انٹرنیٹ ہمارا
HAMARA INTERNET
www.hamarainternet.org

THE ART OF DIGITAL SECURITY FOR PAKISTANI WOMEN

MAKING ALL VOICES COUNT
A GRAND CHALLENGE FOR DEVELOPMENT

DRF
DigitalRightsFoundation
"KNOW YOUR RIGHTS"

THE ART OF DIGITAL SECURITY FOR PAKISTANI WOMEN

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

COPYRIGHT INFORMATION

The Project Of

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

In Collaboration With

MAKING ALL VOICES COUNT
A GRAND CHALLENGE FOR DEVELOPMENT

CONTENT

ABOUT DIGITAL RIGHTS FOUNDATION

Digital Rights Foundation is a research based advocacy organization based in Pakistan focusing on Information & Communication Technology to support human rights, democratic processes, and better digital governance. DRF opposes any and all sorts of online censorship and violations of human rights both on ground and online. We firmly believe that freedom of speech and open access to online content is critically important for the 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 trainings, 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 an Internet that is a space truly shared by all.

ACKNOWLEDGEMENTS

This guidebook would not have been possible had we not joined forces with Making All Voices Count (MAVC). 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

WHY THIS GUIDE BOOK?

There are many digital security guides and manual available online free of cost. However, we realised that there was a need for one for Pakistanis, especially Pakistani women. The challenges we face are different from 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 on line. 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 a taken and doctored using Photo manipulation software . Their faces were superimposed on intimate pictures of others and which in turned 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 honor for is intrinsically connected to women's bodies which is why this kind of blackmail is able to take place in the first place.

Complaints from Pakistani women have driven this initiative. In the absence of proper laws, we realised that not 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 isn't hostile to women. This book is going to help you ensure that you learn how to stay safe online so that you don't limit your online experience.

We know plenty of girls that 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 don't be afraid of digital security being too 'technical,' be more afraid of what could happen if your information is compromised!

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 locations, our viewing habit et al, 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 on line 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 lose the device but 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 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 knows she isn't 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.
(1) The dignity of man and, subject to law, the privacy of home, shall be inviolable.

Sarah starts to talk to her brother 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 isn't 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.

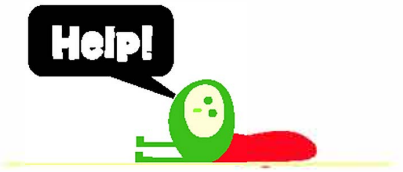
RUN AN ANTIVIRUS CHECK-UP ON YOUR COMPUTER REGULARLY:

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.A 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 email. A virus can install itself on your computer through online downloads, such as websites offering free music or videos, as well as emails, particularly spam email. 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:

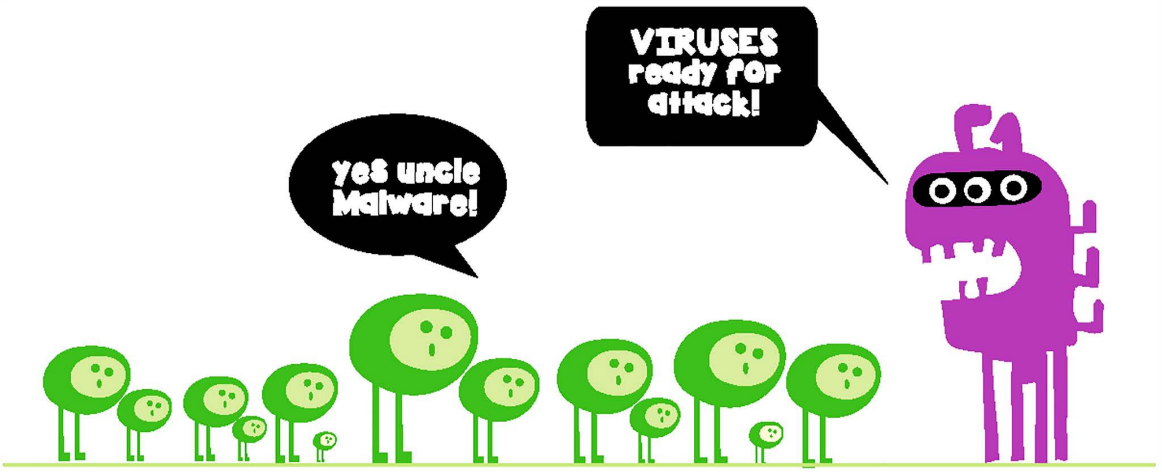
- **Kaspersky**
- **AVG**
- **Avast**
- **Norton Antivirus**
- **Avira**



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 viruses 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-viruses softwares deals 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 always make sure you have a copy of all your data.

TWO FORMS OF STORAGE YOU CAN USE TO STORE YOUR DATA

Use physical device like a USB or An External Hard Drive

Cloud storage which is online data storage.

FEAR

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

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 or

TIP

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

ALERT!

This also means that cloud storage is not safer than storage devices, as data can 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 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 anti virus and anti malware 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 didn't realize 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 lose her data.
Her second problem became obvious when she realized that her supervisor had taken her ID card copy from her hard drive without her knowledge. While the supervisor meant no harm and needed the copy for record keeping, Ateeba realized 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

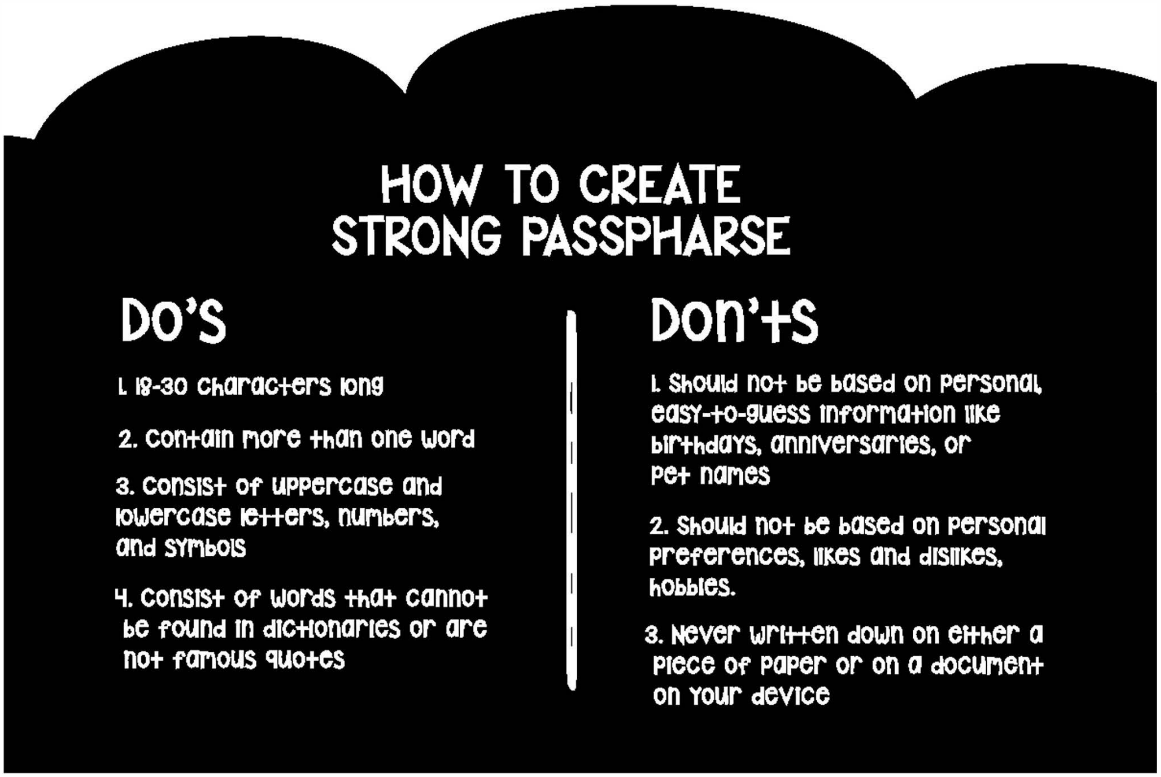
Passwords are the key to digital security. Weak passwords are easy to crack and it is harder for a hacker to access your accounts if your password is a strong one.

Too many of us think our passwords are strong when they are not. It isn't 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 hard to make up especially if you use passphrases instead of passwords.

MAKE THIS A RULE:
My password will always be very strong and I will never share it with anyone.

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 isn't 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.



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 passwords regularly and don't reuse old passwords.

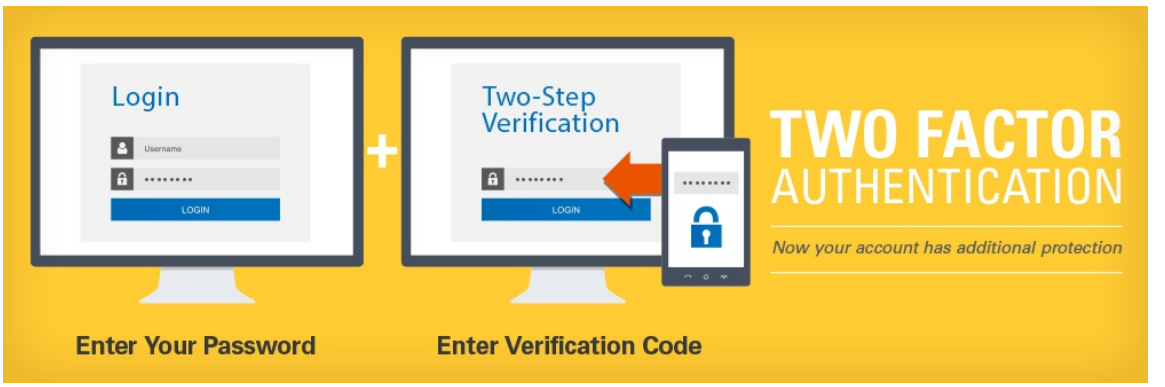
Always remember never to have the same password for every account or to use a password for more than one account. If one account gets hacked, the others could get hacked easily too.

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're 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

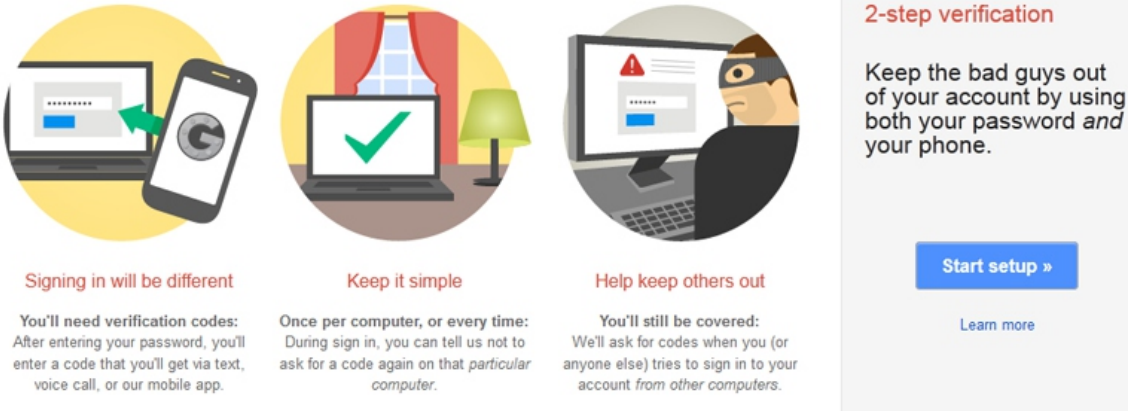
phone, so that even if it is stolen, your data will not be compromised so that even if it is stolen, your data will not be compromised

.

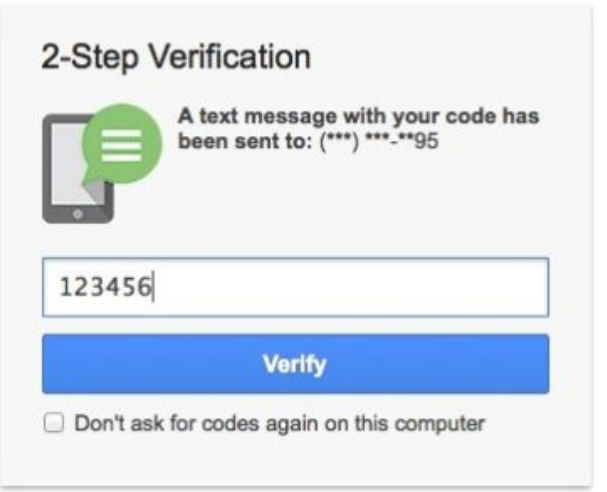
In case of emergencies, Gmail and Twitter allow you to download backup code(s) for when you need to login. (This will come in handy for those times when your phone falls in the toilet and the rice trick just won't work.) Never save these codes on your phone. Print them out or write them somewhere. Keep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

TWO STEP AUTHENTICATION FOR GOOGLE

1



2



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.

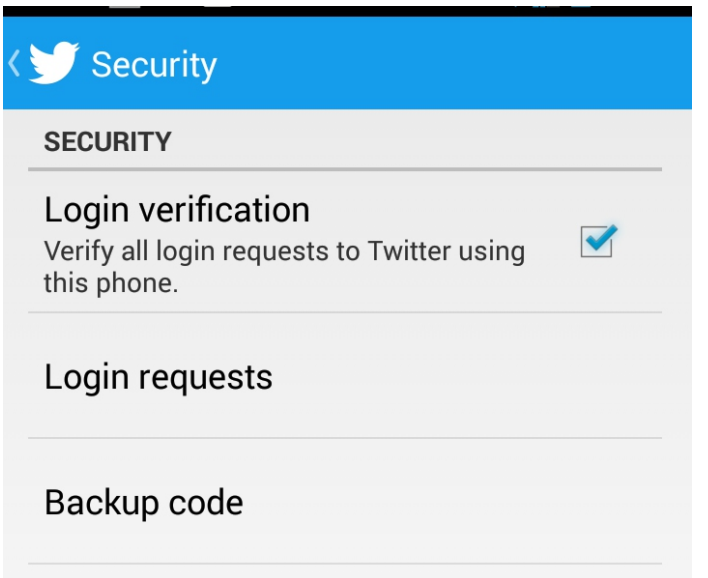
EXAMPLE:

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.
Rukshana's friend Maria told her to take a few precautions

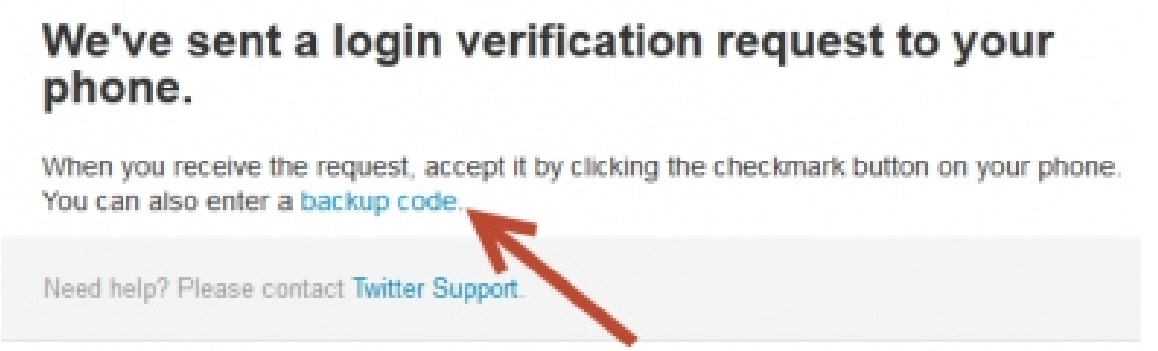
- She told her to immediately activate two factor authentication for all her accounts
- She then told her how to setup notifications for when someone accessed her Facebook account from a browser or computer that she had not saved
- Maria also showed Ruksana how to generate codes for her apps so that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

2-FACTOR AUTHENTICATION FOR TWITTER

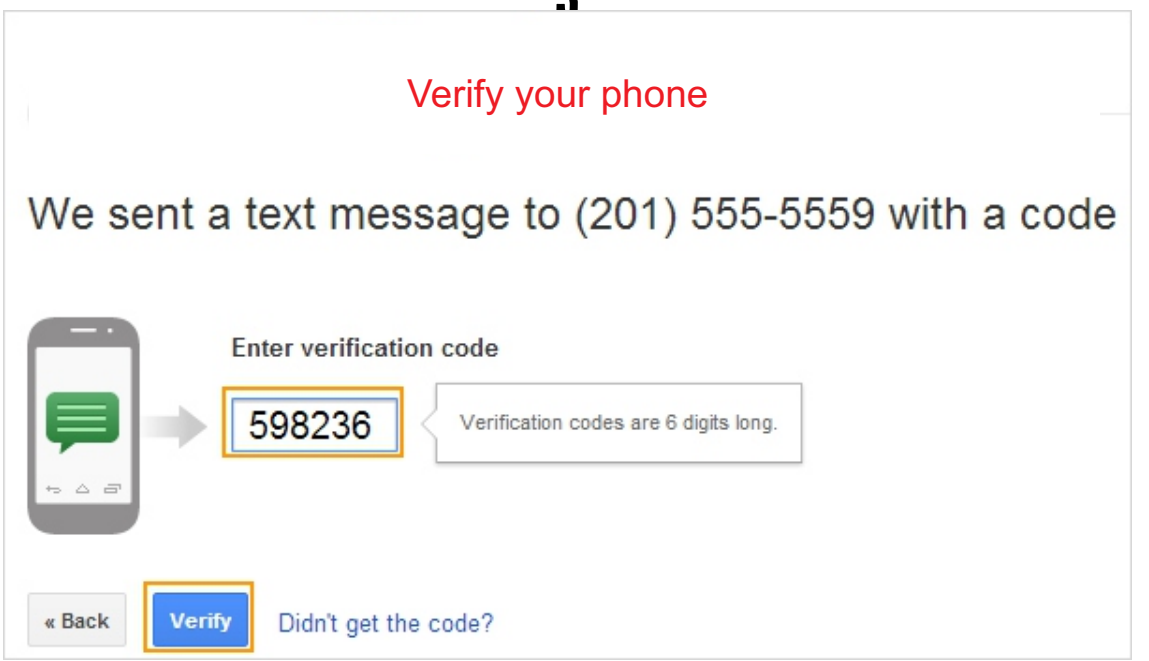
1



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 won't 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's 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've enabled options to block reported attack sites and web forgeries.

7. Never enter your password on a website which isn't 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:

Ensures 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.

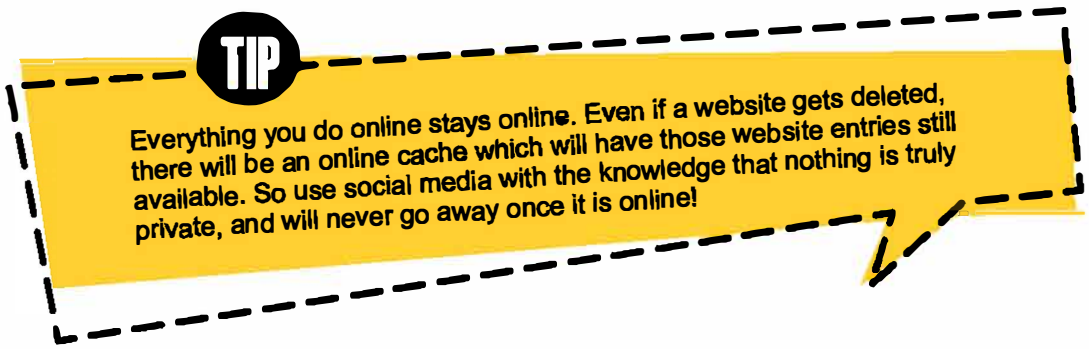
NO SCRIPT:

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 and 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're 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 personalize ads, or track you online. Check your Facebook ad preferences, you'll 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.



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 be aware that it can slow down your computer, and that it retains usage logs.The best option is look at paid but more secure options such as Disconnect or Tunnelbear Another option is installing a VPN add-on,such as Zenmate In your browser. Not allowing your devices access to 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're allowing the application to access our location at all times unless we switch it off. If you don't disable location services, your device 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 don't 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 isn't a pleasant one especially for those who identify as females.

In most cases, the negative experiences that people have online are dismissed, 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 subject to vicious verbal abuse. Have you ever been attacked online for your views? We're 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?

Or could it be because they want others to quit occupying digital spaces? We think they want to silence you and it's 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 wouldn't 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 ARE 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 spaceThey know that if they yelled and swore at you in a lecture hall it wouldn't be tolerated. People would speak up. You would be given support. Trolls, like schoolyard bullies, enjoy having power over someo.

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, an 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're being bullied online and you tell someone about it, you're often told to go offline. This implies that simply by being a social media user, you are responsible for what you're going through. We disagree with this and we'll 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?"

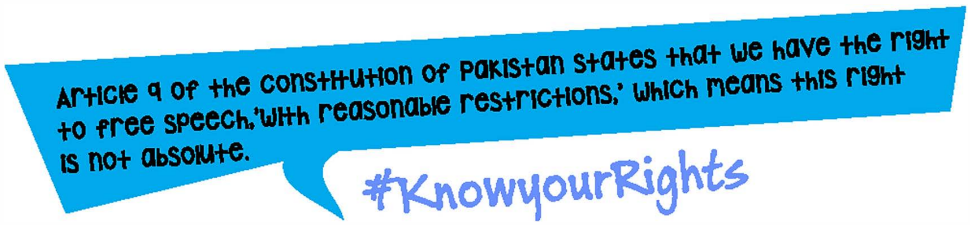
These things are hard to hear especially when they come from loved ones who mean well. They don't want to make us feel bad and they really don't want to see us distressed. These are the only solutions they can think of.

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 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 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 what your views, then any abusive actions they take are their responsibility, not yours.
- Yes, some comments should be ignored, but ignoring doesn't 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 aren't.
- 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 aren't 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 so important to remain on cyber spaces like social media instead of giving up.This is why we advocate creating safe spaces. **#OccupyCyberSpace** .



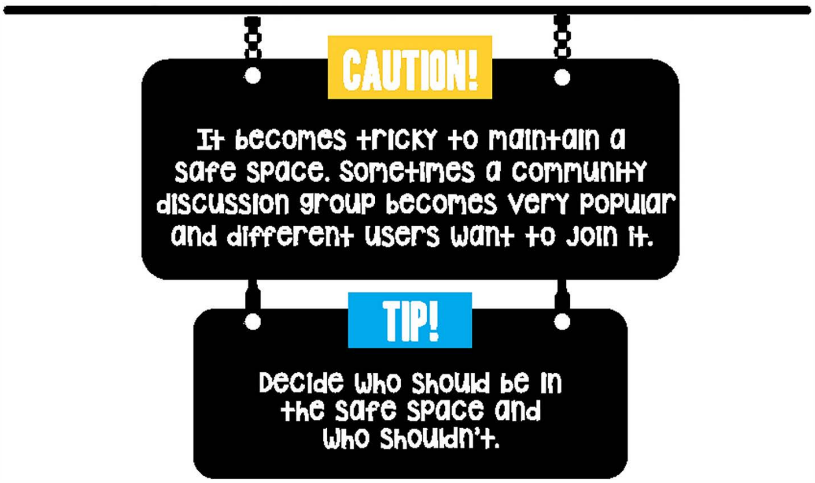
Amina is a blogger who writes about women's rights. Many people do not like her views and she receives many comments on her blog. Many of the comments are nasty. Examples include:

- **KILL YOURSELF!**
- **YOU'RE FAT AND UGLY!**
- **YOU'RE WORTHLESS AND CRAZY!**
- **NO ONE LISTENS TO YOU ANYWAY.**
- **NO ONE LIKES YOU.**
- **YOU'RE 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 distressing. Amina used to feel upset every time she received threats of physical harm.

Amina didn't know how to deal with the comments at first. She spoke to other female bloggers and discovered that she wasn't 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 understand that some people send her these comments hoping to silence her. She continues to write because she refuses to give up and she doesn't want her bullies to win.
Examples like this show us why it is so important to remain on cyber spaces like social media instead of giving up. This is why we advocate creating safe spaces. **#OCCUPYCYBERSPACE**

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 doesn't share them and wishes 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 responses 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 don't want others to hear. You wouldn't expect that someone will scream at you. People would hesitate to attack you in a public space knowing they wouldn't 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'll realise you've changed your mind because of the dialogues you've 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're 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!

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 a 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're 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's offline or online. The streets aren't safe for us because they don't want us in the space they've 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 isn't bad news. Online spaces rely on users to set the tone and we, as users, are in charge of the culture we create. Cultures change and evolve especially in today's rapid information age.
So we're 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 not to vent 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've had a bad day. We must be mindful of ourselves.

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're assuming you would get up and go get help. We're assuming you'd 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 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 support online 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're 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 mean 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 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.
- **Don't 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.
- Don't 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's not okay to judge someone for saying something they may not agree with. This isn't the case in cyberspace however.
- Remember that nothing gets lost in cyberspace. We don't 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'll 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's 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 know 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 instead. **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, don't 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 you 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.**

- 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 you 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 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're confident it can change. **#OccupyCyberSpace**

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