



قسم تكنولوجيا المعلومات
شعبة الامن السيبراني



اساسيات امن المعلومات و الأمان السيبراني



اعداد
ظه علي طه
مسؤول شعبة الامن
السيبراني
MOYS - CERT

امن المعلومات:- حماية المعلومات بكل اشكالها من اي تغير او وصول غير مصرح به الكترونية او غير الكترونية

الامن السيبراني (cyber security) :- حماية الشبكات والاجهزة والبرامج والبيانات من الهجمات والاختراق الخارجي



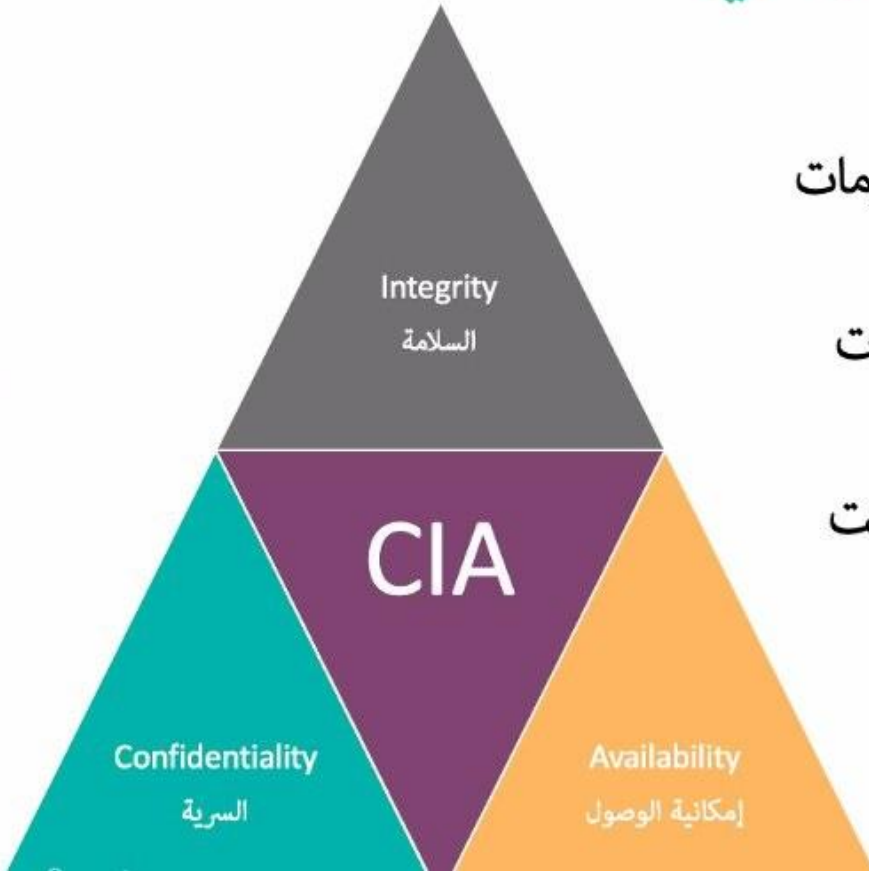
امن المعلومات يهتم بحماية (البيانات والمعلومات) فقط من الهجمات الخارجية بينما يهتم

الامن السيبراني (cyber security) بحماية (البيانات والاجهزة والشبكات)

الامن المعلومات يتعامل مع اي وصول غير مصرح به للبيانات

الامن السيبراني (cyber security) يتعامل مع الجرائم الالكترونية والاحتيال الرقمي

اهداف الامن السيبراني



• السرية Confidentiality

عدم إمكانية الوصول الغير مصرح به للبيانات او المعلومات

• السلامة Integrity

حماية البيانات أو المعلومات من أي تغييرات أو تعديلات

• إمكانية الوصول Availability

امكانية الوصول للبيانات من قبل المصرح له وفي أي وقت



أهداف الأمن السيبراني



التوافر وا تاحة (Availability)

تعني بقاء المعلومة متوفرة للمستخدم وإمكانية الوصول إليها في أي وقت وعدم تعطل ذلك نتيجة لخلل في أنظمة إدارة قواعد المعلومات والبيانات أو وسائل الإتصال .



التكامل وسلامة المحتوى (Integrity)

المقصود بها أن تكون المعلومة صحيحة عند إدخالها وكذلك أثناء نقلها بين الأجهزة في الشبكة والتأكد أنه لم يمسها أي تغيير وذلك باستخدام مجموعة من الأساليب والأنظمة .



السرية (Confidentiality)

تعني منع الوصول إلى ا لمعلومات إلا من الأشخاص ا لمصرح لهم فقط سواءا عند تخزينها أو معالجتها أو عند نقلها عبر وسائل الاتصال وكذلك تحديد صلاحية التعديل والحذف والإضافة .

كلمات المرور (passwords)



كلمات المرور (passwords)



كلمات المرور القوية يجب ان تكون :

• معقدة : تتكون من احرف كبيرة وصغيرة اضافة الى ارقام ورموز .

• طويلة : لا تقل عن (14) رمز .

• غير متكرر : لا تكرر نفس الرمز اكثر من مرتين .

• غير متتالية : لا تحتوي على الانماط المتتالية

مثل [ABC ,QWE ,123] .

• غير شخصية : لا تحتوي على معلومات شخصية مثل الاسم او اسم الطفل ,

الحيوان الاليف , اسم الشريك , البلد , تاريخ الزواج , او برنامجك المفضل .

• فريدة : كل حساب يجب ان يمتلك كلمة مرور مختلفة .

(password)

- password
- Password
- PAssword
- PASsword
- PASSword
- PASSWOrd
- PASSWORd
- PASSWORD
- password
- pAssword
- pASsword
- pASSword
- pASSWOrd
- pASSWORd
- pASSWORD
- password
- paSsword
- paSSword
- paSSWOrd
- paSSWORd
- paSSWORD
- paSSWORD



امثلة عن كلمات المرور

كلمات مرور جيدة	كلمات مرور ضعيفة
\$@rAh	Sarah
Ps\$w0rd	password
P@\$w0rd	Password@123
1R@q	iraq
@li@2o2o	Ali@2020
o77o955o44o	07709550440
l99ol99o	19901990

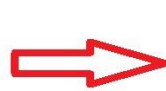


قسم تكنولوجيا المعلومات شعبة الامن السيبراني

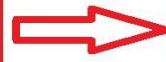


طريقة عمل كلمة مرور للحاسبة

Windows 7



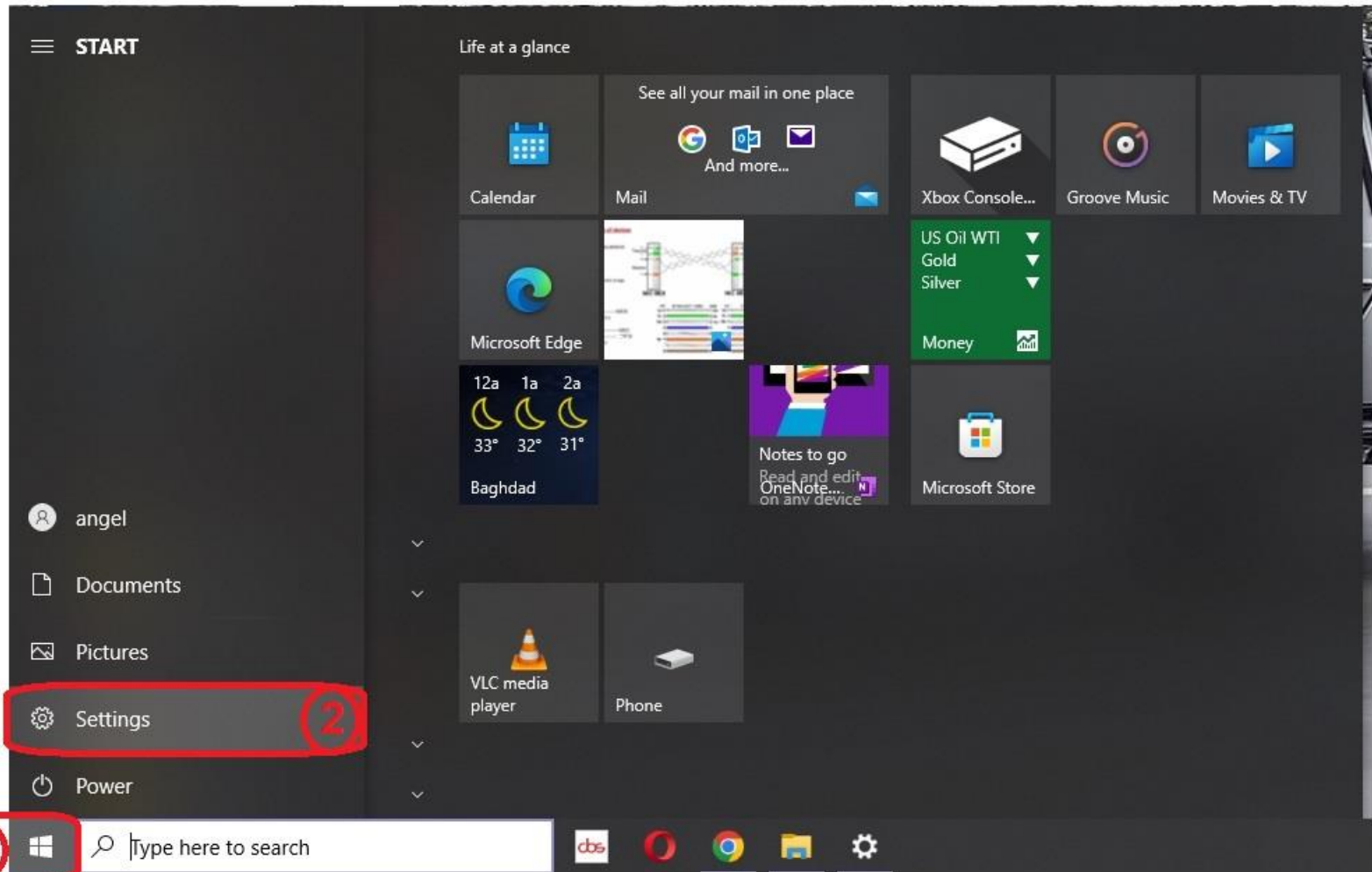
control panel



user account and family safety

The screenshot shows the Windows 7 Control Panel interface. The breadcrumb trail is "Control Panel > All Control Panel Items > User Accounts". The main heading is "Make changes to your user account". A red box labeled "1" highlights the "Create a password for your account" link. Below it are links for "Change your picture", "Change your account name", "Change your account type", "Manage another account", and "Change User Account Control settings". A user profile card for "pc Administrator" is visible. An inset window titled "Create Your Password" is shown, containing the heading "Create a password for your account" and the user name "pc Administrator". It has two input fields: "New password" and "Confirm new password", both highlighted with a red box labeled "2". Red arrows point to these fields with the Arabic text "كتابة كلمة السر" (Write the password) and "تأكيد كلمة السر" (Confirm the password). Below the fields is a "Type a password hint" field and a "Create password" button, which is highlighted with a red box labeled "3".

Windows 10





angel
Local Account
[Sign In](#)

Get even more out of Windows

With a few quick selections, you'll be on your way to enjoying the full Microsoft experience.

[Let's go!](#)

[Skip for now](#)

Find a setting

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Phone
Link your Android, iPhone

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, family

Time & Language
Speech, region, date

Gaming
Xbox Game Bar, captures, Game Mode

Ease of Access
Narrator, magnifier, high contrast

Search
Find my files, permissions

Privacy
Location, camera, microphone

Update & Security
Windows Update, recovery, backup

[Windows isn't activated. Activate Windows now.](#)

Activate Windows
Go to Settings to activate Windows.

← Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

Sync your settings

4

Sign-in options


Manage how you sign in to Windows


Select a sign-in option to add, change, or remove.

 Windows Hello Face
This option is currently unavailable.

 Windows Hello Fingerprint
This option is currently unavailable.


 Windows Hello PIN
This option is currently unavailable.

 Security Key
Sign in with a physical security key.

 Password
Sign in with your account's password.
Your account doesn't have a password before you can use it.

Update your security questions.

[Learn more](#)

 Picture Password
This option is currently unavailable—click to learn more.

Create a password

6

New password

كتابة كلمة المرور

Confirm password

تأكيد كلمة المرور

Password hint

Next

Cancel

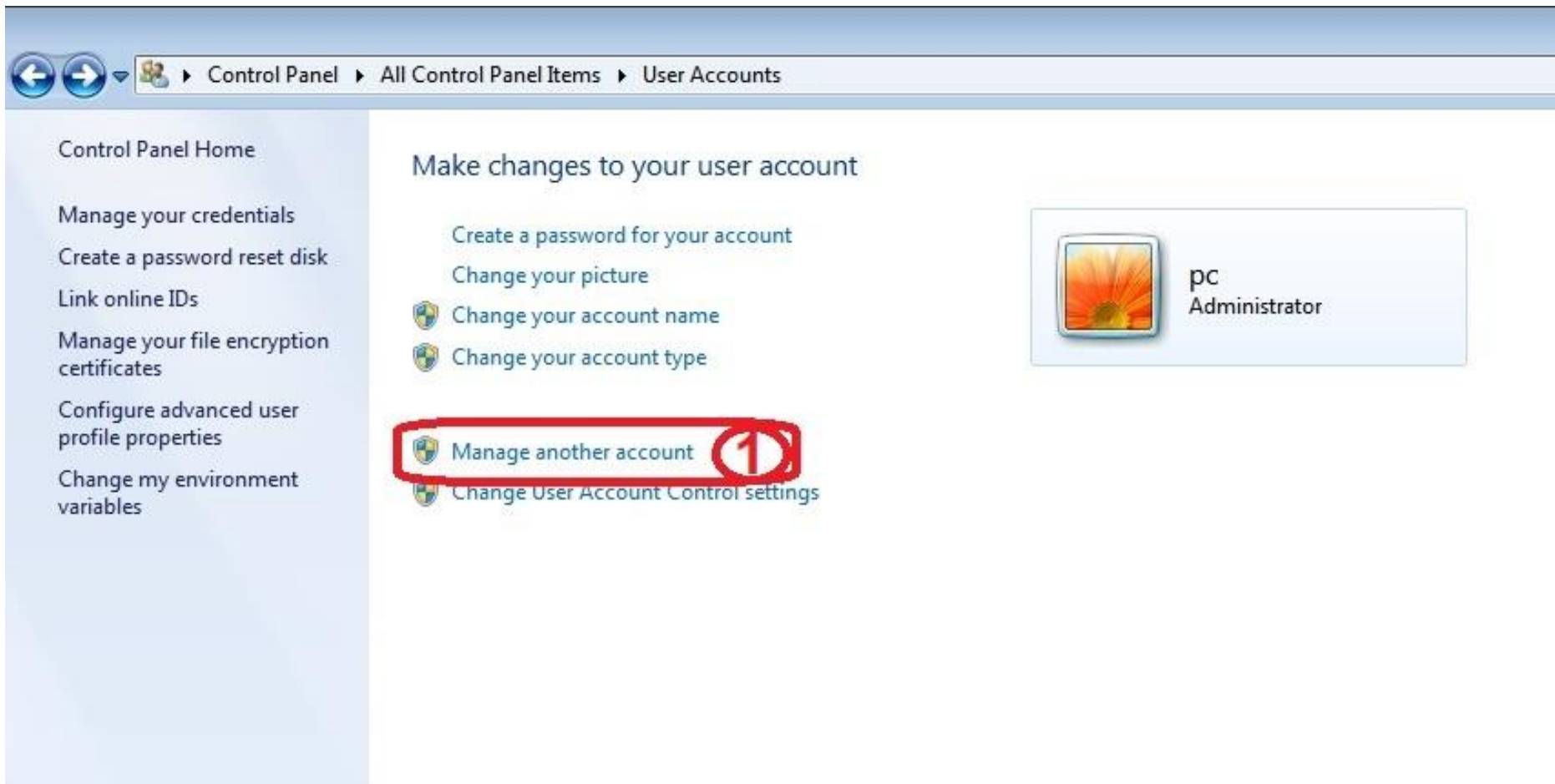
5

Add



انشاء اكثر من مستخدم على الحاسبة

Windows 7



The screenshot shows the Windows 7 Control Panel interface. The breadcrumb navigation at the top reads: Control Panel > All Control Panel Items > User Accounts. On the left, a sidebar lists various control panel options. The main content area is titled "Make changes to your user account" and lists several actions. The "Manage another account" option is highlighted with a red rectangle and a red circle containing the number 1. To the right, a user account card for "pc Administrator" is visible, featuring a sunburst profile picture.

Control Panel > All Control Panel Items > User Accounts

Control Panel Home

- Manage your credentials
- Create a password reset disk
- Link online IDs
- Manage your file encryption certificates
- Configure advanced user profile properties
- Change my environment variables

Make changes to your user account

- Create a password for your account
- Change your picture
- Change your account name
- Change your account type
- Manage another account** 1
- Change User Account Control settings

pc Administrator

Choose the account you would like to change



pc
Administrator



Guest
Guest account is off

Create a new account

2

What is a user account?

Additional things you can do

 Set up Parental Controls

[Go to the main User Accounts page](#)

Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

3

نكتب اسم الحساب

Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

Administrator

Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

[Why is a standard account recommended?](#)

4

Create Account

Cancel

Choose the account you would like to change



pc
Administrator



Guest
Guest account is off



Account 1
Standard user

هنا ظهر
الحساب الجديد

[Create a new account](#)

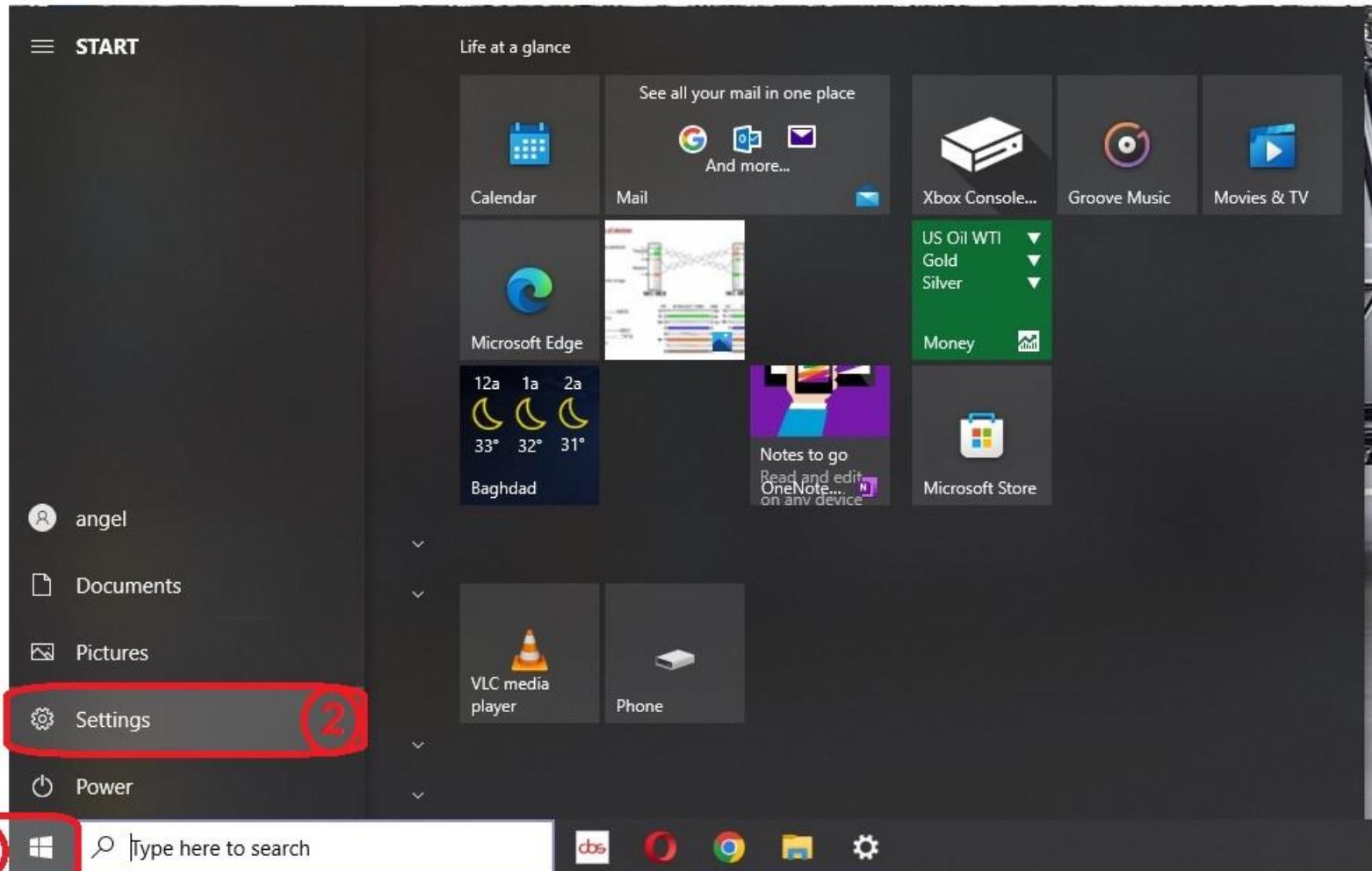
[What is a user account?](#)

Additional things you can do

 [Set up Parental Controls](#)

[Go to the main User Accounts page](#)

Windows 10





angel
Local Account
[Sign In](#)

Get even more out of Windows

With a few quick selections, you'll be on your way to enjoying the full Microsoft experience.

[Let's go!](#)

[Skip for now](#)

Find a setting | 🔍

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Phone
Link your Android, iPhone

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, family

Time & Language
Speech, region, date

Gaming
Xbox Game Bar, captures, Game Mode

Ease of Access
Narrator, magnifier, high contrast

Search
Find my files, permissions

Privacy
Location, camera, microphone

Update & Security
Windows Update, recovery, backup

[Windows isn't activated. Activate Windows now.](#)

[Activate Windows](#)
Go to [Settings](#) to activate Windows.

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

4

Sync your settings

Family & other users

Your family

Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games.

[Sign in with a Microsoft account](#)

Other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

+ Add someone else to this PC

5

Set up a kiosk



Assigned access
Set up this device as a kiosk—this could be a digital sign, interactive display, or public browser among other things.

Bring Family Safety to your phone
Use all of the digital safety features you already know, plus location sharing for the whole family.
[Get the app](#)

Help from the web
[Creating a local user account](#)
[Setting screen time limits](#)
[Switching users](#)

[Get help](#)
[Give feedback](#)

Activate Windows
Go to Settings to activate Windows.

Settings

Home

Find a setting

Accounts

- Your info
- Email & accounts
- Sign-in options
- Access work or school
- Family & other users
- Sync your settings

Microsoft account

Microsoft

How will this person sign in?

Enter the email address or phone number of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email or phone number they use to sign in.

Email or phone

don't have this person's sign-in information

Cancel Next

Terms of Use Privacy & Cookies

Bring Family Safety to your phone

Use all of the digital safety features you already know, plus location sharing for the whole family.

[Get the app](#)

Help from the web

- [Creating a local user account](#)
- [Setting screen time limits](#)
- [Switching users](#)

- [Get help](#)
- [Give feedback](#)

Activate Windows

Go to Settings to activate Windows.

Type here to search

Taskbar icons: cbs, File Explorer, Settings, Microsoft Store

System tray: 11:34 PM, 2022-08-30, Network, Volume, Bluetooth, Battery

Settings

Home

Find a setting

Accounts

- Your info
- Email & accounts
- Sign-in options
- Access work or school
- Family & other users
- Sync your settings

Microsoft account

Microsoft

Create account

someone@example.com

Use a phone number instead

Get a new email address

[Add a user without a Microsoft a](#) **7**

Back Next

Terms of Use Privacy & Cookies

Bring Family Safety to your phone

Use all of the digital safety features you already know, plus location sharing for the whole family.

[Get the app](#)

Help from the web

- [Creating a local user account](#)
- [Setting screen time limits](#)
- [Switching users](#)

- [Get help](#)
- [Give feedback](#)

Activate Windows

Go to Settings to activate Windows.

Type here to search

Taskbar icons: cbs, Chrome, File Explorer, Settings, Edge

System tray: 11:35 PM, 2022-08-30, 2 notifications

← Settings

Home

Find a setting

Accounts

- Your info
- Email & accounts
- Sign-in options
- Access work or school
- Family & other users
- Sync your settings

Microsoft account

Create a user for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

User name *اسم المستخدم*

Make it secure.

Enter password *كلمة المرور*

Re-enter password

Next Back

Bring Family Safety to your phone

Use all of the digital safety features you already know, plus location sharing for the whole family.

Get the app

Help from the web

- Creating a local user account
- Setting screen time limits
- Switching users

Get help

Give feedback

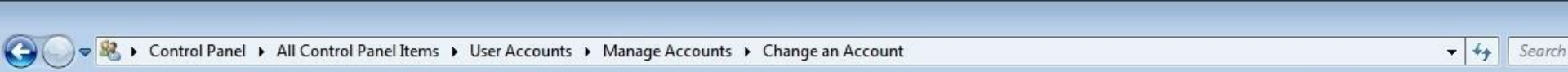
Activate Windows

Go to Settings to activate Windows.



حذف حساب مستخدم من windows

Windows 7

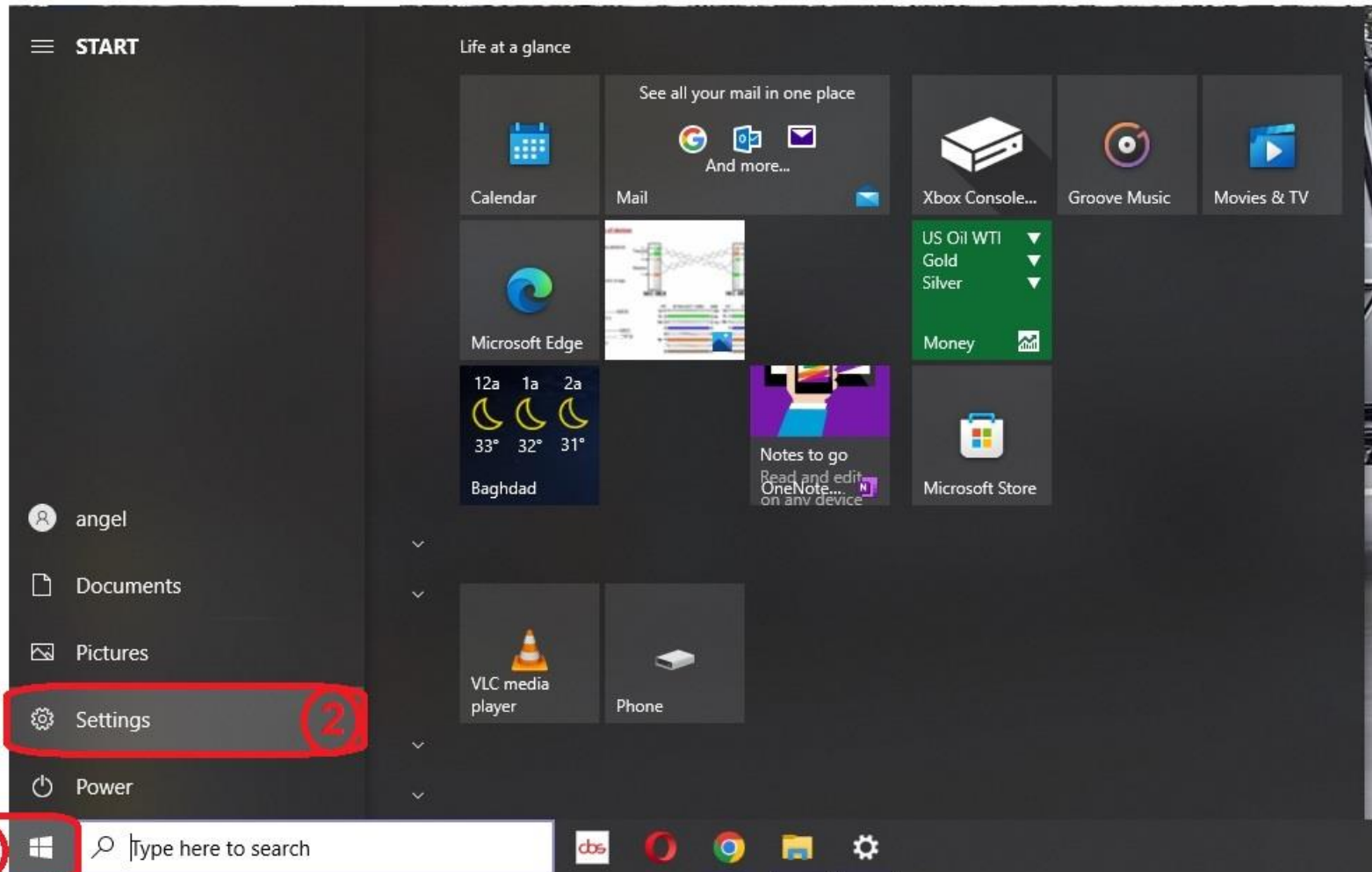


Make changes to Account 2's account

- Change the account name
- Create a password
- Change the picture
- Set up Parental Controls
- Change the account type
- Delete the account (1)**
- Manage another account



Windows 10





angel
Local Account
[Sign In](#)

Get even more out of Windows

With a few quick selections, you'll be on your way to enjoying the full Microsoft experience.

[Let's go!](#)

[Skip for now](#)

Find a setting | 🔍

System
Display, sound, notifications, power

Devices
Bluetooth, printers, mouse

Phone
Link your Android, iPhone

Network & Internet
Wi-Fi, airplane mode, VPN

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, family

Time & Language
Speech, region, date

Gaming
Xbox Game Bar, captures, Game Mode

Ease of Access
Narrator, magnifier, high contrast

Search
Find my files, permissions

Privacy
Location, camera, microphone

Update & Security
Windows Update, recovery, backup

[Windows isn't activated. Activate Windows now.](#)

[Activate Windows](#)
Go to Settings to activate Windows.

← Settings

Home

Find a setting

Accounts

- Your info
- Email & accounts
- Sign-in options
- Access work or school
- Family & other users** **4**
- Sync your settings

Family & other users

Delete account and data?

Delete account and data?

t
Local Account

Deleting this person's account will remove all their data from this PC, including items on their desktop, downloads, documents, photos, music, and other files. If this data hasn't been backed up or saved to another location, such as another PC, it will be lost.

6

Delete account and data

Cancel

+ Add someone else to this PC

t
Local account

Change account type

Remove

5

Set up a kiosk



تغير كلمة المرور للبريد الالكتروني



✍️ Compose

📧 Inbox

☆ Starred

🕒 Snoozed

📌 Important

▶ Sent

📄 Drafts

📁 Categories

^ Less

💬 Chats

📅 Scheduled

📧 All Mail

🕒 Spam

🗑️ Bin

⚙️ Manage labels



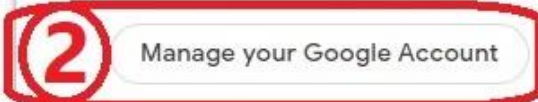
No conversations in Bin.

Terms · Privacy · Programme Policies



Taha Ali

****@gmail.com



Signed out



Signed out



Signed out



Signed out



Signed out

Home

Personal info

3

Data and privacy

Security

People and sharing

Payments and subscriptions

About



Welcome, Taha

Manage your info, privacy and security to make Google w

Privacy & personalisation

See the data in your Google Account and choose what activity is saved, to personalise your Google experience



[Manage your data and privacy](#)

You |

Securi
Check

[Review](#)

- Home
- Personal info**
- Data and privacy
- Security
- People and sharing
- Payments and subscriptions
- About

Password



A secure password helps protect your Google Account

.....

Last changed



General preferences

Manage settings for Google



Language
English (United States)



Input Tools
Type more easily in y



Accessibility
High-contrast colour

Looking for something else?



Search Google Account



Hi Taha

 ****@gmail.com ▾

To continue, first verify it's you

Enter your password

| نكتب كلمة المرور

5

Show password

[Forgot password?](#)

[Next](#)

← Password

Choose a strong password and don't reuse it for other accounts. [Learn more](#)

Changing your password will sign you out on your devices, with some [exceptions](#).

New password

نكتب كلمة المرور الجديده



Password strength:

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

6

Confirm new password تأكيد كلمة المرور الجديده



7

Change password

Password Manager



مدير كلمات المرور

مدير كلمات المرور (Password Manager) :- هو تطبيق برمجي يساعد في توليد واسترجاع كلمات السر المعقدة (password) حيث يقوم بتخزين معلومات تسجيل الدخول لجميع مواقع الويب التي تستخدمها ويساعدك على تسجيل الدخول إليها تلقائياً ويقوم بتشفير قاعدة بيانات كلمات المرور بكلمة مرور رئيسية – كلمة المرور الرئيسية هي الوحيدة التي يجب عليك تذكرها.

أفضل مدير لكلمات المرور

- 1- google
- 2- True Key
- 3- LastPass
- 4- Dashlane
- 5- Roboform
- 6- Stiky Password
- 7- KeePass
- 8- LogMeOnce



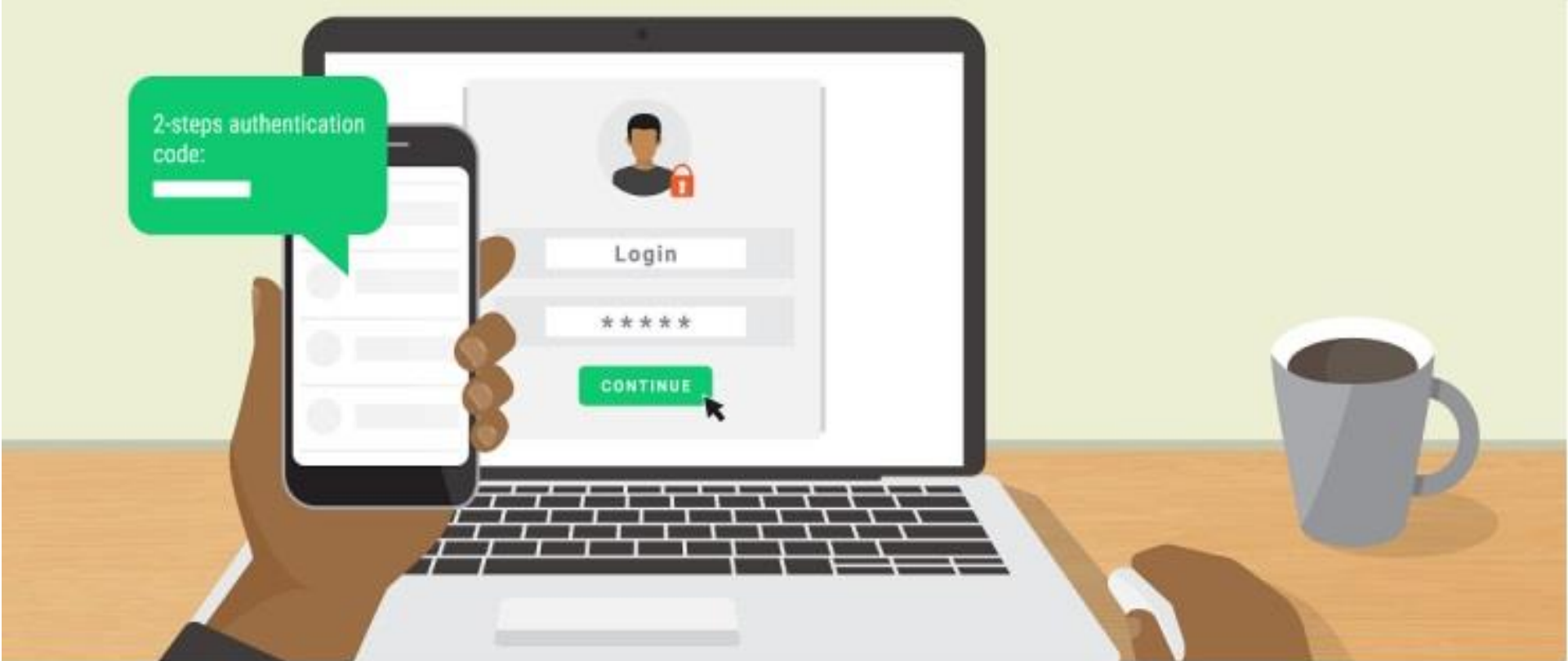


قسم تكنولوجيا المعلومات شعبة الامن السيبراني





مواقع التواصل الاجتماعي



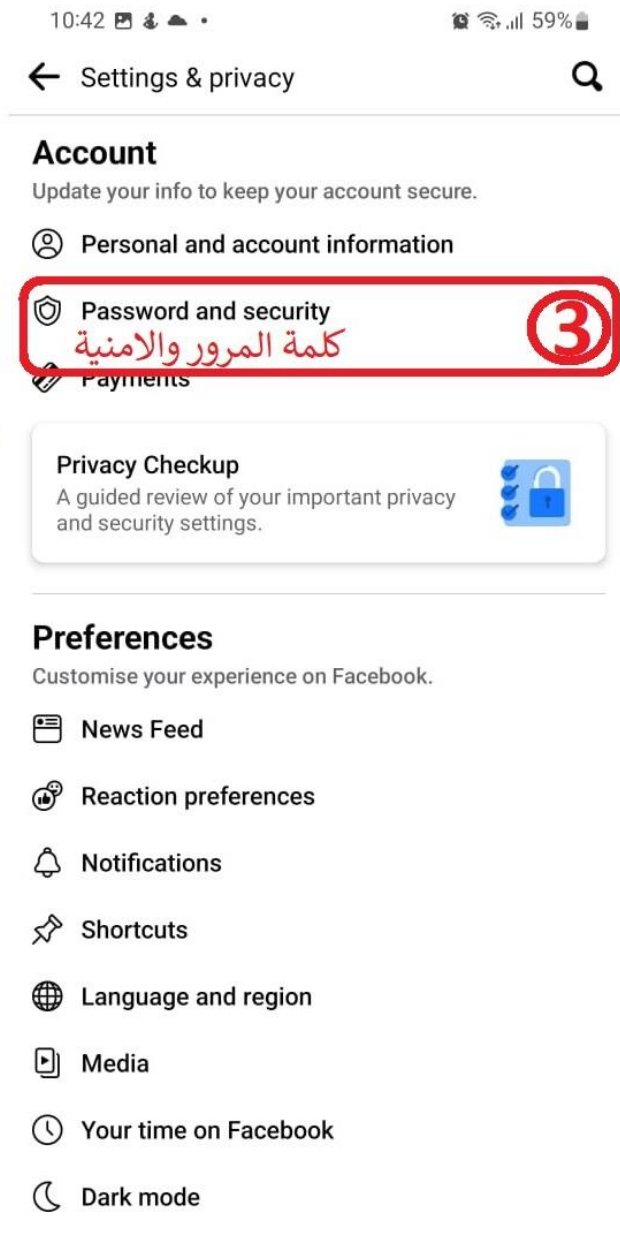
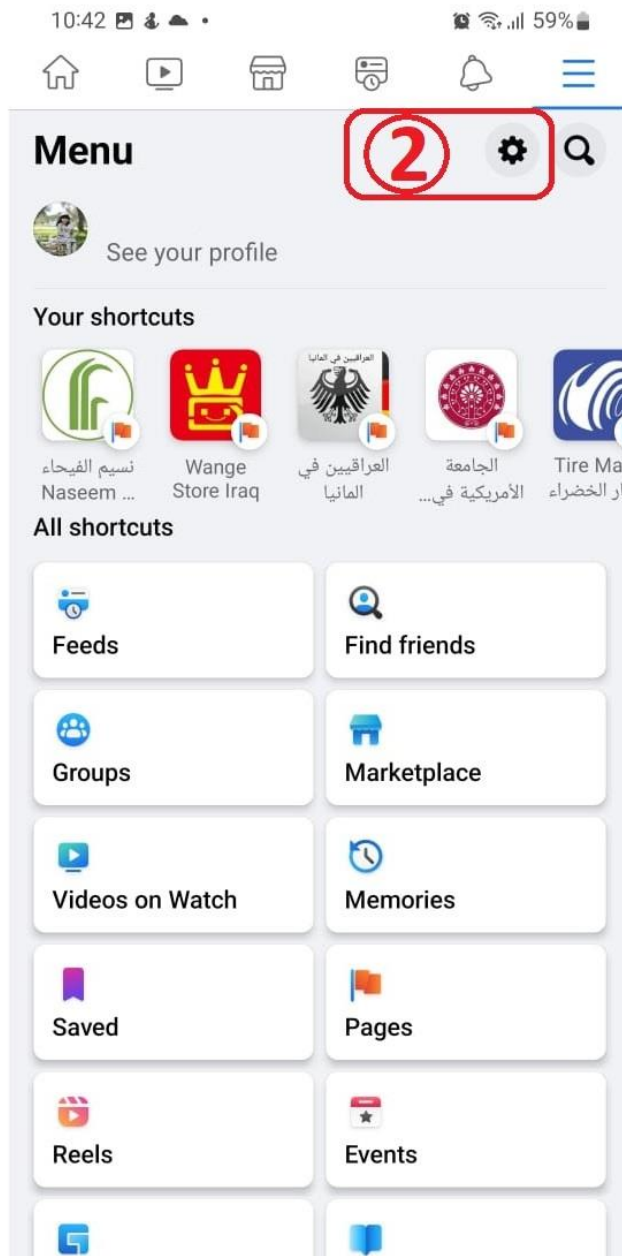
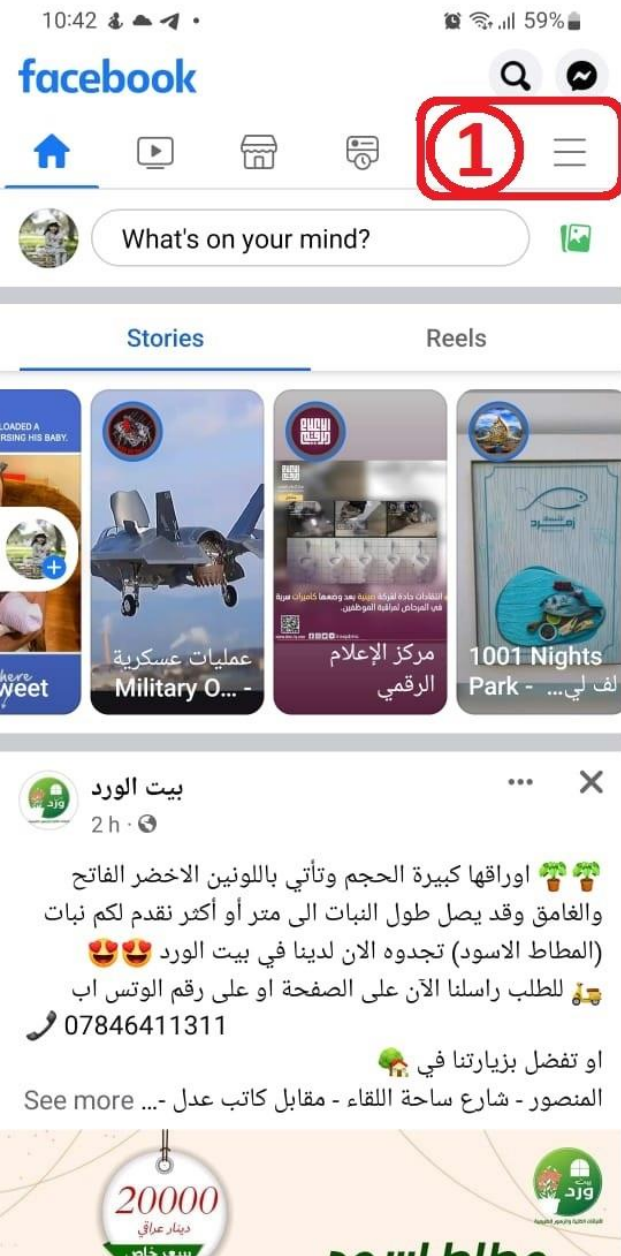
المصادقة الثنائية :- هي ميزة أمان تساعدك في حماية حسابك على مواقع التواصل الاجتماعي بالإضافة إلى كلمة السر الخاصة بك.

إذا قمت بإعداد مصادقة ثنائية، فستتم مطالبتك بإدخال رمز تسجيل دخول خاص أو تأكيد محاولة تسجيل الدخول في كل مرة يحاول فيها شخص ما الوصول إلى مواقع التواصل الاجتماعي من متصفح أو جهاز محمول غير معروف لنا.

Facebook



(Two-Factor Authentication)
(المصادقة بعاملين)





Password and security

Recommended

Check your important security settings
We'll take you through some steps to help protect your account.

Where you're logged in See all

- Samsung Galaxy • Baghdad, Iraq
Facebook app • Active now
- Samsung Galaxy • Baghdad, Iraq
Messenger • 19 hours ago

Login

Change password
It's a good idea to use a strong password that you don't use elsewhere

Two-factor authentication

Use two-factor authentication **4**
We'll ask for a login code if we notice an attempted login from an unrecognized device or browser.

Two-factor authentication



Help protect your account

If we notice an attempted login from a device or browser we don't recognise, we'll ask for your password and a verification code.

Select a security method

Authentication app
Recommended · Use an app such as Google Authenticator or Duo Mobile to generate verification codes for more protection.

Text message (SMS) **5**
Use text messages (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can't be used to reset your password when two-factor authentication is on.

Security key
Use a physical security key to help protect your Facebook account from unauthorised access. You won't need to enter a code.

Continue

Two-factor authentication

Select your phone number

Choose a mobile phone number that is already on your account or add a new number for two-factor authentication. This is the number you will receive your verification code on.

0770 4***67

Add phone number

نكتب الرقم المراد ارسال رمز المصادقة عليه **6**

Continue

← Two-factor authentication

Enter code

Enter the 6-digit code that we sent to +964 *****67 to finish setting up two-factor authentication.

7

نكتب الرمز المرسل



It might take a couple of minutes for your code to arrive. If you're having trouble receiving the code, try reviewing your Facebook text message settings. [Learn more](#).

Please wait for 2:56 before requesting a new code.

Continue

← Two-factor authentication

**Two-factor authentication is on**

+*****67

We'll send a verification code to this number if we notice an attempted login from a device or browser that we don't recognise.

For added protection, this number can't be used to reset your password when two-factor authentication is on.

8**Done**



How to Enable (Two-Step Verification)

كيفية تفعيل التحقق بخطوتين

طريقة توثيق حسابك في الواتساب بخطوتين



2. التحقق بخطوتين

Two-Step verification



1. من الاعدادات < الحساب

Account < settings



4. سيطلب منك وضع رقم تعريف عند تسجيل رقم هاتفك في الواتساب



3. تمكين
Enable



6

6. انتظر بضع ثوان لتمكن الميزه



5

5. سيطلب منك عنوان بريدك الالكتروني للحماية



(Two – Factor Authentication)

(المصادقة بعاملين)



30 Following 1 Follower

- Profile
- Lists
- Topics
- Twitter Circle New
- Bookmarks
- Moments
- Monetisation
- Twitter for Professionals

Settings and privacy

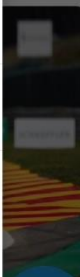
2

الاعدادات و الخصوصية

Help Centre



5h
at
tu.be/



Settings

Search settings

- Your account**
See information about your account, download an archive of your data or learn about your account deactivation options.
- الامان والوصول الى الحساب** 3
Security and account access
Manage your account's security and keep track of your account's usage, including apps that you have connected to your account.
- Monetisation**
See how you can make money on Twitter and manage your monetisation options.
- Privacy and safety**
Manage what information you see and share on Twitter.
- Notifications**
Select the kinds of notification you get about your activities, interests and recommendations.
- Accessibility, display and languages**
Manage how Twitter content is displayed to you.
- Additional resources**
Check out other places for helpful information to learn more about Twitter products and services.

Security and account access

Manage your account's security and keep track of your account's usage, including apps that you have connected to your account.

- الامان** 4
Security
Manage your account's security.
- Apps and sessions**
See information about connected apps and login sessions for your account.
- Connected accounts**
Manage Google or Apple accounts connected to Twitter to log in.



Security

Manage your account's security.

Two-factor authentication

Help protect your account from unauthorised access by requiring a second authentication method in addition to your Twitter password. You can choose a text message, authentication app or security key. [Learn more](#)

المصادقة بعاملين

5

Two-factor authentication

Additional password protection

Enabling this setting adds extra security to your account by requiring additional information to reset your password. If enabled, you must provide either the phone number or email address associated with your account in order to reset your password.

Password reset protection



Security

Two-factor authentication

رسالة نصية

Text message

6

Use your mobile phone to receive a text message with an authentication code to enter when you log in to Twitter.



Authentication app

Use an app to get an authentication code to enter when you log in to Twitter.



Security key

Use a security key that inserts into your computer or syncs to your mobile device when you log in to Twitter. You'll need to use a supported mobile device or web browser.

[Learn more](#)



Add an email address

You need an authenticated email address associated with your account to enable two-factor authentication. We use your email for things like account security and keeping you updated. [Learn more in our Privacy Policy.](#)

7

Get started





Add an email address

A confirmation code will be sent to this address.

Email address

8

كتابة الـ (Email) المراد ارسال رمز التحقق الية

Let people who have your email address find and connect with you on Twitter. [Learn more.](#)

Let Twitter use your email address to personalise our services, including ads (if permitted by your Ads preferences). If you don't enable this, Twitter may still use your email address for purposes including account security and spam, fraud and abuse prevention. [See our Privacy Policy for more information.](#)

Cancel

Send code

Confirm



We sent you a code

Check @gmail.com for your confirmation code, then enter it to confirm this is your email address.

Enter the verification code

كتابة رمز التحقق المرسل الى (Email)

9

[Resend code](#)



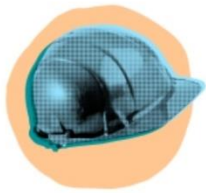
Email address added

You can now finish setting up two-factor authentication.

10

Continue set-up





Protect your account with two-factor authentication in just two steps

- 1 Confirm your phone number
You'll receive a text message with a confirmation code.
- 2 Enter the confirmation code
Two-factor authentication will then be turned on for text message, which you can turn off at any time.

11

Get started



Confirm your phone number

You'll receive a text message with a confirmation code on your mobile phone number +964770*****. Use the code to confirm this is really your number.

Send code

ارسال رمز التحقق الى هذا الرقم

12

Message and data rates from your carrier may apply for text messages.



We sent you a code

Check +964770 **** for your confirmation code, then enter it to confirm this is your phone number.

Enter code

كتابة رمز التحقق المرسل الى هذا الرقم

13

Didn't receive code?

Confirm

7:45

76%



You're all set

You'll receive a text message with an authentication code to enter when you log in to Twitter.

Save this single-use backup code in a safe place.

48be7ndm4ryr

This backup code lets you log in to Twitter if you don't have access to any of your two-factor authentication methods.

14

Done



(Two Factor Authentication)

(تسجيل الدخول بخطوتين)

1

Taha Ali

Find friends on Snapchat
Tap to sync your contacts

Stories
+ Private Story

Add to My Story

Add to Our Story

Friends
Add Friends

My Friends

Bitmoji
Change My Outfit NEW

Edit my Bitmoji

12:33 69%

Settings

MY ACCOUNT

Name Taha Ali

Username

Birthday

Mobile Number 964 770 45'

Email

Password

Two-Factor Authentication 2

Connected Apps

Notifications

Bitmoji

Shazam

Language

ADDITIONAL SERVICES

Asiacell 11:33 PM 46%

تسجيل الدخول بخطوتين

كيفية عمل خاصية تسجيل الدخول بخطوتين

سيطلب منك عند تسجيل الدخول إضافة رمز إضافي بعد كلمة المرور.

سيتم إرسال رمز تسجيل الدخول عبر رسالة نصية (قد تطبق أسعار الرسائل)، أو يمكنك إنشاؤها في تطبيق ما.

بمجرد إدخال رمز تسجيل الدخول الخاص بك، سنتأكد من صحة هويتك.

متابعة 3

تسجيل الدخول بخطوتين

ضع في اعتبارك أنك قد لا تستطيع الدخول إلى حسابك إذا فقدت إمكانية الوصول إلى رمز تسجيل الدخول.

هل تريد تفعيل خاصية تسجيل الدخول بخطوتين؟

هيا لنقم بذلك!

4

تسجيل الدخول بخطوتين

يرجى اختيار طريقة لاستلام رمز التحقق.

رسالة نصية
سيتم إرسال رمز إلى 0770 *****

تطبيق المصادقة
إنشاء رمز التحقق على جهازك باستخدام تطبيق مثل Google Authenticator.

يُعدّ التحقق عبر تلقي رسالة نصية الطريقة الأبسط، لكنّ إذا كنت مسافراً خارج البلاد وليست لديك إمكانية الوصول إلى رقم هاتفك، أو أنك تستخدم تطبيق سناب شات عبر جهاز لوحي (تابلت) أو أي جهاز آخر، فإن استخدام تطبيق مصادقة حل جيد.

تسجيل الدخول بخطوتين

إذا لم لقد أرسلنا رمز التحقق إلى *****+964770. من فضلك أدخله أدناه. يمكن هذا رقمك، يمكنك تغييره.

كتابة رمز التحقق المرسل

إيمز التحقق

6

59 إرسال الرمز مرة ثانية

1	2 ب ت ث	3 اء
4 س ش ص ض	5 د ذ ر ز	6 ح ح خ
7 ن ه و ي	8 ف ق ك ل م	9 ظ ط ع غ
	0	⌫

رمز الاسترداد

التالي

احفظ رمز التحقق الاحتياطي الخاص بك.

احفظ رمز التحقق الاحتياطي الخاص بك.

خذ لقطة شاشة لحفظ رمز التحقق الاحتياطي في ألبوم الصور على هاتفك.

حسناً

إلغاء

احفظ لقطة الشاشة

نسخ إلى ذاكرة التخزين المؤقتة

رمز الاسترداد

التالي

احفظ رمز التحقق الاحتياطي الخاص بك.

8205563478

احتفظ برمز التحقق الاحتياطي هذا في مكان آمن، وإذا لم تتمكن من الحصول على رمز لتسجيل الدخول، ستحتاج إلى هذا الرمز لإعادة تسجيل الدخول مرة أخرى إلى حسابك على سناب شات. وقد لا تستطيع الدخول أبداً بدون ذلك.

احفظ لقطة الشاشة

نسخ إلى ذاكرة التخزين المؤقتة

<

تسجيل الدخول بخطوتين

تخطي

تمّ إنهاء جميع الإعدادات بنجاح!

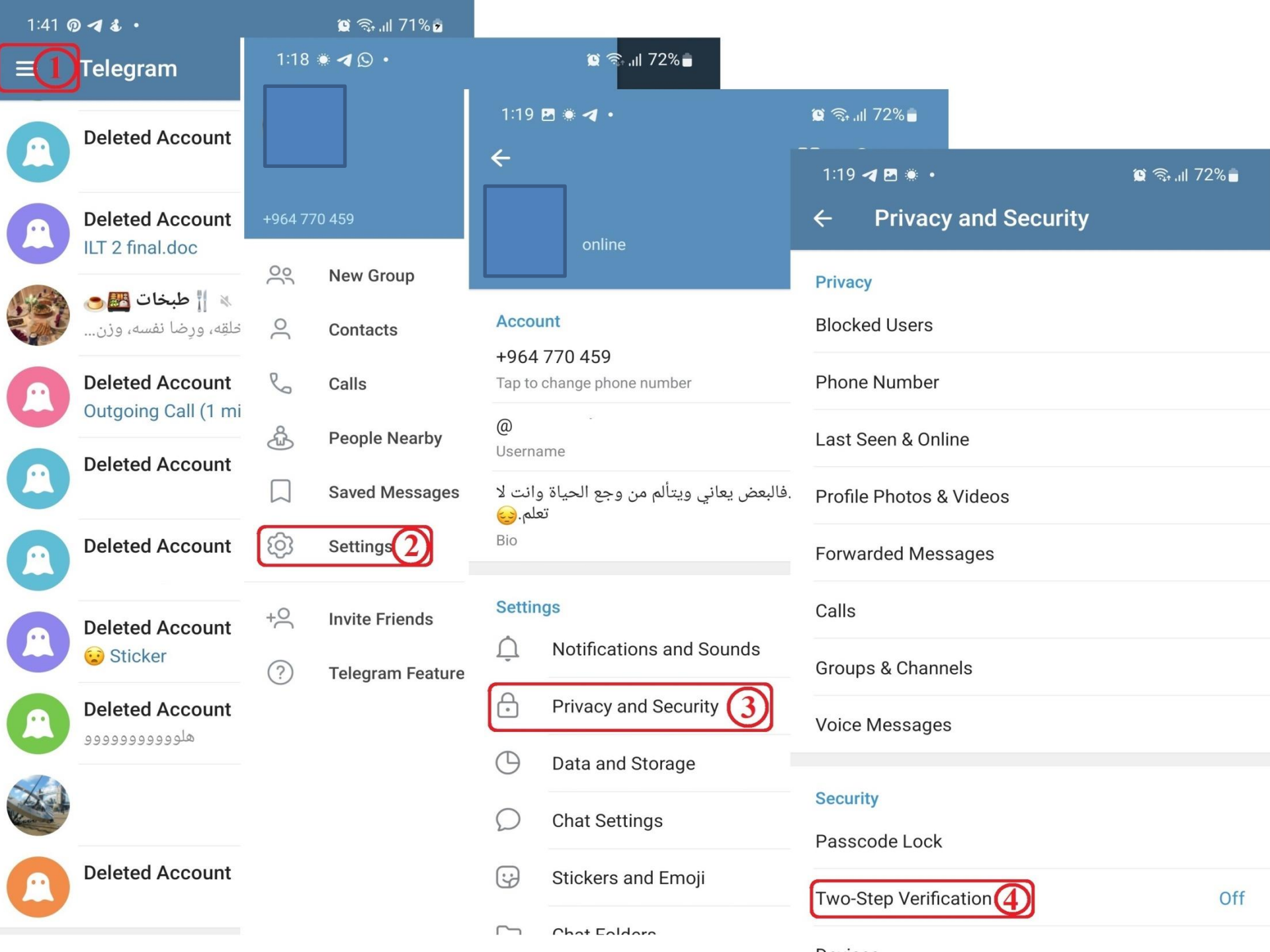
يُمكنك أيضاً الحصول على رموز تسجيل الدخول باستخدام أحد تطبيقات المصادقة، فهذه التطبيقات أكثر أماناً وتمكنك من الحصول على رموز متغيرة باستمرار حتى عندما لا يكون بإمكانك استقبال رسائل نصية، مثلاً عندما تكون مسافراً خارج البلاد.

ضبط إعدادات تطبيق المصادقة



(Two Step Verification)

(التحقق بخطوتين)



Telegram

- Deleted Account
- Deleted Account
ILT 2 final.doc
- طبخات
خلقها، ورضا نفسه، وزن...
- Deleted Account
Outgoing Call (1 mi)
- Deleted Account
- Deleted Account
- Deleted Account
- Deleted Account
Sticker
- Deleted Account
هلوووووووو
- Deleted Account

+964 770 459

- New Group
- Contacts
- Calls
- People Nearby
- Saved Messages
- Settings
- Invite Friends
- Telegram Feature

online

Account

+964 770 459
Tap to change phone number

@
Username

فالععض يعانني ويتألم من وجع الحياة وانت لا تعلم. 😞
Bio

- ### Settings
- Notifications and Sounds
 - Privacy and Security
 - Data and Storage
 - Chat Settings
 - Stickers and Emoji
 - Chat Folders

Privacy and Security

- ### Privacy
- Blocked Users
 - Phone Number
 - Last Seen & Online
 - Profile Photos & Videos
 - Forwarded Messages
 - Calls
 - Groups & Channels
 - Voice Messages
- ### Security
- Passcode Lock
 - Two-Step Verification

Off



Two-Step Verification

You can set a password that will be required when you log in on a new device in addition to the code you get via SMS.

Set Password

5



Create a Password

Enter password

6

نكتب كلمة المرور



Re-enter password

Re-enter password

7

اعادة كتابة كلمة المرور



1:20

72%



Recovery Email

Email

8

نكتب البريد الالكتروني (email)
المراد ارسل رمز المصادقة الية

Skip



1:24

71%



Verification Code

To complete Two-Step Verification Setup, check your email (don't forget the spam folder) and enter the code we just sent you.

9

نكتب الرمز المرسل على الـ Email

Resend Code

1

2

ABC

3

DEF

4

GHI

5

JKL

6

MNO

7

PQRS

8

TUV

9

WXYZ

0

+



1:25

71%



Password Set!

This password will be required when you log in on a new device in addition to the code you get in the SMS.

Return to Settings

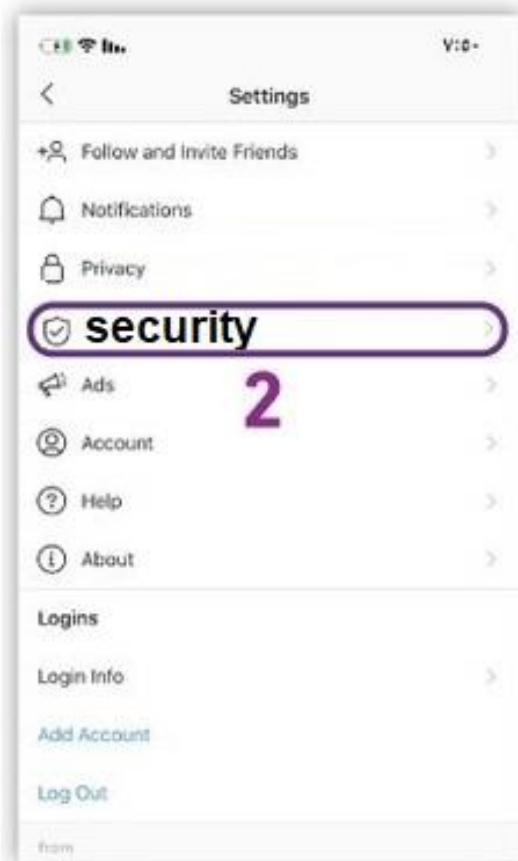


(Two Step Authentication)

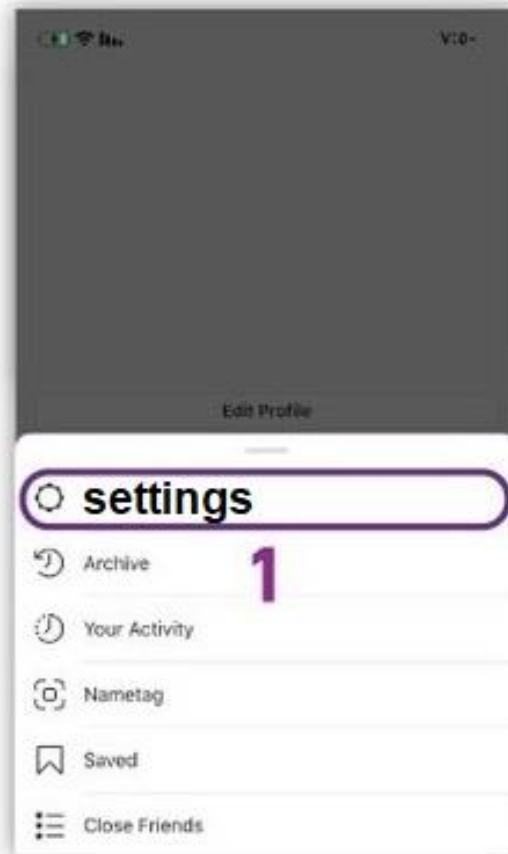
(المصادقة من خطوتين)



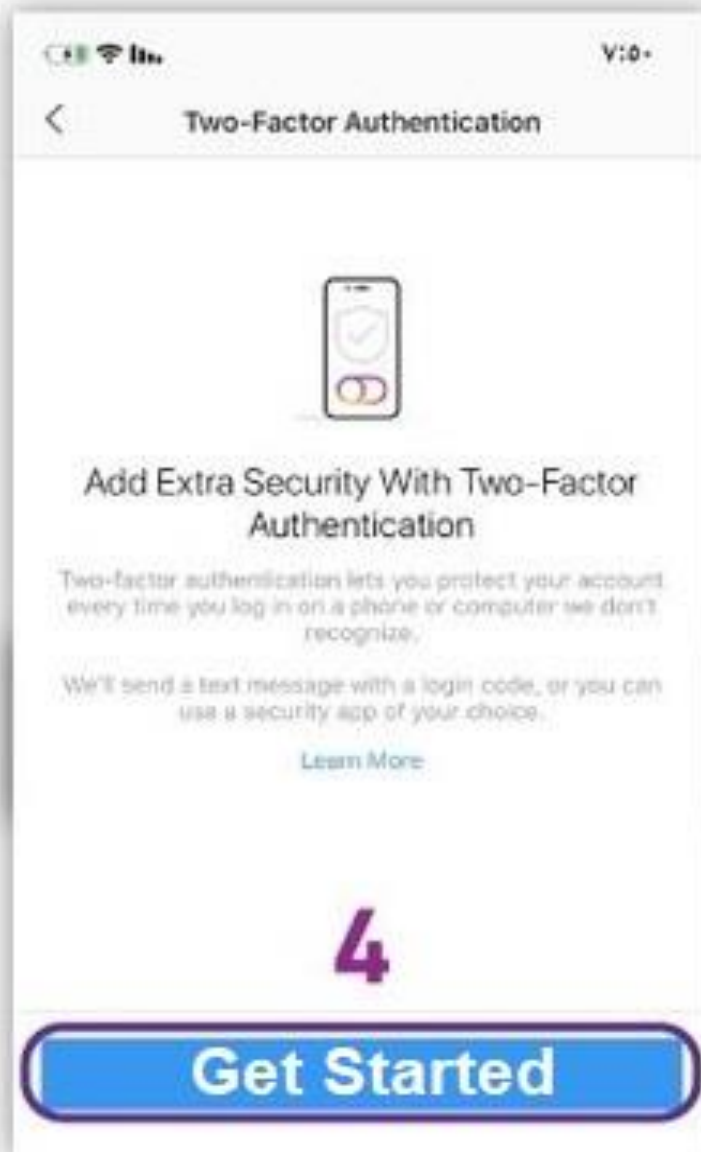
تأمين حساب الانستقرام



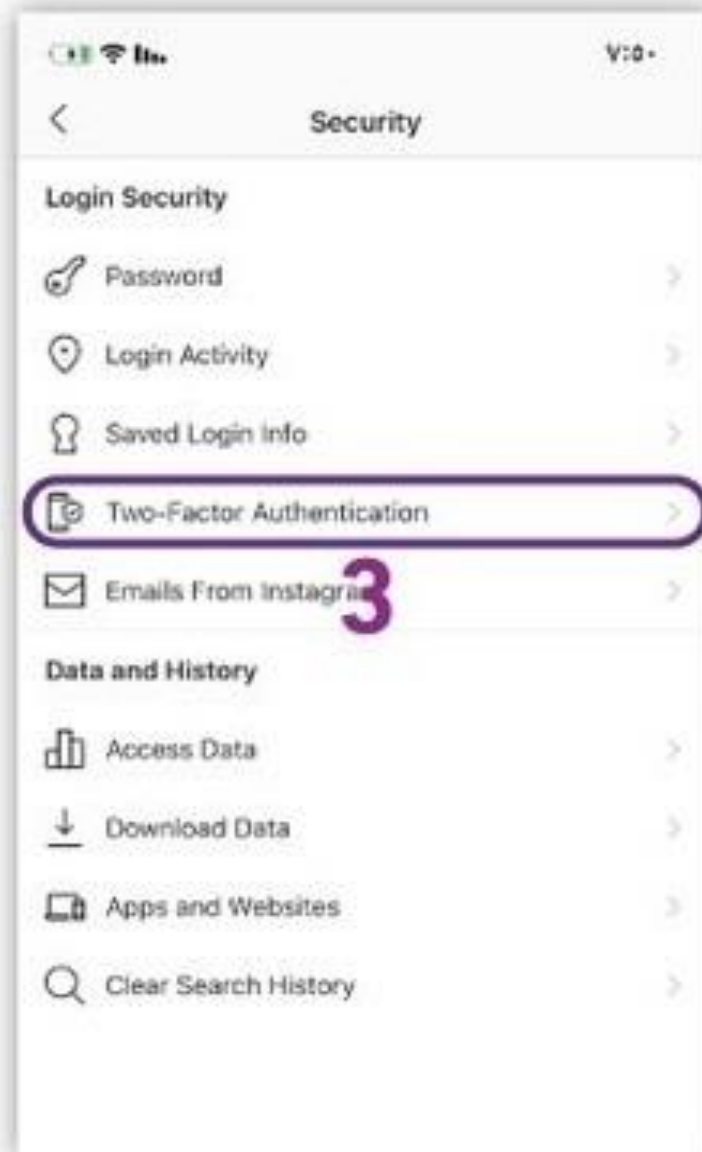
2. الامان security



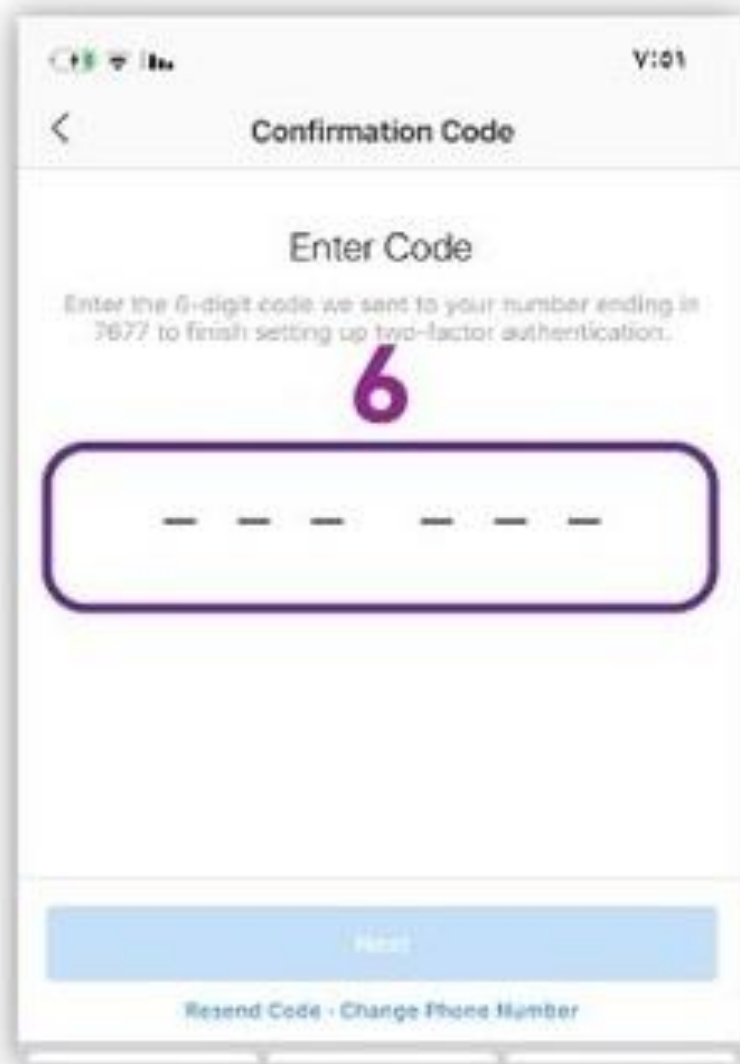
1. الاعدادات settings



4. البدء



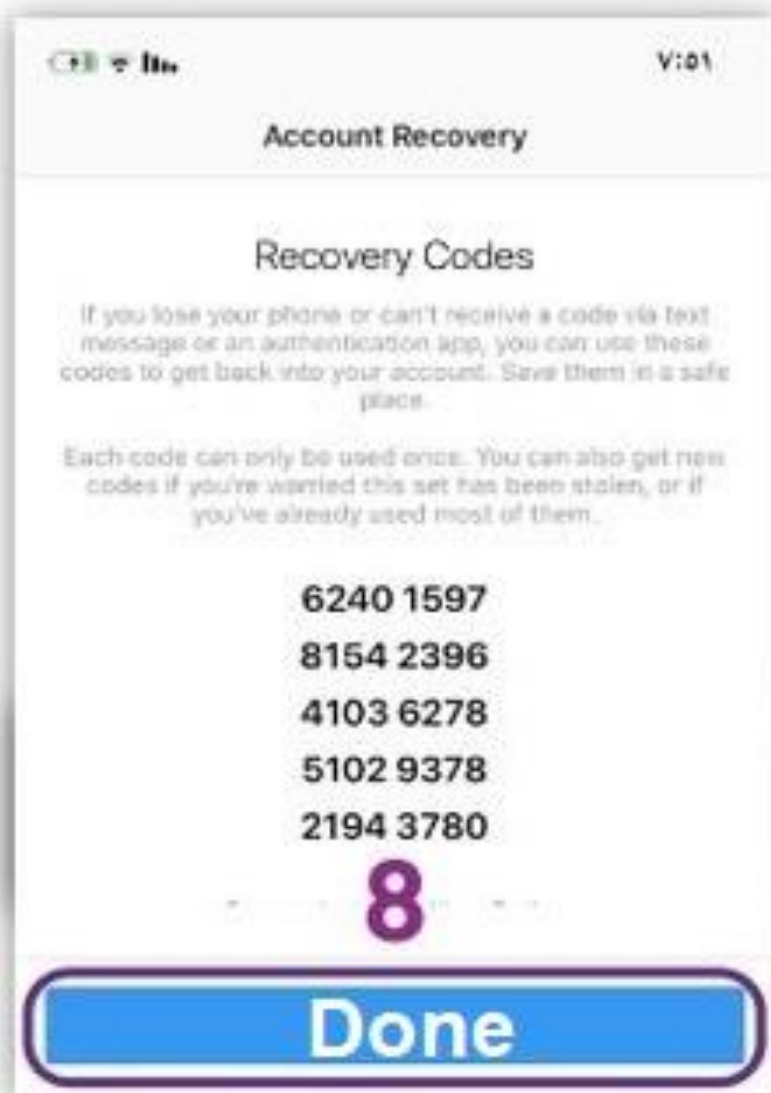
3. التحقق بخطوتين



6. ضع الرقم الذي
سيصلك



5. تفعيل التحقق بالرسائل
النصية



8. تم



7. التالي



قسم تكنولوجيا المعلومات شعبة الامن السيبراني



Security Policies



ماهي السياسات وما الغاية من تطبيق السياسات
في مجال أمن المعلومات والامن السيبراني

ماهية سياسات فى أمن المعلومات :- هي عبارة عن مجموعة من السياسات التي تصدرها الدولة او المؤسسة او المنظمة لضمان امتثال جميع مستخدمي تكنولوجيا المعلومات داخل نطاق تلك (الدولة او المؤسسة او المنظمة الحكومية والغير حكومية) للقواعد والإرشادات المتعلقة بأمان المعلومات المخزنة (ورقيا او رقميا) في أي نقطة في الشبكة أو داخل حدود سلطة تلك المنظمة.

الهدف من هذه السياسات :- هو وضع الإطار العام للحد الأدنى للمعايير وأفضل الممارسات الخاصة بأمن المعلومات الرقمية أو البيانات بكليات التقنية العليا، إضافة إلى وضع الأسس لخطة العمل الواجب تنفيذها لحماية الأصول المعلوماتية الخاصة بكليات التقنية العليا من التهديدات، سواء كانت داخلية أو خارجية، متعمدة أو عرضية، وذلك بما

يضمن

تمهيد

استنادا الى الاوامر الديوانية (5س) لسنة 2011 و (504) لسنة 2015 ولاحقا بقرار مجلس الامن الوطني المتخذ في جلسته (23-2015) في 6/12/2015 المتضمن المصادقة على السياسة العامة لأمن المعلومات وحماية الاتصالات واستنادا الى لصلاحيات المخولة لفريق الاستجابة الوطني للأحداث السيبرانية بموجب الأمر الديواني (66) لسنة 2017 ولجنة (تنسيق وإدارة النشاط الحكومي باتجاه انشاء الحوكمة الالكترونية) المشكلة بالامر الديواني (45) لسنة 2016 ،تم اعداد وثيقة السياسات والمعايير الامن المعلومات ومشاركة البيانات ووضع خطة تنفيذ لها.

الالتزامات

• تطبق هذه السياسة على جميع مستخدمي موارد وممتلكات الدولة العراقية المستخدمة في أنظمة المعلومات والاتصالات في كافة السلطات والمؤسسات التابعة لها إضافة الى كافة شركات القطاعين العام والخاص والتي تتعامل مع المعلومات الحكومية ومعلومات المواطنين.

1

• يتعين على المؤسسات ان تثبت التزاماتها بنظام أمن المعلومات من خلال ضمان تخصيص الموارد الملائمة بما في ذلك الموازنة والموظفين لإدارة برنامج أمن المعلومات حيث قد تؤدي قلة التمويل الى الحيلولة دون تطبيق الضوابط الأمنية المناسبة او تنفيذ برنامج أمن المعلومات. وفيما يتعلق بالموارد، سوف يخفق أفضل الانظمة في حالة عدم توافر الموارد الكافية لإدارة عملياته

2

• يجب على الوزارة تقييم أداء أمن المعلومات وفعالية نظام إدارة أمن المعلومات إضافة الى التدقيق الداخلي وعلى فترات مخططة، لتقديم معلومات بشأن ما إذا كان نظام إدارة أمن المعلومات يتوافق مع متطلبات الوزارة إضافة الى آلية تنفيذه وصيانتته على نحو فعال.

3

الأهداف

1 تهدف هذه الوثيقة إلى وضع أطر العمل، ووضع السياسات والمعايير وتحديد الأدوار والمسؤوليات، وبيان الالتزام الأدنى المطلوب من جميع العاملين داخل الوزارة لضمان أمن وحماية المعلومات.

2 رسم سياسة وطنية موحدة لأمن ونشر ومشاركة المعلومات وحماية الاتصالات، لغرض اعتمادها من قبل المؤسسات الحكومية وغير الحكومية والالتزام بالمعايير والضوابط ووضع التعليمات والإجراءات المناسبة لضمان حماية الأمن الوطني ومصصلحة الدولة العليا.

3 وضع تعليمات وإجراءات حكومية لحماية البنى التحتية للاتصالات وشبكات الحكومة العراقية وأنظمة الحاسبات من التهديدات والاستخدام غير المؤمن بما يوفر شبكة اتصالات مؤمنة او محمية.

4 وضع الآليات التي من شأنها المساعدة في تحديد ووقاية إساءة العمل على شبكات وأنظمة المعلومات التابعة للحكومة العراقية.

وثيقة السياسات والمعايير لأمن المعلومات ومشاركة البيانات

36	سياسة مشاركة البيانات الحكومية	1
47	سياسة الاستخدام المقبول	2
55	سياسة ادارة التغيير	3
57	سياسة امن العاملين داخل المؤسسة	4
59	سياسة السلوك الخاص بأمن المعلومات	5
65	سياسة التدقيق الخاص بأمن المعلومات	6
70	سياسة امن السجلات	7
71	سياسة تصنيف المعلومات	8
82	سياسة اصول نظام المعلومات	9
83	سياسة حماية البيئة المادية	10
90	سياسة استخدام جهاز الحاسوب	11
93	سياسة استخدام الاجهزة المحمولة	12
95	سياسة تأمين المكتب (المكتب النظيف)	13
97	سياسة التعاقد الخارجي	14
101	سياسة النسخ الاحتياطية	15
103	سياسة امن الشبكات	16
107	سياسة التعامل مع الاجهزة الالكترونية منتهية الخدمة	17
109	سياسة مكافحة الفيروسات والبرامج الخبيثة	18
112	سياسة الوصول عن بعد	19
114	سياسة كلمة المرور	20
117	سياسة الشبكات اللاسلكية	21
118	سياسة امن الخوادم (SERVERS)	22
120	سياسة البريد الالكتروني	23
122	سياسة التشفير	24
125	سياسة ادارة الحوادث	25
128	سياسة استمرارية العمل	26
129	سياسة تطوير وصيانة نظام المعلومات	27

سياسة مشاركة البيانات الحكومية

الهدف

تحدد هذه السياسة المبادئ والمعايير الواجب الالتزام بها من قبل الجهات الحكومية وتنطبق على جميع أنواع البيانات القابلة للمشاركة، وتحدد السلوكيات والممارسات المتوقعة من قبل موظفيها، وتعزز التزام المؤسسة بمشاركة البيانات من خلال تطبيق أفضل الممارسات. تهدف هذه السياسة إلى دعم مشاركة البيانات بين الجهات الحكومية لتسهيل تقديم الخدمات للمواطنين والمستفيدين بشكل أفضل، وتسهيل تنفيذ خطة التحول

للحكومة الإلكترونية، وتشمل ما يلي:

1 . المبادئ العامة لمشاركة البيانات.

2 . الأسس القانونية لمشاركة البيانات.

3 . الأغراض المشتركة لحفظ ومشاركة البيانات.

4 . المسؤوليات المترتبة على الجهات الحكومية المعنية بمشاركة البيانات.

5 . معايير البرامج والتطبيقات.

تحديد إجراءات خاصة لمشاركة البيانات بين الجهات الحكومية (البيانات الممكن مشاركتها، كيفية مشاركتها وحفظها ولمن يمكن إعطائها، الغرض المحدد لاستخدامها) حيث ستتكفل الجهات المانحة للبيانات مسؤولية وضع تلك الإجراءات بالتنسيق مع الجهات المختصة.

المجال

تنطبق هذه السياسة على جميع الجهات الحكومية التي تتبادل البيانات والمعلومات فيما بينها إضافة إلى الجهات الحكومية التي تتعامل مع (المواطنين، القطاع خاص، القطاع مختلط) والتي توجب عليها توفير خدمات إلكترونية أساسية.

سياسة الاستخدام المقبول

المجال

توضح هذه السياسة الممارسات الفضلى للاستعمالات المقبولة والممنوعة التي يجب على جميع مستخدمي نظام المعلومات داخل المؤسسة أخذها بعين الاعتبار عند التعامل معها.

الهدف

توفير بيئة نظم معلومات آمنة وموثوقة ومريحة للاستخدام بحيث يتحمل جميع العاملين داخل المؤسسة المسؤولية في الاستعمال الصحيح للمعلومات ومواردها والبنية التحتية لنظام المعلومات داخل المؤسسة.

سياسة إدارة التغيير



الهدف

ضمان امن وحماية نظام المعلومات عند القيام بأي تغيير قد يؤثر عليها.

المجال

تغطي هذه السياسة أي تغيير قد يؤثر على إعدادات أو تنصيب أو إزالة أو إتلاف أي من نظام المعلومات المملوكة للمؤسسة، مثل الملفات والبرمجيات والأجهزة والمعدات والشبكات ووسائط التخزين والوثائق، كما تغطي كذلك الأشخاص المسؤولين عن تقديم طلبات التغيير (مثل مدير النظام) ومراجعتها والموافقة عليها.

سياسة أمن العاملين داخل المؤسسة

الهدف

منع وتقليل المخاطر الناتجة عن الخطأ البشري وسوء الاستعمال – مثل الإتلاف والتدمير – عند التعامل مع نظام تكنولوجيا المعلومات.

المجال

تغطي هذه السياسة جميع العاملين داخل المؤسسة او المراد تعيينهم او التعاقد معهم.

سياسة السلوك الخاص بأمن المعلومات

الهدف

تعزير السلامة العامة وإيجاد بيئة عمل مهنية أمنة يتعامل فيها العاملون داخل المؤسسة بمستوى عال من الأخلاق والمسؤولية أثناء تعاملهم مع المعلومات والبيانات وجميع مكونات نظم المعلومات وممارسة الطرق الصحيحة لحمايتها.

المجال

تغطي هذه السياسة جميع العاملين داخل المؤسسة.

سياسة التدقيق الخاص بأمن المعلومات

الهدف

التأكد من سلامة وامن وتوافر المعلومات ومواردها، والكشف عن إمكانية وقوع الحوادث الأمنية، وضمان وجود وفاعلية الإجراءات المتبعة داخل المؤسسة وتوافقها مع سياسات أمن وحماية المعلومات، وتقييم المخاطر الإجمالية الواقعة على الأنظمة المعمول بها داخل المؤسسة، ودعم الإجراءات التي تساعد على تحديد نقاط الضعف فيها

المجال

تغطي هذه السياسة جميع أنظمة تكنولوجيا المعلومات والسجلات وموارد نظام المعلومات المملوكة للمؤسسة (مثل أنظمة الحاسبات والاتصالات) ، والسياسات والإجراءات والتعليمات والسلطات والمسؤوليات وأية أعمال ترتبط بأية وثائق أخرى داخلية أو خارجية، والمعمول بها في هذه المؤسسة .

سياسة أمن السجلات



الهدف

وضع الضوابط لتحقيق أفضل الممارسات لحماية إنشاء السجلات الحكومية وحفظها والتخلص منها ونقلها وإصدارها والوصول إليها.

المجال

تطبق هذه السياسة على جميع الوثائق التي تعود ملكيتها الى المؤسسة وكل الوثائق التي ترد الى المؤسسة من الجهات الأخرى.

سياسة تصنيف المعلومات

الهدف

حماية كافة أنواع المعلومات وبأى صورة كانت وعلى جميع الوسائط، من الوصول إليها أو استعمالها أو تغييرها أو الإفصاح عنها أو إتلافها بشكل غير مرخص، في جميع مراحل دورة حياتها، بطريقة تتناسب وحساسيتها وأهميتها

المجال

تغطي هذه السياسة جميع المعلومات التابعة للمؤسسة، سواء كانت إلكترونية أو غير إلكترونية.

سياسة سجل أصول نظام المعلومات

الهدف

تحديد وتسجيل جميع أصول نظام المعلومات والاتصالات وحمايتها.

المجال

جميع أصول نظام المعلومات والاتصالات بما في ذلك الأجهزة والبرامج والخدمات وأصول المعلومات وغيرها.

سياسة حماية البيئة المادية

الهدف

ضمان أمن وسلامة نظام المعلومات المادية في المؤسسة وتقليل أثر المخاطر والتهديدات البشرية والبيئية وغيرها من المخاطر التي تؤثر على سلامتها وسريتها.

المجال

تغطي هذه السياسة موارد نظام المعلومات المادية المملوكة للمؤسسة إضافة الى الأمن المادي للعاملين داخل المؤسسة.

سياسة استخدام جهاز الحاسوب

الهدف

ضمان أمن وحماية الحاسوب المكتبي والمعلومات التي يتم التعامل معها أو تخزينها أو معالجتها من خلاله، وتوضيح الطريقة الصحيحة للتعامل معه بشكل آمن.

المجال

تغطي هذه السياسة جميع أجهزة الحاسوب المكتبية داخل المؤسسة، وجميع المستخدمين الذين يسمح لهم باستعمالها أو الوصول إليها.

سياسة استخدام جهاز الحاسوب اللوحي

الهدف

ضمان أمن وحماية المعلومات التي يتم التعامل معها أو تخزينها أو معالجتها من خلال الأجهزة المحمولة أثناء استعمالها أو إصلاحها أو السفر بها إضافة الى حماية الأجهزة المحمولة بحد ذاتها.

المجال

تغطي هذه السياسة جميع الأجهزة المحمولة المملوكة للمؤسسة، مثل أجهزة الحاسوب المحمولة، وأجهزة الاتصال النقالة، والأجهزة المحمولة الأخرى كما تغطي كافة العاملين داخل المؤسسة الذين يستخدمون هذه الأجهزة.

سياسة تأمين المكتب (المكتب النظيف)

الهدف

الغرض من هذه السياسة هو تحديد الحد الأدنى من المتطلبات للحفاظ على "مكتب نظيف" - حيث تكون المعلومات وحسب تصنيفها المتبع في المؤسسة آمنة وذلك للتقليل من خطر وقوع حادث أمني والحفاظ على الوثائق الحساسة التي تترك على سطح المكتب من السرقة.

المجال

تنطبق هذه السياسة على جميع العاملين داخل المؤسسة.

سياسة التعاقد الخارجي

الهدف

ضمان أمن وحماية المعلومات وأنظمة تكنولوجيا المعلومات وسلامتها وتوافرها وخصوصيتها أثناء الاستعانة بمزود خارجي لتوفير خدمات معينة للمؤسسة.

المجال

تغطي هذه السياسة أي مزود خارجي يتم التعاقد معه لتوفير خدمات معينة للمؤسسة، ويشمل ذلك المستشارين ومحلي النظم والباحثين والمبرمجين، والشركات المقدمة والمزودة والداعمة للخدمات، كما تغطي اعتبارات أمن وحماية المعلومات ومواردها، والإجراءات والعمليات والخدمات والاتصالات التي يتم التعاقد الخارجي من أجلها.

سياسة النسخ الاحتياطي



الهدف

ضمان أمن وحماية المعلومات عن طريق أخذ نسخة احتياطية و تخزينها واسترجاعها عند الحاجة بطريقة آمنة وصحيحة.

المجال

تغطي هذه السياسة جميع المعلومات المشمولة بعملية النسخ الاحتياطي- مثل الوثائق والملفات الإلكترونية وغير الإلكترونية، وقواعد البيانات والبريد الإلكتروني، والبرمجيات والأجهزة ووسائل التخزين المستخدمة في النسخ الاحتياطي.

سياسة أمن الشبكات

الهدف

الهدف الرئيسي هو الوصول إلى شبكة مستقرة وأمنة قادرة على تلبية متطلبات العمل الخاص بالمؤسسة وذلك من خلال توضيح آلية التعامل مع عناصر شبكة المعلومات وتحديد الأمور المطلوب توافرها في هذه العناصر لضمان أمن وحماية الأنظمة المرتبطة بالشبكة.

المجال

تغطي هذه السياسة جميع العناصر والمكونات المتعلقة عملها بشبكة نظام المعلومات التابعة للمؤسسة بنوعها السلكية واللاسلكية، إضافة إلى كل البنية التحتية للاتصالات.

سياسة التعامل مع الأجهزة الالكترونية منتهية الخدمة

الهدف

تحديد الضوابط للتعامل مع الأجهزة الالكترونية بعد انتهاء خدمتها والية التعامل معها.

المجال

تغطي هذه السياسة جميع الأجهزة الالكترونية المرتبطة بالشبكة التابعة للمؤسسة او الأجهزة التي كانت تعمل بصورة منفصلة والتي تؤثر على أمن المعلومات وتناقل البيانات داخل المؤسسة او خارجها.

سياسة مكافحة الفيروسات والبرامج الخبيثة

الهدف

حماية موارد ونظام المعلومات من البرامج الضارة والفيروسات

المجال

تغطي هذه السياسة اليات التعامل والمكافحة من البرامج الخبيثة كالفيروسات والديدان وأحصنة طروادة وبرامج التجسس والرسائل المزعجة وغيرها من البرامج التي يمكن أن تهدد أمن وسلامة وتوافقية وخصوصية المعلومات ومواردها وأنظمة المعلومات المعمول بها في المؤسسة.

سياسة الوصول عن بُعد

الهدف

تحديد قواعد وأليات استخدام تقنية الوصول عن بُعد في الدخول لشبكة المؤسسة وذلك لضمان تقليل الأضرار والمخاطر التي قد تنجم عن الاستخدام الخاطئ والغير مصرح به لهذه التقنية.

المجال

تغطي هذه السياسة جميع العناصر والمكونات والموارد المستخدمة في الوصول عن بُعد لشبكة المؤسسة بنوعها السلوكية واللاسلكية.



سياسة كلمات المرور

الهدف

حماية مكونات نظم المعلومات من الدخول غير المشروع إليها عن طريق وضع معايير واضحة لإنشاء كلمات مرور فعّالة، وحمايتها وتغييرها بشكل دوري.

المجال

تنطبق هذه السياسة على جميع كلمات المرور داخل المؤسسة بما في ذلك على سبيل المثال لا الحصر، الحسابات على مستوى المستخدم، والحسابات على مستوى النظام، وحسابات الموقع الإلكتروني، وحسابات البريد الإلكتروني، وحماية شاشة التوقف، والبريد الصوتي.

سياسة الشبكات اللاسلكية

الهدف

تهدف هذه السياسة الى توفير المتطلبات والضوابط الواجب توافرها لحماية شبكات الاتصالات اللاسلكية.

المجال

تغطي هذه السياسة شبكات الاتصالات اللاسلكية وشبكات الاتصالات عبر الاقمار لصناعية (Vsat) إضافة الى الشبكات التابعة لجهات اخرى والتي ترتبط مع الشبكة الخاصة للمؤسسة لأغراض العمل الرسمي بما يتضمنه ذلك من خوادم وموجهات وجدران نارية وأسلاك وبروتوكولات وغيرها من مكونات الشبكة.

سياسة أمن الخوادم (Servers)

الهدف

تهدف هذه السياسة الى فرض الإجراءات والضوابط لحماية الخوادم والتقليل من خطر الوصول الغير مصرح به لهذه الأجهزة إضافة الى اليات التعامل معها.

المجال

تغطي هذه السياسة جميع الخوادم التي تقدم خدمات معينة الى المؤسسة.

سياسة البريد الإلكتروني

الهدف

تهدف هذه السياسة الى وضع الضوابط والتعليمات لضمان الاستخدام الصحيح للبريد الإلكتروني إضافة الى حمايته

المجال

تغطي هذه السياسة جميع انظمة البريد الإلكتروني المعمول بها في المؤسسة، والمتعاملين مع هذه الأنظمة ويملكون حسابات بريد إلكتروني.

سياسة التشفير

الهدف

حماية المعلومات عن طريق وضع القواعد اللازمة لتطبيق خوارزميات التشفير التي تمت مراجعتها وأثبتت فاعليتها وجدارتها عالميا.

المجال

تغطي هذه السياسة إدارة واستخدام برامج ومعدات ومفاتيح التشفير للمعلومات المراد تشفيرها في المؤسسة .

سياسة إدارة الحوادث



الهدف

وضع الضوابط والاليات الصحيحة للتعامل مع الحوادث المتعلقة بأمن المعلومات.

المجال

توضح هذه السياسة الممارسات الفضلى في التعامل مع حوادث أمن المعلومات لجميع العاملين داخل المؤسسة إضافة الى الحوادث الأمنية المتعلقة بموارد نظام المعلومات داخل المؤسسة.

سياسة استمرارية العمل



الهدف

وضع الضوابط لضمان استمرارية العمل وعدم انقطاع أو فشل أنظمة المعلومات والاتصالات، وضمان استئنافها في الوقت المناسب.

المجال

كل أنظمة المعلومات والاتصالات والخدمات المقدمة من قبل المؤسسة إضافة إلى الخدمات والاعمال المقدمة من خلال التعاقدات الخارجية.

سياسة تطوير وصيانة نظام المعلومات

الهدف

ضمان تحقيق المتطلبات اللازمة لتطوير وصيانة نظام المعلومات والخدمات المقدمة من قبل المؤسسة او الخدمات المقدمة من خلال التعاقدات الخارجية.

المجال

تغطي هذه السياسة جميع التطبيقات وأنظمة المعلومات والبرمجيات، سواء في داخل المؤسسة أو عن طريق التعاقد الخارجي، إضافة الى الاعتبارات الواجب اتخاذها من أجل أمن وحماية هذه الأنظمة وسائر المعلومات المتعلقة بها أثناء دورة حياتها.