

VPN



**ABOUT YOUR  
DIGITAL SAFETY**



# Q&A about your digital safety

## Prelude

Of course you are concerned with your digital safety, your computer and mobile accounts, and your passwords.

In this simplified paper, we will provide you with some tips and guidelines on how to boost your digital safety, make it more difficult for your accounts to be hacked or pirated, and reduce any cyber-security threats.

The most important advice:

The best thing you can do to enhance your digital security and maintain your privacy is to change your internet usage habits.

Here, we will show you in a simple way how to be safe.

## **Q: How to create your password?**

All people, in general, forget their passwords so most of them use duplicate numbers, birth dates or phone numbers, which is a big mistake because they will be at greater risk of being hacked. Your personal account can be stolen or pirated by hackers or cybercriminals. Your phone can be hacked and your secrets and personal information can be accessed. Also, you should be aware that if hackers manage to get your Wi-Fi (wireless) network password, they will be there with you; they can steal and drag all the information from your device or from any device on the Wi-Fi network.

## Password

When creating your password, make sure to include upper and lower case letters, numbers and symbols to make it harder to guess or hack.

Therefore, it is recommended that you permanently hide the Wi-Fi network.

**555555**      DUPLICATE NUMBERS  
REPEATED CHARACTERS

**01000000000**      PHONE NUMBER


**2/8/1977**      BIRTH DATE

**THIS IS ALL WRONG** **X**

**A CORRECT PASSWORD CAN BE**

**Ahmed55 \$&@** ✓

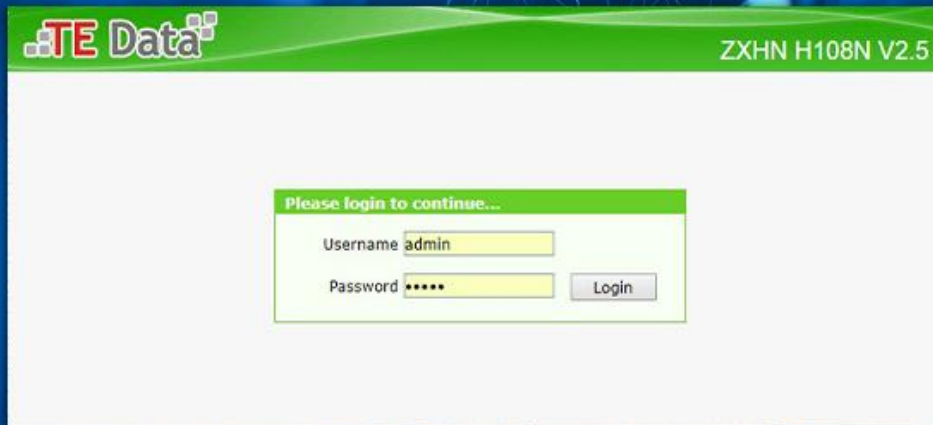
**MAKE SURE TO INCLUDE UPPER AND LOWER  
CASE LETTERS, NUMBERS AND SYMBOLS  
IN YOUR PASSWORD TO MAKE IT  
HARDER FOR HACKERS TO GUESS**



**Q: How to hide the Wi-Fi network?**

- Open any of the web browser's platforms: Google Chrome, Firefox, etc.
- Enter your router IP address in your browser address bar (such as: 192.168.1.1)
- After opening the router page, write your username and password, and if it is the first time to visit the page, you can find the default username and password behind the router.





Follow the directions carefully.

**Q: Do you know that data and files still remain on your phone or computer's hard drive after deleting them or formatting the device?**

There are several ways by which you can recover the data deleted from the phone or computer's hard drive after formatting it or doing a factory reset, but we will explain this later.

The proper way to permanently delete files is to overwrite the data; using the available tools that can write random fake data over the original data on your device, and hence you can ensure that your deleted personal files are irretrievable. To do so, you can use the following applications: "Shreddit - Data Eraser".

**Q: What is meant by hacking?**

It means that there are many intrusive people around us. These people are obsessed with intrusion, curiosity and eavesdropping on others. Using many programs, they can steal your personal pictures and any information from your device or mobile phone, and they can crack your cam and mic.

**Q: How can I be safe in the midst of all this?**

First of all, and as we said before, passwords must be secured to make them hard to crack by hackers.

- For example, when you go anywhere, do not charge your phone battery on a personal laptop, and always have a charger with you wherever you go; because it is very likely that the person who owns the laptop or the device is obsessed with intruding on people's lives that he downloaded hacking programs (software) to steal your private data once the USB charger is connected to his device.

- Don't open the location on your mobile phone except when necessary

- If anyone sends you a link, don't open it. Why?

\* I will make it simple: this link may be a virus that destroys the safety points in your device when you click on it, and consequently, it will crack your device and transmit every step you make to the hacker. We will explain this later.

There is a software program called "Key logger" which is designed to capture and log all keyboard activity by logging every keystroke entered.

### **Q: What is Safe Browsing (VPN)?**

VPN stands for "Virtual Private Network". It establishes a secure connection between you and the internet, which gives you additional online privacy and anonymity. A VPN is quite different from a proxy and is more secure.

There are a lot of easy-to-use VPN software programs for mobile phones, including:

Express VPN

Opera Free VPN

It is easy to download these programs from both Google Play Store and Apple App Store, and you can run them by following the very easy steps. This video will help you download a VPN:

<https://www.facebook.com/146770222053055/videos/1353689898123706>

### **Q: How do I protect my e-mail?**

To protect your email, you can use an encrypted email service such as "Proton Mail": <https://mail.protonmail.com/login>

ProtonMail is an email service provider that was developed in 2013 in Switzerland. It is distinguished by its design that provides users with complete anonymity and security through several features:

1- End to End Encryption: Enables encryption of messages and files before sending them from the user's device.

2- It does not require a phone number or any additional email to create the account.

3- By giving you a small storage space (only a half gigabyte) as a free account, it makes you, or forces you, to delete the old e-mails every so often, and if you want more space, you must pay.

### **Q: What about hacking a Facebook account?**

Thousands of people google "hacking a Facebook account" in an attempt to find a way to either pirate the accounts of others (if they were hackers), or to secure their own accounts (if they are normal users).

\* We will try to simplify the matter using simple language and examples:

We will introduce some security methods in order to show you the tools used by hackers to steal personal accounts and on which programs they depend.

#### 1-Hacking a Facebook account using fake pages:

Hackers can hijack your personal Facebook account using fake pages, which is either created by the hacker himself, or by using the manifold websites that provide such services, which is known in the field of hacking as "phishing".

The hacking process here succeeds as soon as the victim clicks on this malicious link that directs him to a page completely similar to the Facebook login page, where he is asked to enter his username and password into the login form. At this point, the hacker manages to obtain your personal login information and accordingly he can take control of your Facebook account.

So don't do not open any links sent to you by strangers. Also, make sure that the page you opened is a real Facebook page.

#### 2- Hacking a Facebook account using cookies:

Cookies are small text files that can be sent and stored on your computer's hard drive by the web pages you visit, and they are then sent back to the originating website on each subsequent visit. Cookies also contain a unique code that allows tracking your browsing activities on the website, either for statistical or marketing purposes.

#### 3- Hacking a Facebook account using Key Logger:

Key logger programs can capture and record all the keystrokes typed on the computer's keyboard. They are basically normal programs that do not harm the system, but the hacker can exploit them to achieve his purposes; as he can integrate these programs with a picture or any other multimedia segment, or an executable program/file that usually ends with ".exe" using the Social Engineering Toolkit to push you to click on it or download and install it on your device.

And when you fall for this trick, the Key logger will send the logs of all the keystrokes that you made to the hacker's email that he previously prepared, and therefore, he will get to know your Facebook's login information besides other information.

#### 4- Hacking a Facebook account using "Access token"



The Access token is the second password for your Facebook account. It is a specific link/URL page that can be obtained through Facebook apps. Once this code falls in the hacker's hands, he will have full control over your account.

In the recent period, a number of applications have appeared such as: "know who viewed your profile", "write your name on a Coca-Cola bottle", "put your picture with the lion", "hack any Facebook account", and many other provocative phrases, which are nothing but a means for hackers to pirate your account and crack your personal information.

### **Q: Why is it important to change your operating system?**

Most of us use Microsoft's Windows operating system. However, there are other systems such as: the Apple operating system Mac OS X and linux with its various distributions that are developed by computer programmers from around the world. Nothing is 100% secured and there aren't any computer systems that cannot be hacked. All of the aforementioned systems are hackable, but the difficulty of hacking them may increase, compared to the other systems. We recommend that you switch to Linux; it is the most secure operating system.

#### Use the Tor Browser:

This is very useful advice. If you want the government, someone eavesdropping on you, and intruders not to track you, use the Tor Browser; it is a free and open-source browser. It is also secured and enables anonymous communication. The Tor browser runs by bouncing your communications through encrypted messages across multiple computers around the world, making governments and Internet service providers unable to track you or figure out the data you're sending.

It is available here:

<https://tb-manual.torproject.org/>

#### Using browser plugins/extensions & security and privacy programs:

There are dozens of add-ons for popular web browsers- such as Firefox and Google Chrome (we do not recommend using Google Chrome; it has hidden features that can capture your voice and data. It is also a closed source that sends a lot of data to Google's servers periodically)- to further protect your privacy and security.

The following are the most important add-ons and browser extensions that we recommend:

- **HTTPS Everywhere:** It is one of the most important add-ons that you must install. This extension uses the secure (encrypted) HTTPS protocol on the websites you visit whenever possible. There are two types of connection: http and https. Https is the most secure as it provides encrypted communications between you and the website you visit, and the function of this add-on is to use this protocol whenever possible.

- **AdBlock Plus:** This extension blocks on-page ads and pop-ups that may appear to you while browsing, and it is a very popular add-on. You might ask: What is the relationship between ad blocking and security/privacy? You should know that almost all advertising companies track you and your movements as well the websites you visit, and this is in order to customize the ads for you. For instance, ad companies will never show you ads in French if you are from Egypt, but ads will rather appear for you in Arabic and from Egyptian advertisers. AdBlock Plus add-on will immensely protect your privacy and keep your identity anonymous, and hence disable all unwanted tracking practices from advertising companies.
- **Ghostery:** The function of this plugin is to block websites, services and scripts that automatically track you and try to collect information about your identity. Many of the websites you visit try to run scripts (code that runs on your browser) in order to track users and gather information about them. The function of this add-on is to block such automatically-generated scripts, websites and services. You can also control the add-on options if you want.
- **WOT:** Very briefly, the function of this add-on is to inform you about the suspicious websites that contain scams or malicious links infected with malware, and on the other hand, it guides you to the safe websites. So this add-on will be very useful when you are browsing unknown websites for the first time.

Of course, there are many other browser plugins/extensions that you can use to protect your device against viruses and malware (on Windows). There are also many options to choose your antivirus program, but we recommend: Bitdefender, Avira or KasperSky; they are the most successful programs according to the Quality and performance tests for antivirus software, as they are tested on many popular security test websites.

You can also use malware detection and removal tools such as:

Malicious Software Removal Tool (MSRT) from Microsoft Corporation and Spybot.