Guidance Document

Online Protection and Digital Security:

User guide for human rights defenders

Photo: UN Women/Ploy Phutpheng

UNAMA

UN WOMEN

Contents

About this document 4

Disclaimer 4

I. Introduction 5

II. The “top 10” basics of computer and mobile protection 7

III. Create strong passwords and enable multifactor authentication 11

Strong passwords 11

Multifactor authentication 12

IV. Eliminate malware 13

What is malware? 13

How to protect devices from malware 13

V. Browse the Internet safely 14

Securing your router 14

Using public Wi-Fi hotspots 14

Protect yourself when using public Wi-Fi 14

Use safe browsers 15

Use safe search engines 15

Use safe browser extensions/add-ons 15

VI. All about encryption 16

What is “encryption”? 16

a. Communicate safely 16

What is “secure communications”? 16

Security standards 17

Recommendations for secure communications applications 17

How to send secure (encrypted) emails with PGP 18

b. Save and store information securely **18**

Saving photos, videos and data to a device 18

Encrypting and storing files using cloud services 19

Ecryption software 19

VII. Erase data securely **20**

How to clean devices 21

How to permanently erase or wipe data 21

VIII. Prevent phishing **22**

Types of phishing 22

How to protect yourself from digital phishing 23

IX. References and further reading **25**

XI. Emergency assistance **26**

X. Cybersecurity glossary of terms **26**

About this Document

This document was originally produced by the United Nations Assistance Mission for Iraq (UNAMI) to raise awareness of and mitigate online risks faced by human rights defenders, civil society activists and media workers. The original text was adapted to Afghanistan by the United Nations Assistance Mission in Afghanistan (UNAMA) Human Rights Section and UN Women Afghanistan.

Disclaimer

UNAMA and UN Women welcome the opportunity to promote their activities and publications in cooperation with their partners. Please be advised that the information, advice and recommendations (including recommended software and applications) are provided by the authors of this guide for general information purposes only and do not necessarily represent the views of UNAMA or UN Women.

While the authors of this document endeavoured to provide up-to-date and correct information at the time of publication, information technology and digital security threats change rapidly; therefore, accuracy cannot be guaranteed at all times. As such, UNAMA and UN Women make no representation or warranties of any kind about the completeness, accuracy, reliability, suitability or availability of the information, products or services contained herein.

Users should verify the current accuracy and security of information or software prior to use. Resources provided at the end of this guide can help users stay current on secure methods and software.

I. Introduction

Digital security and human rights in Afghanistan

Digital technologies can present avenues to advocate for, defend and exercise human rights. They increasingly shape how people access and share information and can be a forum for discussion and debate. These opportunities can become particularly important when rights and fundamental freedoms in physical or “offline” spaces are threatened. At the same time, digital technologies can equally be used to suppress, limit and violate human rights, such as through surveillance and censorship. Both state actors and private citizens can deploy them to perpetrate abuse and harassment, often reinforcing existing systemic discrimination and marginalization.

Since the Taliban takeover of Afghanistan on 15 August 2021, women’s participation in daily and public life has contracted significantly as de facto authorities have taken steps to limit women’s freedom of movement, access to work and education, and exercise of other fundamental rights and freedoms.[1] In parallel, civic space and media freedoms have diminished.[2] In this context, digital space has provided a vital outlet for Afghans, particularly women and girls, to share their views and experiences, build communities, engage on issues important to them and advocate for their rights. At the same time, digital spaces present the risks and restrictions seen elsewhere. Gendered hate speech targeting prominent Afghan women has reportedly tripled since the Taliban takeover,[3] and individuals have been arrested for posting content online deemed critical of the de facto authorities.

Digital security risks for Afghan women

In November 2023, UNAMA Human Rights and UN Women conducted consultations with Afghan women in media and civil society to better understand their access to digital spaces, the risks and challenges, and recommendations for how to protect their rights and freedoms.

The main risks that women cited were:

- Monitoring and hacking of social media accounts and messaging platforms by members of the de facto authorities and the general public, leading to threats and harassment, both online and offline
- Gendered online abuse, often specifically targeting women because of their public profile working in media or civil society
- Doxing, where personal information such as addresses and phone numbers are publicly shared online
- Social media impersonation, where a person creates a fake profile on social media using personally identifiable information stolen from an individual and posts in their name with the intention of discrediting them

[1] For more information, see the reports on consultations with Afghan women inside the country conducted by UN Women, UNAMA and the International Organization for Migration in November 2023, July 2023, April 2023, January 2023 and August/September 2022. See also: Situation of human rights in Afghanistan: Report of the Office of the High Commissioner for Human Rights, 11 September 2023, A/HRC/54/21.
[2] See: Cooperation with the United Nations, its representatives and mechanisms in the field of human rights: Report of the Secretary-General, 21 August 2023, A/HRC/54/61. See also: M. Gehrig. 2022. Media Restrictions and the Implications for Gender Equality in Afghanistan. Kabul: UN Women.
[3] Afghan Witness. 2023. Violence Behind a Screen: Rising online abuse silences Afghan women.

Women made a range of recommendations on steps to improve their digital security. These included:

- The development of training programmes that not only improve their capacity to protect themselves against digital security risks but also generally increase their digital fluency and confidence in using digital technologies
- Additional support and resources in the Dari and Pashto languages, with women indicating that most social media and messaging platforms (Facebook, Instagram, X, WhatsApp, Signal) do not have resources or information available in these languages
- Financial and technical support to use software and applications aimed at improving digital security, such as secure document sharing and storage services, digital security risk analysis and VPNs (virtual private networks)

II. The “top 10” basics of computer and mobile protection

This section provides the “top 10” tips for improving digital security. These basic steps offer entry points for the main topics covered in greater detail in later chapters.

TIP 1: *Update the operating system, hardware, applications, phone and software regularly*

Companies provide periodic updates of their operating systems and applications to address security gaps. Updating regularly greatly improves a user’s protection against security breaches.

In Windows 11, the user determines when and how to obtain the latest updates to keep devices running smoothly and securely. To manage options and view available updates, select Check for Windows Updates. Or select **Start > Settings > Windows Update**.

- On a **Mac**, follow the instructions available here.
- To update an **Android** phone, follow the instructions available here.
- To update **iOS (iPhone)**, go to the App Store and follow the instructions available here.

Whichever operating system, applications and software are used, make it a priority to update regularly.

TIP 2: *Create strong passwords on all devices*

Users should make sure all passwords are:

- Long (more than 12 characters)
- Complex (containing a mix of uppercase and lowercase letters, numbers and symbols)
- Random, not containing common or personal words, number series, etc.
- Unique (a separate password for each account)
- Confidential (not easy to find on papers or devices)

See Section III for more information on how to create, manage and confidentially store all passwords.

TIP 3: *Use multifactor authentication whenever possible*

- Multifactor authentication dramatically increases digital security.
- Applications specifically designed for multifactor authentication, such as Duo Mobile, Aegis Authenticator and Google Authenticator, are more secure than SMS message authentication.

See Section III for more information and links to recommended applications.

TIP 4: *Install endpoint detection and response (EDR) (anti-malware) software*

- Malicious software can destroy a device, steal personal information or financial assets, or control a device remotely.
- EDR software provides protection from malware on the Internet.
- Install licensed versions of EDR software on every device running Windows, Mac, Linux, iOS or Android. Do not use "cracked software".
- It is important to use free software only from trusted sources.

Install programmes such as Malwarebytes and Avira.

See Section IV for more information.

TIP 5: *Use a safe browser*

- A browser acts as a window to the Internet. If the window is not secure, access and navigation are unsafe, and may be a path to infection from malicious software.
- Many browsers are commercial tools for collecting information, data tracking and targeting for marketing purposes.
- Use safe browsers, such as Firefox, Brave, Firefox Focus, Ghostery Dawn and DuckDuckGo, and regularly update browser software.
- Check the security of add-ons/browser extensions before adding them to the browser.

See Section V for more information.

TIP 6: *Install a VPN*

- A VPN protects the user's Internet connection and privacy online by creating an encrypted tunnel for the user's data and hiding the user's IP address. It allows safe use of public Wi-Fi. Without a VPN for protection, devices and their locations may be tracked and data intercepted.
- Choose a VPN carefully. There are free and paid services that contain malicious software, sell users' information to a third party or cooperate with governments to provide them with users' information.
- VPNs considered safe at the time of publication include Psiphon, TunnelBear and Riseup VPN.

See Section III for more information.

TIP 7: *Use safe open-source software and applications*

- Open-source software and applications are generally more secure than proprietary programmes because they provide their source code to users. This source code is then constantly updated to address security vulnerabilities.
- Using open-source software and applications keeps users from installing pirated or "cracked" proprietary software without a license. Pirated or "cracked" programmes may contain malicious elements that harm devices and should never be used.
- Be aware that not all open-source programmes are secure; always follow the advice of digital security experts before installing new software or applications. It is best to use programmes that have a strong track record, and to clearly understand security programmes and policies regarding privacy.

TIP 8: *Only download apps and software from recognized app stores*

- Unrecognized app stores contain dozens of applications and programmes contaminated with malicious software and back doors that provide the creator with the ability to manage and control devices.
- Only use recognized app stores and official application websites for downloads, such as: Google Play, the Amazon Appstore and the Apple App Store.

TIP 9: *Encrypt computers and phones*

- Encryption provides confidentiality and is fundamental to information security.
- Use encryption to send encrypted messages, safely store information, browse the Internet anonymously and share information more securely.

See Section VI for more information.

TIP 10: *Back up your data*

- The backup process is like storing valuable information in a safe so that it can be recovered if the original data is ever lost, damaged or hacked.
- Manually activate the backup tool provided with the operating system (either in Windows or MacOS) and be sure to complete backups periodically.
- Encrypt backup versions of data for storage.
- Store the backup either on an external hard drive or via a cloud-based service, e.g., Google Drive.

See Section VI for more information.

ADDITIONAL TIP: *Emergency Lockdown Mode*

- iPhone users have an optional, emergency Lockdown Mode to protect against sophisticated and targeted cyberattacks.
- Lockdown Mode limits the functionalities of certain apps, websites and features to reduce the likelihood that spyware can break through to access data stored on devices.

III. Create strong passwords and enable multifactor authentication

Strong passwords

Strong passwords provide the foundation of digital protection. Their strength allows them to withstand the many attacks that target passwords, including phishing operations, keyloggers and other attacks aimed at intercepting data or gaining unauthorized entry to protected accounts or data.[4]

The best defense against these attacks is to prevent them by creating strong passwords and regularly changing them.

A STRONG PASSWORD IS:

1. Long ✓

Use more than 12 characters. The shorter it is, the quicker it can be identified.

2. Complex ✓

Use uppercase and lowercase letters, numbers and symbols.

3. Random ✓

Avoid using numbers or letters in a sequential manner or using personal or family information.
Avoid using birthdates, names of family members or pets in passwords.

4. Easy to remember ✓

Forgetting passwords begins a cycle of retrieval, which requires more information.
Use a password manager (below) if remembering multiple passwords becomes complicated.

5. Confidential ✓

Create and save passwords but only in safe places. Unsafe places include directly in the browser, a phone's notes application, a phone's reminders application, sticky notes on a computer or inside a notebook/agenda. These locations are insecure because they are easy to access.

6. Unique ✓

Each account or service must have its own password. Discovering the password for one account will make other accounts vulnerable if they use the same password.

[4] Attacks aimed at revealing passwords include man-in-the-middle, brute force and dictionary attacks, and credential stuffing. To learn more about common password attacks, see Password Cracking 101: Attacks & Defenses Explained.

7. Periodically changed ✓

Create and save passwords but only in safe places. Unsafe places include directly in the browser, a phone's notes application, a phone's reminders application, sticky notes on a computer or inside a notebook/agenda. These locations are insecure because they are easy to access.

8. Original ✓

Do not use common keyboard patterns, e.g., "Qwerty12345" or "Password123".

Passwords can be saved in hard-to-reach caches or password managers. These caches are strong password generators and a huge number of passwords can be saved in them.

Password managers considered safe at the time of publication include:

1. KeePassXC
2. Bitwarden

Multifactor authentication

Activating the multifactor authentication feature on accounts provides serious protection from hacking and phishing. Multifactor authentication is an additional feature that prompts users to enter a single-use passcode that is generated after they enter their regular password. This single-use password is sent to the user via SMS or email, or accessed via a specific authentication application.

The best way to enable two-step verification is to do so by using an external app. The following applications were considered safe at the time of publication:

1. **Duo Mobile**
2. **Aegis Authenticator (for Android only)**
3. **Google Authenticator (iOS or Android)**

IV. Eliminate Malware

WHAT IS MALWARE?

Malicious software, or "malware", is a term describing software designed with the intent to damage, exploit or disable devices, operating systems or networks. It is used to steal data, gain unauthorized access, disable some or all functions, or damage devices or any related networks.

"Viruses" make up only a small part of the malicious software family. Other types of even more harmful malware may infiltrate and infect devices during Internet use.

The process of eliminating malware requires ongoing preventive steps. Creating barriers to infection and penetration by malicious software allows users to eliminate threats before they enter their devices.

There are many types of malicious software, including Trojans, worms, ransomware, adware, spyware and others.

How to protect devices from malware

The following steps should be followed to protect devices from malware:

1. Install reliable EDR software on every device running Windows, Mac, Linux, iOS or Android systems, including all computers and mobile phones. Note that only one EDR programme should be installed.
2. Only download programmes and applications from their official websites.
3. Regularly update each device's operating systems and applications.
4. Avoid using public and/or unsecured Wi-Fi networks without proper protection (such as a VPN).
5. Do not click on links from strangers or suspicious emails or messages even from known contacts.
6. Avoid sharing personal information.
7. Use a safe Internet browser.
8. Install recommended security add-ons for the browser.

Two EDR programmes considered safe at the time of publication (both free and paid versions) are Malwarebytes and Avira. Note that free anti-virus software offers basic protection against common viruses whereas paid anti-virus software offers more advanced protection.

V. Browse the Internet safely

Risks to users begin when a computer or phone connects to the Internet and a user starts searching or communicating with others.

To increase safety, use secure tools to access the Internet. This helps prevent service providers, authorities or hackers from monitoring users' activity.

Securing your router

Step one involves securing the Wi-Fi hotspot at home or at work by changing the router settings. Request technical assistance for these steps if they are unfamiliar. For basic information about how to configure a router, please see Protecting Against Malware: Secure Your Router.

1. Change the username and password of the router administrator account.
2. Change the IP address of the router.
3. Use a strong and private password for the Wi-Fi.
4. Set encryption settings and choose WPA2-PSK (AES).
5. Update the firmware of the router.
6. Hide the name of the Wi-Fi network.

Using public Wi-Fi hotspots

Public Wi-Fi networks (in cafes, stores, malls, hotels, airports, public transportation, restaurants, etc.) are usually weak in security and can pose serious threats, including:

1. **Threat of packet discovery:** Attackers (hackers) monitor and intercept unencrypted sent or received data transmitted over unprotected networks.
2. **Man-in-the-middle attacks:** Attackers infiltrate the weak Wi-Fi hotspot to be part of the communication between the target victim and the hotspot, to intercept and sometimes modify data in transit.
3. **Deceptive Wi-Fi networks:** Attackers create and set up a free and open hotspot for the public to connect, making it a corridor to collect user data.

Protect yourself when using public Wi-Fi

If possible, use a portable or mobile hotspot rather than public Wi-Fi. Follow these guidelines to protect personal information from attackers while using public communication points:

- Avoid using unknown/insecure hotspots or public Internet whenever possible.
- If using a public network, be sure to enable multifactor authentication for all accounts before use.

- Use a firewall. Most operating systems include this service, as do anti-malware/EDR programmes. Applications considered safe at the time of application include:

  Avira Comodo GlassWire

- On Windows, set up Microsoft Defender Firewall. Instructions can be found here.
- Use a VPN service to encrypt Internet connections and keep online activity private on any network. VPNs considered safe at the time of publication include:

  Windscribe ProtonVPN Psiphon TunnelBear Riseup

Use safe browsers

Browsers are the main gateway to access the Internet and therefore play an important role in online security. It is necessary to choose a safe browser as protection from theft or data privacy violations.

Browsers considered safe at the time of publication include:

Firefox Brave Ghostery Dawn DuckDuck Go Firefox Focus (for iPhones)

For more information about the pros and cons of different browsers, review the guide published by the Freedom of the Press Foundation.

Use safe search engines

Conduct online searches with secure search engines that maintain privacy. Many common search engines, including Google, Bing, Amazon and Yandex, do not meet privacy standards.

The following search engines provided more security and privacy at the time of publication:

DuckDuck Go Qwant StartPage

Use safe browser extensions/add-ons

Browser extensions, or "add-ons" extend the functionality of a programme on another programme, such as a browser. Add-ons are usually not full versions of software but rather are pieces of code that modify a specific interface. The most common add-ons for browsers are toolbars that provide users with instant shortcuts to online services.

The only add-ons or browser extensions that should be downloaded are those that increase the user's security and privacy.

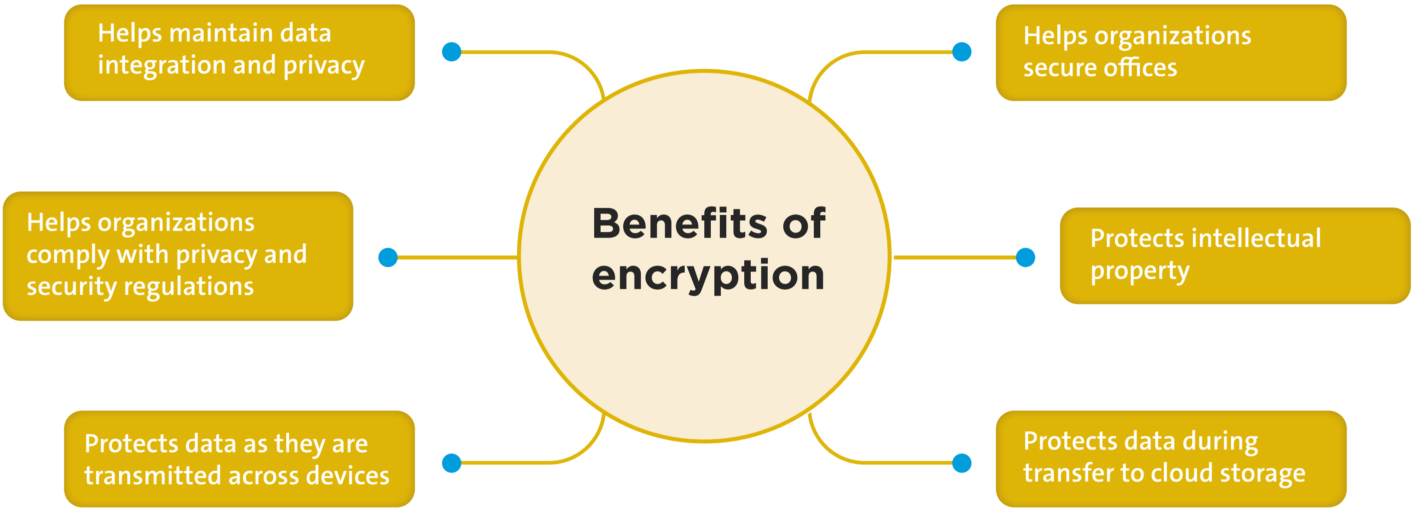
At the time of publication, the following extensions provided users with enhanced security:

HTTPS Everywhere Virus Total Ghostery Malwarebytes Cookie AutoDelete NoScript Privacy Badger

VI. All about encryption

WHAT IS ENCRYPTION?

In basic terms, encryption is the process of transforming data from a readable format into a secret code that can only be "unlocked" by users who hold the secret "key" or password.



Benefits of encryption

Helps maintain data integration and privacy

Helps organizations secure offices

Helps organizations comply with privacy and security regulations

Protects intellectual property

Protects data as they are transmitted across devices

Protects data during transfer to cloud storage

ENCRYPTION CAN BE USED TO:

1. Save photos, videos and data to devices
2. Share files and documents
3. Send emails privately
4. Store files using cloud services
5. Communicate via messages or calls

a. Communicate safely

What is "secure communications"?

Secure communications entails encrypting a user's communications using one or more security protocols to ensure that data flows between a sender and recipient without reaching a third party. Encryption scrambles plain text into a type of secret code that others cannot read, even if they intercept it before it reaches its intended recipients. When the message reaches its recipients, their device uses its own key to unscramble the information back into plain, readable text.

If the connection is not encrypted, governments, groups and individuals with technical backgrounds can listen to or read communications; access, intercept and modify content; plant malware; and open backdoors within the system to transfer data to and from the device.

Security standards

The following criteria are recommended for choosing communications programmes and applications to prevent eavesdropping, spying and unauthorized access to personal information.

- **Communications should be encrypted** between the sender and the recipient, using end-to-end encryption (E2EE), so that even the company or service provider cannot access the content of messages. Messages issued by the sender are encrypted and not decrypted until they reach the recipient's device.
- **No tracking**, meaning that the company that produced the application does not track contact information or collect user data. Most commercial companies collect information about the user and sell it to other companies or countries, such as advertising and marketing companies.
- The application or programme should be **open source**, as discussed above. Open-source software provides the code for applications and programmes to technicians for evaluation and detection of weaknesses. Open-source code also allows a review of whether the producing company collects user information and data. It is best to use programmes with a strong track record and to clearly understand security programmes and privacy policies.
- **An anonymity feature should be available**, meaning that the programme or application can hide the user's personal information (name, phone number, email, geographic location and device ID) even while sending and receiving messages, voice calls and attachments (including .doc, .pdf, .jpeg, .mp3, etc.).

Many users wonder if common applications, including Facebook Messenger, Viber, Telegram, WhatsApp and others, meet the above criteria. A review of the transparency reports that companies periodically produce and evaluations by security technicians indicates that, unfortunately, these applications adhere to *some* of the above standards but often do not meet *all* of them.

Recommendations for secure communications applications

The following criteria are recommended for choosing communications programmes and applications to prevent eavesdropping, spying and unauthorized access to personal information.

Signal

Signal Private Messenger is widely considered one of the safest applications for maintaining privacy and adheres to all aforementioned criteria with one exception: anonymity. Signal requires a phone number to activate it; however, it does not track information or collect user information.

Wire

This application meets the above standards, with an easy user interface. It is available for phones and computers. It does not need to be installed as a programme or application – it can be used within a browser as an extension.

Jitsi

JITSI MEET is a platform for communicating or holding online meetings. Its advantage over other web-based meeting programmes is that it creates an encrypted channel for communications and maintains anonymity. It is not necessary to create an account or enter any personal details. Users may visit the website via a browser, open a chat and share the link with anyone they want to invite to the conversation. The Jitsi application may be installed on computers and mobile phones.

Tresorit

This service also encrypts information from end-to-end. It has a simple interface and maintains the security of information, encrypting it during transmission.

How to send secure (encrypted) emails with PGP

The following criteria are recommended for choosing communications programmes and applications to prevent eavesdropping, spying and unauthorized access to personal information.

The best way to ensure emails are secure is to encrypt them with "PGP", which stands for "pretty good privacy". This is an encryption system used for both sending encrypted emails and encrypting sensitive files. PGP encrypts emails and their attachments to increase the confidentiality of communication by generating a pair of private and public keys needed to "open" the information.

More information on the encryption of emails can be found here.

Note:

PGP is only useable when both the sender and recipient use applications or programmes intended for encrypting and decrypting messages. Many programmes and applications use the OpenPGP standard, so each user does not need to have exactly the same programme; however, they must be equipped to "exchange keys". Communicate with contacts about the best way to establish secure communications before attempting to send encrypted emails.

Mailvelope is a recommended programme that can be used with popular webmail providers such as Hotmail, Outlook, Gmail and Yahoo. It can be added as an extension to browsers including Google Chrome and Firefox. It generates the necessary public and private key pair, then shares the public key with other users for them to add it.

b. Save and store information securely

Users should both encrypt information they share with others and encrypt their own information to securely store it. This section provides a guide to the different ways encryption can be used to store data on a user's devices and in the cloud.

Saving photos, videos and data to a device

Tella is an example of an application that helps keep data more secure. It is used by activists, human rights defenders, civil society organizations, media and specialists in humanitarian work and documentation. It is currently only available for Android devices but an iOS version is in development.

- It is easy to use, with a simple interface.
- Users lock the application via the “pattern method” by creating a shape.
- Users can change the application icon so it cannot be recognized.
- It has a “quick delete” feature to erase data in case the user faces the danger that his or her phone may be seized.
- The application itself can be permanently deleted in cases of immediate danger.

Encrypting and storing files using cloud services

Although many people save and store their sensitive files on their computers or in external hard drives (without encrypting them), this tactic is risky. If unauthorized access occurs, these devices can be taken over and decrypted or individuals could force the user to open the encryption.

It is very important not to leave sensitive information on devices, as this can put the user at risk both online and offline. Storing information securely in the cloud ensures that unauthorized third parties cannot access sensitive information. Users should avoid leaving traces of data on devices that could cause security problems.
“Cloud services” are infrastructure platforms or software hosted by third-party providers made available to users through the Internet.

The following secure cloud services are recommended for storing sensitive information without leaving physical traces:

- Google Drive
- pCloud

It is still important to encrypt data before uploading it to the cloud.

Encryption software

At the time of publication, **VeraCrypt** is a secure open-source programme that encrypts data and saves files on the user’s computer. Only the user can view the data by using a key to decrypt it. VeraCrypt can encrypt data, files and folders, but it can also encrypt entire external volumes such as USB flash drives, hard drives or parts of hard drives. It can be used on Windows, Mac and Linux.

VII. Erase data securely

When a user “deletes” data from a computer, smartphone, digital camera or other device, the data are not actually destroyed. Deletion simply “hides” the data from the user but does not erase them from the device.

This section describes how to securely and permanently erase data, and covers the basic terms associated with security scanning, how the process is conducted, and what safe programmes and applications can be used to erase information so that it cannot be recovered.

It is important to understand the differences among key terms:

Deleting

When something is **“deleted”** from a device, it is simply “hidden”. It is not removed from existence – it can be recovered.

“Hide me, but I’ll be here if you really need to recover me.”

Erasing

Erasing data means it is **“missing”** from the operating system. Before erasure, users often receive advance warnings stating that the data cannot be recovered. Since the operating system cannot see the data, the drive is empty when its contents are reviewed. Data may be erased by “wiping” or “shredding”.

“Are you sure? You’ll NEVER see me again!”

Wiping

When a hard drive or storage device is **“wiped”**, everything contained on it is erased, including anything a user previously deleted that could still be recovered.

“I’m going to erase EVERYTHING.”

Shredding

When a piece of data (usually one or more files or folders) is **“shredded”**, only the specifically selected item(s) are erased and nothing else.

“I’m going to erase this and only this.”

Common questions:

Question

Does deleting files from the desktop and emptying the recycle bin mean that files are permanently and irreversibly removed from the computer or smartphone?

YES [✓ **NO**]

No. Deleting data and emptying the recycling bin marks the space as “available”, but until the “available space” is written over with new information, the underlying data can still be recovered.

Question

Does reformatting a hard drive permanently and irreversibly remove data?

YES [✓ NO]

No. Reformatting is a great way to "delete" data – not "erase" it! The reformatting process marks all space on the device as "available"; however, underlying data can still be recovered until it is written over with new information. This is an acceptable process if the same user is planning to reuse the drive but it does not automatically eliminate sensitive information.

Techniques for recovering deleted files are improving every day, and many types of supposedly "deleted" files (photos, documents, videos, etc.) can be recovered. Disk wiping or shredding ensures that the "available" space created by simple deletion is overwritten, rendering the underlying data unrecoverable.

How to clean devices

To clean a (Windows) computer (delete temporary files and clean up system files), use the system's **Disk Cleanup tool** as follows:

- Go to the Start Menu, then All Programmes, then System Tools, and then select Disk Cleanup (or type Disk Cleanup in the search box, which will open the application).

How to permanently erase or wipe data

One of the most important parts of data wiping involves wiping underlying layers of information and overwriting them with new data. This permanently prevents the possibility of recovery.

- Eraser is a security tool for Windows that completely removes sensitive data from your hard drive.
- BCWipe is a programme for erasing and wiping information.

If you are disposing of your computer system, it is recommended that you remove the hard drive and RAM and destroy them separately and securely as they can contain data.

VIII. Prevent phishing

“Phishing”, also called electronic fraud, electronic solicitation and electronic theft, is a collection of tactics and techniques used to steal or obtain personal information, passwords, business information, financial accounts, etc.. Phishing is one of the most common ways to target users. Preventing phishing is one of the easiest ways for users to protect themselves from becoming a victim.

In simple terms, an attacker exploits a user through a deceptive process or uses social engineering techniques to encourage or force the victim to respond to the attacker’s request. The request usually involves convincing a user to:

- Click a link
- Share information
- Give permissions
- Download files infected with malicious software

An attacker usually waits for the target to make a mistake, and then can obtain the victim’s information and access his or her accounts.

Types of phishing

There are many types of phishing, including:

Spear Phishing

A sophisticated technique that targets a specific person or a group. The attacker collects information about the victim and then uses it to formulate a message that ***appears to be real***. This kind of phishing is generally conducted through emails targeting the victim.

Whaling

Spear phishing technique targeting especially influential and powerful people within companies or organizations.

Pharming

A type of fraud in which the attacker directs the victim from a main/reputable site to another fake site or a site compromised with malicious software. A victim’s information can be intercepted when they enter the site.

Smishing

The use of SMS text messages to defraud the victim by prompting him or her to disclose information about accounts, obtain multifactor authentication numbers or download malicious software into the victim's device.

Search engine phishing

The attacker creates a website on the Internet, puts it on search engines or social media, and offers goods at cheap prices, luring the victim to pay for a product. The victim then enters his or her bank account information, which is stolen and used.

Voice phishing

The attacker uses a voice phone call to trick the victim into believing that the caller is from an official body in order to obtain information from the victim.

How to protect yourself from digital phishing

More information on phishing and examples of phishing emails are available here.

All users should be extremely careful and follow these tips:

1. **Never share sensitive or personal information** with others, and never publish it on social media under any circumstances.

2. **Do not respond under any circumstances to threats received** via messages, emails or social networking sites. Do not interact in any way with those making threats.

3. **Do not open links received**, even from close contacts, without checking them first.

   a. Use Virus Total to check links and files. Do not click links immediately upon receipt – copy the link, open the website, paste the link into the URL Links window, and click Enter. If the result is 0, the link is malware-free. Do not click the link directly – copy and paste it into the browser. If the link is a normal content link, the content will appear in the browser.

4. **Ensure the sites you access have a security certificate and that the link starts with "https://"**. A padlock icon next to the URL in the browser's address bar means that SSL (secure sockets layer) protects the website a user is visiting. SSL keeps Internet connections secure and prevents unauthorized users from reading or modifying information transferred between two systems.

5. **Check the address or phone number of emails and SMS messages**. Often attackers will disguise addresses to make them look similar to reputable contacts, but on closer inspection they do not match the website or person they are pretending to be.

6 **All services you have subscribed to know your name, and their communications to you will include your name.** Any message addressed “to our dear subscriber”, “kind customer” or similar phrases may be a fraudulent message: Take care in handling it.

7 **Any gift or prize you receive is fraudulent** if you have not participated in a competition or contest. Do not engage.

8 **If you receive an email or other communications requesting sensitive information, contact the sender directly via a different method to inquire about the message.**

9 Protect devices with **Internet security and anti-malware programmes**, and **do not install “cracked” or pirated software.**

10 **Enable two-step verification** on all accounts.

IX. References and further reading

For more information, resources and ongoing updates, see the following resources:

1. **Afghanistan Digital Care Guide** (English): This guidance presents information on risks, prevention measures, response steps and important decisions.
2. **Online safety resources for Afghanistan's human rights defenders** (English): As the crisis continues, this information helps you to improve online safety.
3. **Safety of social media** (English): Presents guidance on how to keep safe smartphones and messaging applications.
4. **Set a killer password** (English): Describes how to create a strong password.
5. **Safety of the browser** (English): Makes recommendations on how to change browsers to incognito mode and use VPN.
6. **Security risks** (English): Presents information on protections in virtual spaces.
7. **Evading the misuse of biometric data** (English): What we should do and not do with biometrics.
8. **How to thwart digital surveillance** (English): Guidance on masking a file location, securing data and information, protecting yourself from malware, and online file storage.
9. **How to delete a digital history** (English): Keeping safe and deleting email and social media accounts.
10. **Internet shutdowns and blockages** (English): Usage of VPN and secure communications during Internet shutdowns and blockages.
11. **A toolkit for civil society organizations** (English): Information on advocacy in restricted spaces.
12. **Front Line Defenders** (English): Information and support on digital and other security risks for human rights defenders.
13. **Security-in-a-Box** (English): Digital security information, training guides and other resources.
14. **Surveillance self-defense** (English): Tips and tools for safer online communications, run by the Electronic Frontier Foundation.
15. **Digital security helpline** (English): Provides rapid-response emergency assistance.

XI. Emergency assistance

In case of emergency, please refer to the following addresses:

1. Front Line Defenders (emergency contact)

2. Reporters Without Borders

3. Afghan Journalists Safety Committee (safety-committee.org)

4. Window for Women Human Rights Defenders of the Women's Peace and Humanitarian Fund (wphfund.org)

5. The Crisis Response Fund (civicus.org), with urgent funding for civil society actors

6. The European Union Human Rights Defenders Mechanisms (ProtectDefenders.eu – You have the right to defend rights)

X. Cybersecurity glossary of terms

Unless otherwise noted, the following definitions are from the United Nations Terminology Database (UNTERM).

- **Adware:** A type of software application that displays adverts of some kind while it is running. Sometimes developers will offer a "free" version of their software on the condition that you have to view adverts; they get paid by the number of people clicking on the ads. Quite often, there is also a paid version of the same software that is advert-free.

- **Cache:** A temporary storage area where frequently accessed data can be stored for rapid access.

- **Cracked software:** A "crack" or a "patch" is a programme designed to activate, register or extend the trial period of a proprietary programme that normally requires a serial number to prevent piracy and unauthorized use. Using a "crack" or "patch" to access software programmes is always illegal.[5]

- **Encryption technology:** Enables the user to shield data saved on USB drives, mobile devices, flash disks, pen drives, CDs or hard disks. An encrypted document cannot be read or viewed by unintended recipients, even if they have possession of the document itself.

- **End-to-end encryption (E2EE):** The application of encryption to communications tools and services, such that only the users of the tool or service have access to plain-text messages. Many forms of encryption are deployed by service providers to secure communications in a way that prevents unauthorized third-party access, but the service provider implementing it still has access to the relevant user data.

[5] See Wikipedia on "software cracking".

- **Firewall:** A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in hardware and software, or a combination of both.

- **IP address:** A unique number that information-technology devices use to identify and communicate with each other on a computer network, based on the Internet Protocol (IP) standard. Any participating network device – e.g., routers, computers, printers, fax machines – must have its own unique address. It is the equivalent of a street address or a phone number for a computer or other network device on the Internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or another device on a network.

- **Keylogger:** A tool that records user activity, such as keystrokes, and that can send this information to an attacker using email or other methods.

- **Malicious software or "malware":** Software designed to infiltrate or damage a computer system without the owner's informed consent. Software is considered malware based on the perceived intent of the creator rather than any particular features. It includes computer viruses, worms, trojan horses (trojans), spyware, dishonest adware and other malicious and unwanted software. The word "malware" is a combination of "malicious" and "software".

- **Onion routing:** The technological basis of the Tor network. The name is derived from the onion-like structure of the encryption scheme used, which is secured several times over many layers. The goal of onion routing is to use the Internet with as much privacy as possible, routing traffic through multiple servers and encrypting it at every step.[6]

- **Open-source software:** This is a generic term for software (applications and system software) where source code is openly available to any user. A programme can be used, copied, studied, modified and redistributed without restriction.

- **PGP:** This stands for "pretty good privacy", an asymmetric public-key encryption software capable of ensuring the confidentiality and authenticity of electronic communications.

- **Phishing:** A tactic for committing online fraud and identity theft. For example, a "phisher" sends out an email that poses as a legitimate business request – for example, from a bank asking customers to verify financial data. The email includes a link that purports to go to a legitimate banking website. The site is bogus, however, and when the victim types in account numbers, passwords or other sensitive information, those data are captured and subsequently used by the phisher to commit fraud.

- **Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid. Some forms of ransomware encrypt files on the system's hard drive (a.k.a. cryptoviral extortion), while others simply lock the system and display messages intended to coax the user into paying.

- **Spyware:** Computer software that collects personal information about users without their informed consent. Personal information is secretly recorded with a variety of techniques, including logging keystrokes, recording an Internet web browsing history and scanning documents on the computer's hard disk.

- **Trojan or Trojan horse:** A programme that appears legitimate but performs some illicit activity when run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy the user's stored software and data. A Trojan is similar to a virus, except that it does not replicate itself.

[6] For more information, see The Tor Project at: https://www.torproject.org.

- **VPN:** A “virtual private network” offers a controlled pathway through the Internet to which only authorized users have access and along which only authorized data can travel.
- **Worms:** A computer term referring to malicious parasitic programmes, similar to viruses, that replicate and spread across networks looking for vulnerable machines to infect. Unlike viruses, worms do not infect other computer programme files. Worms can create copies on the same computer, or can send copies to other computers via a network.

UN Women Afghanistan Country Office
www.unwomen.org
www.unama.unmissions.org

UNAMA

UN WOMEN