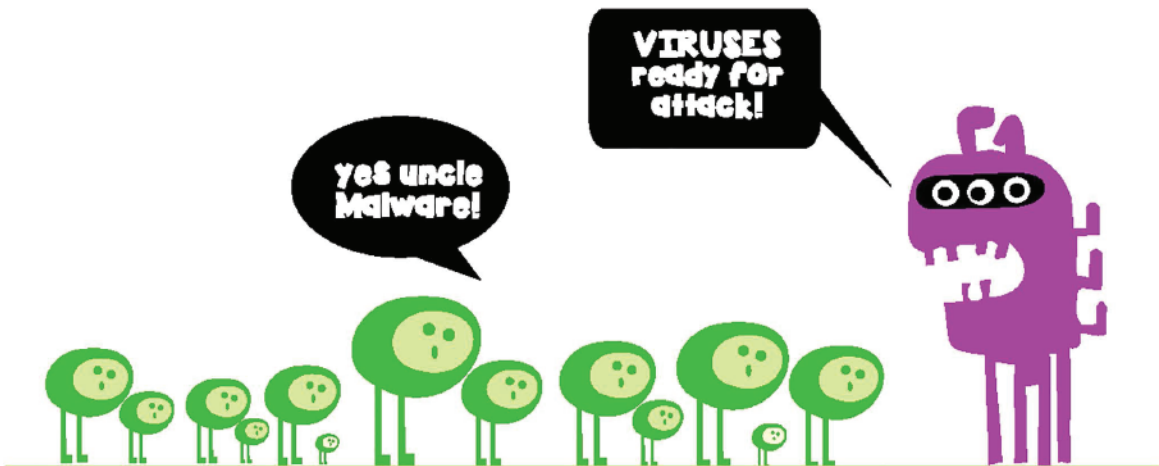
- Kaspersky
- AVG
- Avast
- Norton Antivirus
- Avira



MALWARE SCANS

Malware is short for “malicious software.” It is an umbrella term for various types of malicious code or programs which can cause harm to a computer system. All virus are malware, but not all malware are viruses, but can also include spyware, ransomware, etc.

Computers need anti-malware software as well, as most anti-virus softwares del with traditional threats like Trojan viruses, worms, etc. Anti-malware software focuses on more current threats, including the many forms of malware which are being developed around the world by professional criminals and hackers. They can infect your computer and spy on you through keyloggers (recording keystrokes) or steal your banking information. This is why it is important to use an anti-malware program as an additional layer of security for your device, along with anti-virus software. We recommend Malwarebytes, Lavasoft, and Spybot (anti-spyware adds a third layer of security if used with Malwarebytes or Lavasoft.)



BACKUP YOUR DATA

Ever lost an essay a day before it's due? Has your computer ever crashed wiping away all your data? Losing data is often distressing and sometimes it can't be recovered. This is why you should make sure you have a copy of all your data.



Use physical device like a USB or an External Hard Drive

FEAR

Some users prefer cloud storage because they fear losing their data storage devices in a secure location, so that even if your laptop is stolen, your backup will be safe.

Cloud storage which is online data storage.

WHAT IS CLOUD STORAGE?

Cloud storage is convenient as it does not require any physical equipment. Stored data exists online, and is physically maintained on servers that belong to the hosting company, such as Google.

TIP

Keep your hard drive in one area of your house such as a drawer in your bedroom. Always store it there so you don't worry about having to look for it.

ALERT!

Be mindful that cloud storage is not safer than storage devices, as cloud stored data can also be hacked into or stolen.

WARNING!

Always be careful when borrowing a USB stick or allowing someone to use yours. We caution against this. Sometimes people will deliberately install spyware or other malware on their USB stick to infect a target's computer. Sometimes husbands and fiances do so in order to spy on their wives, or ex-husbands may do so in order to blackmail their ex-wives. Cases have arisen where women have been blackmailed after their computers were infected and their data was stolen. So be careful. We also caution against using USB stick for shared computers. We realise it's common practice to do so and sometimes there are no other alternative.

HERE ARE SOME TIPS:

Don't add anything to the USB other than the file you need.

Run the USB through antivirus and antimalware software every single time you use it.

Example:

Ateeba learned how to back up her data on an external hard drive and USB stick but what she did not realise was that she also needed to learn how to protect her files.

On her internship she took her hard drives and USBs to her new office. The same drives and USBs that she had been using for a whole range of activities at college. The storage devices included copies of her ID card, pictures from a field trip, many of her assignments, and more.

Ateeba's first problem showed itself when a USB she frequently stored things on became infected with a virus at work and caused her to loose her data.

Her second problem became obvious when she realised that her supervisor had taken her ID card copy from her hard drive without her knowldge. While the supervisor meant no harm and needed the copy for record keeping, Ateeba realised that someone else could have simply stolen it - and other information along with it.

Ateeba began ensuring the physical security of her hard drive and USB from that point was more secure, protected from external problems. Data for women in Pakistan is often more sensitive from their male counterparts. For instance, nothing would have happened to Ateeba's colleague Ali had he given over a USB with his pictures on it to someone - but for Ateeba there was a real chance that her pictures could be misused, as we have previously mentioned.

SECURE PASSWORDS

Passwords are the key to digital security. Weak passwords are easy to crack and it is harder for a hacker to access your accounts if your password is a strong one.

Too many of us think our passwords are strong when they are not. It is not enough to use long passwords; hacking software can use dictionary words to scan through possible words in a password, and hack into accounts by cracking the password. A strong password isn't that hard to make up especially if you use passphrase instead of passwords.



Password sharing is alarmingly common. While many think that there is no harm in sharing passwords with close friends or family, remember that if their information gets compromised, yours could too. Secondly, this is not a good habit. You should value your privacy even though females are not encouraged to value it in our culture. This culture will change only if we change it ourselves.

Passphrases are longer than the characteristic six-eight letter password, and they are harder to crack if created well.

HOW TO CREATE STRONG PASSPHARSE

DO's

- 1) 18-30 characters long
- 2) Contain more than one word
- 3) Consist of uppercase and lowercase letters, numbers, and symbols
- 4) Consist of words that cannot be found in dictionaries or are not famous quotes

DONT's

- 1) Should not be based on personal, easy-to-guess information like birthdays, anniversaries, or pet names
- 2) Should not be based on personal preferences, likes and dislikes, hobbies
- 3) Never written down on either a piece of paper or on a document on your device

One way to create a secure passphrase is to create a mnemonic device, which is a technique in memorizing information. For example, if you pick a sentence, you can replace letters with numbers, or just use the first, second, last letter of each word.

FOR EXAMPLE:

Best friends don't ask for your password, they value your privacy and understand the importance of digital security!

Becomes, b5D'@4up,tVURP&uti0DS as a password.

Remember to change your password regularly and do not use old passwords.

Always remember never to have the same password for every account or to use a password for more than one account. If one account gets hacked, the other could get hacked easily too.

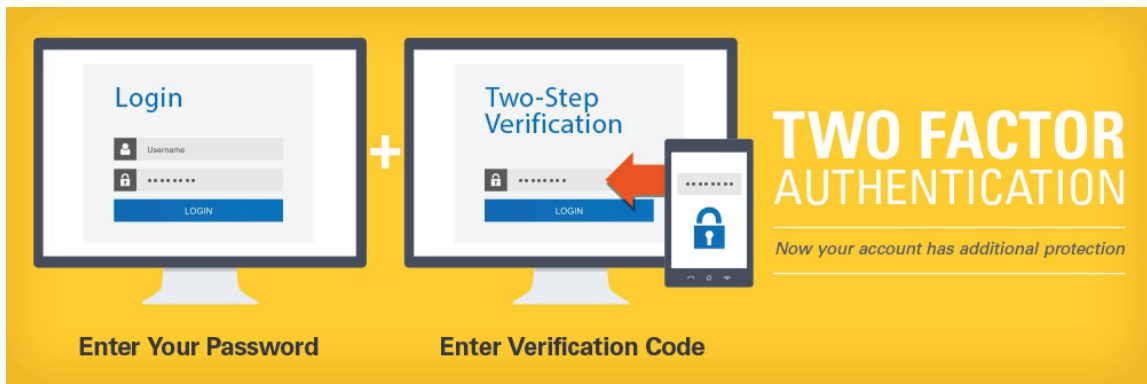
If remembering several passwords is difficult for you, a very useful tool is KeePass which is a free program that generates and stores strong passwords for you. You only have to remember your master password, which should be a strong, uncrackable passphrase.

If you use KeePass (or KeePassX for Mac), make sure you store your KeePass database on a USB stick or another form of external storage. If you store it on your computer, hackers may be able to access it if your security is breached.

Remember: Even a KeePass passphrase should never be written down or shared with anyone.

TWO FACTOR AUTHENTICATION

You may have heard people talk about two-step authentication. It might sound too complicated for you to even read about, but in reality, it's actually quite easy. Two-factor authentication is when you link your phone and your cellphone number with your online accounts for an added layer of security. Whenever you log in, you will be required to add a code which will either be sent to your phone via SMS or an automated phone call, or through an app. If you visit your security settings on your social media or email account, you will have the option to set up two-factor verification. Google, Facebook, Yahoo, Twitter, Hotmail, etc. will ask you for your phone number, and then send you a code to verify that it is correct. Once you input that number, you are all set! Now, the next time you login, after entering your password, you will be asked for a code



As great as it is to have your cellphone linked to your online accounts, don't forget, this is Pakistan. How will you log in on Eid or some other day when cellphone signals are blocked? Or even if you're traveling abroad and forgot to turn off two-step verification? Many people get locked out of their accounts when their numbers are not functional. That's what authenticator apps are for. These apps will give you a code every time you open it. Gmail uses the Google Authenticator app, which you can download for free, along with a QR code reader app, which will be used to scan a code every time you want to set up a new email account on Google Authenticator. (Both apps are relatively small, for those struggling with low memory on their phones.)

The Facebook app has a built-in code generator, but it is also an invasive app which uses your phone's camera, and mic, and accesses your contacts, call list, SMS, gallery, etc. without permission. So for those who opt out of using the Facebook app, you can also use Google Authenticator to set up code generation for Facebook.

Hotmail also has a verification app called Microsoft Account, which requires you to approve login requests every time you access your email. Twitter functions in the same way; if you go to your settings, you can add your phone number to the app, and then enable account verification from security settings. Every time you login to Twitter from a browser, you will have to approve the request from your Twitter app.

REMEMBER:

Two-factor authentication means that your cellphone becomes more valuable. Always lock your

phone, so that even if it is stolen, your data will not be compromised so that even if it is stolen, your data will not be compromised

In case of emergencies, Gmail and Twitter allow you to download backup code(s) for when you need to login. (This will come in handy for those times when your phone falls in the toilet and the rice trick just won't work.) Never save these codes on your phone. Print them out or write them somewhere. Keep them somewhere secret and safe.

TWO STEP AUTHENTICATION FOR GOOGLE

1



Signing in will be different

You'll need verification codes:
After entering your password, you'll enter a code that you'll get via text, voice call, or our mobile app.



Keep it simple

Once per computer, or every time:
During sign in, you can tell us not to ask for a code again on that *particular* computer.



Help keep others out

You'll still be covered:
We'll ask for codes when you (or anyone else) tries to sign in to your account from *other* computers.

2-step verification

Keep the bad guys out of your account by using both your password *and* your phone.

[Start setup »](#)

[Learn more](#)

2

2-Step Verification



A text message with your code has been sent to: (**) ***-**95

Verify

☐ Don't ask for codes again on this computer

3

2-step verification

Help keep the bad guys out of your account by using both your password *and* your phone.

Get Started



4

Set-up 2 factor verification for

Set up your phone Add a back up Confirm

Tell us what kind of phone you use, and then you'll set up a way to get your verification codes



Android



Now open and configure google authenticator

The easiest way to configure google authenticator is to scan the QR code

1 In google authenticator, select Scan a barcode

2 use your phone's camera to scan this QR code



When the application is configured, click Next to test it.

EXAMPLE:

Ruksana began receiving weird messages online after she began her online business. While studying business she realized she could earn more money if she worked from home and her shop could be online. However, she never realized how problematic dealing with customers could prove online.

Hidden behind a cloak of anonymity, some people thought they could say or do whatever they wanted. One day when crude and abusive messages from one man became too much for her to handle, she reported him and then blocked his profile completely.

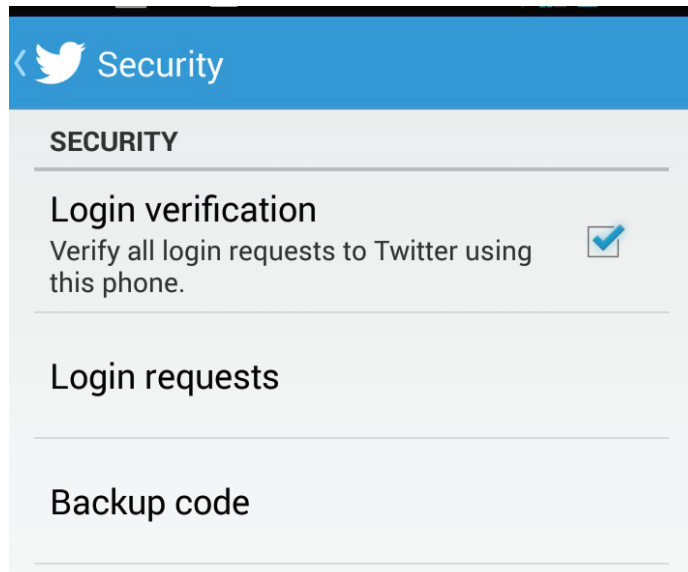
The next thing Ruksana knew, someone began trying to hack into her account on Facebook. She also got notifications that someone was trying to reset her Gmail password. Ruksana knew that if she did not act fast she could end up losing not just access to her account but also access to the page she had created for her online business.

Ruksana's friend Maria told her to take a few precautions

- She told her to immediately activate two factor authentication for all her accounts
- She then told her how to setup notifications for when someone accessed her Facebook account from a browser or computer that she had not saved
- Maria also showed Ruksana how to generate codes for her apps so that she did not have to login with her password from other devices

2-FACTOR AUTHENTICATION FOR TWITTER

1



2

We've sent a login verification request to your phone.

When you receive the request, accept it by clicking the checkmark button on your phone. You can also enter a [backup code](#).

Need help? Please contact [Twitter Support](#).

3

Verify your phone

We sent a text message to (201) 555-5559 with a code



Enter verification code

598236

Verification codes are 6 digits long.

« Back

Verify

[Didn't get the code?](#)

BROWSER SECURITY

Your browser can be vulnerable to threats even if you have active anti-virus software running and regularly scan your computer for viruses and malware. That is why additional steps are required for a secure browser.

BROWSER SECURITY BEGINS WITH THE MOST BASIC STEPS

1

Never leave your accounts signed in, even if you are the only one using your device. You could lose it, or it could get stolen, or you could get hacked. Even if you have a password on your device, you should always logout of all sessions every time you shutdown your computer, or put it in sleep mode.

2

Use a private window (Firefox) or go into incognito mode (Google Chrome) to go into private browsing mode. In private browsing, your browser will not save a record of the websites you visit or your download history; however, your ISP, workplace/school administrator, or the websites you visit will still have a trace of you.

3

Never save your history; it is easier to bookmark a page rather than compromise on your digital security.

4

Clear your cookies and temporary Internet files regularly.

5

In browser settings, enable a 'do not track' option so that websites will not track you.

6

Ensure that you have enabled options to block reported attack sites and web forgeries.

7

Never enter your password on a website which is not the official email/social media website. The same goes for any sensitive information, especially credit card info.

BROWSER ADD-ONS

The next step in browser security is add-ons or extensions. You might use browser add-ons to download videos or music already. Similarly, there are browser add-ons or extensions to protect your privacy and security by blocking cookies, trackers, and pop-up ads.

HERE ARE SOME ADD-ONS THAT ARE MUST-HAVES FOR YOUR BROWSER:

HTTPS EVERYWHERE:

Ensure that you are connected securely to a website through (HTTPS) which will keep your information private, rather than an insecure one (HTTP) wherever possible.

PRIVACY BADGER:

This add-on ensures that other websites will not track you.

"WHEN YOU CLICK THE FACEBOOK LIKE SHARE BUTTON OR TWEET SOMETHING DIRECTLY FROM A WEBSITE, YOUR REACTION IS RECORDED AND USED TO TRACK YOUR ONLINE ACTIVITY TO CREATE A DIGITAL SHADOW OF YOU. HOW INVASIVE! ADD-ONS LIKE PB OR GHOSTERY WILL ENSURE THAT NO WEBSITE WILL BE ABLE TO TRACK YOU."

DID YOU KNOW!

NO SCRIPT:

A script is a little program that some websites will run in your browser. Sometimes, these scripts can have security vulnerabilities, and this is why you need NoScript, so that no script can run in your browser without permission.

SOCIAL MEDIA SECURITY & ANONYMITY

Social media is fun but can become problematic if your security is too relaxed. This is more important because social media platforms are constantly changing their security and privacy settings, meaning that content that was previously private or visible to specific users only, can suddenly become visible to all your friends or to the public. Here are some basic tips for online security:

- If you like using public posts, be mindful of what information you put in such posts. Nothing that is personal or identifiable should ever be made public. This includes public photos as well, whether they are of you or friends or family.
- Check your security and privacy settings regularly to update them and to ensure that changes implemented by websites have not affected you.
- To maintain anonymity, you can prevent users from looking you up through your email address or phone number, and even from sending you messages through your security settings.
- Facebook allows you to see where you are logged in and which browsers you are logged on to.
- Review this information regularly to ensure that you have not accidentally left a session logged in anywhere, or that your account has not been compromised.
- Ensure that social media websites cannot personalise ads, or track you online. Check your Facebook ad preferences, you will be horrified by the large number of keywords used to identify your “ad preferences.”
- Don’t let social media websites track your location. Make sure that this option is disabled.
- Never check in or announce where you are on social media, specially if you are not live-updating an event. Even if you add the update after you have returned home, hackers, stalkers, and others who wish you harm can still create a profile of you based on the places you visit frequently, which are you visit the most, etc. This can crossover into offline dangers.
- Check your tag settings to ensure that you are not tagged in unnecessary pictures or updates

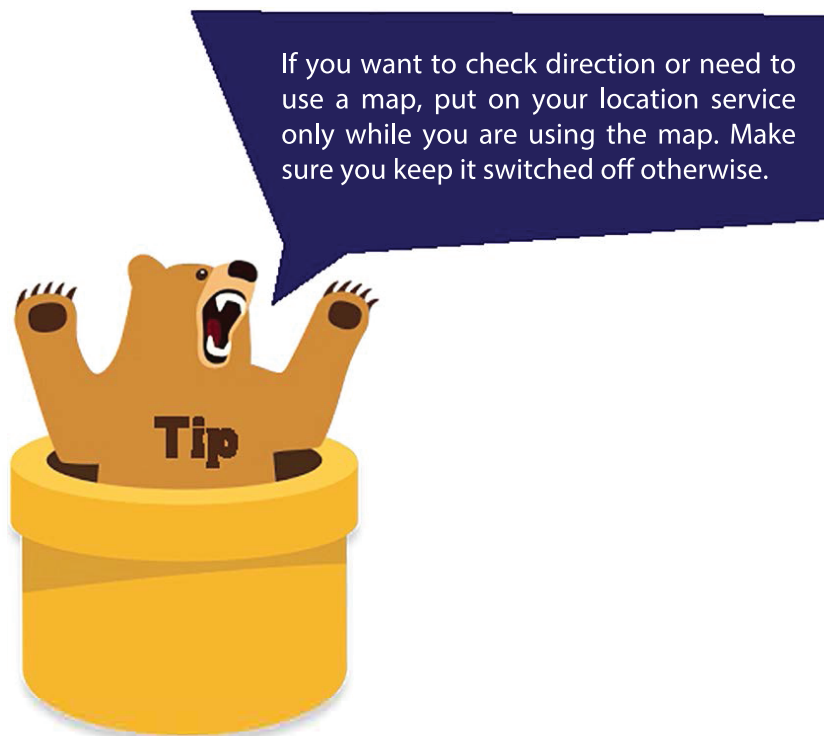
TIP

Everything you do online stays online. Even if a website gets deleted, there will be an online cache which will have those website entries still available. So use social media with the knowledge that nothing is truly private, and will never go away once it is online.

VPN:

You can use a VPN (virtual private network) which hides your location and your browser is directed to servers in other countries. You can install a free VPN service onto your computer such as Hotspot

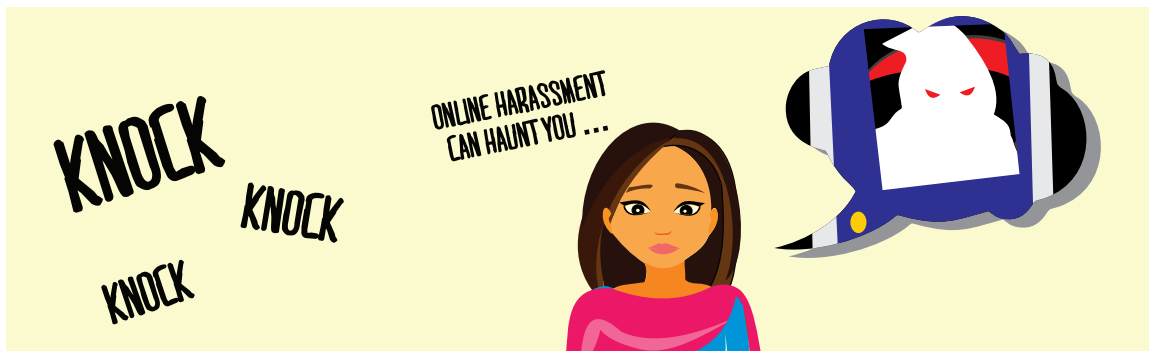
but beware that it can slow down your computer, and that it retains usage logs. The best option is to look at paid but more secure VPNs such as Disconnect or Tunnelbear. Another option is installing a VPN add-on, such as Zenmate in your browser. Not allowing your devices to access your location is a good practice we recommend. While we all need to use location services on our phones or other devices to get directions from online maps, we often forget that in doing so we are allowing the application to access our location at all times unless we switch it off. If you don't disable location services, your devices can be easily tracked to find out where you are physically.



CYBER HARASSMENT AND SAFE SPACES ONLINE

Imagine someone is knocking on your door whenever they like and when you open it, they yell at you, abuse you, and demean you. Or imagine someone stands outside your house day and night yelling abuses at you. You would probably call the police and others would come to help you or tell him to go away.

People take abuse and harassment very seriously when it impacts our physical space, but not when it takes place in cyberspace. We recognise why someone's physical space is theirs and we also know we shouldn't invade other people's physical spaces like their houses or offices. We don't go to people's houses uninvited and most of us do not call people late at night because we respect their space and privacy.



Yet when someone speaks about being cyber bullied or harassed, they are often blamed. This is because there is no physical space that was violated. Social media, and the internet in general, necessarily relies on users to set the tone. Unlucky for us, the tone that has been set is not a pleasant one especially for those who identify as females.

In most cases, the negative experiences that people have online are dismissed and devalued, as offline abuse or harassment is taken seriously, being regarded as being more visible. It is important to remember that one's online space is just as valuable as one's physical space. As with any public space, the internet belongs to everyone. In a report, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, concluded that internet access is a basic human right. In real life, even in public, no one has the right to make you uncomfortable by invading your personal space, or to bully or harass you, however, the same principles apply to your personal space online as well.

Even though there is nobody to abuse or physically strike in a digital space, we are often subjected to vicious verbal abuse. Have you ever been attacked online for your views? We are assuming you felt really bad about it. Sometimes we have to block people from abusing us further.

Some online abusers, or 'trolls', are relentless and keep making new profiles even when you block them. Think about why they do this. Why do they keep abusing us? Is it only because they are sad, angry people?

"OCCUPY DIGITAL SPACES"

Or could it be because they want others to quit occupying digital spaces? We think they want to silence you and it's not okay to resist being silenced. When people express unpopular opinions, users often emerge not just as individuals but also in mobs to silence them. People give threats online that they would not dare to make offline, such as telling people they are praying for their death.

REMEMBER

- If someone is being mean to you online or saying things that distress you, it is never your fault.
- Even if you're expressing an opinion others don't like, you do not deserve it.
- You are never asking for it!

THINK ABOUT IT:

You are being subjected to abuse because your words and your comments, which are essentially your property, are being attacked. You are being attacked because most users know there will be repercussions for them. They know they will be in trouble if they attacked you in physical space. They know that if they yelled and swore at you in a lecture hall, it would not be tolerated. People would speak up. You would be given support. Trolls, like schoolyard bullied, enjoy having power over someone. They enjoy distressing another person.

This is similar to bullying because we are aware that bullying creates a cycle of abuse. One person feels powerless because someone more powerful than them made them feel bad. So the next person they take their anger out on gets bullied by them, and so on, creating a vicious chain. It's a hard cycle to defeat, but it's not impossible. The first step towards defeating it is to recognise it.

If you are being bullied online and you tell someone about it, you are often told to go offline. This implies that simply by being a social media user, you are responsible for what you are going through. We disagree with this and we will explain why.

WE OFTEN HEAR

"Why are you online anyway?"
"Why aren't you blocking him?"
"Why were you saying that in the first place?"
"Ignore! Do not feed the trolls."
"Deactivate your account."
"The internet isn't safe for women, so why are you on it?"

These things are hard to hear especially when they come from your loved ones who mean well. They do not want to make us feel bad and they really do not want to see us distressed. These are the only solutions they can think of.

REMEMBER

- You are online because you have a right to use the internet. Anyone who tells you to stop using it is basically asking you to give up a right.
- You get to decide who you want to block or engage with online. Some people engage with trolls and it sometimes work. If you block someone, they can always make another profile so while we recommend blocking, we also caution that it's not always a solution.

- Whatever you say online, you have the right to free speech and expression. If someone chose to get angry about your views, then any abusive actions they take are their responsibility, not yours.
- Yes, some comments should be ignored, but ignoring does not solve problems. Sometimes it is necessary to stand up for your opinions and for yourself, but remember to pick your battles. Some are worth it, and some are not.
- If you deactivate your account, your bully has won. You have conceded your space. He now has been further empowered and emboldened. He will now think he can get away with harassing. By occupying your space, you are resisting, not just for yourself but for every bullied and vulnerable person online.
- When it comes to violence against women, we are not safe anywhere. We are not safe in our homes, in public spaces, in the workplace, etc. Nothing will become safe for women until we claim that space and make it safe for ourselves.

This is why it is important to remain on cyber spaces like social media instead of giving up. This is why we advocate creating safe spaces. **#OccupyCyberSpaces**

Article 9 of the Constitution of Pakistan states that we have the right to free speech, 'with reasonable restrictions.' which means this right is not absolute.

#KnowyourRights

Amina is a blogger who writes about women's rights. Many people do not like her views and she receives many comments on her blog. Many of the comments are nasty. Examples include:

- **KILL YOURSELF!**
- **YOU ARE FAT AND UGLY!**
- **YOU ARE WORTHLESS AND CRAZY!**
- **NO ONE LISTENS TO YOU ANYWAY.**
- **NO ONE LIKES YOU.**
- **YOU ARE GOING TO GO TO HELL FOR THIS.**
- **YOU SHOULD BE RAPED!**
- **I WANT TO KILL YOU.**
- **I WANT TO THROW ACID ON YOUR FACE.**
- **YOUR EXISTENCE IS WORTHLESS.**

Some of the comments are long, detailed and very disturbing. Amina used to feel upset every time she received threats of physical harm.

Amina initially did not know how to deal with the distressing comments on her blogs. She spoke to other female bloggers and discovered that she was not alone. Most had received similar comments and threats. The group helped her connect with an activist who had experience with dealing with these issues. They also decided to set up a supportive community for each other. She discovered that the women who received the most hate were the ones who were most vocal or went against the grain. Female writer and journalists told her they were used to being trolled that it no longer distressed them. This alarmed Amina. Humans should not have to become desensitised in order to cope.

First, Amina started moderating comments and stopped approving any hateful comments. When her trolls realised she was ignoring their abuse, they gave up. One, however, persisted and continued to leave comments. She consulted her supportive community and they helped her report the person leaving the comments. It took a few months for the comments to stop, and she still receives some awful comments or emails sometimes. She now understands that some people send her these comments hoping to silence her. She continues to write because she refuses to give up and she does not want her bullies to win.

Examples like this show us why it is important to remain on cyber spaces like social media instead of giving up. This is why we advocate creating safe spaces. **#OccupyCyberSpaces**

A safe space can be set up as a closed group on a social media site or a mailing list. It can be a closed blog or a forum.



- 1) What are your values? Those who share them should join. If someone does not share them and wished to learn then you need to decide as a group if you should let that user in.
- 2) Be open to learning and having your views challenged.
- 3) Come up with policies like disallowing screen captures within the group or on user profiles, and leaking information from group discussions.
- 4) Discuss possible response within the group towards members who are personally attacking others and violating confidentiality.
- 5) Arguments can and do get heated. That's okay as long as everyone's being respectful and making an effort to hear other views. Be open minded.
- 6) What should you do if a conversation gets nasty? Come up with strategies regarding how to diffuse such a situation.

Exercise the same caution you would in your physical life. You go to places where you feel safe especially when you want to have a conversation with friends that you do not want others to hear. You would not expect that someone will scream at you. People would hesitate to attack you in a public space knowing they would not be allowed to. So make it a rule of thumb: your online space should be safe like your offline spaces are. Both spaces should be places where you can debate, discuss, argue, and learn. Both spaces will expand on your knowledge and sometimes you will realise you have changed your mind because of the dialogue you have had that challenged your views.

One of the best ways to turn the internet into a safe space for everyone is to set up support groups where people can help each other if they are being harassed online. Your safe space can become a place where you can set up support groups and be there for each other in case the trolls attack!

REPORT CYBER HARASSMENT AT

FEDERAL INVESTIGATION AGENCY
<http://www.nr3c.gov.pk/creport.php>

Digital Rights Foundation.
help@digitalrightsfoundation.pk

**Heartmob is a tool that was created
to help end harassment online. Check it
out here: <https://iheartmob.org/>**



REPORTING CYBER HARASSMENT

Step One:

Report the Cyber Harassment to the Social Media platform

Your social media platforms are more responsive than you might think, if you feel uncomfortable online--use the following tools at your disposal immediately. It's easy and effective!

Reporting Harassment on Facebook

To report harassment on Facebook use the following link:

<https://www.facebook.com/help/?help>

Reporting Harassment on Twitter

Click the following link to report cyber harassment on Twitter:

<https://support.twitter.com/>

<https://help.twitter.com/en/rules-and-policies/twitter-report-violation>

Reporting Harassment on Instagram

To keep yourself safe on Instagram report it on the following link:

<https://help.instagram.com/>

Reporting Harassment on Snapchat

Take a step and report cyber harassment on this link:

<https://support.snapchat.com/en-US>

Privacy Violation

Facebook

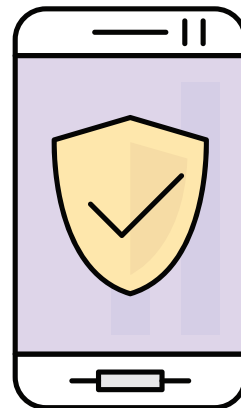
Fill out this form if someone is using your picture, video or other information without your consent:

<https://www.facebook.com/help/contact/144059062408922>

Instagram

Report any video or photo violating your privacy by filling out this form:

<https://help.instagram.com/contact/482633291790470>



Step TWO:

Report to Law enforcement agencies

If you find yourself in a situation that requires assistance from the police, file a report with the National Response Center for Cyber Crime (NR3C), FIA. You'll need to file an application addressed to the Deputy Director along with printed screenshots as proof.

Reporting to FIA

Do not stay quiet if you are being harassed online. Cyber Crimes must be reported nearest NR3C branch.

The FIA's Cyber Crime Wing offices are located in

- ✓ Karachi
- ✓ Lahore
- ✓ Quetta
- ✓ Peshawar
- ✓ Rawalpindi
- ✓ Islamabad

The FIA's helpline is 9911 and they can also be contacted on the following online form:

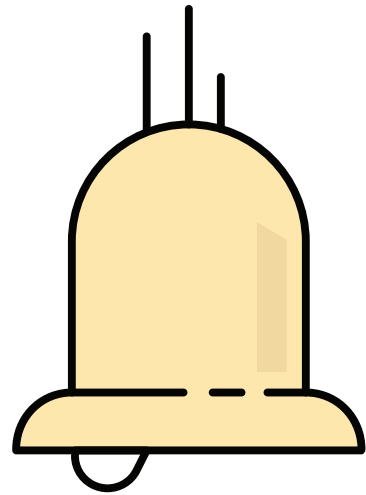
<http://www.nr3c.gov.pk/creport.php>

Reporting to PTA

You can report harassment through text messages and calls to the Pakistan Telecommunication Authority (PTA). While the PTA is not a prosecuting body, they will be able to block and remove numbers. You can contact them through the following numbers:

0800-55055

051-9225329-31



Step THREE:

Contact Cyber Harassment Helpline

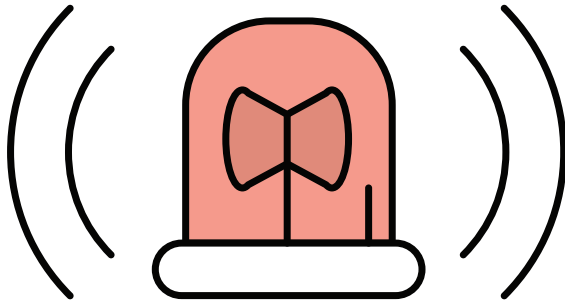
Cyber Harassment Helpline

If you're confused on how to approach law enforcement or need additional support, do not hesitate to DRF's Cyber Harassment Helpline. Launched in December 1, 2016, the Helpline is Pakistan's first dedicated helpline addressing issues of online abuse and violence providing a free, safe, gender-sensitive and confidential service. The Helpline Support Staff gives legal advice, digital security support and psychological counselling to victims of online harassment.

The toll free number [0800-39393] is available to people looking for help between 9am to 5pm, 7 days a week. The Support Staff can also be contacted via email at helpdesk@digitalrightsfoundation.pk and our Facebook page

<https://www.facebook.com/DigitalRightsFoundation/>.





I NEED SUPPORT

PCSW

1043

RESCUE

1122

FIA

9911

CYBER

**HARASSMENT
HELPLINE**

0800 39393

PTA

0800

55055

ROZAN

HELPLINE

0800

22444

POLICE

EMERGENCY

15

GOOD TO KNOW

- 70% of women don't report cyber harassment to law enforcement agencies (LEAs) when they are harassed *
- 47% women believe that their complaints won't be taken seriously when they go to the LEAs *
- 45% women believe that reporting harassment to LEA's is embarrassing *
- 72% of women are not aware of any laws relating to cyber harassment in Pakistan **
- Only 51% understand a little about the terms and conditions of social media websites **
- Among girls below 18 years of age, about 55% women use smartphones **
- 67% of women use Facebook on the internet according to our sample group**
- About 81% women above the age of 25 use Facebook **
- 79% of women use their devices regularly **
- According to our study, 50% women identified Facebook as the worst platform for online harassment **
- 70% of women are afraid of posting pictures online because they could be misused **
- 25% of women have witnessed a girl being bullied by men online **
- 40% of women had been stalked and harassed via messaging apps **
- 48% of women knew someone who had stopped using the internet after being harassed online **

* *Cyber Harassment Helpline 1 year report*

** *Measuring Pakistani Women's Experience of Online Violence*

HOW TO CREATE HAMARA INTERNET

As a citizen of any country, you are aware of your social contract with your state. However, the internet has no state, no government, and there is no such thing as virtual social contract.

This is why the internet can become a dark and scary place sometimes. The history of humanity is one of power struggles and humans have created all sorts of new tools to further their pursuit of power. We brag that we are at the top of the food chain. We take pride in having power and display sources of power, such as wealth.

Modern technology, like the internet, is also the realm of the powerful. Those who can afford to use it more frequently get the most space. Those who have the privilege of time to post more than others also get heard more. Those who say what others want to hear become popular far more easily than those who are critical of popular views.

In Pakistan, there are far more male users than female users. Men use violence to silence women and other vulnerable groups whether it is offline or online. The streets are not safe for us because they do not want us in the space they have claimed as their own. Offices can be hostile for the same reason. The list of spaces that become unsafe for us is endless.

It is no surprise that the powerful want to maintain power in all spaces which is why people from marginalised groups end up getting abused online. They want us to concede the space to them and give up trying to claim it. The more we try, the more backlash we get.

But this is not bad news. Online spaces rely on users to set the tone and we, as users, are in charge of the culture we create. Culture changes and evolve especially in today's rapid information age.

So we are in charge now and we get to decide if we want to make the internet a safe space for all. Can you imagine living in a world where people behaved well online?

Change begins with you. It's easy to point fingers at others and not see ourselves as part of the problem. Remind yourself that although you may not be a cyberbully, you are part of a culture where cyberbullying is normalised and accepted as part of online experiences. People expect to get cyber bullied at some point in their life. Surely that shouldn't be the case?

In order for us to become good citizens of the internet, or Netizens, we have to follow some rules as well. For example, we have to try to not vent out our anger online. We have to be aware that we could be repeating a cycle of abuse by being mean to someone online just because we have had a bad day. We must be mindful of our actions.

Humans are social animals that like to associate with groups of people who they feel understand them. That's why we value our families and friends. When they go through a hard time, we support them, sometimes even when we don't agree with them.

Would you support a friend if they were attacked in a physical space? We are assuming you would get up and go get help. We are assuming you would fight back on your friend's behalf knowing they would be too upset to say anything.

Do you always support a friend or family member who is being cyber bullied? Do you respond to

their abuser to reason with them? Do you try to fight back hate speech with your own counter narrative?

We've come up with some basic suggestions you can apply to help make the internet a safe space. Here's the most crucial thing: behave online like you would offline.

- **Always provide the same online support that you would offline.** If a friend is being bullied, be there for them and help them solve their problem instead of ignoring it.
- **Stand up to bullies** and don't tolerate being bullied. Instead of saying, "I am being bullied", say "I will not be bullied even though you are trying."
- **Be kind to others.** Allow others to express opinions you don't like. Listen and engage.
- **Respect people's privacy.** If you feel uncomfortable knowing someone is obsessively checking your profile, you shouldn't do the same.
- **Whenever you share something, stop to think about the content.** Is it verified and reliable? Is it factually sound? Is it offensive? Is it meant to induce fear? Remember that content spreads rapidly online which is why hoaxes spread easily. Do you want to be part of a culture that spread misinformation, or do you want to be someone that can be seen as a reliable source?
- **When sharing, always credit the author.** We often share images without even thinking about the source of the image. Who made it? Who took it? Make sure you give them credit for their work.
- **Do not copy and paste someone else's words** and put them up as your own unless you have permission from the author to do so. You don't plagiarise in university so you should refrain from doing so online.
- Do not upload someone's picture without their consent. We often upload pictures without people's permission and don't realise what the repercussions could be for them. They may get into all sorts of trouble so we must remain mindful of repercussions. **Consent is crucial.**
- **People say all sorts of silly things sometimes,** often without thinking. We have gut reactions and we accept that as part of being human. However, when we express gut reactions in front of someone, they can see our body language and our expressions. **They may get appalled** but they realise that it is not okay to judge someone for saying something they may not agree with. This is not the case in cyberspace however.
- Remember that nothing gets lost in cyberspace. We do not see faces or hear tones; we only see words and we impose our emotions on them. We react to people's reactions. We start to see them through our own lens. This lens is biased. We read take one article or tweet and decide whether we like or dislike someone. In other words, **we become very judgemental** which gets in the way of changing the culture. **Try the opposite.** Try not reacting and judging so that you can see the human instead of just their words.
- It is easy to become part of the crowd. Sometimes users on social media decide something is worthy of ridicule and start to mock it. It can be an article expressing an unpopular opinion. Some ideologies are also seen as worthy of mockery such as feminism. While some find this fun, this is a form of bullying. When a member of a group knows they will be mocked for expressing themselves, they will hesitate to do so. Try not to become part of the problem. Instead, resist the urge to join in and become part of the solution. **Resist the mob mentality!**

- Many people hide their bigotry behind humour. They make offensive jokes such as sexist jokes and further mock those who try to explain to them that such jokes are bullying. If someone suspects they will be ridiculed, they will hesitate to express themselves. Even if you find it funny, if a joke is offensive to any group, do not share it or encourage it because this is a form of violence which is largely psychological in nature. **Resist becoming part of the problem.**
- Sometimes people lash out at others behind the safety of their screens. They say things that are hurtful and this is especially difficult if it is someone you know such as a friend who have always had pleasant interactions with. If a friend is suddenly hostile, remember that there is a human behind that avatar who may be going through a hard time. Instead of reacting, reach out to them. **If they realise they upset you, learn to forgive as well.**
- If you have influence online, remember that it is a privilege that the vast majority do not have. You are in a position of power and you get to decide how to use that power. You can use it positively to help change the culture. **Be aware of that power and use it wisely.**

We hope you can apply these tips and want to join those of us who want to make the internet a safe space. If we harness our collective power, we are confident it can change.

#OccupyCyberSpaces #HamaraInternetKyaHai

RESOURCE LIST

There are many websites you can consult for digital security. Here are some we recommend.

Heartmob <https://iheartmob.org/>

Crash Override <https://www.crashoverridenetwork.com/>

Troll Busters <http://www.troll-busters.com/>

Zen manual

https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual

Tactical Tech's Security In A Box <https://securityinabox.org/en>



HAMARA
INTERNET

مختلف ذرائع کی تفصیل

ڈیجیٹل دفاع کے لیے آپ کو بہت سی ویب سائٹس مل سکتی ہیں۔ ان میں سے چند ایک ہم آپ کے لیے تجویز کرتے ہیں۔

Heartmob <https://heartmob.org/> ★

Crash Oversight <https://www.crashoverridenetwork.com/> ★

Troll Busters <http://www.troll-busters.com/> ★

Zen manual ★

https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual

Tactical Tech's Security In Box <https://securityinbox.org/en> ★

★ بہت سے لوگ اپنے تعصب بھرے ذہن پر مزاح کا پردہ ڈال دیتے ہیں۔ ایسے لوگ جنسی قسم کے توہین آمیز لطیفے بناتے ہیں اور مزید جب ان سے کوئی ہلنگ کی شکایت کرتا ہے تو وہ آگے سے مذاق اڑاتے ہیں۔ اگر کسی کو یہ اندیشہ ہو کہ ان کا تمسخر اڑایا جائے گا تو پھر وہ اپنی رائے دینے سے ہچکچاتے ہیں۔ اگر کسی جماعت کے لیے کوئی لطیفہ توہین آمیز ہوتا ہے وہ کتنا ہی مزاحیہ ہی کیوں نہ ہو، اسے شیر یا اس کی حوصلہ افزائی کبھی نہ کریں کیونکہ یہ بھی تشدد کی ایک شکل ہے جس کا نفسیاتی طور پر استعمال کیا جاتا ہے۔ ان معاملات پر مزاحمت کرنے سے مسائل کھڑے ہو سکتے ہیں۔

☆ بعض لوگ حفاظتی سکرین کے پیچھے سے دوسروں پر وار کرتے ہیں۔ وہ کوئی ایسی بات کر دیتے ہیں جو بہت تکلیف دہ ہوتی ہے اور خاص طور پر اگر ایسا آپ کے کسی جان پہچان والے شخص کے ساتھ ہو۔ تاہم ایک بات یاد رہے کہ اس اواٹار (Avatar) کے پیچھے ایک انسان موجود ہے جو شاید کسی مشکل وقت سے گزر رہا ہو۔ ایسی باتوں پر رد عمل دکھانے کی بجائے اس تک پہنچیں۔ اگر وہ اپنی غلطی مان لے تو پھر معاف کرنا بھی سیکھ لیں۔

★ اسی طرح اگر آپ کے مزاج میں ناگواری پیدا ہو رہی ہے اور آپ کے غصے کو ابھارا جا رہا ہے تو اپنی ڈیوائس سے کہیں دور چلے جائیں۔ اسے خود سے دور رکھیں۔ باہر گھومنے چلے جائیں اور جب مزاج میں کچھ بہتری آئے تو واپس آن لائن آجائیں۔

★ اگر آپ آن لائن اثر و رسوخ رکھتی ہیں تو یاد رہے یہ آپ خصوصی اہمیت کے حامل ہیں ورنہ ہر کسی کو ایسی اہمیت حاصل نہیں ہوتی۔ آپ کو ایک طاقت ور حیثیت حاصل ہے اور آپ کو یہ فیصلہ کرنا ہے کہ اس طاقت کا استعمال کیسے کرنا ہے۔ آپ اس کا مثبت استعمال کر کے ثقافتی تبدیلی لانے میں مددگار ثابت ہو سکتے ہیں۔ اپنی اس طاقت سے باخبر رہیے اور دانشمندانہ طریقے سے اس کا استعمال کریں۔

ہم اُمید کرتے ہیں کہ آپ ان تجاویز کو بروئے کار لاسکتی ہیں اور ہمارے ساتھ شامل ہو کر انٹرنیٹ کو ایک محفوظ جگہ بنانا چاہیں گی۔ اگر ہم اپنی مجتمع طاقت کے ساتھ کمر کس لیں تو ہم پورے اعتماد کے ساتھ ایک مثبت تبدیلی لاسکتی ہیں۔

#OccupyCyberSpace

★ کسی کے الفاظ کی ہو بہو نقل اُتار کر انہیں اپنا بنا کر پیش مت کریں بلکہ ایسا کرنے سے پہلے ان الفاظ کے تخلیق کار سے ضرور اجازت لے لیں۔ آپ یونیورسٹی میں کسی قسم کی چوری نہیں کرتے لہذا آں لائن بھی ایسا کرنے سے باز رہیں۔

★ کسی کی تصویر اس کی رضامندی کے بغیر آپ لوڈ نہ کریں، ہم اکثر ایسا بغیر اجازت کرتے ہیں اور اس حقیقت سے واقف نہیں ہوتے کہ ان کے کیا نتائج برآمد ہوں گے۔ ایسے لوگ جن کی تصاویر آپ بغیر رضامندی کے بھیج دیتے ہیں ان کے لیے کتنے مسائل کھڑے ہو سکتے ہیں لہذا ہمیں ان نتائج سے آگاہ رہنا چاہیے۔ رضامندی بہت اہم ہے۔

★ بعض دفعہ لوگ بہت سی اچھی باتیں بغیر سوچے سمجھے کر جاتے ہیں اور ہم فوری ردِ عمل دکھاتے ہوئے اسے ایک انسان ہونے کے ناطے قبول کر لیتے ہیں۔ تاہم جب ہم ایسا فوری ردِ عمل کسی کے سامنے کرتے ہیں تو وہ ہماری جسمانی حرکات اور ہمارے تاثرات جان رہے ہوتے ہیں۔ وہ کو فرزدہ تو ہو رہے ہوتے ہیں لیکن وہ اس بات سے بھی واقف ہوتے ہیں کہ ان کا کسی کو جج کرنا ٹھیک بات نہیں ہے۔ تاہم سائبر سپیس میں ایسا کچھ نہیں ہوتا۔ یاد رکھیں سائبر سپیس میں کوئی کسی کی حرکات کو نہیں دیکھ رہا ہوتا۔ نہ ہی ہم چہرے دیکھ رہے ہوتے ہیں نہ ہی کسی کی جسمانی حرکات و سکنات کا پتہ چلتا ہے، ہم صرف الفاظ دیکھ رہے ہوتے ہیں اور ہم اپنے جذبات انہیں الفاظ کے ساتھ نتھی کر دیتے ہیں۔ ہم لوگوں کے ردِ عمل پر اپنا ردِ عمل دکھاتے ہیں۔ ہم انہیں اپنے ہی سانچے سے پرکھ رہے ہوتے ہیں۔ ایسا سانچا ہمیشہ متعصب ہی ہوتا ہے۔ ہم کیا کرتے ہیں کہ کوئی سا ایک آرٹیکل یا ٹویٹ کو لے کر یہ فیصلہ کرنا شروع کر دیتے ہیں کہ ہم اسے پسند کریں یا نا پسند۔ دوسرے الفاظ میں یوں کہیں تو بے جا نہ ہوگا کہ ہم اپنے آپ میں جج بن جاتے ہیں اور یہ چیز ثقافتی تبدیلی کی راہ میں حائل ہوتی ہے۔ اس سے ہٹ کر یہ کیا کریں کہ ردِ عمل اور دوسروں کو جج کرنا چھوڑ دیں تاکہ دوسرے آپ کو الفاظ کی بجائے انسان نظر آئیں۔

★ کسی بھی مجمع کا حصہ بننا بہت آسان ہوتا ہے۔ بعض دفعہ صارفین سوشل میڈیا پر کسی بے ہودہ چیز کو ہاتھوں ہاتھ لیتے ہیں اور اس کا مذاق اڑانا شروع کر دیتے ہیں۔ وہ کوئی ایسا آرٹیکل ہو سکتا ہے جو غیر مقبول رائے رکھتا ہو۔ نظریہ حقوقِ نسواں جیسے نظریات کو بھی مذاق کے قابل سمجھا جاتا ہے۔ یہ بھی ایک قسم کی بلیک ہوتی ہے۔ جب کسی جماعت کا کوئی رکن یہ سمجھتا ہے کہ انہیں خود کو ظاہر کرنے پر ان کا مذاق اڑایا جائے گا تو وہ اپنے خیالات کا اظہار ہی کرنا چھوڑ دیتے ہیں۔ کوشش کریں کہ آپ مسائل کا حصہ نہ بنیں۔ بلکہ آگے بڑھ کر اس میں شامل ہو کر مزاحمت کریں اور مسائل کے حل میں اپنا حصہ ڈالیں۔ فسادِ ذہنوں سے دور رہیں۔

کیا آپ ایک طبعی مقام پر اپنی ایسی سہیلی کی مدد کریں گی جس پر حملہ ہوا ہو؟ ہم یہ تصور کر رہے ہیں کہ آپ اسی وقت اٹھیں اور اس سہیلی کی مدد کریں۔ ہم یہ بھی جانتے ہیں کہ آپ اپنی اس سہیلی کی جگہ یہ جانتے ہوئے خود ڈرین گی کہ اس کے مزید کچھ کہنے سے وہ خود کافی پریشان ہو جائے گی۔

کیا آپ اپنی کسی ایسی سہیلی یا رشتے دار کی مدد کرتی ہیں جسے سائبر بلیڈ کیا گیا ہو؟ کیا آپ اس کو گالی دینے والے کو منہ توڑ جواب دیتی ہیں؟ کیا آپ اپنے مخالف حریف کو منہ توڑ جواب دینے کی کوشش کرتی ہیں؟

یہاں ہم آپ کو چند بنیادی تجاویز دیتے ہیں جنہیں آپ انٹرنیٹ کو ایک محفوظ مقام بنانے کے لیے استعمال کر سکتی ہیں۔ سب سے پیچیدہ بات یہ ہے کہ آپ آن لائن ایسا رویہ رکھیں جیسا کہ آپ آف لائن رکھتی ہیں۔

★ آن لائن ہمیشہ ایسے ہی حمایت کریں جیسے آپ آف لائن کرتی ہیں۔ اگر ایک سہیلی کو بلیڈ کر دیا گیا ہے تو ہمیشہ اس کے ساتھ رہیں اور اس کا مسئلہ حل کرنے میں اس کا ساتھ دیں تاکہ اس سے کنارہ کشی کریں۔

★ بلیڈ ہونا کسی صورت گوارہ نہ کریں اور بلیز کے خلاف کھڑے ہو جائیں۔ ”مجھے بلیڈ کیا جا رہا ہے“ کہنے کی بجائے یہ کہیں ”میں بلیڈ کبھی نہیں ہوں گی اگرچہ تم ایسا کرنے کی کوشش کر رہے ہو“۔

★ دوسروں کے ساتھ نرمی سے پیش آئیں۔ دوسروں کو آپ کی ناپسندیدہ رائے کا اظہار کرنے دیں۔ اسے سنیں اور برسرِ پیکار ہو جائیں۔

★ لوگوں کی پرائیویسی کا خیال رکھیں۔ اگر کوئی آپ پر حاوی ہوتے ہوئے آپ کی پروفائل جاننے کی کوشش کرتا ہے اور آپ کو یہ جان کر بُرا لگتا ہے تو آپ بھی اسی کی طرح نہ کریں۔

★ جب بھی آپ کوئی معلومات شیئر کرنے لگیں تو خود سے یہ سوالات ضرور کریں کیا یہ معلومات موزوں اور تصدیق شدہ ہیں؟ کیا یہ حقیقت پر مبنی ہیں؟ کیا یہ توہین آمیز ہیں؟ کہیں اس کا مقصد خوف پھیلانا تو نہیں۔ یاد رکھیں کوئی بھی معلومات انٹرنیٹ پر تیزی سے پھیلتی ہیں اسی وجہ سے دھوکہ بازی آسانی سے پھیلتی ہے۔ کیا آپ کسی ایسی ثقافت کا حصہ بننا چاہتی ہیں جس کا مقصد جھوٹی خبروں کو پھیلانا ہو، یا آپ خود کو ایک معتذر ذریعہ بنانا چاہتے ہیں؟ فیصلہ آپ پر ہے۔

★ جب بھی کوئی کام شیئر کریں تو اس کے مصنف کو ضرور سراہیں۔ ہم اکثر تصاویر کو یہ سوچے بغیر شیئر کر دیتے ہیں کہ اسے کس نے بنایا؟ کس نے اٹھایا ہے؟ اس بات کو ہمیشہ یقینی بنائیں کہ آپ دوسروں کے کیے گئے کام پر اسے ضرور سراہیں گی۔

یہ کوئی حیرت کی بات نہیں ہے کہ طاقت ور ہر مقام پر اپنی طاقت برقرار رکھنا چاہتا ہے یہی وجہ ہے کہ پسماندہ جماعتوں کے لوگ آن لائن گالیاں کھا کر بس کر دیتے ہیں۔ وہ ہم سے تسلیم کروانا چاہتے ہیں کہ ہر جگہ ان کے لیے ہے اور ہم کسی چیز کے بھی دعوے دار نہ ہوں۔ ہم جتنی آگے بڑھنے کی کوشش کرتی ہیں اتنا ہی ہمیں ناکامی کا سامنا کرنا پڑتا ہے۔

لیکن یہ کوئی بری خبر نہیں ہے۔ آن لائن مقامات کا انحصار صارفین کے مرتب رویے پر ہوتا ہے اور ہم بحیثیت صارف اپنی ثقافت کی تشکیل کے ضامن ہوتے ہیں۔ ثقافتیں بدل کر خصوصاً آج کے تیز ترین دور کو مرتب کرتی ہیں۔ آج کے دور کے ضامن ہوتے ہوئے اگر ہمیں انٹرنیٹ کو سب کے لیے محفوظ بنانا ہے تو ابھی فیصلہ کرتا ہے۔ کیا آپ اس دنیا کا تصور کر سکتی ہیں جس میں آن لائن رہ کر لوگ اچھے اخلاق کو فروغ دیں؟

تبدیلی آپ سے شروع ہوتی ہے۔ دوسروں پر انگلی اٹھانا بہت آسان ہوتا ہے اور خود کو مسائل پیدا کرنے کا موجب ٹھہرانا سب سے زیادہ مشکل ہوتا ہے۔ اپنے آپ کو یاد دلاتی رہیں کہ آپ کو سائبر بلی نہیں کیا جاسکتا اور اس بات پر ڈٹی رہیں کہ سائبر بلنگ عام ہوگئی ہے اور اسے آن لائن تجربے کے طور پر تسلیم کریں۔ لوگوں اپنی زندگیوں میں سائبر بلیڈ ہونے کے لیے خود کو تیار رکھیں۔ درحقیقت ایسا ہونا نہیں چاہیے۔

ہمیں انٹرنیٹ کا بہترین باشندہ بننے کے لیے کچھ قواعد کے ساتھ چلنا پڑے گا۔ مثال کے طور پر ہمیں کوشش کرنی چاہیے کہ ہم آن لائن اپنے غصے کو ہوانہ دیں۔ ہمیں اس بات کے لیے خبردار رہنا پڑے گا کہ ہمارے اوپر گالیوں کی بوچھاڑ ہو سکتی ہے اور کسی کی جانب سے ہمیں ہدف بنایا جاسکتا ہے محض اس لیے کہ شاید ہمارے لیے وہ ایک بُرا دن ہو۔ الغرض ہمیں خود کو چوکنا رکھنا چاہیے۔

انسان ایک معاشرتی جانور ہے جو لوگوں کی اس جماعت کے ساتھ رہنا پسند کرتا ہے جنہیں وہ سمجھتا ہو کہ اس کی بات سنیں گے۔ اس لیے ہم اپنے رشتہ داروں اور احباب کو اہمیت دیتے ہیں۔ جب وہ کسی مشکل میں پڑتے ہیں تو ہم ان کی مدد کرتے ہیں کبھی کبھار تو اس وقت بھی مدد کرنی پڑتی ہے جب ہم ان سے اتفاق نہیں کر رہے ہوتے۔

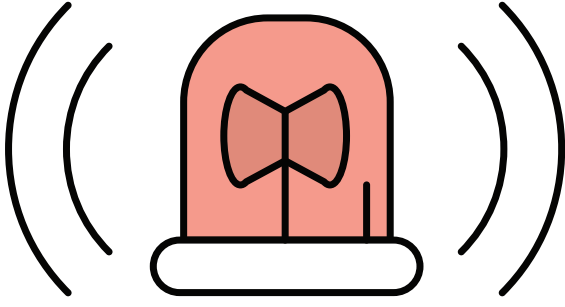
”ہمارا انٹرنیٹ“ کی تشکیل

ایک ملک کا باشندہ ہونے کے ناطے آپ اپنے ملک کے ساتھ ہونے والے سماجی معاہدوں سے باخبر رہتی ہیں۔ تاہم انٹرنیٹ کی نہ تو کوئی ریاست ہوتی ہے نہ ہی کوئی حکومت ہوتی ہے اور نہ ہی کوئی ظاہری سماجی معاہدے جیسی کوئی چیز ہوتی ہے۔

یہی وجہ ہے کہ بعض دفعہ انٹرنیٹ ایک تاریک اور ڈراؤنی جگہ بن سکتی ہے۔ بنی نوع انسان کی تاریخ میں یہ بات روزِ اول سے پائی جاتی ہے کہ وہ طاقت کا استعمال کرتے ہیں اور طاقت کی خواہش کو بڑھانے کے لیے انسانوں نے بہت سے نئے ہتھیار بنالیے ہیں۔ ہم غذائی تسلسل پر بڑی شیخی بگھارتے ہیں۔ ہم طاقت رکھنے اور اپنی طاقت کے استعمال پر بہت فخر کرتے ہیں۔

انٹرنیٹ جیسی جدید ٹیکنالوجی بھی ایک طاقت ور حلقہ ہے جو اس کے استعمال کی استطاعت رکھ سکتے ہیں وہ اس پہ بہت سی جگہ حاصل کر لیتے ہیں۔ جو لوگ اس بات کو اپنا استحقاق سمجھتے ہوئے پوسٹ بھیجتے ہیں انہیں بہت کچھ سننا بھی پڑتا ہے۔ جو لوگ مقبول رائے پر تنقید کرتے ہیں ان کی نسبت وہ لوگ زیادہ آسانی سے مقبولیت حاصل کر لیتے ہیں جو ایسی بات کا زیادہ پرچار کرتے ہیں جو ہر عام انسان سننا چاہتا ہے۔

پاکستان میں خواتین کی نسبت مرد صارفین کی تعداد کافی زیادہ ہے۔ سب نہیں لیکن زیادہ تر مرد چاہے آن لائن ہوں یا آف لائن تشدد کا استعمال خواتین یا دوسری غیر محفوظ جماعتوں کو خاموش کرانے کے لیے کرتے ہیں۔ ہمارے لیے تو گالیاں بھی محفوظ نہیں رہی، کیونکہ جس جگہ کو اپنی ملکیت سمجھتی ہیں اس میں ہمارے لیے جگہ نہیں ہوتی۔ اسی وجہ سے دفاتر بھی نقصان دہ ہو سکتے ہیں اور پھر ایک کبھی نہ ختم ہونے والی تفصیل موجود ہے۔



مجھے مدد چاہیے

PCSW

1043

RESCUE

1122

FIA

9911

CYBER

HARASSMENT
HELPLINE

PTA

0800

55055

ROZAN

HELPLINE

0800

22444

0800 39393

POLICE

EMERGENCY

15

کیا آپ جانتے ہیں؟

- 70 فیصد عورتیں قانون نافذ کرنے والے اداروں کو cyber harassment رپورٹ نہیں کرتیں *
- 47 فیصد عورتوں کا ماننا ہے کہ قانون نافذ کرنے والے ادارے انکی شکایات کو سنجیدہ نہیں لیں گے *
- 45 فیصد عورتوں کا ماننا ہے کہ قانون نافذ کرنے والے اداروں سے حراست کی بات کرنا شرمندگی کا باعث ہے *
- 72 فیصد عورتیں cyber harassment کے متعلق پاکستان میں کسی بھی قانون سے ناواقف ہیں **
- صرف 51 فیصد عورتیں شوکل میڈیا ویب سائٹ کے قوانین و ضوابط سے واقف ہیں **
- 18 سال سے کم عمر لڑکیوں میں تقریباً 55 فیصد اسمارٹ فون کا استعمال نہیں کرتیں **
- 67 فیصد عورتیں (ہمارے ریسرچ سامپل کے مطابق) انٹرنیٹ پر فیس بک کا استعمال کرتی ہیں **
- 25 سال سے زائد تقریباً 81 فیصد عورتیں فیس بک کا استعمال کرتی ہیں **
- 79 فیصد عورتیں روزانہ اپنے موبائل فون / لیپ ٹاپ کا استعمال کرتی ہیں **
- 50 فیصد عورتیں ہماری تحقیق کے مطابق فیس بک کو آن لائن حراست کے لئے سب سے برا قرار دیتی ہیں **
- 70 فیصد عورتیں اپنی تصویریں آن لائن لگانے سے اسلیپ ڈرتی ہیں کہ کہیں کوئی غلط استعمال نہ کر لے **
- 25 فیصد عورتوں نے آن لائن کسی لڑکی کو لڑکے کے ہاتھوں ہراساں ہوتے دیکھا ہے **
- 40 فیصد عورتوں کا تعاقب اور حراست messaging app کے ذریعے کی گئی ہے **
- 48 فیصد عورتیں کسی ایسی عورت کو جانتی ہیں جس نے حراست کے بعد انٹرنیٹ کا استعمال بند کر دیا *

* cyber harassment ہیلپ لائن کی پہلے سال کی رپورٹ

** پاکستانی عورتوں کے آن لائن تشدد کے تجربات

• ایف-آئی-اے کورپورٹ کرنا:

اگر آپ کو آن لائن ہراسیت کا نشانہ بنایا جاتا ہے تو آپ خاموش نہ رہیں۔
سائبر کرائم کی قریبی سائبر کرائم کے نیشنل ریسپونس سینٹر کی شاخ میں
رپورٹ ہونی چاہیے۔

ایف-آئی-اے کی شاخیں مندرجہ ذیل شہروں میں موجود ہیں۔

✓ کراچی

✓ لاہور

✓ کوئٹہ

✓ پشاور

✓ راولپنڈی

✓ اسلام آباد

ایف-آئی-اے کی ہیلپ لائن 9911

اس کے علاوہ مندرجہ ذیل آن لائن فارم کے ذریعے بھی ان سے رابطہ کیا جاسکتا ہے:

<http://www.nr3c.gov.pk/creport.php>

تیسرا مرحلہ

سائبر ہراسمنٹ ہیلپ لائن پر رابطہ کرنا:

اگر آپ اس الجھن کا شکار ہیں کہ قانون نافذ کرنے والے اداروں سے کیسے رابطہ کریں یا آپ کو اس سلسلے میں مزید مدد دینے والے ہوتو ڈیجیٹل رائٹس فاؤنڈیشن
کی سائبر ہراسمنٹ ہیلپ لائن پر رابطہ کرتے ہوئے ہچکچاہٹ کا شکار نہ ہوں۔ یہ ہیلپ لائن یکم دسمبر 2016 کو آغاز ہوئی، یہ پاکستان کی پہلی وقف شدہ
ہیلپ لائن ہے جو کہ آن لائن ہراسیت اور تشدد جیسے مسائل کے خلاف مفت، محفوظ، صنفی حساس اور آزادانہ حل فراہم کرتی ہے۔ ہیلپ لائن کا عملہ آن لائن
ہراسمنٹ کے شکار لوگوں کو قانونی مشورہ، ڈیجیٹل سیکورٹی کے مسائل میں مدد اور نفسیاتی مشاورت مہیا کرتے ہیں۔

ٹول فری نمبر **0800-39393** ہفتے کے سات دن صبح 9 بجے سے شام 5 بجے تک لوگوں کی مدد کے لیے مہیا ہوتا ہے۔

ہیلپ لائن کے عملے سے ای میل اور فیس بک کے ذریعے رابطہ کیا جاسکتا ہے۔

helpdesk@digitalrightsfoundation.pk

<https://www.facebook.com/DigitalRightsFoundation/>



**CYBER
HARASSMENT
HELPLINE**

**0800-39393
EVERYDAY
9 AM - 5 PM**



CYBER HARASSMENT HELPLINE

پہلا مرحلہ

سوشل میڈیا کو سائبر ہراسیت کے لیے رپورٹ کریں:
آپ کا سوشل میڈیا آپ کی سوچ سے بھی زیادہ ذمہ دار ہے، اگر آپ آن لائن ہوتے ہوئے بے سکون محسوس کریں تو اپنے طور پر مندرجہ ذیل طریقے استعمال کریں۔ یہ آسان اور موثر ہیں۔

نجی معلومات کی پوشیدگی کی خلاف ورزی:

فیس بک:

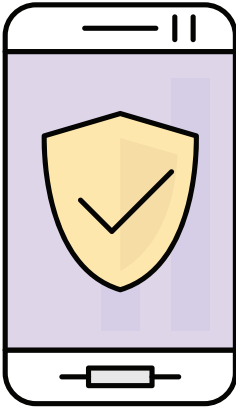
اگر کوئی آپ کی تصاویر، ویڈیوز اور دوسری معلومات آپ کی اجازت کے بغیر استعمال کر رہا ہو تو اس کو رپورٹ کرنے کے لیے مندرجہ ذیل فارم پر کریں۔

<https://www.facebook.com/help/contact/144059062408922>

انسٹا گرام:

اگر کوئی آپ کی تصاویر، ویڈیوز اور دوسری معلومات آپ کی اجازت کے بغیر استعمال کر رہا ہو تو اس کو رپورٹ کرنے کے لیے مندرجہ ذیل فارم پر کریں۔

<https://help.instagram.com/contact/482633291790470>



• سائبر ہراسیت کے لیے فیس بک کو رپورٹ کرنا:

سائبر ہراسیت کے لیے فیس بک کو رپورٹ کرنے کے لیے مندرجہ ذیل لنک استعمال کریں۔

<https://www.facebook.com/help/?help>

• سائبر ہراسیت کے لیے ٹویٹر کو رپورٹ کرنا:

سائبر ہراسیت کے لیے ٹویٹر کو رپورٹ کرنے کے لیے مندرجہ ذیل لنک استعمال کریں۔

<https://support.twitter.com/>

<https://help.twitter.com/en/rules-and-policies/twitter-report-violation>

• سائبر ہراسیت کے لیے انسٹا گرام کو رپورٹ کرنا:

سائبر ہراسیت کے لیے انسٹا گرام کو رپورٹ کرنے کے لیے مندرجہ ذیل لنک استعمال کریں۔

<https://help.instagram.com/>

• سائبر ہراسیت کے لیے سنپ چیٹ کو رپورٹ کرنا:

سائبر ہراسیت کے لیے سنپ چیٹ کو رپورٹ کرنے کے لیے مندرجہ ذیل لنک استعمال کریں۔

<https://support.snapchat.com/en-US>

دوسرا مرحلہ

قانون نافذ کرنے والے اداروں کو رپورٹ کرنا:

اگر آپ ایسی صورت حال سے دوچار ہوں جس میں آپ کو پولیس سے رہنمائی کی ضرورت ہو تو سائبر کرائم کے نیشنل ریسپانس سینٹر (ایف-آئی-اے) کو رپورٹ درج کروائیں۔ ایک درخواست بمعہ سکریں شاٹ، پرنٹ کی شکل میں، ثبوت کے طور پر جمع کروانے کی ضرورت ہوتی ہے۔

آپ انہی ہدایات پر عمل کریں جو آپ طبعی زندگی میں کریں گی۔ آپ ان مقامات پر جاتی ہیں جہاں آپ خود کو محفوظ سمجھتی ہیں خاص طور پر جب آپ اپنے دوستوں سے ایسی گفتگو کرنی پڑے جو آپ چاہتی ہوں کہ اسے کوئی اور نہ سنے۔ آپ کبھی یہ نہیں چاہیں گی کہ کوئی آپ پہ چلائے۔ لوگ اس بات کو سمجھتے ہیں کہ انہیں کسی بھی عوامی مقام پر آپ پر حملہ کرنے کی اجازت نہیں ملے گی اس لیے وہ ایسا کرنے سے ہچکچائیں گے۔

پس اس مشق کو روزمرہ کے تجربے کے طور پر کریں: آپ کا آن لائن مقام اتنا ہی اہم ہونا چاہیے جتنا آپ کا آف لائن مقام۔ دونوں مقام ایسے ہونے چاہئیں کہ جہاں آپ بہت کچھ سیکھ بھی سکیں اور اپنے خیالات، جذبات اور احساسات کا اظہار کر سکیں۔ دونوں مقامات آپ کے علم میں اضافہ کریں گے اور کبھی کبھی آپ کو اپنا ذہن بدلنے کی بھی ضرورت پڑے گی ان باتوں کے لیے جن پہ آپ کے خیالات کو چیلنج کیا گیا ہو۔

انٹرنیٹ کو ایک محفوظ مقام پر چلانے کے لیے سب سے بہترین طریقہ یہ ہے کہ آن لائن ہر اسٹاپ ہوئے لوگوں کے حامی گروپس ایسی جگہ مرتب کریں جہاں وہ ایک دوسرے کی حمایت کر سکتے ہوں۔ آپ کا مرتب کیا ہوا محفوظ مقام ایک ایسا پلیٹ فارم بن سکتا ہے جہاں آپ حامی گروپس مرتب کر سکتے ہیں اور کسی عیار یا مکار بندے کے حملے سے مل کر نیٹننے کے لیے ایک جگہ ڈٹے رہ سکتے ہیں۔



احتیاط

ایک محفوظ مقام کو برقرار رکھنا پیچیدہ مرحلہ ہوتا ہے۔
بعض دفعہ ایک مباحثی گروپ بہت مقبول ہوتا ہے اور
صارفین اس میں شامل ہونا چاہتے ہیں۔

تجویز

چند ایسے اصول بنائیں کہ اس محفوظ مقام
میں کن لوگوں کو شامل نہیں کرنا چاہیے۔

- ★ آپ کی روایات کیا ہیں؟ جو انہیں سمجھتے ہیں انہیں شامل ہونا چاہیے۔ اگر کوئی اس سے صرف نظر کرتا ہے لیکن وہ انہیں سمجھنا چاہتا ہے تو اس صارف کو اپنے گروپ میں رکھنے کے لیے آپ کو مشاورت کے بعد فیصلہ لینا چاہیے۔
- ★ سیکھنے اور اپنے نظریات کو چیلنج ہونے پر خندہ پیشانی کا ثبوت دیں۔
- ★ اپنے گروپ سے معلومات کا باہر آنے اور نو سکریں کچرنگ جیسی حکمت عملیوں کے ساتھ آئیں۔
- ★ اپنے ان جوازوں کے بارے میں سوچئے جو آپ ان لوگوں کو دیتے ہیں جو دوسروں پر ذاتی حملے کرتے ہیں اور جو کسی کی رازداری کی روگردانی کرتے ہیں۔
- ★ بحث و مباحثہ زور پکڑتے رہتے ہیں۔ یہ بات تب تک ٹھیک ہے جب تک سب کا احترام کیا جا رہا ہو اور دوسروں کے خیالات کو سننے کی کوشش کی جاتی رہی ہو۔ اپنے ذہن کو کشادہ کریں۔
- ★ جب ایک گفتگو ناگوار صورت حال اختیار کر جائے تو اس وقت کیا کرنا چاہیے؟ ان حکمت عملیوں سے وابستہ رہیں جو ایک ایسی صورت حال سے نمٹنے سے متعلق ہوں۔

جو ایسے مسائل سے نبرد آزما ہونا جانتی تھی۔

ان خواتین نے یہ فیصلہ بھی کیا کہ ایک دوسرے کی مدد کرنے کے لیے ایک حمایتی گروپ تشکیل دیا جائے۔ معلوم کرنے پر اسے پتہ چلا کہ جن خواتین کو ایسی نفرت انگیزی کا سامنا کرنا پڑا ان میں سے زیادہ تر خواتین عام حالات سے ذرا ہٹ کر انسانی حقوق کی باتیں کرتی تھیں۔ خواتین صحافیوں اور مصنفین نے اسے بتایا کہ وہ ایسی عیار یا مکار باتوں کی عادی ہو گئی تھیں اور یہ باتیں اب انہیں زیادہ پریشان نہیں کرتی۔ آمنہ کے لیے یہ بڑی تشویش ناک بات تھی۔ کیونکہ انسان کسی اور سے نبرد آزما ہونے کے لیے احساسات سے عاری کیسے ہو سکتا ہے۔

آئین پاکستان کی شق ۱۹ یہ بتاتی ہے کہ ہم 'معقول شرائط کے ساتھ' تقریری آزادی رکھتے ہیں، جس کا مطلب یہ ہوا کہ یہ حق مکمل نہیں ہے۔

#KnowYourRights

آمنہ نے سب سے پہلا قدم یہ اٹھایا کہ اعتدال پسندانہ تبصرے دینے شروع کیے اور کسی بھی نفرت انگیز تبصرے کی حمایت کرنا ترک کر دی۔ جب اسے تنگ کرنے والوں کو یہ بات سمجھ آئی کہ وہ ان کی گالیوں کی کوئی پروا نہیں کرتی تو انہوں نے اسے تنگ کرنا چھوڑ دیا۔ لیکن ان میں سے ایک نے تبصرے دینا بند نہ کیا۔ اپنے حامی گروپ سے رابطہ کرنے پر اس کی یہ مدد ہوئی کہ اس دھمکی آمیز تبصرہ کرنے والے شخص کی رپورٹ کر دی گئی۔ ان تبصروں کو ختم ہونے میں چند ماہ لگ گئے لیکن اب بھی آمنہ کو کبھی کبھار کچھ خوفناک قسم کی ای میلز اور تبصروں کا سامنا کرنا پڑتا ہے۔ اب آمنہ سمجھ چکی ہے کہ ایسے تبصرے اسے خاموش کرانے کے لیے بھیجے جاتے ہیں۔ لیکن اب اس نے اپنی تحریریں بھی جاری کرنا شروع کر دی ہیں اور ایسے ہتھکنڈوں کے سامنے ہتھیار پھینکنے سے انکار کر دیا ہے اور اب وہ اپنے بلیز کو جیتنے کا کوئی موقع فراہم نہیں کرتی۔

اسی لیے ہتھیار ڈالنے کی بجائے سائبر پلیٹ فارم جیسے سوشل میڈیا پر رہنا نہایت اہمیت کا حامل ہے۔ اسی لیے ہم محفوظ وسعتیں تشکیل کرنے کی حمایت کرتے ہیں۔

سوشل میڈیا یا ایک میلنگ لسٹ پر ایک نزدیکی گروپ تشکیل دے کر ایک محفوظ جگہ مرتب کی جاسکتی ہے۔ یہ ایک کلوزڈ بلاگ یا ایک فورم بھی ہو سکتا ہے۔

★ اگر آپ اپنا اکاؤنٹ ڈی ایکٹیوٹ کر دیتے ہیں تو سمجھیں آپ کو تنگ کرنے والا جیت گیا۔ آپ نے اسے مزید شہ دے دی ہے۔ اب وہ مزید طاقتور ہو گیا ہے اور اسے مزید شہل گئی ہے۔ اب وہ سوچے گا کہ وہ ہر اس کے اپنے مذموم مقاصد حاصل کر سکتا ہے۔

★ کیا عورتوں کے لیے محفوظ جگہ ہے؟ جب عورتوں کے خلاف تشدد کی بات ہوتی ہے تو یقیناً ہم کہیں پھر بھی محفوظ نہیں ہیں۔ نہ ہی ہم اپنے گھروں میں محفوظ ہیں، نہ ہی پبلک مقامات پر اور نہ ہی کام کاج کی جگہ پر۔ کوئی بھی مقام خواتین کے لیے تب تک محفوظ نہیں ہوگا جب تک ہم کسی مقام کا دعویٰ کر کے اسے اپنے لیے محفوظ نہیں بنا لیتی۔

آمنی ایک بلاگر ہے جو خواتین کے حقوق سے متعلق کافی کچھ لکھتی رہتی ہے۔ بہت سے لوگ اس کی رائے سے اتفاق نہیں کرتے اور اسے اپنے بلاگ کے جوابی صفحات پر کافی تنقید کا سامنا بھی کرنا پڑتا ہے۔ ان تبصروں میں سے کافی سارے بد خوئی پر مبنی ہوتے ہیں جن میں سے چند مثالیں مندرجہ ذیل ہیں:

★ اس کام کے لیے تم جہنم جاؤ گی!

★ تمہاری آبروریزی ہونی چاہیے!

★ میں تمہیں قتل کر دوں گا!

★ میں تمہارے چہرے پر تیزاب پھینک دوں گا!

★ تمہاری زندگی بے مقصد اور بے کار ہے!

★ خود کو مار ڈالو!

★ تم بہت موٹی اور بھدی ہو!

★ تم پاگل اور بے کار ہو!

★ کوئی تمہاری بات سننے کو تیار نہیں!

★ کوئی تمہیں پسند نہیں کرتا!

بعض تبصرے کافی لمبے، جامع لیکن پریشان کر دینے والے ہوتے ہیں۔ آمنہ کو جب بھی ایسی جسمانی نقصان پہنچانے کی دھمکیاں موصول ہوتی ہیں تو وہ بہت زیادہ پریشان ہو جاتی۔

در اصل آمنہ اس بات سے ناواقف تھی کہ ان تبصروں سے کیسے نبٹنا ہے۔ جب اس نے دوسری خواتین بلاگرز سے اس بات کا تذکرہ کیا تو اسے پتہ چلا کہ یہ سب سہنے والی وہ اکیلی عورت نہیں تھی۔ ان میں سے بعض کو تو بالکل ویسی ہی دھمکیاں اور تبصروں کا سامنا کرنا پڑا۔ خواتین کی اس جماعت نے اس کی مدد کرتے ہوئے اسے ایک ایکٹیوسٹ سے ملایا

کہا جاتا ہے کہ آپ آف ان ہو جائیں۔ اس کا مطلب یہ ہوا کہ ایک سوشل میڈیا صارف ہونے کے ناتے آپ ان سب باتوں کے خود ذمہ دار ہیں۔ ہم اس بات سے متفق ہرگز نہیں اور ایسا کیوں ہے، آئیے بیان کرتے ہیں۔

ہم اکثر سنتے ہیں:

”آپ پھر بھی آن لائن کیوں ہیں؟“

”آپ اسے بلاک کیوں نہیں کر رہی؟“

”آپ یہ سب پہلے کیوں کر رہی ہو؟“

”درگزر کریں ایسے لوگوں کے منہ مت لگیں!“

”اپنا اکاؤنٹ ڈی ایکٹیوٹ کر دیں۔“

”انٹرنیٹ تو ویسے بھی خواتین کے لیے محفوظ نہیں ہے آپ تنہا کیوں ہو؟“

یہ باتیں ناقابلِ برداشت ہوتی ہیں خصوصاً جب آپ کے جاننے والے آپ کے پیارے ایسا کہیں۔ چونکہ وہ ہمیں پریشان ہوتا نہیں دیکھ سکتے لہذا ایسی باتوں کا انہیں یہی حل نظر آتا ہے۔

یاد رکھیں:

★ آپ آن لائن ہیں کیونکہ انٹرنیٹ استعمال کرنا آپ کا حق ہے اور جو کوئی آپ کو اس کے استعمال سے روکتا ہے تو بنیادی طور پر آپ کو آپ کے حق سے دستبردار کرنا چاہتا ہے۔

★ یہ یصلہ آپ کو کرنا ہے کہ آپ کو کس سے بات کرنی ہے اور کس کو بلاک کرنا ہے۔ بعض لوگ عیار یا مکار لوگوں سے بات شروع کر دیتے ہیں اور بعض دفعہ یہ کام آتی ہے۔ اگر آپ کسی کو بلاک کر دیتی ہیں تو وہ نئی پروفائل بنا لیتے ہیں حالانکہ ہم آپ کو بلاک کرنے کی تجویز دیتے ہیں لیکن ساتھ ساتھ ہم خبردار بھی کرتے ہیں کہ یہ مکمل حل نہیں ہے۔

★ جی ہاں، بعض کمٹس سے درگزر کر جانا چاہیے لیکن درگزر کرنا مسائل کا حل نہیں ہوتا۔

بعض عیار یا مکار تو اتنے بے رحم ہوتے ہیں کہ ہلاک کیے جانے کے باوجود نئی پروفاکل بنا لیتے ہیں۔ آپ ذرا سوچئے وہ ایسا کیوں کرتے ہیں۔ وہ کیوں بار بار گالیاں دیتے ہیں؟ کیا اس لیے کہ وہ غم و غصے سے بھرے ہوتے ہیں؟ یا شاید وہ آپ کو وہاں سے چلتا کرنا چاہتے ہیں؟ ہم سمجھتے ہیں کہ وہ آپ کو خاموش کرنا چاہتے ہیں تو خاموش رہ کر مذاحمت کرنے میں کوئی مضائقہ بھی نہیں۔ جب لوگ کسی غیر مقبول رائے کا اظہار کرتے ہیں تو صارفین اکثر ایسے لوگوں کو چپ کرانے کے بلوائیوں کا سہارا لیتے ہیں۔ لوگ آن لائن دھمکیاں دیتے ہیں کہ دوسرا بندہ زبانی کلامی بھی اپنی رائے نہ دے، بعض دفعہ تو ایسی بھی دھمکیاں دیکھنے کو ملتی ہیں کہ ایسا کرنے سے وہ اپنی موت کو دعوت دے رہے ہیں۔

یاد رکھیں:

اگر کوئی آپ کو آن لائن تنگ کرے یا کوئی ایسی بات کرے جس سے آپ کو پریشانی کا سامنا ہو تو یہ آپ کا قصور نہیں ہے، آپ خواہ ایسی رائے کا اظہار کر رہے ہوں جو دوسروں کو نا پسند ہو تب بھی آپ ایسے سلوک کے مستحق نہیں۔

ذرا سوچئے: آپ پر گالیوں کی بوچھاڑ کی جارہی ہو محض اس لیے کہ آپ کے الفاظ یا آپ کی رائے جو صرف آپ کی ملکیت ہیں ان کو ہدف بنایا جا رہا ہو۔ آپ کو صرف اس لیے نشانہ بنایا جا رہا ہوتا ہے کیونکہ زیادہ تر صارفین جانتے ہیں کہ یہاں ان کی بات زیادہ سنی جائے گی اور ان کی حوصلہ افزائی بھی ہوگی۔ وہ یہ بھی جانتے ہیں کہ آپ کے طبعی مقام پر آپ پر حملہ کرنے سے ان کے لیے مسائل کھڑے ہوں گے۔ مثلاً، اگر وہ آپ پر لیکچر ہال میں برسیں گے یا برا بھلا کہیں گے تو ان کی باز پرس ہوگی۔ لوگ بولیں گے اور آپ کو حمایت بھی ملے گی۔

بلیر جیسے عیار یا مکار لوگ دوسروں پر اپنی طاقت کا مظاہرہ کر کے خوش ہوتے ہیں۔ وہ دوسروں کو پریشان کر کے انہیں خوشی ملتی ہے۔ یہ بھی ہلنگ کرنے کے مترادف ہے کیونکہ ہم اس بات سے آشنا ہیں کہ ہلنگ کرنے سے گالیوں کے ایک دورائے کی تخلیق ہوتی ہے۔ کوئی بھی شخص ایسی صورت میں خود کو کمزور محسوس کرتا ہے کیونکہ ان پر کوئی مسلط ہو کر ان کو بُرا محسوس کرانے پر تڑا ہوا ہے۔ لہذا دوسرا شخص بلیڈ (Bullied) ہونے پر بھڑک جاتا ہے۔ ہار جیت کا یہ عمل بہت مشکل ہوتا ہے، لیکن ناممکن ہرگز نہیں۔ اس صورت میں پہلا قدم ایسی صورت حال سے اچھی طرح سے آگاہ ہونا ہوتا ہے۔

جب کبھی آپ کو آن لائن بلیڈ (Bullied) کیا جاتا ہے اور آپ اس کا اظہار کسی اور سے کرتے ہیں تو آگے سے آپ کو

ساترہرا سمنٹ اور محفوظ مقامات

آپ تصور کریں کہ جب کوئی چاہے آپ کے دروازے پر دستک دے اور آپ کے دروازہ کھولنے پر وہ آپ پر برس پڑے، آپ کو گالیاں دے اور آپ کی بے عزتی کرے۔ یا فرض کریں کوئی آپ کے گھر کے باہر کھڑا ہو کر دن رات آپ پر گالیوں کی بوچھاڑ کرتا ہو۔ لامحالہ ایسی صورت حال میں آپ پولیس کو اطلاع کریں گی اور دیگر لوگ آپ کی مدد کریں گے یا اس شخص کو جاننے کے لیے کہیں گے۔ اس میں کوئی شک نہیں کہ ہم اپنے ظاہری مقام پر پیدا ہونے والے خطرات اور پریشانیوں کو بہت سنجیدگی سے لیتی ہیں لیکن جب بات ساترہرا سپیس کی ہوتی ہے تو اسے سنجیدگی سے نہیں لیتیں۔ ہم اس بات سے بھی بخوبی آگاہ ہیں کہ ہر کسی کا اپنا طبعی مقام ہوتا ہے اور ہم یہ بھی جانتی ہیں کہ ہمیں کسی کے طبعی مقامات یعنی گھروں اور دفاتر میں نہیں گھسنا چاہیے۔ اسی طرح ہم کسی کے گھر بن بلائے نہیں جاتے اور ہم میں سے بہت سے لوگ دوسروں کو رات گئے تک فون بھی نہیں کرتے کیونکہ ہم ان کے مقام اور ذاتی زندگی کا احترام کرتے ہیں۔



اس کے علاوہ جب کوئی ساترہرا بلیڈ (Bullied) یا ہراساں ہونے کی بات کرتا ہے تو اسے اکثر مورد الزام ٹھہرایا جاتا ہے کیونکہ وہاں کسی طبعی مقام کو نقصان نہیں پہنچتا۔ سوشل میڈیا اور عام انٹرنیٹ لہجہ مرتب کرنے کے لامحالہ صارفین پر انحصار کرتے ہیں۔ یہ ہماری بد قسمتی ہے کہ جو لہجہ انٹرنیٹ پر ترتیب دیا جاتا ہے وہ خصوصاً خواتین کے لیے کوئی خوش آئند نہیں۔

اگرچہ یہاں کوئی اس لیے نہیں آتا کہ اس گالیوں یا دھکوں سے نوازا جائے لیکن پھر بھی ہمیں اکثر دلکش بے ہودہ گالیوں کا نشانہ بنایا جاتا ہے۔ کیا اپنے خیالات کے اظہار پر آپ پر کبھی کوئی حملہ کیا گیا ہے؟ ہم جانتے ہیں کہ آپ کو اُس وقت کتنا بُرا لگا ہوگا۔ بعض دفعہ تو ہمیں ان گالیوں سے مزید بچنے کے لیے ایسے لوگوں کو بلاک کرنا پڑتا ہے۔

ہماری یہ تجویز ہے کہ اپنی ڈیوائس کو اپنے مقام تک رسائی حاصل نہ کرنے دینا ایک اچھی مشق ہے۔ حالانکہ آپ کے فون یا دیگر ڈیوائسز پر آپ کو آن لائن نقشوں سے ہدایات حاصل کرنے کے لیے اپنے مقام کے بارے میں بتانے کی ضرورت ہوتی ہے، لیکن ہم یہ بھول جاتے ہیں جب ہم آف لائن ہو جاتے ہیں تب بھی ہم ان ایپلیکیشنز کو اپنے مقام تک رسائی کی اجازت دے رہے ہوتے ہیں۔ اس طرح اگر ہم اپنی لوکیشن خدمات کو بند نہیں کرتے تو ہماری ڈیوائسز کا تعاقب کر کے ہمارے طبعی مقام کا با آسانی پتہ چلایا جاسکتا ہے۔

اگر آپ اپنی سمت دیکھنا چاہتی ہیں یا آپ کسی نقشے کی مدد حاصل کرنا چاہتی ہیں تو اپنی لوکیشن خدمات کو تب ہی استعمال کریں جب آپ نقشے کا استعمال کر رہی ہوتی ہیں۔ بصورتِ دیگر اس سروس کو بند رکھنے کی یقین دہانی کر لیں۔



★ سوشل میڈیا ویب سائٹس کو اپنے مقام کا تعاقب نہ کرنے دیں اور اس بات کو یقینی بنائیں کہ ایسے تمام آپشن ڈس ایبل ہو گئے ہیں۔

★ اس بات کا اعلان کبھی نہ کریں کہ آپ سوشل میڈیا میں کہاں پر موجود ہیں، خصوصاً جب آپ کسی ایونٹ کی براہ راست آپ ڈیٹنگ نہ کر رہی ہوں۔ یہاں تک کہ گھر واپسی پر بھی جب آپ آپ ڈیٹ ڈال رہی ہوں تب بھی اس بات کا اعلان نہ کریں ورنہ آپ کو نقصان پہنچانے والے ہیکرز یا سٹاکرز آپ کی حالیہ نشست کو دیکھتے ہوئے آپ ہی کی ایک پروفائل بنا سکتے ہیں۔ یہ آپ کے لیے آف لائن خطرات کے حامل بن سکتے ہیں۔

★ اپنی ٹیگ ترتیبات کا معائنہ کر لیں تاکہ اس بات کی یقین دہانی ہو سکے کہ آپ نے غیر ضروری تصاویر یا آپ ڈیٹس ٹیگ ان نہیں کیں۔

تجزیہ

آپ جو کام آن لائن کرتی ہیں وہ آن لائن ہی رہ جاتا ہے۔ حتیٰ کہ اگر ایک ویب سائٹ مٹ بھی جاتی ہے تب بھی ایک آن لائن cache موجود رہے گا جو ابھی تک دستیاب ہونے والی ویب سائٹ اینڈریز کو اپنے پاس رکھے گا۔ لہذا سوشل میڈیا کے بارے میں یہ علم ضرور رکھیں کہ صحیح معنوں میں یہاں کچھ بھی نجی نہیں ہے اور ایک بار آن لائن آنے والی چیز کبھی نہیں جاتی۔

VPNS:

دوسرے ممالک میں سرورز سے اپنے براؤزرز کو ہدایت دلوانے اور اپنے مقام کی دستیابی کو چھپانے کے لیے آپ (Virtual Private Network) VPN کا استعمال کر سکتے ہیں۔ آپ Hot Spot Shield جیسا ایک VPN اپنے کمپیوٹر میں شامل کر سکتی ہیں لیکن ہوشیار رہیں کہ یہ آپ کے کمپیوٹر کی رفتار دھیمی کر سکتا ہے۔ اس کے علاوہ اپنے براؤزر میں zenmate جیسا ایک VPN شامل کرنے کا بھی اختیار آپ رکھتی ہیں۔

سوشل میڈیا سیکورٹی اور گمنامی

اگر آپ اپنے دفاع کے بارے میں بہت زیادہ مطمئن ہیں تو یہ جان لیں کہ سوشل میڈیا نہ صرف ایک مذاق بلکہ کافی مسائل پیدا کر سکتا ہے۔ یہ بھی ایک بہت اہم بات ہے کہ سوشل میڈیا اپنی دفاعی اور پرائیویسی ترتیبات میں وقتاً فوقتاً تبدیلیاں لے کر آتے ہیں یعنی جو چیزیں پہلے بہت زیادہ یا صرف خاص لوگوں کو دکھانے کے لیے ہوتی تھیں ان پلیٹ فارمز کی لمحہ بہ لمحہ بدلتی حکمت عملیوں کے باعث وہی معلومات عوامی بھی بن سکتی ہیں اور انہیں کوئی بھی دیکھ سکتا ہے۔ مندرجہ ذیل آن لائن دفاع کے لیے چند تجاویز دی جا رہی ہیں:

★ اگر آپ عوامی پوسٹ کا استعمال زیادہ پسند کرتے ہیں تو اس بات کو مد نظر رکھیں کہ ان پوسٹ میں آپ کس قسم کی معلومات ڈال رہے ہیں۔ عوامی پوسٹ میں اپنی ذاتی یا قابل شناخت معلومات نہ ڈالئے کیونکہ اس تک عام عوام کی رسائی بھی ہو سکتی ہے۔ ان معلومات میں آپ اور آپ کے دوستوں کی تصاویر کی طرح عوامی تصاویر بھی شامل ہوتی ہیں۔

★ اپنی دفاعی اور پرائیویسی ترتیبات کو روزانہ کی بنیاد پر دیکھتے رہیے تاکہ وہ اپ ڈیٹ رہیں اور اس بات کی یقین دہانی بھی ہو جائے کہ ویب سائٹس کی تبدیلیوں کا آپ پر کوئی فرق نہیں پڑا۔

★ گمنامی رکھ کر آپ صارفین سے اپنے ای میل ایڈریس یا فون نمبر یہاں تک کہ اپنی دفاعی ترتیبات کے ذریعے انہیں پیغامات بھیجنے سے روک سکتی ہیں اور اس طرح اپنا دفاع کر سکتی ہیں۔

★ فیس بک آپ کو یہ دیکھنے کی اجازت دیتا ہے کہ آپ کہاں سے لاگ ان ہوئی ہیں اور کس براؤزر پر آپ لاگ ان ہوئے ہیں۔ اس بات کو مستقل بنیادوں پر ذہن میں رکھیے کہ آپ نے کبھی حادثاتی طور پر بھی کسی سیشن کو کسی بھی جگہ پر لاگ ان نہیں چھوڑا ہوگا یا آپ کے اکاؤنٹ کو کبھی کوئی نقصان نہ ہوا ہوگا۔

★ اس بات کی یقین دہانی کر لیں کہ سوشل میڈیا ویب سائٹس آپ کا آن لائن تعاقب یا ذاتی اشتہار نہیں بنا سکتیں۔ اپنی

★ فیس بک preferences چیک کریں آپ یہ دیکھ کر ڈر جائیں گی کہ آپ کی "ad preferences"

شناخت کرنے کے لیے ایک بڑی تعداد میں keywords کا استعمال کیا جاتا ہے۔

BROWSER ADD-ONS

براؤزر سکیورٹی میں اگلا قدم add-ons یا extensions ہوتا ہے۔ آپ شاید ویڈیوز یا میوزک ڈاؤن لوڈ کرنے کے لیے براؤزر add-ons پہلے سے ہی استعمال کرتی ہوں۔ اسی طرح کوکیز، ٹریکرز اور پاپ اپ اشتہارات بلاک کر کے اپنی رائیو لسی اور دفاع کو بچانے کے لیے براؤزر add-ons ہوتے ہیں۔ یہاں چند add-ons دیئے جا رہے ہیں جو آپ کے براؤزر کو ضرور رکھنے چاہئیں۔

HTTPS EVERYWHERE:

یہ یقین دہانی کراتا ہے کہ آپ HTTPS کے ذریعے ایک ویب سائٹ سے محفوظ طریقے سے منسلک ہو گئی ہیں، ایسا کرنے سے جہاں تک ممکن ہو سکتا ہے آپ کی معلومات HTTP جیسی غیر محفوظ کی نسبت زیادہ نجی اور محفوظ رکھی جائے گی۔

PRIVACY BADGER:

یہ add-ons یقین دہانی کراتی ہے کہ دوسری ویب سائٹس آپ کا تعاقب نہیں کریں گی۔

جب آپ فیس بک کے Share بٹن پر کلک کرتی ہیں، یا سیدھے ہی کسی ویب سائٹ سے کوئی ٹویت کرتی ہیں تو آپ کا رد عمل ریکارڈ کر لیا جاتا ہے اور آپ کی آن لائن حرکات دیکھنے میں استعمال ہوتا ہے کہ آپ کا ایک ڈیجیٹل شیڈو بن جائے۔ یہ کتنی ناگوار بات ہے! PB اور GHOSTERY جیسی add-ons اس بات کو یقینی بنائیں گی کہ کوئی ویب سائٹ آپ کا تعاقب نہیں کر پائے گی۔

کیا آپ جانتی ہیں!

NO SCRIPT:

سکرپٹ ایک ایسا چھوٹا پروگرام ہے جنہیں چند ویب سائٹس آپ کے براؤزر پر چلا دیں گی۔ بعض دفعہ یہ سکرپٹس دفاعی کمزوریاں رکھ سکتی ہیں اور یہی وجہ ہے کہ آپ کو نو سکرپٹ کی ضرورت پڑتی ہے، تاکہ نو سکرپٹ بغیر کسی اجازت کے آپ کے براؤزر میں چل سکے۔

3

اپنی ہسٹری کبھی محفوظ نہ رہنے دیں کیونکہ آپ کی ڈیجیٹل سکیورٹی کو نقصان پہنچانا بگ مارک کے ایک پیچ کے لیے نہایت آسان ہوتا ہے۔

4

ہمیشہ اپنی عارضی انٹرنیٹ فائلیں اور کوکیز کو ختم کر دیں۔

5

اگر آپ چاہتی ہیں کہ ویب سائٹس کے ذریعے آپ کا تعاقب نہ ہو تو براؤزر ترتیبات میں جا کر "do not track" آپشن کو enable کر دیں۔

6

اس بات کی یقین دہانی کر لیں کہ آپ نے ممکنہ حملہ آور، ویب سائٹس اور ویب جعل سازی کو بلاک کرنے کے لیے تمام آپشنز کو آن کر دیا ہے۔

7

کسی ایسی ویب سائٹ پر اپنا پاس ورڈ کبھی داخل نہ کریں جس کی آفیشل ای میل یا آفیشل سوشل میڈیا ویب سائٹ نہ ہو۔ کیونکہ یہ راستہ آپ کی کسی بھی حساس معلومات خصوصاً کریڈٹ کارڈ معلومات تک جاتا ہے۔

براؤزر سکیورٹی

خواہ آپ اپنے کمپیوٹر پر وائرس اور مالویئر سے مقابلہ کرنے کے لیے ایک بہترین اینٹی وائرس چلائیں اور روزمرہ کی بنیاد پر اپنے کمپیوٹر کو سکین بھی کر لیں لیکن آپ کا براؤزر پھر بھی خطرات سے دوچار ہو سکتا ہے۔ اس لیے براؤزر کو محفوظ بنانے کے لیے اضافی اقدامات درکار ہیں۔

براؤزر سکیورٹی کا آغاز نہایت بنیادی اقدامات سے ہوتا ہے:

1

اپنے اکاؤنٹ کو کبھی لاگ ان نہ چھوڑ کر نہ جائیں چاہے آپ ایک ہی ڈیوائس کیوں نہ استعمال کر رہی ہوں۔ آپ اس سے کسی بھی طرح ہاتھ دھو سکتی ہیں۔ حتیٰ کہ اگر آپ نے پاس ورڈ بھی لگایا ہو پھر بھی ہر بار کمپیوٹر بند کرنے سے پہلے ہر ایک سیشن سے لاگ آؤٹ ہو جائیں یا پھر اسے سلیپ موڈ میں ڈال دیں۔

2

پرائیویٹ براؤزنگ موڈ میں جانے کے لیے (فائر فاکس میں) ایک پرائیویٹ ونڈو استعمال کریں یا (گوگل کروم میں) incognito موڈ میں جائیں۔ اس طرح آپ کا براؤزر موڈ آپ کے آنے کا کوئی ریکارڈ محفوظ نہیں رکھ پائے گا اور نہ ہی آپ کی ڈاؤن لوڈ ہسٹری محفوظ رکھ پائے گا، تاہم ابھی بھی آپ کا انٹرنیٹ خدمت مہیا کار، آپ کے کام کی جگہ یا سکول کا منتظم یا جس ویب سائٹ میں آپ گئے تھے، آپ کا تعاقب کر سکیں گے۔

2

We've sent a login verification request to your phone.

When you receive the request, accept it by clicking the checkmark button on your phone. You can also enter a [backup code](#).

Need help? Please contact [Twitter Support](#).

3

Verify your phone

We sent a text message to (201) 555-5559 with a code



Enter verification code

598236

Verification codes are 6 digits long.

« Back

Verify

Didn't get the code?

دوسری بات جو رخسانہ کو پتہ چلی وہ یہ کہ کسی نے اس کے فیس بک اکاؤنٹ کو ہیک کرنے کی کوشش کر دی ہے۔ اسے ایک آن لائن نوٹیفیکیشن بھی ملا کہ کوئی اس کے جی میل پاس ورڈ کو تبدیل کرنے کی کوشش کر رہا ہے۔ رخسانہ جانتی تھی کہ اگر اس نے جلد از جلد کچھ نہ کیا تو نہ صرف وہ اپنے اکاؤنٹ تک رسائی کھودے گی بلکہ اپنے آن لائن کاروبار کے لیے بنائے گئے پیجز سے بھی ہاتھ دھو بیٹھے گی۔

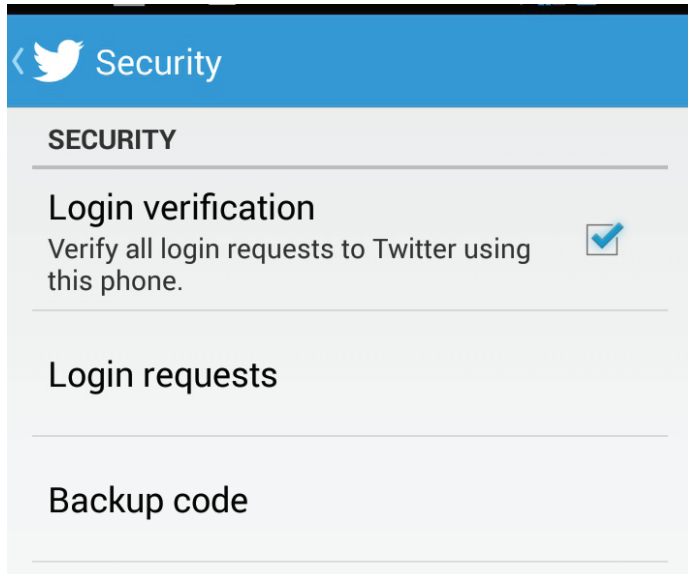
رخسانہ کی سہیلی ماریہ نے اسے چند حفاظتی اقدامات کے بارے میں بتایا:

اس نے اسے بتایا کہ فوراً سے پیشتر اپنے تمام اکاؤنٹس کے لیے two factor authentication کو ایکٹیویٹ کرے۔ پھر اس نے اسے بتایا کہ جب کوئی کسی انجانے براؤزر یا کمپیوٹر سے اس کے فیس بک اکاؤنٹ تک رسائی حاصل کر لے تو اس لیے نوٹیفیکیشنز کو کیسے مرتب کرنا ہے۔

ماریہ نے رخسانہ کو یہ بھی سمجھایا کہ اسے اپنی ایپس کے لیے کوڈز کیسے بنانے چاہیے تاکہ اسے اپنی دیگر مشینوں سے لاگ ان ہونے کے لیے ایک ہی پاس ورڈ کا استعمال نہ کرنا پڑے۔

2-FACTOR AUTHENTICATION FOR TWITTER

1



Hotmail بھی ایک تصدیقی ایپ رکھتا ہے جسے مائیکروسافٹ اکاؤنٹ کہا جاتا ہے، جو ہر بار ای میل تک رسائی کے وقت لاگ ان درخواست کی مانگ کرتا ہے۔ ٹویٹر بھی ایسے ہی کام کرتا ہے اور آپ اپنی ترتیبات میں جائیں تو آپ ایپ میں اپنا فون نمبر ڈال سکتی ہیں اور پھر سیکیورٹی سینگلز سے اکاؤنٹ کی تصدیق کو قابل استعمال بنا سکتی ہیں۔ ہر بار جب آپ ایک براؤزر سے ٹویٹر کو لاگ ان کرتی ہیں تو آپ کو اپنی ٹویٹر ایپ سے آئی درخواست کو ماننا پڑتا ہے۔

یاد رکھیں: **Two-Factor Authentication** کا مطلب یہ ہے کہ اب آپ کا موبائل بہت اہمیت کا حامل ہو گیا ہے۔ ہمیشہ اپنا فون لاگ رکھیں، تاکہ کبھی اگر یہ گم یا چوری ہو جائے تو آپ کے ڈیٹا کو کوئی نقصان نہ پہنچے۔


ہنگامی حالات میں، جی میل اور ٹویٹر آپ کو اس بات کی اجازت دیتے ہیں کہ آپ بیک اپ کو ڈاؤن لوڈ کریں جب آپ کو لاگ ان ہونے کی ضرورت ہو۔ (یہ ان ہنگامی حالات میں استعمال ہو سکتا ہے جب مثال کے طور پر آپ کا موبائل پانی میں گر جائے اور کوئی تدبیر کارگر نہ رہے)۔ ان کوڈز کو اپنے موبائل میں کبھی محفوظ نہ کریں۔ ان کا پرنٹ نکال لیں یا کسی محفوظ جگہ پر لکھ لیں۔ ان کو کسی خفیہ اور محفوظ مقام پر منتقل کریں۔

مثلاً: اپنا آن لائن کاروبار کرنے کے بعد رخسانہ کو غلط قسم کے پیغامات ملنے شروع ہوئے۔ بزنس کی تعلیم حاصل کرتے ہوئے اس نے سوچا تھا کہ وہ گھر سے آن لائن دوکان چلا کر بہت سے روپے کماسکتی ہے۔ لیکن وہ اس بات سے ناواقف تھی کہ آن لائن کاروباری لین دین کرنا کتنے مسائل پیدا کر سکتا ہے۔

گمنامی کا لبادہ اوڑھ کر کچھ لوگ یہ سمجھتے ہیں کہ وہ آن لائن جو چاہے کر سکتے ہیں۔ ایک دن رخسانہ کو غلط قسم کے اور گالیوں سے بھرے پیغامات موصول ہونے لگے اور جب رخسانہ کے لیے ان پیغامات کی بہتات نے پریشانی کھڑی کر دی تو اس نے اس شخص کی پروفائل کو مکمل طور پر بلاک کر دیا۔

2

2-Step Verification

 A text message with your code has been sent to: (***).***95

[Verify](#)

☐ Don't ask for codes again on this computer

3

2-step verification

Help keep the bad guys out of your account by using both your password *and* your phone.



[Get Started](#)

4

Set-up 2 factor verification for

Set up your phone Add a back up Confirm

Tell us what kind of phone you use, and then you'll set up a way to get your verification codes

Now open and configure google authenticator

The easiest way to configure google authenticator is to scan the QR code

1 In google authenticator, select Scan a barcode

2 use your phone's camera to scan this QR code



When the application is configured, click Next to test it.

اپنے آن لائن اکاؤنٹس کو اپنے موبائل فون سے منسلک کرنا کتنا بہترین ہوتا ہے، لیکن یہ مت بھولیں کہ یہ پاکستان ہے۔ اس وقت آپ کیا کریں گی جب عید یا کسی اور تہوار کے موقع پر جب موبائل فون سگنل بلاک کر دیئے جاتے ہیں؟ یا آپ بیرون ملک سفر پر جا رہی ہوں اور آپ دو طرفہ تصدیقی عمل کو بند کرنا بھول جائیں؟ بہت سے لوگ تو اس وقت بالکل ہی کچھ نہیں کر سکتے جب ان کے نمبر ایسے مواقعوں پر کام نہیں کر رہے ہوتے۔ ایسے ہی مواقعوں کے لیے authenticator apps بنی ہوئی ہیں۔ آپ جب بھی انہیں کھولیں گی تو یہ ایپس آپ کو ایک کوڈ دیں گی۔ جی میل Google Authenticator app استعمال کرتا ہے، جسے آپ

QR کوڈ ریڈر ایپ کے ساتھ مفت ڈاؤن لوڈ کر سکتی ہیں، یہ ایپ Google Authenticator پر ہر بار آپ کو ایک نیا اکاؤنٹ مرتب کرنے کے لیے ایک کوڈ سکین کرنے میں استعمال ہوگی۔ (دونوں ایپس موبائل فون کی میموری میں کافی کم جگہ گھیرتی ہیں) فیس بک اپنے اندر پہلے سے موجود کوڈ بنانے والی ایپ رکھتا ہے، لیکن یہ بھی ایک متجاوز ایپ ہے جو آپ کے موبائل کا کیمرہ اور مائیک استعمال کر کے آپ کے رابطوں، کال کی تفصیلات، پیغامات اور گیریلری وغیرہ تک بغیر اجازت رسائی حاصل کر لیتی ہے۔ لہذا وہ صارف جو فیس بک کی اس ایپ سے گریز کرنا چاہتی ہیں وہ بھی فیس بک پر کوڈ بنانے کے لیے Google Authenticator کو ترتیب دے سکتی ہیں۔

TWO STEP AUTHENTICATION FOR GOOGLE

1



Signing in will be different

You'll need verification codes:
After entering your password, you'll enter a code that you'll get via text, voice call, or our mobile app.



Keep it simple

Once per computer, or every time:
During sign in, you can tell us not to ask for a code again on that particular computer.



Help keep others out

You'll still be covered:
We'll ask for codes when you (or anyone else) tries to sign in to your account from other computers.

2-step verification

Keep the bad guys out of your account by using both your password and your phone.

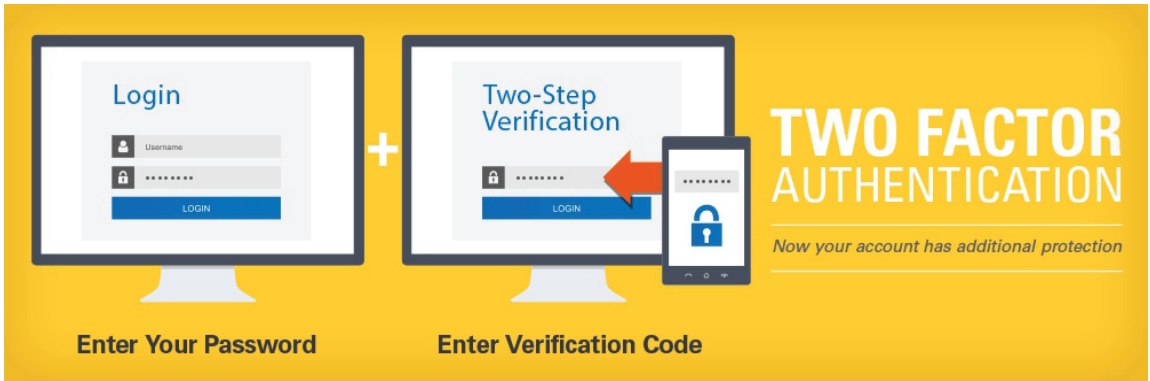
[Start setup »](#)

[Learn more](#)

آن لائن اکاؤنٹس محفوظ کرنا

Two-Factor Authentication

آپ نے لوگوں کو دو طرفہ تصدیق کے بارے میں بات کرتے سنا ہوگا، یہ آپ کو شاید اس کے بارے میں پڑھنا کافی مشکل لگے گا لیکن درحقیقت اس کا طریقہ نہایت آسان ہے۔ جب آپ دوہری سیکورٹی کے لیے اپنا موبائل فون اپنے آن لائن اکاؤنٹ کے ساتھ منسلک کرتی ہیں تب وہ Two-Factor Authentication ہو جاتی ہے۔ جب آپ لاگ ان ہوتی ہیں تو آپ کے موبائل فون پر خود کار کال یا پیغام یا کسی ایپ کے ذریعے ایک کوڈ بھیجا جاتا ہے جسے آپ کو اپنے اکاؤنٹ کو لاگ ان کرنے کے لیے ڈالنا پڑتا ہے۔ اگر آپ اپنے ای میل یا سوشل میڈیا اکاؤنٹ پر سیکورٹی ترتیبات میں جاتی ہیں تو آپ کو Two-Factor Authentication کو مرتب کرنے کا موقع فراہم کیا جاتا ہے۔ گوگل، فیس بک، یاہو، ٹویٹر ہاٹ میل وغیرہ آپ سے آپ کا فون نمبر پوچھتے ہیں اور پھر اسی نمبر پر آپ کو ایک کوڈ بھیجتے ہیں، یہ دیکھنے کے لیے کہ وہ صحیح بھی ہے کہ نہیں۔ ایک بار آپ اپنا موبائل نمبر دے دیتی ہیں تو سب ٹھیک ہو جاتا ہے، اگلی بار جب آپ لاگ ان ہوتی ہیں تو پاس ورڈ ڈالنے کے بعد آپ سے ایک کوڈ پوچھا جاتا ہے۔



★ ذاتی، آسان اندازہ لگائے جانے والی معلومات جیسے سالگرہ، مختلف مواقعوں یا پالتو جانوروں کے ناموں پر مبنی نہ ہو

★ ذاتی ترجیحات، پسندنا پسند، مشاغل وغیرہ پر مبنی نہ ہو

★ یاد رکھنے میں آسان ہو اور کسی کاغذ پر یا اپنی ڈیوائس کے کسی مسودہ میں اس کو کبھی تحریر نہ کریں

mnemonatic device (یادداشت کا فن) بنانا پاس فریز کو محفوظ بنانے کا ایک طریقہ ہے، یہ معلومات کو یاد رکھنے کی ایک تکنیک ہے۔ مثلاً، آپ کوئی مکمل جملہ لیتی ہیں اور پھر اس کے ہر لفظ کا پہلا، دوسرا یا آخری حرف یا نمبر کو ترتیب دے کر ایک لفظ بنا لیتی ہیں۔

مثال کے طور پر: Best friends don't ask for your password, they value your privacy and understand the importance of digital security!

اس جملے کا پاس فریز کچھ یوں بنے گا، b5D'@4up,tVURP&uti0DS

ہمیشہ یاد رکھیں

ایک سے زیادہ اکاؤنٹس کے لیے ایک جیسا ہی پاس ورڈ نہ رکھیں کیونکہ ایک اکاؤنٹ ہیک ہو جاتا ہے تو دیگر اکاؤنٹس کو ہیک کرنا بھی آسان ہو جاتا ہے۔

اگر زیادہ پاس ورڈ یاد رکھنا مشکل ہوں تو Keeppass جیسے مفید ٹول کا استعمال کریں یہ ایک مفت پروگرام ہے جو مضبوط پاس ورڈز کو آپ کے لیے بناتا بھی ہے اور انہیں محفوظ بھی کر لیتا ہے۔ آپ کو صرف اپنا ماسٹر پاس ورڈ یاد رکھنا ہوتا ہے، یہ پاس فریز مضبوط اور ناقابلِ تسخیر ہونا چاہیے۔

اگر آپ Keeppass (یا Mac کے لیے Keeppass) استعمال کرتی ہیں تو اس بات کی یقین دہانی کر لیں کہ آپ نے اپنا کی پاس ڈیٹا بیس USB یا ایکسٹرنل سٹوریج میں محفوظ کر لیا ہے۔ اگر آپ اسے اپنے کمپیوٹر میں محفوظ کرتی ہیں تو ہیکرز آپ کی سیکورٹی کی خلاف ورزی کرتے ہوئے اس تک رسائی حاصل کر سکتا ہے۔ یاد رکھیں Keeppass پاس فریز کبھی کسی جگہ نہ لکھا جائے اور نہ ہی کسی کے ساتھ اس کی بابت کوئی بات کریں۔

پاس ورڈز محفوظ کریں

ہم میں سے بہت سے لوگ یہ سمجھتے ہیں کہ ان کے لگائے پاس ورڈز بہت مضبوط ہوتے ہیں۔ لمبے پاس ورڈز لگانا ہی کافی نہیں ہوتا، Hack کرنے والے سافٹ ویئر پاس ورڈز میں سے ممکنہ الفاظ کے ذریعے ڈکشنری سے مدد لے کر الفاظ کو سکین کرتے ہیں اور پھر پاس ورڈز کو کریک کر کے اکاؤنٹس کو Hack کر لیتے ہیں۔ ایک مضبوط پاس ورڈ بنانا کوئی مشکل کام نہیں ہے خصوصاً جب آپ پاس ورڈز کی بجائے پاس فریز کا استعمال کرتی ہیں۔

ایک اصول بنالیں:

میرا پاس ورڈ ہمیشہ بہت مضبوط رہے گا اور میں کبھی بھی اس کو کسی کے ساتھ share نہیں گی۔

اپنا پاس ورڈ دوسروں کے ساتھ شیئر کرنا خطرناک حد تک عام ہو چکا ہے۔ حالانکہ بہت سے لوگ یہ سمجھتے ہیں کہ اپنے قریبی دوستوں یا گھر والوں سے پاس ورڈز شیئر کرنے سے کوئی نقصان نہیں پہنچتا لیکن یاد رہے کہ کبھی اگر ان کی معلومات کو کبھی کوئی نقصان پہنچتا ہے تو آپ کی جو معلومات ان کے پاس ہوتی ہے اس کو بھی نقصان پہنچ سکتا ہے۔ دوسری بات یہ کہ ایسی عادت کو ترک کر دینا چاہیے جس سے آپ کو نقصان پہنچتا ہو۔ آپ کو اپنی پرائیویسی کا ہر صورت خیال رکھنا چاہیے اگرچہ ہمارے معاشرے میں خواتین کی پرائیویسی کو اہمیت نہیں دی جاتی۔ معاشرے میں تبدیلی تب ہی ممکن ہے جب ہم خود سے اس میں تبدیلی نہیں لائیں گی اور اپنی شخصیت میں بھی مثبت تبدیلیاں لانا ہمارے لیے بہت ضروری ہے۔

Passphrases چھ، سات الفاظ کے کرداروں پر مبنی پاس ورڈز سے نسبتاً زیادہ طویل ہوتے ہیں اور اگر انہیں صحیح ترتیب دیا جائے تو انہیں کریک کرنا قریب ناممکن ہو جاتا ہے۔ ایک مضبوط پاس فریز کچھ اس طرح سے ہوگا:

★ اسے 8 سے 30 کرداروں پر مبنی ہونا چاہیے

★ ایک سے زیادہ الفاظ پر مشتمل ہو

★ چھوٹے بڑے الفاظ، نمبر اور اشاروں پر مشتمل ہو

★ ایسے الفاظ پر مشتمل ہو جو ڈکشنری سے ہٹ کر ہوں یا مشہور اقوال بھی نہ ہوں

مثال:

عتیبہ نے یہ سیکھ لیا کہ کسی USB یا بیرونی ہارڈ ڈرائیو میں اپنا ڈیٹا بیک اپ کیسے کرنا ہے لیکن وہ یہ نہ جان سکی کہ اسے اپنی فائلیں بچانے کے لیے کیا کرنا چاہیے۔

اپنی انٹرن شپ پر وہ اپنی ہارڈ ڈرائیو اور USB اپنے نئے دفتر اپنے ساتھ لے گئی۔ یہ وہی ڈرائیو تھیں جو کالج میں وہ اپنے کام کے لیے استعمال کرتی رہی۔ ان میں اس کے شناختی کارڈ کی نقل، اس کے مختلف تعلیمی دوروں کی تصاویر، اس کی بہت سی اسائنمنٹس اور بہت سی دیگر ذاتی معلومات پر مبنی چیزیں موجود تھیں۔

سب سے پہلا مسئلہ جو عتیبہ کو پیش آیا وہ یہ کہ دفتر کے کمپیوٹر میں لگاتے ساتھ ہی اس کی USB میں موجود تمام ڈیٹا وائرس سے بُری طرح متاثر ہو گیا اور بالآخر وہ اپنے سارے ڈیٹا سے ہاتھ دھو بیٹھی۔

اس کا دوسرا مسئلہ بہت ہی واضح تھا جب اسے پتہ چلا کہ اس کے سپروائزر نے اس کے علم میں لائے بغیر اس کے شناختی کارڈ کی نقل اس کی ہارڈ ڈرائیو سے حاصل کر لی تھی۔ اگرچہ اس سپروائزر کا مقصد اسے نقصان پہنچانا نہیں تھا بلکہ محض ریکارڈ کے لیے وہ نقل حاصل کی گئی تھی۔ عتیبہ جان گئی تھی کہ کسی اور نے یہ حرکت کر کے اس کی ساری معلومات کو بڑی آسانی سے چُرا لیا ہے۔

تب سے عتیبہ جان گئی تھی کہ کسی اور نے یہ حرکت کر کے اس کی ساری معلومات کو بڑی آسانی سے چُرا لیا ہے۔ تب سے عتیبہ نے اپنی ہارڈ ڈرائیو اور USB کی حفاظت کو یقینی بنانے پر کام شروع کر دیا۔ پاکستانی خواتین کے لیے ان کا ڈیٹا اپنے مرد ہم منصبوں کی نسبت زیادہ حساس ہوتا ہے۔ مثال کے طور پر عتیبہ کے دفتری ساتھی علی کو اپنی USB کسی کو دینے اور اپنی تصاویر کو کھودینے کا اس پر کوئی خاطر خواہ اثر نہیں ہوگا۔ لیکن عتیبہ کے لیے یہ امکان موجود تھا کہ اس کی تصاویر کو چُرا کر ان کا غلط استعمال کیا جاسکتا تھا۔

تجويز

خبردار!

اپنی ہارڈ ڈرائیو کو اپنے گھر کے بیڈروم کی الماری کے کسی دراز میں محفوظ کر لیں تاکہ جب آپ کو اسے ڈھونڈنا پڑے تو زیادہ وقت نہ ہو۔

اپنی ہارڈ ڈرائیو کو اپنے گھر کے بیڈروم کی الماری کے کسی دراز میں محفوظ کر لیں تاکہ جب آپ کو اسے ڈھونڈنا پڑے تو زیادہ وقت نہ ہو۔

خبردار! ہمیشہ USB کے لین دین میں احتیاط برتیں۔ بعض دفعہ لوگ کسی کے بھی کمپیوٹر کو ہدف بنا کر نقصان پہنچانے کے لیے اس سے USB لے کر اس میں جان بوجھ کر مالمویر ڈال دیتے ہیں۔ کبھی کبھار شوہر حضرات اور منگیتر صاحبان اپنی بیویوں پر جاسوسی کی غرض سے ایسا کرتے ہیں اور کبھی کبھی سابقہ شوہروں کی جانب سے اپنی سابقہ بیویوں کو بلیک میل کرنے کے لیے ایسا کیا جاتا ہے۔ ایسے بہت سے واقعات دیکھنے میں آئے ہیں جب خواتین کے کمپیوٹروں کو متاثر کر کے ان سے ڈیٹا چرا کر ان خواتین کو بلیک میل کیا گیا ہے۔ لہذا بہت محتاط رہیں! ہم آپ کو شیئرڈ کمپیوٹروں پر بھی USBs کے استعمال سے آپ کو خبردار کرتے ہیں۔ ہم اس بات سے آگاہ بھی ہیں کہ یہ ایک عمومی فعل ہے اور بعض

دفعہ ایسا کرنے کے علاوہ اور کوئی چارہ نہیں ہوتا۔ یہاں آپ کو چند تجاویز دی جاتی ہیں:

☆ مطلوبہ فائل کے علاوہ اس USB میں اور اس کمپیوٹر سے کچھ نہ ڈالیں۔

☆ ہر بار استعمال سے پہلے USB کے لیے اینٹی وائرس یا اینٹی مالمویر ضرور چلائیں۔

اپنے ڈیٹا کا بیک اپ رکھنا

کیا کبھی آپ نے مضمون کو پیش کرنے سے ایک دن قبل کھویا ہے؟ کیا کبھی آپ کا کمپیوٹر آپ کے سارے ڈیٹا سمیت خراب ہو گیا ہو؟ بعض دفعہ اپنا ڈیٹا گنوا دینا بہت تکلیف دہ ہوتا ہے اور کبھی کبھار اسے ڈیٹا کو واپس حاصل بھی کیا جاسکتا ہے۔ اسی لیے آپ کو ہمیشہ اپنے ڈیٹا کی نقول اپنے پاس محفوظ رکھنی چاہیے۔



ایک تو یہ کہ تمام ڈیٹا ایک USB میں محفوظ کر لیں بعض صارف طبعی آلہ کھودینے کے ڈر سے اس کی نسبت cloud storage کو زیادہ اہمیت دیتے ہیں، اس لیے USB جیسے آلات کو کسی محفوظ جگہ رکھنا بھی ضروری ہوتا ہے تاکہ اگر کبھی آپ کا لیپ ٹاپ وغیرہ چوری بھی ہو جائے تو آپ کا بیک اپ محفوظ رہے۔

دوسرا طریقہ یہ ہے کہ آن لائن جا کر cloud storage میں محفوظ کر لیں۔

cloud storage اس لیے بھی سہل ہے کیونکہ اسے کسی طبعی آلے کی ضرورت نہیں پڑتی۔ اس کے ذریعے آپ کا تمام ڈیٹا آن لائن محفوظ کر لیا جاتا ہے اور Google یا Dropbox جیسی کمپنیاں آپ کے ڈیٹا کو قائم رکھتی ہیں۔

Kaspersky ❖

AVG ❖

Avast ❖

Norton Antivirus ❖

Avira ❖

Sophos ❖

مالوئیر سکین:

مالوئیر ”مالیشنس سافٹ ویئر“ کا مختصر نام ہے۔ کمپیوٹر نظام کو نقصان دینے والے مختلف قسم کے مالیشنس کوڈ یا پروگراموں کے لیے ایک متفقہ اصطلاح ہے۔ تمام وائرس مالوئیر ہوتے ہیں لیکن تمام مالوئیر صرف وائرس نہیں ہوتے بلکہ اس میں سپائی ویئر، ریشم ویئر وغیرہ شامل ہوتے ہیں۔

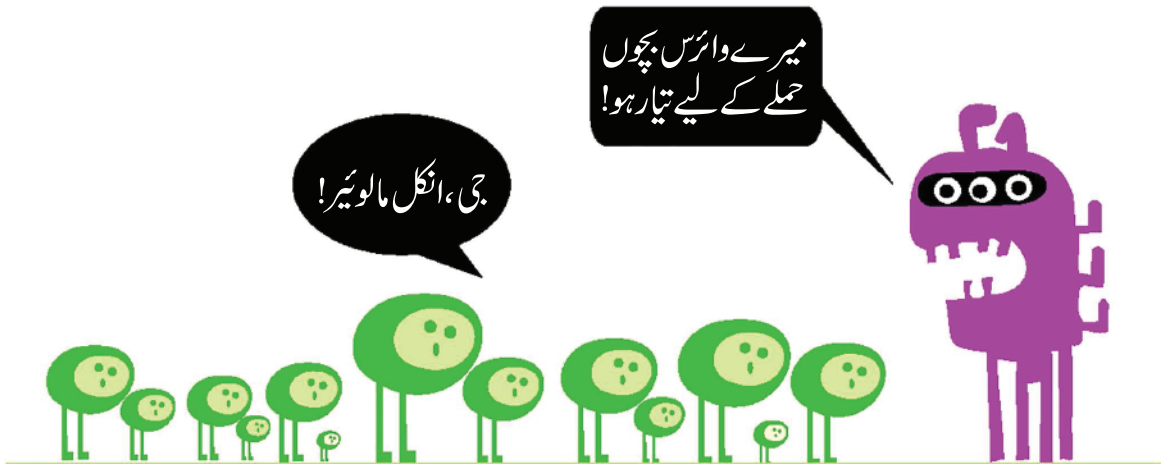
کمپیوٹروں کو اینٹی مالوئیر سافٹ ویئر کی بھی ضرورت ہوتی ہے، کیونکہ زیادہ تر اینٹی وائرس روایتی خطرات جیسے Trojan وائرس، worms وغیرہ سے نبرد آزما ہوتے ہیں۔ اینٹی مالوئیر سافٹ ویئر نے خطرات پر نظر رکھتے ہیں جن میں پوری دنیا سے پیشہ اور مجرم اور ہیکرز کی جانب سے بنائے گئے بہت سی اقسام کے مالوئیر شامل ہیں۔ یہ مالوئیر آپ کے کمپیوٹر کو نقصان پہنچا کر اور keyloggers keystrokes ریکارڈ کر کے آپ کا تعاقب کر سکتے ہیں یا آپ کے بینک کی معلومات چُر سکتے ہیں۔ اس لیے اینٹی وائرس کے ساتھ ساتھ آپ کی مشین کی بہتر حفاظت کے لیے اینٹی مالوئیر کا استعمال کریں (اگر Malwarebytes یا Lavasoft کے ساتھ اینٹی سپائے ویئر استعمال کیا جائے تو آپ کی مشین کی دوہری سیکیورٹی ہو جاتی ہے)۔

سارہ اپنے رازداری پرائیویسی کے حق کے بارے میں اپنے بھائی سے بات کرنا شروع کرتی ہے۔ وہ اپنے گھر میں خلوت اور اعتماد سے متعلق گفتگو کا آغاز کرتی ہے۔ وہ یہ جانتی ہے کہ اپنا حق حاصل کرنے کے لیے اسے کچھ وقت لگے گا اور جب کبھی وہ اپنے بھائی کو قائل نہ کر سکتی تو اسے پریشانی کا سامنا بھی کرنا پڑتا۔ پھر بھی وہ خود کو یہ باور کروا سکتی ہے کہ اسے اپنے حق کے لیے لڑنا ہے اور بالآخر اس کا بھائی اس پر قدغن لگانے کی بجائے اس پر اعتماد کرنے لگتا ہے۔

مستقل بنیادوں پر ایک اینٹی وائرس چلائیں:

وائرس آپ کے کمپیوٹر کو متاثر کرنے والا ایک نقصان دہ کوڈ یا پروگرام ہوتا ہے اس سے آپ کے کمپیوٹر پر ہونے والے اور ہوئے تمام کام مٹائے جاسکتے ہیں، آپ کا ڈیٹا تبدیل کیا جاسکتا ہے یا اس کا تعاقب کیا جاسکتا ہے۔ آن لائن ڈاؤن لوڈز جیسے کسی ویب سائٹ پر کوئی مفت ویڈیو یا میوزک وغیرہ کو کھولنے سے، اسی طرح ای میلز خاص طور پر سپام ای میلز کے ذریعے آپ کے کمپیوٹر پر ایک وائرس خود سے آسکتا ہے۔ اس لیے آپ ایسے کسی بھی لنک پر کلک نہ کریں جو کسی بیگانی جگہ سے آتے ہوں۔ یاد رکھیں، ایسی کسی بھی ای میل کو آگے بھیجنے سے پہلے ایک بار ضرور سوچ لیں جن میں تصاویر، ویڈیوز، آڈیو یا تہنیتی کارڈز موجود ہوں کیونکہ یہ چیزیں بعض دفعہ وائرس کے روپ میں موجود ہوتی ہیں۔

اپنے ویب براؤزر کے بچاؤ کے لیے ہمیشہ ایک اینٹی وائرس چلا کر رکھیں اور وقتاً فوقتاً اسے جدید ورژن میں اپ ڈیٹ کرتی رہیں۔ روزمرہ کے ایسے بچاؤ کے علاوہ اس بات کو ملحوظ رکھیں کہ اپنے سسٹم کو مسلسل سکین کرتی رہیں تاکہ اس بات کی یقین دہانی ہو کہ آپ کی مشین ہر قسم کے وائرس سے محفوظ ہوگئی ہے۔ ہمیشہ اچھے اینٹی وائرس سافٹ ویئر استعمال کریں جیسے:



اپنی مشینوں کو محفوظ کریں

اب ہم اپنی مشینوں کی حفاظت کے بارے میں بات کرتے ہیں۔ ایک چھوٹی سی غلطی آپ کی مشین کو غیر محفوظ چھوڑ سکتی ہے اور وہ ہے پاس ورڈ یا کوڈ کا استعمال نہ کرنا۔ آپ کی ڈیوائس تب زیادہ غیر محفوظ ہو جاتی ہے جب آپ اسے غیر مقفل چھوڑ جاتی ہیں۔

ایک اصول بنالیں

اپنے ہر ذاتی کمپیوٹر، لیپ ٹاپ یا موبائل وغیرہ پر ہمیشہ کوئی پاس ورڈ یا کوڈ لگا کر رکھیں۔ کیونکہ اس میں آپ کا ڈیٹا پڑا ہے اور اگر کبھی وہ مشین چوری ہو جائے تو صرف مشین ہی نہیں جاتی بلکہ آپ کا قیمتی ڈیٹا بھی چلا جاتا ہے۔

سارہ کا بھائی روزانہ اس کا فون چیک کرتا تھا۔ اگر کبھی وہ اپنا فون اسے دینے سے انکار کرتی تو وہ اس کے ساتھ لڑ پڑتا تھا۔ وہ اس کے پیغامات اور تصاویر تک دیکھ لیتا تھا۔ یہ سب کچھ جھیلنے والی سارہ کوئی اکیلی لڑکی نہیں ہے۔ پاکستانی خواتین کو عموماً اپنے گھر والوں کے ساتھ اپنے پاس ورڈ شیئر کرنے پڑتے ہیں۔ اگر وہ ایسا نہ کریں تو ان سے زبردستی وہ معلومات لی جاتی ہیں۔

اگرچہ سارہ اس بات سے واقف ہے کہ وہ پرائیویسی رازداری کا حق رکھتی ہے لیکن وہ اس بات سے بھی ڈرتی ہے کہ اگر وہ زیادہ مزاحمت کرے گی تو اس کے ساتھ کیا ہوگا۔ وہ جانتی ہے کہ اس کا بھائی اسے سماجی کڑی نگرانی کا ہدف بنا رہا ہے اور وہ یہ بھی جانتی ہے کہ یہ سمسنے والی وہ اکیلی نہیں ہے۔ اس کی ایسی بھی سہیلیاں ہیں جنہیں اپنے ڈیجیٹل آلات کھلے رکھنے اور اپنے گھر کے افراد کے ساتھ اپنے کوڈز وغیرہ شیئر کرنے پڑتے ہیں۔ ان میں سے کئی تو اپنے خلوت کے حق کی مانگ کے لیے سرگرداں رہتی ہیں اور اس حق کی مانگ کی صورت میں آنے والے ردِ عمل کا سامنا بھی کرتی ہیں۔

آرٹیکل ۱۴

انسانی عظمت کی حرمت وغیرہ۔۔۔۔۔

(۱) قانون کے تحت، انسانی عظمت اور گھر کی خلوت کی حرمت ہونی چاہیے۔

اپنے تمام ای میل ایڈریسز کو تلاش کریں یہ دیکھنے کے لیے آپ کی ای میل کہاں بھیجی گئی ہے
یا ممکنہ طور پر اس کا کہاں غلط استعمال کیا گیا ہے۔

یہ دیکھنے کے لیے کہ آپ کا پتہ یا اثاثوں کے ریکارڈ آن لائن کہاں پائے جاسکتے ہیں،
اپنے گھر اور دفتر کے پتے تلاش کریں اور ایک ریورس ایڈریس لگ اپ سرانجام دیں۔

اب آپ کو اندازہ ہو گیا ہوگا کہ آپ کا ڈیجیٹل شیڈو کیا ہے اور اسے کتنی آسانی سے دریافت کیا جاسکتا ہے، سوچئے کہ
اپنے ڈیجیٹل شیڈو کے بارے میں جاننا آپ کے لیے کتنا ضروری ہے؟

یہ جاننے کے لیے ڈیجیٹل شیڈو اور کتنے طریقوں سے کام کرتا ہے

Tactical Technology Collective

کا آن لائن جائزہ لیں:

<https://immersion.media.mit.edu/>

DuckDuckGo جیسا سرش انجن استعمال کریں، جو آپ کی پرائیویسی کا تحفظ کرتا ہے۔

اپنی غیر فعال، پچھلی آن لائن پروفائلوں کی طرح اپنی فعال پروفائلوں پر اپنے تمام صارف ناموں کے لیے تلاش کریں، یہ دیکھنے کے لیے کہ کیا کچھ آن لائن ہے۔

اپنے موبائل فون اور اپنے دیگر فون نمبروں کی تلاش کریں، یہ دیکھنے کے لیے آپ کے کون سے فون نمبر کی معلومات آن لائن موجود ہیں، ایک ریورس فون لک اپ کریں۔



ڈیجیٹل شیڈوز

آپ کی ہر قسم کی آن لائن کارروائی اپنے پیچھے ڈیجیٹل امور کا سراغ چھوڑ جاتی ہے جو کہ آپ کی شناخت ظاہر کرتی ہے۔ یہ معلومات ویب سائٹس کے ذریعے جمع کی جاتی ہیں اور اجتماعی طور پر ان کو آپ کی شناخت کرنے، حتیٰ کہ آپ کے تعاقب میں استعمال کیا جاسکتا ہے۔ اسے آپ کا ڈیجیٹل شیڈو کہتے ہیں: ایسی پروفائل جو آپ کی شناخت ظاہر کرتی ہے۔ اس طرح کی معلومات ان کمپنیوں کی جانب سے لی جاتی ہیں جو آپ کی معلومات اشتہارات بنانے والوں کو بیچ کر بے پناہ منافع کماتے ہیں۔ فیس بک جیسی کمپنیاں تو باقاعدہ قانونی طور پر ایسا کرتی ہیں جبکہ غیر مقبول، چھوٹی کمپنیاں صارفین کی کم تعداد کے ساتھ ایسا کرتی ہیں۔ جن پرائیویسی پالیسیوں کے ساتھ ہم رضامندی کا اظہار کر کے یقین دہانی کر لیتے ہیں کہ کمپنی ہماری معلومات جیسے ہمارے کریڈٹ کارڈ کی معلومات یا فائی، یا ہمارے مقام کے بارے میں جان لے دراصل ان معلومات کو دوسری کمپنیوں کو بیچ دیا جاتا ہے۔ ادھر ہم یہ سمجھ رہے ہوتے ہیں کہ ہم ان مصنوعات کا آن لائن استعمال کر رہے ہیں لیکن دوسری طرف ہم خود مصنوعات کے طور پر کمپنیوں کو بیچ دیئے جاتے ہیں اور وہ کمپنیاں ہماری خریدار بن جاتی ہیں۔

اپنے ڈیجیٹل شیڈو کے متعلق جاننا آپ کے لیے بہت ضروری ہے کیونکہ ان معلومات کو دوسرے بھی استعمال کر سکتے ہیں۔ اگر کوئی آپ کا تعاقب کر سکتا ہے تو وہ آپ کو ہراساں کرنے کے لیے بھی ان معلومات کے استعمال سے ممکنہ طور پر ایسا کر سکتا ہے۔ بعض دفعہ خواتین یہ شکایت کرتی نظر آتی ہیں کہ ان کے سابقہ شوہر کی جانب سے ان کا موجودہ مقام جاننے کے لیے ڈیجیٹل ٹریسر کا استعمال کیا گیا ہے۔ آپ اپنا ڈیجیٹل شیڈو کیسے جان سکتی ہیں؟ ڈاکسنگ (Doxing) تب ہوتی ہے جب کسی نقصان دہ ارادے کے ساتھ کسی شخص کے متعلق آن لائن معلومات جاری کی جائیں۔ کسی کو ڈاکسڈ (Doxed) کرنے کے لیے ہیک کرنے کی ضرورت نہیں پڑتی۔ آپ ڈیجیٹل شیڈو کا استعمال کر کے آپ کی معلومات کو آسانی سے تلاش کیا جاسکتا ہے۔

یہ جاننے کے لیے آپ کی معلومات کتنی آسانی سے آن لائن دستیاب ہوتی ہیں سیلف ڈاکسنگ کر کے دیکھئے: یاد رہے، گوگل پر تلاش کرنے سے آپ کو اپنی آن لائن معلومات کی تفصیلات کے بارے میں زیادہ معلومات نہیں ملے گی۔

اس سے پہلے کہ ہم بات کا آغاز کریں ایک نہایت مفید تجویز آپ کے سامنے رکھنا چاہتے ہیں: اس فن کو سیکھنے کے لیے آپ کو نہ تو ایک انجینئر بننے کی ضرورت ہے، ناکمپیوٹر سائنس میں کسی مہارت کی ضرورت ہے یا ڈیجیٹل سیکورٹی کو مرتب کرنے کے لیے ناہی کسی مہارت کی ضرورت ہوتی ہے۔ حتیٰ کہ اگر آپ تکنیکی علم نہیں بھی رکھتے تب بھی آن لائن سیکورٹی اور رازداری کو یقینی بنانا ایک بنیادی امر ہے اور اس کے لیے کوئی خاص مہارت اور علم درکار نہیں ہوتا۔ لہذا اس بات سے نہ ڈریئے کہ ڈیجیٹل سیکورٹی کو جاننا کوئی بہت ہی تکنیکی کام ہے، ہاں اس بات سے ضرور درنا چاہیے کہ آپ کی معلومات پر کسی قسم کے سمجھوتہ کی صورت میں آپ کے ساتھ کیا کچھ ہو سکتا ہے۔

تعارف

ایک معروف صحافی جہانزیب حق کا کہنا ہے کہ پاکستان میں موجود انٹرنیٹ صارفین کی کل تعداد کا ۷۰ سے ۵۸ فیصد مرد حضرات ۲۰۱۲ء ہیں۔ پاکستانی ایف آئی اے کا کہنا ہے کہ اگست 2014 سے اگست 2015 کے دوران سائبر کرائم کے ۲۰۳ مقدمات درج ہوئے جن میں سے تقریباً ۵۴ فیصد صرف خواتین کو سوشل میڈیا پر پیش آنے والے سائبر ہراسمنٹ سے متعلق تھے۔

پاکستان میں اس امر کی ضرورت ہے کہ یہاں زیادہ سے زیادہ خواتین کو آن لائن لانے، ڈیجیٹل مقامات پر زیادہ سے زیادہ حفاظتی تدابیر اور ایسی آن لائن ثقافت کو فروغ دینا ہے جو خواتین دشمن نہ ہو۔ یہ کتاب آپ کو یہ سیکھنے میں مدد دے گی کہ خود کو آن لائن رہ کر کیسے محفوظ رکھنا تاکہ پھر کبھی آپ کو اپنے آن لائن کاموں کو محدود نہ کرنا پڑے۔

ہم ایسی کئی لڑکیوں کو جانتے ہیں جنہوں نے فیس بک کا استعمال اس لیے ترک کر دیا کیونکہ ان کی پروفائل تصور کو چرا لیا گیا تھا، یا واٹس ایپ پر غیر پسندیدہ پیغامات ملنے کے بعد انہوں نے خود پر پابندی لگا دی۔ یہ بالکل ٹھیک نہیں۔

فیس بک کے ذریعے خریداری سے لے کر واٹس ایپ پر اپنی اسائنمنٹس کے تبادلے تک جوان اور عمر رسیدہ خواتین انٹرنیٹ اور دیگر ڈیجیٹل آلات کس استعمال بہت سے کاموں کے لیے کرتی ہیں۔ بعض دفعہ جب وہ دیکھتی ہیں کہ ان جگہوں پہ آن لائن آنے سے ان کو خطرات درپیش ہوتے ہیں تو وہ سرے سے ان خدمات کا استعمال ہی ترک کر دیتی ہیں۔ ان کے حفاظتی خدشات انہیں آن لائن دنیا کے مثبت استعمال سے بھی روک دیتے ہیں۔

اس کتابچے کے ذریعے ہمارا مقصد آپ کو یقین سکھانا ہے کہ کس طرح آن لائن رہتے ہوئے خود کو محفوظ رکھنا ہے۔ جس طرح آپ اپنے گھر کی حفاظت کرتی ہیں بالکل ایسے ہی ڈیجیٹل لحاظ سے بھی خود کو محفوظ رکھیں۔ آپ کی مشینوں کی طرح آپ کا ڈیٹا، آپ کی سوشل میڈیا پروفائل کے اور آپ وہ الفاظ جو آپ اپنے تبصرے کے طور پر چھوڑتے ہیں یہ سب بھی آپ ہی کا اثاثہ ہیں۔

اس گائیڈ کی ضرورت

اگرچہ ڈیجیٹل سیکورٹی پر مبنی بہت سی مفت اور آن لائن کتابیں دستیاب ہیں۔ تاہم ہمیں اس بات کا اندازہ ہے کہ پاکستانی انٹرنیٹ صارفین خصوصاً خواتین کے لیے ایک ایسی گائیڈ کا ہونا بہت ضروری تھا۔ اس ملک میں جو چیلنجز ہمیں درپیش ہیں وہ دیگر ممالک سے قطعی مختلف ہیں۔ آن لائن دیئے گئے مسائل اور ان کے حل ہمارے ثقافتی حقائق سے بالکل مختلف ہیں۔ اس کی مثال یوں دی جاسکتی ہے کہ دنیا کی کسی اور تہذیب و ثقافت میں کسی بھی خاتون کے لیے فیس بک پہ اپنی تصویر ظاہر کرنے سے اسے کسی قسم کے سیکورٹی خدشات کا سامنا نہیں کرنا پڑتا لیکن پاکستانی خواتین کے لیے (خصوصاً وہ کوئٹہ جو اپنی تصویر فیس بک پہ نہیں رکھنا چاہتیں) یہ ایک خطرہ بن سکتا ہے۔

بہت سی خواتین نے یہ شکایت درج کرائی ہے کہ ان کے چہروں کی پروفائل تصاویر کو فوٹو شوپ کی مدد سے ان تصاویر کا غلط استعمال کیا جاتا ہے۔ ان کے چہروں کے خدوخال کو وہاں سے اٹھا کر دوسری غلط قسم کی تصاویر کے اوپر بڑی صفائی سے چسپاں کر کے بعد ازاں ان خواتین کو بلیک میل کیا جاتا ہے۔ یہ جانتے ہوئے کہ ان خواتین نے کوئی غلط کام نہیں کیا لیکن پھر بھی نہ تو وہ اپنے گھر والوں سے اس معاملے پر مدد مانگ سکتی ہیں اور نہ ہی وہ قانون نافذ کرنے والے اداروں تک رسائی حاصل کر سکتی ہیں۔ کیونکہ ہماری تہذیب میں ایک خاندان کی نیک نامی ان کی خواتین کی پاکیزگی اور پاکدامنی سے جڑی ہوتی ہے اس لیے اس طرح کی بلیک میلنگ معرض وجود میں آ سکتی ہے۔

پاکستانی خواتین کی جانب سے آنے والی شکایات نے اس گائیڈ بک کے ارتقا کی طرف ہماری توجہ مبذول کرائی۔ ہم اس بات کا اعادہ کرتے ہیں کہ مناسب قوانین کی عدم دستیابی کی وجہ سے آن لائن ہراسمنٹ کو استثناء حاصل ہے۔ مزید برآں، یہ بھی ایک حقیقت ہے کہ پاکستانی خواتین کے لیے ایسی کوئی جامع گائیڈ موجود نہیں تھی جو ان کے حل کے لیے کام کر سکتی۔ اگرچہ ڈیجیٹل سیکورٹی کے لیے استعمال ہونے والے آلات ایک جیسے ہوتے ہیں لیکن اس میں ہمارا ثقافتی نقطہ نظر بھی شامل ہے۔ ہم نے اس میں انٹرنیٹ تہذیب کے قیام کے لیے تجاویز بھی پیش کی ہیں کہ جس سے ہمیں مزید درپیش چیلنجز کا سامنا کرنا پڑے۔

خراج تحسین

رہنما کتاب کو تشکیل دینا کبھی ممکن نہ ہوتا اگر (FNF) Friedrich Naumann Foundation کی مدد شامل حال نہ ہوتی۔ ان کی مکمل حمایت سے ہم اس قابل ہوئے کہ اس کتاب کو خواتین طالبات کیلئے تحریر کر سکیں جسکی بدولت ہم پر امید ہیں کہ یہ ان طالبات کی نہ صرف آن لائن بچاؤ اور تحفظ میں مدد لے گی بلکہ ان کا آن لائن مقام انہیں واپس دلانے میں بھی مدد کرے گی۔

مصنفین: نبیہہ مہر شیخ، غوثیہ راشد سلام، لعبت زاہد
ایڈیٹرز: نگہت داد، عدنان احمد چوہدری، عشبہ العین
مترجم: علی کامران
ڈیزائنر: افراء خالد

سیکنڈ ایڈیشن ریو اینڈ ڈ :

سیرت خان، فریحہ یاسر، جنت فضل، ہائرہ باسط، شائلہ خان، جی کامران، حمزہ ارشاد، علی کامران

ہمارا انٹرنیٹ سے متعلق

ہمارا انٹرنیٹ (Hamara Internet) ڈیجیٹل رائٹس فاؤنڈیشن کی ایک رہنما مہم ہے جس کا مقصد خواتین کے خلاف بڑھتی ہوئی ٹیکنالوجی سے متعلق خطرات اور آن لائن تشدد کی روایات سے نبرد آزما ہونا ہے۔ ایچ آئی پی کا مقصد ایک ایسی تحریک تشکیل دینا ہے جو آسان اور محفوظ ڈیجیٹل ماحول کو فروغ دے جس میں خواتین آزادی کے ساتھ ڈیجیٹل دنیا میں حصہ لے سکیں۔ آگاہی مہم نشستوں، تحقیق، اور ڈیجیٹل حفاظتی سامان کے ساتھ اس مہم کا مقصد خواتین کی صلاحیتوں کو سامنے لیکر آنا ہے تاکہ ان کی آن لائن جگہ انہیں واپس دی جاسکے اور پاکستان میں بڑھتے ہوئے ڈیجیٹل دنیا میں جنسی امتیاز کو کم کیا جاسکے ایچ آئی پی اس بات کو مد نظر رکھتی ہے کہ انٹرنیٹ ایک ایسی جگہ ہے جسے سب لوگوں کو برابری کی بنیاد پر استعمال کرنا چاہیے۔



DigitalRightsFoundation
"KNOW YOUR RIGHTS"

کی پیشکش

Friedrich Naumann
STIFTUNG FÜR DIE FREIHEIT

معلومات برائے حق طبابت و اشاعت

یہ گائیڈ بک Creative Commons Attribution-ShareAlike (CC BY-SA) لائسنس کے تحت دستیاب ہے

ڈیجیٹل ہراسمنٹ بھگاؤ اور محفوظ ہو جاؤ



Digital**Rights**Foundation
"KNOW YOUR RIGHTS"



ڈیجیٹل ھراسمنٹ بھگاؤ اور محفوظ ھو جاؤ

