Digital Security Manual

Digital Security Manual

Edited by

Nada Kabary

Technical research

Mohamed Tita
Norhan Tharwat

Translated by

Khaled Hosny

Motoon extends thanks and gratitude the to our colleague Kholoud Bidak for her efforts and contributions in the prototype of this manual, and also to The Bussy Project for providing the stories included in this manual.

Motoon also thanks the technical researchers working on the issues of the digital security in the Arabic region for all their efforts.

Table of contents

Introduction

Although most Egyptian are not technologically savvy, not a small number of them use computers and smart phones daily, both personally and professionally. Lately, out digital identities became part of who we are in the real world. Everyday we use digital tools like email, social media, instant messages, file sharing, or even ride charing services. All these programs and services know too much about us; our communications, close friends, places we visit, and even photos and other digital media and files about us, and more. It is important to be aware of the risks our digital media and identities are subject to, so that we can protect them. Technology has given us unprecedented ways to keep and share information, but it also made these information subject to new risks and bigger challenges.

Why this manual?

For Motoon, digital security is one of the most important topics we work on through training and consulting for institutes, corporations, and individuals. While working with different groups in this area, we concluded that it is time for us to write a manual that sheds light on some digital habits that people do all the time thinking that it makes their digital life more easier or secure, while we found that these habits account for most of the cases of digital security attacks we have dealt with. These “bad digital habits” helps the attacker to reach its goal, whether it is hacking digital accounts or stealing data that can be abused in different ways. In this manual we are concerned with informing users of technology about the habits that put them and others in danger without them realizing it. We also found it important to give advices and suggest safer applications and tools, in an attempt to help readers of this manually not only in realizing the dangers they might face, but also in having solutions for the bare minimum of digital security.

The methodology used in this manual

In preparing this manual, the team relied on true stories after holding a workshop to collect stories about digital security attacks with help from Bussy, in addition to teams own experience from providing support in the Tech-clinic to cases subjected to digital attacks during two years. In the team’s opinion, it is better to demonstrate digital security risks with actual stories, as it better reflects on the majority of risks most of us face, either because of things we got accustomed to doing, or because of using tools and applications that lack the required security features just because they are popular in our communities. We selected

seven stories that have many similarities and recurring mistakes, to highlight how to avoid the digital security risks and recommend safer tools and applications that help avoid falling in the same risks again. The manual starts by explaining how the internet works, then lists the major tech players that has access to your information and digital identity, either for commercial, personal, or security reasons. The manual ends with an appendix containing technical information about the tools and applications that our team recommends, explaining their most prominent features and properties, as well as links documenting how to use them on your operating system of choice.

Our right for privacy

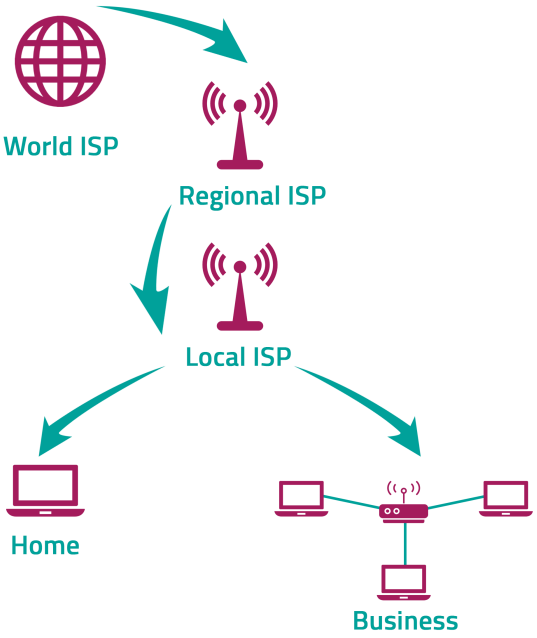
We think this manual is a small contribution in establishing Article 12 of The Universal Declaration of Human Rights, which is an important document in the history of human rights, written by delegates from all over the world, and was adopted by United Nations General Assembly on 10 December 1948 as Resolution 217 at Paris, as a shared goal all nations should aspire to achieve. For the first time it specifies the basic humans rights that should be protected universally.

Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

How the internet works?

It is important to know how the internet works for better understanding of the the risks we face while using technical tools and applications mentioned in this manual. We can simply say that the internet is big network made of smaller ones connected together, and there are billions of computers and other equipment inside these networks connected to each other via Internet Protocol (IP) and sharing various types of content, either publicly or with restricted access. When you type an address for a website you want to visit in your browser, the browser sends a request containing various information, including domain name (like google.com), to servers dedicated to this purpose that convert the domain name to the IP address of the server that hosts the requested website, and then the browsers sends to that server a request for the website content using the suitable protocol (HTTP in case of web page). This is called server/client relationship, and most communication protocols inside the internet depend on it for managing their connection.



What do these know about you?

1. Internet service provider (ISP):

When you connect to the internet without any extra security measures, then the ISP can access the following information:

1. Your IP address and physical location.
2. The websites you request and their domain names.
3. The content you are accessing (in case the website does not use the secure HTTPS protocol).
4. In case of accessing the internet from a smartphone, it can also know the device model and the manufacturer.

2. Network admin in work, hotel, or public networks:

1. Your IP address and physical location.
2. The websites you request and their domain names.
3. The content you are accessing (in case the website does not use the secure HTTPS protocol).

3. Facebook:

Facebook is one of the most data hungry services; when yoy open Facebook website in your browser, it can collect the following information:

1. The website can record mouse cursor movements, as well as the other websites currently open in the browser.
2. Your physical place, the type of your computer, the OS and the browser you use.
3. Records and analyzes your data to make a profile of your personal preferences and habits on the internet, to be used for targeted ads that has higher chance in getting your attention.
4. When using Facebook application on a smartphone, it is easy to notice the high number of permissions that the application requests (camera, microphone, phone log, storage, sensors, geolocation).

Stories

First story

It was your phone, it is mine now.

I was in a birthday party, by the middle of the party I felt some discomfort and decided to leave early, and when I arrived home I found that my phone was missing and had to return to the party where I looked for my phone but couldn't find it, and asked the staff of the place but the answer was "no, we didn't find any phone".

Back home I was very upset about losing my phone, and out of nowhere someone I don't know sent me a friend request on Facebook. This person profile had my photo and my personal information except my name. Honestly, I didn't know what to do and decided to just accept the friend request and so he became one of my Facebook "friends", other friends warned me "it is fake and is stealing everything about you". In the same day another one sent me a friend request, and since I had nothing else to do I accepted it and we started chatting together, and after a while I felt he knows things about me or wants to show me that, but I didn't recognize him and started to worry something is not right.

We continued to talk for 3 days before we decided to meet. We met at a cafe and he kept telling me he knows stuff about me and I was scared, and didn't know how he came to know these things. He offered to give me a ride home which I accepted, and while in his car he told me "don't you want to know how I came to know so much stuff about you?" then he showed me my phone, which I quickly grabbed from his hands shouting "this is my phone!"

- "It was your phone, it is mine now"
- "Where did you get it from?"
- "I bought it at used phones shop, and all your email accounts were unlocked, and it had all your photos"

I didn't see this coming! I asked him to close the email accounts and delete the photos. Days later, he contacted me and wanted to hangout together which I firmly refused, then he started threatening me with the messages and photos I had on my phone.

To protect your privacy in your smartphone, we recommend the following:

1. Chose a strong and unpredictable password for your phone.
2. Enable phone tracking feature in case it gets lost or stolen.
3. Enable disk encryption.
4. Don't accept friend requests from people you don't know.

If you are buying a new phone:

1. When buying a new Android phone make sure that OS version supports full disk encryption, as there are phones on the market that does not supports encryption (some of Huawei phones for example).
2. Enable full disk encryption and chose strong password for unlocking the phone.
3. Newer iOS devices come with full disk encryption enabled by default.
4. Enable phone tracking feature in case it gets lost or stolen.

Second story

So you can't find your laptop, tell me how you gonna do your work now!

About two years ago there were some issues between me and my husband that ended with divorce. One day we had a big fight because he wanted me to quit my job and be a housewife because "my family should be my priority"! I refused to quit my job, so he threatened me with divorce and taken my children away from me, and almost expelled me out of the house, the fight got bigger and I told him I'm not leaving my house and my children, and went to my room with my children, locked it and went to sleep.

In the morning I called my mother to come and watch the children while I'm away at work, and started packing my stuff to leave as soon as my mom arrives as I was late to work, but I couldn't find my laptop! I looked everywhere and still couldn't find it! Which lead me to think he toke it as a revenge, knowing it would negatively affect my job as I keep my work files on my personal laptop and not on my work computer.

The first thing I did is calling him, but he didn't answer my calls for a while, and later sent me a Whatsapp message "So you can't find your laptop, tell me how you gonna do your work now!", obviously I was furious and it was then I knew I can't live with someone like this who would steal my stuff to hinder my job, as he knows I'm a lawyer and all my case preparations are my laptop and a month of two worth of work is already on it.

I immediately filed for divorce without thinking twice. Months later I was shocked when he started to send me personal photos that were on the laptop and threatened me put them publicly on the internet if I didn't ask the court to dismiss the divorce case. I decided to ignore his messages until he started sending defamation messages about me to my clients from my personal email account. I also discovered that he was following my work from my email account that was open on the laptop he toke.

To protect your personal laptop, we recommend the following:

1. Use an operating system that supports data protection.
2. Keep a backup of your data, especially important ones, on an external storage.
3. Chose a strong and unpredictable password for your personal computer.

The operating system and encryption are your starting point for protecting your personal computer:

1. Using a secure operating system is above everything else, and password alone is not enough as it can be cracked in most operating systems.
2. It is also important for the operating system to support encrypting the storage device, and this is the only safe measure against stealing your data when someone else gets physical access to your device.
3. Using third-party applications to encrypt specific data on your storage device can be very handy, and it is very important to keep a backup of such data on external storage devices, and make sure to use trusted applications and strong passwords in the encryption.

Suggested tools and applications in this case:

1. Veracrypt
2. Full disk encryption on GNU/Linux
3. Bitlocker "Windows"
4. Filevault "MAC"

Third story

Did you open my computer!

I must start my story with a confession: I take naked photos of myself, it is part of a defense mechanism I developed for myself to like my body in a world full of ads for losing weight and plastic surgeries that makes me hat my body and the cellulite. I always try to take photos of myself and look to it and find positive things about my body and find beauty in every detail, ignoring the stinking standards of the world around me.

Two years ago, I had a phone that automatically uploads photos to my Dropbox account, and I use that account everywhere; on my phone, work computer, and personal laptop. I didn't feel I need to be extra cautious around work as I was working in a respected institute that supported personal rights.

In that institute there was someone in managerial position who wanted to date me, but I declined his advances, and he simply and respectably said "you are not interested, as you like". But one day I was surprised t find my work computer open while I was away, and that manager is that manager is the only other person who has the computer password. I asked him directly "did you open my computer?" and his answer was that he didn't like the way I was talking to him, and I better change it or else! And if I have a complaint, I should go the formal way, which I did.

That day when I returned home, I found a Facebook account sending me a friend request, and it was using a cropped version of one of may naked photos as a profile picture. I was breathless, I couldn't think or even cray. It was a very bad feeling, and the worst part was that I didn't know why he was doing this, even blackmailing has a goal; monetary, sexual, but this seemed to be just trying to hurt me, or revenge, or whatever was his goal but I couldn't tell what is it.

The formal complaint went nowhere as this person was trusted by so many people and he never harassed any other woman (or so I was told by the person receiving my complaint), and because I didn't have any proof that he is the person behind all of this.

After lots of reports to Facebook the account was closed, and that person seems to never have tried to do this again. However, I'm living in constant fear, and always feel threatened that someone wrongfully has something that belongs to me and can use it whenever he wants, without anyone believing me or stopping that person.

If you are using your personal accounts on work devices, we recommend the following:

1. Disconnect personal accounts from work devices.
2. Take precautious measures to protect the device and the data on it.
3. Use an operating system that supports data protection.
4. Chose a strong and unpredictable password for your work device.
5. Stop automatic signing into your personal accounts on word devices.
6. Stop Dropbox from uploading data automatically.

When you have to share private files and data across the internet, make sure to do the following:

1. Chose a safe file sharing service.
2. We highly recommend using file sharing service that uses end to end encryption and has a good reputation.

Suggested tools and applications in this case:

1. Firefox send
2. Mega.nz

Fourth story

Do you have WiFi? What is the password?

It was the last day in the exams, and as usual we went off from the university to start the long summer holiday. We went for launch, then me and my friends hanged out in a cafe, and as usual asked about the password of the WiFi and connected to the network as we are used to do.

Months later, out of nowhere someone was sending me personal photos on Whatsapp that I only have on my Facebook account, I shouted on him and blocked him. Later, a different number was sending me voice notes that I had sent to my friends, and screenshots from my private conversation! I didn't know what to do and freaked out, and the only thing that came in mind is to ask him "What do you want from me? How did you get these things?"

He went silent, and for complete month I lived in fear until one day a number I don't know called me, and when I answered he said "I gave you time to think how you are going to reward me to not send the photo to your father". I told him "What do you want from me? How did you get these things" and he said "None of your business, that is what I do, how much are you going to pay?", and I said in return "How I guarantee that want make these things public anyway?" and he just hanged on me.

That same day I found another girl who was me at the cafe that day had the same trouble. We went to a friend of ours who runs a phone repair shop and gave him our phones, he did things we didn't fully understand and asked if we connect to public WiFi networks which we answered with a yes. He said we should report the issue to the police and track the person who is blackmailing us. We had to tell our families and reported the matter to the police and were able to track him down, turns out he worked on that cafe we went to after the exams. Since them, me and my friend felt vulnerable and lived in constant fear that he might have other copies of the photos that he might use to revenge from us.

Steps to safely connect to a public network:

1. One must be aware that in any given network there is at least someone he is tasked with running and maintaining that network, this may be called a network administrator or something else. This person has complete control over the network and can do many things like blocking certain websites, throttling network speed, knowing the websites people connect to from within the network, manipulating the unsecured data and content transmitted through the network, and even (if he has the required skills) steal personal data transferred over the network unsecured.
2. Using TOR network encrypts the internet connection and helps conceal your identity and location, and also protects your data from manipulation or unauthorized access, and also helps with circumventing censorship.
3. Always access websites through HTTPS protocol, as it encrypts the connection between you and the website in both directions, and also allows the web browser to verify the identity of the website to make sure you are not redirected to a fake one which helps protecting you from phishing attacks and from intercepting and manipulating your data. Reading browser error and warning messages is also very important as it can be an alarm for a possiple attach or fake website.
4. Do not share sensitive data over a public network, even after applying all the measures above, or at least make sure to use specialized encryption software.

Suggested tools and applications in this case:

1. Tor Browser. Although Tor website is blocked in Egypt, a mirror of it can be accessed from *tor.eff.org*.

2. Use HTTPS Everywhere add-on for your browser and usr it to always connect with HTTPS protocol with websites that support it.

Fifth story

New fake account everyday!

This is the first time I tell this story, and I don't know why I didn't do that before. May be because I thought it was insignificant, or may be because I wanted to forget it and move on, or may be because I felt embarrassed by it.

About 6 years ago I was engaged, and during that period someone appeared on Twitter and seemed to be obsessed about me, he always commented on things I write, gets into conversations between me and anyone else. I don't know what happened or when things took a turn to the worse, but he started harassing me and my friends, may be he asked me about something and I gave him an answer he didn't like and that angered him.

I don't really know, but one day I woke up to several fake accounts impersonating me, and whenever I report one, five new ones appear. At first, he was creating accounts on Twitter and Facebook, getting them deleted on Facebook was easy as Facebook was fast in responding to reports and took the matter seriously, but on Twitter it was different.

After awhile these accounts turned pornographic, and I remember one of them was called "[my full name] tits". My fiancee freaked out and kept asking me to close my Twitter and Facebook accounts, but that wasn't the answer! I did hesitantly for a week, then opened them again as I wasn't going to let some sick person control my life! I didn't really understand what he wants, but the more I ignore him the more it gets worse. I tried to find someone to hack his account as things turned really ugly and he started sending messages to my friends saying harmful things about me, like when he sent to my fiancee a message saying "she is homosexual and is using you to fool the people around her".

I keep thinking, after this whole experience, what would it be like if I lived in some village or more conservative community? I would have been defamed and it is possible that my family or one of my relative would have decided to punish me or force me to marry someone, or if I were married my husbanded would have wanted a divorce, as this is how things usually happen around here and it is always the woman's fault!

In case there are fake accounts using your name:

1. You must tell your friends and followers and warn them to avoid these fake accounts.
2. Ask your friends to report these accounts the company behind the social network, and do not think you reporting them is enough.

Sixth story

My birthday is a password I'm not going to forget!

I forget everything, and since I started using the internet I have one password for nearly all my online accounts. For a very long time I used my birthday as a password for email, Facebook and even my phone and my laptop, because my birthday is a password I'm not going to forget!

On day I tried to log into my email account, but it kept telling me "wrong password", and checked if caps lock was on or if I was using different keyboard language, but everything was fine and I still could log in. I decided to check Facebook, and the same happens, and by the I realized that all my online accounts were stolen! I didn't know what to do!

I tried everything I can to regain access to my accounts but failed, until a friend of mine who is good was computers helped me and I was able to restore access to my email account (which I didn't have any security features or recovery methods enabled) as well as Facebook account.

Of course, I now know it was the password and whoever stole my account is someone who knows me and was able to guess my password, and because I didn't secure my email enough he was able to change the password without me getting notified. I didn't manage to know who he was, and I still have bad memory and I keep forgetting my password and resetting it!

To chose a strong password:

1. Avoid password that are easy to guess by knowing some personal information about you.
2. Do not use the same password for different accounts, as sometimes user information and password databases of some services get leaked which will expose your password and allow attackers to access your accounts on other services.
3. Enable extra security measures that most email provider has.
4. Make sure to regularly change the passwords of your important and sensitive accounts.
5. Use a strong password as much as possible.

6. You can use random password generation and management applications.

If you are sharing sensitive information via email that might put you in danger, try the following:

1. Use email services that provide message encryption, like ProtonMail and Tutanota.
2. Riseup is a platform interested in supporting activists in all public work fields, and provides services such as email and VPN that are safe and do not keep data bout users and their messages, but does not yet support end to end encryption.
3. You can use Thunderbird email client with Enigmai add-on for sending and receiving messages encrypted with GPG encryption.

Suggested tools and applications in this case:

1. KeePassXC

Seventh story

The account, the page and the group are all lost!

A while ago I was working on awareness campaign, me and group of people interested in the same subject decided to create a Facebook page to publish our campaign events and activities and any other content we make for the targeted groups. I went ahead and created the page from my personal account and added 3 other friends as moderator for the page to coordinate publishing the content and replying to the messages we receive.

Sometime later my account was stolen and I couldn't restore access to it, and because I diddn't enable the security features, the person who stole the account was able to close the page and we couldn't restore it as I was the creator and the only administrator of the page. We lost months worth of work. We also had a private Facebook group and another Facebook Messenger group that I also created to coordinate the work, and they had information that would put us and other people in danger, and both were similarly lost.

To protect your work on Facebook:

1. Enable two factor authentication feature.
2. Use an anonymous account to mange the page.
3. Have more administrator on the page, with real accounts.
4. Avoid using Facebook Messenger to send messages to the group running the campaign.

5. Do not use unencrypted or untrusted services for sending images and data.
6. Do not share data on private groups on Facebook (when creating a private group, make sure that users are aware that stealing an account of one member puts the rest of the group in danger, as it allows the attaker to access all data accessible to group members).

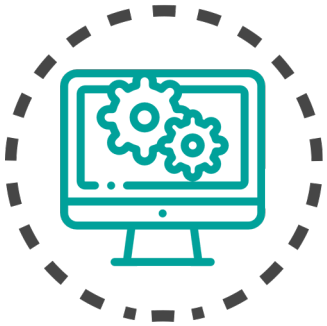
In case it is necessary to use Facebook to communicate and share data in a private group, we suggest the following:

1. Get rid of sensitive information regularly.
2. Do not share sensitive or personal information on an unencrypted or untrusted platform.
3. Do not keep login sessions open on your devices all the time.
4. Make anonymous accounts to mange the page, and create it while connecting through TOR network, and do not use the phone number of any member of the group as that puts them in danger.
5. Enable two factor authentication for any personal accounts.
6. Use encrypted and open source instant messaging platforms.
7. Be aware about Facebook user rights agreement, the nature of the platform and its privacy and data protection policies.

Suggested tools and applications in this case:

1. Tor Browser
2. https://facebookcorewwwi.onion
3. Google Authenticator.
4. Signal Private Messenger
5. Wire Private Messenger

Tools and applications technical manual



First: Encryption

Encryption is the process of turning data from its plain, readable form, to a form that can be only read be people who are authorized to do so.

Data can be encrypted in various ways:

System disk encryption

Operating systems support encrypting data available on the storage devices to prevent any access to this data without first booting the system and successfully logging into user account. After login, the operating system makes the data on the disk available to the user on demand, while keeping it encrypted on the disk. This is supported by both desktop operating systems, as well as mobile ones like Android and iOS.

Full or partial disk encryption on GNU/Linux systems

Most Unix-like operating systems and its distributions support full or partial disk encryption during installation, bit because of the plurality of these systems, it is hard to describe the process in specific steps.

1. If you currently use on of these systems and already have experience with managing them, you probaly know how to do disk encryption using LUKS, wither during installation or afterwords.

2. If you use one of these systems but do not know how to do the encryption, it is better to ask a more experienced person before trying for the first time.
3. If you are planning to switch to one if these systems, make sure to check the documentation of the system you are choosing before installation to find how to activate disk encryption during installation.

Note: enabling full or partial disk encryption on Unix-like systems requires full reformatting of the disk which means complete loss of any data stored on it, so we greatly advice that you make a backup of all data before encryption.

Encrypting system disk on Windows

Microsoft Windows supports, in its "professional" versions (either Windows Pro or Windows Enterprise), disk encryption using bundled BitLocker application.

Note: when running BitLocker for the first time, make sure to generate recovery code for restoring the encrypted disk, and make sure to keep it somewhere safe, to be used in case you forgot the password or the system got corrupted and you had to copy your data to somewhere else.

To enable this feature:

1. Search for Bitlocker in the system search feature in both Windows 8 and Windows 10.
2. Start Bitlocker to enable the feature. You need system administrator rights to be able to do that, and the system might ask for the administrator password.
3. Bitlocker will start running, follow the instruction on the screen to complete the process.

When done the disk containing operating system will be encrypted, making your data safer in case the computer gets stolen.

For more detailed and illustrated instructions, please visit: *pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html*

Encrypting system disk on macOS

maOS, starting from OSX Lion, supports disk encryption using bundled FileVault application, which uses XTS-AES 128 chipher. To enable disk encryption, do the following:

1. Make sure the computer is connected to power outlet if it is a laptop.

2. Open FileVault from Security & Privacy screen in System Preferences.
3. Press the lock icon and enter your password to be able to change FileVault settings.
4. Click Turn On FileVault.
5. After configuring FileVault, restart the system.
6. The next screen will as for password.
7. The application wil start encrypting the disk for the first time and it will take sometime, but this will happen in the background and you will be able to use your device normally in the meantime. Any new files you create will be encrypted by default.

Note: you must setup disk recovery, using one of the following:

1. You can keep recovery codes on iCloud account.
2. You can also save the codes as well as few questions and answers that Apple keeps so that you can restore the disk by contacting Apple and answering the questions.
3. You can request the codes directly during encryption setup, and save them in somewhere safe (especially not on the same computer). Press the triangle icon to display the codes if they are hidden.

For more detailed and illustrated instructions, please visit: *support.apple.com/en-us/HT204837*

Encrypting iOS devices

Encrypting iOS devices like iPhone and iPad is rather simple, setting a password or a PIN number for the device will activate encryption automatically. To set a password if there os no one already:

1. Go to Settings.
2. Select Touch ID & Passcode.
3. Select Turn Passcode On and chose a good password for the device.

Encrypting Android devices

To enable encryption on devices running, do the following:

1. Open Settings application, then Security section.
2. If you already use a password to protect your device, skip to next step. If not, you will have to set a password even if

you have other means to unlock your device. Got to Screen Lock and set a suitable password.

3. Make sure the device is connected to the power outlet and the battery is at least 80% charged.
4. Select Encrypt Phone.
5. Wait for the process to complete.

Android supports also encrypting SD cards. Do the following steps:

1. Open Settings application, then Security section.
2. Follow instructions as above and select Encrypt SD card.

Note that encrypted SD card will be readable only on the same Android device, and must be reformatted to be used on other devices and the data on it will be lost.

Disk and files encryption

There are applications for encrypting disks and files, and they are designed to protect the data available on these disks. The applications decrypts the data on demand when a user who has the correct password asks for it. Disk encryption applications can be used to hide the encrypted disk so that the owner of the disk can safely deny its presence in what comes to be called plausible-deniability.

One of the encryption applications that that this feature is VeraCrypt, which is an multi-platform application, easy to use, and has good reputation. VeraCrypt supports encrypting folders as well as removable disks, and plausible-deniability of the encrypted data.

For easy and illustrated steps to install and configure VeraCrypt, visit: *veracrypt.fr/en/Beginner's Tutorial.html*

Second: Cloud services for data storage

There are hundreds of websites that provide cloud storage services, but we can't trust them all, as most pf them have purely commercial goals, and it is possible that many of them sell or hand the data they have to authorities.

Before selecting a service to store your backups, make sure to do the following:

1. Read the privacy policy and terms of services to make sure your data is safe.
2. The service must support safe file transfer via HTTPS protocol, to make sure that data transferred between your computer and the website can't be intercepted.

3. Make sure the service offers data encryption.

For personal use we recommend Mega cloud storage service, as it provides the required privacy and security features which famous services like DropBox do not provide.

Mega also offers data encryption on the server, which means no one can access your data, including the service owners.

Its most important features include:

1. Mega offers cloud storage services from the browser as well as a dedicated application that you can install on your computer (for Linux, Windows and macOS).
2. You can also install Mega app on iOS, Android and even Windows Phone devices from the app store.
3. You can enable storing your data directly on Mega cloud service instead of storing it on less secure services like Google Drive.
4. Mega offers also instant messaging either from the website of its MegaChat application. It uses end to end encryption for both written and voice messages, making it a secure service.

You can download Mega application from *mega.nz/startpage*

Third: Sharing encrypted files

To share encrypted files with others in an easy way, you can use Firefox Send service that Mozilla launched in August 2017. Its most important features include:

1. Allows uploading and encrypting files up to 10 gigabyte.
2. Gives you a link to the uploaded file that you can share with any one over any digital communication channel.
3. Removes the encrypted files 24 hours after aploading it, or immediately after it gets downloaded once.
4. You can use Firefox Send from any browser without any additional plugins.

To learn how to use Firefox Send, check the video tutorial *youtu.be/ZGWZGYtAS3U*. You can visit the service website on *send.firefox.com*.

Fourth: Secure and encrypted messaging services

Email

We should start by noting the difference between email service providers and email clients. The service providers are Gmail, Ya-

hoo, Hotmail and the likes, while email clients are applications like Microsoft Outlook, Mozilla Thunderbird and Opera Mail.

Email service providers

Many of us prefer using the GMail as email service provider, but if you have sensitive messages that might put you and others in danger, then you highly recommend Tutanota email service.

Tutanota is an open source email service provider built around the concept of encrypting your messages by default, including the message body, title, email addresses, and attachments. Tutanota features include:

1. Allows you to encrypt messages between you and others even if they use other email service providers, by using encryption by password feature.
2. Tutanota uses end to end encryption.
3. Tutanota also supports GPG, but both ends need to have GPG keys.
4. When sending messages to more than one person using other email providers, Tutanota support having separate encryption passwords for each.
5. Tutanota offers also secure applications for iOS and Android devices that can be installed from app store.

Important tips when using Tutanota:

1. Access Tutanota only on secured devices (running secure operating systems, use encrypted storage, etc.)
2. Access Tutanota only on secure browsers like Firefox or Tor Browser.
3. In case encryption is illegal in your country, using Tutanota continuously can draw the attention of authorities.

To know how to register and send messages on Tutanota, you can check the video tutorial on *youtu.be/qUgQxxhr3EY*, you can open Tutanota account from *app.tutanota.com/#register*.

Email clients

If you have more than one email account over several service providers and want to mange your emails in a one place, we recommended using Thunderbird, a free open source, multi-platform email clients that supports many email protocols and service providers.

Some of Thunderbird features include:

1. Thunderbird supports many email protocols and service providers, and allows you to add all your email accounts in one place.
2. Ability to read and compose email messages offline.
3. Ability to send and receive encrypted email messages.
4. Thunderbird features an tabbed interface similar to Firefox.
5. We can search the web from Thunderbird, either from the search field or by highlighting a word and selecting web search.
6. Thunderbird allows filtering messages, by specific words or subjects.
7. You can add extensions to Thunderbird.
8. You can create local folders on Thunderbird to mange your messages.
9. Thunderbird can also protect you from phishing attacks, which is one of the most common email attacks.
10. Thunderbird works on Linux, Windows and macOS.

If you chose Thunderbird for email management, you get also another important security feature; the Enigmail add-on that gives you access to GPG encryption and key management from Thunderbird.

To learn how to use Thunderbird for managing you email and how to install Enigmail, follow the instructions in the following links.

For Linux users:

securityinabox.org/ar/guide/thunderbird/linux

For Windows users:

securityinabox.org/ar/guide/thunderbird/windows.

Secure instant messaging

Most of us depend on common instant messaging services without checking if they provide basic security features. For example, Facebook Messenger can not be considered a secure service as it does not give any substantial guarantees about the levels of encryption it uses.

It is important to also note that most instant messaging services and general, and Google ones in particular, keep the data and messages you share in three main places; the sender account, the platform servers, and receiver account. This shows

that deleting a message from one of the ends does not mean it is gone entirely, as it could still be stored in other places.

For sending and receiving sensitive or important messages, it is better to use other platforms like Signal and Wire as they provide encryption and do not save plain messages.

You can install Signal and Wire for iOS and Android devices from the app store.

Fifth: Secure browsers and necessary plugins

Firefox

Web browsers are very central to digital lives on the internet, and although most people now use Google Chrome, we highly recommend replacing it with Mozilla Firefox Quantum.

Why Mozilla Firefox?

1. Firefox blocks web trackers, and forgets your browsing history.
2. Some ads are hidden trackers that follows you everywhere, and Firefox Quantum adds a new way to stop them.
3. Blocking ads and trackers and their scripts, web pages load 44% faster.
4. It loads pages faster and uses less memory.

Firefox has many easy to use add-ons that enhances the privacy and security of your browsing experience. You can select the add-ons you want and configure them to fit your needs. If are using a computer you do not manage (at an internet cafe, or at work), you might need to re-configure the add-ons every time you use the browser.

We recommend HTTPS Everywhere add-on for all browsers, to force the browsers to load pages over HTTPS protocol whenever possible and thus encrypt the data transmitted between the browser and the web servers, disallowing an third-party from knowing the natures of said data, and decrease the probability of being subjected to a password phishing attacks.

You can download Firefox from *mozilla.org/ar/firefox*, you can also find add-ons in *addons.mozilla.org/en-US/firefox*.

Tor Browser

As we showed solutions for encrypting sensitive messages that may put you and others in danger, we also recommended people who do sensitive activities on the web to use Tor Browser

and the Onion protocol. Tor Browser is a free open source browser that encrypts your internet connection and routes your internet through many rely nodes to conceal your identity and physical location while browsing the web, and protect your data from stealing and manipulation, and also help in circumventing censorship.

Some of Tor browser features include:

1. Prevents websites and internet service providers from tracking your browsing habits.
2. Tor network can be used to publish websites anonymously.
3. Tor Browsers can be used to join chat rooms and forums anonymously.
4. Tor protects users from activity analysis attacks.

Tor Browser can be downloaded from *tor.eff.org*.

Sixth: Password management software

If you are one of the people who keep forgetting things and have many accounts that you need to manage, we recommend using password management and generation applications to make thinks simpler for you, and avoid having to use simple or single password everywhere.

We recommend KeePassXC, a free open source applications that stores passwords for you and act like a password safe. You can manage all your passwords in a single place and you can have stronger, more hard to guess passwords without having to remember them by heart. All you need to remember is the master password that you can use to unlock the password database.

Some of KeePassXC features include:

1. Storing not just account usernames and passwords, but you can also create entries to save important things like bank account numbers, serial numbers, or basically anything you want to remember.
2. You can create an automatic lock that closes KeePassXC after a period of inactivity, to prevent others from accessing your passwords while you are away.
3. You can organize your passwords in KeePassXC in the form of folders for different password groups.

To learn how to use KeePassXC , you can watch this video tutorial *youtu.be/z-cKvTUUgNQ*, and you can install it from *keepassx.org/downloads*.

Seventh: Two factor authentication

Although it is important to set a strong and unique password, it might still be possible to crack some accounts with different methods like phishing attacks. Two factor authentication works as an additional fortification against this kind of attacks.

Two factor authentication is a security protocol adopted by many online platforms like Google and Facebook to secure user accounts. It basically works by adding an additional step to user login that requires proving the user identity after entering the password, usually by entering a sequence of random numbers that changes regularly at fixed intervals, that the user gets from a dedicated application.

One of the most widely used two factor authentication applications is Google Authenticator, which has the following features:

1. Can be used with most platforms that support two factor authentication, not just Google services.
2. Can be download freely from the app store on iOS and Android devices.

Two factor authentication can be activated from the security settings on the platforms that support it. To enable it on Google platform, follow the steps in *support.google.com/accounts/answer/1066447*.

Epilogue

We tried our best to provide an easy and simple technical manual for the average user of the internet. As we believe in our role in raising digital security awareness, we always welcome questions and inquiries through any of our communication channels. You can always ask for technical support from Motoon though our Tech Clinic service, you just need to file this form *https://goo.gl/6X2yYn*.