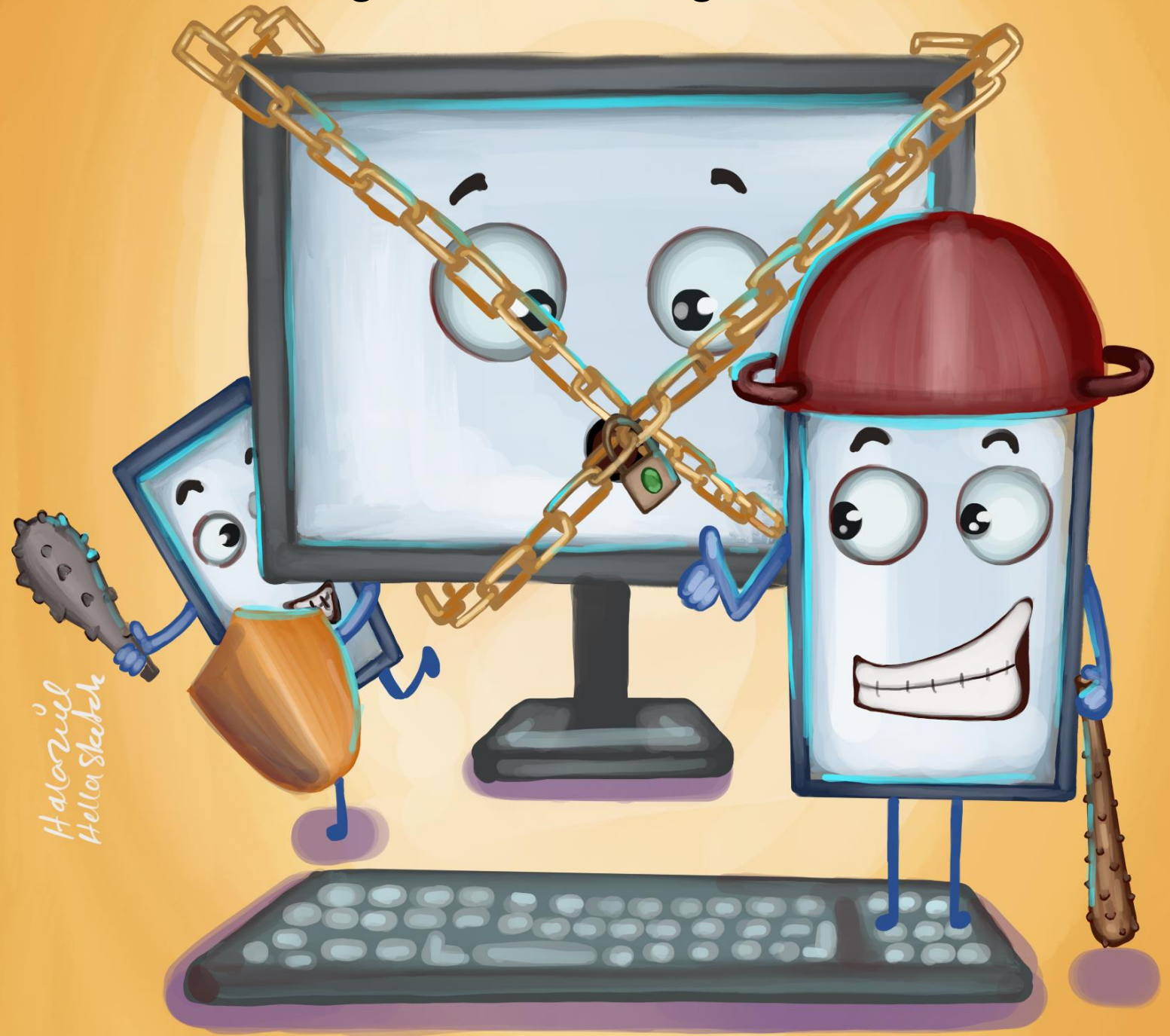


# Online Protection and Digital Security

## User guide for human rights defenders



*Hazarziel  
Hella Skabeh*

# #BeSafe



Human Rights Office  
United Nation Assistance Mission for Iraq  
(UNAMI)  
بعثة الأمم المتحدة لمساعدة العراق  
(يونامي)



الشبكة العراقية  
للإعلام المجتمعي

## Article 19

### Universal Declaration of Human Rights

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.





Digital Safety Manual by INSM\_Network is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

**Disclaimer**

- 1. Introduction**
- 2. “Top Ten” basics of computer and mobile protection**
- 3. Create strong passwords and enable multi-factor authentication**
  - Strong passwords
  - Multi-factor authentication (MFA)
- 4. Eliminate malware**
  - What is Malware?
  - How to protect devices from malware
- 5. Browse the Internet safely**
  - Securing your router
  - Using public Wi-Fi hotspots
  - Protect yourself using public Wi-Fi
  - Use safe browsers
  - Use safe search engines
  - Use safe browser extensions/add-ons
- 6. All about encryption**
  - What is “encryption”?
  - a. Communicate safely**
    - What is “secure communication”?
    - Security standards
    - Recommendations for secure communications applications
    - How to send secure (encrypted) emails with PGP
  - b. Save and store information securely**
    - Saving photos, videos, and data to a device:
    - Encrypting and storing files using cloud services:
    - Encryption software:
- 7. Erase data securely**
  - How to clean devices
  - How to permanently erase or wipe data:
- 8. Prevent phishing**
  - Types of phishing
  - How to protect yourself from digital phishing
- 9. References and further reading**
- 10. Cybersecurity glossary of terms**

## Disclaimer

The United Nations Assistance Mission for Iraq (UNAMI)'s Human Rights Office welcomes the opportunity to promote its activities and publications in cooperation with its 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 UNAMI.

While the authors of this document endeavored to provide up-to-date and correct information at the time of publication, information technology and digital security threats change rapidly and therefore accuracy cannot be guaranteed at all times. As such, UNAMI makes no representation or warranties of any kind about the completeness, accuracy, reliability, suitability or availability with respect to the information, products or services contained herein. Users should verify the current accuracy and security of information or software prior to use. Resources are provided at the end of this guide to help users stay current on secure methods and software.

## safeguarding human rights online in Iraq



### Human rights apply equally online and offline

In his Call to Action<sup>1</sup> for Human Rights, the United Nations Secretary General emphasized that digital technologies have opened up new frontiers, providing new means to advocate for, defend and exercise our rights. At the same time, these new technologies are too often used to violate human rights and shrink civic space, including through online surveillance, repression, censorship and harassment.

In Iraq, human rights defenders increasingly rely on digital technologies to monitor, document, report, and advocate for human rights. Journalists, civil society organizations, activists, and other members of the public go online to share their opinions, promote debate and generate support. For example, when widespread anti-Government demonstrations started on an unprecedented scale in October 2019 in multiple governorates across Iraq, the online space provided a key platform to mobilize and organize, share real-time information and report on developments, including human rights violations.

At the same time, however, online platforms can also serve as sites for threats, intimidation and harassment of protestors, including by hacking into private accounts or “doxing” individuals, exposing them to additional offline security threats. Moreover, cases of piracy, electronic extortion, data theft, intellectual property infringement and violations of privacy continue to rise in Iraq.

Effectively safeguarding human rights online poses enormous challenges due to constantly evolving technologies and the ‘invisibility’ of perpetrators. Within this

---

<sup>1</sup> The [Call to Action](#) is the Secretary-General’s transformative vision for human rights. Underpinning the work of the entire UN system, human rights are essential to addressing the broad causes and impacts of all complex crises, and to building sustainable, safe, and peaceful societies

context, individual users of digital technologies need to stay abreast of developments and take proactive measures to protect their privacy, safety, and data confidentiality.

This guide has been developed by the Iraqi Network for Social Media (INSM), with the support of the Human Rights Office, United Nations Assistance Mission in Iraq (UNAMI) to provide in particular human rights defenders with practical tools to protect themselves from hackers and other abusers. The guidelines form part of the “Digital Rights and Digital Security” project, which has been implemented since 2021 by INSM with UNAMI’s support, to raise awareness and mitigate online risks while increasing the protection of Iraqi human rights defenders in the digital space.

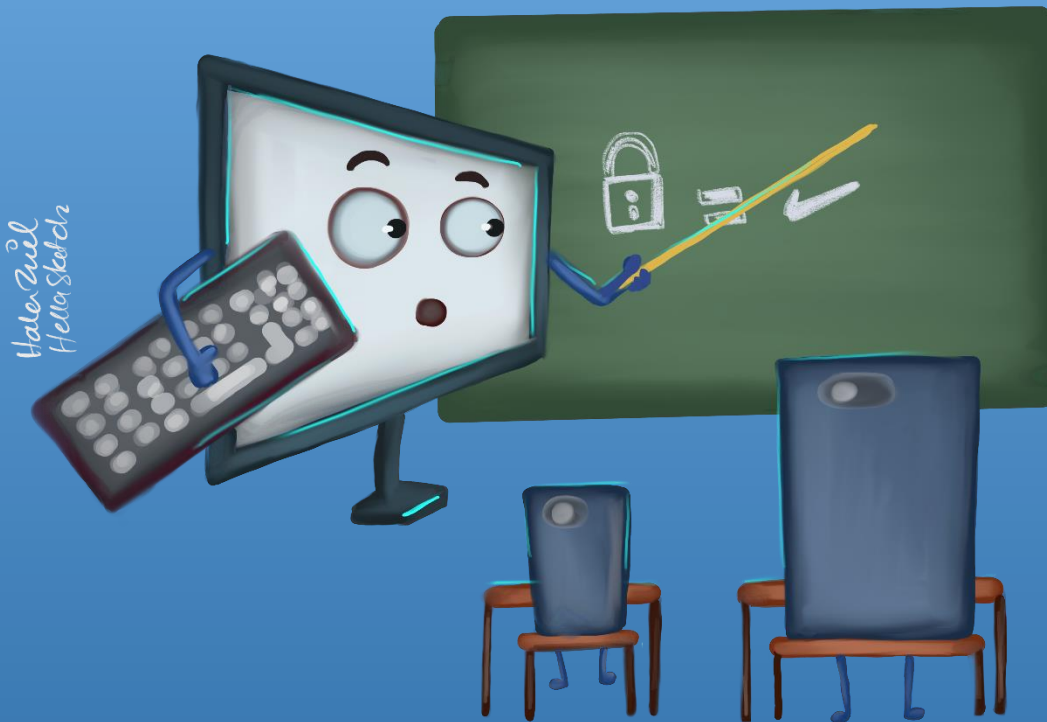
This manual is for everyone. It guides users through the basic steps and tools they need to address digital risks and prevent online and offline danger.

**#Be\_Safe**



# 02

## basics of computer and mobile protection



01

Update operating system, hardware, applications

02

Create strong passwords on all devices

03

Use Multi-Factor Authentication (MFA) whenever possible

04

Install (Anti-Malware) software

05

Use a safe browser

06

Install a Virtual Private Network (VPN)

07

Use safe open-source software and applications

08

Only download apps and software from recognized App Stores

09

Encrypt computers and phones

10

Backup your data

## **“Top Ten” basics of computer and mobile protection**

**T**his section provides the “Top Ten Tips” for improving a user’s digital security. These basic steps provide an entry point to the main topics covered in-depth in later chapters.

### **Tip 1: Update operating system, hardware, applications, phone and software regularly.**

Companies provide periodic updates to 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 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 upper 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 Multi-Factor Authentication (MFA) whenever possible**

- Multi-factor authentication dramatically increases digital security.
- Applications specifically designed for multi-factor 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.
- Install programs 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 is 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 Tor, Firefox, Brave, Firefox Focus, Ghostery Dawn, and DuckDuckGo; regularly update browser software.
- Check the security of add-ons/browser extensions before adding them to the browser.

See [Section V](#) below for more information.

### **Tip 6: Install a Virtual Private Network (VPN)**

- VPN stands for “virtual private network” – a service that 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 for safe use of public WiFi. Without a VPN for protection, devices and their locations may be tracked or data may be 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, or Riseup VPN.

See [Section III](#) below for more information.

### **Tip 7: Use safe open-source software and applications**

- “[Open-source](#)” software and applications are generally more secure than proprietary programs, 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 using pirated or “cracked” proprietary software without a license. Pirated or “cracked” programs may contain malicious elements that harm devices and should never be used.
- Be aware that not all open-source programs are secure: always follow the advice of digital security experts before installing a new software or application.

### **Tip 8: Only download apps and software from recognized App Stores**

- Unrecognized App Stores contain dozens of applications and programs 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.

### **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 on encryption tools.

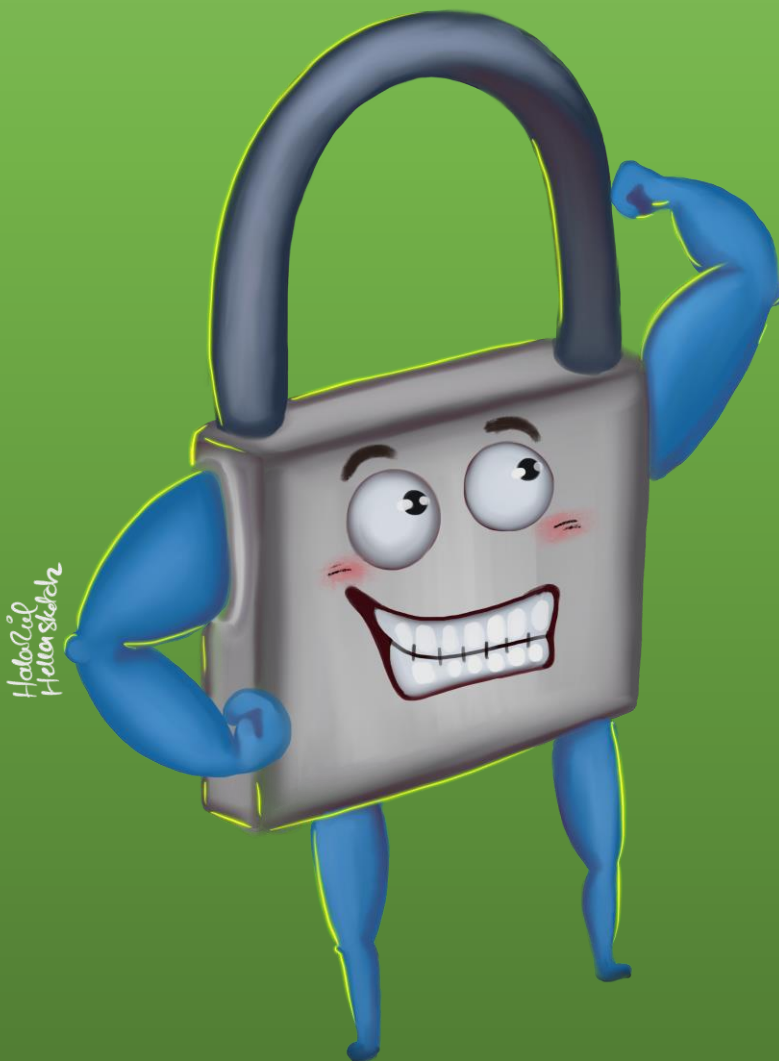
### **Tip 10: Backup your data**

- The backup process is like storing valuable information in a safe so that it can be recovered if the original data is every lost, damaged or hacked.
- Manually activate the backup tool that is 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., [Mega](#).

# 03



Create strong passwords and  
enable multi-factor



## Create strong passwords and enable multi-factor 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 others attacks aimed at intercepting data or gaining unauthorized entry to protected accounts or data.<sup>2</sup>

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.
7. **Periodically changed:** How long a password may be used before changing depends on the level of risks each user faces. In normal situations it is recommended to change passwords every three months. When changing a password, a user should fully exit the application or service on all devices.
8. **Original:** Do not use common keyboard patterns, e.g., 'Qwerty12345' or 'Password123'

---

<sup>2</sup> Attacks aimed at revealing passwords include man-in-the-middle (MITM), brute force and dictionary attacks, and credential stuffing. To learn more about common password attacks, see [Password Cracking 101: Attacks & Defenses Explained](#).



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](#)

### **Multi-factor authentication (MFA)**

Activating the multi-factor authentication feature on accounts provides serious protection from hacking and phishing. Multi-factor 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 either sent to the user via SMS, email, or accessed via a specific authentication application.

Many users activate this feature via SMS text message on their mobile phones. However, using SMS-based multi-factor authentication has additional risks in Iraq, due to vulnerabilities used to attack SIM cards (called “Simjacker” attacks<sup>3</sup>).

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

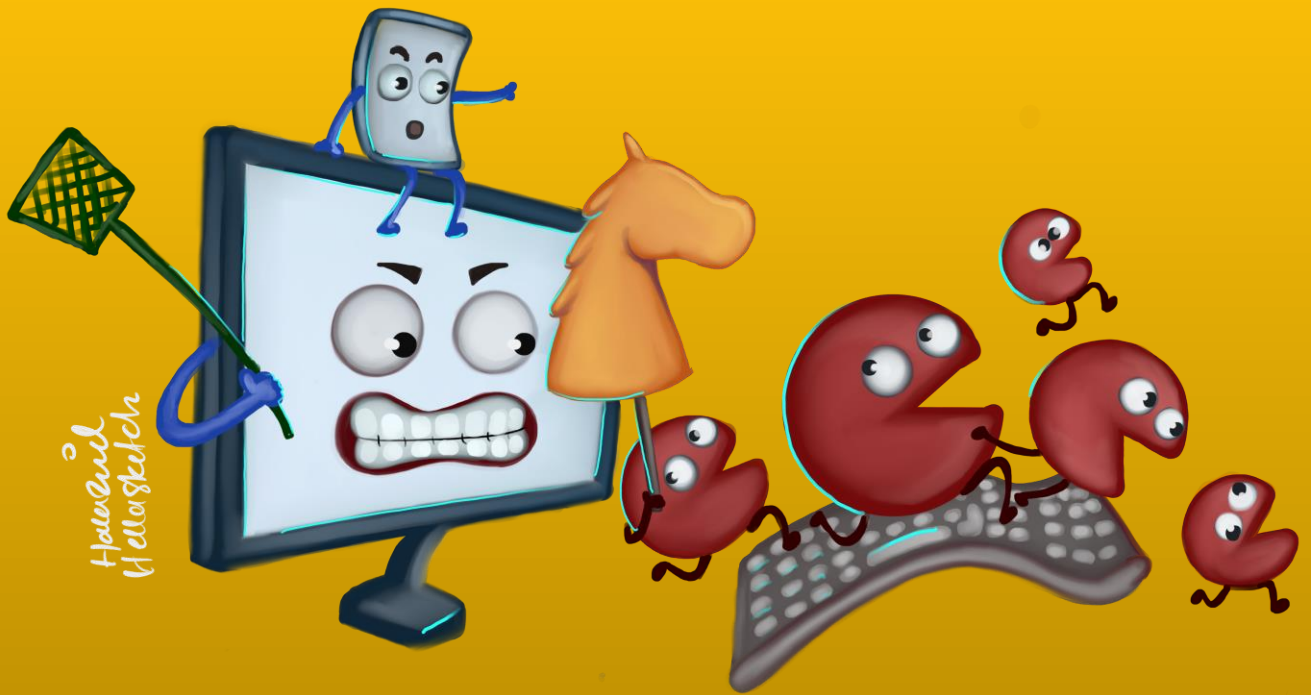
1. [Duo Mobile](#)
2. [Aegis Authenticator](#) (for Android only)
3. [Google Authenticator](#) ([iOS](#) or [Android](#))

---

<sup>3</sup> According to a report published in October 2019, Iraq is among the list of 29 countries in which telecom segments suffer from a loophole increasing vulnerability to Simjacker attacks. Some SIM cards contain a pre-installed Java applet called the S@T Browser, which, if incorrectly configured, can open the SIM to malicious commands from attackers, fraudsters, and censors who wish to gain access to a user’s phone content. See ZDNet, These are the 29 countries vulnerable to Simjacker attacks, 11 October 2019, available at: <https://www.zdnet.com/article/these-are-the-29-countries-vulnerable-to-simjacker-attacks/>

# 04

## Eliminate malware



## Eliminate malware

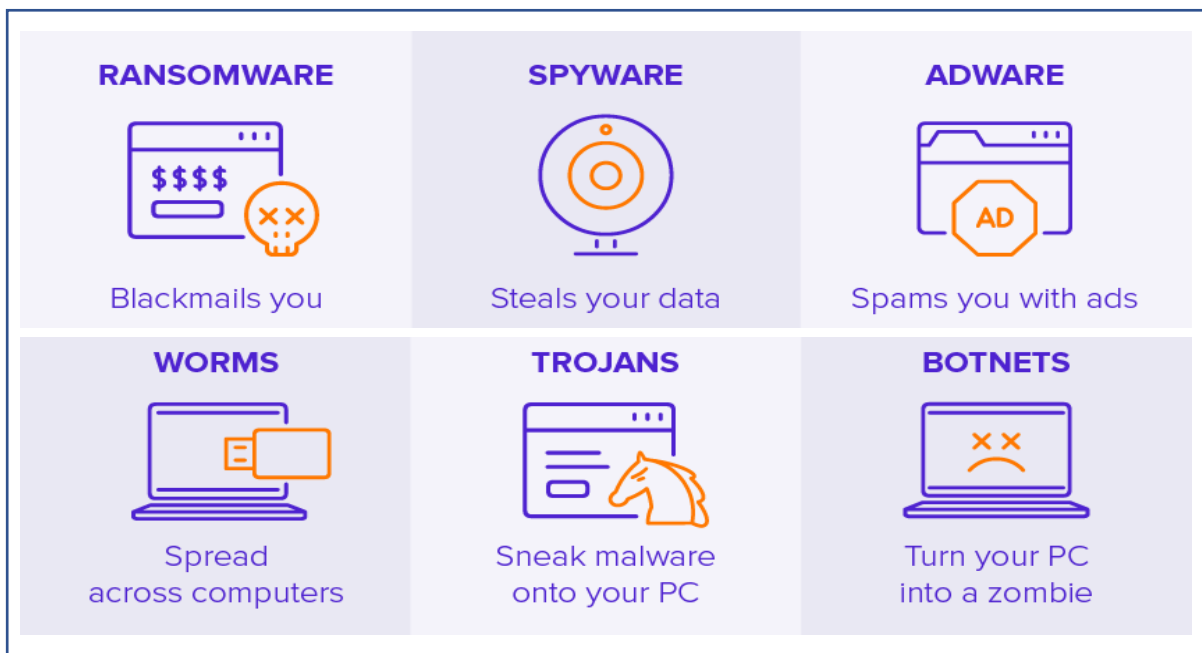
### What is Malware?

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, while 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.

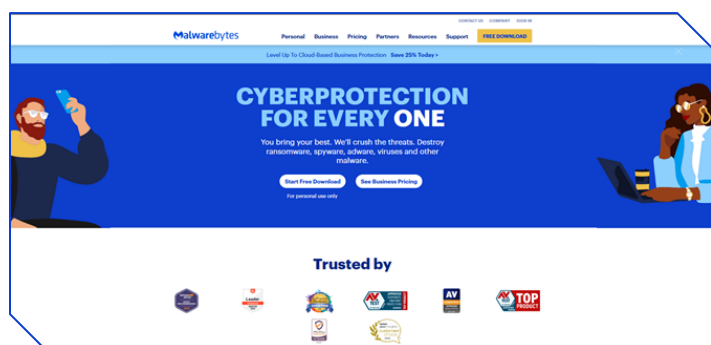


## How to protect devices from malware

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

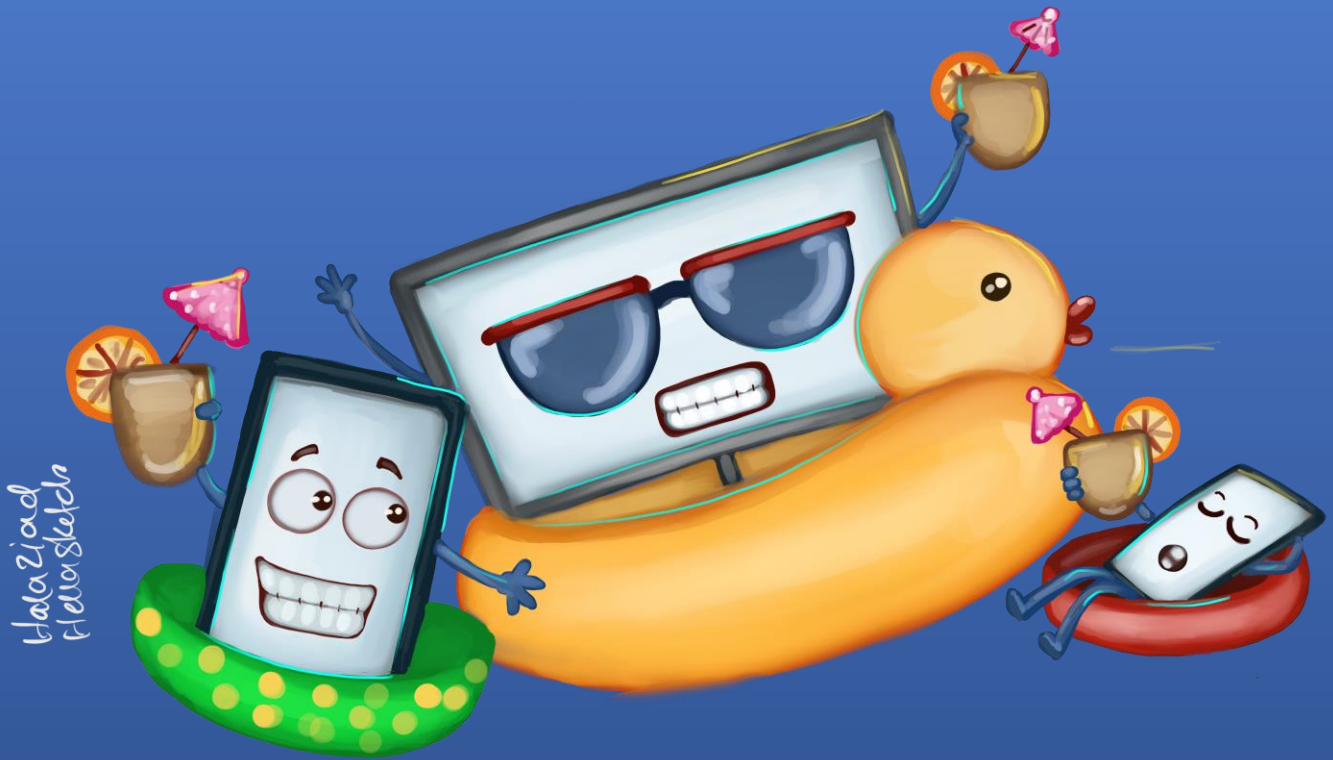
1. Install reliable Endpoint Detection and Response (EDR) software on every device running Windows, Mac, Linux, iOS or Android systems, including all computers and mobile phones. Note that only one EDR program should be installed.
2. Only download programs and applications from their official websites.
3. Regularly update each device's operating systems and applications.
4. Avoid using public and/or unsecured WiFi networks without the 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 browser while browsing the Internet.
8. Install recommended security add-ons for the browser.

Two EDR programs considered safe at the time of publication (both free and paid versions) are Malwarebytes and Avira.



# 05

## Browse the Internet safely



## 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.<sup>4</sup>

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 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, airport, public transportation, restaurants, etc.) are usually weak in security and can pose serious threats to the user, 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 using public Wi-Fi

Follow these guidelines to protect personal information from attackers while using public communication points:

---

<sup>4</sup> For basic information about how to configure a router, please see Security in a Box, "Protecting against Malware: Secure your Router", available here: <https://securityinabox.org/en/phones-and-computers/malware/>

- Avoid using unknown/insecure hotspots or public internet whenever possible.
- If using a public network, be sure to enable multi-factor authentication for all the accounts before use.
- Use a firewall. Most operating systems include this service, as do anti-malware/Endpoint Detection and Response programs. Applications considered safe at the time of application include:
  - Avira
  - Comodo
  - GlassWire
- Use a VPN service to encrypt internet connection and keep online activity private on any network. VPNs considered safe at the time of publication include:
  - 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:

Tor Browser (available on computers and Android phones) is one of the best browsers available for maintaining security, privacy and anonymity. Activists and journalists operating in environments with security risks, such as in Iraq, may choose to use Tor for its heightened security.

Other browsers considered safe at the time of publication include:

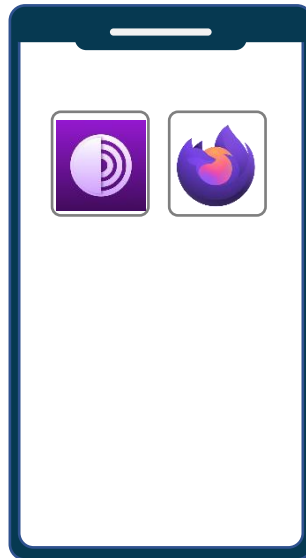
FireFox

Brave

Ghostery Dawn

DuckDuckGo

Firefox Focus



For more information about the pros and cons of different browsers, review the guide published by the Freedom of the Press Foundation available [here](#).

### **Use safe search engines**

Searches should also be conducted using 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:

- [DuckDuckGo](#)
- [Qwant](#)
- [StartPage](#)

### **Use safe browser extensions/add-ons**

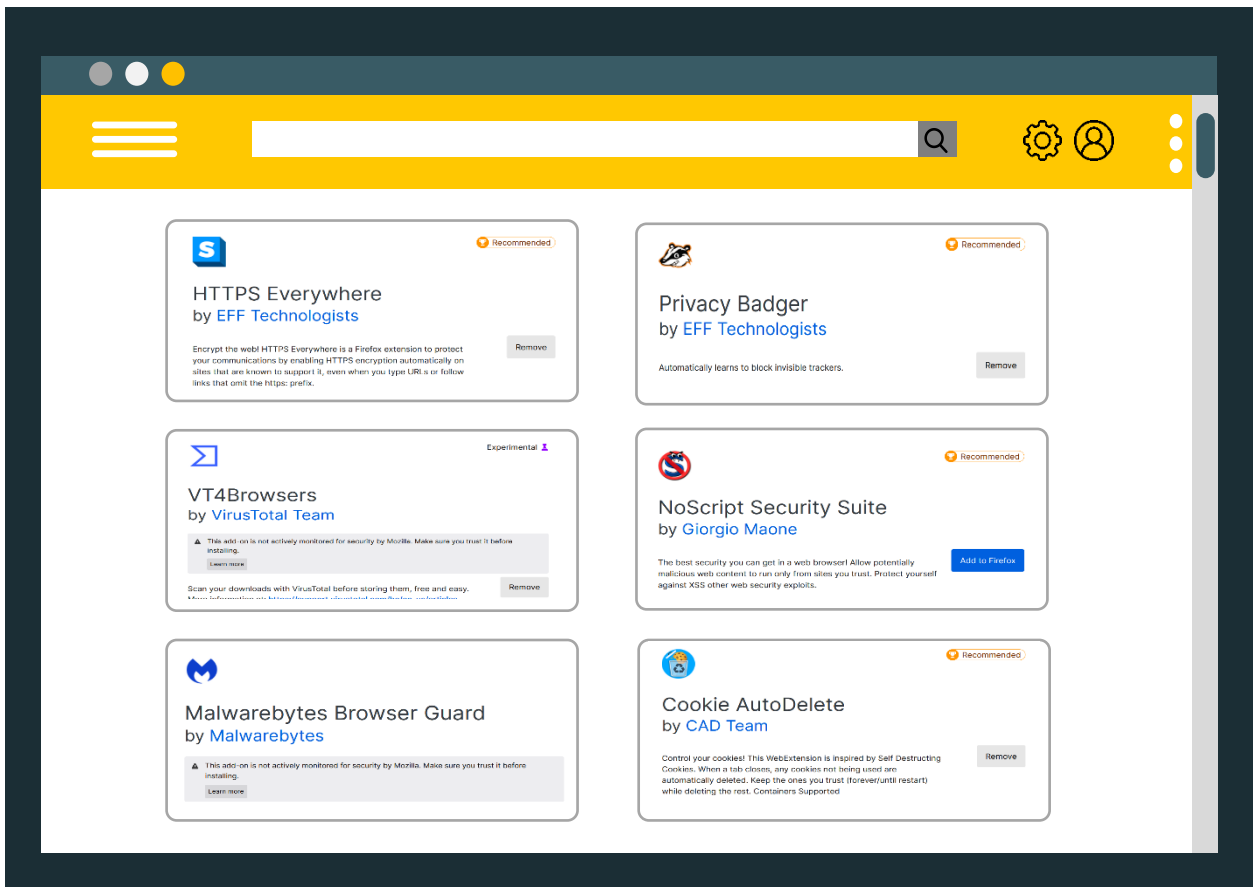
Browser extensions, or “add-ons”, extend the functionality of a program on another program, such as a browser. Add-ons are usually not full versions of software but are rather pieces of code that modify a specific interface. The most common add-ons for browsers are toolbars that provide users with instant 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 provide users with enhanced security:

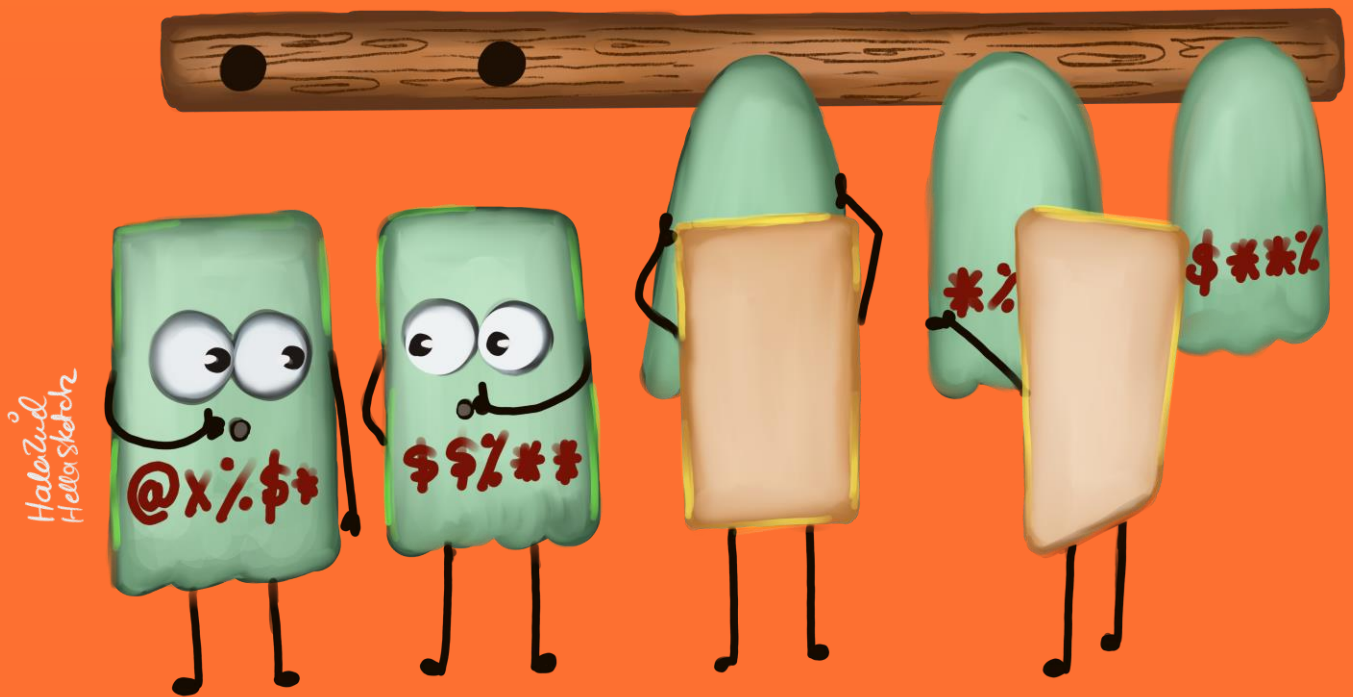


- HTTPS Everywhere
- Virus Total
- Ghostery
- Malwarebytes
- Cookie AutoDelete
- NoScript
- Privacy Badger



# 06

## All about encryption



## 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.

### Encryption has six benefits:

1. Helps maintain data integration and privacy.
2. Helps organizations comply with privacy and security regulations.
3. Protects data as they are transmitted across devices.
4. Helps organizations secure offices.
5. Protects intellectual property.
6. Protects data during transfer to cloud storage.

### Encryption can be used to securely:

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 communication”?

Secure communication is the process of encrypting a user’s communications using one or more security protocols to ensure that data flows between the sender and the 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 would use 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 the communication and access its content, intercept and modify it, 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 communication programs and applications, to ensure communications free from eavesdropping, spying and unauthorized access to personal information.

- **Communication 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 are issued by the sender encrypted and are 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, like advertising and marketing companies.
- The application or program should be **open source**, as discussed above. Open source software provides the code for applications and programs to technicians for evaluation and detection of weaknesses. Open source code also allows review of whether the producing company collects user information and data.
- **An anonymity feature should be available**, meaning that the program 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 sending and receiving 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 indicate that unfortunately those applications adhere to *some* of the above standards, but they often do not meet them *all*.

### Recommendations for secure communications applications

- [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 program or application – it can be used within the browser as an extension.

- **[Signal](#)**: Signal Private Messenger is widely considered one of the safest applications for maintaining privacy and adheres to all of the aforementioned criteria with one exception: anonymity. Signal requires a phone number to activate it; however, Signal does not track information and does not collect the information of users.
- **[Jitsi](#)**: JITSI MEET is a platform for conducting communication or holding online meetings. Its advantage over other web-based meetings programs is that it creates an encrypted channel for communications, and it 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.
- **[OnionShare](#)**: To send large or sensitive files and information to people, institutions, or civil society organizations, the best option is to use OnionShare. OnionShare uses “[onion routing](#)” in the Tor network to transfer information, making it very secure and ideal for human rights defenders. OnionShare has a simple and easy-to-use interface, with multiple versions for Windows, Mac and Linux operating systems. The program also includes a chat platform that supports anonymity.
- **[Tresorit](#)**: This service also encrypts information from end-to-end. It has a simple interface and maintains security of information, encrypting it during transmission.

## How to send secure (encrypted) emails with PGP

The best way to ensure emails are secure is to encrypt them with “[PGP](#)”. PGP 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.

Unfortunately, Using an email that does not use end to end encryption will expose its user to risks, so experts always advise using ProtonMail and Tutanota services or encrypting email messages using PGP

**Note: PGP** is only useable when both the sender and the recipient use applications or programs intended for encrypting and decrypting messages. There are many programs and applications that use the OpenPGP standard, so each user does not need to use exactly the same program; 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 program that can be used with popular webmail providers such as Hotmail, Outlook, Gmail and Yahoo. It can be added as an extension to browsers like 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 not only encrypt information they share with others, they should also 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 and 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:

- [Mega](#)
- [pCloud](#)

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

### **Encryption software:**

**[VeraCrypt](#)**: At the time of publication, VeraCrypt is a secure open source program 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.

# 07

## Erase data securely

HaloZaid  
Hella Skatdz



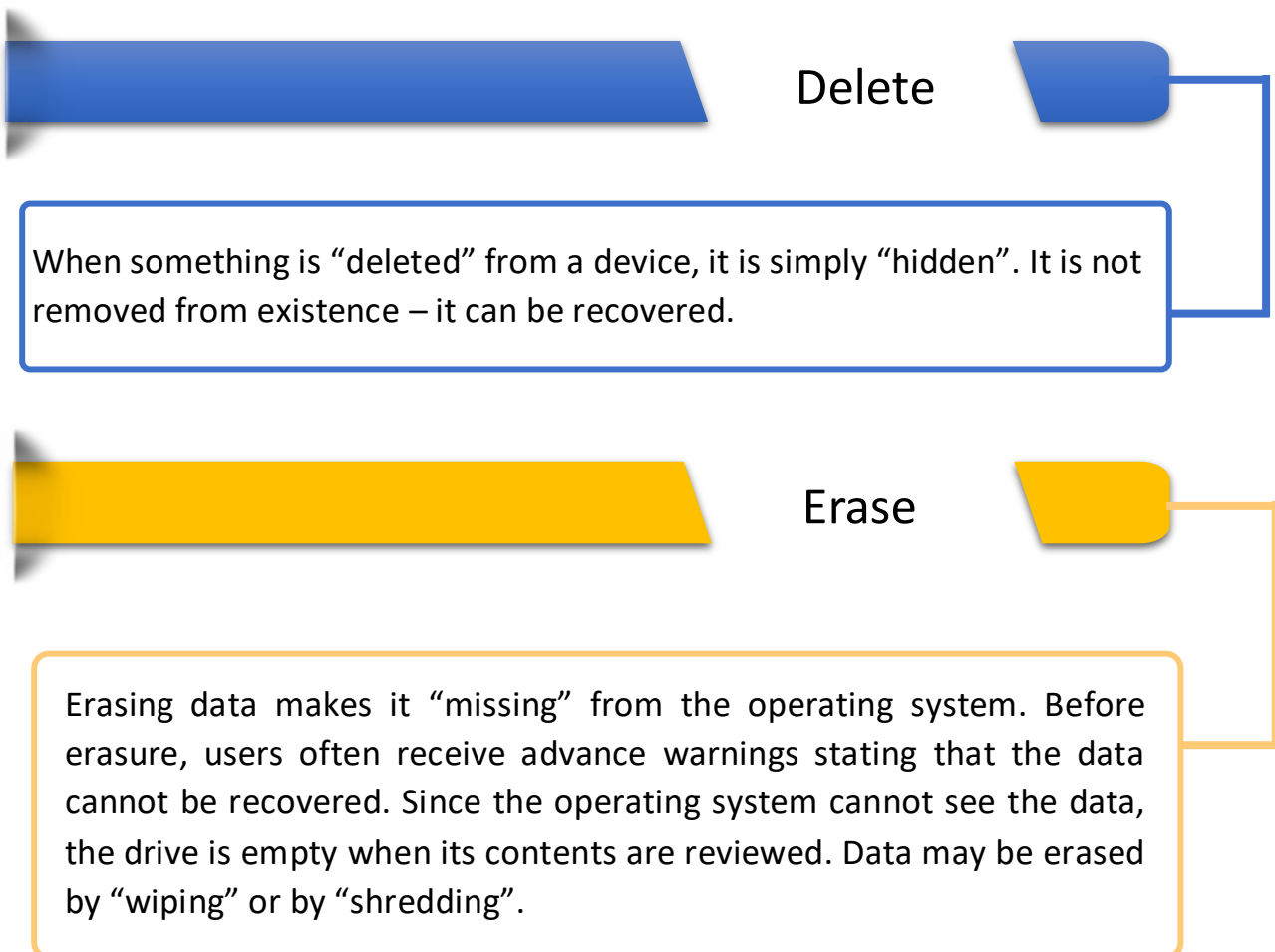



## Erase data securely

When a user “deletes” data from a computer, smartphone, digital camera or other device, the data is not actually destroyed. Deletion simply “hides” the data from the user but does not erase it 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 programs and applications can be used to erase information so that it cannot be recovered.


It is important to understand the difference between these key terms:





Wipe

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.



Shred

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.

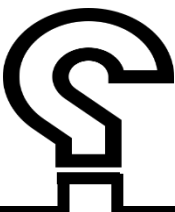
**In other words:**

Delete: "Hide me, but I'll be here if you really need to recover me"

Erase: "Are you sure? You'll NEVER see me again!"

Wipe: "I'm going to erase EVERYTHING"

Shred: "I'm going to erase this and only this"



**Common questions:**

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



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.

Does reformatting a hard drive permanently and irreversibly remove data?



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.

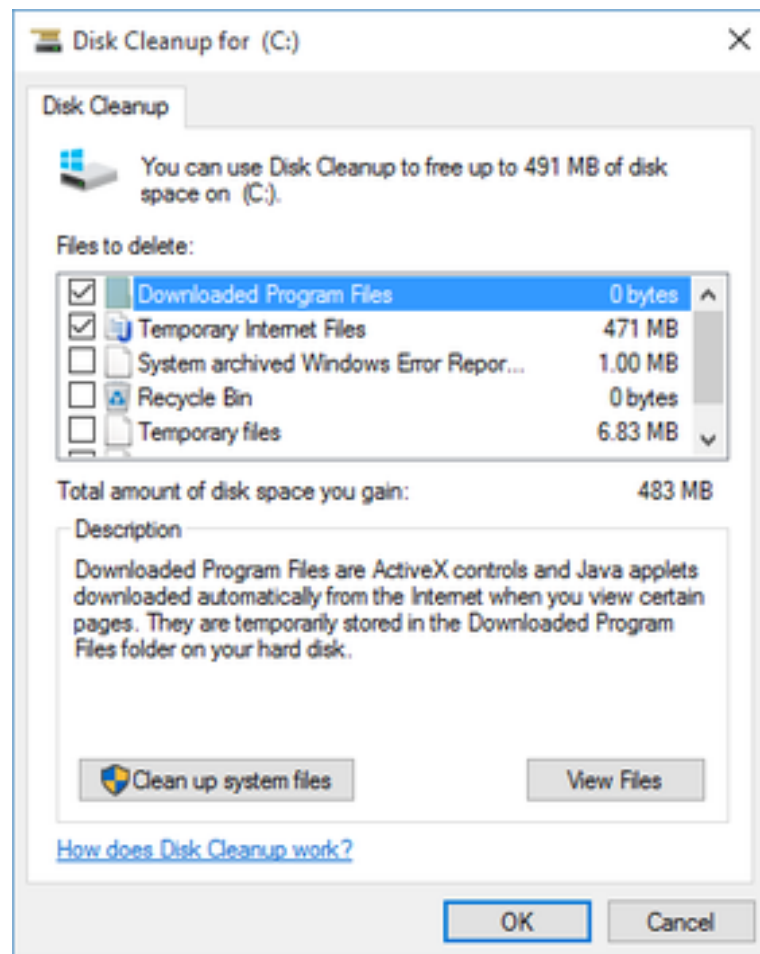
Techniques for recovering deleted files are improving every day, and many types of supposedly “deleted” files (photos, documents, videos, etc.) can be recovered. Disk wiping or shredding ensures that the “available” space created by simple deletion is overwritten, rendering the underlying data unrecoverable.

One of the most common mistakes in Iraq is selling used devices to another party without fully wiping the underlying data. This has caused many problems and lawsuits when information the previous user believed to be erased was recovered. The best advice is not to buy or sell used devices.

## 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 **Start Menu**, then **All Programs**, then **System Tools**, then select "**Disk Cleanup**" (or type "Disk Cleanup" in the search box, which will open the application's location).

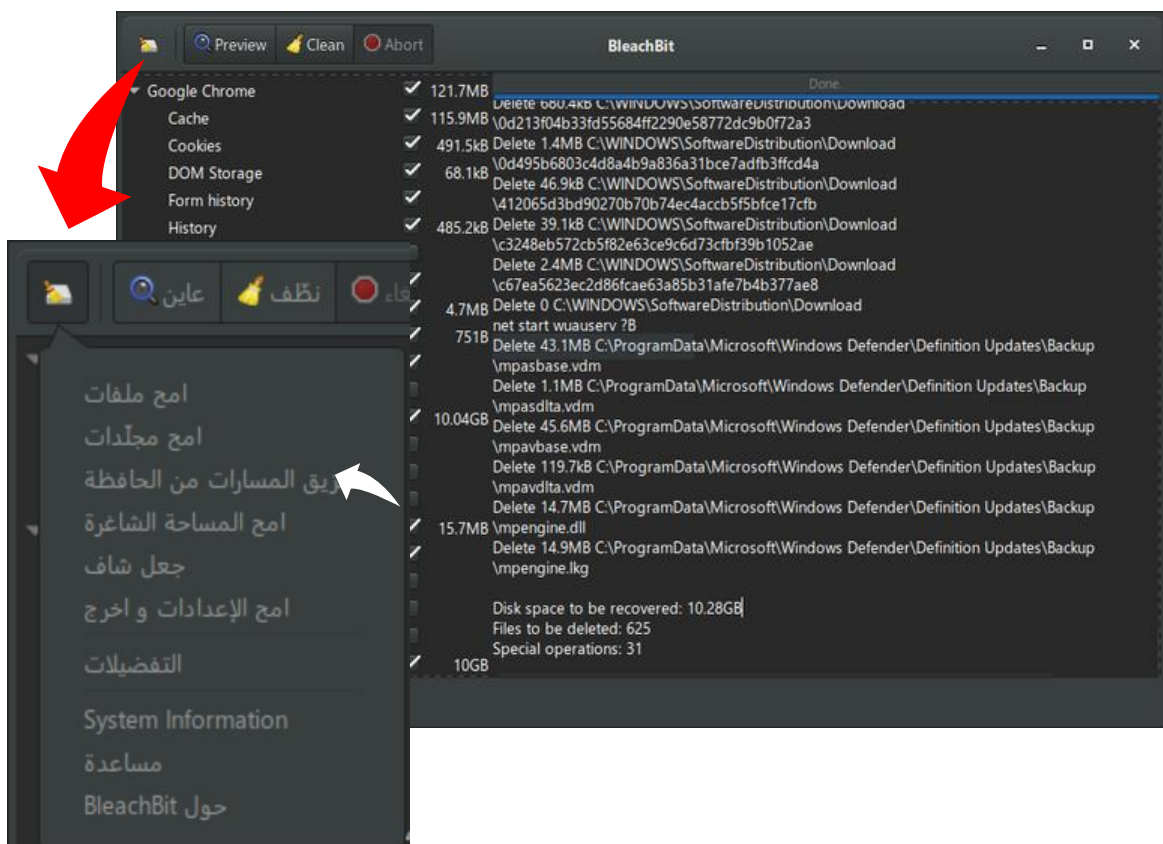


### How to permanently erase or wipe data:

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.

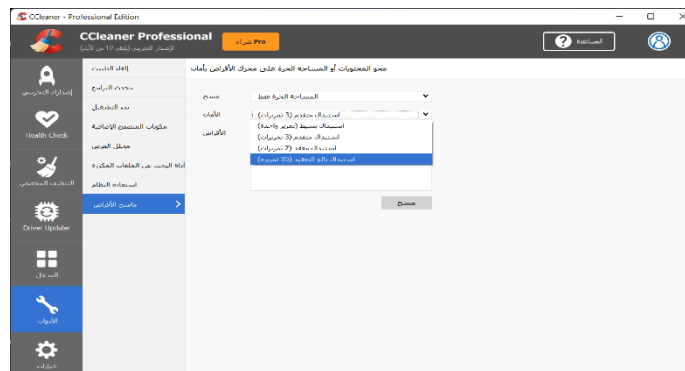
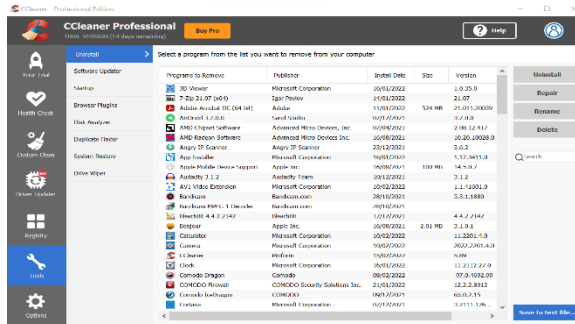


**BleachBit:** This free, open-source program can be used on Windows and Linux devices to erase files, folders, free space, erase settings, and shred tracks from the clipboard.

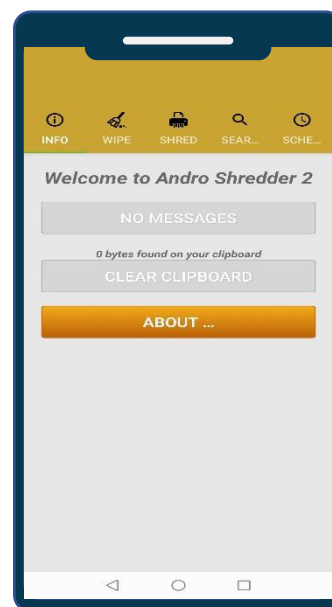




**CCleaner:** A program for erasing and wiping information. It can provide standard privacy protection, standard cleaning, regular updates to the system and software, performs PC health checks, cleans browsing history and keeps it private, detects and removes internet trackers, and prevents the device from running out of space.



**Andro Shredder:** An application for Android phones to erase, shred, and wipe information and to free up space.



# 08

## Prevent phishing



## 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 users are targeted, and preventing phishing is one of the easiest ways users can 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:

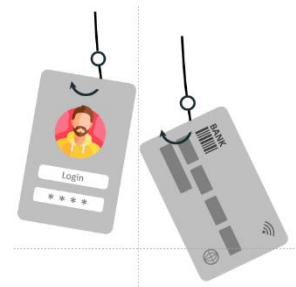
- Click a link
- Share information
- Give permissions
- Download files infected with malicious software

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

### Types of phishing

There are many types of phishing, including:

1. **Spear phishing:** 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.



2. **Whaling:** Spear phishing technique targeting especially influential and powerful people within companies or organizations.

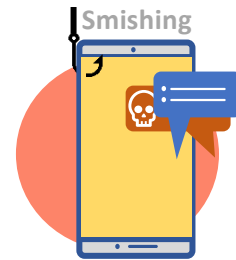




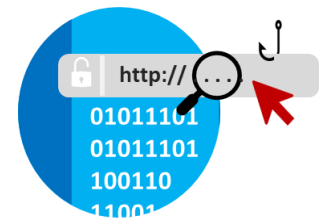
3. **Pharming:** A type of fraud in which the attacker directs the victim from a main/reputable site to another fake site or a site that has been compromised with malicious software. A victim's information can be intercepted when they enter the site.



4. **Smishing:** The use of SMS text messages to defraud the victim by prompting him or her to disclose information about accounts, obtain multi-factor authentication numbers, or download malicious software into the victim's device.



5. **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.



6. **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 the information they want from the victim.



## How to protect yourself from digital phishing

All users should be extremely careful and follow these tips:

1. **Never share sensitive or personal information** with others, and never publish it to social media under any circumstances.
2. **Do not respond under any circumstances to threats received** via messages, e-mails, or social networking sites. Do not interact *in any way* with the threateners.
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 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 that appears as “To our dear subscriber”, “kind customer” or similar may be a fraudulent message: take care in handling.
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 communication 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 programs**, and **do not install “cracked” or pirated software**.
10. **Enable two-step verification** on all accounts.

09

References and  
further reading

## References and further reading

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

1. **Digital Protection** ([Arabic](#)) – Security information, training manuals and recommended tools in Arabic.
2. **Security-in-a-Box** ([Arabic](#) and [English](#)) – Digital security information, training guides and other resources.
3. **FrontLine Defenders** ([Arabic](#) and [English](#)) – Information and support on digital and other security risks for human rights defenders.
4. **Salama Tech** ([Arabic](#)) – Digital security news, self-learning resources, technical support, training and urgent assistance.
5. **Committee to Protect Journalists** ([Arabic](#) and [English](#)) – Digital Safety Kit for Journalists
6. **Surveillance Self-Defense** ([Arabic](#) and [English](#)): Tips, tools and how-to's for safer online communications, run by the Electronic Frontier Foundation.
7. **Cyber Kurds** ([Kurdish](#)) – Kurdish language information on digital security.
8. **Rory Peck Trust** ([Arabic](#) and [English](#)) – NGO dedicated to safety, support and welfare of freelance journalists.
9. **Safe Sisters** ([English](#)) - Fellowship program and resources specifically aimed at women human rights defenders, journalists or media workers, and activists to train on digital security challenges.

# 10

## Cybersecurity glossary of terms

## Cybersecurity glossary of terms

Unless otherwise noted, the definitions contained below may be found in the United Nations Terminology Database (UNTERM), available [here](#).

- **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 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 program designed to activate, register, or extend the trial period of a proprietary program that normally requires a serial number to prevent piracy and unauthorized use. Using a “crack” or “patch” to access software programs is always illegal.<sup>5</sup>
- **Encryption technology:** Enables the user to shield data saved on USB drives, mobile devices, flash disks, pen drives, CD 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 communication tools and services, such that only the users of the tool or service have access to the 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.
- **Firewall:** A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.
- **IP address:** A unique number that information-technology devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any participating network device

---

<sup>5</sup> See [Software cracking - Wikipedia](#)

— e.g. routers, computers, printers, Internet fax machines — must have its own unique address. Can be thought of as 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 network 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. A combination of the words "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.<sup>6</sup>
- **Open source software:** This is a generic term for software (application and system software) where source code is openly available to any user; A programme that can be used, copied, studied, modified and redistributed without restriction.
- **PGP:** PGP 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 e-mail that poses as a legitimate business request – for example, from a bank asking customers to verify financial data. The e-mail includes a link that purports to go to a legitimate banking website. However, the site is bogus and when the victim types in account numbers, passwords or

---

<sup>6</sup> For more information, see The Tor Project at <https://www.torproject.org>



other sensitive information, that data is 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 some may 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 Internet web browsing history and scanning documents on the computer's hard disk.
- **Trojan or Trojan Horse:** A program 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.
- **VPN:** A “virtual private network” is a network that offers a controlled pathway through the Internet to which only authorized users have access and along which only authorized data can travel.
- **Worms:** 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 program files. Worms can create copies on the same computer, or can send the copies to other computers via a network.

**Team leader**

**Content writing & Visual design**

**Cartoonist**

**Linguistic references (Arabic)**

**Hayder Hamzoz**

**Aso Wahab**

**Hala Zead**

**Mohammad Abdullah**



Human Rights Office  
United Nations Assistance Mission for Iraq  
(UNAMI)  
بعثة الأمم المتحدة لمساعدة العراق  
(يونامي)



## Online Protection and Digital Security

User guide for human rights defenders

2022