

## الوعي الأمني

### فيما يلي عدة نصائح لجعل كلمة المرور أقوى:

- 1 - يجب أن لا تقل كلمة المرور عن ٨ خانات.
- 2 - يجب أن تحتوي كلمة المرور على كل مما يلي: أحرف كبيرة وصغيرة وأرقام ورموز خاصة مثل %&\*
- 3 - تجنب استخدام مفردات موجودة بالقاموس مثل: house , Car
- 4 - تجنب استخدام معلوماتك الشخصية كرمز سري مثل رقم جوالك أو تاريخ ميلادك حيث أنه هنالك الكثير من الأشخاص الذين يعرفون هذه المعلومات عنك.
- 5 - لا تستخدم نفس كلمة المرور لعدة حسابات أو أجهزة.
- 6 - لا تخبر أي شخص عن كلمة مرورك مهما كان السبب، و لا تقم بتخزينها على سطح مكتبك أو في أوراق الملاحظات.
- 7 - احرص على تغيير كلمة مرورك بشكل دوري.

### التحقق من التطبيقات التي يُمكنها الوصول إلى كاميرا وميكروفون هاتف الايفون:

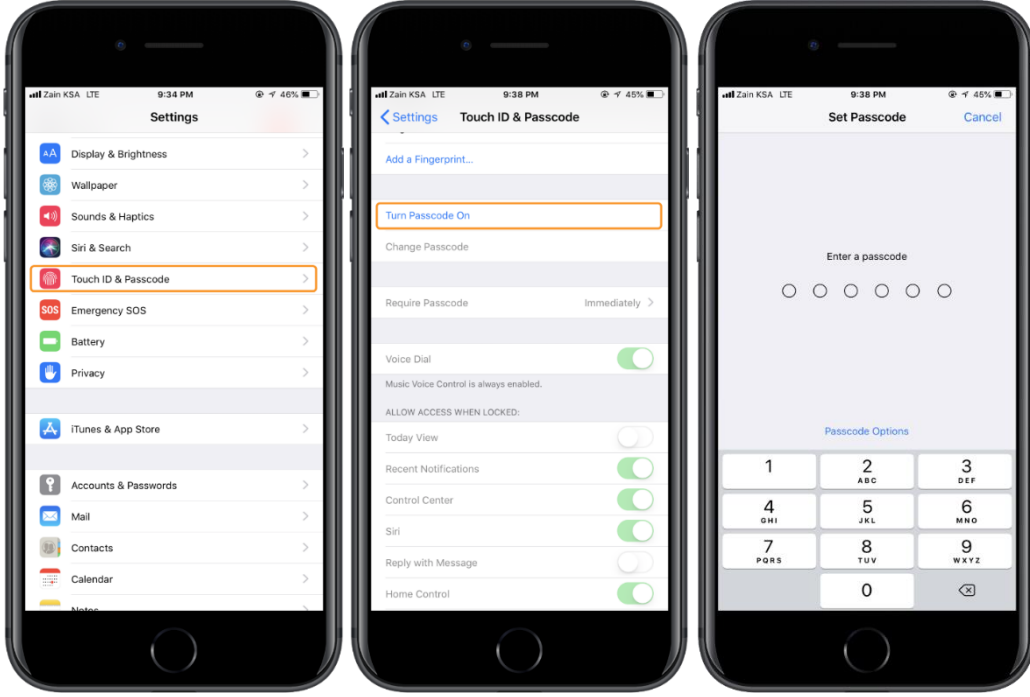
- خطوة 1 :افتح الإعدادات واسحب لأسفل وانقر على الخصوصية Privacy
- خطوة 2 :انقر بعد ذلك على الميكروفون Microphone ، من ثم أوقف أي من التطبيقات التي لا تُريدها الوصول إلى الميكروفون.
- خطوة 3 :ارجع إلى إعدادات الخصوصية، وانقر على الكاميرا Camera ، ومن ثم انقر على مفتاح التبديل بجوار أي تطبيق لإيقاف وصوله للكاميرا.



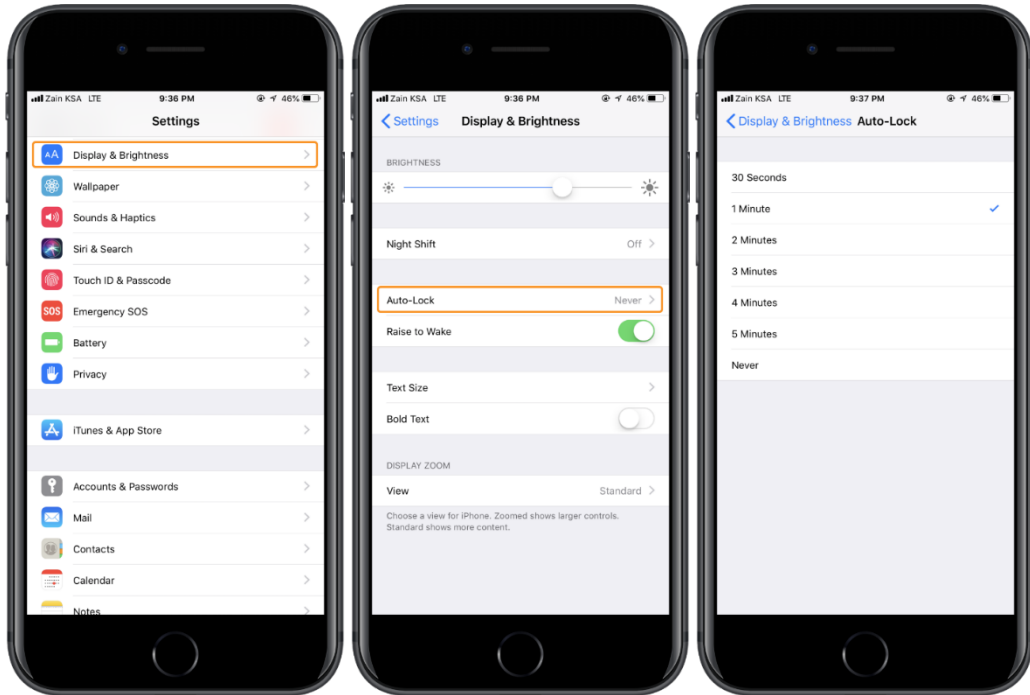
إذا قوّرت منح الوصول لأحد التطبيقات يُمكنك دائمًا تشغيله مرة أخرى من إعدادات الخصوصية.

## نصائح لأمن الجوال والأجهزة اللوحية:

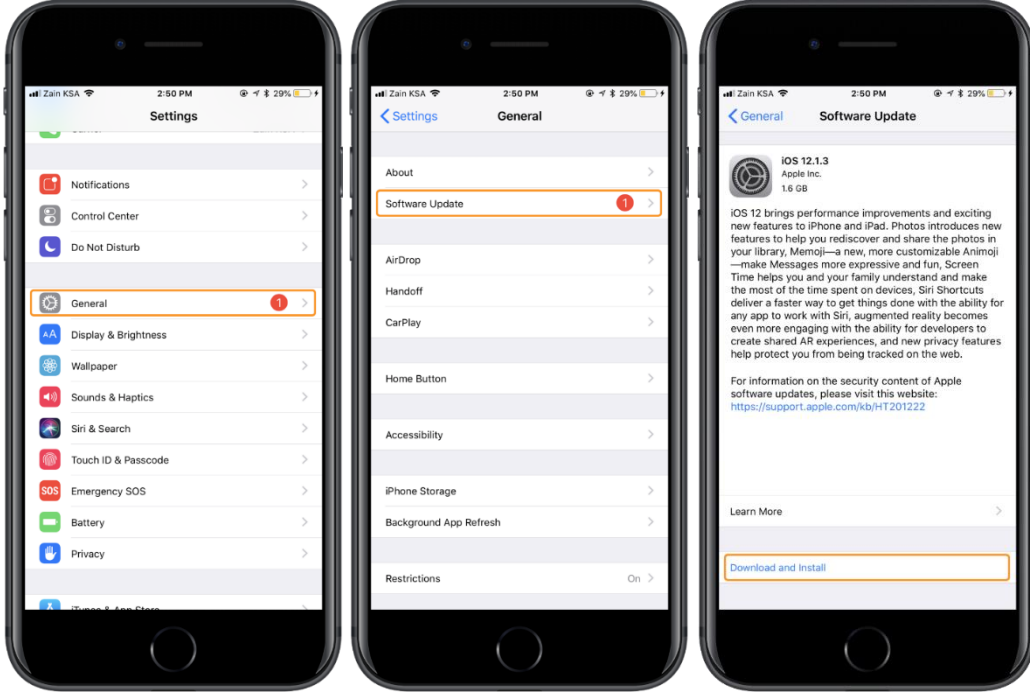
1- قفل الشاشة برقم سري.  
عن طريق الذهاب إلى الإعدادات ← Touch ID ورمز الدخول ← تشغيل رمز الدخول ← إدخال الرمز وتأكيده.



2- تفعيل القفل التلقائي خلال فترة معينة.  
عن طريق الذهاب إلى الإعدادات ← شاشة العرض والإضاءة ← قفل تلقائي ← تحديد الفترة المرادة.



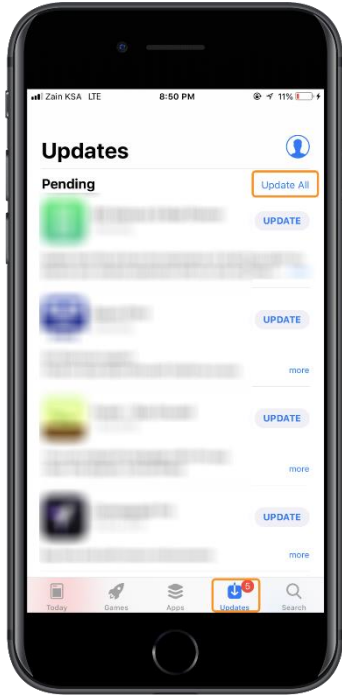
3- الحرص على تحديث نظام التشغيل إلى آخر إصدار.  
عن طريق الذهاب إلى الإعدادات ← عام ← تحديث البرامج ← تنزيل وتثبيت.



4- عدم تثبيت التطبيقات المشبوهة أو تحميل التطبيقات من المصادر غير الموثوقة (أي خارج المتاجر الرسمية).  
5- تحديث التطبيقات إلى آخر إصدار.  
عن طريق الذهاب إلى الإعدادات ← iTunes Store و App Store ← تفعيل تحديثات.



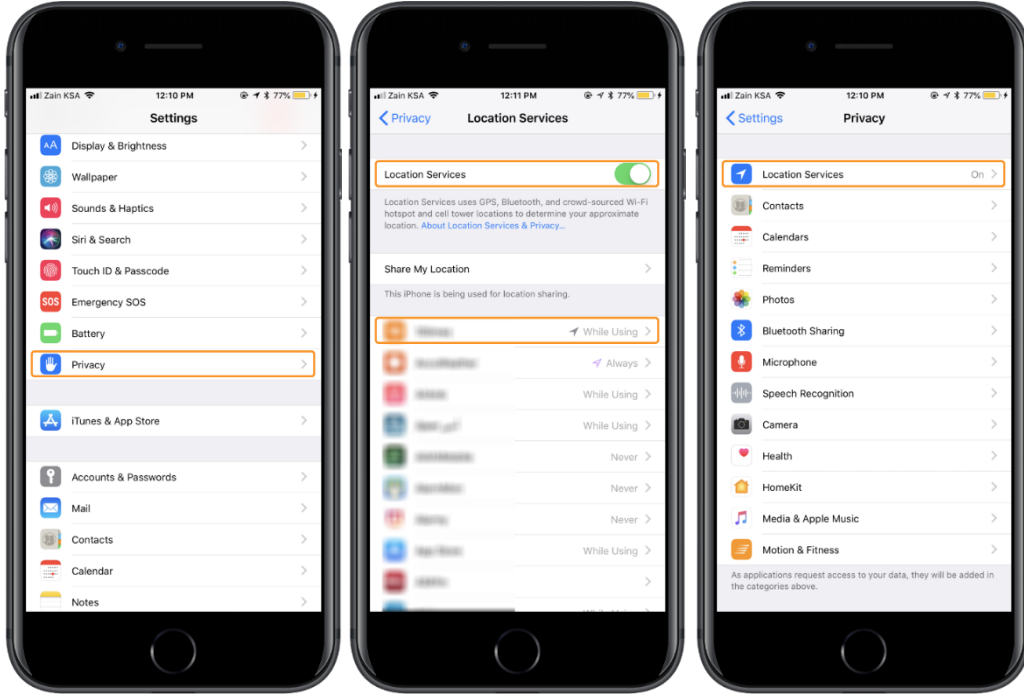
أو عن طريق فتح App Store ← تحديثات ← تحديث الكل.



6- إلغاء أذونات التطبيقات/صلاحيات الوصول غير الضرورية (مثال: سماح الوصول للميكرفون غير ضروري ببرنامج لتعديل الصور).  
عن طريق الذهاب إلى الإعدادات ← اختيار التطبيق المراد التأكد من صلاحيات وصوله ← تعديل الصلاحيات حسب الضرورة.



7- إغلاق مشاركة الموقع في الكاميرا والتطبيقات الأخرى.  
عن طريق الذهاب إلى الإعدادات ← الخصوصية ← خدمات الموقع ← إغلاق خدمات المواقع أو تعديل إعدادات الموقع لكل تطبيق على حدة.



8- تفعيل العثور على الـ iPhone / Find My iPhone.  
عن طريق الذهاب إلى الإعدادات ← الحساب/Apple ID ← iCloud ← تشغيل العثور على الـ iPhone.



9- النسخ الاحتياطي.

عن طريق الذهاب إلى الإعدادات ← الحساب/Apple ID ← iCloud ← نسخة iCloud احتياطية ←  
تشغيل نسخ iCloud احتياطي ← موافق.



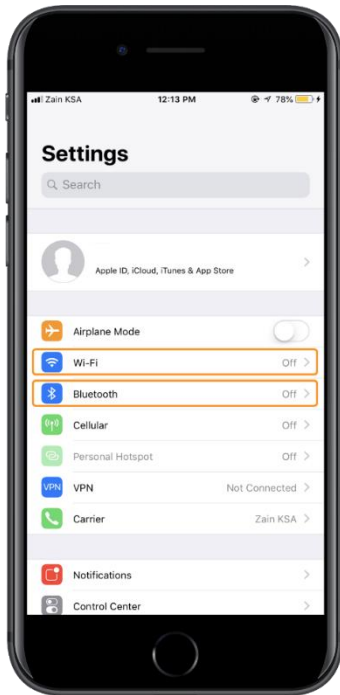
10- الإبلاغ عن رسائل النصب والاحتيال بإعادة إرسالها إلى 330330.

11- عدم الاتصال بشبكات الواي-فاي العامة.

12- تجنب تفعيل الروت وعمل الجيلبريك.

13- تعطيل البلوتوث والواي-فاي بحالة عدم استخدامهما.

عن طريق الذهاب إلى الإعدادات ← إيقاف Wi-Fi, Bluetooth.

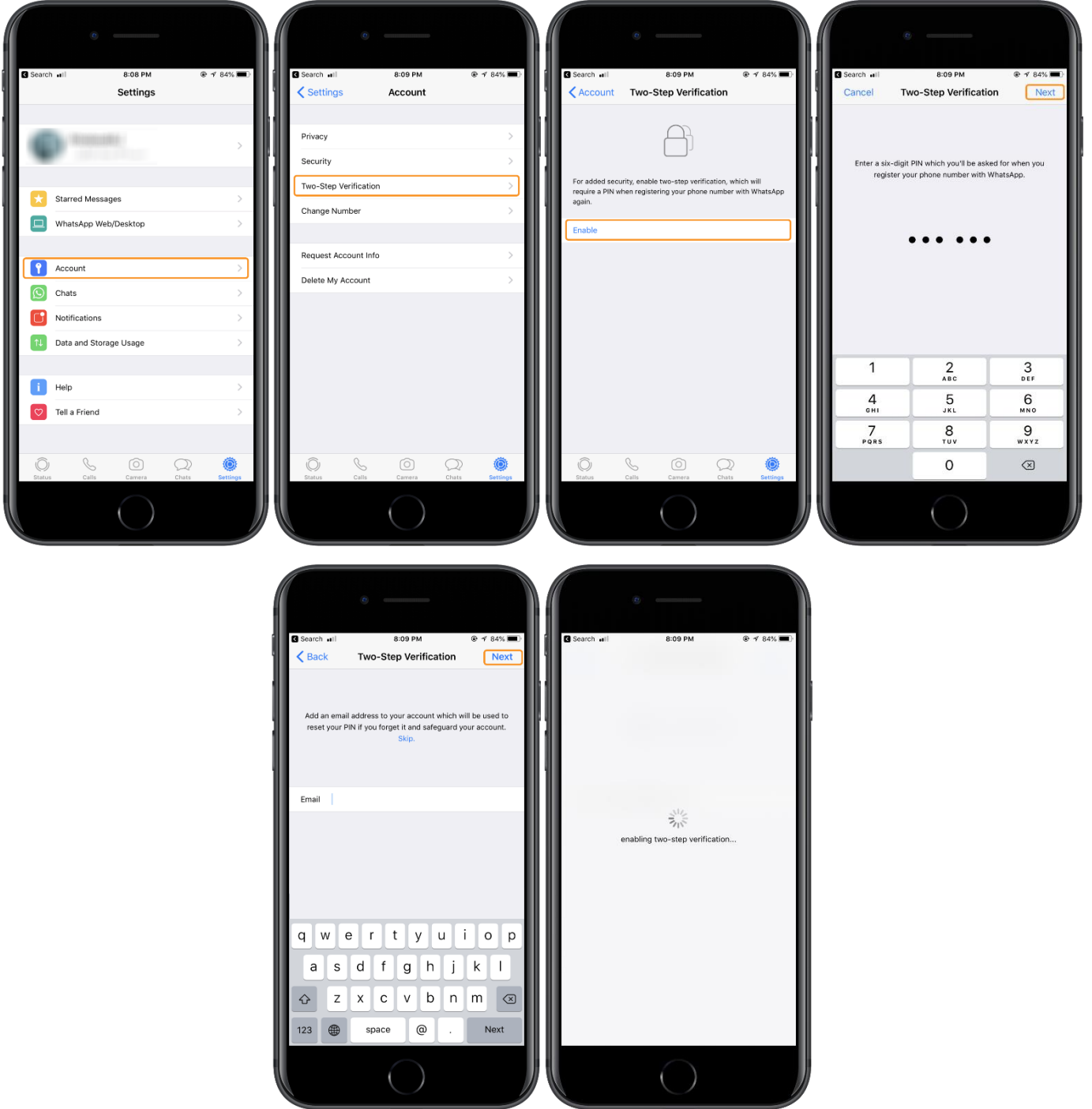


14- تغطية كاميرا الجهاز.

## الأمن في وسائل التواصل الاجتماعي:

- 1- اختيار كلمة مرور قوية وعدم مشاركتها مع الآخرين.
- 2- تمكين التحقق الثنائي (مثال: رقم الجوال والبريد الإلكتروني).  
يمكن البحث بمركات البحث عن كيفية تمكين التحقق الثنائي  
ببعض التطبيقات، حتى غير تطبيقات وسائل التواصل الاجتماعي مثل تطبيقات البنوك، هنا مثال على  
تمكينها بتطبيق واتساب:

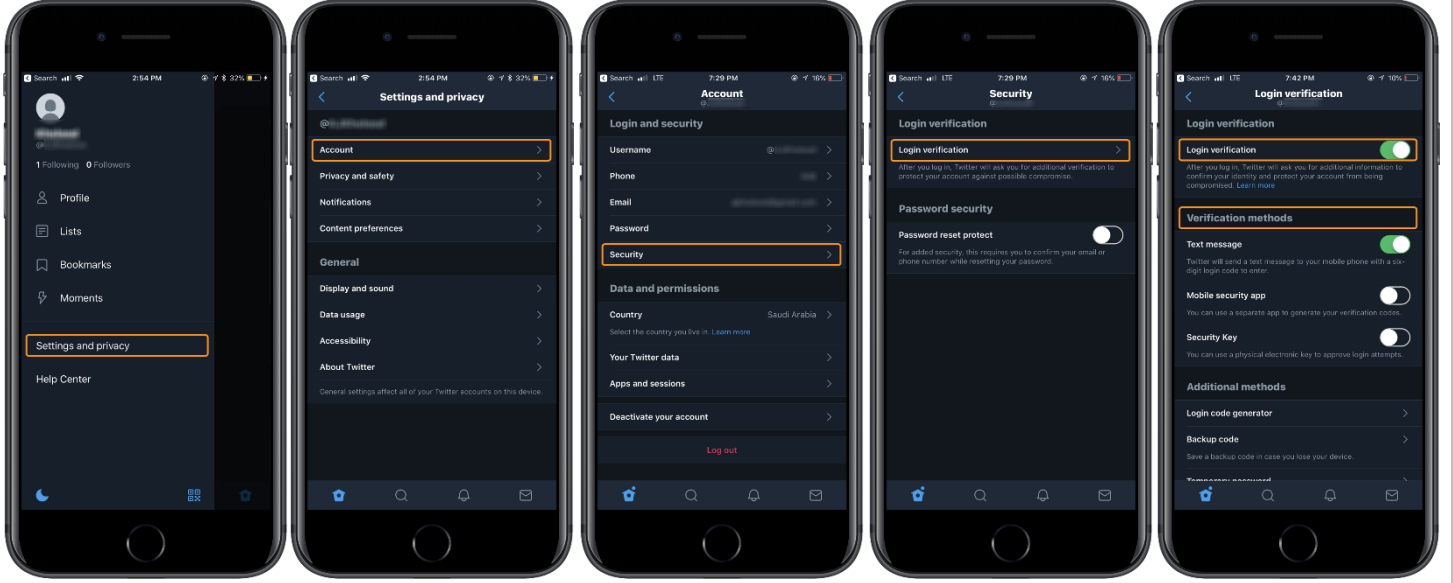
عن طريق فتح تطبيق واتساب ← الإعدادات ← الحساب ← التحقق بخطوتين ← تمكين ← إدخال رقم  
مرور وتأكيده ← اختيارية إدخال البريد الإلكتروني وتأكيده ← التالي ← تم.





كمثال آخر، يمكن تفعيل خاصية مشابهة بتطبيق تويتر:

عن طريق فتح تطبيق تويتر ← الإعدادات والخصوصية ← الحساب ← الأمان ← توثيق تسجيل الدخول  
← تفعيل توثيق تسجيل الدخول واختيار أساليب التوثيق المناسبة.



- 3- الحذر من نشر المعلومات الشخصية الحساسة على وسائل التواصل الاجتماعي.
- 4- الحذر من انتهاك قوانين الجرائم المعلوماتية (نشر صور ملتقطة لأشخاص بغير إذنهم، الابتزاز الإلكتروني، الإرهاب والمواضيع السياسية، القذف، انتحال الهوية،...).
- 5- الحذر من الضغط على أي رابط مجهول.
- 6- استخدام التطبيقات الأصلية فقط وعدم استخدام التطبيقات المعدلة (مثل: تطبيق بلس).
- 7- التبليغ عند التعرض لأي تهديد أو عند مشاهدة أي محتوى ينتهك الشروط (التبليغ لإدارة التطبيق نفسه / كلنا أمن).
- 8- الانتباه إلى الإعدادات الأمنية بكل تطبيق.

## قسم أمن المعلومات

### عمادة الاتصالات و تقنية المعلومات