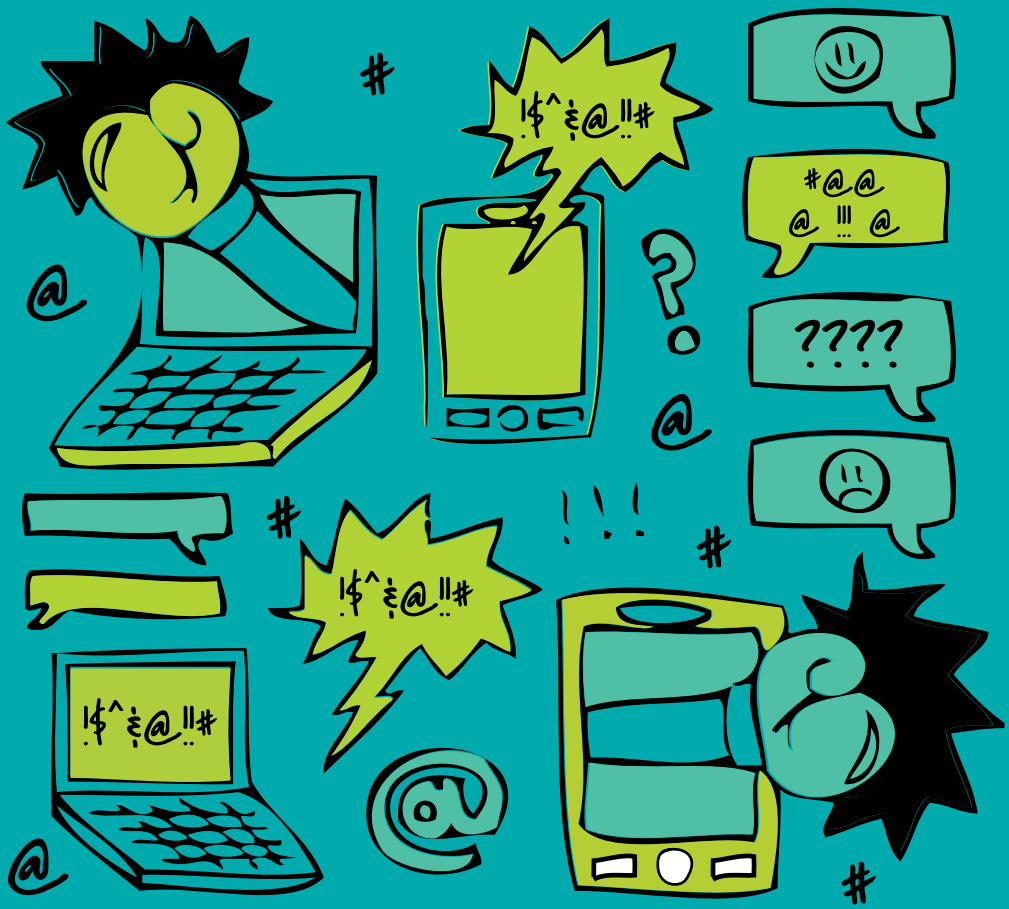



# Online Violence

## Prevention, Reporting & Remedy

A 'Bytes for All' Publication | November 2013, v1.0

## Disclaimer

The contents of this guide are a compilation of generally recommended practices for protection from online violence, mechanisms available for reporting violence and means of obtaining remedy. This guide is by no means meant as an exhaustive or authoritative list of measures or recommendations on the subject. As with technology and its uses, such measures continue to evolve at a rapid pace.

---

**Research by** Shoaib Taimur

## Introduction

The emergence of social media networks has made it easier for us to be connected with others. Unfortunately it brings with it many security and privacy related issues. According to a study conducted and published by Computer Magazine (June 2013), the privacy management of 16 popular social networking sites, including Facebook and Twitter, is "seriously deficient." Social media networks were designed to make our lives easier but unfortunately, like all free services, they come with a hidden price. Social networks are increasingly being used as a tool for identity theft, stalking, harassment, invasion of privacy, and other forms of violence. Sexual predators are also using these tools to their advantage. With increased penetration of the Internet and mobile telephony, Pakistan is no different in this respect, with the role of these technologies being used for purposes of crime and violence expanding at an alarming rate. This booklet aims to define different forms of online violence, provide tips on how to help prevent cyber violence and crime, and reporting as a measure to obtain remedy.

## What is cyber bullying, stalking and harassment?

### Cyber bullying

The definition of cyber bullying is bullying which takes place using electronic technology. It encompasses equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

### Cyber stalking or harassment

The Oxford Dictionary defines cyber stalking as the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. Harassment can range from false



accusations, defamation, threats, identify theft or damage to equipment. Cyber stalking also includes exploitation of minors, be it sexual or otherwise.

Online violence, including bullying and harassment, can be severely traumatizing and humiliating for the victims and their families, with sometimes serious consequences. Therefore it is important for everyone to be aware of preventive as well as remedial measures for protection online.

## Protecting yourself online

This section aims to provide tips on maintaining digital security and privacy, as these are considered essential in helping with online safety. Following these practices can help prevent violations of privacy, blackmail, harassment and bullying etc.

• Make sure that all your devices such as smart phones, tablets, laptops and computers have a password. This will make it more difficult for anyone to physically access your data in the event of theft or if a device is left unattended at your workplace, home or elsewhere.

• Whether at work or anywhere else, make sure to lock your screen while away to restrict access to information. Do not leave smartphones unattended, even inside a bag.

• Do not use easy to guess passwords like dates of birth, names of your loved ones, words in a dictionary etc., as these are easily hacked by those intent on theft, stalking etc. Do not use the same password everywhere and do not write it down anywhere. Use a good browser extension like LastPass to manage your passwords.

• Do not share your private plans on social networks as it makes it easy for stalkers to track you down.

• In the event that someone has hacked into your system, disconnect and get your computer cleaned. Meanwhile use your phone to talk to people

instead of messaging or sharing information with your friends and family.

• In the event that you need the assistance of a third party to disinfect your laptop/PC/Mac, you should make sure there is no personal information which can be accessed. Either supervise it or make sure that all private information is backed up on an external drive or on the Cloud. Ideally, private information should be maintained in encrypted form.

• Always use an anti-virus/firewall/anti-spyware solution to prevent your system from getting infected with malicious software designed to either hack into your email/ social media accounts, to access or destroy information on your computer or in your online accounts, or to spy on you.

• Limit what you put online as criminals/cyber stalkers use the web to hunt for victims. Sometimes information can be leaked from popular websites which are hacked from time to time. One best practice is to change your password frequently.

• Do not share personal pictures on your public feed on social media such as Facebook or Twitter. If you are an Instagram user, restrict your feed to those you approve/ trust.

• Cyber stalkers usually tend to be people you know or have interacted with. A useful practice against hacking is to use a separate email account for social media accounts and to keep it confidential. This should make hacking into your other accounts harder. Educate yourself on two-step verification system used by service providers, and secure all your accounts. Make sure you have all the backup information stored in a secure place, in case you lose your phone. The two-step verification system is available for Google, Twitter, Facebook and Outlook email accounts.

• There is no need to enter your real date of birth and birthplace while filling out forms on a website (except for visas/ other official work requiring authentic bio-data).



• Profile pictures used for social media are best if neither very clear, nor give your location away.

• Gender neutral pseudonyms may prove useful in avoiding cyber-stalkers.

• Do not share any passwords or intimate photos with a partner, as it can lead to ugly situations in the event of a breakup. There have been cases where male partners have circulated pictures, contents of conversations or emails etc. of their ex-girlfriends online as revenge.

• Remain up to date with Facebook and other social media privacy settings as default settings are changed frequently. Keep testing to check from different browsers, whether your information can be accessed by people outside your circle or not.

• Sometimes it helps to search for your name on the Internet to find out if there is any information on you on the Internet. If you find your pictures or personal information on websites you have not authorized, you can request the webmaster or the service provider to remove them.

• One strategy to avoid stalkers is to block them. If you use Facebook, block the user from contacting you. Twitter also has a block option which prevents harassment. In case of harassment via the telephone, use a call/text blocking option. Further, your telephone service provider can help block unwanted calls/texts when requested. Serious cybercrimes/threats should be reported to the local police unit or the cybercrime unit of the Federal Investigation Agency (see section ‘Reporting Offline’ below). Document any violations, threats or harassment (see section ‘Documenting the Evidence’ below).

• Do not engage with strangers who persistently request you to add them on Facebook. If they do not pay heed, do not hesitate to block or report them to Facebook (see section ‘Reporting online – Facebook’ below) for further action against them.

• In the event that an interaction with a cyber-stalker gets hostile, block or

stop all interaction.

• If you own your own web domain, make sure that your private information is not accessible to whomever does a WHOIS search on you. It only costs a few dollars to hide that information from cyber-stalkers.

• Inform your family if you are facing any problems. It is important to keep them in the loop lest there are any issues later.

• One way to avoid cyber-stalkers is to use applications such as True Caller (available for Android and iOS). Such applications crowd source user information from the phones of other users. These applications can help identify the subscribers of unfamiliar callers/numbers.

• Do not feed the troll/bully. Ignoring and blocking are frequently successful, especially at the early stages of harassment.

• In order to guard your privacy, maintain your digital footprint. Everything you post online combines to make your digital footprint (see section 'What is s digital footprint' below).

### Underage users

Extra care must be exercised for the protection of underage users of social media. They can easily endanger themselves and their families, and must be supervised in their use of social media. Minors are often targeted by pedophiles.

- o Remain aware that Facebook has a minimum age limit of 13 for its users. Parental guidance and supervision is key in keeping children safe in their use of social media.

- o Supervise online activity of minors as predators/pedophiles use the Internet and social media to target them.

- o Educate children under your care on the risks or dangers inherent to the use of the Internet. Make sure they do not provide any personal information such as real names, addresses, their school name or phone numbers to strangers.



## Reporting online violence

In the unfortunate event of becoming a victim of online violence, reporting the crime is important for obtaining remedy. This section aims to provide tips on how to report, online as well as offline. It is always helpful to collect as much evidence as possible, and sometimes may prove crucial in obtaining redress. The evidence should be backed up in a safe and secure place. This section provides tips on evidence gathering and reporting.

### Documenting the evidence

Online search engines such as Google may prove helpful in tracking down cyber stalkers. If you ever received email or text messages from someone, there is a chance you can track them down via a search. A simple search of the email address or phone number may help track down real identities along with detailed information.
At times cyber harassers do not hide their identity while harassing others. In such cases, you can report them to the organization they work for, with the help of supporting evidence (screenshots etc). There is always a chance that the person's organization is listed on their Facebook or Twitter profile. If not, a search on the Internet in identifying them may prove helpful.

Much evidence can be documented using screenshots of online violence. Obtain an application to take screenshots or learn how to use your keyboard to do the same. Make copies of the evidence and keep backups on the Cloud as well as on a backup drive.

### Taking screenshots - on a PC

With the content you want to take a screenshot of displayed on your screen:

• Click the Print Screen key (frequently, this key is located in the upper right-hand corner of the keyboard) - depending on your keyboard, you

may have to press the CTRL and the Print Screen keys at the same time.

• Save the image as an image file using a software such as Microsoft Paint:

o open Microsoft Paint

o select Start > All Programs > Accessories > Paint

o click anywhere on the white part of the screen

o select Paste from the Edit menu at the top of your screen

o select File > Save As

o select JPG from the Save As menu in the pop-up box

o type in a filename for your image

o choose a location on your hard drive to save to

o click Save

### Taking screenshots - on a Mac

With the content you want to take a screenshot of displayed on your screen:

• simultaneously hold down the three keys: Command, Shift, and 4

• press the spacebar - a camera icon will appear

• tap the touchpad to take the picture - it should appear on your desktop as a file named 'Picture 1'

### Documenting e-mail as evidence

• Take a screenshot of the email.

• Copy the email including headers (all the #'s and symbols that you see at either the top or bottom of the screen in the email). This contains the subject, name and e-mail address. This information can pinpoint where the e-mail was sent from. All email programs have options to show headers.

• Copy and paste email into a Word document and SAVE.

• Print a copy of the email and put it in a safe location.

### Saving evidence from a website

• Take screenshots of the Homepage of the website; this is the main page that shows the name of the website.

• Take screen shots of all pages and information that may constitute relevant evidence.

• If dates and times are listed as to when the website was updated last, include these in the screenshots as well.

• Save and copy the website's address.

• Print off the front page of the website and all the pages relevant as evidence.

• Go to the hosting company's website. For example, for www.blogger.com/xyz the hosting company's website would be www.blogger.com.

• Contact the company and report the website.

(Reference: http://www.girlsguidetoendbullying.org/pdf/Saving_Evidence.pdf)

## Reporting online - Facebook

### Fake or dummy accounts

To report a fake or dummy account on Facebook:

• go to the account's Timeline

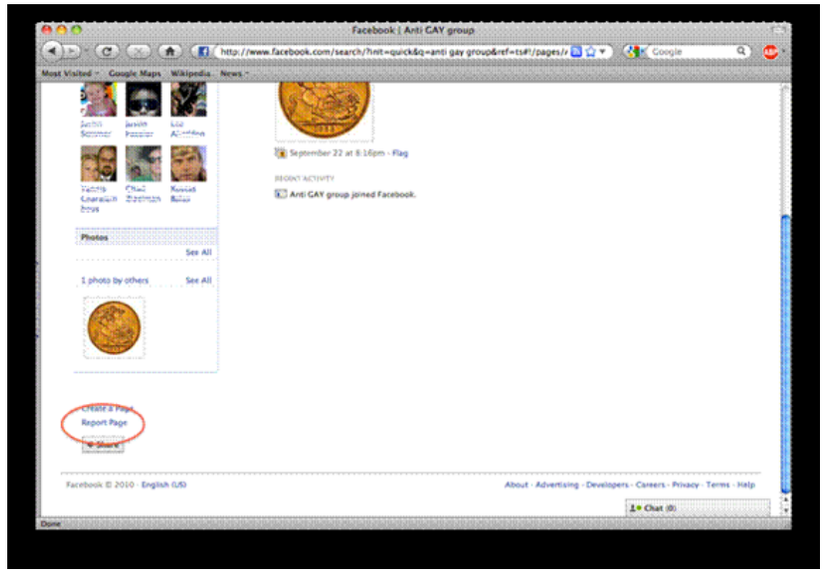
• click on the gear and select the Report/Block option

• report following the Facebook notes on how to file a report

Facebook specifies it will take action either if someone is impersonating you or a friend, or if a user is using your photographs and passing them off as his/her own, and/or if the person is not real.

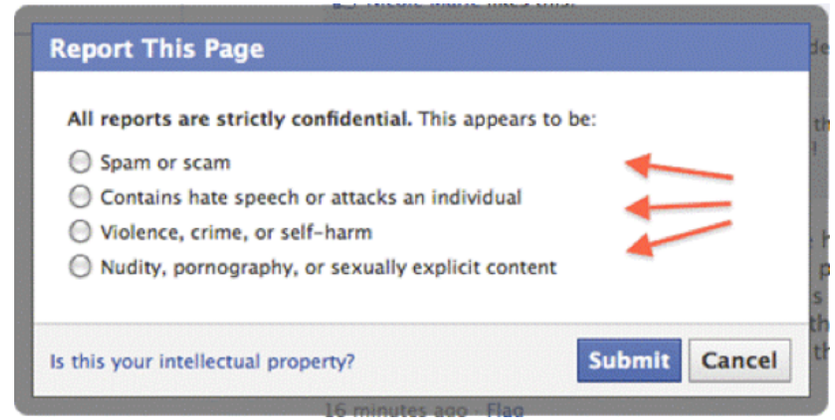
## Groups or pages

1. Click on the "Report Page" link in the left sidebar.



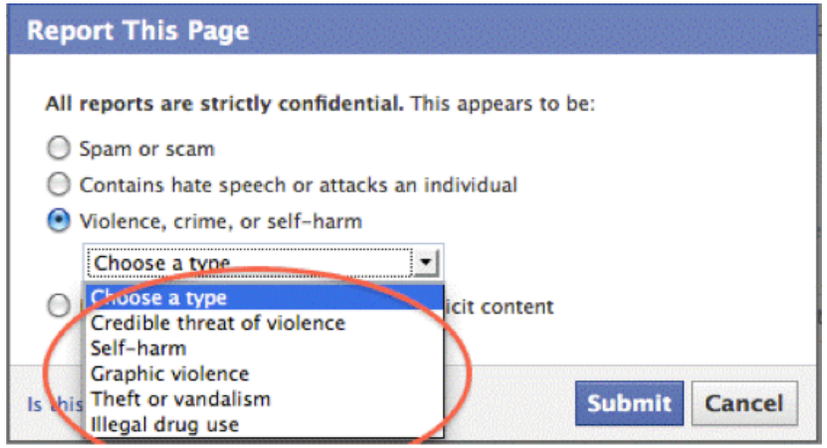

2. Select the appropriate option of the pop up window that appears, taking care to mark the correct category.






3. You will get an additional dropdown menu for the "Contains hate speech or attacks an individual".

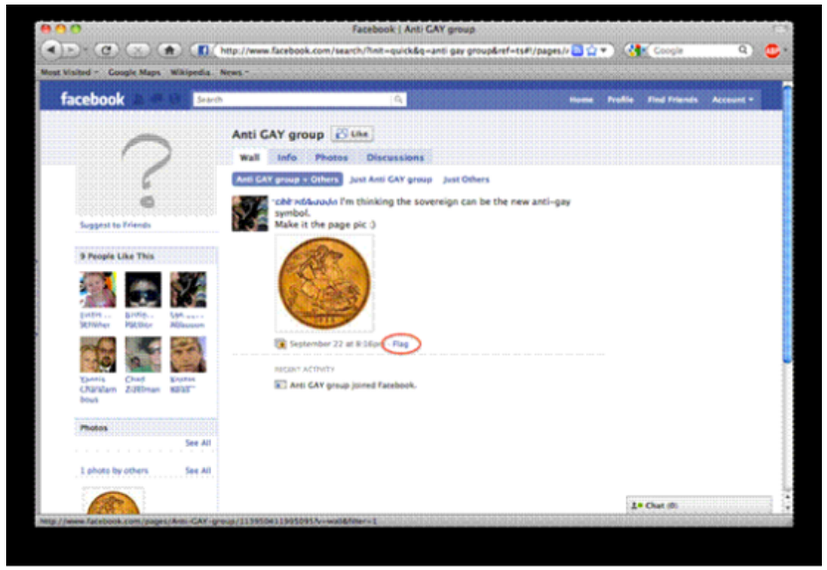

4. Selecting "Violence, crime, or self-harm" will give you another dropdown menu from which you can select the category of violence.




(Pictures and guide are courtesy of www.stopcyberbullying.org)

## Individual posts

1. Flag the offensive post by clicking on the 'Flag' link.



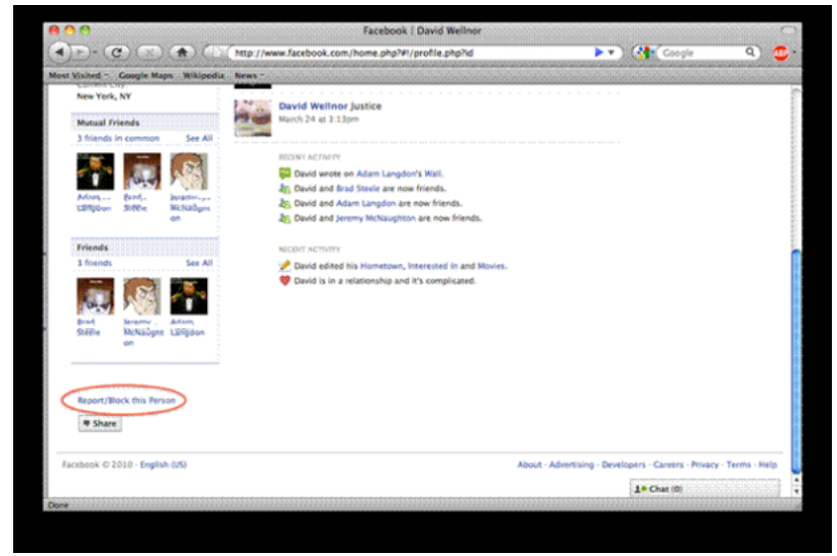

2. Once you flag the post, you are given the option of undoing it or reporting it as abusive.



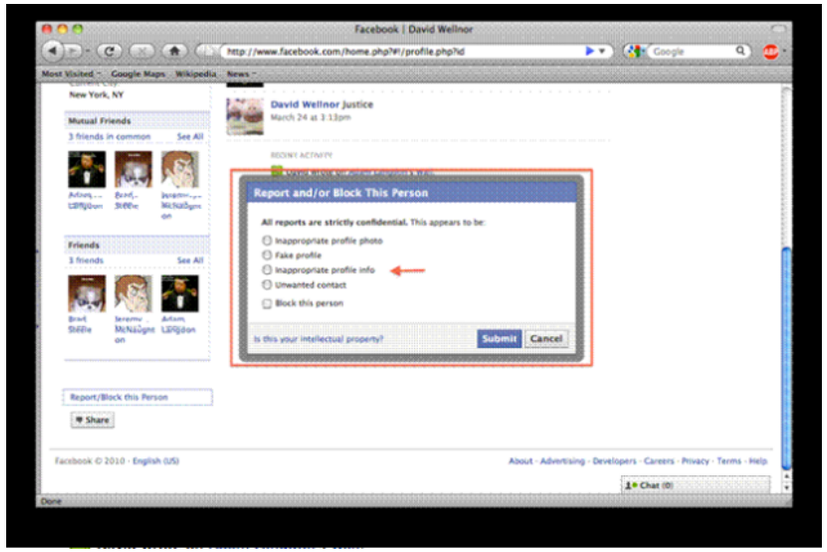

## A user

Be aware that Facebook retains all user information. This means Facebook can access such information even after it has been deleted by the user. This includes users' IP addresses and all private communication. Thus, in case of being harassed or stalked, it is useful to report the user to Facebook.

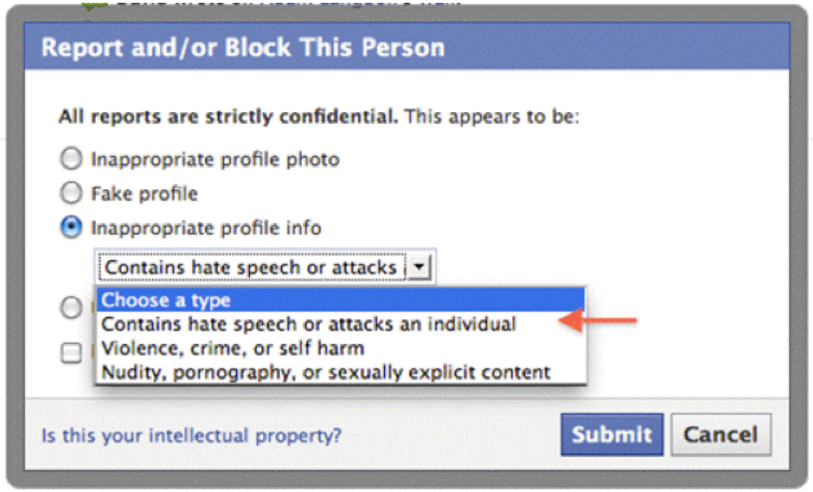
1. Select the "Report/Block this Person" to begin the process of blocking.



2. Select the option for “Inappropriate profile Info”.




3. The “Inappropriate profile info” option has a dropdown menu to choose various options from.

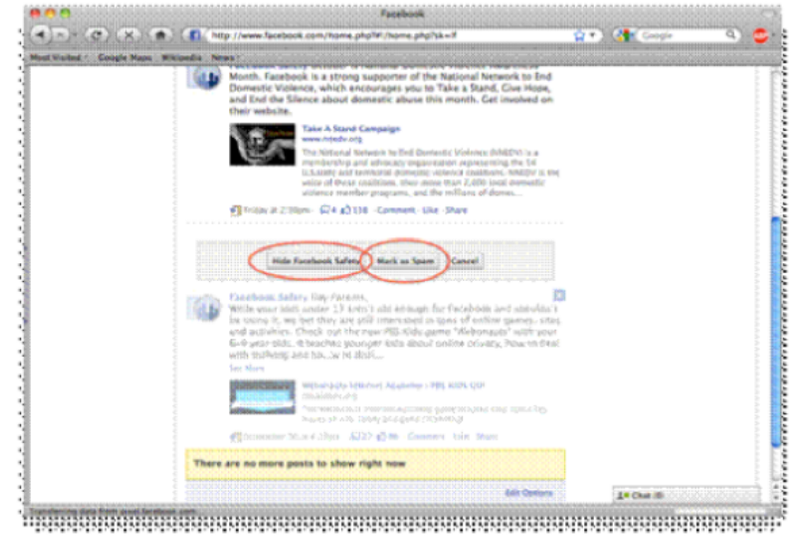





## Content on your feed

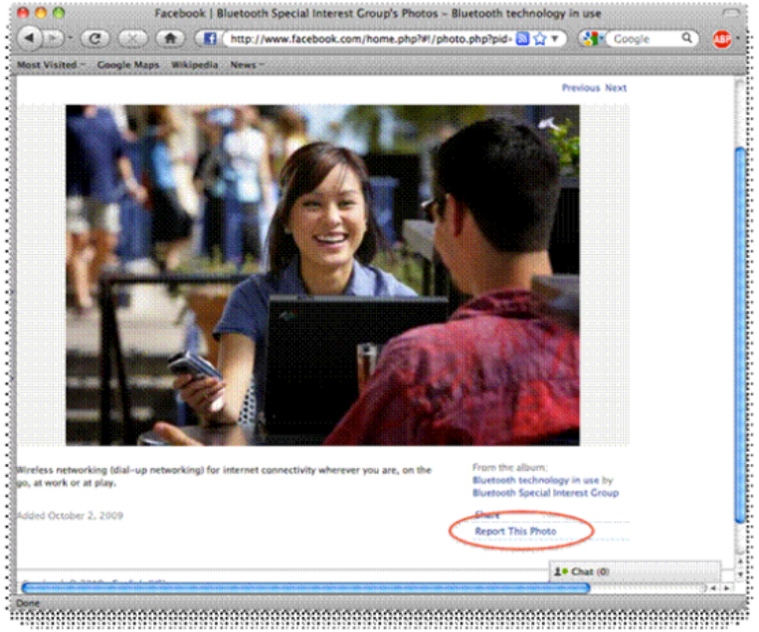
1. If you are tired of spam or offensive posts on your feed, you can flag it as spam. Click on the “x” as circled.


2. You will be presented with options whether you want to mark it as spam or hide it.

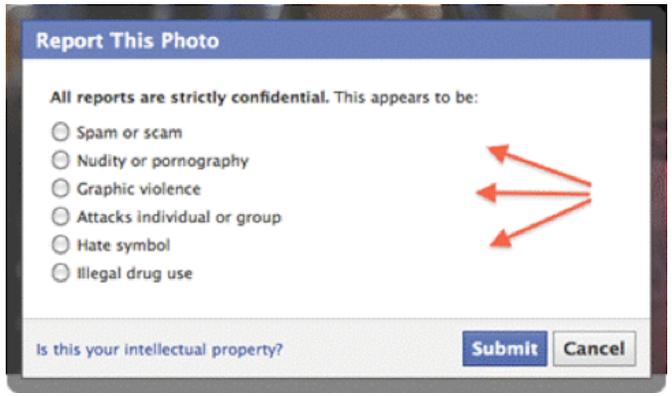


## Photographs

1. Click on the "Report This Photo" link in the lower right portion of the screen.




2. Select the reason you want to report the photograph. In this instance, you can choose the "Attacks individual or group" option.

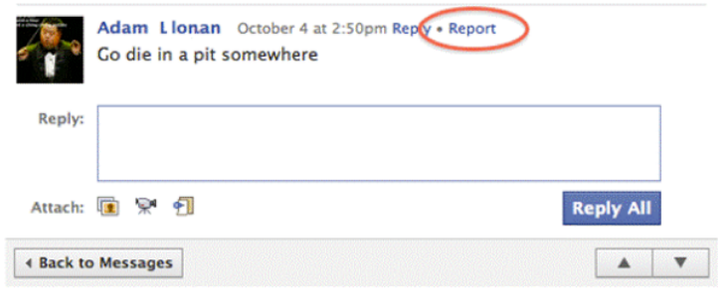





3. This option allows you to categorize the type of attack.


## Messages

1. To report an offensive message, click on "Report".




2. Select the reason you want to report the message. You are also given the option of blocking the user.


## Reporting online - Twitter

### A user

Go to: https://support.twitter.com/forms/abusiveuser. You will be asked to explain why you are reporting a user and to respond to follow-up questions about the actions you are reporting.

### An imposter

Twitter has a strict policy against impersonation. If someone is impersonating you or a friend on twitter, you can take action by filling out a form as explained below. Twitter will not take action if the user shares a common name and has no affiliation with any other person. Only if an account is misleading or deceptive will it be treated as an impersonation by Twitter. Similarly, a parody account has immunity as long as it is made clear that it does not represent a real person. Thus, a parody account should be titled with a prefix such as "not", "fake" or "fan" for clarity.
To report a Twitter account for impersonation, fill out the form at https://support.twitter.com/forms/impersonation.

• Choose the option "I am being impersonated" > "A user is pretending to be me or someone I know" > "I am the person being impersonated".

• The next option asks the user if they have submitted a report before



along with faxing a copy of the government issued ID card. If not, details of the issue at hand can be provided.

• Provide the user name of the person impersonating you.

• Select one of the following options:

  o using my full name, common name or alias
  o using my photo or image
  o posting as if they were me
  o using my phone number or address

In addition, you may specify whether you want the username suspended or whether you want to take control of the account.

## Reporting online – Instagram

### Impersonation

To report impersonation on Instagram, you will be required to provide:

• two clear photographs of government issued ID (ID card / passport front page).

• your name, email address and username of the offending account and as much evidence as possible (in the shape of comments and image URLs).

## Reporting offline

### The Federal Investigation Agency

If you are the victim of a cybercrime, do not hesitate to report it to police in your local area, or the cybercrime wing of the Federal Investigation Agency (FIA). To report a cybercrime to the FIA:

• write down the application in English or Urdu, giving detail of the problem along with any evidence

• include you're your name, national identity card (CNIC) number, postal

address and contact numbers

• email or fax to the FIA National Response Center for Cyber Crimes (NR3C) at 051-9266435 or email it to helpdesk@nr3c.gov.pk

Expected response time for emails is 24 hours, whilst that for faxes and postal mail is seven days. You will be given a tracking number for your complaint. This tracking number may be used to check status updates for your complaint.

Further contact details are as follows:

Project Director
National Response Center for Cyber Crimes
FIA Head Quarter
G-9/4, Islamabad
Tel: # 051-9106380
Fax: # 051-9106383

OR

Help Desk
National Response Center for Cyber Crimes
FIA Head Quarter
G-9/4, Islamabad
Tel: # 051-9106384
Cell: # 0336-6006060
Fax: # 051-9106383
Email: helpdesk@nr3c.gov.pk

### Pakistan Telecommunications Authority (PTA)

Unwanted phone calls and text messages/ spam texts may be reported to the PTA at the number 9000. The details required are:

• text to be reported, copied verbatim

• the mobile phone number of the source (number of the sender)



• your own name and CNIC number
• any other details

## What is a digital footprint

A digital footprint is the aggregate of the trails or traces of your activity or interactions in electronic environments. On the Internet, your digital footprint includes all content you have ever uploaded, a record of the websites you visited, the searches you conducted, information you accessed and record of what you downloaded etc. Examples would include your Facebook profile, your tweets, photographs you shared or videos you uploaded etc. It is best to consider thoroughly before posting online, as some material may remain online forever once posted.

### Cyber stalkers and digital footprints

It is easy to track a person online if they have a digital footprint. That is a good enough reason for some people to feel nervous, as it can attract the attention of cyber-stalkers. Sometimes it is not easy to delete all traces of your presence online, so the last resort is to delete your digital footprint. It is not 100 percent effective but most traces can be removed in this manner.

### Deleting your digital footprint

• Make a list of all the networks you are registered on and begin deleting your presence on these one by one.

• One way to delete traces of your Internet presence is to go to http://justdelete.me/. This is a directory of direct links to various websites so that you can delete your accounts. The links are color-coded to indicate the difficulty level of account deletion. They are categorized as easy, medium, hard and impossible. Some of the links give information on how one can delete an account while there is no information for some websites.

• There are certain websites which won't allow you to delete your accounts. An alternative is to overwrite the information with fake information. Create a fake email account and associate your account with it so that all email alerts will go to that account, ensuring there is no

authentic information in your new email account. Once the undeletable account is associated with your new fake email account, cancel this email account.

• Check your primary email and see how many mailing lists you are on. The emails should have an unsubscribe option which will allow you to unsubscribe yourself from these lists.

• If you have deleted your old blog, ensure you are not on the Wayback Machine. The Wayback Machine archives all sorts of digital content so that there is a record of it. Sometimes this can be used by people to find information on you. To exclude yourself, send an email to info@archive.org or follow the instructions given on http://archive.org/about/exclude.php.

• It is important to remember that you can only erase what you have posted when deleting your social media presence, not anything others might have posted. However, you may report such activity to obtain redress.

• For a comprehensive guide on deleting your Facebook and Twitter accounts, please read the following guides:

  o Facebook Guide
    http://www.wikihow.com/Permanently-Delete-a-Facebook-Account

  o Twitter Guide
    http://www.wikihow.com/Delete-a-Twitter-Account

Bytes for All (B4A), Pakistan is a human rights based think tank with a focus on Information and Communication Technologies (ICTs). It experiments and organizes debate on the relevance of ICTs for sustainable development and strengthening human rights movements in the country. At the forefront of the digital and Internet rights movement and struggle for democracy, B4A focuses on capacity building of human rights defenders on their digital security, online safety, and privacy.

Working on various important campaigns particularly against Internet censorship and surveillance in Pakistan, B4A focuses on cyberspace issues, awareness raising, and policy advocacy from civil liberties & human rights perspectives. The globally recognized and award winning Take Back The Tech! campaign is the flagship of B4A, which focuses on the strategic use of ICTs by women and girls to fight violence against women in Pakistan.

B4A partners and collaborates with a wide network of local & international human rights defenders and civil society organizations, and its team's commitment lies in protecting civil liberties in Pakistan.

---

**Bytes for All, Pakistan**
House 273, Street 17, F-10/2, Islamabad, Pakistan
+92 (51) 2110494-5 | www.bytesforall.pk
info@bytesforall.pk | @bytesforall




Cover Design by Rabeea Arif