Afghanistan

Digital Care Guide

رهنمایی مصونیت دیجیتالی افغانستان

دافغانستان لپاره د ډیجیتالي مصونیت لارښود

REPORTER OHNE GRENZEN

Care is Resistance

1 Emergency hotlines for digital emergencies

2 Prepare for digital emergencies, detention and check-points: Make a plan

3 Special advice for women journalists

4 Secure your online accounts, phone, tablet, and computer

5 Delete your digital history and minimize your online footprint

6 What to do if you lost your device

7 Recover your account

8 VPNs: protecting against spying, attacks & censorship

9 Secure video conferencing

10 Secure file sharing & online storage

Please note: The information and resources provided in this guide are current as of May 2022. We plan on making an updated version available every six months for at least next two years. The updates will be available for download at: https://helpdesk.rsf.org/digital-security-guide/afghanistan-digital-care-guide/

Credits

Care is Resistance

Caring for myself is not an indulgence, it is self-preservation and that is an act of political warfare

Audre Lorde

Taking care of your device and data is not only to protect yourself, but also your whole community. Journalists, media workers, and activists run the risk of their lives, in case, online and other data, apps, and/or contacts are being used as evidence against them or someone linked to them. Access to this data, apps etc. might be gained.
The following scenarios might occur:

- Confiscation of, and access to phones, tablets, computers, smart watches, and other storage devices (USBs, external hard drives, etc.) during raids, searches, detention, at check-points etc.

- Surveillance of digital communication and online connections

- Digital attacks on devices and accounts

- Open Source Intelligence – research on publicly available platforms like Facebook or Wikipedia

Being aware, that not all risks can be prevented, certain steps such as having less data on our devices, using secure channels of communication and securing our devices can reduce the likelihood or impact of, that data or apps being turned into evidence.
At the same time, some of these secure practices can turn into risks, if secure apps would be detected and framed as indicators of being linked to the wrong actors (e.g. international community or alike).

Risk	Prevention Steps	Response Steps	Remarks
Confiscation of and access to phones, tablets, computers and smart watches during raids, searches, detention and checkpoints etc.	▪ Reducing data on our devices to the bare and inconspicuous but realistic minimum ▪ Securing data on our devices ▪ Securing devices ▪ Creating encrypted backups of all data	▪ Not giving access to the devices ▪ Remotely wiping devices or automatic wiping of devices on failed login-attempts ▪ Informing affected people ▪ Recovering data and accounts	▪ Important decision: Will you give access to your devices under pressure? ▪ Consider, if encrypted backups or other encrypted files and folders could trigger attention and pose an additional risk for you?
Surveillance of digital communication and online connections (by authorities, their allies, internet service providers, telecommunication companies)	▪ Securing online accounts ▪ Using secure online services (end-to-end encrypted messengers, online storage, searches, video conferences, etc.) ▪ Securing our internet access through VPN or alike	▪ Document the surveillance if possible ▪ Activate mechanisms of abuse protection of the service providers ▪ Backup and de-activate the affected accounts	▪ Secure apps and channels like VPNs might trigger attention themselves and might be risky to use
Digital attacks on devices and accounts (spyware and hacking attacks and planting of evidence by authorities and their allies, criminals)	▪ Securing devices ▪ Securing online accounts ▪ Updating of firmware and software ▪ Refusing contact requests by unknown persons through social media	▪ Document attacks and all evidence ▪ Take the attacked device offline ▪ Recover accounts via the provider or emergency helplines ▪ Enable 2-Factor-Authentication on regained accounts	
Open Source Intelligence (OSINT) research on publicly availableplatforms like Facebook or Wikipedia	▪ Reducing digital footprint by removing information or request-ing the removal of information from online platforms	▪ Trying to remove evidence from online platforms	▪ Be aware that a lot of online information cannot be removed completely and if done then only with delays due to distributed backups and platforms like the way-backma-chine and other internet archiving services.

1 Emergency hotlines for digital emergencies

If you are a journalist, activist, or civil society member who needs emergency assistance, Access Now's Helpline provides 24/7 digital security support.

Please note:
The Helpline team does not speak local Afghan languages.

More options

https://cpj.org/emergency-response/how-to-get-help

https://www.frontlinedefenders.org/emergency-contact

Digital Rights Foundation can also take cases via helpdesk@digitalrightsfoundation.pk

If you suspect, that your phone got attacked with spyware or alike, the Emergency VPN by the Civilsphere project can help you check:
https://www.civilsphereproject.org/emergency-vpn

2 Prepare for digital emergencies, detention and check-points: Make a plan

To build online safety, determine what threats you face and which of your online activities might put you at risk — your threat model. This first look at digital security https://www.accessnow.org/first-look-at-digital-security/ can help you get started in answering those questions. When thinking about risks, please keep the following in mind:

2.1.

Make a plan for the possibility that you or someone you know could be detained by authorities.
Take a look at this guide:
https://digitalfirstaid.org/en/arrested/
by RaReNet and CiviCERT — which includes digital security precautions — for more.

There is also the Coping-with-Prison-Guide
https://coping-with-prison.org
which includes tips for families, supporters and lawyers of detained persons.

2.2.

At checkpoints and during raids, be prepared that authorities could confiscate or force you to unlock your device. Do not take your phone with you when going out. Or take a phone, which has no sensitive data like contacts or alike with you. Minimize the amount of data you save on your devices, especially on mobile ones.

The golden rule is: if in doubt, delete!

No information is worth risking your life or putting friends at risk. (Tips below on how to delete content and accounts.)
Make up your mind, if you would give access to your devices or not. It is not an easy decision, but good to think about it before it happens. Be aware, that fingerprint or Face-ID can be easily unlocked by force, if you are present. On iOS there is the emergency option to switch from FaceID or Fingerprint to passcodes by pressing the power button several times (older iPhones) or by initiating power off / Emergency SOS by pressing and holding either volume button and the side button simultaneously for 2 seconds (newer iPhones).

Make yourself used to this option, if you might need to use it.
Apps that can pose security risks, for you or others:

- Address / Contact List
- Messenger Apps
- Facebook Account
- Twitter or other Social Media Accounts
- Emails
- Notes & voice notes
- Photos
- Search and Web history
- Youtube videos you have watched / Google account
- Documents you have stored on your laptop / phone
- VPN Apps
- Google / Apple Maps data and location history (significant locations for Apple, location history for Google)
- Calendar App may contain sensitive entries as well
- Music Apps (some music might be taken as “politically or religiously inappropriate”)
- Dating Apps

Be aware, that you need to clean the bin of deleted items and that a thorough forensic analysis might bring back traces of these deleted contents. In case you want to delete everything from your phone: keep at least some personal images to show the use of the phone.

2.3.

Change contacts in your address book into Dari or Pashtu language and spelling and check if you need to remove international numbers.

- Your address book, messenger contacts and chat histories should not contain foreign-sounding names or addresses.

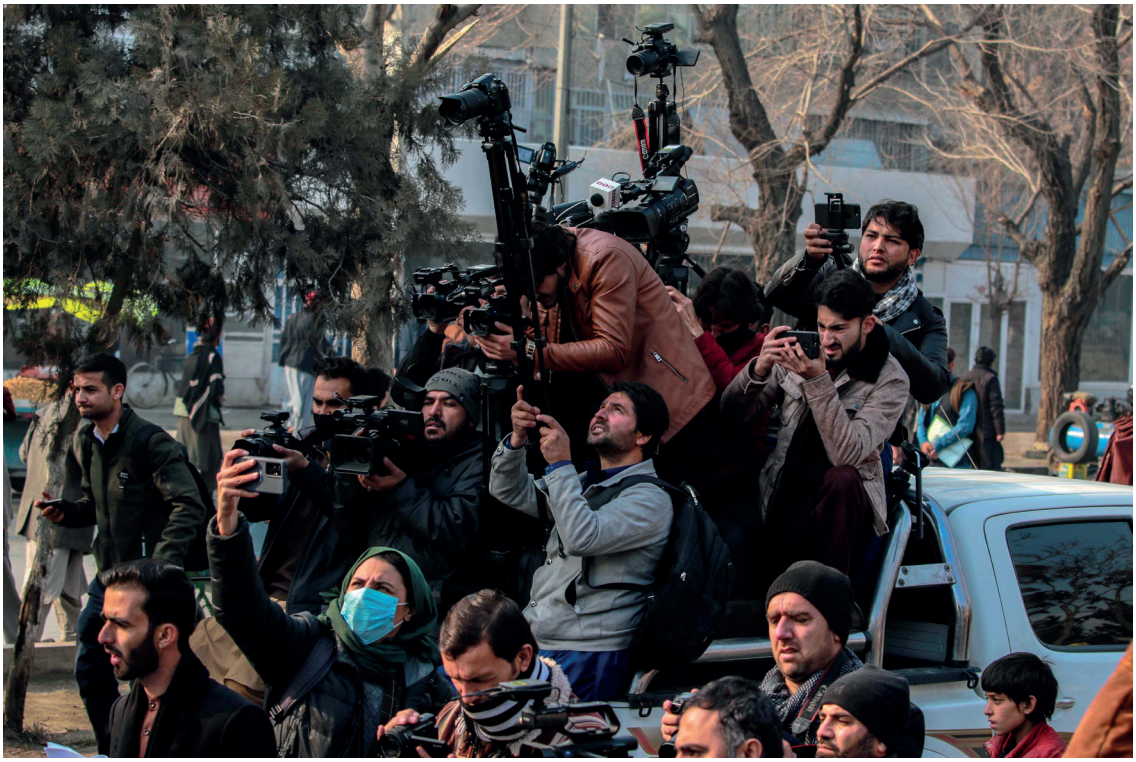
- If you need to preserve a list with those addresses, do not keep them on your phone or laptop!
  Send them to yourself on an email account that is not your primary address. Do not save the password for that account on your phone or laptop and do not leave a reference of this email on your device (e.g. if sending an email from your primary email account to your other email address, the email is still in the sent-folder).

- Delete any harmful emails from your Inbox, Archive, Sent, and Draft folders. Make sure to clear the bin after deleting the emails.

2.4. For messengers and other onlinegroups:
Activate several admins beforehand for each chat group, so several people / admins can actually do a kick-out of a member contact if needed (e.g. if someone's phone gets confiscated).

2.5. Don't respond to contact requests via social media, if they don't come via friends or trusted channels. There are cases, the T. "dressed" as foreign journalists, requested interviews and, afterwards abused the information and tracked the victim down.

2.6. Create functional email addresses instead of personalized ones, so not to contain names or alike, which could identify you.



—
epa09663664 Journalists cover the protest as people demand the unfreezing of central banks assets abroad, in Kabul, Afghanistan, 02 January 2022. The protesters criticized the United States President Joe Biden and the international community for allowing the people of Afghanistan to starve due to the economic crises, and urged them and the Taliban government to help them. The return of the Islamists, criticized of human rights abuses during their previous regime during 1996-2001, prompted the US to freeze its foreign assets, while a large part of the international community imposed economic sanctions and blocked aid.
Photo: picture alliance/EPA/STRINGER

3

Special advice for women journalists

If you are identified as a woman, you may face unique digital security threats. Check out this guide:
https://digitalrightsfoundation.pk/wp-content/uploads/2017/11/Hamara-Internet-Guidebook-English-Version-2016.pdf

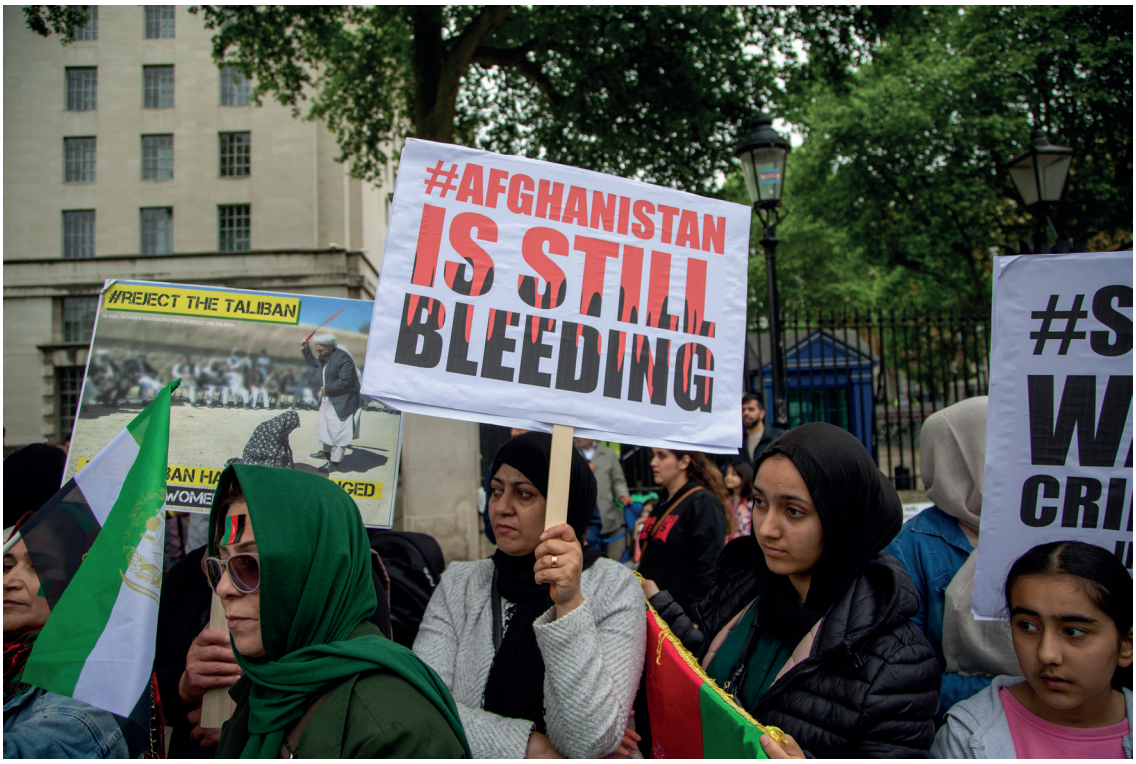
from the Digital Rights Foundation for tips;
they also provide services in Pashto:
https://digitalrightsfoundation.pk/services/

There is an online safety guide for women facing abuse by Chayn
https://www.chayn.co/
in several languages below.

Pashto:
https://chayn.gitbook.io/diy-online-safety/pashto-p-tw

Farsi:
https://chayn.gitbook.io/diy-online-safety/farsi-farsy

English:
https://chayn.gitbook.io/diy-online-safety/english



—
May 15, 2022, London, England, United Kingdom: Afghans protesters stage anti-Taliban demonstration outside Downing Street. (Credit Image: Â© Tayfun Salci/ZUMA Press Wire

4 Secure your online accounts, phone, tablet, and computer

4.1.

Require passwords to unlock your phone and computer, and enable fulldisk encryption. If, however, you think it might trigger attention if your device is searched, have a story ready to justify or just secure your data on the laptop securely. Turn the device off if left unattended and when going through a security check.
See point 2, if you will be willing to share your passwords or access to your devices or not.

4.2.

Use an end-to-end encrypted messaging app,

like Whatsapp:	https://whatsapp.com
or Signal:	https://signal.org
or Wire:	https://wire.com

for texting and enable disappearing messages and/or clear chats regularly. Be aware, that apps like Signal or Wire, which are not so frequently used or only used by “international” non-governmental organizations (INGOS) or “NGO people” might trigger attention, although they might be as such safer than Whatsapp.
An alternative to Signal for Android is a Signal-based messenger, called Molly, which might not trigger attention:
https://molly.im/

4.3.

Check the security settings on your accounts. See whether you have missed any important action items, and set up security alerts. If possible enable 2-Factor-Authentication (2FA) using an authentication app like freeOTP:
https://freeotp.github.io/

or Aegis for Android (as it has a lock with password feature):
https://getaegis.app/

and Raivo for iOS:
https://apps.apple.com/us/app/raivo-otp/id1459042137

Google (on mobile phones):
https://myaccount.google.com/security-checkup/
be aware, that if you connected your account to a phone number, your account might become traceable through the phone number!

Facebook:
https://www.facebook.com/help/799880743466869/
if you are using Facebook Messenger, it is better to use "Secret Conversations."

Whatsapp:
https://faq.whatsapp.com/general/verification/how-to-manage-two-step-verification-settings/?lang=en

Telegram:
https://telegram.org/blog/sessionsand-2-step-verification

https://2fa.directory/de/#email
links to documentation for all email providers
Make sure to write down the backup or recovery codes you get and keep them separate from your phone to recover your account if your phone is broken/stolen/out of battery!

More info:
https://ssd.eff.org/en/module/how-enable-two-factor-authentication

4.4.

If you want to change your phone or phone number due to anonymity reasons, be aware, that you always need to change both the phone AND the SIM-card. As both identify separately but at the same time to the phone towers (SIM-card number plus IMEI-Number of the phone), changing only one of them won't suffice because, the other one still identifies you!

5 Delete your digital history and minimize your online footprint

It's uncertain if and to what extent Taliban forces are currently surveilling people, notably human rights defenders and journalists, online. The situation is developing quickly, and it could be helpful to delete online information:
https://news.trust.org/item/20210817111442-4d73x

that may hurt your online safety in Afghanistan.
Following is some guidance from WIRED:
https://www.wired.com/story/how-to-clean-up-your-digital-history/

and Human Rights First:
https://www.humanrightsfirst.org/sites/default/files/How%20to%20delete%20your%20history_updated.pdf

Farsi version here:
https://twitter.com/dooley_dooley/statu s/1427223031429181441

Attention:

- Be careful about giving personal information to third-party services.
- Some platforms have data retention policies that archive accounts for law enforcement.
- Your deleted data may still be retained locally on your laptop or phone.

5.1. How to delete selected content like photos and posts and secure use

A general short guide in Farsi:
https://twitter.com/dooley_dooley/status/1427223031429181441

Facebook:
https://www.facebook.com/help/261211860580476/

- The Taliban have an active presence on Facebook and may use FB to identify who is openly opposed to them, who works with foreigners, and who has resources that might be exploited.

- Facebook has launched a one-click-tool to quickly lock down their account. When their profile is locked, people who aren't their friends can't download or share their profile photo or see posts on their timeline:
  https://twitter.com/ngleicher/status/ 1428474008295464965

- Create a 'local' account with only ocal friends that you keep on your phone app to avoid being associated with your international contacts. Keep your account as generic as possible, no political or religious content. Use a generic photo as profile picture, you might want to use a pseudonym. Be aware, that if you bind your new account to a phone number, your account might become traceable through the phone number!

- Make sure the "about" section of your account is not visible to the public. Do not add any job history to your account.
  Make sure your previous affiliations with any foreign entity including your job history is not visible on your account.

- If you want to keep your 'international account,' only log on to it when you are in the safety of your home. Do not store the password on your phone or your laptop.

- Check your Facebook posts (delete ANYTHING that is potentially objectionable), your friends' list (delete anybody who may raise suspicion, especially if foreign), and check what groups and pages you have liked in the past.

- Check your Facebook photos, especially profile and cover photos. Check the settings of all these photos, including the old photos, and make sure these photos are not visible to the public and only your rusted friends can view them. If you have any "questionable" photos, delete them.

- Restrict who can see your friend lists (and ask all friends to do the same). This can be done in Settings / How People find and contact you / Who can see your friends list? / "Only me."

- Do not tag fellow Afghans in Facebook

- Disable the functionality that others can tag you in photos
  https://www.hongkiat.com/blog/prevent-facebook-tagging/amp/

1. Review posts and photos that people, including your friends, have tagged you in the past, and if "problematic", remove the tags.

Twitter:
https://www.businessinsider.com/how-to-delete-old-tweets-from-twitter-2018-12

- Similar rules (as for Facebook) apply for twitter or other social media accounts. Review your list of whom you follow, and unfollow anyone or delete any tweets that could be objected to by the Taliban.

- Make sure you have not activated "tweet with location" in your Twitter setting. If you have, disable it.

- Delete old tweets:
https://semiphemeral.com

LinkedIn:
https://www.linkedin.com/help/linkedin/answer/3003/delete-content-you-ve-shared?lang=en

Instagram:
https://help.instagram.com/997924900 322403

Signal:
https://support.signal.org/hc/en-us/articles/360007320491

Telegram:
https://telegram.org/faq#q-can-idelete-my-messages

Messenger:
https://www.facebook.com/help/messenger-app/1944003114491 72

WhatsApp:
https://faq.whatsapp.com/android/chats/how-to-delete-messages/

Google Search:
https://support.google.com/websearch/troubleshooter/3111061?hl=en

TikTok:
https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/privacy-controls

Wikipedia:
If you find information on Wikipedia or other Wikimedia projects that could cause harm to you or other people in Afghanistan, please email ca@wikimedia.org and put AFG in the subject line. Review your friends' profile pictures and cover photos. If any of them has a "questionable" photo (for example: showing a flag or a banner that could be considered Anti-Taliban), ask them to change their it. If in doubt, delete this contact.

5.2.

How to delete entire accounts

Facebook:
https://www.facebook.com/help/224562897555674/

Twitter:
https://help.twitter.com/en/managing-your-account/how-to-deactivate-twitter-account

LinkedIn:
https://www.linkedin.com/help/linkedin/answer/63?lang=en

Instagram:
https://help.instagram.com/448136995230186/

Signal:
https://support.signal.org/hc/en-us/articles/360007061192-Unregister-or-Delete-Account

Telegram:
https://my.telegram.org/auth?to=delete

WhatsApp:
https://faq.whatsapp.com/android/account-and-profile/how-to-delete-your-account/?lang=en

Google:
https://support.google.com/accounts/answer/32046?hl=en

Additionally, request to delete cached Google results here:
https://google.com/webmasters/tools/removals

Microsoft/Hotmail:
https://support.microsoft.com/en-us/help/12412/microsoft-account-how-to-close-account

Yahoo:
https://en-global.help.yahoo.com/kb/SLN2044.htm

Protonmail:
https://protonmail.com/support/knowledge-base/delete-account/

5.3.

How to deal with photos

- Make sure you review all of the photos you keep on your phone to make sure that there are no 'objectionable' photos (such as of you with an American flag, you with foreigners, or of women without hijab or your family abroad).

- If in doubt, delete! It is understandably hard for you to delete photos that mean something to you, but remember they could potentially put you or others at risk.

- If you want to keep them, store them in the cloud, which does not use your main account, under a name and password that is not recorded anywhere, and delete them from your phone. See for example: What is and how to use Google Drive * English Video with Persian subtitle *

https://youtu.be/EbVnObwFJic

- There are some apps that allow you to keep photos hidden behind a 'decoy' folder or that pretend to be another app (such as Secret Calculator or Private Photo Vault), but remember this is not safe because other people know about these types of apps, too.

5.4.

Online searches Google / Youtube

Before browsing websites that could be seen as Anti-Taliban:

- Enable the private browsing mode in your browser
- If possible do not accept cookies
- Do not save bookmarks
- Do not save login data or passwords
- Do not login to websites with Google or Facebook or connect them to a third party website account

In general:

- Try to use browsers (like Mozilla Firefox) that protect your privacy and enable additional privacy settings

- Make sure to build a history of "safe"websites you visited (i.e. do not always surf in privacy mode). Your computer should show some entries so that no one will get suspicious.

- Make sure you are not logged in to browsers such as Firefox or Google Chrome (for example make sure you are not logged in to Chrome browser with your Google / Gmail account). If you browse the internet while logged in to your account, your account will keep a record of all your activities. Remove sensitive search results

https://www.humanrightsfirst.org/sites/default/files/How%20to%20delete%20your%20history_updated.pdf

https://twitter.com/dooley_dooley/status/1427223031429181441

Request removal of actual site content:
Removing the search result does not remove the content.
You will have to work with the owner of each site to remove your information from that site.

On Youtube & Google

- Remember that if you search youtube videos, this may show on your google account on your phone (the two accounts are usually linked)

- Regularly delete the "search history" on your YouTube and Google accounts.See how to delete Google activity

https://support.google.com/accounts/answer/465

This "self-doxing" guide:
https://guides.accessnow.org/self-doxing.html

might also be useful for understanding how much information about you is publicly available and minimizing things that can put you at risk, especially for activists who are detained and questioned about their views. You could be newly targeted for things you've posted, or based on your networks:
https://twitter.com/BBCWomansHour/status/1427287851016798213

If you discovered particularly sensitive information on a site, and you've been able to remove it from the site, also enter the URL of the specific page where the information was on
https://archive.org/web/

If there is an archived copy there, please contact help@accessnow.org for support.
https://cpj.org/2019/09/digital-safety-remove-personal-data-internet/

Online Search and People Finder services:
https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List

https://www.eff.org/deeplinks/2020/12/doxxing-tips-protect-yourself-online-howminimize-harm

6 What to do if you lost your Device

If that happens, it's impotant to act quickly to lessen the risk of someone else accessing your accounts, contacts, and personal information. Check out this Digital First Aid guide: https://digitalfirstaid.org/en/topics/lost-device/ to learn how to assess your risk, and what to do next.

6.1.

If possible, lock and wipe the phone remotely

Android:
https://support.google.com/accounts/answer/6160491?hl=en

Samsung:
https://www.samsung.com/za/support/mobile-devices/how-do-i-use-find-my-mobile-to-remotely-wipe-my-samsung-galaxy-s6-edge-plus/

iPhone:
https://www.igeeksblog.com/how-to-erase-data-from-lost-stolen-iphone-ipad-remotely/

6.2.

Kick the number of the lost phoneout of all social media groups (to prevent that the person finding the phone might gain access to those social media groups), for this activate several admins beforehand for each chat, so several people/admins can actually do this kick-out

- Whatsapp
- Signal
- Telegram

6.3.

Change all passwords for all accounts affected (including for their reset/recovery email addresses) and enable 2-Factor-Authentication on these accounts where possible.

6.4.

Inform your contacts about the loss of the phone and the risk that your contacts might be abused by the person finding and accessing your phone.

7 Recover your account

Most social media platforms, email services, and other sites have resources to help you recover your account. Major platforms also typically have ways to report any unusual account activities. We've listed several guides below. And also check out this first-aid guide:
https://digitalfirstaid.org/en/topics/account-access-issues

Google (Recover)
https://support.google.com/accounts/answer/183723

Facebook (Report):
https://www.facebook.com/hacked
(Recover):
https://www.facebook.com/notes/10157814523321886/

Instagram (Support steps):
https://help.instagram.com/149494825257596

Twitter (Support steps):
https://help.twitter.com/en/safety-and-security/twitter-account-hacked

8 VPNs: Protecting against Spying, Attacks & Censorship

VPNs build an encrypted tunnel between your device and the exit provided through the VPN. So it can not only access websites etc, which might be blocked and censored, but protect your surfing and traffic from being surveilled.

- If you are already using a VPN, continue with the same one, but check, if it is working properly. If you don't use a VPN so far, it might draw attention to you! Check out, which VPNs are mostly used to hide well in the crowd.

- All of this only helps if you download these tools before censorship or network shutdowns happen. Your use of these tools can often be detected by your Internet provider, and show up as installed apps visible to anyone looking at your unlocked phone.

- Once installed and running, check, if your VPN is working properly: https://ipleak.net

---

VPNs with good anti-censorship track records:

- TunnelBear:

https://www.tunnelbear.com/download
(Windows, MacOSX, Linux, iOS, Android)

Note:
Tunnelbear is currently free for users in Afghanistan for up to 10G/ month. Not available in Google App store, but users can download an APK from the official Telegram channel (Global)
https://t.me/tunnelbearofficial

If people are having problems connecting to Tunnelbear, report issues:
https://forms.office.com/Pages/ResponsePage.aspx

- Mullvad https://mullvad.net/en/download/
  (Windows, MacOSX, Linux, iOS, Android)
  €5/month; free licenses available from helplines like help@accessnow.org,
  anonymous purchasing method without sign-up and also accepts cash and crypto

- VPNGate https://www.vpngate.net
  (Windows, MacOSX, Linux, iOS, Android)
  a list of public VPN relay servers hosted by volunteers around the world.

- ProtonVPN https://protonvpn.com
  (Windows, MacOSX, Linux, iOS, Android, Chromebook)
  Free tier available.

- Bitmask https://bitmask.net
  (Windows, MacOSX, Linux, Android) is an open source VPN. You can use a built in provider (https://riseup.net or https://calyx.net) or start your own. Many other VPNs are available out there, but not all have made efforts to evade censorship or have good and proven security, privacy, and business practices. This review is a good place to start if you are looking for additional options:
  https://www.nytimes.com/wirecutter/reviews/best-vpn-service/

- A good resource for how VPNs work, what they do and what they don't help with is here:
  https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

Please note that most (if not all) VPN "review" sites profit off of VPN purchases and/or are owned by the same companies which own the VPNs.

Dedicated anti-censorship tools:

Make your risk assessment, if these apps could pose a risk to you (like triggering attention), if they are found on your devices or their use otherwise discovered.

- Psiphon is a free and open source censorship circumvention VPN that uses a variety of techniques to bypass Internet censorship
  https://www.psiphon3.com/en/download.html
  (iOS, Android, Windows)
  Download via email: Send an email to get@psiphon3.com to receive mirror download links of Psiphon in multiple languages.

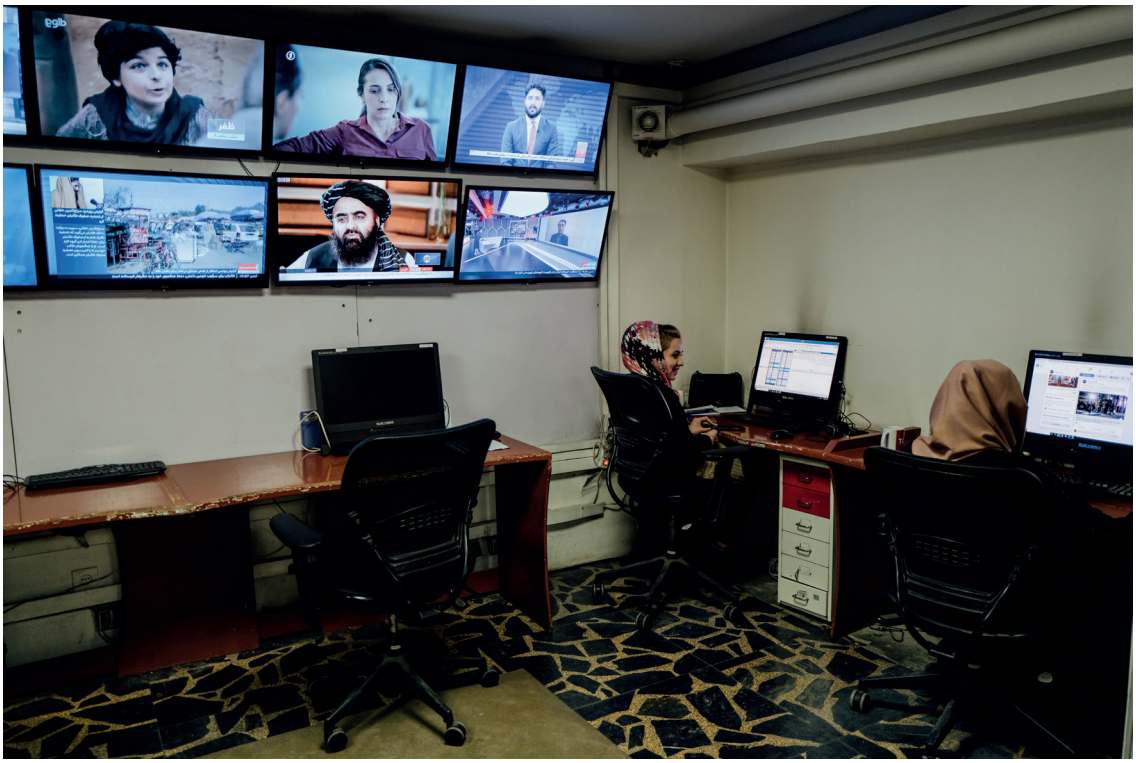
- Lantern is a free and open source censorship circumvention VPN that uses a variety of techniques to bypass Internet censorship.
  https://getlantern.org/en_US/index.html
  (Windows, MacOSX, Linux, iOS, Android)

- Tor Browser is the de-facto anonymity web browser that uses the Tor network for improved anonymity and provides censorship circumvention.
  https://www.torproject.org/download/
  (Windows, MacOSX, Linux, Android);
  Download via email:
  Send a request to GetTor gettor@torproject.org
  specifying your operating system (and your locale).
  Ex: “windows fa”

- OnionBrowser (iOS)
  https://onionbrowser.com

  https://apps.apple.com/us/app/onion-browser/id519296448

—
©Adrien Vautier / Le Pictorium/MAXPPP - Adrien Vautier / Le Pictorium - 24/11/2021 - Afghanistan / Kabul - In the newsroom of the Tolo News channel in Kabul on November 24, two journalists are working. The media now has more women than at the beginning of the year, before the Taliban took over.



9 Secure Video Conferencing

Messengers which allow for secure video calls. Be aware, that Signal and Wire might trigger attention, as they might not be so widely used in your communities.

Signal https://signal.org

- End-to-end encrypted video calls available for up to 8 participants
- Tied to the mobile phone number

Wire https://wire.com

- End-to-end encrypted video calls available for up to 4 participants (free version)
- Possibility of signing up without phone number

WhatsApp https://whatsapp.com

- End-to-end -encrypted video calls available for up to 4 participants
- Part of META-company (formerly Facebook, so meta-data is going to be captured)

JitsiMeet

- Video calls for up to 25 participants on trusted servers
- Free to use
- On computers access with browsers, apps available for Android and iOS
- Trusted Providers: https://meet.greenhost.net https://meet.systemli.org

Secure use guides

https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools

https://www.frontlinedefenders.org/en/resource-publication/jitsi-meet-simple-and-secure-video-conferencing-platform

App downloads for phones https://jitsi.org/downloads/

If you need to use conferencing tools like zoom.us make sure, that you enable the end-to-end -encryption feature:

https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings

10 Secure File Sharing & Online Storage

For storing documents securely on your computer or securing (encrypting) files before uploading them for online sharing and storage, the app Veracrypt https://veracrypt.fr allows to save encrypted containers (folders) on harddrives and online storages, Google Drive or on Dropbox, which to outsiders look like normal or system files. After using Veracrypt to encrypt a document like this, opt for deleting the application afterwards (including from Trash), to avoid that the app draws attention.
See: How to Use Veracrypt *English Video with Persian subtitle"
https://youtu.be/C25VWAGl7Tw

10.1. File Sharing: Secure (end-to-end encrypted) options

https://ufile.io/
- for non-registered users:
  max 10 files (max 5GB per file),
  max 30 days hosting

https://send.tresorit.com/
- for non-registered users: up to 5GB

https://send.tresorit.com/
- upload is limited to 50mb and files are stored
  no longer than 12 hours!

https://cryptpad.fr/drive/
- anonymous registration necessary –
  up to 1GB free hosting
  The name might draw attention!!!

If you are using the TOR-Browser: https://www.torproject.org/

Onionshare: https://onionshare.org

10.2. Online Storage

- Use online storage only through browser,
  not through installed apps!

If you use a cloud-access from an organizational server, be aware, that the URL/Link used might give away the name of the organisation and this can be seen by the Internet Service Providers. In this case the use of a VPN is reducing the risk.

- these commercial ones might draw less attention:

  https://mega.io
  (20gb for free)

  https://sync.com
  (5gb for free)

  https://cryptpad.fr/drive
  The name might draw attention!!!

- Google Drive and OneDrive and iCloud are not end-to-end-encrypted, so the servers can see, what you have uploaded, if you don't protect it beforehand
  (like ZIP-file with password on it or something similar)

- You may have a need to store documents somewhere (such as copies of your family's passports, your employment contracts, papers that document danger you have been exposed to).

- The best thing to do is to ensure these documents are saved in a secure cloud storage that does not use your main email account, or sent to a secure email address that you can access but is not your main known account, and not stored on your phone or your computer.

- Academics/students who need to save sensitive documents and/or information can use the Article 26 Backpack initiative by the University of California, Davis. Documents will be saved on cloud. Instructions available in English, Farsi and Dari.

  https://backpack.ucdavis.edu

  https://human-rights.ucdavis.edu/news/afghanistan-emergency-resource-information

Credits

This guideline is based on interviews
with Afghan journalists as well as on these guides:

1. Online safety resources for Afghanistan's human rights defenders (EN):
https://www.accessnow.org/online-safety-resources-afghanistan/

2. Checklist for Afghans. Minimise Risk through Data on Phones/Devices
(20 August 2021; EN, Dari, Pashto):
https://docs.google.com/document/d/19GPJDmMLPagNnbumZwmKZGJaliRMFmHiJKtuvmL-6wl8/edit

3. Digital Security Resources for Afghanistan.
+ Internet Shutdowns, Online Privacy (EN, Dari):
https://drive.google.com/drive/folders/1v9WvDvoCPjP13Y2Lsd0hqwDt6mqEgvtW

Scan the QR code
for the digital version
of this care guide.

https://helpdesk.rsf.org/digital-security-guide/afghanistan-digital-care-guide/

RSF REPORTER OHNE GRENZEN

BERLIN

Senatsverwaltung
für Wirtschaft, Energie
und Betriebe

د دغه لارښود ډیجیټالي بڼې ته د لاسرسي لپاره لطفا" د QR کډ اسکن کړئ.

https://helpdesk.rsf.org/digital-security-guide/afghanistan-digital-care-guide/

REPORTER OHNE GRENZEN

10.2. انلاين ذخيره کول

- د انلاين ذخيره کولو لپاره يواځې او يواځې له مرور کوونکو يا براوزرونو نه کار واخلئ. په کمپيوټر او موبايل کې نصب شوې برنامې مه کاروئ.

که تاسو Could Access لاس رسي لپاره د خپل سازمان سرور کاروئ، متوجه وسئ چې د UR/Link استفاده کېدونکی لينک ممکن ستاسو د سازمان نوم ښکاره کړي او تاسو ته د انترنټ خدمات وړاندې کوونکی وتوانيږي چې هغه وويني. په دې برخه کې له VPN ګټه اخستل خطر کموي.

- هغه کوم چې تجارتي دي ممکن توجه جلب کړي:

20) https://mega.io جی.بی وړيا)
5) https://sync.com جی.بی وړيا)
https://cryptpad.fr/drive
نوم ممکن دی د توجه د جلب کېدو سبب شي!!!

Google Drive، OnveDrive و iCould د بشپړ کډ کولو نوعيت نه لري. له دې امله د هغه څه د مشاهده وړتيا لري چې اپلوډ کړي مو دي، خو کله چې تاسو هغه وار له مخه نوي حفاظت کړي. (د مثال په توګه: د کډ کړل شوي ZIP او يا هغه ورته توکو کارونه)

ممکن اړتيا ولرئ چې ځينې اسناد چېرته ذخيره کړئ. (لکه: د کورنۍ د غړو د پاسپورت کاپي، ستاسو کاري قراردادونه، هغه اسناد چې تاسو ته د متوجه خطر ښکارندیونه کوي.)

د اسنادونو د ذخيره کولو لپاره هغه ښه کار چې کولی شئ، دا دی چې هغه په يوه خوندي (کلاوډ- Could) فضا کې ذخيره کړئ، چې ستاسو له اصل ايمل سره په اړيکه کې نه وي. او يا هم هغه يوه بل مصون ايمل ته وروستوی چې تاسو کولئ شي لاس رسی ورته پيدا کړئ، خو ستاسو اصلي ايمل نه دی، او ستاسو په تلفون او يا هم کامپيوټر کې نه دی ذخيره شوی.

اکادميسنان/ محصلين څوک چې د حساسو اکادميکو او يا هم خپلو مهم سندونو د خوندي کولو په هڅه کې دي، کولی شي د Article 26 Backpack طرحې څخه چې د کالفورنيا داويس پوهنتون جوړه کړې، کار واخلي. اسنادونه به په کلاوډ فضا کې ذخيره شي. د دغې طرحې د ګټې اخستنې د لارښود په لاندې لينک کې په انګليسي او دري ژبو وړاندې شوی.
https://human-rights.ucdavis.edu/news/afghanistan-emergency-resource-information
يا هم دری:
https://backpack.ucdavis.edu/?language=fa

امتياز

دا لارښود له افغان خبريالانو سره د مرکو او همدا راز د دغو لاندو لارښونو پر اساس جوړ شوی:

1 | په افغانستان کې دښر حقونو مدافعانو لپاره د انلاين خوندیتوب سرچينې |
https://www.accessnow.org/online-safety-resources-afghanistan
EN

2 | د افغانانو لپاره چک ليست| په تلفونونو او وسايلو کې د معلوماتو له لاړې خطر کم کړئ|

https://docs.google.com/document/d/19GPJDmMLPagNnbumZwmKZGJaliRMFmHiJKtuvmL6wl8/edit
EN, Dari, Pashto

3 | د افغانستان لپاره د ډيجيټالي امنيت سرچينې/منابع: د انترنت پرې کېدل او انلاين خصوصي حريم|
https://drive.google.com/drive/folders/1v9WvDvoCPjP13Y2Lsd0hqwDt6mqEgvtW
EN, Dar

10 په خوندي توګه د فايلونو شريکول او په انلاين بڼه يې ذخيره کول

په کامپيوټر کې په خوندي توګه د فايلونو د ذخيره کولو او يا هم په انلاين بڼه د ذخيره کولو مخکې په بشپړ ډول د فايلونو د کڅ ورکونې لپاره Veracrypt :
https://veracrypt.fr
اجازه ورکوي چې خپل فايلونه او په يوه کڅ شوي فولدر کې په آنلاين ډول په Google Drive او يا Dropbox کې ذخيره کړئ او نورو ته د يوه عادي فايل او يا کمپيوټري سيستم په توګه ښکاري.
په دې ډول له Veracrypt څخه د فايلونو له ذخيره کولو وروسته هغه له خپل کامپيوټر څخه پاک کړی او د کامپيوټر د باطلې سطل مو هم پاک کړی. دا چې ويرا-کريپ څنګه کارول کيږي په انګليسي ژبه دغه ويديو وګورئ چې په ليکي ډول فارسي ژباړه هم لري.
https://youtu.be/C25VWAGl7Tw

10.1. د فايلونو شريکول | په بشپړ ډول (د کڅ کولو) اختياروونه

/https://ufile.io
- د نا راجستر شوي کارووونکو لپاره: نهايتاً 10 فايل (5 ګيګابايت د هر فايل لپاره)، يوه مياشت وړيا خدمات

https://send.tresorit.com/
- د نا راجستر شوي کارووونکو لپاره، او تر 5 ګيګابايت پورې د استفادې له قابليت سره

https://send.tresorit.com/
- ا پلود يې تر 50 ګيګابايت پورې دی او فايلونو تر ۱۲ ساعتونو زيات نه په کې ذخيره کيږي.

https://cryptpad.fr/drive/
- په نا پېژنده توګه نوم ثبتونه لازمي ده.| تر يو GB وړيا هاستينګ لري. نوم يې ممکن توجه ځان ته جلب کړي!!!

که تاسو د Tor مرور کوونکی يا براوزر کاروئ.
https://www.torproject.org/
يا هم OnionShare:
https://onionshare.org

9

په خوندي او مصون توګه ويديو کنفرانس

هغه پيام رسوونکي يا مسنجرونه چې د ويديويي تماسونو زمينه هواري. پام مو وي چې له زيګنال او وايِر نه ستاسو په ټولنه کې احتمالاً کار اخيستنه لږ وي او ممکن د توجه د جلب سبب وګرځي.

- زيګنال :

https://signal.org

- وايِر | په بشپړ ډول کډ شوی ويديويي تماسونه د حداقل 8 کسانو لپاره په يوه وخت په کې کارو کېدای شي.
- ستاسو د تلفون په شمېر پورې تړلی اپليکشن دی

- وايِر :

https://wire.com

- په بشپړ ډول کډ شوي ويديويي تماسونه حداقل څلور کسانو ته پر يوه وخت برابرولی شي.(وړيا ډول خدمات)
- د تلفون شمېرې پرته هم د استفاده وړی دی

- واتساپ :

https://whatsapp.com

- په بشپړ ډول کډ شوي تماسونه په يوه وخت د حداقل څلور کسانو لپاره وړاندې کوي
- د ميتا – کمپنې يوه برخه ده. (پخوا فيسبوک، په همدې اساس په پام کې ده ميتا-ديتا واخستل شي.)

جتسی میت- JitsiMeet

- په اعتباري سروونو کې پر يوه وخت تر ۲۵ مخاطب پورې تصويري اړيکې يولی شي
- په وړيا ټوګه ګټه اخيستنه
- په کامپيوټرونو کې د براوزرونو – يا مرور کوونکو له لارې لاس رسی ورته ممکن دی، د اندوراید او iOS لپاره هم اپليکشن لرِي.
- د خدماتو باوري او د اعتماد وړ وړاندې کوونکی:

https://meet.greenhost.net

https://meet.systemli.org

- په مصون ډول د ګټې اخيستو لارښود:

https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools

https://www.frontlinedefenders.org/en/resource-publication/jitsi-meet-simple-and-secure-video-conferencing-platform

- د تلفونونو لپاره د اپليکيشن دانلود:

https://jitsi.org/downloads/

- که اړتيا وه چې د انلاين کنفرانسو له وسيلو کله https://zoom.us ګټه واخلئ، ځان مطمين کړئ چې د بشپړ کډ کولو خصوصيت يا اختيار فعال کړی.

https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings

- ټوور – Tor :

- د بلقوه ناپېژنده پاتې کېدو لپاره یو براوزر یا مرور کوونکی دی چې د Tor له شبکې څخه د ناپېژنده پاتې کېدو په خاطر کار اخلي.

https://www.torproject.org/download/

(Windows, MacOSX, Linux, Android);

د ایمل له لارې یې دانلود کړئ:

GetTor ته یو ایمل ایمل واستوئ، او خپل عامل سیستم او (سیمه) ورته مشخص کړئ. د مثال په توګه: "windows fa"

- اونیون مرور کوونی – OnionBrowser (iOS) :

https://onionbrowser.com

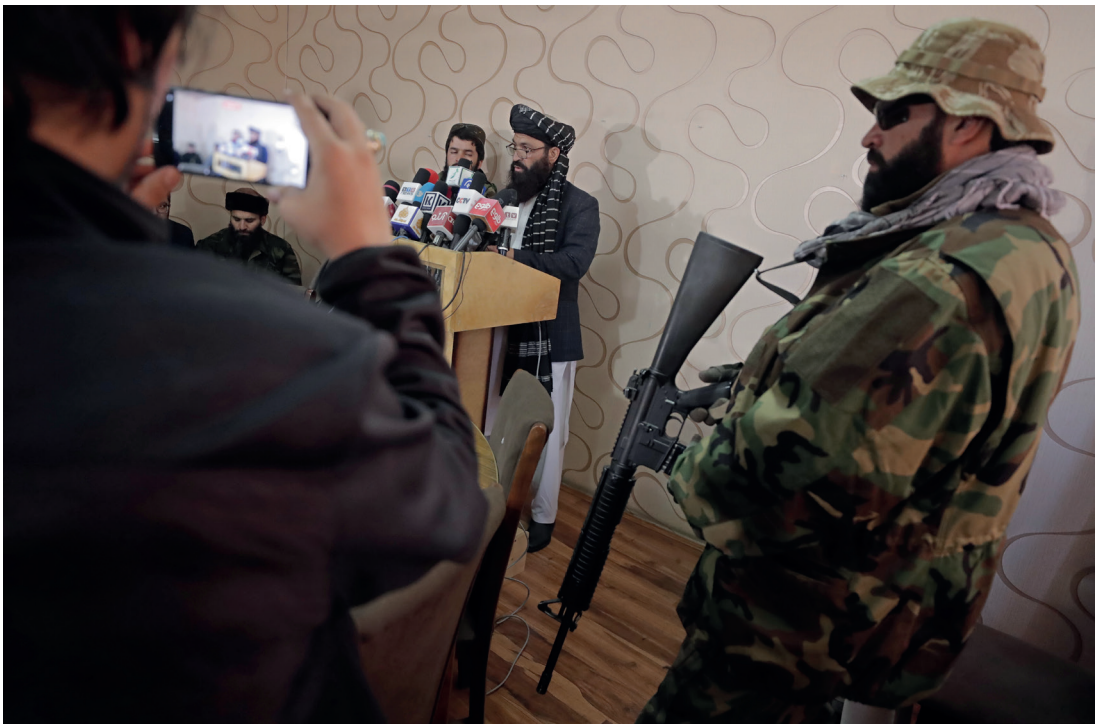
https://apps.apple.com/us/app/onion-browser/id519296448

—

د افغانستان د پاسپورت عمومي ریاست مشر، علم ګل حقاني له خبریالانو سره په یوې میاشت ځنډ وروسته د ۲۰۲۱ کال د ډسامبر په ۱۸ نېټه په کابل کې د دغه ریاست د خدماتو پر بېرته فعالېدو خبرې کوي چې د ګنه ګوڼې، د وسایلو د خرابوالي له ځنډ سره مخ شوي وو. هغه ووېل چې اوس ټولو ولایتونو کې د ډسامبر له ۱۸ نېټې د ورځې ۳۰۰۰ پاسپورټونو غوښتنلیکونو ته رسېدنه کېږي. د اګست میاشتې له راهیسې ټول افغانستان د طالبانو په واک کې دی. دوی له ۱۹۹۶ تر ۲۰۰۱ کال هم دلته حکومت کړی، چې نظام یې پر شدیدو شرعي محدودیتونو، د بشر حقونو پر سرغرونو او د اتباعو پر پراخ هجرت والړ و.

تصویر:

picture alliance/EPA/MAXIM SHIPENKOV



- وی.پی.ان.گیټ – VPNGate :

https://www.vpngate.net

(Windows, MacOSX, Linux, iOS, Android)

د عمومی VPN د ریلي سرورونو لېست چې په تولنه نړۍ کې د رضاکارانو لخوا کوربه کیږي.

- پروټون وی.پی.ان – ProtonVPN :

https://protonvpn.com

(Windows, MacOSX, Linux, iOS, Android, Chromebook)

په وړیا توګه د لاس رسي وړ دی.

- بیت ماسک – Bitmask :

https://bitmask.net

(Windows, MacOSX, Linux, Android)

دا VPN یوه خلاصه سرچینه ده. تاسو کولی شئ چې د تیار شویو VPNs څخه چې د riseup.net) یا (caly.net) لخوا وړاندې کیږي ګټه پورته کړئ، او هم خپل یو پیل کړئ.

ډېر نور VPNs هم د لاس رسي وړ دي، خو ټولو بیا د سانسو د مخنځه وړلو، د سه امنیت درلودو، د خصوصي حریم د ساتنې او یا د سه تجارتي چلند لپاره موثړي هڅې نه دي کړي. که د لا زیاتو مواردو د امتحانولو په هڅه کې یاست، لاندې ادرس ته مراجعه به یو سه پیل وي:

https://www.nytimes.com/wirecutter/reviews/best-vpn-service/

د VPNs د فعالیت د څرنګوالي په اړه چې دوی څه کوي او ایا کومو برخو ته د ګټې اخستنې وړ نه دي؟ دا لاندې لینک یوه سه منبع ده:

https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

لطفاً پام ولرئ، چې اکثراً (خو ټول نه) د VPN "بیاکتنې" سایټونه د VPN له خرڅلاوي څخه ګټه پورته کوي او/یا د ورته شرکتونو ملکیت دی چې د VPNs ملکیت لري.

د سانسور ضد لپاره ځانګړي وسایل:

یو څېړنه ترسره کړئ چې ایا دا برنامې به تاسو ته د خطر د رامنځته کېدو سبب شي. (لکه: د پاملرنې جلب)، که هغه ستاسو په وسایلو(کامپیوټر/مبایل) په نصب شوي شکل وموندل شي او یا هم دا کشف شی چې تاسو له هغو استاده کوئ.

-

Psiphon د خلاصې منبعې د سانسور د سانسو د لرې کولو VPN دی چې له مختلفو تکتیکو څخه د سانسور د لرې کولو لپاره کار اخلي.

https://www.psiphon3.com/en/download.html

(iOS, Android, Windows)

- د ایمل له لارې دانلود:

دغه ادرس ته (get@psiphon3.com) یو ایمل واستوئ، ترڅو د Psiphon دانلود لیکنونه په مختلفو ژبو ترلاسه کړئ.

- لاټرن – Latern :

- دا د خلاصې منبع د سانسور د لرې کولو یو VPN دی چې له مختلفو تکتیکونو څخه د سانسور د لرې کولو په خاطر کار اخلي.

https://etlantern.org/en_US/index.html

(Windows, MacOSX, Linux, iOS, Android)

8

VPNs: د جاسوسۍ، حملو او سانسور په وړاندې ساتنه

VPNs ستاسو د وسیلې (کامپیوټر/موبایل) او د وړاندې کړل شوې خروجي (exit) ترمنځ د VPN په وسیله یو کډ شوی تونل جوړوي. په همدې اساس دا کار هغه ویب سایټونو ته د لاس رسي اجازه درکوي چې یا مسدود شوي او یا هم سانسور شوي او ترڅنګ یې په انټرنټي فضا کې ستاسو له فعالیت و ترافیک هم ساتنه کوي.

- که پخوا مو له VPN ګټه اخیستې له همغه یوه سره مخ ته ولاړ شئ، او چک یې کړئ چې سم کار کوي. په غیر صورت کې له یوه نوي VPN څخه ګټه پورته کړئ. او دا کار ممکن ستاسو پام ځان ته راجلب کړئ. چې کوم یو VPN د خلکو ترمنځ د پټېدو لپاره موثر دی.

- دا کار هغه وخت موثر وسېدلی شي له دې مخکې چې تاسو له سانسور سره مخ شئ او یا هم ستاسو دستګاه خاموشه شي، هغه دانلو کړئ. له دغه ابزار څخه استفاده کول ممکن ډېر وخت ستاسو د انټرنټ وړاندې کوونکي لخوا تثبیت شي، او ستاسو په تلفون کې د یوې نصب شوې برنامې په توګه هغه کس ته چې ستاسو قفل ناشوي تلفون ته لاس رسی لري د مشاهده وړ وي.

- له انستال او اجرا وروسته یې یو ځل چک کړئ چې VPN مو سم کار ورکوي:
ipleak.net

د سانسور ضد VPNs له ښه ترک ریکاډونو سره

- تیونل بییر – TunnelBear :
https://www.tunnelbear.com/download
(Windows, MacOSX, Linux, iOS, Android)

یاداشت: تیونل بییر د اوس لپاره په افغانستان کې خپلو استفاده کوونکو ته دې میاشتې تر ۱۰ جي.بي وړیا خدمات لري. په ګوګل اپ ستور کې د موندنې وړ دی، خو کاروونکي یې کولی شي چې یو APK د تلګرام له رسمِ کانال دانلود کړي.
https://t.me/tunnelbearofficial

کوم کسان چې د تیونل بییر له استفادې سره په ستونزو کې وي، کولئ شي هغه راپور کړئ:
https://forms.office.com/Pages/ResponsePage.aspx

- مولواد – Mullvad :
https://mullvad.net/en/download/
(Windows, MacOSX, Linux, iOS, Android)

میاشتنی لګښت 5 یورو؛ د ګټې اخستنې جواز له مرستندویه خطونو (help@accessnow.org) د لاس رسی وړ دی، پېر یې په ناپېژنده او له نوم ثبتونې پرته ترسره کیږي. همدارنګه د ډیجیټالي ارز ترڅنګ کولی شي له نقدو پیسو هم استفاده وشي.

7

خپل اکونټ/حساب بیا ترلاسه کړئ

اکثراً ټولنیزې رسنۍ، د ایملونو خدمات او نور سایټونه پلاتفورمونه داسې یوه منبع لري چې د تاسو د حساب د بیا ترلاسه کولو سره مرسته کوئ. ډېرې پلاتفورمونه په اکونټونو کې د غیر معمول فعالیتونو د راپور ورکونې لارې هم لري. مونږ څو لارښودونه لیست کړي، تاسو سره په دغه برخه کې مرسته وکړي. د ډیجیتالي بېړنیو مرستو لاندې لارښود ته پام وکړئ. |
https://digitalfirstaid.org/en/topics/account-access-issues

د ګوګل بیا ترلاسه کول :
https://support.google.com/accounts/answer/183723

د فیسبوک راپور کول :
https://www.facebook.com/hacked

د فیسبوک بیا ترلاسه کول :
https://www.facebook.com/notes/10157814523321886/

د انستاګرام د ملاتړ پراونه :
https://help.instagram.com/149494825257596

د ټویټر د ملاتړ پراونه :
https://help.twitter.com/en/safety-and-security/twitter-account-hacked

6 د موبایل او یا کامپیوټر دې ورکېدو په صورت کې څه وکړو

که داسې یو څه پېښ شي، ډېره مهمه ده په عاجله ټوګه اقدام وکړئ او وتوانېږئ چې خپل اکونټ/انلاین حساب، مخاطبینو او شخصي معلوماتو ته د لاس رسي کچه کمه کړئ.
زمونږ د بېړنیو ډیجیتالي مرستو لارښود ته پام وکړئ.
https://digitalfirstaid.org/en/topics/lost-device/
ځکه باید دا ارزیابي شي چې په به بل پراو کې څه وکړو.

6.1.

که ممکن و، تلفون له لرې لارې قفل کړئ او یا یې مواد پاک کړئ.

اندرواید – Andriod :
https://support.google.com/accounts/answer/6160491?hl=en

سامسونګ – Samsung :
https://www.samsung.com/za/support/mobile-devices/how-do-i-use-find-my-/mobile-to-remotely-wipe-my-samsung-galaxy-s6-edge-plus

آیفون – iPhone :
https://www.igeeksblog.com/how-to-erase-data-from-lost-stolen-iphone-ipad-remotely/

6.2.

د ورک شوي تلفون شمېره د ټولنیزو رسنیو له ګروپونو لرې کړئ.(په دې هدف چې د تلفون موندونکی ونتوانېږئ چې ستاسو دغو ټولنیزو ګروپونو ته لاس رسی پیدا کړئ.)، د دغه فعالیت د ترسره کولو لپاره باید له مخکې د هر ګروپ لپاره څو سمبالوونکي ولرئ، ځکه مختلف مدیران/سمبالوونکي کولئ شي دا شمېره په اساني سره پاکه کړئ.

- Whatsapp
- Signal
- Telegram

6.3.

د اغیزمن شویو حسابونو/اکونټونو پاسوردونه بدل کړئ، (د بیا ترلاسه کولو / بیاځل تنظیم په ګډون) او 2AF اختیار هم دغه اکونټونو لپاره چې ورتیا یې لري ورته فعال کړئ.

6.4.

د خپل تلفون د ورکېدو په صورت کې خپل مخاطبین خبر کړئ او همدا راز د هغوی په وړاندې هم د هغه کس لخوا چې تلفون ورسره دی، شته خطر ورته تشریح کړئ، ترڅو پوه وي.

د سایت د واقعي محتوا د لمنځه وړلو غوښتنه وکړئ: د پلټنې د پایلو لمنځه وړل د محتوا د لمنځه وړلو سبب نه ګرځي.
په هر سایت کې د خپلو اطلاعاتو د لمنځه وړلو لپاره باید د هغه سایت له خاوند سره په اړیکه کې شئ.
په یوتیوب او ګوګل کې

- پام مو وي، که تاسو په یوتیوب کې ویډیو لټوئ، دا ممکن په تلفون کې د تاسو په ګوګل حساب کې هم ښکاره کړل شي.(دا دوه حسابونه معمولاً سره وصل وي.)

- په منظم ډول په یوتیوب او ګوګل اکونټونو کې د خپل لټون مخینه پاکه کړئ.

په ګوګل کې د خپلو فعالیتونو د پاکولو د څرنګوالي لپاره لاندې لینک ته مراجعه وکړئ.
https://support.google.com/accounts/answer/465

«د ځان افشا» لارښود - Self-doxing Guide:
https://guides.accessnow.org/self-doxing.html
ممکن د دغه درک لپاره چې څومره اطلاعات د تاسو په اړه په عموم ډول د لاس رسي وړ دي او حداقل کچې ته د هغو د راکمولو په برخه کې چې تاسو خطر سره مخ کولی شي، له تاسو سره مرسته وکړي. په ځانګړې توګه هغه فعالان چې زنداني شوي، او د خپلو نظریاتو لپاره تر پوښتونو راغلي. امکان لري چې ډېر ژر د هغه شیانو لپاره مو چې پست کړي دي، هدف وګرځئ.
https://twitter.com/BBCWomansHour/status/1427287851016798213

که ستا په کوم سایت کې حساسیت پارونکي معلومات ومومدل او بیا وتوانېدی چې هغه له ویب سایت څخه حذف کړئ، همداراز د مخصوصي صفحې URL چې په هغه کې معلومات و، دلته هم ورداخل کړئ.
https://archive.org/web/
که یې ارشیف او ذخیره شوې کاپي موجوده وه، بیا د مرستې لپاه له لاندې ادرس سره په اړیکه کې شئ.
help@accessnow.org
https://cpj.org/2019/09/digital-safety-remove-personal-data-internet/

انلاین لټون او د وګړو/خلکو د موندنې خدمات:
https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List

https://www.eff.org/deeplinks/2020/12/doxxing-tips-protect-yourself-online-howminimize-harm

5.3.

له عکسونو سره څنګه برخورد/ چلند وکړو

- ډاډه شئ چې په موبایل کې مو خپل ټول شته عکسونه لیدلي او پوهیږئ چې هېڅ یو سر خوږونکی تصویر په کې نه شته. (لکه: د امریکا له بیرغ سره ستاسو خپل عکس، تاسو له بهرنیانو سره، یا ښځې له حجاب پرته، یا تاسو د خپلې کورنۍ له غړو سره په بهر کې.)

- که شک لرئ، لمنځه یې یوسئ. دا د درک وړ ده چې د عکسونو لمنځه وړل به درته سخت وي، خو په پام کې ولرئ چې هغه تاسو او نور په بلقوه ډول له ګواښ سره مخ کوي.

- که غواړئ هغه له ځان سره وساتئ. نو په کلاوډ – Could کې یې ذخیره کړئ او هغه اکونټ چې ورته کارول کیږي باید ستاسو اصلي حساب نه وي. د هغو نوم او پاسورد تر دې پخوا بل هېڅ ځای نه وي ثبت شوی او وروسته یې له خپل تلفون پاک کړئ. د مثال په توګه: ګوګل درایف څه دی او څنګه کارول کیږي؟ په اړه یې دا انګلیسي ویډیو چې فارسي لیکلې ژباړه لري وګورئ.
https://youtu.be/EbVnObwFJic

- ځینې پروګرامونه شته چې دا امکان تاسو ته برابروي ترڅو خپل عکسونه په یوه دوکه ورکوونکي فولډر کې چې په ظاهر کې بل پروګرام غوندې ښکاري(لکه: مخفی ماشین حساب یا د عکس خصوصی البوم) په کې پټ کړئ. خو پام مو وي دا چلند مصون نه دی، ځکه نور خلک هم د دا ډول پروګرامونو په اړه معلومات لري.

5.4.

انلاین لټون – ګوګل – یوټیوب

په هغه ویب سایټونو کې چې ممکن د طالبانو ضد معلوم شي له لټون مخکې دا کارونه وکړئ:

- په خپل براوزر کې د خصوصي لټون حالت فعال کړئ
- که ممکن و، Cookies مه درسره منئ
- بوک مارکونه مه ذخیره کوئ
- ډېټا/معلومات یا پاسورد مو مه ذخیره کوئ
- د ګوګل او فیسبوک ویب سایټونو ته له ورننوتو ډډه وکړئ او یا هغه د یوه دریم شخص د ویب سایټ اکونټ ته وصل کړئ

په ټوله کې:

- هڅه وکړئ چې له دې مرورکوونکو -براوزرونو (لکه: موزیلا فایرفاکس) څخه کار واخلئ، چې ستاسو له خصوصي حریم ساتنه کوي او د خصوصي حریم ډېر نور تنظیمات فعال کړئ.

- ډاډ ترلاسه کړئ، د هغه مصون ویب سایټونو لیدنه مو چې کړې د هغوی یوه مخینه درسره جوړه کړئ. (د مثال په توګه: تل د خصوصي حریم په حالت کې فعالیت مه کوئ.) ستاسو کامپیوټر/موبایل باید ښکاره کړي چې ځینې دخولې ګانې لري، ترڅو چې څوک پر تاسو شک ونه کړي.

- ډاډ ترلاسه کړئ چې فایر فاکس او ګوګل کروم مرورکوونکو ته نه یې ورداخل شوي.(د مثال په توګه: مطمین شئ چې تاسو د کروم مرورګر ته په خپل ګوګل اکونټ/جیمل سره نه یې ورداخل شوي.) که کله هم خپل حساب ته ورداخل شوي یاست، او انترنت مو مرور کړی وي، ستاسو حساب د ټولو فعالیتونو مخینه ذخیره کوي.
د حساس لټون پایلې لمنځه یوسئ
https://www.humanrightsfirst.org/sites/default/files/How%20to%20delete%20-your%20history_updated.pdf-

https://twitter.com/dooley_dooley/status/1427223031429181441

5.2.

| څه ډول ټول اکونټونه حذف کړو

فیسبوک – Facebook :
https://www.facebook.com/help/224562897555674/

ټویټر – Twitter :
https://help.twitter.com/en/managing-your-account/how-to-deactivate-twitter-account

لینکډ ان – LinkedIn :
https://www.linkedin.com/help/linkedin/answer/63?lang=en

انسټاګرام – Instagram :
https://help.instagram.com/448136995230186/

زیګنال – Signal :
https://support.signal.org/hc/en-us/articles/360007061192-Unregister-or-Delete-Account

ټلګرام – Telegram :
https://my.telegram.org/auth?to=delete

واټساپ – WhatsApp :
https://faq.whatsapp.com/android/account-and-profile/how-to-delete-your-account/?lang=en

ګوګل – Google :
https://support.google.com/accounts/answer/32046?hl=en
سربېره پر دې، د دغه لینک په وسیله کولی شئ، د ګوګل په پټه حافظه کې د ذخیره شویو پایلو د حذف غوښتنه هم وکړئ.
https://google.com/webmasters/tools/removals

مایکروسافټ/هاټمیل – Microsoft/Hotmail :
https://support.microsoft.com/en-us/help/12412/microsoft-account-how-to-close-account

یاهو- Yahoo :
https://en-global.help.yahoo.com/kb/SLN2044.htm

پروټون میل – Protonmail :
https://protonmail.com/support/knowledge-base/delete-account/

- ډاډمن شئ چې تاسو د ټویټ کولو لپاره د ټویټ د موقعیت ښودلو تنظیمات نه دي فعاله کړي. که داسې مو کړي وي، هغه غیر فعال کړئ.

- پخواني ټویټونه پاک کړئ:
https://semiphemeral.com

لینکدان – Linkedin
https://www.linkedin.com/help/linkedin/answer/3003/delete-content-you-ve-shared?lang=en

انستاګرام – Instagram
https://help.instagram.com/997924900 322403

زیګنال – Signal
https://support.signal.org/hc/en-us/articles/360007320491

ټلګرام – Telegram
https://telegram.org/faq#q-can-idelete-my-messages

مسنجر – Messenger
https://www.facebook.com/help/messenger-app/1944003114491 72
واتساپ – WhatsApp
https://faq.whatsapp.com/android/chats/how-to-delete-messages/

ګوګل لټون – Google Search
https://support.google.com/websearch/troubleshooter/3111061?hl=en

ټیک ټاک – TikToK
https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/privacy-controls

ویکي پدیا:
که مو په ویکي پدیا یا د ویکي مدیا په نورو پروژو کې داسې کوم اطلاعات ومومئ چې کولی شي تاسو ته او یا په افغانستان کې نورو کسانو ته صدمه ورسوي، لطفاً د هغه په اړه له دغه ایمل ادرس سره په اړیکه کې شئ. ca@ wikimedia.org او د موضوع د عنوان په برخه کې AFG ورته ولیکئ.
د خپلو ملګرو د پروفایل یا مخینې یا کاوور عکس چک او مرور کړئ. او که هر کوم د دغو عکسونو درته د پوښتنې وړ وه،(د مثال په توګه: که د طالبانو پر ضد یې د یوه بیرغ یا بنر ښکارندینه کوله) له دوی وغواړئ چې بدل یې کړي. که پرې مشکوک وئ، بیا هغه د خپلو ملګرو له لیست څخه پاک کړئ.

- یو سیمه ییز اکونټ جوړ کړئ او یواځې د خپلو سیمه ییزو دوستانو لپاره مو وي، ترڅو په خپل تلفوني پروګرام کې د هغو په ساتلو سره له خپلو نړېوالو مخاطبینو سره له اړیکې مخ نیوی وکړئ. خپل اکونټ ترڅو چې ممکن وي عمومي یې کړئ، سیاسي او مذهبي مطالب مه خپروئ.
له یوه عمومي عکس څخه د پروفایل په توګه کار واخلئ او ممکن تاسو د دغه اکونټ لپاره یو مستعار نوم هم وکاروئ. خو پام وکړئ که خپل نوی حساب د تلفون له شمېرې سره وصل کړئ، ممکن د تلفون د شمېرې له لارې تعقیب شئ.

- ځان ډاډمن کړئ چې د اکونټ د معلوماتو څانګه مو د عموم لپاره د مشاهدې وړ نه ده. خپل اکونټ ته مو هېڅ ډول کاري سابقه مه وراضافه کوئ. ډاډ ترلاسه کړئ چې ستاسو پخوانۍ هېڅ ډول اړیکه چې له بهرنیو بنسټونو سره وه او یا ستاسو کاري سابقه په اکونټ کې د لیدلو وړ نه ده.

- که غواړئ له خپل نړېوال اکونټ څخه کټه واخلئ، یواځې داسې وخت هغه ته ورداخل شئ چې یا په امن ځای او یا هم په کور کې یاست. د هغه پاسورد په خپل لب تاپ او یا موبایل کې مه ذخیره کوئ.

- خپل فیسبوکي پستونه وڅېړئ (هر هغه شی چې په بلقوه توګه د اعتراض د رامنځته کېدو سبب ګرځېدلی شي، پاک یې کړئ.)، د دوستانو په نوملړ کې مو (هر هغه کس حذف کړئ چې کولی شي د شک د رامنځته کېدو سبب وګرځي په ځانګړې توګه بهرنیان.)، هغه صفحې او ګروپونه مو چې پخوا لایک/خوښ کړي هم وڅېړئ.

- د خپل فیسبوک خاصتاً د پروفایل او د مخینې عکس (کاوور فوتو) چک کړئ.
د دغو عکسونو ټول تنظیمات وڅېړئ هم د پخوانیو عکسونو په ګډون او مطمین شئ چې دا عکسونه پرته له ستاسو د اعتماد وړ دوستانو نور څوک نه شي لیدلی.
که کوم (سئوال پاروونکی) عکس لرئ، پاک یې کړئ.

- د دوستانو د لیست مشاهده مو محدوده کړئ، ترڅو نور کسان یې ونه شي لېدلئ. (او له ټولو دوستانو مو وغواړئ چې همداسې وکړي.) دا کار ستاسو د فیسبوک د تنظیماتو په برخه کې برابرېږي. |
“How People find and contact you / Who can see your friends list? / “Only me.

- خپل افغان وطنوال په فیسبوک کې مه تګ/tag کوئ.

- هغه بټنې چې کولی شي تاسو په عکسونو کې تګ کړئ، غیر فعاله کړئ.
https://www.hongkiat.com/blog/prevent-facebook-tagging/amp/

1. هغه پستونه او عکسونه چې ملګرو مو تاسو پخوا په کې تګ کړي یاست، مرور کړئ، که د ستونزې د جوړېدو سبب کېږي، تګ تري لرې کړئ.

ټویټر - Twitter
https://www.businessinsider.com/how-to-delete-old-tweets-from-twitter-2018-12

- فیسبوک ته ورته قواعد پر ټویټر او نورو ټولنیزو رسنیو هم پلي کېږي.
د هغه کسانو لیست چې تاسو فالو کوي/څاري وګورئ، هر څوک او یا هر ټویټ چې کولی شي د طالبانو مخالفت راوپاروي، د هغه لغوه او یا یې حذف کړئ.

5 خپله ډيجيتالي مخينه حذف کړئ او د انلاين فعاليت نښه مو کمه کړئ

دا لا نده روښانه چې ايا او څومره د دښمن ځواکونه د بشر حقونو د مدافعانو او د خبريالانو انلاين فعاليت څاري او که نه؟ دا وضعيت په سرعت سره د ودې په حال کې دی او د انلاين معلوماتو پاکول کولی شي موثر ووسئ.
https://news.trust.org/item/20210817111442-4d73x

دا ممکن په افغانستان کې ستاسو انلاين مصونيت او خوندیتوب ته صدمه رسوي. لاندې ځينې لارښونې د WIRED لخوا وړاندې شوي.
https://www.wired.com/story/how-to-clean-up-your-digital-history/

همداراز Human Rights First لاندې معلومات وړاندې کوي.
https://www.humanrightsfirst.org/sites/default/files/How%20to%20delete%20your%20history_updated.pdf

فارسي ښه يې :
https://twitter.com/dooley_dooley/statu s/1427223031429181441

پاملرنه:
- د دريم ډلې خدماتو ته د خپلو شخصي معلوماتو په ورکولو کې ډېر پام وکړئ.
- ځيني پلات فورمونه د معلوماتو د ساتنې پاليسي ګانې لري، چې د قانوني د اجرا لپاره حسابونه آرشيف کوي.
- ممکنه ده چې ستاسو حذف شوې ډېټا/معلومات لا هم په محلي کچه ستاسو په تلفون او يا کمپيوټر کې وساتل شي.

5.1

5.1 | څه ډول ټاکل شوي محتويات لکه عکسونه او پستونه پاک کړو او يا يې په خوندي توګه وکاروو.
لاندې يې په اړه فارسي لارښود دی: |
https://twitter.com/dooley_dooley/status/1427223031429181441

فيسبوک – Facebook
https://www.facebook.com/help/261211860580476/

- طالبان په فيسبوک کې پراخ حضور لري او ممکن له هغو د هغه کسانو چې ورسره په اشکارا ډول مخالفت لري او يا له بهرنيانو سره کار کوي او يا هم هغه کسان چې د ګټې اخستنې مناسبې سرچينې دي، د دوی د پېژندو په خاطر استفاده کړي.

- فيسبوک د اکونټ د قفل کولو لپاره داسې وسيله/ابزار جوړ کړي چې کولی شي په يوه کېکاږلو سره، ټول پروفايل قفل شي، ترڅو هغه کسان چې ستاسو ملګري نه دی، ونه توانيږي چې د پروفايل عکس او يا ليکنې دانلود کړي. |
https://twitter.com/ngleicher/status/ 1428474008295464965

4.3.

په خپل اکونټونو کې امنیتي تنظیمات چک کړئ.
وګورئ چې آیا تاسو کومو مهمو مواردو ته پام کړئ او که نه او هم د امنیتي خبرداري بټنه فعاله کړئ.
که امکان یې وه، تاسو د (2AF) اپشن/اختیار چې په بشپړ ډول ورته Factor-Authentication 2- وایي، هغه د هویت د تصدیق کولو په یوه پروګرام لکه freeOTP فعاله کړئ.:
https://freeotp.github.io/

او یا هم Aegis د Andriod لپاره (څکه په پاسورد سره د قفل کېدو قابلیت لري.)
https://getaegis.app/

او همدارنګه Raivo د iOS لپاره :
https://apps.apple.com/us/app/raivo-otp/id1459042137

ګوګل (په موبایل ټلفونونو کې) :
https://myaccount.google.com/security-checkup/
پام وکړئ، که تاسو خپل اکونټ د کوم تلفون له شمېرې سره وصل کړی وي، ستاسو اکونټ کېدای شي چې د تلفون د شمېرې له لارې تعقیب کړل شي.

فیسبوک :
https://www.facebook.com/help/799880743466869/
که تاسو د فیسبوک له مسنجر کار اخلئ دا ښه ده چې له (Secret Conversations) څخه کار واخلئ.

واتساپ :
https://faq.whatsapp.com/general/verification/how-to-manage-two-step-verification-settings/?lang=en

ټلګرام :
https://telegram.org/blog/sessionsand-2-step-verification
لاندې لینک د ټولو ایمل ادرس وړاندې کوونکو په اړوند اسناد دي.

https://2fa.directory/#email
ډاډه شئ چې ملاتړیز او بیاموندونکي کډونه مو له خپل تلفونه د باندې چېرې نوټ کړئ چې د تلفون د غلا، ماتېدو او یا هم د بطرۍ د ختمېدو په صورت کې خپل اکونټ بیا ترلاسه کړئ.

نور معلومات:
https://ssd.eff.org/en/module/how-enable-two-factor-authentication

4.4.

که غواړئ، چې د ناپېژنده پاتې کېدو لپاره، د تلفون شمېره نوې کړئ، او یا تلفون بدل کړئ. پام مو وي چې تل دواړه یو ځای سره بدل کړئ.
سره له دې چې دواړه په جلا جلا ډول خو په یو وار د تلفوني ټاورو لخوا پېژندل کیږي. (سیم کارت نمبر + د تلفون IMEI نمبر)، د یوه بدلول کفایت نه کوي ځکه دویم یې لا هم د پېژندنې قابلیت لري.

4

خپل انلاین اکونټونه، تلفون، تبلیت او کامپیوټر خوندي کړئ

4.1.

د تلفون یا د کامپیوټر د خلاصولو لپاره د داخلېدو رمز ته اړتیا لرئ د خپلې وسیلې لپاره د ټول دسک -رمز ورکونې بټن فعاله کړئ. (که فکر کوئ، د تاسو د وسیلې د پلټنې په صورت کې دا مورد پام ځان ته راجذبوي، د توجیه او د خپل موبایل یا لب تاب د امن کولو لپاره وار له مخه یو جوړ کړی داستان له ځان سره، ویلو ته ولرئ.) که چېرې د تالاشي له کوم ځای سره مخ شوئ، خپله وسیله خاموشه کړئ، او د نه پاملرنې په حالت یې پرېږدئ. که کله مو غوښتل چې د خپلې وسیلې (کامپیوټر/موبایل) رمز شریک کړئ او کنه نه؟ د معلوماتو لباره په دوهمه برخه کې شته نکاتو ته پام وکړئ.

4.2.

په بشپړ ډول کډ شویو برنامو لکه

واتساپ :
https://whatsapp.com
یا زیګنال :
https://signal.org
یا وایر :
https://wire.com

څخه استفاده وکړئ او د لیکلو پیامونو لپاره د پیامونو د ورکېدو بټنه فعاله کړئ او یا هم په منظم ډول خپل مسجونه پاکوئ.
پام مو وي، چې د زیګنال او وایر په شان پروګرامونه په معمول ډول نه کارول کیږي، او یا هم د سازمانونو او نړېوالو موسسو د غړو او یا د غیر دولتي بنسټو د استازو لخوا کارول کیږي، ممکن چې د پام د اوښتو سبب شي. سره له دې چې ممکن دا له واتساپ ډېر مصون هم وي.
خو د زیګنال لپاره په Andriod کې یو بدیل زیګنال میشته مسنجر شته، چې Molly یادیږي او ممکن ډېره توجه ځان ته را جلب نه کړي.
https://molly.im/

3

د ښځينه خبريالانو لپاره ځانګړې سپارښتنې

که تاسو د يوې ښځې په توګه تثبيت او وپېژندل شئ، ممکن تاسو له ځانګړو ډيجيتالي امنيتي ګواښونو سره مخ شئ. لاندې د ډيجيتالي حقونو د بنسټ لارښود ته پام وکړئ.|
https://digitalrightsfoundation.pk/wp-content/uploads/2017/11/Hamara-Internet-Guidebook-English-Version-2016.pdf

---

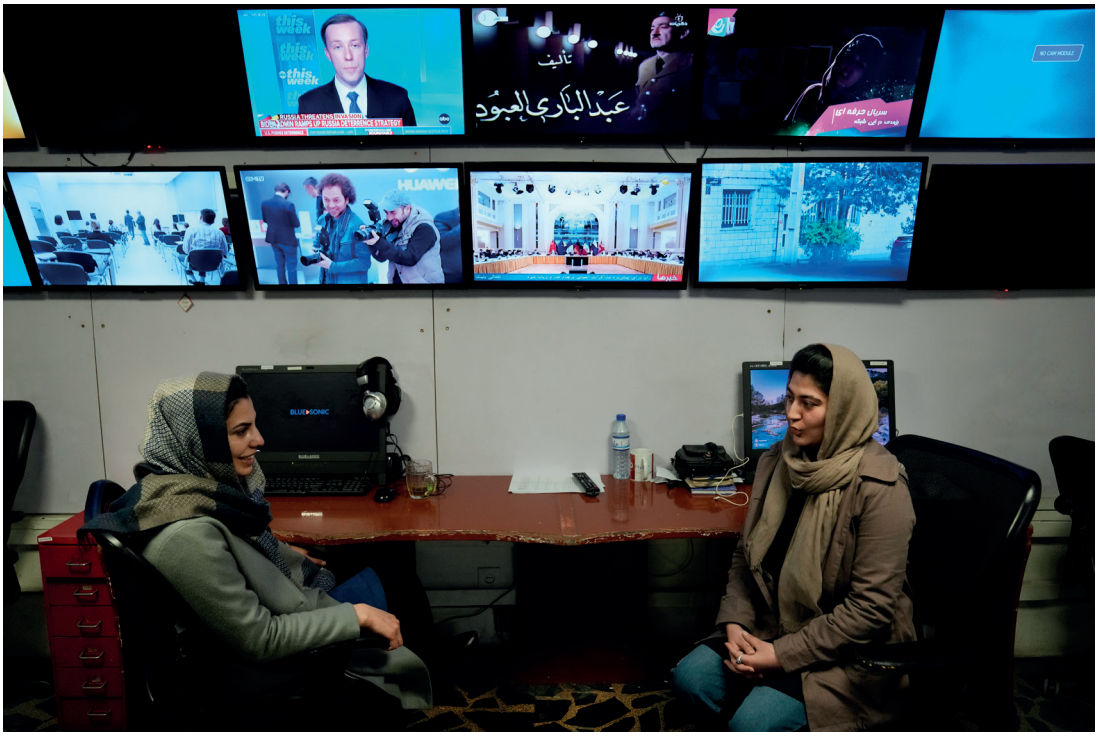
دا بنسټ همدا راز په پښتو ژبه چوپړتياوې وړاندې کوي.|
/https://digitalrightsfoundation.pk/services

د هغه ښځو لپاره چې له ناوړه استفادې سره مخ دي د Chayn لخوا د انلاين مصونيت يو لارښود جوړ شوی. دا لارښود په مختلفو ژبو دی.
/https://www.chayn.co

پښتو :
https://chayn.gitbook.io/diy-online-safety/pashto-p-tw

فارسي :
https://chayn.gitbook.io/diy-online-safety/farsi-farsy

انګليسي :
https://chayn.gitbook.io/diy-online-safety/english



—

په Genoa کې افغان کډواله ژورنالیست راحیل سیاح او همداراز افغان ډایرکټر، پرودیوسر او سکرین رایټر الوک امیری چې په روم کې د هزاره کانو د ټول وژنې په هکله جوړ شوي اعتراض کې ښکاري.

تصویر: ماتیو ناردون / Pasific Press

- یاداشتونه او غږیز یاداشتونه
- عکسونه
- پلټنه/ په ویب کې د پلټنې مخینه
- په یوټیوب کې ستاسو کتلې وېډیوګانې/ ګوګل اکونټونه
- په کامپیوټر او تلفون کې ذخیره شوي اسناد
- د VPN پروګرامونه
- د ګوګل/ او اپل مپ اطلاعات او د موقعیتونو مخینه (د اپل لپاره ځانګړي موقعیتونه، د ګوګل لپاره د موقعیتون مخینه)
- د تقویم برنامې – جنتري چې ممکن په کې د ننوتو حساس معلومات شامل وي
- د موزیک پروګرامونه (ځینې موزیکونه ممکن د سیاسي او مذهبي اړخه مناسب ښکاره نه شي.)
- د دوست موندنې پروګرامونه

پام مو وي چې پاک شوي توکي د خپل کامپیوټر/موبایل د باطله سطل نه هم پاک کړئ او دا چې د یو متخصص شخص یو تحلیل کولی شي چې د حذف/پاک شویو توکو اثار را پیدا کړي.

کله چې غواړی هر څه له تلفون نه پاک کړی، حداقل خپل ځینې شخصي تصویرونه وساتئ ترڅو ښکاره کړي چې له دې تلفون کار اخستل کېده.

2.3.

په خپل تلفون کې د اړیکو د شمېرو د خاوندانو نومونه پښتو او یا دري ته واړوئ، او وګورئ که اړتیا وه نړېوالې شمېرې له خپل موبایل پاکې کړئ.

- په ګرځنده تلفون کې مو شته ادرسونه، د مسنجر مخاطبین، او یا د خپل چت مخینه چې د بهرنیو نومونو او یا د ادرسونو ښکارندوی وي
- که غواړئ چې د مخاطبینو یو نوملړ یا ادرسونه درسره ولرئ، هغه په خپل تلفون او یا لب تاپ کې مه ساتئ! هغه خپل ځان ته په یوه ایمل در ولېږئ چې ستاسو اصلي ایمل نه وي. د هغه ایمل د خلاصولو کډ او ادرس په خپل لب تاپ یا تلفون کې مه درسره ذخیره کوئ او د هغو نښه په خپل وسیله که مه پرېږدئ. (د مثال په توګه: که تاسو له خپل اصلي ایمل بل ایمل ته پیام استوئ، لا به یې کاپي ستاسو د استونې به فولدر کې پاتې وي.)

- هر هغه ایمل چې درته زیان جوړولی شي، له خپل پیام خونې، د استونې له برخې، او یا د لومړني پړاو له برخې پاک کړئ او ډاډه شئ چې د باطلې فولدر مو هم پاک کړئ.

2.4.

د مسنجر او نورو انلاین ګروپونو لپاره: وار له مخه څو مختلف کسان د دغو ګروپونو د مدیرانو په توګه وټاکئ، ځکه د اړتیا په وخت د دغو ګروپونو مدیران کولئ شي یو غړی له ډلې حذف کړي.
(د مثال په توګه: که له چا یې تلفون مصادره شي.)

2.5.

د ټولنیزو رسنیو له لارې د اړیکو نیولو غوښتنو ته ځواب مه وایاست، که اړیکې ستاسو د ملګرو او یا د اعتمادي کانالونو له لورې نه وي. داسې پېښې شته چې یوه کس ځان بهرنی خبریال معرفي کړی دی او د مرکې غوښتنه یې کړې، خو بیا د ورکول شوي اطلاعاتو څخه یې منفي ګټه اخیستې او بیا یې د قرباني د تعقیب لپاره کاروي.

2.6.

د خصوصي شویو ایمل ادرسونو پر ځای له ترکیبي ایملونو څخه کار واخلئ، په دې مفهوم چې دا ایملونه ستاسو د نوم او محتویاتو بیانوونکي نه وي ترڅو په وسیله یې ستاسو هویت تشخیص نه شي.

2 د ډیجیتالي ببړني حالت، د نیونې او د تالاشي سیمې لپاره چمتو وسئ | یو پلان جوړ کړی

د انلاین مصونیت د تامینولو لپاره، دا تشخیص کړئ چې له څه ډول ګواښ سره مخ یاست او یا کوم انلاین فعالیت تاسو له خطر سره مخ کوي ـ د ګواښ نوعیت څه ډول دی؟ د ډیجیتالي امنیت په اړه دغه لاندې لینک تاسو سره مرسته کوي چې خپلو پوښتونو ته ځواب پیدا کړی.

https://www.accessnow.org/first-look-at-digital-security/

کله چې د ګواښ په اړه فکر کوئ، لطفاً دا لاندې مواردو ته هم پام وکړی.

2.1.

یو پلان جوړ کړئ او هغه د دې لپاره چې احتمال یې شته ممکن تاسو او یا هم له تاسو سره یو ارتباط لرونکی کس به د چارواکو لخوا ونیول شي. لاندې لارښود ته پام وکړئ.

https://digitalfirstaid.org/en/arrested/

دا د RaReNet او د CiviCERT لخوا ترتیب شوی او په کې د ډیجیتالي امنیت خوندیتوب په اړه معلومات په کې ځای پر ځای شوي دي.

همدا راز له زندان سره د مقابلې لارښود هم موجود دی.

https://coping-with-prison.org

دغه لارښود کې د نیول شوي شخص د کورنۍ غړو، د هغه ملاتړ کوونکو او وکیلانو لپاره معلومات را ټول شوي.

2.2.

2.2 | د تالاشي/پلټنې په ځایونو کې او د حملې پر مهال چمتو وسئ دا چې چارواکي به ستاسو (کامپیوټر او موبایل) مصادره کړي او یا به پر تاسو فشار راوړي ترڅو هغه ورته خلاص کړی. خپل تلفون له ځان سره د باندې مه وباسئ، او یا هم داسې یو تلفون درسره واخلئ چې حساس اطلاعات لکه د اړیکو شمېرې او یا ورته معلومات په کې نه وي. په خپلو وسایلو خاصتاً موبایل کې د ډېټا/معلوماتو د ذخیرې سطح ټېټې کچې ته راوړسوئ. – طلائي قانون دا دی: که شک کوئ، معلومات مو له لاسه یوسئ. هېڅ داسې معلومات د دې ارزښت نه لري چې په خاطر یې ستاسو او یا ستاسو د یوه ملګري ژوند له خطر سره مخ شي. (دلاندې نکات د محتویاتو او اکونټونو د له لاسه ورولو لپاره دي.)

>> پریکړه وکړئ چې آیا غواړئ چې خپلو وسایلو/دوایسونو ته لاس رسی ولرئ او که نه؟ دا به یوه ساده پرېکړه نه وي، خو ښه دا ده مخکې له دې چې ورسره مخ شئ په اړه یې فکر وکړئ. پام مو وي چې د تاسو د حضور په صورت کې ممکن دی ستاسو د ګوتې اثر او یا Face-ID د فشار په وسیله درباندې خلاص کړل شي. په iOS البته پخوانیو ایفونونو کې د ببړني حالت اختیار/اپشن شته چې څو ځله د پاور دکمې په فشار ورکولو سره ممکن د Face-ID او یا د ګوتې د اثر له مرحلې د رمز غوښتنې پرمخ ته ورداخل شي. همداراز په نویو ایفونونو کې په پیل کې د Emergency SOS په خاموشه کولو او د دوه ثانیو لپاره د غږ او یا د بغلې دکمې په هم مهاله کیکاړلو سره دا کار کیږي. له دې طریقې څخه د ګټې اخستنې لپاره ځان چمتو کړئ، که د هغو استفاده ته مو اړتیا درلوده.

هغه پروګرامونه/Apps چې تاسو او یا نورو ته د خطر سبب ګرځېدلی شي.

- ادرسونه/ د اړیکو شمېرې
- د مسنجر پروګرام
- د فیسبوک اکونټ
- ټویټر او د ټولنیزو رسنیو نور حسابونه
- ایملونه

1

د ډیجیټالي ښېړنیو حالتونو لپاره د تلفونونو ښېړنې کړښې

که تاسو یو خبریال، فعال او یا هم د مدني ټولنې غړی یاست او په عین وخت کې ښېړنې مرستنې ته اړتیا لرئ، Access Now`s Helpline درته په ۲۴ ساعته توګه د ډیجیټالي امنیت په برخه کې مرسته ترسره کوي.

نوټ: د ملاتړ ټیم به تاسو سره د افغانستان په سیمه ییزو ژبو خبرې ونه کړي.

نورا ختیارونه:

https://cpj.org/emergency-response/how-to-get-help

https://www.frontlinedefenders.org/emergency-contact

د ډیجیټالي حقونو بنسټ دا ډول قضیو ته د لاندې ادرس له لارې ځواب وایي.

helpdesk@digitalrightsfoundation.pk

که ګمان کوی چې ستاسو پر تلفون د Spyware په وسیله او دې ته ورته پروګرامونو باندې حمله شوې، Emergency VPN د Civilsphere پروژې له لارې درسره مرسته کوي ترڅو خپل تلفون چک کړی او وپاکوئ:

https://www.civilsphereproject.org/emergency-vpn

خطر	د مخ نیوي مرحلې	د ځواب ویلو مرحلې	ملاحظات
د حملې، پلټنې، نیونې او د تالاشي پر مهال د موبایلونو، تبلیټونو، کامپیوټرونو او د ځیرک لاسي ساعتونو مصادره او یا هغوی ته لاس رسی پیدا کول.	▪ زمونږ په Device (کامپیوټر/ موبایل) کې د معلوماتو یا ډیټا د ساتنې کچه نا محسوس خو واقعبینانه حداقل ته را ټیټول ▪ زمونږ په Device کې د معلوماتو یا ډیټا مصون او خوندي کول ▪ د وسایلو مصون کول ▪ اټولې ډیټا یا معلوماتو ته د کډ لرونکي Backup جوړول	▪ وسایلو(کامپیوټر/موبایل) ته نه لاس رسی ▪ له لرې لارې د دستګاه پاکول او یا Device ته د داخلیدو د بې پایلې هڅې په نتیجه کې په اتوماتیک بنه د کامپیوټر/موبایل پاک کول ▪ متاثر کیدونکي او احتمالي خطر سره د مخ کسانو خبرول ▪ د معلوماتو او اکونټونو بیا موندنه او بېرته ترلاسه کول	▪ امهمه پرېکړه کول آیا تر فشار لاندې به اجازه ورکړئ چې ستاسو وسیلې (کامپیوټر/موبایل) ته لاس رسی ترسره شي؟ ▪ په پام کې مو وي چې ایا کډ لرونکی ملاټر (Backup) او یا کډ لرونکي فایلونه توجه ځان ته راجلبوي او ایا تاسو به له خطر سره مخ کړي؟
د ډیجیتالي اړیکو او انلاین ارتباطاتو نظارت/ څارنه (البته د چارواکو، د هغوی د متحدینو، د انټرنټي خدماتو وړاندې کوونکو او مخابراتي شرکتونو لخوا)	▪ د انلاین اکونټونو خوندی کول ▪ له انلاین خوندي خدمتونو ګټه اخیستنه (لکه بشپړ کډ شوي مسنجرونه، انلاین ذخیره کول، لټونونه، ویډیو کنفرانسونه او داسې نور) ▪ د VPN او یا د ورته ابزارو له لارې انټرنټ ته زمونږ د لاس رسي خوندي کول	▪ د امکان په صورت کې د ترسره کېدونکي نظارت/څارنې په اړه اسناد را ټول کړئ ▪ د خدماتو وړاندې کوونکو له لوري د ناوړه کټې اخستنې د حفاظت د میکانیزمونوفعالهکول ▪ متاثره او متضرر کېدونکي اکونټونه Backup او غیر فعاله کړئ	▪ مصون او خوندي پروګرامونه او یا چینلونه لکه VPNs ممکن دی، پام ځان ته راجذب کړي او د ګواښ د رامنځته کېدو سبب شي
پر ډیجیتالي وسایلو او اکونټونو حملې (د جاسوسۍ وسیلې، هک کوونکې حملې، د چارواکو او یا د هم مجرمانو له لوري د شواهدو ځای پرځای کول.)	▪ د دستګاو خوندي کول ▪ د انلاین اکونټونو خوندی کول ▪ د اجرایي سیستم او پروګرامونو اپډېټ کول ▪ د ټولنیزو شبکو له لارې د ناپېژنده اړیکو د غوښتنې ردول	▪ حملې او ټول شواهد مستند کړئ ▪ حمله شوې دستګاه خاموشه وساتئ ▪ اکونټونه مو د خدماتو د وړاندې کوونکو او یا د بېړنۍ مرستې د غوښتنې د خطونو له لارې ترلاسه کړئ. ▪ د بیا ترلاسه شویو اکونټونو لپاره مو د 2FA اپشن/اختیار فعاله کړئ	
د خلاصې سرچینې اطلاعات (اوسنت)	په مختلفو پلاټفورمونو کې کله ټټون چې په عمومي شکل د لاس رسي وړ وي. (لکه فیسبوک او وکي پدیا)	▪ د معلومات په لمنځه وړلو او یا له نورو پلاټفورمونو څخه د اطلاعاتو د لرې کولو په غوښتنې سره په دیجیتالي فضا کې دخیل نښان د پاتې کېدو کچه کمه کړئ	▪ هڅه وکړئ چې له انلاین پلاټفورمونو شواهد لمنځه یوسئ	▪ متوجه وسئ، چې ډېرې معلومات به په بشپړ ډول لمنځه نه ځي، او که داسې وشي هم نو یواځې په وېشل شوي ملاټر کې د ځنډ او د پلاټفورمونو د بېا راګرځېدو ماشین او د ذخیره کوونې د نورو خدماتو له امله به وي.

پاملرنه کول، یعنی مقاومت کول دي.

" ځان ته پاملرنه کول، زیاده غوښتنه نه ده، بلکې د خپل ځان د خوندي ساتلو په مفهوم ده، او دا د سیاسی جګړې یوه کړنه ده." (اودره لرده)

خپلو وسایلو(کامپیوټر/موبایل) او ډېټا یا معلوماتو ته پام کول، نه یواځې د خپل ځان خوندي ساتنه ده، بلکې د ټولې ټولنې د خوندي ساتنې په مفهوم ده.

خبریالان، د رسنیو کارکوونکي او فعالان خپل ژوند له ګواښ سره مخ کوي، که د دوی له انلاین ډېټا/معلوماتو، برنامو، او اړیکو څخه د هغوی او یا د بل کس په وړاندې چې له دوی سره په اړیکه کې دي، د شواهدو په توګه کار واخستل شي.
امکان لري، چې دا ډول ډېټا یا معلوماتو، برنامو او داسې نورو مواردو ته لاس رسی ترسره شي.
همدارنګه ممکنه ده، چې کله هم دا لاندې سناریوګانې رامنځته شي.

- د حملې، لټونې، نیونې او د تالاشي پر مهال د ټلفونونو، ټبلیټونو، کامپیوټرونو، د ځېرک ساعتونو او د نورو بیا ترلاسه کېدونکو(USB ګانو، هارډسکونو، او نورو ځېزونو) مصادره کول او هغوی ته لاس رسی پیدا کېدل.

- د ډیجیټالي ارتباطاتو او انلاین اړیکو څارل کېدل
- پر وسایلو(کامپیوټرونو/موبایلونو) او اکونټونو د ډیجیټالي حملو ترسره کېدل
- د خلاصې سرچینې اطلاعات | پر هغو پلاټفورمونو تحقیق کول چې په عام شکل ورته لاس رسی کیږي، لکه: فیسبوک او ویکي پدیا

د دې په پوهېدو چې نه شو کولی له ټولو متوجه ګواښونو مخ نیوی وکړو، خو د ځینو ځانګړو اقداماتو په ترسره کولو سره لکه په خپلو وسایلو(کامپیوټر او موبایل) کې د کمو معلوماتو په ځای پر ځای کولو، د اړیکو له خوندي کانالونو څخه د کار په اخیستلو او د خپلو وسایلو په مصون کولو سره کولی شو دا احتمال چې یاد ډېټاوې او پروګرامونه زمونږ په وړاندې د شواهدو په توګه وکارول شي، کم کړو.
په عین وخت کې، ځینې دا خوندي اقدامات به په ګواښ هم بدل شي، که چېرې زمونږ انلاین پروګرامونه له غلط لوبغاړو (نړېوالې ټولنې او یا هغه ته ورته سازمانونو) سره د مرتبطو شاخصونو په توګه په پام کې ونیول شي.

6 د موبایل او یا کامپیوټر دې ورکېدو په صورت کې څه وکړو

7 خپل اکونټ/حساب بیا ترلاسه کړئ

8 VPNs: د جاسوسۍ، حملو او سانسور په وړاندې ساتنه

9 په خوندي او مصون توګه ویډیو کنفرانس

10 په خوندي توګه د فایلونو شریکول او په انلاین بڼه یې ذخیره کول

ستاسو د پاملرنې وړ: کوم معلومات او منابع چې دغه ډیجیتالي لارښود کې ځای پر ځای شوي، د ۲۰۲۲ کال د مې میاشتې له راهیسې دي او د دوه کلونو لپاره به په هر شپږو میاشتو کې اپدیت یا نوي کیږي. د معلومات نوې شوې بڼه له دغه آدرس څخه دانلود کولی شئ:
https://helpdesk.rsf.org/digital-security-guide/afghanistan-digital-care-guide/

پاملرنه کول، یعنی مقاومت کول دي

1

د ډیجیتالي ببړنیو حالتونو لپاره د تلفونونو ببړنۍ کرښې

2

د ډیجیتالي ببړني حالت، د نیونې او د تالاشي سیمې لپاره چمتو وسئ | یو پلان جوړ کړی

3

د ښځینه خبریالانو لپاره ځانګړې سپارښتنې

4

خپل انلاین اکونټونه، تلفون، تبلیت او کامپیوټر خوندي کړئ

5

خپله ډیجیتالي مخینه حذف کړئ او د انلاین فعالیت نښه مو کمه کړئ

دافغانستان

لپاره د ډیجیتالي مصونیت لارښود

برای دستیابی به نسخه دیجیتالی این رهنمود لطفا" کد QR را اسکن کنید.

https://helpdesk.rsf.org/digital-security-guide/afghanistan-digital-care-guide/

REPORTER OHNE GRENZEN

- این هایکه تجارتی هستند ممکن باعث جلب توجه کمتر باشد:

20) https://mega.io جی.بی رایگان)
5) https://sync.com m جی.بی رایگان)
https://cryptpad.fr/drive
نام ممکن باعث جلب توجه شود!!!

OnveDrive، Google Drive و iCould نوعیت رمزگذاری سرتاسری را ندارند. بناً این سرورها قادر به مشاهده آنچه اپلود کرده اید، هستند، اما اگر شما آن را از قبل حفاظت نکرده باشید. (به طور مثال: استفاده از فایل با ZIP رمزگذار شده یا موارد مشابه.)

ممکن نیاز داشته باشید که تا اسنادی را در جای ذخیره کنید.(مانند: کاپی پاسپورت های اعضای خانواده، قراردادهای کاری شما، اسناد که مستند کننده خطری باشد که شما با آن مواجه شده اید.)

بهترین کاری که برای ذخیره سازی امن اسنادهایتان انجام داده می توانید اینست که آن را در یک فضای ابری مصون ذخیره کنید که با ایمل اصلی شما استفاده نمی‌شود. یا هم آن را به یک ایمل آدرس مصون دیگری ارسال کنید که شما می‌توانید به آن دسترسی داشته باشید و حساب کاربری اصلی شما نیست و در تلفون و یا هم در کامپیوتر تان ذخیره نشده است.

اکادمیسن‌ها/محصلین کسانی که ضرورت به مصون سازی اسناد و یا معلومات حساس دارند، می‌توانند از طرح Article 26 Backpack که توسط پوهنتون کالفورنیا داویس ارائه شده استفاده کنند. اسناد در فضای ابری ذخیره خواهند شد. رهنمایی استفاده از آن به زبان‌های انگلیسی و دری در لینک ذیل قابل دسترس است.
https://human-rights.ucdavis.edu/news/afghanistan-emergency-resource-information

یا هم به زبان دری:
https://backpack.ucdavis.edu/?language=fa

این دستورالعمل بر مبنای مصاحبه ها با خبرنگاران افغان و همچنین با در نظرداشت رهنماهای ذیل ساخته شده است:

1 منابع مصونیت آنلاین برای مدافعان حقوق بشر افغانستان
https://www.accessnow.org/online-safety-resources-afghanistan
EN

2 چک لیست برای افغان ها کاهش خطر از طریق دیتا/ داده های تلفون‌ها/دستگاه‌ها (20 اگست 2021)
https://docs.google.com/document/d/19GPJDmMLPagNnbumZwmKZGJaliRMFmHiJKtuvmL6wl8/edit
EN, Dari, Pashto

3 منابع امنیت دیجیتالی برای افغانستان: قطع شدن انترنت و حریم خصوصی آنلاین
https://drive.google.com/drive/folders/1v9WvDvoCPjP13Y2Lsd0hqwDt6mqEgvtW
EN, Dari

10 به اشتراک گذاری مصون فایل و ذخیره سازی آنلاین

برای ذخیره کردن اسناد به شکل مصون در کامپیوتر و یا هم امن ساختن (رمزگذاری) فایل ها قبل از به اشتراک گذاری و یا ذخیره آنلاین، برنامه Veracrypt اجازه میدهد تا پوشه‌های رمزگذاری شده را در سخت افزار و یا به شکل آنلاین، در Google Drive یا در Dropbox ذخیره کنید و به دیگران به شکل عادی و یا فایل های سیستم کامپیوتری به نظر می رسد.

https://veracrypt.fr

پس از استفاده Veracrypt برای رمز گذاری سند به این شکل، پس از آن برنامه را حذف کنید به شمول حذف کردن از Trash دستگاه تان، تا اینکه برنامه باعث جلب توجه نشود. اینکه از Veracrypt چگونه استفاده کنید به این ویدیو که زبان انگلیسی با زیر نویس فارسی است توجه کنید.

https://youtu.be/C25VWAGl7Tw

10.1. اشتراک گذاری فایل گزینه های (سر تا سر رمز گذاری شده)

https://ufile.io

- برای کابران راجستر ناشده: نهایتاً 10 فایل (5 گیگابایت برای هر فایل)، با یک ماه میزبانی رایگان

https://send.tresorit.com

- برای استفاده کننده های راجستر ناشده قابلیت استفاده تا 5 گیگابایت

https://send.tresorit.com

- اپلود تا به 50 میگابایت می‌باشد و فایل ها تا بیشتر از 12 ساعت در آن ذخیره نمی‌شوند.

https://cryptpad.fr/drive

- ثبت نام به شکل ناشناس لازم است. تا یک جی.بی میزبانی یا هاستینگ رایگان دارد. نام ممکن است جلب توجه نمائید!!!

اگر شما مرورگر Tor را استفاده می‌کنید. :

https://www.torproject.org

یا هم OnionShare:

https://onionshare.org

10.2. ذخیره سازی آنلاین

- برای ذخیره سازی آنلاین تنها و تنها از مرورگر های استفاده کند، نه از برنامه های نصب شده در دستگاه (کامپیوتر/موبایل)!

اگر شما برای دسترسی ابری – Could Access از سرور سازمان تان استفاده می‌کنید. متوجه باشید که UR/Link استفاده شونده ممکن است نام سازمان را نشان بدهد و ارائه دهنده‌گان خدمات انترنتی شما می‌توانند آن را ببینند. در این قسمت استفاده از VPN خطر را کاهش می‌دهد.

9 برگزاری ویدیو کنفرانس مصون

مسنجرها/ پیام رسان‌هایکه زمینه تماس‌های ویدیویی مصون را فراهم می‌سازد. در نظر داشته باشید، که استفاده از زیگنال و وایر به دلیل اینکه در اجتماع شما احتمالاً کاربرد بیشتر ندارد، ممکن باعث جلب توجه شود.

- زیگنال :

https://signal.org

1. تماس های ویدیویی رمزگذاری شده سر تا سر را برای حداقل هشت اشتراک کننده همزمان فراهم می سازد
2. وابسته به شماره تماس موبایل همراه تان می‌باشد

- وایر :

https://wire.com

1. تماس های ویدیویی رمزگذاری شده سر تا سر و قابل دسترسی برای تا به چهار اشتراک کننده(نسخه رایگان)
2. امکان داخل شدن بدون داشتن شماره تماس تلفون همراه را دارد

- واتساپ :

https://whatsapp.com

1. تماس های ویدیویی رمزگذاری شده سر تا سر و قابل دسترسی با به چهار اشتراک کننده
2. بخشی از میتا-کمپنی (قبلاً فیسبوک، بنابراین میتا-دیتا قرار است گرفته شود.)

جتسی میت- JitsiMeet :

- تماس های تصویری برای تا به 25 مخاطب در سرورهای قابل اعتماد
- استفاده بدون هزینه
- در کامپیوترها دسترسی از طریق مرورگر امکان پذیر است، برنامه‌ها برای Andriod و iOS وجود دارند
- ارائه کننده‌گان قابل اعتماد :

https://meet.greenhost.net
https://meet.systemli.org

رهنمای استفاده مصون:

https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools

https://www.frontlinedefenders.org/en/resource-publication/jitsi-meet-simple-and-secure-video-conferencing-platform

---

دانلود اپلیکیشن برای تلفون ها:

https://jitsi.org/downloads

اگر نیاز به استفاده از ابزارهای کنفرانس مانند https://zoom.us داشتید، مطمئن شوید که ویژگی رمزگذاری end-to-end را فعال کرده اید. :

https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings

---

- تورر – Tor :

یک مرورگر برای ناشناس بودن بلقوه است، که از شبکه Tor برای ناشناس باقی ماندن و دور ساختن سانسور انترنتی استفاده می‌کند.

https://www.torproject.org/download/

(Windows, MacOSX, Linux, iOS, Android)

از طریق ایمل آن را دانلود کنید:

به GetTor (gettor@torproject.org) یک درخواست بفرستید با مشخص سازی سیستم عامل تان و(منطقه تان). به طور مثال: "windows fa"

- مرورگر اونیون – OnionBrowser (iOS) :

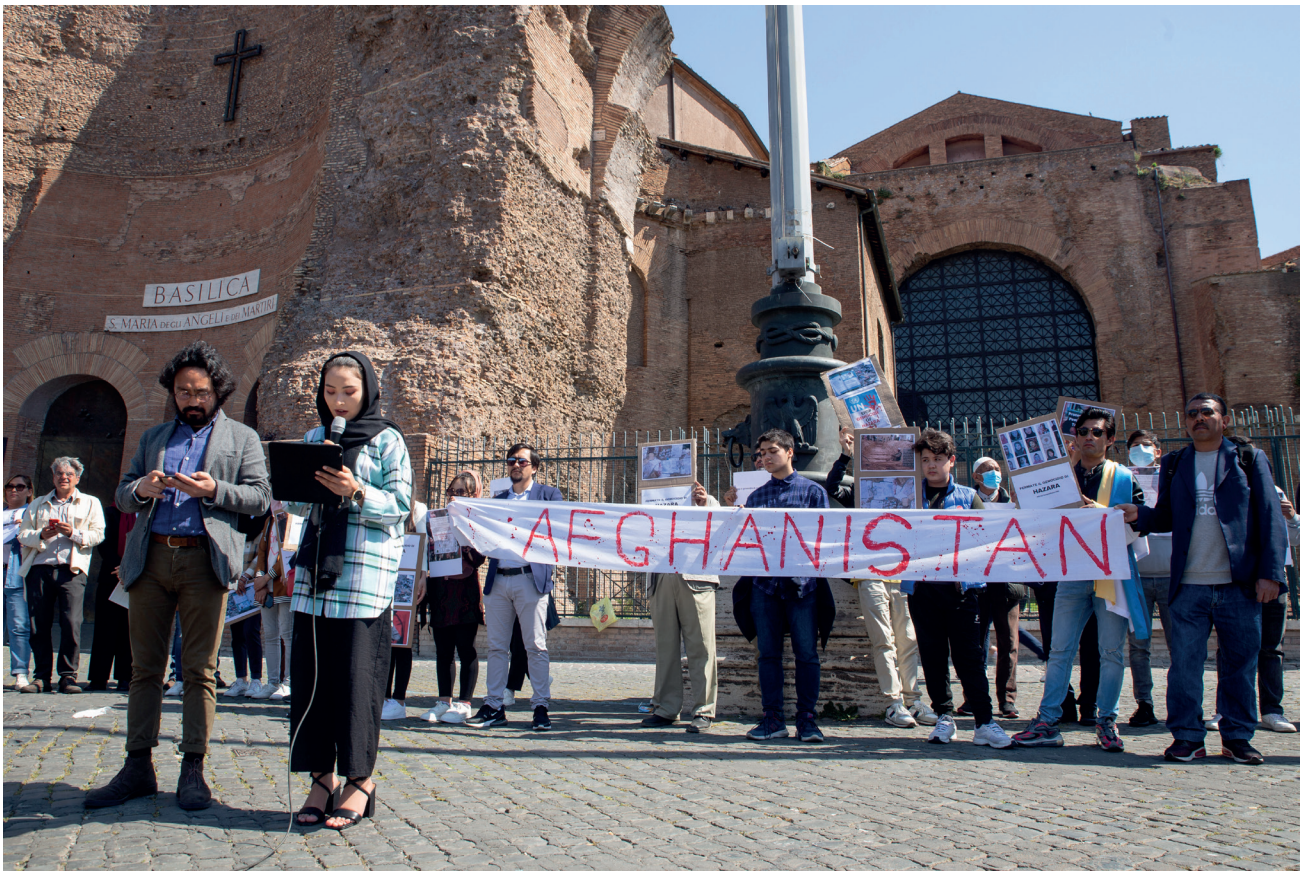
https://onionbrowser.com

https://apps.apple.com/us/app/onion-browser/id519296448

—

راحیل سیاح، ژورنالست مهاجر افغان در Genoa و الوک امیری، دایرکتر، سکرین رایتر و پرودیوسر افغان در اعتراضی در روم اند که در برابر جینوساید مردم هزاره برگزار شده بود.

عکس: متیو ناردونه/ Pascific Press



- وی.پی.ان.گیت – VPNGate :

https://www.vpngate.net/

(Windows, MacOSX, Linux, iOS, Android)

یک لیست از سرورهای عمومی VPN دریافت و ارسال که توسط رضاکارانی از سراسر جهان میزبانی شده.

- پروتون وی.پی.ان – ProtonVPN :

https://protonvpn.com/

(Windows, MacOSX, Linux, iOS, Android, Chromebook)

به شکل رایگان قابل دسترس است.

- بیت ماسک – Bitmask :

https://bitmask.net/

(Windows, MacOSX, Linux, Android)

این VPN یک منبع باز است. شما می‌توانید از VPN های از قبل تهیه شده توسط ارائه دهنده (riseup.net) یا (calyx.net) استفاده کنید و یا هم خودتان یکی را راه اندازی کنید.

بسیاری از VPN های دیگر نیز قابل دسترس هستند، اما تمامی آنها تلاش های موثر برای فرار از سانسور یا داشتن امنیت بهتر، حفظ حریم خصوصی و یا رفتارهای تجارتی خوب نداشته اند. اگر به دنبال امتحان گزینه های بیشتر هستید، نگاه بر این آدرس آغاز خوبی بوده می‌تواند:

https://www.nytimes.com/wirecutter/reviews/best-vpn-service

- برای چگونگی فعالیت VPN ها، اینکه آنها چی انجام می‌دهند و یا هم با کدام موارد کمک کننده نیستند؟ این یک منبع خوبی بوده می‌تواند:

https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

لطفاً توجه داشته باشید که اکثراً (نه همه) سایت های مرور VPN از خرید VPN ها سود می‌برند و یا هم مرتبط به همان شرکت های هستند که مالک VPN ها می باشند.

ابراز های مختص برای ضد سانسور:

یک ارزیابی انجام دهید که این برنامه‌ها آیا باعث ایجاد خطر برای شما خواهد شد. (مثل: جلب توجه)، اگر آنها در دستگاه شما به شکل نصب شده دریافت شوند و یا هم این کشف شود که شما از آن استفاده می‌کند.

Psiphon یک VPN برای دور ساختن سانسور منبع باز است که از تکنیک های مختلف برای دور ساختن سانسور انترنت استفاده می‌کند.

https://www.psiphon3.com/en/download.html

(iOS, Android, Windows)

- دانلود از طریق ایمل:

یک ایمل به آدرس (get@psiphon3.com) بفرستید تا لینک های دانلود Psiphon را با چندین زبان دریافت کنید.

- لاترن – Latern :

این یک VPN دور ساختن سانسور برای منبع باز است که از روش های مختلف برای دور ساختن سانسور انترنتی استفاده می‌کند.

https://getlantern.org/en_US/index.html

(Windows, MacOSX, Linux, iOS, Android)

8

VPNs: محافظت در برابر جاسوسی، حملات و سانسور

VPNها باعث ایجاد یک تونل رمزگذاری شده بین دستگاه (کامپیوتر/موبایل) شما و خروجی های ارائه شده از طریق VPN می‌شود. بنابر این تنها زمینه دستیابی به ویب سایت های را که مسدود و یا سانسور شده را برایتان می‌دهد بلکه از فعالیت و ترافیک شما در فضای انترنتی به منظور جلوگری از نظارت شدن حفاظت می‌کند.

- اگر قبلاً از VPN استفاده نموده اید، با همان یکی به کار خود ادامه دهید. اما بررسی کنید که درست کار می‌کند. درغیر این صورت از VPN جدید استفاده کنید، و این کار ممکن باعث جلب توجه شما شود! بررسی کنید که کدام VPN ها بیشتر برای پنهان شدن در بین جمعیت موثر است.
- این همه زمانی کارا خواهد بود، که شما قبل از اینکه سانسور اتفاق بیفتد و یا هم شبکه خاموش ساخته شود، آن را دانلود کنید. استفاده از این ابزار ممکن است اغلب توسط ارائه دهنده انترنت شما شناسایی شود و به عنوان برنامه‌های نصب شده در تلفون همراه تان، قابل مشاهده برای هر کسی باشد که به تلفون قفل نشده شما نگاه می‌کند.
- پس انستال و اجرا، یکبار بررسی کنید که VPN به درستی کار میدهد:
https://ipleak.net

VPN های ضد سانسور با سابقه خوب:

- تیونل بییر – TunnelBear :

https://www.tunnelbear.com/download
(Windows, MacOSX, Linux, iOS, Android)

یاداشت: تیونل بییر برای فعلآ به کابران در افغانستان ماهانه تا 10 جی.بی استفاده رایگان است. در گوگل آپ ستور قابل دسترس نیست، اما کابران می‌توانند یک APK را از کانال رسمی تلگرام دانلود کند.
https://t.me/tunnelbearofficial

اگر افراد در استفاده از تیونل بییر با مشکل مواجه شوند، می‌توانند آنرا گزارش کنند:
https://forms.office.com/Pages/ResponsePage.aspx

- مولواد – Mullvad :

https://mullvad.net/en/download
(Windows, MacOSX, Linux, iOS, Android)
قیمت ماهانه 5 یورو؛ مجوزهای استفاده از خطوط کمکی مانند (help@accessnow.org) قابل دسترس است، روش خرید به شکل ناشناس و بدون ثبت نام نیز صورت می‌گرد. همچنین در کنار ارز دیجیتالی می‌تواند برای خرید آن از پول نقد استفاده کرد.

7

حساب کاربری/ اکونت تان را بازیابی کنید

اکثری سکوهای رسانه های اجتماعی، خدمات ایمل و دیگر سایت ها منابع دارند که برای بازیابی حساب شما برایتان کمک می‌کند. بیشترین سکوها/پلاتفورم ها به طور معمول راه های برای گزارش دهی فعالیت های غیر معمول اکونت ها دارند. ما چندین رهنما را در ذیل لیست کردیم. همچنین این رهنمایی کمک های اولیه را ببنید:
https://digitalfirstaid.org/en/topics/account-access-issues

بازیابی گوگل :
https://support.google.com/accounts/answer/183723

گزارش کردن فیسبوک :
https://www.facebook.com/hacked
بازیابی فیسبوک :
/https://www.facebook.com/notes/10157814523321886

مراحل حمایت برای انستاگرام :
https://help.instagram.com/149494825257596

مراحل حمایت برای تویتر :
https://help.twitter.com/en/safety-and-security/twitter-account-hacked

---

6 اگر دستگاه (کامپیوتر/موبایل) خود را گم کردید، چی باید کرد

اگر چنین اتفاق بیفتد، خیلی مهم است که باید به طور عاجل وارد عمل شوید و بتوانید خطر دسترسی یکی را به حساب کابری/اکونت، مخاطبان و معلومات شخصی تان کاهش بدهید.

رهنمایی کمک های اولیه دیجیتالی ما را ببنید.

https://digitalfirstaid.org/en/topics/lost-device

چون یاد بگیرد که خطر را چگونه ارزیابی کنید و در مرحله بعدی چی کار باید بکنید.

6.1.

اگر امکانش وجود دارد، تلفون را از راه دور قفل و پاک کنید.

اندوراید – Andriod :
https://support.google.com/accounts/answer/6160491?hl=en
سامسونگ – Samsung :
https://www.samsung.com/za/support/mobile-devices/how-do-i-use-find-my-mobile-to-remotely-wipe-my-samsung-galaxy-s6-edge-plus/
آیفون – iPhone :
https://www.igeeksblog.com/how-to-erase-data-from-lost-stolen-iphone-ipad-remotely

6.2.

شماره تماس تلفون گم شده را از گروپ های رسانه‌های اجتماعی خود حذف کنید. (به منظور جلوگیری از اینکه شخصی دریافت کننده تلفون قادر به دسترسی به این گروپ‌های رسانه های اجتماعی شما نشود.)، برای انجام این فعالیت از قبل باید چندین مدیر مختلف برای چت ها داشته باشید، چون افراد مختلف/مدیران می‌تواند به راحتی این شماره را حذف کند.

- Whatsapp
- Signal
- Telegram

6.3.

تمام رمزهای عبوری برای حساب های متاثر شده را تغییر بدهید، (به شمول ایمل های بازیابی/ یا تنظیم دوباره) و 2AF را برای تمام اکونت ها که قابلیت آن را دارد فعال بسازید.

6.4.

مخاطبین خود را در مورد گم شدن تلفون تان اطلاع دهید و همچنان آنها را از خطر متوجه برایشان مبنی بر سوی استفاده شان توسط فرد که تلفون شما را پیدا کرده است و به آن دسترسی دارد، آگاه سازید.

https://twitter.com/dooley_dooley/status/1427223031429181441
حذف محتوای واقعی سایت را درخواست کنید: حذف نتیجه جستجو باعث حذف محتوا نمی شود. برای حذف اطلاعات خود از آن سایت باید با صاحب هر سایت در تماس شوید.

در یوتیوب و گوگل

- بخاطر داشته باشید اگر شما در یوتیوب ویدیو جستجو می‌کنید، این ممکن در حساب کاربرِ گوگل تان در تلفون هم نمایش داده شود. (این دو حساب معمولاً با هم وصل هستند.)

- به طور منظم سابقه جستجو در یوتیوب و اکونت گوگل تان را حذف کنید.
برای چگونگی حذف فعالیت های گوگل به لینک ذیل مراجعه کنید.
https://support.google.com/accounts/answer/465

این رهنمای «افشای خودی» - Self-doxing Guide
https://guides.accessnow.org/self-doxing.html
ممکن است برای درک اینکه چقدر اطلاعات در مورد شما به شکل عموم در دسترس است و به حداقل رساندن چیزهایی که می تواند شما را در معرض خطر قرار دهد، مفید باشد، به ویژه برای فعالانی که بازداشت شده اند و در مورد نظراتشان مورد سوال قرار گرفته اند.
امکان دارد به زودی بخاطر چیزهایی که پست کرده اید یا بر اساس شبکه هایتان هدف واقع شوید.
https://twitter.com/BBCWomansHour/status/1427287851016798213

اگر شما در سایتی معلومات حساسیت برانگیز خاصی را دریافتید و قادر به حذف آن از ویب سایت شدید، همچنین URL صفحه مخصوص را که معلومات در آن قرار داشت را اینجا نیز وارد کنید.
https://archive.org/web
اگر کاپی آرشیف شده آن موجود بود، پس برای کمک به این آدرس تماس بگیرد.
help@accessnow.org
https://cpj.org/2019/09/digital-safety-remove-personal-data-internet/

جستجوی آنلاین و خدمات دریافت افراد:
https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List

https://www.eff.org/deeplinks/2020/12/doxxing-tips-protect-yourself-online-howminimize-harm

5.3.
نحوه برخورد ما با عکس ها

- مطمین شوید که همه عکس های موجود در موبایل خود را دیده اید و میدانید که هیچ عکس که دردسر ساز باشد وجود ندارد. (مانند: عکس خودتان با پرچم امریکا، شما با خارجی‌ها، یا زنان بدون حجاب و یا شما با اعضای خانواده تان در خارج از کشور.)

- اگر شک دارید، حذف اش کنید. این قابل درک است که حذف چنین عکس ها برایتان دشوار خواهد بود، اما بخاطر داشته باشید که آنها به شکل بلقوه شما و یا دیگران را با خطر مواجه می‌کند.

- اگر می‌خواهید که آنها را با خود داشته باشید، آن عکس ها را در فضای ابری یا Cloud اکونتی ذخیره کنید، که حساب اصلی شما نباشد، نام و رمز عبوری آن نیز قبلآ هیچ جای ثبت نشده باشد و سپس از تلفون تان حذف اش کنید. ببینید به طور مثال: Google Drive چیست و چگوه استفاد می‌شود؟ * ویدیویی انگلیسی با زیر نویس فارسی*
https://youtu.be/EbVnObwFJic

- برخی از برنامه‌ها وجود دارد که این امکان را به شما فراهم می‌سازد تا عکس‌های تان را در پوشه (فولدر) فریب دهنده یا به ظاهر برنامه‌های دیگر(مثل ماشین حساب مخفی یا البوم عکس خصوصی) پنهان کنید. اما بخاطر داشته باشید این روش مصون نیست چون دیگران نیز در مورد چنین برنامه‌ها اطلاع دارند.

5.4.
جستجوی آنلاین – گوگل – یوتیوب

قبل از جستجو در ویب سایت‌های که می‌تواند ضد طالبان به نظر برسند:

- حالت مرورگر- جستجوگر خصوصی را در مرورگر فعال کنید
- اگر امکان داشت Cookies را نپذیرید
- بوک مارک‌ها/ نشانک ها را ذخیره نکنید
- دیتا/معلومات وروردی یا پاسورد تان را ذخیره نکنید
- از ورود به وب‌سایت‌ها با Google یا Facebook خوداری کنید یا آن را به یک حساب وب‌سایت شخص ثالث وصل نکنید

در عموم:

- کوشش کنید که از مرورگر های (مثل: موزیلا فایرفاکس) را استفاده کنید که از حریم خصوصی شما محافظت می‌کند و تنظیمات حریم خصوصی بیشتر را فعال می‌کند.

- اطمینان حاصل کنید که یک سابقه از ویب سایت های مصون را که بازدید کرده اید، ایجاد کنید. (به طور مثال: همیشه در حالت حفظ حریم خصوصی فعال نباشید.) کامپیوتر/موبایل شما باید نشان دهنده برخی ورودی ها باشد، تا هیچ کسی بر شما مشکوک نشود.

- مطمین شوید که به مرورگرهای مثل فایرفاکس و گوگل کروم log in نه شده اید (به طور مثال: اطمینان حاصل کنید که شما به مرورگر کروم به اکونت گوگل/جمیل وارد نشده اید.) اگر در حالی که وارد حساب کاربری خود شده اید، اینترنت را مرور می کنید، حساب شما سابقه تمام فعالیت های شما را نگه می دارد. نتایج جستجو حساس را از بین ببرید
https://www.humanrightsfirst.org/sites/default/files/How%20to%20delete%20-your%20history_updated.pdf

5.2.

حذف تمام اکونت ها/
حساب های کاربری

Facebook – فیسبوک
https://www.facebook.com/help/224562897555674/

Twitter – توییتر
https://help.twitter.com/en/managing-your-account/how-to-deactivate-twitter-account

LinkedIn – لینکد ان
https://www.linkedin.com/help/linkedin/answer/63?lang=en

Instagram – انستاگرام
https://help.instagram.com/448136995230186/

Signal – زیگنال
https://support.signal.org/hc/en-us/articles/360007061192-Unregister-or-Delete-Account

Telegram – تلگرام
https://my.telegram.org/auth?to=delete

WhatsApp – واتساپ
https://faq.whatsapp.com/android/account-and-profile/how-to-delete-your-account/?lang=en

Google – گوگل
https://support.google.com/accounts/answer/32046?hl=en

علاوه بر این، از طریق این لینک می‌توانید درخواست حذف نتایج ذخیره شده در حافظ پنهان گوگل را بدهید.
https://google.com/webmasters/tools/removals

Microsoft/Hotmail – مایکروسافت/هاتمیل
https://support.microsoft.com/en-us/help/12412/microsoft-account-how-to-close-account

Yahoo -یاهو
https://en-global.help.yahoo.com/kb/SLN2044.html

Protonmail – پروتون میل
https://protonmail.com/support/knowledge-base/delete-account/

لغودنبال کردن و یا حذف کنید.

- مطمین شوید که شما موقعیت توییت کردن را در بخش تنظیمات تویتر تان فعال نه کرده اید. اگر چنین است، آن را غیر فعال کنید.
- توییت های قبلی را حذف کنید:

https://semiphemeral.com

لینکدان - Linkedin
https://www.linkedin.com/help/linkedin/answer/3003/delete-content-you-ve-shared?lang=en

انستاگرام - Instagram
https://help.instagram.com/997924900322403

زیگنال - Signal
https://support.signal.org/hc/en-us/articles/360007320491

تلگرام - Telegram
https://telegram.org/faq#q-can-i-delete-my-messages

مسنجر - Messenger
https://www.facebook.com/help/messenger-app/1944003114491172

واتساپ - WhatsApp
https://faq.whatsapp.com/android/chats/how-to-delete-messages/?lang=en

جستجوی گوگل - Google Search
https://support.google.com/websearch/troubleshooter/3111061?hl=en

تیک تاک - TikToK
https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/privacy-controls

ویکی پدیا:
اگر در ویکی پدیا یا سایر پروژه‌های ویکی‌مدیا اطلاعاتی پیدا کردید که می‌تواند به شما یا سایر افراد در افغانستان آسیب برساند، لطفاً در مورد آن به این آدرس ایمل کنید - ca@wikimedia.org و AFG را در نوار مطلب یا Subject Line بنویسید.

عکس پروفایل و یا پس منظر حساب های کابری دوستان تان را مرور کنید. اگر هر کدام از آنها عکس سئوال برانگیز (به طور مثال: نمایش یک پرچم یا بنر ضد طالبان) را داشتند، از آنها بخواهید تغییر اش دهد. اگر مشکوک بودید آن آدرس را حذف کنید.

https://twitter.com/ngleicher/status/1428474008295464965

- یک حساب/اکونت محلی بسازید و تنها برای دوستان محلی تان باشد تا با نگه داشتن آن در برنامه تلفونی تان از ارتباط شدن با مخاطبین و تماس های بین المللی تان جلوگیری شود. اکونت تان را به اندازه که ممکن باشد عمومی بسازید، محتویات سیاسی و مذهبی نشر نکنید. از یک عکس عمومی به حیث تصویر پروفایل استفاده کنید و ممکن شما برای این اکونت یک نام مستعار هم استفاده کنید. اما متوجه باشید اگر حساب جدید تان را با شماره تلفون وصل کنید، ممکن از طریق شماره تلفون ردیابی شوید.

- مطمین شوید که بخش معلومات اکونت شما برای عموم قابل مشاهد نیست. هیچ سابقه کاری را به اکونت/ حساب تان اضافه نکنید. اطمینان حاصل کنید که هیچ ارتباط قبلی شما با نهادهای خارجی و یا سابقه کاری شما در اکونت تان قابل مشاهد نیست.

- اگر می‌خواهید از اکونت بین‌المللی خود استفاده کنید، فقط زمان وارد آن شوید که در مکان امن و یا در خانه هستید. رمز عبوری آن را در موبایل یا لب تاپ تان ذخیره نکنید.

- پست های فیسبوک خود را بررسی کنید (هر آنچه که به طور بلقوه قابل اعتراض بوده می‌تواند را حذف کنید.)، لیست دوستان تان (هر آن کسی را حذف کنید که می‌تواند باعث ایجاد شک شود خاصتاً اگر خارجی باشد.)، و صفحات و گروپ های را که در گذشته پسند کرده اید، هم بررسی کنید.

- عکس های فیسبوک تان خاصتاً تصویر پروفایل و پس منظر را بررسی کنید. تنظیمات تمامی این عکس ها را بررسی کنید به شمول عکس های قدیمی و مطمین که این عکس ها قابل مشاهده بجز دوستان قابل اعتماد برای دیگران نیست. اگر کدام عکس (سوال برانگیز) دارید را حذف کنید.

- مشاهده لیست دوستان را محدود بسازید تا دیگران دیده نتواند. (و از تمام دوستان بخواهید که چنین کنند.) این موارد در بخش تنظیمات فیسبوک تان تنظیم می‌شود.

/ ? How People find and contact you / Who can see your friends list
".Only me"

- هم دیاران افغان تان را در فیسبوک برچسب/تگ نکنید.

- گزینه را که دیگران می توانند شما را در عکس ها برچسب گذاری کنند غیرفعال سازید.
https://www.hongkiat.com/blog/prevent-facebook-tagging/amp/

1. پست ها و عکس های را که قبلآ دوستان تان شما را تگ کرده، مرور کنید اگر باعث ایجاد مشکل می‌شوند، برچسب را حذف کنید.

Twitter - تویتر
https://www.businessinsider.com/how-to-delete-old-tweets-from-twitter-2018-12

- قواعد مشابه به فیسبوک بر تویتر و دیگر رسانه‌های اجتماعی نیز اعمال می‌شود. لیست کسانی که شما را دنبال می‌کنند را مرور کنید، هر کسی را و یا هر تویت که می‌تواند مخالف طالبان را به همراه داشته باشد،

5 سابقه دیجیتالی خود را حذف کنید و ردپای آنلاین خود را کاهش دهید

این هنوز دقیق نیست که آیا و تا چی اندازه نیروهای دشمن/هکران بر مردم خاصتاً مدافعان حقوق بشر و خبرنگاران نظارت آنلاین دارند یا خیر. این اوضاع به سرعت در حال توسعه است و حذف معلومات آنلاین می‌تواند موثر واقع شود.
https://news.trust.org/item/20210817111442-4d73x
این ممکن به مصونیت آنلاین شما در افغانستان صدمه بزند. در ذیل بعضی از رهنمایی های توسط WIRED ارائه شده.
https://www.wired.com/story/how-to-clean-up-your-digital-history/

همچنین Human Rights First معلومات ارائه میدهد.
https://www.humanrightsfirst.org/sites/default/files/How%20to%20delete%20your%20history_updated.pdf

شکل فارسی
https://twitter.com/dooley_dooley/status/1427223031429181441

توجه:
1. در مورد به ارائه معلومات شخصی به خدمات گروه ثالث متوجه باشید.
2. برخی سکوها یا پلات فورم‌ها خط و مشی نگهداری دیتا/داده‌ها را دارند که حساب‌های کاربری را برای اجرای قانون آرشیف می‌کنند.
3. امکان دارد دیتا حذف شده شما هنوز به شکل محلی در لب تاپ و یا تلفون شما حفظ باشد.

5.1. چگونه محتویات انتخاب شده، مثل عکس و پست‌ها را حذف کنیم و یا آن را به شکل مصون استفاده کنیم.

نظری بیندازید بر این رهنمایی کوتاه فارسی:
https://twitter.com/dooley_dooley/status/1427223031429181441

فیسبوک – Facebook
https://www.facebook.com/help/2612118605804 76/

طالبان حضور فعال در فیسبوک دارند و ممکن از آن برای شناسایی افراد که با آنها آشکارا در مخالفت هستند، یا کسانی که با خارجی ها کار می‌کنند و یا هم کسانی که منابع قابل بهره گیری دارند، استفاده کند.

- فیسبوک ابزاری را ساخته که با یک کلیک آنها می‌تواند اکونت شان را قفل کند. زمانی که پروفایل شان قفل شود، افراد که دوستان شان نیستند، قادر به دانلود و یا اشتراک گذاری عکس پروفایل و یا پست های صفحه شان نمی‌باشند.

4.3.

تنظیمات امنیتی در حساب‌های کاربری خود را بررسی کنید.
ببنید آیا موارد اقدامات مهمی را متوجه شده اید یا خیر و نیز گزینه هشدار امنیتی را تنظیم کنید.
اگر ممکن بود شما گزینه (2AF) یا همان گزینه برای 2-Factor-Authentication را با استفاده از یک برنامه تصدیق هویت مانند freeOTP فعال سازید.

https://freeotp.github.io/

یا هم Aegis را برای Adnriod (چون گزینه قفل شدن با قابلیت رمز عبوری را دارد)

https://getaegis.app/

و همچنین Raivo برای iOS
https://apps.apple.com/us/app/raivo-otp/id1459042137
گوگل (در تلفون های موبایل):
https://myaccount.google.com/security-checkup/
توجه داشته باشید، اینکه اگر حساب کاربری خود را با یک شماره تلفون وصل ساخته اید، اکونت شما می‌تواند از طریق شماره تماس قابل ردیابی باشد.

فیسبوک:
https://www.facebook.com/help/799880743466869
اگر شما از مسنجر فیسبوک استفاده می‌کنید این بهتر است که از (Secret Conversations) استفاده کنید.

واتساپ:
https://faq.whatsapp.com/general/verification/how-to-manage-two-step-verification-settings/?lang=en

تلگرام:
https://telegram.org/blog/sessions-and-2-step-verification

لینک ذیل اسناد مرتبط به تمام ارائه کننده‌گان ایمل است.
https://2fa.directory/#email

مطمین شوید که کدهای حمایتی و بازیابی خود را بیرون از تلفون به طور جداگانه یاداشت کنید که در دزدیده شدن، شکستن و یا اتمام باطری تلفون بتوانید حساب کاربری خود را بازیابی کنید.
معلومات بیشتر:
https://ssd.eff.org/en/module/how-enable-two-factor-authentication

4.4.

اگر می‌خواهید که بخاطر ناشناس بودن، شماره تلفون و یا تلفون خود را تغییر بدهید. بخاطر داشته باشید که همیشه هر دو را همزمان باید تغییر داد.
هر چند هر دو به طور جداگانه اما همزمان توسط تاورهای تلفون شناسایی می‌شود. (شماره سیم کارت + IMEI نمبر تلفون)، تغییر یکی آنها کافی نیست بخاطریکه دومی شما را هنوز شناسایی کرده می‌تواند.

4

حساب‌های کاربری آنلاین، تلفون، تبلیت و کامپیوتر خود را مصون سازید

4.1.

برای باز کردن تلفون و کامپیوتر تان نیاز به رمز عبوری دارید و مرز گذاری تمام-دیسک یا دستگاه همراه تان را فعال کنید. (اگر فکر می‌کنید، در صورت جستجوی دستگاه تان این مورد باعث جلب توجه می‌شود، یک داستان از قبل آماده برای توجیه و یا امن سازی معلومات در لب تاپ تان داشته باشید.) زمانی با کدام محل تلاشی مواجه شدید دستگاه تان را خاموش ساخته و در حالت عدم مراقبت رها اش کنید. به نکات شماره 2 مراجعه کنید. در صورتیکه مایل به اشتراک گذاری رمز عبوری و یا دسترسی به دستگاه (کامپیوتر/موبایل) تان بودید و یا هم خیر.

4.2.

از برنامه‌های پیام دهی رمز گذاری شده سرتا سر

مثل واتساپ https://whatsapp.com

یا زیگنال https://signal.org

یا وایر https://wire.com

استفاده کنید و برای پیام‌های نوشتار گزینه ناپدید شدن پیام‌ها را هم فعال کنید و یا هم مسج‌هایتان را به طور منظم حذف کنید.

متوجه باشید، که برنامه‌های چون زیگنال و وایر که به شکل معمول مورد استفاده قرار نمی‌گیرند و یا هم مورد استفاده سازمان‌ها و افراد مرتبط به موسسات بین‌المللی و نهادهای غیر دولتی هستند، ممکن باعث جلب توجه بیشتر شوند. هرچند که آنها ممکن مصونتر از واتساپ هم باشند.

یک جایگزینی برای زیگنال در Android یک پیام رسان مبتنی بر زیگنال به نام Molly است که ممکن است توجه را جلب بیشتر به خد نکند:

https://molly.im/

3

توصیه های ویژه برای زنان خبرنگار

اگر شما به عنوان یک زن شناسایی شوید، ممکن شما با تهدیدهای امنیتی دیجیتالی منحصر به فرد رو به رو شوید.
به روش موجود در این رهنما بنیاد حقوق دیجیتالی توجه کنید.

https://digitalrightsfoundation.pk/wp-content/uploads/2017/11/Hamara-Internet-Guidebook-English-Version-2016.pdf

---

این بنیاد همچنین به زبان پشتو ارائه خدمات می‌کند.

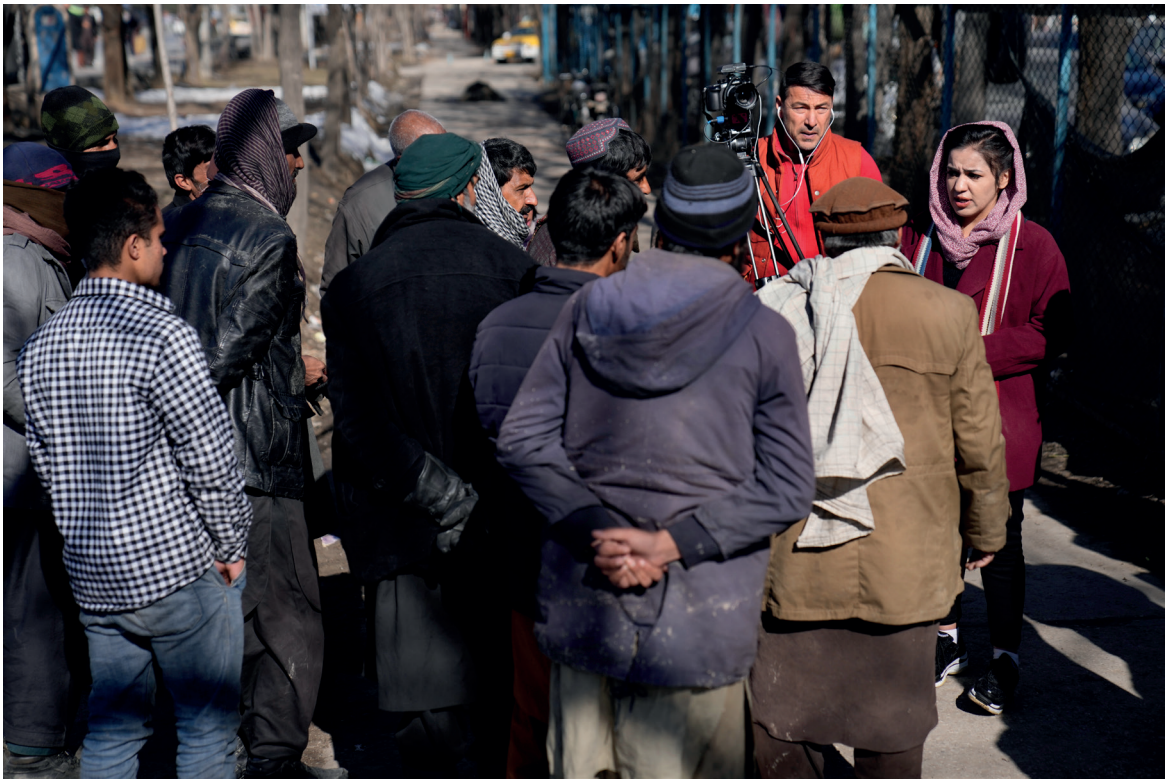
/https://digitalrightsfoundation.pk/services

یک رهنمایی مصونیت آنلاین توسط Chayn برای زنانیکه با آزار و اذیت رو به رو هستند نیز وجود دارد.
این رهنما به زبان‌های مختلف است.
https://www.chayn.co/

پشتو
https://chayn.gitbook.io/diy-online-safety/pashto-p-tw

فارسی
https://chayn.gitbook.io/diy-online-safety/farsi-farsy

انگلیسی
https://chayn.gitbook.io/diy-online-safety/english



—
اسما سهین، خبرنگار تلویزون طلوع که ۲۲ سال دارد. او در حال مصاحبه با مردم در کابل است. سه شنبه ۸ فبروری، ۲۰۲۲ او و همکارش بینش کوشش کردند که افغانستان را با صدها خبرنگار دیگر که فرار کردند و یا برای ترک افغانستان همرایشان کمک صورت گرفت، بعد از تسلط طالبان در اگست ۲۰۲۱ کشور را ترک کنند.
سروی که از سوی سازمان خبرنگاران بدون مرز و انجمن آزاد خبرنگاران افغانستان صورت گرفت، نشان میدهد که ۲۳۱ رسانه در کشور مسدود شده و بعد از تسلط طالبان در کابل ۶۴۰۰ خبرنگار وظایف شان را از دست داده است.

عکس: از یک سال قبل از تسلط طالبان بر کابل است. (AP Photo/ Hussein Malla)

- یاداشت‌ها و یاداشت‌های صوتی
- عکس‌ها
- جستجو/ سابقه جستجو در ویب سایت‌ها
- ویدیوهای یوتیوب را که تماشا کرده اید/اکونت گوگل
- اسنادهای را در کامپیوتر و تلفون همراه تان ذخیره کرده اید
- برنامه‌های VPN
- داده‌های Google/Apple Maps و تاریخچه موقعیت مکانی (مکان‌های مهم برای اپل، سابقه موقعیت مکانی برای Google)
- برنامه تقویم – جنتری که احتمالاً حاوی ورودی‌های حساس نیز باشند
- برنامه‌های موزیک (برخی موزیک‌ها ممکن از لحاظ سیاسی و مذهبی مناسب جلوه نکنند)
- برنامه‌های دوستیابی

آگاه باشید، که شما باید موارد حذف شد را از سطل باطله تلفون/کامپیوتر تان پاک کنید و اینکه یک تحلیل از فرد متخصص ممکن است آثار از موارد حذف را باز گرداند.

در مورد که می‌خواهید همه چیز را از تلفون تان حذف کنید: حداقل برخی از تصاویر شخصی تان را نگهدارید تا نشان بدهد که تلفون مورد استفاده قرار گرفته است.

2.3.

نام افراد تماس گیرنده در لیست تلفون همراه تان را به حروف زبان دری یا پشتو تغییر دهید و بررسی نمائید اگر نیاز بود، شماره تماس‌های خارجی/بین‌المللی را نیز از موبایل تان حذف کنید.

- آدرس‌های موجود در تلفون همراه تان، مخاطبین مسنجر و یا سابقه چت تان نباید حاوی و بیانگر نام‌ها و آدرس‌های خارجی باشد.

- اگر می‌خواهید یک لیستی از این مخاطبین و یا آدرس‌ها را با خود نگهداشته باشید، آنها را در تلفون یا لب تاپ تان حفظ نکنید! آنها را به خودتان به آدرس ایمل ارسال کنید که ایمل اصلی تان نباشد. رمز عبوری و یا حساب کاربری آن ایمل را در موبایل و لب تاپ تان ذخیره نکنید و سرنخ از آن را در دستگاه تان نگذارید. (به طور مثال: اگر شما از ایمل اصلی تان به ایمل دیگر تان پیام میفرستید، پیام ارسال شده هنوز در پوشه ارسال موجود می‌باشد.)

- هر نوع ایمل زیان آور را از پیام خانه، آرشیف، بخش ارسال، و یا پوشه پیش نویس حذف کنید و مطمئین شوید که پوشه باطله را هم پاک کرده اید.

2.4.

برای مسنجرها و دیگر گروه‌های آنلاین: از قبل چندین فرد را به حیث مدیر گروه‌های مختلف انتخاب کنید چون در صورت نیاز یکی از مدیران آن گروه می‌تواند یک عضو را حذف کند.
(به طور مثال: اگر تلفون کسی از نزد او مصادره شود.)

2.5.

به درخواست‌های تماس از طریق رسانه‌های اجتماعی پاسخ ندهید، اگر تماس از طرف دوستان تان و یا کانال‌های قابل اعتماد نباشد. مواردی وجود دارند که یک فرد ناشناس خود را خبرنگار خارجی معرفی کرده و تقاضای مصاحبه می‌کند و اما بعداً از اطلاعات ارائه استفاده سو کرده و سپس قربانی را ردیابی می‌کند.

2.6.

بجای ایمل آدرس‌های خصوصی شده، ایمل آدرس‌های کاربردی یا ترکیبی بسازید، به این معنی که ایمل حاوی نام شما و یا محتویات نباشد که هویت شما به واسطه آن تشخصی شود.

2 آماده‌گی برای حالت اضطراری دیجیتالی، دستگیری و محلات تلاشی | یک طرح بسازید

برای ایجاد مصونیت آنلاین، تشخیص دهید که با کدام نوع تهدید شما رو به رو هستید و کدام فعالیت آنلاین تان شما را با خطر مواجه می‌سازد – نوع تهدید شما چیست؟ این نگاه نخست به امنیت دیجیتالی به شما کمک می کند که به چنین سئوالات خود پاسخ بیابید.

https://www.accessnow.org/first-look-at-digital-security/

زمانی که در مورد تهدید فکر می‌کنید، لطفاً موارد ذیل را نیز به خاطر داشته باشد.

2.1.

یک برنامه بریزید برای این احتمال که شما و یا یکی از افراد را که می‌شناسید ممکن توسط مقام‌ها بازداشت شود. به این رهنما یک نگاهی بیندازید.

https://digitalfirstaid.org/en/arrested/

این توسط RaReNet و CiviCERT ترتیب شده و شامل اقدامات احتیاطی امنیت دیجیتال برای اطلاعات بیشتر است.

همچنین رهنمای مقابله با زندان نیز وجود دارد.

https://coping-with-prison.org

این رهنما شامل نکاتی برای خانواده‌ها، حمایت کننده‌گان و وکیلان افراد بازداشت شده است.

2.2.

در محلات تلاشی و در هنگام حمله یا یورش، آماده باشید اینکه مقام‌ها دستگاه‌های شما (کامپیوتر/موبایل) را مصادره خواهند کرد و یا هم بر شما فشار می‌آورند تا آن را باز کنید. تلفون تان را با خود به بیرون نبرید، یا هم یک تلفونی را با خود بردارید که دیتا/اطلاعات حساس مثل شماره های ارتباط و یا معلومات مشابه در آن موجود نباشد. مقدار دیتا/ داده‌های را که در دستگاه‌های خود خاصتاً موبایل تان ذخیره می‌کنید به حداقل برسانید.

– قانون طلایی اینست: اگر شک دارید، حذف اش کنید.
هیچ اطلاعاتی ارزش این را ندارد که به خاطر آن زندگی خود و یا دوستان تان را در مخاطره بیندازید.(نکات ذیل برای چگونگی حذف محتویات و حساب‌های کاربری است.)
تصمیم بگیرید که آیا می‌خواهید به دستگاه‌های تان دسترسی داشته باشید یا خیر. این یک تصمیم ساده نخواهد بود، اما خوب است قبل از اینکه اتفاق بیفتد در مورد آن فکر کنید. توجه داشته باشید در صورت حضور شما، این ممکن است که اثرانگشت و یا هم Face-ID با استفاده از زور باز ساخته شود. در iOS البته آیفون های قدیمی گزینه اضطراری وجود دارد که با چندین بار فشار دادن دکمه پاور، این ممکن است که از Face-ID و یا اثرانگشت به مرحله رمز عبوری وارد شوید. همچنین در آیفون های جدید این کار در ابتدا با خاموش کردن / Emergency SOSو برای دو ثانیه با فشار دادن و یا محکم گرفتن دکمهء صدا و یا دکمه کناری به شکل همزمان رخ میدهد. خود را آماده کنید که از این روش استفاده کنید اگر احتمالاً ضرورت به استفاده آن را داشتید.
برنامه‌ها/App های که می تواند باعث خطرات امنیتی برای شما و دیگران شود:

- آدرس/لیست تماس‌ها
- برنامه مسنجر
- اکونت فیسبوک
- تویتر و دیگر حساب‌های کاربری اجتماعی
- ایمل‌ها

1

خطوط تلفون اضطراری برای حالت‌های اضطراری دیجیتالی

اگر شما یک خبرنگار، فعال و یا هم عضو جامعه مدنی هستید و در عین حال شما نیاز به کمک اضطراری دارید، Access Now`s Helpline حمایت امنیت دیجتالی 24 ساعته را برایتان ارائه می‌کند.

یاداشت: تیم حمایت با زبان‌های محلی افغانستان با شما صحبت نخواهد کرد.

گزینه‌های بیشتر:

https://cpj.org/emergency-response/how-to-get-help

https://www.frontlinedefenders.org/emergency-contact

بنیاد حقوق دیجیتالی نیز به چنین پرونده‌ها از طریق آدرس ذیل رسیدگی میکند.
helpdesk@digitalrightsfoundation.pk

اگر گمان دارید که تلفون شما با نرم افزارهای جاسوسی یا موارد مشابه مورد حمله قرار گرفته است، Emergency VPN توسط پروژه Civilsphere برایتان به منظور بررسی تلفون تان کمک فراهم می‌کند:
https://www.civilsphereproject.org/emergency-vpn

خطر	مراحل پیشگیری	مراحل پاسخ دهی	ملاحظات
مصادر و یا دسترسی به تلفون‌ها، تبلیت‌ها، کامپیوترها و ساعت های هوشمند دستی در جریان حمله/یورش، جستجو، دستگیری و همچنین محلات تلاشی و غیره.	▪ کاهش دیتا/داده‌ها معلوماتی در دستگاه‌های (کامپیوتر/ موبایل) ما به حداقل نا محسوس اما واقع بینانه ▪ مصون سازی دیتا/معلومات در دستگاه‌های ما ▪ مصون سازی دستگاه ها ▪ ایجاد پشتیبانی رمزگذاری شده برای تمام دیتا/معلومات ها	▪ عدم دسترسی به دستگاه‌ها (کامپیوتر/موبایل) ▪ پاک کردن دستگاه‌ها از راه دور و یا پاک کردن به شکل خودکار/ اتوماتیک در صورت تلاش ناموفق برای ورود به دستگاه ▪ با خبر سازی افراد در معرض خطر یا متاثر شونده ▪ بازیابی معلومات و حساب های کاربری/اکونت ها	▪ اخذ تصمیم مهم: آیا تحت فشار اجازه خواهید داد که به دستگاه (کامپیوتر/موبایل) تان دسترسی صورت بگیرد؟ ▪ در نظر داشته باشید، آیا پشتیبان های رمزگذاری شده و یا فایل های رمزگذاری شده باعث جلب توجه و ایجاد خطر به شما می شود؟
نظارت بر روابط دیجیتالی و ارتباطات آنلاین (توسط مقام‌ها، متحدین آنها، ارائه کننده‌های خدمات انترنتی، و شرکت های مخابراتی)	▪ مصون سازی اکونت های آنلاین ▪ استفاده از خدمات مصون آنلان (پیام رسان های رمزگذاری شده سر تا سر، ذخیره سازی آنلاین، کنفرانس های ویدیویی و غیره.) ▪ مصون سازی دسترسی ما به انترنت از طریق VPN یا ابزار مشابه به آن	▪ نظارت را در صورت امکان مستند سازی کنید ▪ فعال سازی میکنازیم های حفاظت از سوء استفاده توسط ارائه دهندگان خدمات ▪ حساب‌های متاثر شده یا آسیب پذیر را پشتیبانی و غیر فعال کنید	▪ برنامه‌ها و یا کانال های مصون مثل VPN ها ممکن باعث جلب توجه شوند و یا خود باعث ایجاد خطر و تهدید گردند
حملات دیجیتالی بر دستگاه‌ها و اکونت ها (افزارجاسوسی، حملات هک کننده، و جابجایی شواهد از سوی مقام‌ها و متحدین شان یا هم مجرمان)	▪ مصون یا امن سازی دستگاه ها ▪ امن سازی حساب‌های کاربری آنلاین ▪ به روز سازی سیستم اجرایی و نرم افزار ها ▪ رد درخواست ارتباط توسط افراد ناشناس از طریق رسانه‌های اجتماعی	▪ حملات و تمام شواهد را مستند سازی کنید ▪ دستگاه های حمله شده را خاموش نگه دارید ▪ اکونت‌ها را از طریق ارائه کننده و یا خط تماس های کمکی بازیابی کنید ▪ گزینه 2FA را برای اکونت های بازیابی شده فعل سازید.	
هوش یا اطلاعات منابع باز (اوسنت) | جستجو در سکوهای که به شکل عموم قابل دسترس هستند، مثل فیسبوک و ویکی پدیا	• کاهش ردپای در فضایی دیجیتالی با حذف معلومات یا با درخواست حذف معلومات از سکوهای و پلاتفورم های آنلاین	▪ کوشش کردن برای حذف شواهد در سکوهای یا پلاتفورم های آنلاین	▪ متوجه باشید، که بسیاری از معلومات به شکل کامل حذف نخواهد شد، اما اگر این کار صورت بگیرد به دلیل تاخیر در پشتبیانی های توزیع شده و پلاتفورم ها مثل ماشین بازگشت و سایر خدمات ذخیره سازی است.

مراقبت کردن، مقاومت است.

" مراقبت از خودم یک زیاده خواهی نیست، بلکه این به معنی حفاظت از خودم می‌باشد و یک کنش از جنگ سیاسی است." (اودره لرده)

مراقبت از دستگاه (کامپیوتر/موبایل) و دیتا یا معلومات تان نه تنها به مفهوم محافظت از شخص شما، بلکه محافظت از تمام جامعه است.

خبرنگاران، کارمندان رسانه‌ها و فعالان زندگی خود را به مخاطره می‌اندازند، اگر در صورتیکه از دیتا/ معلومات آنلاین، آپ‌ها، و یا ارتباطات شان به حیث شواهد علیه آنها و یا شخصی دیگری که با آنها در ارتباط است، استفاده شود.
ممکن است دسترسی به چنین دیتا یا معلومات، برنامه‌ها و غیره اتفاق بیفتد.
همچنین ممکن است سناریو های ذیل نیز رخ بدهند.

- مصادره و یا دسترسی به تلفون‌ها، تبلیت‌ها، کامپیوترها، ساعت‌های هوشمند و دیگر دستگاه‌های قابل بازیابی(USB ها، هاردسک‌های بیرونی، و غیره) در جریان یورش، جستجو، دستگیری و یا در محل تلاشی و غیره

- نظارت از ارتباطات دیجیتالی و یا تماس‌های آنلاین
- حملات دیجیتالی بر دستگاه‌ها (کامپیوتر/موبایل) و حساب‌های کاربری
- هوش منابع باز| تحقیق روی پلاتفورم‌های که به شکل عام قابل دسترس هستند، مانند: فیسبوک و ویکی پدیا

با اطلاع از اینکه نمی‌توان از تمام خطرات جلوگیری کرد با برخی اقدامات مشخص مثل داشتن دیتا یا اطلاعات کمتر در دستگاه‌ها، استفاده از کانال‌های مصون ارتباطی و امن سازی دستگاه‌های ما (کامپیوتر/موبایل) می‌توان احتمال و یا اثرگذاری اینکه چنین دیتاها و برنامه‌ها به شواهد علیه ما تبدیل شوند را کاهش داد.
در عین حال، برخی از این اقدامات امن به خطرات نیز تبدیل خواهند شد، اگر app ها و برنامه‌های شناسایی شده به حیث شاخص‌های مرتبط با بازیگران اشتباه (جامعه بین‌المللی و یا نظیر آن) در نظر گرفته شود.

6 اگر دستگاه (کامپیوتر/موبایل) خود را گم کردید، چی باید کرد

7 حساب کاربری/ اکونت تان را بازیابی کنید

8 VPNs: محافظت در برابر جاسوسی، حملات و سانسور

9 برگزاری ویدیو کنفرانس مصون

10 به اشتراک گذاری مصون فایل و ذخیره سازی آنلاین

لطفا" توجه داشته باشید: معلومات و منابع که در این رهنمود دیجیتالی ارائه شده، از ماه می ۲۰۲۲ به بعد است و ما در هر شش ماه محتویات و منابع آن را بروزرسانی مینمایم. محتویات بروز شده از این آدرس قابل دانلود خواهد بود:
https://helpdesk.rsf.org/digital-security-guide/afghanistan-digital-care-guide

امتیاز

مراقبت کردن، مقاومت است

1 خطوط تلفون اضطراری برای حالت‌های اضطراری دیجیتالی

2 آماده‌گی برای حالت اضطراری دیجیتالی، دستگیری و محلات تلاشی | یک طرح بسازید

3 توصیه های ویژه برای زنان خبرنگار

4 حساب‌های کاربری آنلاین، تلفون، تبلیت و کامپیوتر خود را مصون سازید

5 سابقه دیجیتالی خود را حذف کنید و ردپای آنلاین خود را کاهش دهید

رهنمایی مصونیت دیجیتالی

افغانستان صفحه 1

دافغانستان صفحه 26

لپاره د ډیجیتالي مصونیت لارښود

RSF REPORTER OHNE GRENZEN