



**Digital
Rights Foundation**

"KNOW YOUR RIGHTS"

The background of the cover is a vibrant yellow, populated with various white line-art icons of journalistic equipment. These include several microphones of different shapes and sizes, video cameras, and handheld recording devices. A prominent, thick, red diagonal brushstroke cuts across the middle of the page, separating the yellow background from a solid red section at the bottom. The text 'GUIDEBOOK DIGITAL SECURITY FOR JOURNALISTS' is printed in large, white, bold, sans-serif capital letters within this red section.

**GUIDEBOOK
DIGITAL SECURITY
FOR JOURNALISTS**



ABOUT

Digital Rights Foundation envisions a place where all people, and especially women, are able to exercise their right of expression without being threatened. Digital Rights Foundation believes that a free internet with access to information and impeccable privacy policies can encourage such a healthy and productive environment that would eventually help not only women, but the world at large.



ACKNOWLEDGEMENTS

The Digital Security Guidebook for Journalists is authored by Luavut Zahid, edited by Hija Kamran and Nighat Dad, and reviewed by Digital Rights Foundation's team members Hamza Irshad and Adnan Chaudhri.

This Guidebook wouldn't have been possible without the support of good folks at Free Press Unlimited and Foundation Open Society Institute Pakistan. Follow their work at

<https://www.freepressunlimited.org/> and

<https://www.opensocietyfoundations.org/about/offices-foundations/foundation-open-society-institute-pakistan>

respectively.

CONTENTS



INTRODUCTION	1
COMPUTER HYGIENE	2
MOBILE SECURITY	5
CREATING & MAINTAINING SECURE PASSWORDS	8
SAFE & SECURE BROWSING	11
SAFE & SECURE USE OF SOCIAL NETWORKING SITES	16
THE LEGAL ROUTE	40
DEALING WITH ONLINE HARASSMENT	43
PROTECTING DEVICES FROM MALWARE & HACKERS	49
HOW TO PROTECT SENSITIVE COMPUTER FILES	52
DESTROYING SENSITIVE INFORMATION EFFECTIVELY	54
HOW TO RECOVER FROM DATA LOSS	56
USING TOR & VIRTUAL PRIVATE NETWORKS	58
USING VPNs & PROXIES	60
SECURE CHATS & PGP	62
USING ANDROID & iPHONE SAFELY	85
HOW TO STAY SAFE WHEN USING YOUR MOBILE	88



SO YOU'RE A JOURNALIST.

Almost all of your work is either connected to your laptop or desktop, with a considerable amount of that work often routed through your phone. While you edit away at a story on your laptop, you are talking to sources on your phones. It wasn't always like this. What was once a handwritten piece or a typewriter produced article, is now possible on your own laptop. What was once a portable tape recorder is now an app on your phone. The nature of media is changing not just in Pakistan but all over the world - and with the increased digitization of content, has also come the increased digitization of your profession. And like yin and yang, and bread and jam, technological progress too is coupled with technological threats.

But why should you care about technological threats?

The very tools that have made your job so much easier can compromise your security - and for journalists in Pakistan, the threats associated with tech are manifold. Pakistan is the fourth most dangerous country in the world for journalists -and that is not a stat that should be taken lightly. While there's no chance that you will just up and quit your job because of the dangers associated with it, you can make an effort to keep yourself safer online.

The Digital Rights Foundation has created a series of chapters which can tell you exactly how to make sure your digital presence does not compromise your non-digital life. In preparing this guidebook, we took the help of Maria, who is also a journalist just like you, and went through the motions of making herself more secure after finding out how security threats were affecting her life and work.



COMPUTER HYGIENE

More than a decade ago, a sort of revolution took place in local media. TV channels entered the scene once again and kicked the industry out of its sleep. The work had changed, the people had not - but the revival shook things up and a technological shift became apparent. Newspapers, too, began increasingly relying on technology to get their work done, and journalists too were seen scrambling to keep pace.

Maria realized early on that avoiding technology was not going to be an option. The idea of 'digital first' flooded the scene and even journalists that typically avoided new forms of media could no longer shy away. As time went by, using laptop to get work done became a norm, and then a little further down the line, having apps for documents and media files on one's phone also became passé. Maria relied on her tools and gadgets a lot - and if one were to suddenly give up on her, she didn't know what she would do. And that is what happened. One fine day, Maria watched her deadline fly by as her hard drive breathed its last. All that work, all that data, gone in a few seconds.

LAPTOPS & DESKTOPS - TALES OF INSECURITIES

Where did Maria go wrong? She didn't understand the importance of her digital hygiene. Security threats to digital tools like laptops and computers are as old as laptops and computers themselves.

Whether you're an electronic journalist or dabble in some print, the likelihood is that like Maria, your work revolves around your laptop. You either create your stories on your system, or bring in materials that can be turned into one.



WHAT DOES YOUR COMPUTER NEEDS SECURITY AGAINST?

Viruses, spyware, malware and more - there are digital germs all over the place and they are out to get your data.

VIRUSES:

Maria's hard disk and her data went up in flames because of a virus that she hadn't detected. A Trojan, worm, backdoor virus, etc can infect your system and turn it upside down. Different viruses attack your system differently and they come with many names and flavors.

A virus can infiltrate your system through a portable device such as a USB or external hard drive, or even through a webpage you've visited or email you've received. But don't let your data and files become victims of a virus like Maria did.

PREVENTION vs CURE:

Viruses can be dealt with in two ways. You can either prevent them from doing any damage, or try to take the bull by the horns once you've been infected. Start with getting the right kind of anti-virus and depending on which operating system (are you on Windows or using a Mac?) you're using you will have different options available to you.



PREVENTION

View external forces with suspicion! Maria has been very careful about the files she downloads from her emails. When the sender is not known to her she sends the file to her trash can instead of trying to peak.

Removable media is not always your friend. A USB or external hard drive can be infected with their own brand of viruses, so be careful and be vigilant. Run them through a virus scan before opening them on your system if you can't avoid them completely. Avoid the auto-play like plague.

Sharing is not caring. Journalists often can't avoid using their USBs or hard disk on other systems; and in some cases you will have to give your removable media to others. Avoid this as much as possible; you don't know the digital hygiene habits of other systems and people, and have no idea what your own trusted device may do to your system once it's been with someone else.

CURE

Tell your software to update itself regularly. All programs will come with this feature so that you don't have to go through the hassle.

Maria made the mistake of not updating her anti-virus program. Don't be like Maria. New viruses are being released on a very regular basis, and virus definitions - the stuff that tells your anti-virus what is and isn't a virus - are also updated regularly. Not updating your anti-virus regularly means it may not know of new viruses that exist, and won't be able to stop them.

If you enable round the clock protection for your system, your anti-virus should be able to trap a potential problem in its net. You should also schedule a weekly thorough check for your entire system.

COMMON MISTAKES

Don't install more than one anti-virus software on your laptop or computer. The more is certainly not the merrier in this case and often the two (or more?!) anti-viruses on your system will slow it down immensely - and in some cases they may actually start fighting each other because they identify the other as a virus.

Don't think having a simple anti-virus is going to protect you enough. There's a whole world worth of problems for you to tackle.



MOBILE SECURITY

A lot of the work we do as journalists happens over phones these days. Like Maria, many of you must own a smart phone (and some of you may even have a second phone just for the job!). Communication has never been this efficient - or this dangerous - for journalists. Take a moment to think about it. What kind of sensitive information are you carrying around in your phone. When Maria took a deeper look, this is what she found.

Types of data on your phone

Contacts of everyone from people in the news organizations to source's recordings of calls that she had made while talking to people about her stories so that she could transcribe them or use them as a referencer later, a long line of texts that contained sensitive details about stories or sources, photos and videos that she had created with her phone, documents that were stored in it because she often downloaded work files to edit them when she was on the go. Maria also realized that many of the apps she used were tracking her location courtesy her phone.

The thing is, information that you have on your phone is sensitive and could be vulnerable. When you look at it often you don't see a security risk because what's in a picture you took while you were doing a story, right? The reality is that every piece of data a journalist creates can at some point backfire. The data that you send to someone, and the data that you store on your phone itself, is sensitive. So what do you do?



The Nitty-Gritty

Remember that your mobile phone is running on a network owned by a commercial entity. This means that said entity has access to just about any and every piece of information you send forth from your mobile. With the new Prevention of Electronic Crimes Act (PECA) 2016, ISPs could even keep user data for up to a year. So think twice about what you use your phone for.

If you own a smart phone, you're practically using a minicomputer and not just a simple phone. So treat it like a minicomputer and be as vigilant for its security and safety as well. Think hard about who you call, what you speak about, when you communicate and where from. Can your call location, for instance, be tracked later, and reveal something about a source? Can your text messages be intercepted with sensitive details about a story?

What sort of data trail are you leaving behind because of your phone? Does an app, like Facebook or Twitter, highlight your location when you use it through your phone? Are there permissions you need to revoke?

Keeping yourself safe

- Your phone comes with a 15-digit serial IMEI number that can help identify it uniquely. Dial `*#06#` to find out yours and keep it noted somewhere safe
- Make sure your phone has a password on it at all times and avoid sharing it with anyone
- Never give your phone to someone else - even someone you would typically trust



- Physically mark your storage card and/or SIM so that you can spot if they have been changed or tampered with
- Keep a conscious record of the information that is stored on your SIM and avoid storing sensitive or vulnerable information
- If at any time you need to give your phone to someone for updates or repair work, ensure that your data has been deleted or moved from your phone beforehand
- Don't throw away or sell your phone without ensuring that sensitive data has been taken off of it first. At times something as simple as your own picture, and not even a source, could be used against you by someone with malicious intent
- Create regular backups of the information on your phone. Mobile security isn't just about fighting an external threat, your phone could die a sudden death at the hand of a virus, and you could lose all your important data
- Last but not least, ensure that the security measures you are using to keep your phone safe and your communication safe are being employed by the people you are communicating with. Your measures are only going to work if the other person also pays heed to their security. If they do not, then you're going to be a sitting duck.



CREATING & MAINTAINING SECURE PASSWORDS

A journalist in Pakistan is only as safe as their password is. Maria has always had trouble coming up with the right kind of password and has had to develop the habit of cultivating passwords that are strong. Around ten years ago Maria used the phrase ‘mariaizkool’ as all her passwords. Her work as a journalist, and a couple of compromised accounts, taught her she had to do better. Maria was making a couple of mistakes. Can you spot if you’re making them too?

Mistakes

- Using the same password for multiple account is a big problem. If you lose the password for one, you lose the password for all.
- Shorter passwords are easier to hack and crack. A password should ideally be at least 13-18 characters long and should contain numbers and characters.

Does that description fit your password?

- Using a password that you think is meaningful and easy to remember is often a bad idea. For example, you may think a popular name, location or your date of birth is easy to remember, but it may also be easy to guess for someone else.
- Do not let your browser remember your passwords - a hacker can steal them right from under your nose.
- Do not use your personal information as a password.
- Sharing is not caring in this case and it does not matter how close someone is, simply never share your password with them. Getting compromised by proxy is never a nice feeling.



So how good is your password? Head over to howsecureismypassword.net to find out. Or run it through Kaspersky's secure password check. That should tell you how long it will take for a typical computer to crack open your account.

For a stronger password do the following

Take a memorable phrase and reduce it into a code. For example, Maria went with her older password and gave it a new spin. "Maria is cool" became "m|zk00". A phrase that means something to you is easier to remember for you and not for anyone else. Edward Snowden has a method where you select a memorable or amusing phrase and rework it with keyboard characters and punctuations. You can also use a password generator but beware that since this isn't your brain coming up with the password, you can forget it as easily as you created it.



THINGS TO KEEP IN MIND

1

A strong password isn't 100% foolproof. Someone could still gain access to your super strong password and use it against you. How? Through various methods, including spyware, social engineering, etc.

2

Use a password keeper like KeyPass so that you don't have to strain your memory. In the digital age, there's a digital solution to just about every problem. LastPass or pwSafe will perform the same function.

3

Don't use public PCs or someone else's system if you don't know or trust them. They could be rigged with keyloggers and other malicious software that can steal your data.

4

You need to be vigilant about your digital hygiene. A strong password is a sitting duck on a compromised machine.

5

Turn on your multifactor authentication where possible to avoid the likelihood of a single password compromising your entire account.

6

Regularly update your passwords. There's no reason to feel so proud of a password that you simply hold onto it for months and months. The average age of even the best password should be 72 days and no more.



SAFE & SECURE BROWSING

Maria has sat through one news story after the other about people just like her - other journalists that are being spied on, monitored and compromised in one way or the other. Just like her, you too must have raised an eyebrow when you read about NSA's surveillance, or that authorities in Pakistan were looking to beef up their own eagle eye. What's a journalist to do?

Never fear as long as encryption is near.

As a general habit, make sure that the connection you are using is secure. Maria learned to do this the hard way when her browsing habits began getting the better of her. Secure Sockets Layer (SSL) encryption makes it possible to add another level of security to your web browsing. All regular web addresses start with an HTTP at the head.



However, a secure website will give you a **HTTPS** at the start. The extra S points to a secure connection. You can monitor the address bar to see which websites automatically have an SSL certificate and which don't.



An HTTPS address will also come coupled with a small lock symbol that is at times displayed in the address bar itself and at others displayed elsewhere in the browser depending on what you're using. But what difference does this really make? Simply put, an HTTP connect is like you posting a box of goodies to your friend's house but not sealing the box shut with tape.

If the delivery guy, or someone else who notices the box, sees it open then your goodies maybe stolen - and if nothing is stolen it's more your luck than anything else.

Your data over the internet is pretty similar. It's a box of goodies waiting for someone to steal it, unless you add in some HTTPS tape to the mix. HTTPS doesn't just ensure that your data is not intercepted by someone in the middle, it also makes sure that you are connecting to a website after verifying its security certificate.

THINGS TO KEEP IN MIND

- ✓ Your browser will generally alert you if something doesn't seem right. Like if a website's certificate is expired or simply doesn't exist, or if the information on the server and the certificate do not correspond.
- ✓ Getting an add-on extension for your browser to keep HTTPS on everywhere will remove the hassle of you having to keep an eye on it manually. Do a little research on the security add-ons that you can install to your browser to stay safe.
- ✓ HTTP only connections create a lot of caches and store cookies that can be used to track you later, in comparison HTTPS can keep you safer.



BROWSING

- They can collect information about your identity
- They can unwillingly help you acquire malicious software and viruses
- Keep a collection of information about the websites you frequent, and how you behave online
- Store your passwords and other sensitive information (autofill is a big bad thing, avoid it!)
- Most journalists don't realize that their choice of browser has a lot to do with how safe they are. Get Firefox if you're using Windows and Chromium if you're on Mac. A more secure browser is Tor, but we'll get to that later in this chapter.

The Right Browser

Once you've acquired the right browser, you need to move on to your browsing habits. The likelihood is that you're doing all your work on a single browser - change that. Hopefully nobody is going to spy on you when you're looking up new shoes on Daraz.pk. So don't go for Tor for regular use but make sure you are using it when you're doing something sensitive relating to a story or a source.

Extension

Adding an extension to your browser can also wipe your identity and location out of the equation. You can also find an extension that can prevent your browser from tracking your behavior, passwords and more. Firefox also has a robust set of extensions to augment privacy. No reason for you to not use them.

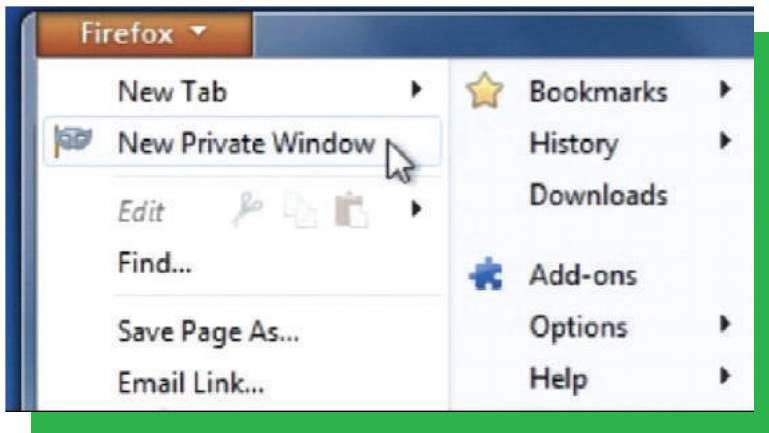


No Script

Sounds complicated and weird and like Maria, you probably don't know what it means. NoScript blocks JavaScript in your browser. <https://noscript.net/> can help you turn it off. In case it's turned on, it can be used to grab your password, infect you with viruses and malware, and even steal a whole host of other data about you. You will need to take a look at which websites you're allowing JavaScript to run on after you go on with this option. Some experts suggest simply getting rid of Java altogether, but we aren't quite there yet.

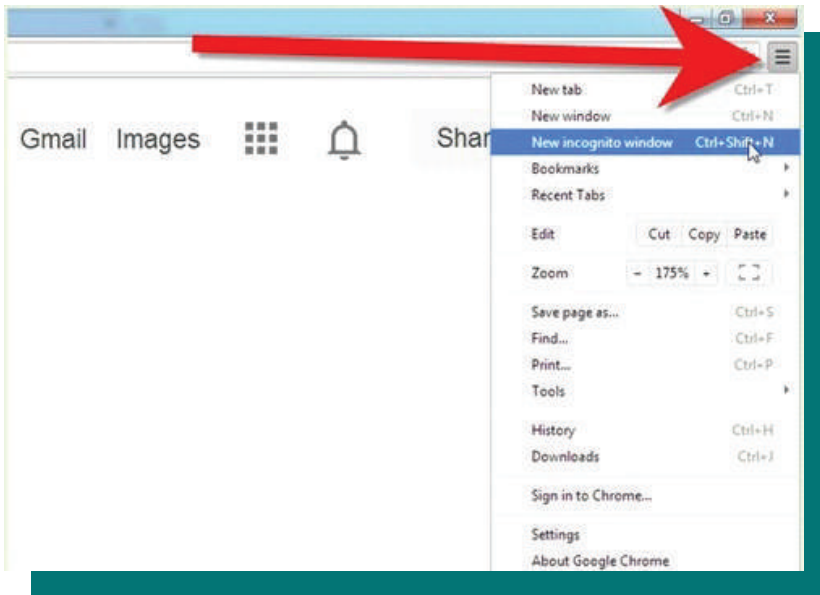
Become a Ghost

Private or anonymous browsing is another option for you to keep the tracking away. Both Firefox and Chrome come with these options. Within Firefox this is known as 'in private browsing' and can be accessed like this:





In Chrome, it's called "incognito" and you do it like this:



THINGS TO KEEP IN MIND

- Do not make use of the auto complete feature on shared laptops and computers. What may be a second of convenience for you can turn into a golden opportunity for someone else.
- Avoid saving your passwords into your browser.
- Regularly clear out your cache, history and cookies.
- Make sure you know what information needs to be shared where. Sensitive information like your passwords, bank details, etc should not be shared with anyone.
- Avoid sharing your number and address with any websites that ask for them. No website can ever make it obligatory for you to give up this information - and the ones that do should be avoided anyway.
- A Firefox browser will at times clash with Tor on Mac, otherwise it's a perfectly good option to use there too.



SAFE & SECURE USAGE OF SOCIAL MEDIA NETWORKING SITES

Various studies have been conducted on the topic of social media and its evolving relationship with journalists. What was once just good as a pastime has become a serious tool for finding new stories, scopes, sources and more.

Maria found a study by two professionals from the Indiana School of Journalism, which consisted of responses from 1,000 journalists, and found that the data really resonated with her.

The study found that 40% of the respondents felt that social media was important to their jobs. Maria agreed, she didn't know what any TV channel or newspaper would do without their Facebook page or Twitter account.

The study also showed that Twitter was the most popular means of finding news. Maria realized that colleagues and peers were using it to find breaking news, see what other news outlets were upto and even recognized that a couple of her own stories had come from there.

Social media is also an important tool to promote one's own work and engage with their audience directly, with many journalists using it solely to do this very task and nothing else. However, social media networks come with their own set of problems. And learning how to stay safe and secure as you use them has never been more important than now.

The extended version of this guidebook is uploaded on our website - <https://digitalrightsfoundation.pk/services/>.

The guidebook contains steps to ensure privacy of the following social media platforms:

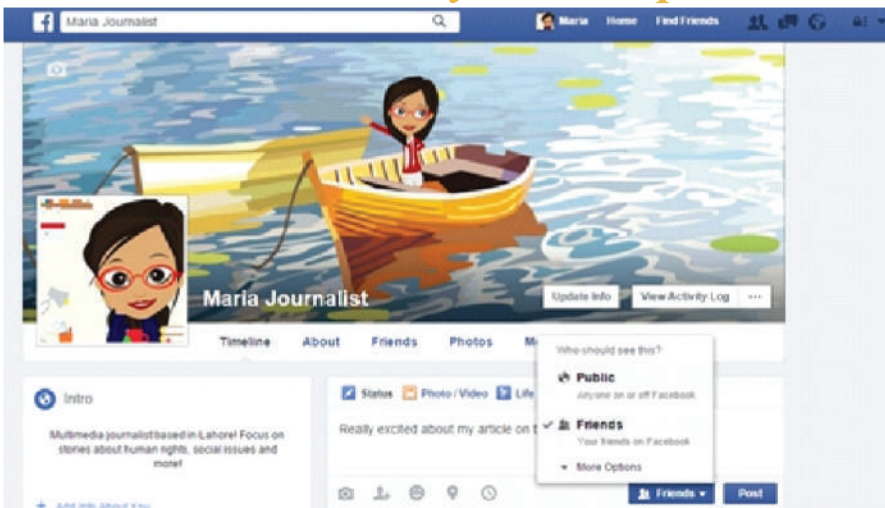


Facebook

Facebook has a few provisions you should know about when you're trying to stay safe and secure.

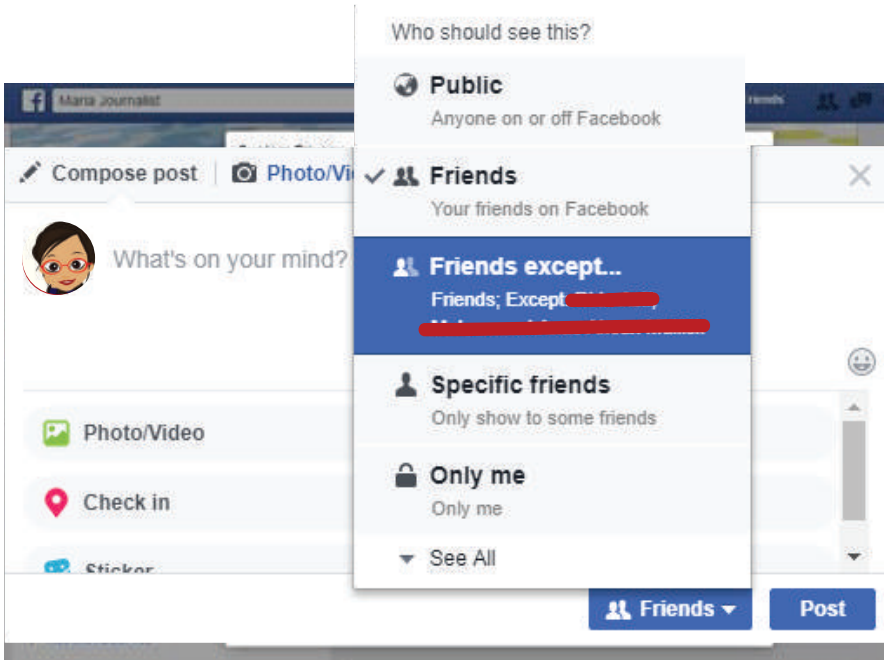
https://web.facebook.com/ajax/marketing/tour/privacy_tour.php is a good link to get started if you don't know much about your own privacy.

Let's start with your own posts



Facebook allows you to pick who the posts you are making are available to. You can choose to show it only to your friends i.e. the people who are on your contact list, or you can choose to make it public, or even to just a few friends.

Journalists often post things publicly because they have an audience to engage with. But sharing sensitive or private details publicly on Facebook can lead to trouble. While you are okay with some people viewing your post, you may not want others to see it. In this case you click more options and opt for custom settings.

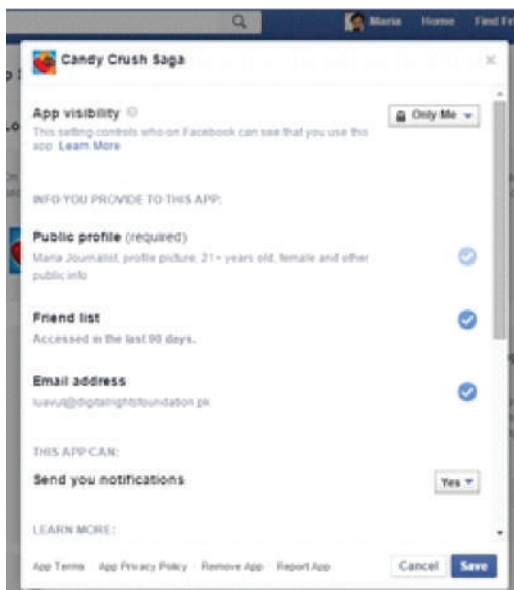


Here you can pick names of people on your friends list that you want to make the post available to, and can choose individuals or groups that you want to hide it from.

Similarly, your pictures can also be posted (including your profile picture and timeline photos) with privacy in mind.



Don't make any image publicly available if you think that it can be misused. Maria's friend Minerva is popular blogger online who had her pictures stolen from her Facebook. The images were used in a hate campaign on social media that was meant to attack her. Learn from her mistake, keep your posts and pictures safe.



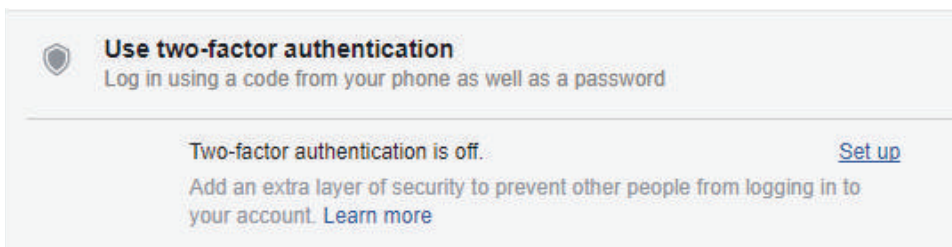
Next have a look at the apps that you have installed on Facebook. An app is anything from a Candy Crush Saga game to Twitter's connection to Facebook. Have a look and see which app has access to which of your content. If you do not use an app anymore then delete it. If you think an app has access to something you don't like, get rid of it.



Facebook has a robust set of security settings for you to peruse through and keep yourself safe. Apart from letting you approve of the browsers and apps that you generally will use Facebook on, pick your Trusted Contacts, create a public OpenPGP key and legacy contact. This section also lets you come up with actual alerts that you can use to figure out if your account is compromised. For instance, the Login Alerts section shoots out an email to you as soon as someone logs into your account from a new device (phone or laptop).

You can also create Login Approvals, also known as Two-Factor Authentication. Whenever you login from a new device, a second code is sent to your phone without which the login cannot be completed. This step makes it exceptionally hard for anyone to break into your account.

First pick the option that requires a second security code for login:



Facebook will walk you through the process of using your phone for the task.



Enter your phone number:

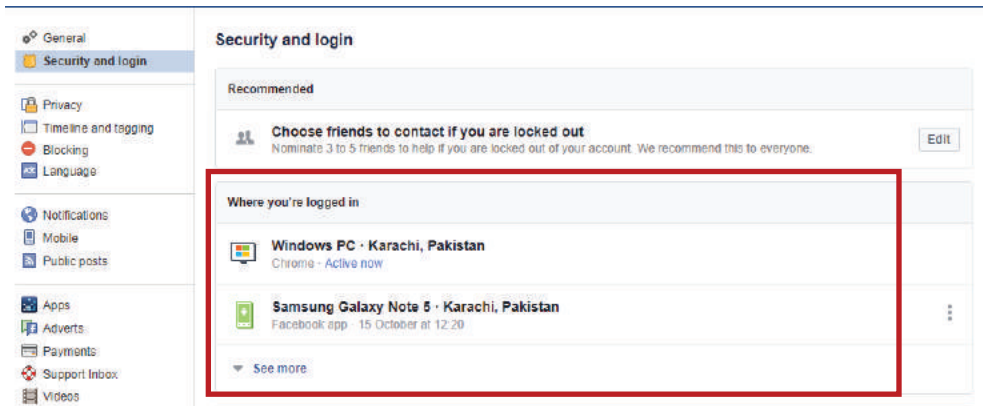
A screenshot of a Facebook dialog box titled "Confirm your number". The dialog has a blue header bar. Below the header, there is a "Country code" dropdown menu set to "Pakistan (+92)", a "Phone number" input field with the placeholder text "Enter your number", and a "Confirm number by" section with a radio button selected for "Sending me a text". Below these fields is a paragraph of text: "Confirming your mobile number helps you reset your password if you ever need to, find friends, get SMS updates and more. Only you will see your number." At the bottom right of the dialog are two buttons: "Continue" (in blue) and "Cancel" (in white).

Facebook will now send a code to your mobile number via SMS. Enter the code, and you're done!

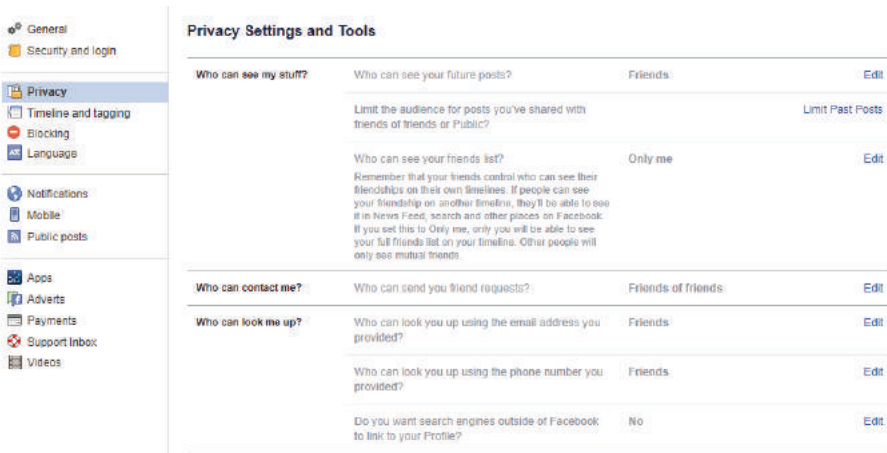
A screenshot of a Facebook dialog box titled "Enter your confirmation code". The dialog has a blue header bar. Below the header, there is a message: "You should receive a text on [redacted] with your confirmation code soon." Below this message is an input field with the placeholder text "Enter confirmation code". At the bottom left of the dialog is a link: "Resend Code (please wait at least 5 minutes before requesting another code)". At the bottom right are two buttons: "Confirm" (in blue) and "Cancel" (in white).

The code generator will automatically create new codes after every 30 seconds which you can use to login to your account. Apps such as Google Authenticator are a great tool that you can install on your phone to manage accounts, which use two-factor authentication. This feature comes in handy when you are travelling.

Facebook will also let you review your current sessions to see where your account is logged in and functional and will terminate any that you find suspicious.



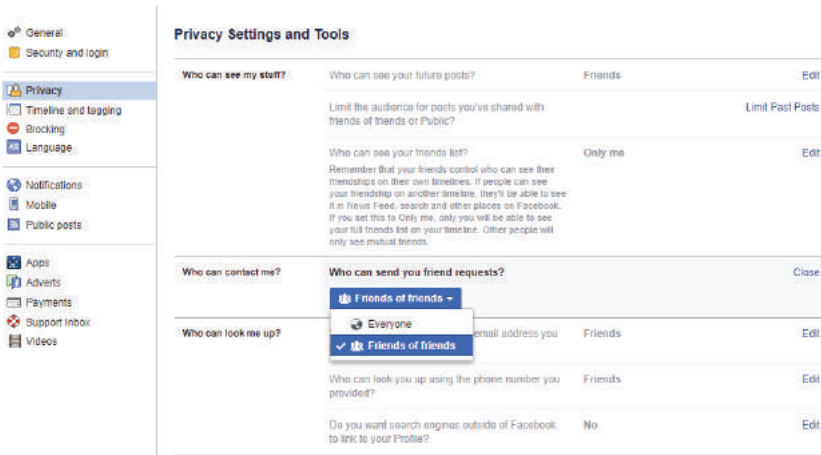
Similarly, privacy settings on Facebook aren't that complicated.



So who can see your stuff? You can edit this setting to select the audience you want. Post privacy has already been discussed before. The second option “Review all your posts and photos you’re tagged in” lets you review the posts that you are tagged in. You can either allow or deny tags that people create for you on Facebook.

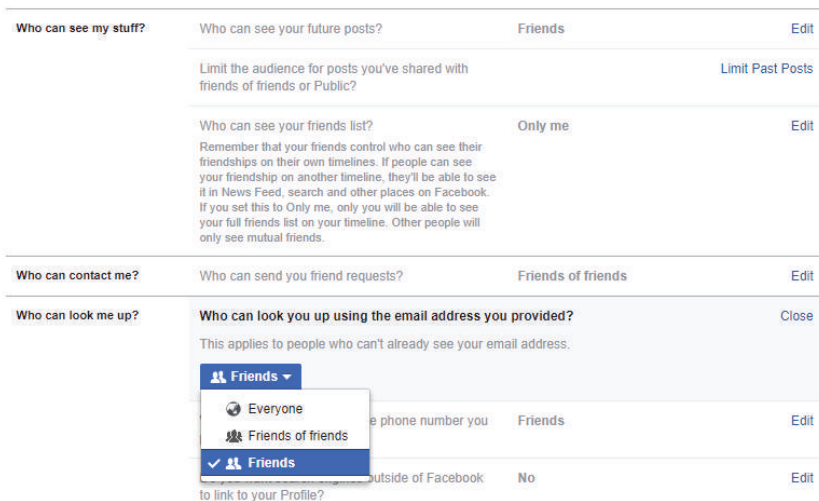


The privacy section also lets you choose who can contact you. You can pick Everyone or the more private option of Friends of Friends.



Similarly, there is option for you to pick who can look you up using the email address you've provided for Facebook.

Privacy Settings and Tools





Depending on the level of security you want, you can opt for one of the three options here. Journalists that engage their audiences a lot through Facebook would prefer that 'Everyone' find them through their email address, while others that maintain more personal profiles would opt for 'Friends' only. The settings are the same for the phone number that you've listed on Facebook.

You can either pick whether you want search engines to be able to link to your profile by choosing Yes or No from the same menu.

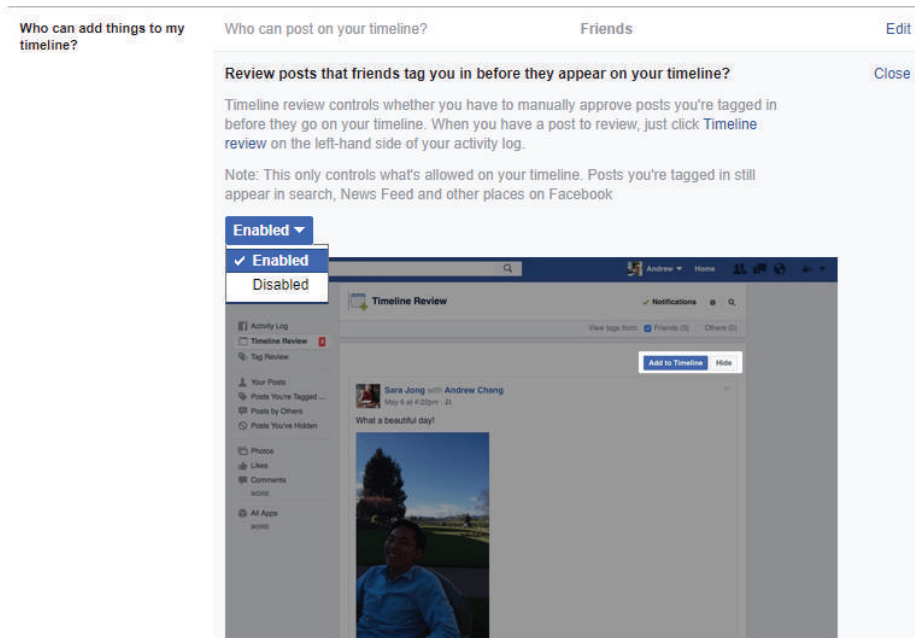
The Timeline and Tagging Settings allow you to pick who can post and tag you in posts that appear in your timeline. You can choose whether you want just your own posts to show up on your timeline or if you're okay with your friends posting on it too:

Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Close
	<div style="border: 1px solid #ccc; padding: 2px;"><div style="background-color: #4267b2; color: white; padding: 2px; display: flex; align-items: center;">👤 Friends ▾</div><div style="padding: 2px; display: flex; align-items: center;"><input checked="" type="checkbox"/> 👤 Friends</div><div style="padding: 2px; display: flex; align-items: center;"><input type="checkbox"/> 🔒 Only me</div></div>	
	Friends tag you in before they post on your timeline?	On Edit
Who can see things on my timeline?	Review what other people see on your timeline	View As
	Who can see posts you've been tagged in on your timeline?	Only me Edit
	Who can see what others post on your Timeline?	Only me Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On Edit
	When you're tagged in a post, who do you want to see it?	Only me Edit



Meanwhile, you can also pick whether you want people to be able to tag you in their posts. While some journalists would prefer to disable this because if they are popular, they will get tagged way too often, others may see it as a good way of interacting with people and allow it.



Use the “View As” option to see who can see things on your timeline. And also confirm who can view the posts that you have been tagged in on your timeline by fixing the audience for said posts. Since the posts that people may tag you in are unpredictable, it would be better to not allow this and opt for 'friends' or 'only me' settings.



Who can see things on my timeline? Review what other people see on your timeline [View As](#)

Who can see posts you've been tagged in on your timeline? [Close](#)

- Only me
- Everyone
- Friends of friends
- Friends
- Only me**
- Custom
- More Options

Who can see posts you've been tagged in on your Timeline?	Only me	Edit
Who can see your own posts before you post them?	On	Edit
Who do you want to see posts you've been tagged in that aren't already in it?	Only me	Edit
Who sees tag suggestions when photos that look like yours are tagged?	No one.	Edit

How can I manage tags people add and tagging suggestions?

Facebook also lets you review the tags people create of you. Keep this option enabled.

Review **Review posts that you're tagged in before the posts appear on your timeline?** [Close](#)

Timeline review controls whether you have to manually approve posts you're tagged in before they go on your timeline. When you have a post to review, just click **Timeline review** on the left-hand side of your activity log.

Note: This only controls what's allowed on your timeline. Posts you're tagged in still appear in search, News Feed and other places on Facebook

Enabled

- Enabled**
- Disabled



You can also manage your tags by picking who you want to add into the audience:

The screenshot shows the 'How can I manage tags people add and tagging suggestions?' section of Facebook settings. It includes several options with 'Edit' links:

- Who can see things on my timeline?** Review what other people see on your timeline. [View As](#)
- Who can see posts you've been tagged in on your timeline?** **Only me**. [Edit](#)
- Who can see what others post on your Timeline?** **Only me**. [Edit](#)
- Review tags people add to your own posts before the tags appear on Facebook?** **On**. [Edit](#)
- When you're tagged in a post, who do you want to add to the audience if they aren't already in it?** [Close](#)

A dropdown menu is open for the last option, showing the following choices:

- Only me** (selected)
- Friends
- Only me** (with a checkmark)
- Custom

And pick who sees tag suggestions based on what you look like.

The screenshot shows the 'Who sees tag suggestions when photos that look like you are uploaded?' section of Facebook settings. It includes the following options:

- Review tags people add to your own posts before the tags appear on Facebook?** **On**. [Edit](#)
- When you're tagged in a post, who do you want to add to the audience if they aren't already in it?** **Only me**. [Edit](#)
- Who sees tag suggestions when photos that look like you are uploaded?** [Close](#)

The 'Who sees tag suggestions...' section contains the following text:

When a photo that looks like you is uploaded, we'll suggest adding a tag of you. This helps save time when adding tags to photos, especially when labelling many photos from one event. Suggestions can always be ignored and no one will be tagged automatically. [Learn more.](#)

A dropdown menu is open, showing the following choices:

- No one.** (selected)
- Friends
- No one.** (with a checkmark)

Below the dropdown, there is a section titled 'These Photos?' with the text: 'The photos you uploaded were grouped automatically so you can quickly label and notify friends in these pictures. (Friends can always untag themselves.)'

Two photo thumbnails are shown, each with a tag for 'Albert Hong' and a close button:

- Albert Hong
- Albert Hong

Facebook also gives you extensive options to block users, messages, app invites, pages, etc. in the 'Manage Blocking' section. Feel free to block abusive content when and as you see fit.



Facebook Profile Picture Guard

Facebook has also introduced a new feature known as the Profile Picture Guard, to prevent misuse of profile pictures. This new feature gives more control to users by limiting who can download and share their profile pictures.

When the guard is turned on, people who are not friends on Facebook would not be able to share or download your profile picture. Also, only you and your friends can tag your picture on facebook. In addition to this, a blue border and a shield around the profile picture will also be shown as a visual cue of protection.

Here is how you can turn on the Profile Picture Guard:



Help Protect Your Profile Picture

Use profile picture guard to help your profile picture stay more secure.

Turn On Profile Picture Guard

If you see the above notification, it means that you can turn on the Guard. Click on ‘Turn on Profile Picture Guard’, which will redirect you to a page that will let you choose a new picture or add a guard to the existing picture.



Once you have turned on the guard, Facebook will also give you an option to choose a design, in the form of lines and patterns, which you can have on top of your picture. According to Facebook, adding a design overlay to a picture means that others are at least 75 percent less likely to copy it.

Although this new feature would help in controlling the misuse of profile pictures, it still has loopholes and it is unlikely that it would stop people from copying profile pictures overnight. While the introduction of this new feature is commendable, unfortunately users can still take screenshots from their mobiles. Hopefully, Facebook will soon try to amend these loopholes but for now we can laud this initiative and feel more at ease with this new feature.



Twitter

Journalists love Twitter. Pakistani journalists can't get enough of it. We have already talked about the stats and facts related to its popularity, now let's discuss how to stay safe on it. Twitter is a microblogging website that can totally land you in deep trouble if you aren't more vigilant.

Pull up the setting's menu after you login. The settings should be in the left-hand bar once you've opened them. Click on Privacy and safety:

Account	>
Privacy and safety	>
Password	>
Mobile	>
Email notifications	>
Notifications	>
Web notifications	>
Find friends	>
Muted accounts	>
Muted words	>
Blocked accounts	>
Apps	>
Widgets	>
Your Twitter data	>
Accessibility	>

Pick the option that requires additional information when a password reset request is sent to Twitter for your account.

While this won't stop an expert from cracking your codes, it will still be a deterrent that could keep your account safe. You can do it like this:



Security

Login verification Verify login requests

After you log in, Twitter will send a SMS message with a code to that you'll need to access your account.

[Setup a code generator app](#)

Use an authenticator app to generate a time-based passcode that can be used to access your account.

[Get Backup Code](#)

Save this backup code to ensure that you can still log in if you ever lose access to your device.

[Generate app password](#)

Generate a temporary password to log in to devices and apps that require Twitter credentials.

Password reset verification Require personal information to reset my password

For added security, this requires you to confirm your email or phone number while resetting your password.

Your twitter photofeed used to be simple but now you can be tagged by people in the posts that they create. You can change your settings to disallow people from tagging you. And in the same vein also protect your tweets:

Privacy and safety

Privacy

Tweet privacy Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more.](#)

Photo tagging Allow anyone to tag me in photos

Only allow people I follow to tag me in photos

Do not allow anyone to tag me in photos



While protecting your tweets means that they will only be available to a limited audience, you will be much safer than before.

Twitter, like Facebook, has the option to add locations to your posts. Go to the tweet location section and uncheck it. Furthermore, it would be a good idea to delete all location information from your account:

Tweet location Tweet with a location

If selected, you can add a location to your Tweets, such as your city or precise location, from the web and via third-party applications. This setting does not affect Twitter for iOS or Android. [Learn more](#)

[Delete location information](#)

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Like other social media sites, Twitter too lets you pick how accessible you are through your personal information. Since it is a more public medium than Facebook, anonymity needs to be considered. To control who can discover you on Twitter using your email address or phone number, go to Settings and Privacy > Privacy and Safety > Discoverability. Untick both the options to control how people search you on Twitter.

Discoverability Let others find you by your email address
 Let others find you by your phone number

This setting will take effect once you add a phone number. [Add now](#)

[Learn more](#) about how this data is used to connect you with people.

Now take a deeper look at what third party apps have access to your account as well.

Go to Settings and Privacy > Apps. Here, you'll see all the apps that you have given access to your Twitter feed. The good thing here is that you can also check when the access was granted. Revoke access to the apps that you don't recognize or don't want on your profile anymore.



Applications

These are the apps that can access your Twitter account. [Learn more.](#)

You will need to [generate a temporary password](#) to log in to your Twitter account on other devices and apps. [Learn more.](#)



Facebook Connect

Post Tweets to your Facebook profile or page.

[Connect to Facebook](#)

Having trouble? [Learn more.](#)



Twitter for Android

Twitter for Android

Permissions: read, write, and direct messages

Approved: Monday, July 7, 2014 at 6:03:23 PM

[Revoke access](#)



Mobile Web by Twitter

Twitter Mobile Web

Permissions: read, write, and direct messages

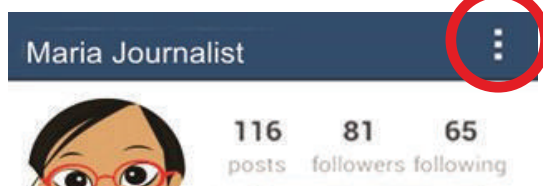
Approved: Friday, February 20, 2015 at 11:55:09 PM

[Revoke access](#)

Instagram

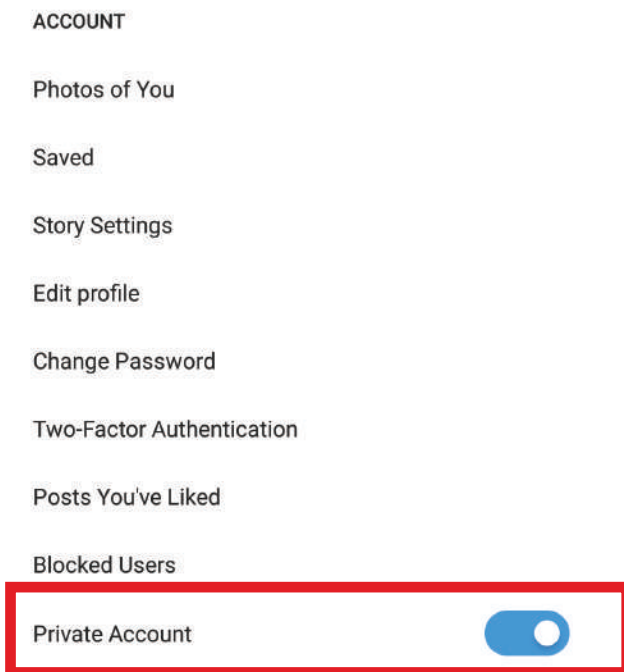
Any good multimedia journalist can be found on Instagram. Even journalists that aren't into multimedia or don't function as photojournalists can be found on Instagram. It's a good way to connect with not just people you know but also a wider audience. Hashtags originally found their way into the mainstream through mediums like Instagram.

But of course there's always the matter of security and privacy that one needs to think of. To keep your profile photos private, go to your profile > click on the three dots (⋮) on the top right corner of the screen.





Under ‘Account’, towards the end, you'll see an option “Private Account” that allows your posts to remain private. Turn this security setting on.



Move on to the people that you don't know. Social networks are full of strangers and you end up following a lot of people that you don't know simply for the traffic they may bring to the table. However, after a little while you realize that some of them are posting inappropriate comments on your pictures. What are you to do?

Block them of course.

Go to your Profile > Followers. Tap on the three dots (⋮) next to the person you wish to remove off your profile and click “Remove”. Be informed that this option won't block the person, but only deletes them off from your followers.



Report...

Block

Hide Your Story

Copy Profile URL

Send Message

Send Profile as Message


Turn On Post Notifications

To Block them, go to their Profile and click (⋮) on the top right corner and click Block.

The information on your profile should always be kept private, and what you share on it should not be something that can put you in any kind of danger. To make sure that you're not sharing any sensitive information with the world of strangers, go back to your main profile and click on the 'Edit your Profile' option. Look at what information you're adding in and take out details that are too personal.



A screenshot of the Instagram 'Edit profile' interface. At the top, there is a header bar with a close button (X) on the left and a checkmark on the right. Below the header, the text 'Change Photo' is partially visible. The form contains several input fields: 'Name' with the value 'Maria Journalist', 'Username' with the value 'maria', and 'Website' which is currently empty. The 'Bio' field is highlighted with a red rectangular border and contains the text 'Bio'. Below the 'Bio' field, there is another 'Bio' label and a text input area.

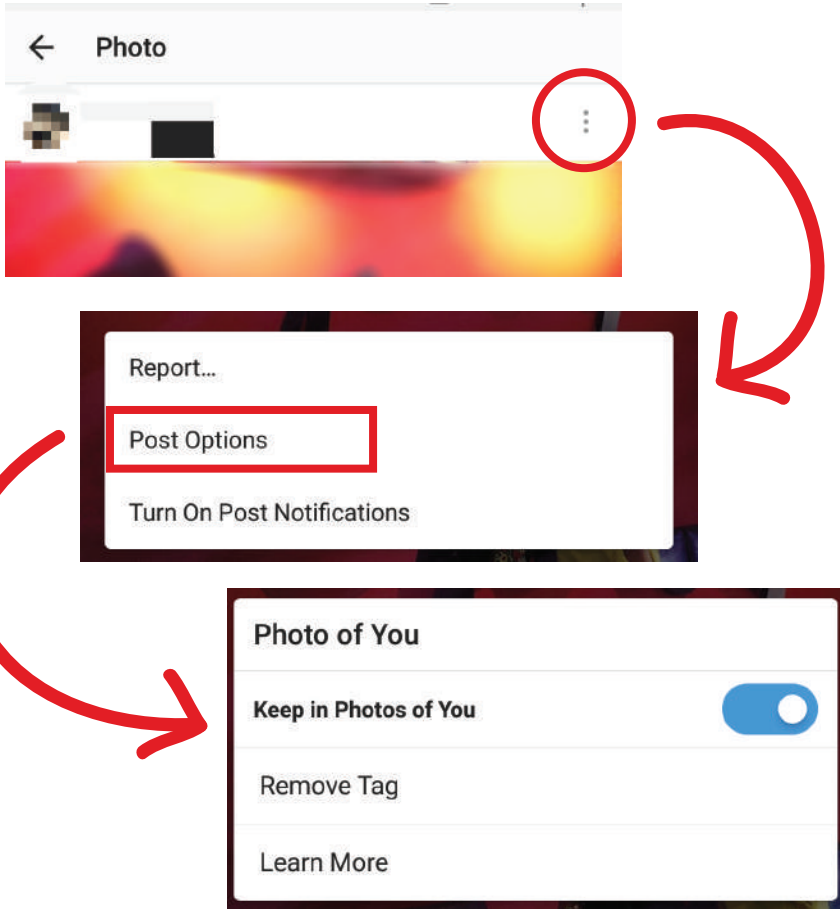
Like other social networking websites, people on Instagram can tag you in their photos which are not necessarily yours, or the photos you don't want online. Because all of your tagged photos automatically make it to your timeline under "Photos of You" or this  icon, it's important that you give extra attention to where you get tagged in and by whom.

If someone tags you in an unwanted photo, go to that photo, click on (⋮) on the top right corner, click on "Post Options", and move on to click "Remove Tag" in case you want to remove your profile tag off the photo, or turn "Keep in Photos of You" option off to stop the photo from appearing on your profile.

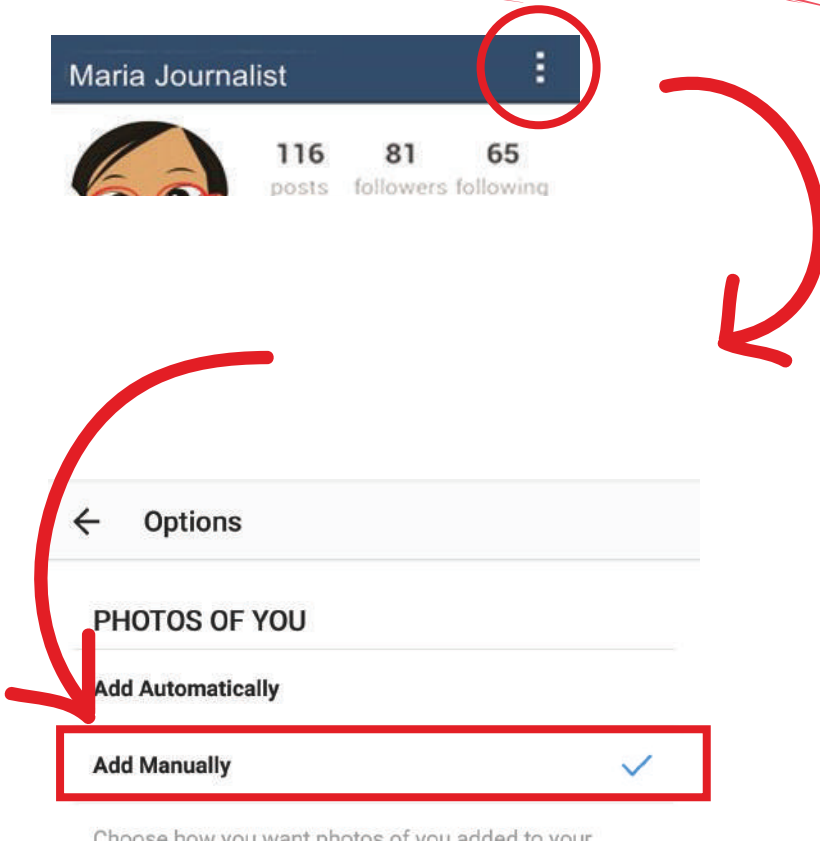
Similarly, you can also Report the photo by going in the same (⋮) menu and click "Report".




Removing Photo Tag on Instagram

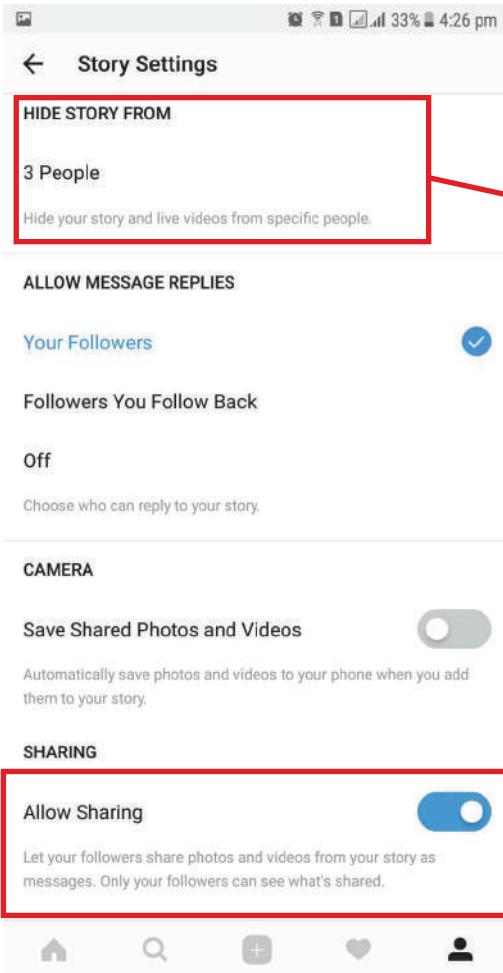


While you're at it, also make sure that the photo tagging is set to be manually accepted under Settings. People should not be able to tag you in just about any post, you are a journalist after all. So go to your main profile, and click on (⋮) on the top right corner. Look for the “Account” section, and under that you’ll find the option of “Photos of You”. Click on it, and select “Add Manually” on the screen that follows. Here’s a pictorial guide for your convenience:



Recently, we've seen a new feature changing the way we experience social media very quickly - the Stories! Once this was an exclusive feature for Snapchat, an app famous among teenagers, but now everyone has jumped the bandwagon after Snapchat's success, and Instagram didn't stay behind either. While the photos posted on Insta Stories remain their for only 24 hours, but it's important to keep their privacy under consideration. Ideally you would want everyone to see what you're posting because it feels good to see people taking interest in your content but it's not always recommended. Important is to restrict the audience of these stories as well.

To do this, go to your Profile >  > Account > Story Settings.



Here, you can control who CAN'T see your story. So even if somebody is following you and can see your regular feed, they won't be able to see what you post on your story.

This option allows your followers to share your photos and videos among themselves, but be warned that you won't be notified about this sharing. While it may not pose any security threat, it's still better that you keep this option off.



THE LEGAL ROUTE

Journalists are often disproportionately affected by cybercrime. Maria found it ironic that she wasn't just being targeted by the government but also had to worry about the audience that sometimes didn't find an article too pleasing. Writing about Balochistan, minority issues and even women's rights sometimes meant a barrage of abuse was heading her way. It's one thing to have to tackle a government agency and another when it's the very people you're creating your pieces for.

While most journalists face online harassment, female journalists are more vulnerable to it and experience it in gendered ways.

There is good news and there is bad news.

Cybercrime laws do exist in Pakistan. While their efficacy and the way they have been created can be debated on, they do provide an outlet to people looking to report digital crimes.

Overview of Laws

In Pakistan, cybercrimes come under the following acts. The Electronic Transaction (Re-organization) Act, 1996, The Wireless Telegraph Act, 1933, The Telegraph Act, 1885, Electronic Transaction Ordinance 2002, The Payment Systems and Electronic Fund Transfers Act, 2007, and a relatively new Prevention of Electronic Crimes Act 2016 (PECA).



These laws deal with electronic transactions, records, communications, data, documents, and more, malicious code such as malware or spyware, cyber stalking, spamming, spoofing etc.

As a journalist, you should be able to get help immediately, because often your lack of action will not just mean you are compromised but also that your source maybe in trouble.

How to report cyber harassment and threats

Once you realize that you are compromised or vulnerable in some way, start by ensuring that your own privacy and security is top notch and then move towards reporting to the authorities at once.

Let your friends and family know about the situation so that you have a proper support system setup for yourself. In case your accounts have been hacked or you've lost control of them, this will also help your friends and family steer clear of interacting with the hacker.

Your next step should be to approach the Federal Investigation Agency's (FIA) National Response Centre for Cybercrimes (NR3C). Visit <http://www.nr3c.gov.pk/creport.php> to report the crime. Make sure that you hand over your details properly; the NR3C does not deal with anonymous reports for obvious reasons.

You can also report the crime by sending an email to helpdesk@nr3c.gov.pk in case you haven't been able to fill out the form or have too much detail. Include all evidence of the harassment in your email.

While the online reporting mechanism is in place at the NR3C website, it's not as effective as one would think. It's advisable that anyone who wishes to report an official complaint with the



FIA should visit their offices located in Karachi, Lahore, Islamabad, Peshawar, Quetta, and Rawalpindi, with a couple of documents ready and in hard copy when they visit the office. These are:

- ✓ An application addressed to the deputy director of the branch with a detailed explanation of the incident
- ✓ Prints of the screenshots of all the evidences
- ✓ All the numbers or email addresses or URLs used by the perpetrator to contact the victim
- ✓ Copy of CNIC of the complainant

The Cyber Harassment Helpline

To address increasing number of cases of cyber harassment and to provide initial relief to the victims in distress, Digital Rights Foundation started Pakistan's first Cyber Harassment Helpline in December 2016. The Helpline provides free, confidential, non-judgmental, and gender-sensitized services to the victims and survivors of cyber harassment through the toll-free number 0800-39393 everyday and via email on helpdesk@digitalrightsfoundation.pk.

The Cyber Harassment Helpline has legal advisors, digital security experts, psychological counsellors, and a strong referral system readily available. They answer any queries that the callers might have, and to take them through the step-by-step legal or digital security process, and to provide them psychological relief that often becomes extremely essential in the wake of traumatic experiences online.

CYBER HARASSMENT HELPLINE

0800-39393



ONLINE HARASSMENT

Journalists in Pakistan come under fire constantly for the work that they do. The threat level is no joke, and this is no safe country for anyone in this profession. However, when it comes to the audience side, often female journalists find themselves receiving an unbalanced amount of hate because of their work. Getting bullied, threatened, and abused online is nothing new for many journalists. Anytime Maria writes an article that proves to be controversial or challenges the norms, she faces extreme backlash. There have been times where she has shut down her online presence, and other times where she has simply stopped writing altogether.

The fact is that no female journalist should have to limit their work because of online harassment. In the past, social media campaigns on both Facebook and Twitter have targeted female journalists for opinions and views that any male journalist would be applauded for.

Why does this happen more to women?

- Female journalists, and women at large, are seen as softer targets online. Abusers find it easy to sit behind a screen - often while enjoying anonymity - and say and do whatever they want without consequence. The modus operandi for most women is to retreat, and online harassers know this all too well.
- Because women opt out of their online experience instead of fighting back, the abuse only becomes much worse.
- Pakistan's society has deep rooted issues with patriarchy and misogyny. Those attitudes then seep into different professions including journalism. When a woman is attacked, many a times the response is to ask what she did to deserve it, instead of



asking what could have been done to prevent the abuser from behaving in the manner that they did.

- Women are often afraid to report to their superiors. Issues of harassment are either hushed down or not taken seriously. Some that try to push forward anyway are instead branded hot-headed, impossible and/or attention seekers.
- By removing barriers to harassment and silencing women, we create a loop whereby a female journalist is not only attacked frequently, but also silenced more often.
- Often abuse originates from within the media fraternity itself. There have been times where female journalists have been attacked by their audience online and their male colleagues have made the situation worse. Being ridiculed for their opinion or work from within their organizations is nothing new to female journalists, but online it takes a much worse shape.

So what can one do to deal with the abuse?

- Take a break. While quitting social media completely is no solution, taking a break just to regroup your thoughts and plan of action is a good idea.
- Invest your time away from social media into a support system. A collection of likeminded friends and peers can help you tackle online hate and abuse. There is strength in numbers, it is harder for online trolls to attack when they know a backlash may be on its way.
- Know that this is not a problem that is unique to you. Online harassment will always be much worse for female journalists. The only thing you can do is keep working and not back down.



- Lobby for change at the work place. Does your office take online harassment seriously? If not, then grab a few of your colleagues and try to get the management to understand the ground realities.
- Acknowledge that getting harassed, be it online or offline, is not part of your job and not something you signed up for. Learn to actively report content online and do it frequently. At times, reporters get tired of reporting profiles and posts that are targeting them - but if you don't report, no action can or will be taken.
- Learn to also discern the severity of the situations you are in. It doesn't take long for an online threat to become real offline. Know when to go beyond reporting online and reach out to the law enforcement agencies.

Why you can't afford to quit social media

- The vast sea of contacts and sources that exist in the online world cannot be accessed in the offline world. From reaching out to a minister sitting in another country to connecting with a colleague in the next room - we use social media for everything. Quitting means giving up on many tools that make your job easier.
- Social media is used to disseminate and promote your work. Not being a part of it is akin to putting an enormous amount of effort into baking a cake and then refusing to put it on the table.
- Stories, stories and stories. Many times a scoop is waiting just around the corner in a social media post. If you aren't using social media, you won't be able to get the right story at the right time to your audience.



TYPES OF HARASSMENT

Types of Online Harassment	What is it?	How to tackle it?
THREATS	<p>This involves a person following someone's every move online from checking out their social media profiles to the articles that they write, and then harassing them. Online stalkers are able to do the same thing offline stalkers do: they trace your shadows and the moves you make - only this time everything is digital.</p>	<p>First report to the platform where you are receiving threats. If things get out of control then approach the FIA for help.</p>
IMPERSONATION	<p>Fake profiles on Facebook and Twitter are common these days. Someone can simply copy your basic information, a few of your pictures, and develop a new profile and pretend to be you. Female journalists face these issues regularly.</p>	<p>First report this as a fake profile to the social media website, and ask your friends to do the same. Inform your family, friends, and colleagues about your fake profile so they don't interact with the perpetrator and don't end up compromising any personal information.</p>



Types of Online Harassment	What is it?	How to tackle it?
DOXING	<p>This is when your personal information including your contact, your email address, your physical address, etc is made public online. What this does is give people online access to your life offline. When a person issues a threat about your article or project online, at times you can ignore online harassment thinking it will just go away with time - but what do you do when an online harasser shows up offline?</p>	<p>Start by reporting to the platform that is hosting your personal information. Simultaneously approach the FIA for legal action so that the person doxing you can be found and prosecuted. In cases where the platform is slow to react or isn't taking your information down, use the Digital Millennium Copyright Act against them. Your personal information and data is YOURS, you shouldn't sit by when it's made public and do nothing.</p>
DOGPILING	<p>This is where you find that you write an article or produce a news piece that people may not agree with. Offline people will shake their fists and move on, but online they band together and start attacking the author with insults, threats and more. Dogpiling can make</p>	<p>The best solution to massive online harassment is to take a step back and basically take a break. The abusers are plenty in number but there's only one of you. Apart from this, once you have had a sufficient break also make sure that your own support network</p>



Types of Online Harassment	What is it?	How to tackle it?
	<p>Twitter accounts unusable because of the barrage of abuse. Often things go to a point where a journalist ends up shutting down their online media presence.</p>	<p>is trying to help you counter the abuse. In the online world, fighting back sometimes requires stepping back first and letting the cavalry arrive.</p>
TROLLING	<p>Trolling is something every journalist is well versed in. Hostile comments, hate speech and generally disgusting behavior online in the discussion threads is the hallmark of trolling. Trolls often behave in this manner only to incite other people - many a times they can back off at the last minute under the garb of everything being a joke.</p>	<p>The best way to deal with a troll is to simply ignore them. The main purpose behind a troll's actions is to get a reaction from the person they are harassing, the more you engage the more you play into their game. If it gets too out of hand then address the troll in a rational manner. Remember that they aren't there to debate you in earnest, they're just trying to stir the pot - and they win if you lose composure.</p>



PROTECTING DEVICES FROM MALWARE & HACKERS

Malware/Spyware

Spyware is a very real problem for journalists working in Pakistan. If your system is infected and compromised by spyware, your story and your safety isn't the only thing you are going to be compromising - your sources can also find themselves in danger.

Like you, Maria too at one point believed that her system may have spyware. She was working on an extremely sensitive story and saw her laptop camera light go on. Since she hadn't turned her webcam on, she didn't know what else could have done this. A little research showed her what a spyware is and what it can do.

Malicious software created with the specific aim of keeping tabs on what someone is doing with their laptop (or even mobile) is known as spyware. The information is stolen from your computer and then sent to another through your own device's internet connection.

Spyware also come in all shapes and sizes. Some are extensive and will take screen captures of everything you're doing, record what you're talking about while you're using your system, and even send information on your location across to the person spying on you. Others have limited features but can do an equal amount of big damage i.e. a keylogger can record every single stroke you make on your laptop - so your passwords, your story, any contact information - anything that you've typed on your system - can be compromised. And the person spying on you doesn't have to move an inch or gain physical access to your device. For a journalist this can mean anything from losing their entire digital security to



having their pictures or videos for a story compromised.

So where does it come from? A spyware can be put into your system through a malicious web page. It can also be installed onto your system by someone you trust. and it can be downloaded by you by mistake. Pakistan's government has been rumored to have invested in FinFisher software, whose main aim is to spy on people.

How to get ride of Spyware?

- ✓ Have a look at DETEKT at <https://resistsurveillance.org/> This is a tool created especially for people like Maria and you. Journalists and human rights defenders use it regularly to fight out spyware.
- ✓ Check out SpyBot while you're at it. It can get rid of most malware and can root out problems.
- ✓ Don't let any webpage automatically download files into your system.
- ✓ Check the programs and features for items that you don't remember installing. The add or remove programs part of your laptop/PC will offer you a list of programs installed - get rid of anything you don't recognize (but run a quick search online to make sure you aren't deleting a file that came with the system).
- ✓ Reinstall your OS or go back to factory settings (but practice caution because this will delete all of your data and files along with the spyware).



The Signs: Do you have Spyware?



Do you see new toolbars, favourites or other links that you never added to your browser?



Is your homepage or search program acting a little funny? Things change too fast and least when you expect them to?



Do you try to visit a website only to have your browser reroute you elsewhere.



Pop-up ads keep showing up even though your system isn't connected to the internet?



Your computer has become super slow but you aren't running that many programs. Spyware will weigh your system down because it uses a lot of memory.



Your webcam lights up but you aren't using any program that is using it.



HOW TO PROTECT SENSITIVE COMPUTER FILES

A digital hack isn't the only way to lose your data. When Maria was on assignment in a remote village in Khyber Pakhtunkhwa, she decided to take her camera along and get some photography done. However, when she came back she realized her laptop was gone.

As media transforms, our methods of reporting and covering issues is also changing and becoming more digital. Grabbing your laptop and taking it along for the long haul isn't an alien concept and many journalists do it all the time.

Like Maria, you must be thinking the likelihood of you being able to simply skip taking your laptop or mobile phone along is very slim. You aren't wrong. And you really shouldn't limit your reporting by leaving your tools at home.

Three things can happen to your laptop or phone. You can either lose them, they can get stolen, or they can be confiscated while you're in the field. In all the cases, being prepared is better than finding out your entire scoop is gone.

What to do?

Maria has over the years developed a couple of steps she can take to keep sensitive information safe on her system.

- Make sure all your digital devices such as laptops or mobiles, or even tablets, are protected with passwords.
- Some devices will let you limit the number of password attempts that can be made on your device. If someone tries to enter the wrong password, in a bid to guess what it is, one too many times, your device can lock itself and/or erase all data inside it.



- Encryption is your friend, use it liberally. Your hard drives can be encrypted i.e. the data of a file can be scrambled or turned into a code that no one else will be able to crack. You can use the BitLocker Drive Encryption if you're on Windows, and turn on FileVault if you're using Mac.
- A secret partition that contains all your sensitive files sounds a little like mission impossible, but is often imperative for a journalist to do. You can use Veracrypt for both Windows and Apple systems.
- Invest in a decent cloud service and make sure you backup your files very regularly. There are many options that you can use for free including OneDrive, Google Drive, and DropBox.
- If you are super particular about your data then you can also keep it on a removable storage device.
- Encrypting your files before you upload them somewhere is generally a good practice so that they don't get compromised if your online account does.

THINGS TO REMEMBER

- ✓ Cloud storage is only as good as your internet connection. If you're in the field and covering a story from a place where the internet connection is particularly poor then you won't be backing up those files anytime soon.
- ✓ If someone can steal or confiscate your laptop, they can also take your removable storage. So stay vigilant and never keep all your eggs in the same basket, and all your storage in the same bag.
- ✓ While the more popular cloud storage options exist and there are options that take privacy to another level. Both Spideroak and Wuala can offer better security and privacy, which is essential for journalists.



DESTROYING SENSITIVE INFORMATION EFFECTIVELY

As a journalist you will work on many articles and/or reports that include audio, video or text evidence that you have quoted anonymously or with the identity of the source removed. This is run-of-the-mill for many journalists. But that information remains sensitive no matter how much time goes by.

So what can you do? Make sure you destroy sensitive information in a manner that it cannot be recovered by someone else.

GONE FOREVER

Sending a file into the trash bin and then emptying the trash bin gets rid of the file, right?

Not really.

There's another step, one that no journalist thinks about and most don't even know about. On your hard drive is a place where files end up after they've been booted out of the trash bin. While you may think they cannot be recovered, someone with the right kind of tools can actually find them later. Instead what you need to do is wipe your file clean.

- ✓ For Windows users, the Get Eraser tool is a good option, while Apple users can use Get Permanent Eraser
- ✓ Use a data wiping tool so that you overwrite the file data multiple times and ensure that there is no way to retrieve it
- ✓ Use the 'Secure Empty Trash' option to delete the data



Remote Wipes

It's one thing to actually delete files when your device is sitting in your hand, and it's another when it's been stolen or taken from you. A journalist should always know how to go James Bond on their device and disable it from somewhere else. Think of it as reverse hacking, though you'll be the one breaking into your own system.

- Start by installing an appropriate software to remote wipe your system
- Set it up and make sure all your sensitive files are plugged into the system for deleting
- Make sure you don't use this feature out of a sheer state of panic and end up losing your data
- Backing up your data can help you avoid any possible catastrophe as you get rid of your data

However, be cautioned that this method generally works when your system is connected to the internet. So if the person who's taken your laptop does not ever connect to a friendly Wi-Fi, you won't be able to wipe your data.



HOW TO RECOVER FROM DATA LOSS

So you know how to protect your sensitive data and files, and you know how to get rid of them too. But what about the time where you lose them but never intended to?

Maria felt pretty good about all the ways she was keeping her data safe but didn't think what she herself could do to recover it if it ever escaped her grasp.

How does one lose data anyway? Like this:

- Your hard drive can crash leaving you in the lurch
- Your USB or SD card got wiped accidentally (or on purpose by someone else)
- A virus ravaged your system and now some files are missing
- Power went up and down and your device couldn't take it anymore and gave up on you
- You didn't remove the hard drive or USB safely from the computer (oh yes, this can actually be a problem)
- Formatting your storage device without realizing the consequences

People, and journalists in particular, find new and improved ways to lose their data all the time so this is nothing to worry about. And while not all of your data is recoverable all the time, it never hurts to try and it never hurts if you are only able to recover it in parts.



So what do you do?

- Find an appropriate software and get cracking. Recover My Files (www.recovermyfiles.com) is a good option to get things out of the Recycle Bin after you've been affected by a virus or formatted your drive. This has both a free and paid version.
- Recuva is a freeware with a cool name that you can use to recover files lost from your camera, MP3 player, and your Windows laptop.
- Recovery isn't the only thing you should worry about. Create a backup policy for yourself to follow. You will need to make a conscious effort to figure out where your important data and files are located and where they are being backed up.
- A good habit is to use OneDrive or a similar service to store all your important files.



USING TOR & VIRTUAL PRIVATE NETWORKS

You might have heard of Tor. Maria found it after realizing the ‘Incognito’ on her chrome wasn’t protection enough for the kind of things she was trying to do. Once she started hearing the stories about government agencies tracking journalists she began wondering how safe it really was to assume ‘it’ll be okay’.

Tor offered her the anonymity she needed. What it does is route all the web traffic through its own network i.e. The Onion Router. The Router is basically a network of computers known as Tor nodes. These are encrypted connections and once you start a session on Tor you will be connected to one.

The websites that you visit will not be able to see where you are visiting from or who you are. Unless you use a service that knows who you are (for eg: sign into Facebook or Gmail) you remain super anonymous.

And because there are no free lunches in the world there is also a problem with Tor: it’s slower than your average browser. The simple reason for this is that because it is routing all your traffic through other places it takes time for your communication with the browser to get through, and come back.

Tor functions with an HTTPS-everywhere setting. Extensions that are harmful are already blacklisted on it and avoided.

Tor is also useful for journalists because it helps them access websites that are locally blocked and cannot be bypassed. It’s a huge pain to have to look up a proxy anytime you want to access websites and pages that the government may have taken down. Facebook itself has been victim to this form of censorship many a



time. And up until very recently, YouTube itself needed proxies to run.

THINGS TO REMEMBER

- Don't try to run websites or perform tasks online that require superior speed because that's one area Tor suffers in
- Don't open documents like pdfs or word files on Tor. These formats have aspects that connect to the internet independently and can reveal your actual IP address
- Don't forget to update your Tor



USING VPNs & PROXIES

Pakistan ranks 139 on the Press Freedom Index 2017 making it one of the worst countries for press freedom in the world. Maria, like many other journalists, has had to work with limited online access to some content. While things are nowhere near as bad as they are in China, the occasional official statements about a ban on Facebook or Whatsapp worry her immensely.

But she's found that there are ways to get around censored content. Tor is an excellent tool to do so while remaining safe, but Tor isn't the only fish in this sea.

Anyone who didn't know what a proxy was found out when YouTube was banned. They are used widely amongst Pakistanis, and especially journalists. As a reporter or editor you do not have the option of quitting internet - your very job is to find things people don't want to let anyone see. Services such as Bitmask and Psyphon can help you bypass censorship.

The real tool here, however, is a VPN connection. A Virtual Private Network (VPN) is something like Tor but they function a little differently. Tor uses multiple connections to keep you safe, while a VPN will use only one.

Most VPNs will cost some money. Riseup.net offers a free service for those who are looking, however, there are also partially free services that can be used. A plugin like the Zenmate, Blue Box or Stealthy, for example, can help you switch to another connection within your browser. This will not affect other activity on things that are using internet, like Skype for example (or another browser).



THINGS TO KEEP IN MIND

- Your privacy and security are only as good as your VPN provider. If your provider is tracking what you're doing then there's nothing you can do about it so pick one carefully
- Free services are generally slow and will not offer good speeds.
- Browser extension have been known to get hacked in the past, so don't rely on them too much



SECURE CHATS & PGP

The need for keeping our conversations with our sources safe has never been greater. Maria knows that some articles are sensitive, and some sources - if compromised - would land into hot water for talking to her. Often people ranging from NGO workers to government employees give her information anonymously. If their details were to somehow leak or be exposed, she would be directly responsible for the aftermath.

So how does she ensure that her chats and email are safe? Well, she didn't need to go the long yard to keep her interactions safe, and you don't either. There are many free and fairly simple tools that you can use to keep your privacy super private. PGP or Pretty Good Privacy is a decent first step to take when you're doing this.

What is PGP?

It's simply encrypted technology that blankets your emails with a layer of protection, making it harder for it to be cracked open, stolen or compromised in anyway. This layer of protection is added in before you shoot out your email and then unwrapped when the receiver wants to see it.

PGP isn't just about keeping yourself safe. It can also open up option to sources that want to reach out to you for a potential story but are afraid to do so.

How does it work?

- You generate a PGP key or keypair
- You then create a nifty little passphrase - which basically means a super strong password
- Make your public key public (yes, really). The public key is



typically put up on a website or “keyserver” which acts as an email directory where CPC keys can be found for email addresses.

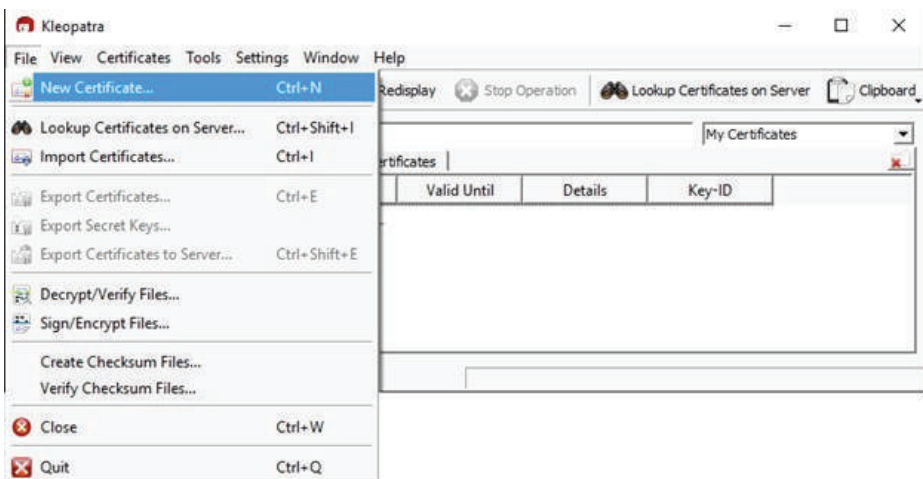
→ And finally, one more secret key that you've created will be needed to decrypt messages you receive.

Sounds a little complicated? Well let's take it step by step. There are a couple of apps that you will need to get things done. Start by heading over to <https://www.gpg4win.org/>. This is where you will find and install the Kleopatra App. GPG basically offers secure email and encryption options for Windows users.

So what does Kleopatra do?

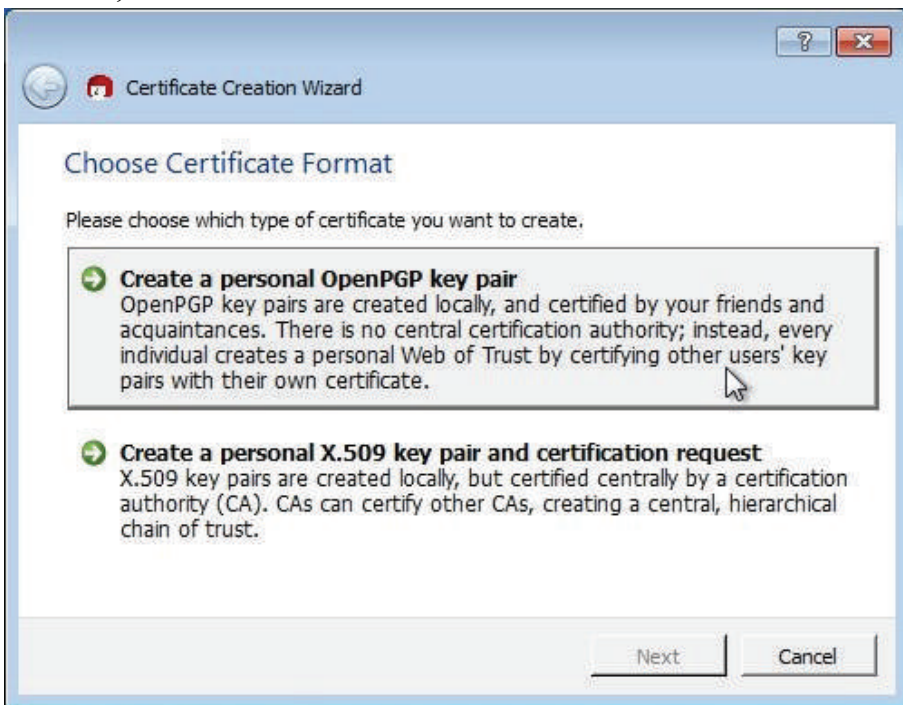
This is basically a certificate manager and a universal crypto GUI. It will be taking care of the keys you create for the emails that you need to send and receive.

Once installed, open the app and create a new certificate. Only add emails that you will be using encryption on. You will be clicking on the File menu and picking the first option to do this, like this:

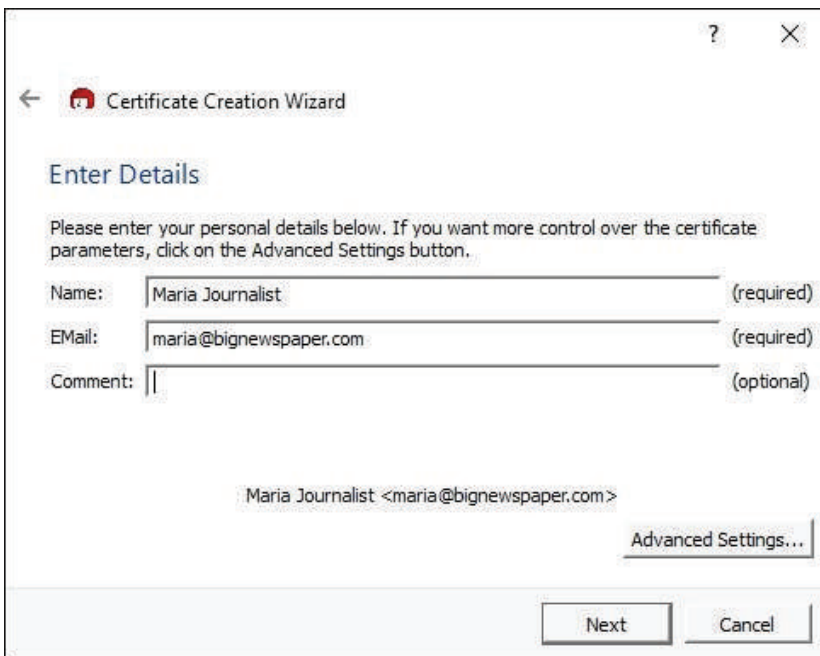




Your next step will include letting the Wizard do most of the dirty work. Select the 'Create a personal OpenPGP key pair' option and click next, like this:

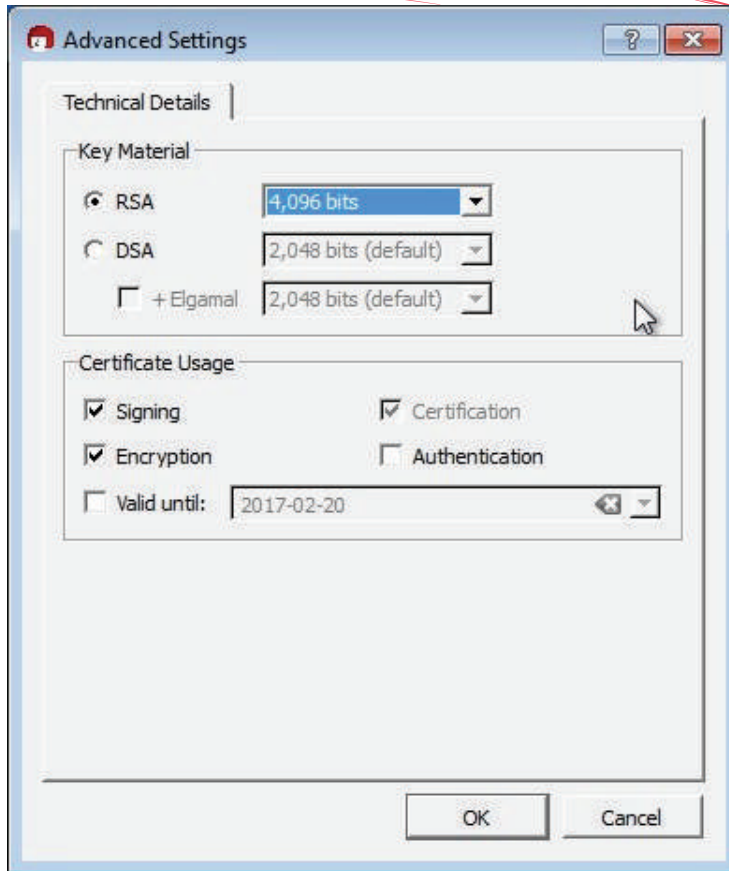


When you move to the next screen you can fill out all the details that are needed i.e. your name, the email you want to use, and a comment if you've got something to say.



The image shows a Windows-style dialog box titled "Certificate Creation Wizard". The window has a title bar with a question mark and a close button (X). Inside the window, there is a back arrow and the title "Certificate Creation Wizard". Below this, the section "Enter Details" is displayed. A message reads: "Please enter your personal details below. If you want more control over the certificate parameters, click on the Advanced Settings button." There are three input fields: "Name:" with the text "Maria Journalist" and "(required)" to its right; "EMail:" with the text "maria@bignewspaper.com" and "(required)" to its right; and "Comment:" with an empty field and "(optional)" to its right. Below the fields, the text "Maria Journalist <maria@bignewspaper.com >" is shown. To the right of this text is a button labeled "Advanced Settings...". At the bottom of the dialog box are two buttons: "Next" and "Cancel".

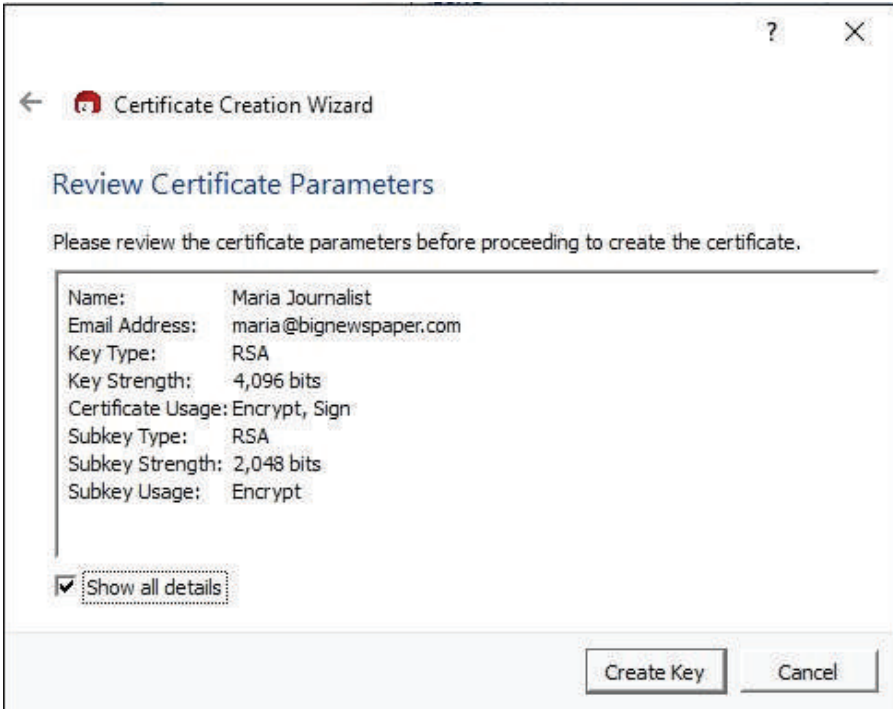
Before you hit next, make sure you open up the advanced settings and go here:



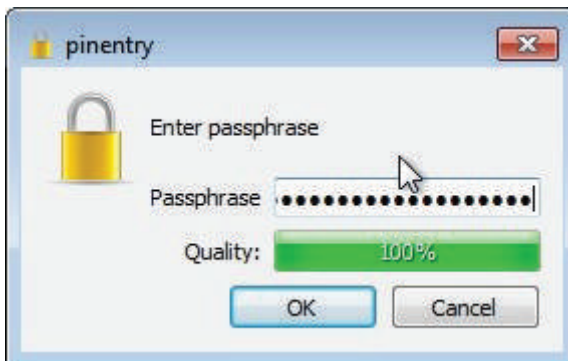
This is where you can take a better look at your key strength and then change things around. Under the 'Key Material' section, you should make sure that RSA is checked. Also click on the drop down menu and increase the strength to 4096 bits or 4mbs. Once you're done, simply click OK.



The next step will look something like this:

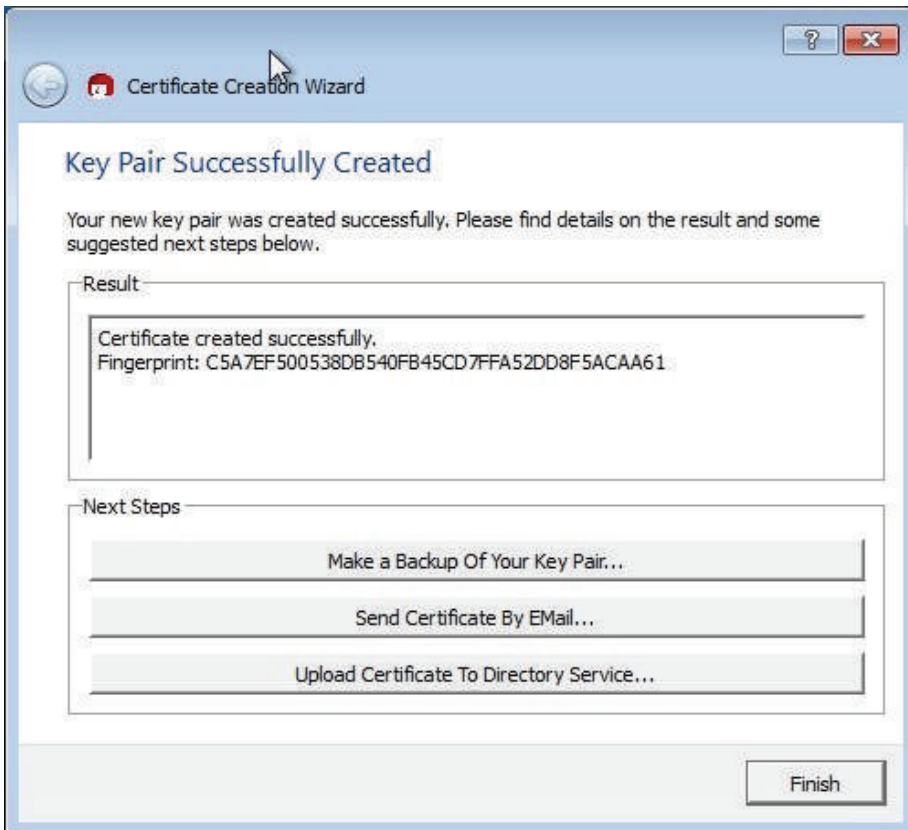


Now hit create key and wait for the magic to happen. At this point you will be asked to create a passphrase. Make sure that you spend some time doing this. Your passphrase is the magic set of letters that allows you to communicate securely. It needs to be long, it needs to be strong, and it needs to be written down somewhere because if you lose it, you will lose your encrypted emails:





Now wait for a bit for your key to be created and then go ahead and do a little happy dance before you click 'Finish'.



What you have now are a few more options. You should make a backup, send the certificate by email and upload to a directory service. But do you know what you're going to do with the key pair you just created? This is where you need to understand what public and private keys are.



Public keys are typically used to encrypt the data that you are sending, and personal keys are used to decrypt the data you are receiving. Private keys are to be guarded with your life, some people keep them in a shoebox.

Once you are done creating your key, you can right click on 'Export Certificates'. Save the file wherever you like and check it out by opening it in notepad. The whole lot of gibberish you see is both your public and private key:

```
C5A7EF500538DB540FB45CD7FFA52DD8F5ACAA61.asc - Notepad
File Edit Format View Help
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQINBFTnmk0BEAC122jBGmJHwmoadyuon0Cl1t1I1oUR47kuqx1t43PUjxcAnYBQR
ygpBM6LA7TsCswuF6n2bLV2D1LPHhG0D92LRqBoorQh9x0YAegFufuy/bqd88Hao
w2/VeItAiuuewsB7+HNrG1lWCxamJULJ3+kFogglG+neoeb/CLchV9C8zbVLDX
a3KFIZsZAN1St/35tG3YsqSn10I1J0wDunh8yQ7nf3EEzbHDrWNRX1ZjYnPrbSj+
DCo1kpy7n0H1iPahYvwj10w327rY1x1vc/TI4DYmuQ9LhIGB4y01QIL2Fn+cyjrc
v2wjknLD2edkHmj2T65ZmkpTApwUa17lDSAFzbrFA1cncnb1jzhq0RFRI7XEutV
IBB2I3ved3v+BbuQP/ybR1b5XfzcgBHyM6cXLSctVCGEuyBatw1Pfus56NmkbhN
gTXRASZKPyxhI8AHb14l046TtPFUSUHQNvN7EQ9i72TD0xTbd9mJiL2nLxcSewbv
OC7ZJDVvoFPd6Mu2KmoboLOE4lFwCBU2VjofB7PEo9+/9coeQ3UEX/kbd3LO3P8I
7OspmPoL/dh9xRy2jn19PAz1NPhk1TVAmDGEAm6jcnIFUFZgCOEPfBkIXIIEKfH
f5l7eqwTrGEfxyyz+Kg5ouTj115+fSN7G4jGF13SobttwR1t0lba5U96wARAQAB
tDNNTFBfaXNfbXl1f1BTRUMgKgrIG5vdcBqaykgPGlhbWVjdHvhbGx5bGVAZmJp
Lmdvdj6JAjkeEwECACMFAlTnmk0CGw8HCwkIBWMCARVYCAIJCgsEFGIDAQIEAQIX
gAAKCRD/p53Y9ayqYe1pEACCr8FotpGoqbmTDXDipeon6zugw+5h6qmack2Vwjd2
4yIhS8ZThYZ7vPi0kDY7ewi4Fw0kRgrM9D+bTEwBkeA9Z5hsGf50CBuONRDRzrG/
kFoE7ZwiZTM0ASdlLYrcqRM94GBowkg5BF3IH+63dLg4jMLY05uwgVhpBMCAed8
wMmOEGZG8nden6Y0Pqyo8+8op3hshjUw5Y00woQPCYCM9Ei6GwNjFkXukB4ZDS7
9Q1rQPr4wM5FBGzyfKJewg8+A5HSw2ncsTbcYUawuMw1AtQR9XEmKowb9/5fSkX
sfhotFImyDEP9wy8KzGxdxtH9LFOP1Jm5TXPlvnyppqwxz1oATx5on+pwmsGexjmm
9tkPRMGoafDcmJnjC0uYgAGUKigdTh0oTXB1TKDND4yiwd1yh1hvjt13IZjrZEHc
neQ8iMz0pdQXIVfASdbsMIHxzEM2VTLfq2mIhQFP6vjile9+vacsHh97a2thMOBd
b1KnPounbf9I8+zJoqfKcfEqEU2oRPMTbSvgt0tzyBnHF19/F01aek6JelJAzrw
a92MxXBHJQBTvPDTg4ZCSGtTJUixD4x5MSgoU+E80Q3f4jh+dPOXlYpw5ajTrEY0
5LgkrFM/cA/xmsA1bdcvkhNcmSyzwE+wZqwh/5dwanZpu9neOBpbj+y6UwB5k6l
dg==
=wtkL
-----END PGP PUBLIC KEY BLOCK-----
```



If you want to access your private key then simply click on 'Export Secret Keys'. Select where you want to save the file and check the 'ASCII Armor' option that you are given and click OK. And voila, you now have your private key.

In order for you to communicate with someone through PGP, it is important to note that you cannot send encrypted emails to someone that is not using encrypted emails as well. For journalists around the world, this can prove tricky at times because if a source cannot use the services that can protect them, they can only go so far. What many journalists do is simply use PGP and leave it as an option for their sources. Many others use it within their organizations to keep data and information safe from prying eyes - this is exceedingly relevant for journalists that are operating in Pakistan.

THINGS TO REMEMBER

- You can add an expiration date based on the level of threat you face and your threat management practices.
- You can add users by adding another account. However, this is not an advised practice. Generally people are better off making separate keys. The reason for not using the same key twice is simple: it's the same as using the same password for two accounts: if you lose one you lose both.



So now that you have the Kleopatra app and your key pair figured out, you need an app to actually send emails through.

Head over to

<https://www.mozilla.org/en-US/thunderbird/>

Download Thunderbird.

This is an email application that looks a lot like outlook. It's not too hard to set up and has plenty of features so you can use multiple accounts on it.

Once you've installed Thunderbird go to

Tools > Account settings

Click on 'Account Actions

Hit the 'Add Mail Account' button

Enter your email account details

Press continue

Typically Thunderbird will be able to pick up the most suitable settings for your account. When this does not work go into Manual Configuration and set up your account.

Once you have configured your email

Download Enigmail from here:

<https://www.enigmail.net/index.php/en/download>

You should go into

Tools>Addons in the upper right corner

Click on 'Install Add-on From File'

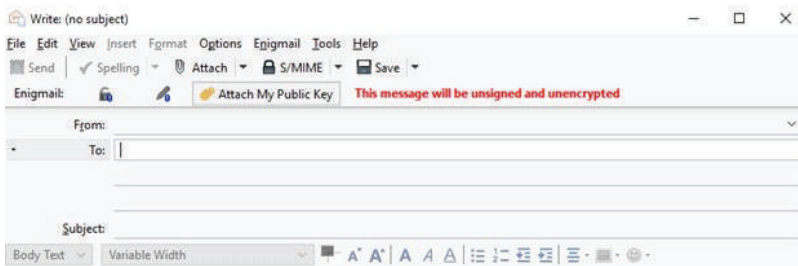
Alternatively you can also just install it and then drag and drop it into the setup wizard that will do most of the work you don't have to. Enigmail basically helps you access and manage authentication and encryption feature. It helps Thunderbird send and receive



digitally signed and/or encrypted messages. You can use the keys you created with Kleopatra or make new ones with Enigmail (however, it's not recommended to make a new one key within Enigmail because it does not offer the options that Kleopatra does).

The keys you created and saved before can be dragged and dropped into Enigmail key management (or Kleopatra itself for that matter).

Lets test things out now. Hit the 'Write' button at the top of your menu bar and you should get this screen:



Attach your Public Key to the email before sending it to whoever it is meant for. Remember not to encrypt this email because it will not be possible for people to open and save your key unless they can access your email. The next email you send can be encrypted.

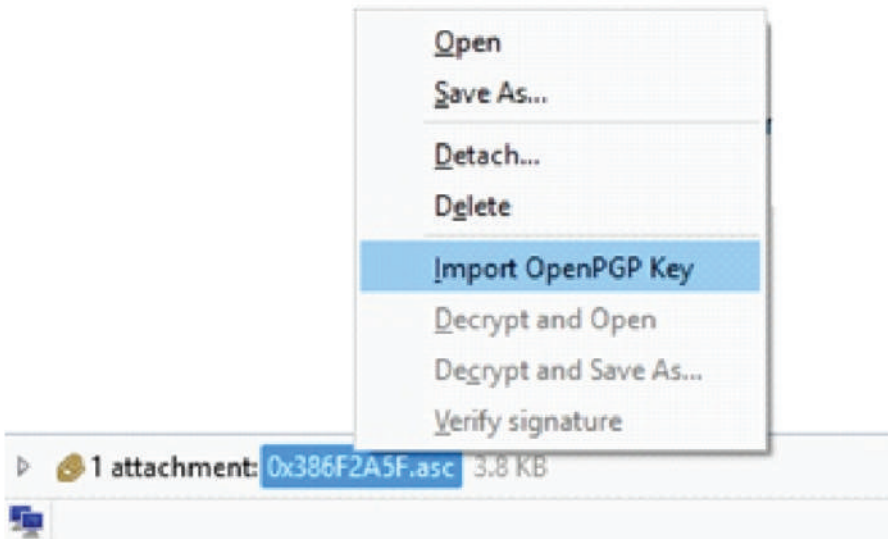
Also note that you don't need to send your public key to the same person every time. Make sure that you also have your contacts public key as well. When someone sends you their key it will be in the form of an attachment. The file will have a .asc extension. You can import it like this:



Subject **Re: key**

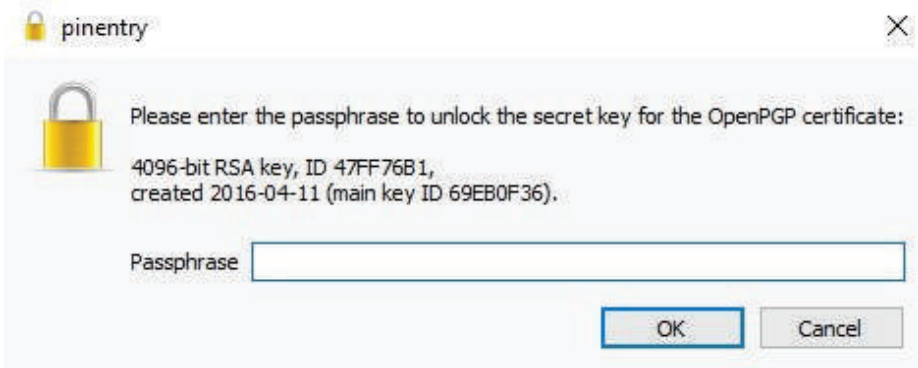
To Me☆

Find attached my key

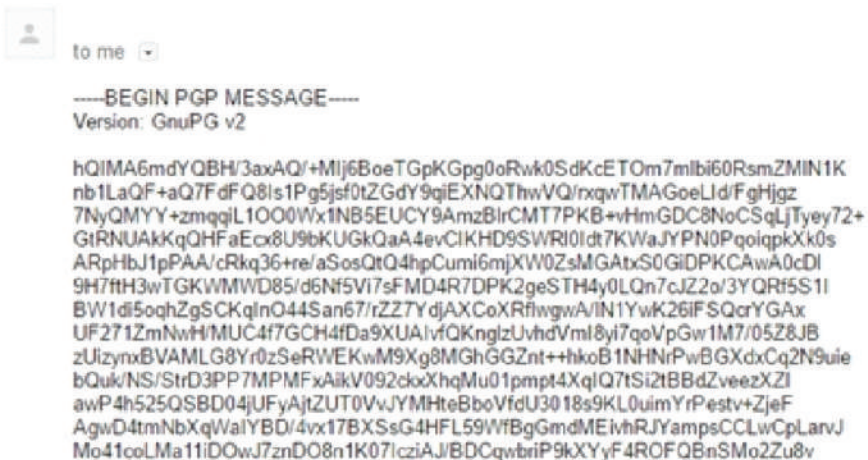


Simply right click and select the “Import OpenPGP Key” option and let the software do the rest.

You can now send and receive encrypted emails. Whenever you send an encrypted email you will not have to make any different moves or any extra effort except clicking on the encryption button. However, when you receive an encrypted email you will be prompted for your passphrase in order to access the content, like this:



Unless you have your passphrase, you are not going to be getting into this email. Encrypted emails also show up as gibberish in other inboxes. For instance, if you are a regular Gmail user and go to your inbox to open an encrypted email, you will see the following:



Like riding a bicycle, this will only seem a little tricky the first few times you do it. Once you get used to it, things will become easier for you - and a whole lot safer too.



DON'T FORGET

- No tool is 100% effective and can only guarantee an added layer of protection at best.
- Keep your codes and passwords safe and far away from anyone's eye - even people you trust.
- PGP is only as good and secure as the person you're interacting with. Sending a PGP email to someone that has bad digital hygiene can and will compromise you too.



OTR - PROTECTING YOUR CONVERSATIONS

Once you've figured out how to encrypt your emails, the likelihood is that like Maria, you too, are realizing that the email is just the tip of the iceberg. You have entire conversations with sources online, discuss potential stories with your editors, and chat away with fellow reporters about your angle. If at any step you compromise yourself and your sources, the missed deadline will be the least of your problems.

So how do you talk the talk without letting the digital walls in on your conversation? Look into safe chats. For Maria, “off the record” has meant something completely different throughout her career. And like her, you too can enjoy the irony of OTR or OFF THE RECORD options that allow you to hold conversations that are encrypted, but will most likely be entirely on the record. Some journalists have pointed out that the utility of OTR is even more significant than that of PGP.

Typically an OTR will use end-to-end encryption so the government, your ISP and even the messaging service itself won't be able to see what's inside your messages.

Maria found that her sources were more comfortable giving her scoops when they knew their conversation was OTR.

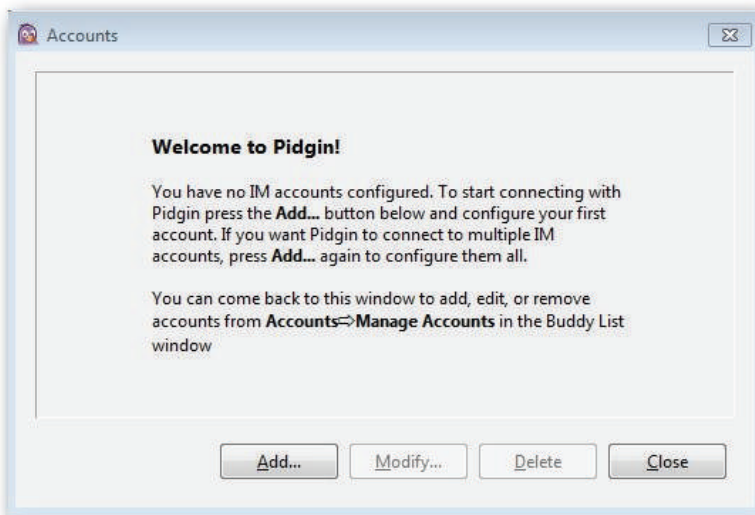
What are your options? Pidgin and Adium are both OTRs that get the job done. OTR can be used with AIM, Google Talk, ICQ, Yahoo! Messenger, MSN Messenger, or any other protocol Pidgin or Adium support.

OTR also provides authentication, so you have some guarantee you're talking to the actual person. Even if their account were compromised and someone else attempted to talk to you with their screen name, you'd see an error because the encryption information wouldn't match.

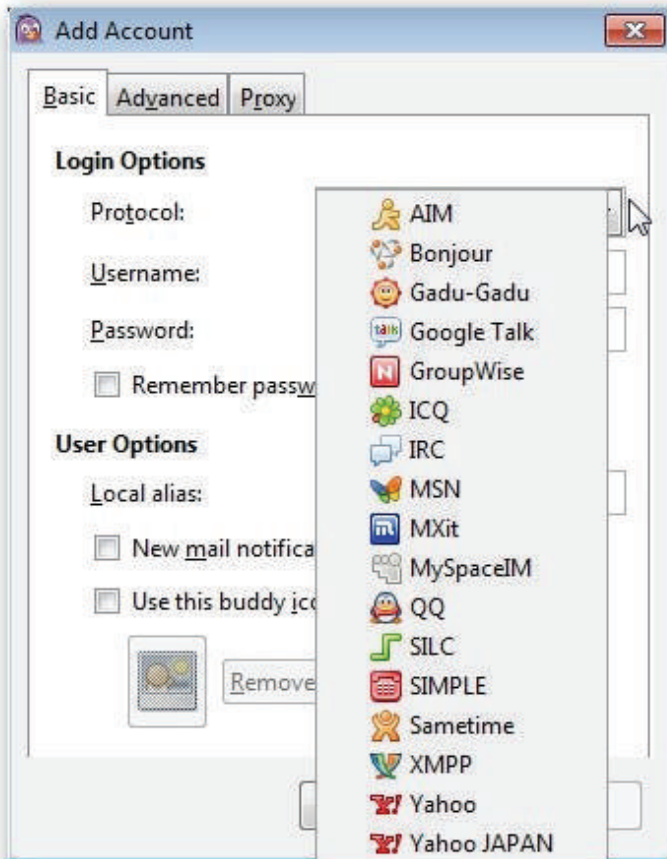


The Pidgin instant messenger has an OTR plug-in. You can add in a wide range of accounts into this messenger as well from Google Talk to Yahoo chat (but who uses that anymore?).

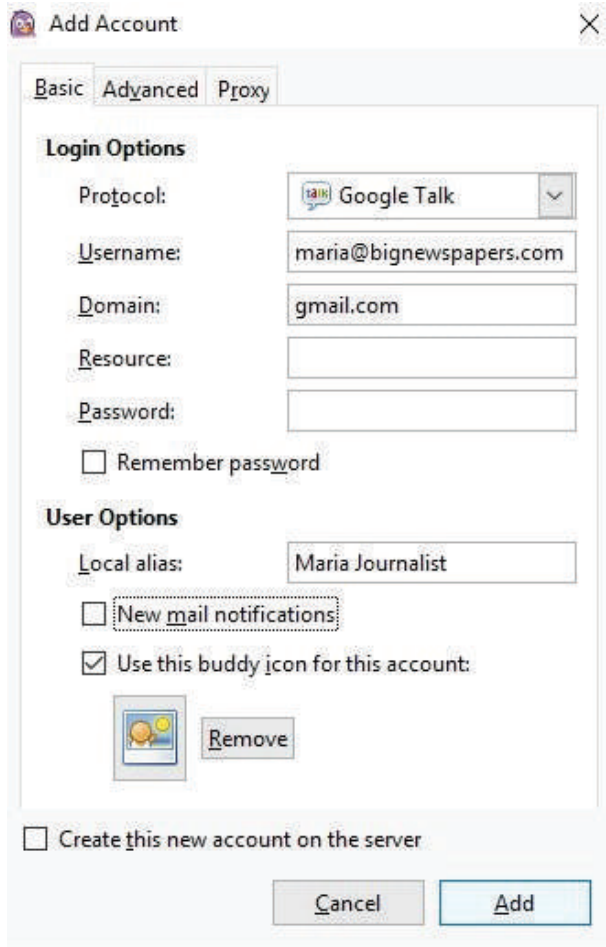
Head over to <http://www.pidgin.im/about/> and install the messenger. Once you have added it you can click on the 'Add' button to add a chat network like this:



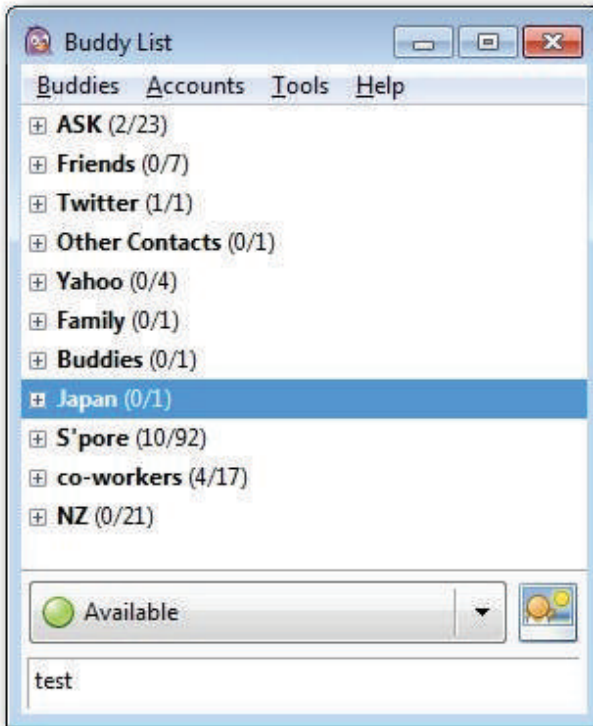
You can choose from a wide list of chat services in the 'Protocol' drop down menu, like this:



This is where you will pick the service you want, add in your username and password. Also pick your local alias (your username) and buddy icon (your picture) for the account and click add, like this:

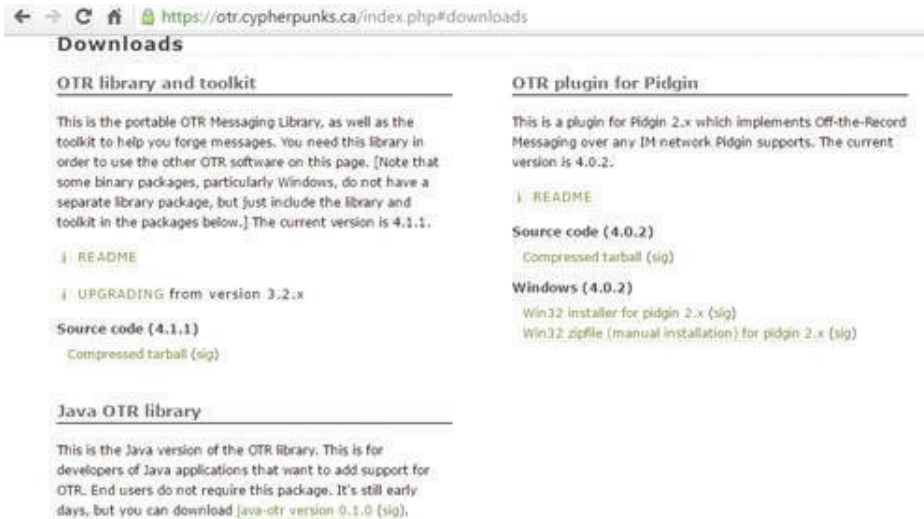


It's honestly that simple to add an account into Pidgin. You can add as many accounts as you like into it and it should not be a problem. The Accounts tab will have a 'Manage Accounts' section that can be easily used to see what accounts you have added. You can add, modify, and delete the accounts through this section as well. All of your chat groups from the different accounts should show up like this:

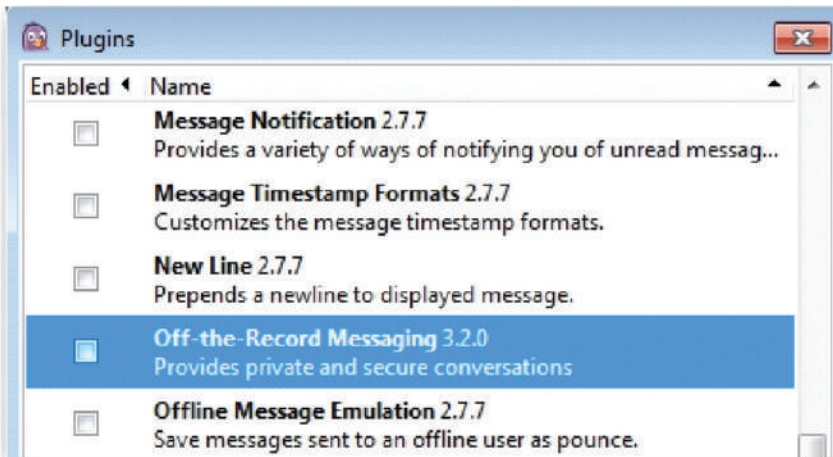


The next thing you need to do is encrypt your conversations through Pidgin. Up till now all the steps tell you how to install a chat software and nothing else. Without encryption, it's just another app that doesn't offer you all too much - apart from allowing you to bring all your communication to the same platform.

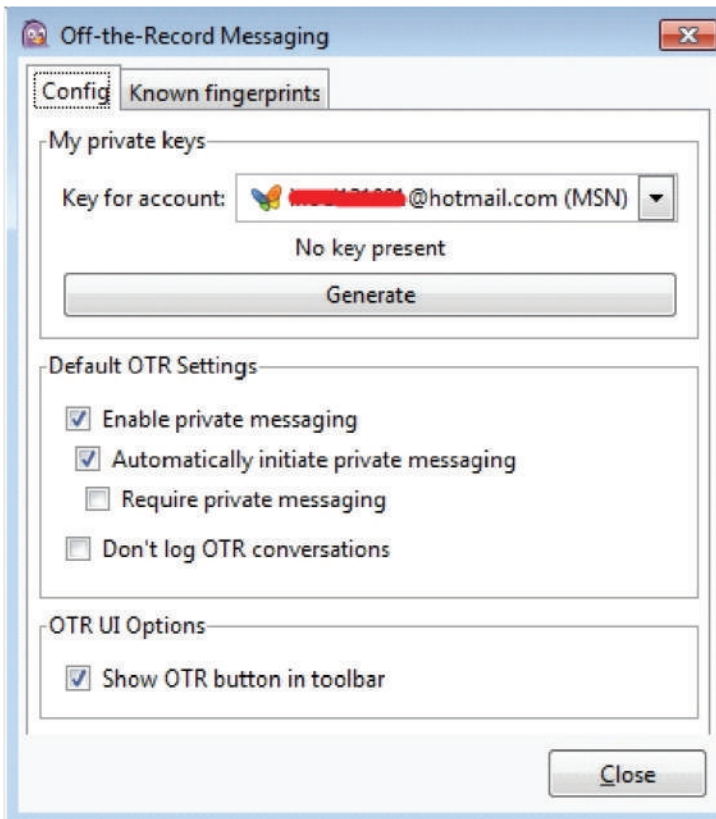
Start by heading over to <http://jabberzac.org/register/> and register yourself. Once you have done this go to <https://otr.cypherpunks.ca/> and open up the downloads section. Download Windows (4.0.2), which is going to be your OTR plugin for Pidgin like this:



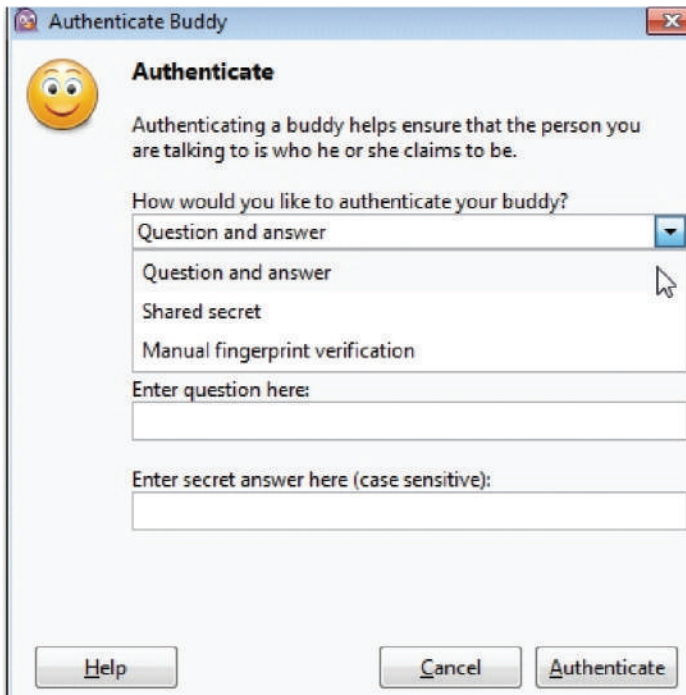
Once you have installed it simply enable it from the Plugin screen.



Your OTR button will show up in your chat screen and can be used to initiate a secure chat channel. Just like PGP, you will be using Keys to get things done. Generate a key so that it can be used to encrypt your discussions.



Remember that the plugin will function on four levels of privacy. What this means is that you first start by enabling encryption by clicking on the OTR button. The conversation remains 'unverified' until and unless the person at the other end is verified. You can easily verify your buddy by picking the 'Authenticate Buddy' option from the OTR menu as you chat. You can verify them through a question and answer, a shared secret or their OTR fingerprint like this:



With the question and answer, your buddy will have to correctly answer the question you have asked. You will follow a similar step for a shared secret. Once your buddy's answer goes through, your chat will become 'Private', otherwise the failed authentication is reported and that is the end of that. There is a high likelihood that your buddy has either mistyped or is an imposter, in case they are not able to provide the right information.

The last method is the fingerprint. Go to 'Authenticate Connection' from your OTR button and then click on 'Advanced', like this:



Call up the person you are talking to and ask them to read their fingerprint out to you to verify that it truly does belong to them. These are steps that need to be followed for every person you decide to add to your OTR list.

It seems a little tricky but once you are done setting it all up, it will be worth the time you have spent on it!



USING ANDROID & iPHONE SAFELY

The go to choice when it comes to smart phones is either an iPhone or an Android set. Journalists are now using their phones as an extension of themselves. They are literally their sidekicks in reporting. But with a great and powerful smartphone comes a bigger set of problem.

But Maria didn't think of this as a bigger problem because she thought as long as she has her phone in her hand, things are in her control and so is her data. Little did she know that as easy as it is for someone to get into her email accounts, it's equally possible for someone to sneak into her phone without her even knowing, and all of it while she has her phone in her hand. Once a a hacker with malicious intentions gets into her phone remotely, not only her data but also her sources can get into trouble as well.

HERE'S WHAT YOU NEED TO KEEP IN MIND:

- ✓ Androids will generally save a lot of your data and fork it over to Google - the same company that has a secret deal with the government that led to the return of YouTube. Your account history page can show you what you've been up to. Information captured on iPhones is sent in a similar fashion to Apple.
- ✓ You need to keep a check on the amount of data your mobile transmits, be it an Android or iPhone. Turn off your internet and Wi-Fi when it's not in use.



- ✓ See that your social media updates aren't ratting you out. Information that you do not want public should not be shared publicly. Be wary and be careful.
- ✓ While generally updating is the number one go-to rule when it comes to digital hygiene; in the case of journalists and their Androids and iPhones this isn't exactly true. Turn off auto-updates because when your phone does that, it links to the nearest tower and reveals your location. You can update your device at your own convenience later.
- ✓ Make sure the information going out of your phone is being sent anonymously. Get Orbot for your Android [this is basically Tor for your cell phone].
- ✓ Don't jailbreak your iPhone - nothing good will come out of it. You may gain access to some free apps, but you also more or less open up your phone to more security flaws and risks.
- ✓ Similarly, don't root your Android device. Once you do this, you basically open up your phone to a whole host of new viruses, threats and malware.
- ✓ Avoid third party downloads at all costs.
- ✓ Download anti-virus and anti-malware apps.
- ✓ Make sure that your phone has a remote wipe/lock app installed in case it is stolen or lost.
- ✓ Try not to save all of your passwords into your phone. While



the auto complete feature helps save a little bit of time and seems convenient, it can land you in hot waters.

- ✓ Keep a close check on your app permissions, be it on Android or iPhone. While iPhones are the more secure of the two, there is always a chance you could be inviting trouble. Avoid apps that ask for permissions that they shouldn't need. For instance, there is no reason for a camera app to ask for access to your text messages.
- ✓ Use a VPN to protect your internet activity.
- ✓ Don't let your phone automatically connect to a Wi-Fi or internet connection. Always manually pick the connection.
- ✓ Your lock screen notifications could be the end of you. Get rid of them to ensure that sensitive data does not reveal itself through a notification.
- ✓ Your Apple ID and iCloud should both be running on two factor authentication, as should Google and it's connected services.
- ✓ While Siri and Google Assistant are a nifty tools, you should disable it on lock screen. They have a lot of information about you so allowing someone else to gain access to it through them would be a bad idea and a big mistake.
- ✓ Keep the location of your phone off at all times. GPS is a great tool for tracking you down physically. You wouldn't want any unwanted person to know your location and creep you out while you're having lunch with friends, or on an assignment.



HOW TO STAY SAFE WHEN USING MOBILE PHONE

As journalists, you most likely use your mobile devices to not only develop and capture content but also share it, edit it and more. From finding news, to recording it and disseminating it - this is one tool that has a lot of tricks up its sleeve. Maria realized that having a smart phone was giving her an edge at work - but having a smart phone was also a significant security risk.

Maria came up with a check list of things that she always needed to be conscious of when it came to her phone.

CHECKLIST

- 1 What kind of information was running through it? What calls, emails, texts, etc was she sending and receiving? Was this information sensitive? If yes, then how sensitive?*
- 2 What kind of sources were stored on her phone? Were her contacts being copied to another source like a backup on Google or Hotmail? If stolen or hacked, would her phone compromise her sources?*
- 3 How often were location services turned on through her cell phone? How easy was she making it for someone to track her?*
- 4 What pictures, videos or text had she produced through the phone which could compromise her story or source if stolen?*



These are questions everyone needs to ask themselves. Maria realized that some steps needed to be taken to keep her mobile safe, and her mobile usage safer. So what did she do?

- *She began removing EXIF data before uploading any videos or images. EXIF data can reveal a whole host of information including the location of the image, the time it was taken, the phone used to take the picture, the device used to store the picture and more. While at first, the task seemed tedious and long, once Maria made a habit of it things got easier.*
- *For more important calls and sources Maria began keeping a journal with names and numbers instead of storing them on her phone. That's not all, she went a step further and bought herself an old feature phone. The legendary 3310 isn't just unbreakable, it also has no modern functions that can allow someone to record calls made to or from it - Maria loves her feature phone, you should get one too.*
- *In times where using an old mobile was not possible, Maria invested her efforts into a VOIP application like Signal or WhatsApp which are also end-to-end encrypted, so that the likelihood of her calls being tracked was lower.*
- *Instead of automatically storing sent and received messages, Maria made sure that none of her texts were saved on her device - be it a smart phone or a feature mobile.*
- *Maria additionally ensured that all her communication was conducted through OTR, when the source was one that would be easily compromised. Apps such as Signal also offered Maria a good solution.*



→ *When not in use, Maria ensured that her internet connection was disabled. If it's not turned on, it cannot transmit data to or from her phone. While this one is a step not many would be willing to take, it has the benefit of reducing the likelihood of one getting tracked through their GPS by a whole lot.*

THINGS TO REMEMBER

No measure you take to secure your mobile phone usage is 100 percent foolproof. Threats are ever evolving, strategies that work today may not work next year. Keep your eyes and ears open and be smart about your digital hygiene

Encryption doesn't just exist for laptops and computers, it's also pretty useful on your phone - use it.

Be wary of the kind of data your service provider can collect off of your phone.

Third party apps are bad for your phone - they collect a lot of information and can compromise your data.

Try turning your phone off every once in a while. In dangerous situations or critical stories, it's better to leave the phone behind than to find out later that it helped act as a bug against you.



Disclaimer

The information in this guidebook was verified correct at the time of writing, but technology and interfaces change rapidly and some of the material may not remain current over time.

www.digitalrightsfoundation.pk

 /DigitalRightsFoundation

 @DigitalRightsPK