
NUB
NAHDA UNIVERSTY IN BENI SUEF
جامعـــــة النهضـــة – بنى ســـــويف

الاجندة

- ✓ التعريف بنظام التحول الرقمي وتطوير جامعة لا ورقية
- ✓ الهوية الرقمية
- ✓ أهمية التوثيق الرقمي
- ✓ مميزات وسلبيات الحسابات الالكترونية
- ✓ تعريف الاختراق وأنواع المخترقين
- ✓ اهم أسباب الاختراق
- ✓ هل يمكن معرفة المخترق من قبل المحققين؟؟ وكيف تثبت حقك ؟
- ✓ المخاطر على العمل التجاري اثر الهجمات الالكترونية والاختراقات .
- ✓ امن المعلومات واهميته واعتباره امن قومي
- ✓ التعريف بطرق حماية الأنظمة الالكترونية من الاختراق
- ✓ الأمور الواجب اتباعها في حالة التعرض للاختراق
- ✓ نصائح عامة حول حماية الحسابات الشخصية ومنصات التواصل الاجتماعي
- ✓ كيف تعرف انك مخترق؟؟
- ✓ إجراءات المحافظة على أمن المعلومات للمؤسسات
- ✓ شرح عملي

التحول الرقمي

تعريف التحول الرقمي

بناء مصر الرقمية والوصول إلى مجتمع مصري يتعامل رقميًا في كافة مناحي الحياة. وتعزيز تنمية البنية التحتية لتكنولوجيا المعلومات والاتصالات وتحسين الخدمات الرقمية في الجهات الحكومية، وذلك لتحسين أداء الوزارات والهيئات الحكومية الأخرى، ورفع جودة الخدمات وكفاءتها من خلال تحسين بيئة العمل، وتوفير الدعم لعملية صناعة القرار وإيجاد حلول للقضايا التي تهم المجتمع.

التحول الرقمي

هل الامر اجباري ام اختياري ؟

في غضون سنوات قليلة جدا سوف يصبح الامر اجباريا في العمليات التالية محليا قبل دوليا

- التعاملات المالية
- تجديد رخصة القيادة
- البحث عن وظيفة
- الحجز في تذاكر الطيران والقطارات والرحلات البعيدة
- دفع فواتير الماء والكهرباء والغاز
- الشراء عبر الانترنت او من خلال المتاجر
- الفاتورة الالكترونية
- التعليم والبحث العلمي

Digital Identity

الهوية الرقمية

هو حسابك الالكتروني المميز لك على الانترنت الذي لا يتشابه مع شخص اخر ويمكن تشبيه على انه بصمتك الكترونية التي تحدد هويتك الحقيقة مثل بصمة الحضور والانصراف داخل الجامعة.

من خلاله تستطيع ان تتواصل مع الاشخاص الموجودين في داخل او خارج العمل.

واستخدامه في التطبيقات الالكترونية والبرامج المختلفة ضمن خطة التحول الرقمي

ويعتبر البريد الالكتروني هو بمثابة تلك البصمة لتتمكن من استخدام تلك الخدمات

البريد الإلكتروني
E-Mail

هو اولي خطوات التحول الرقمي الذي لابد من توافره لبدء عملية التحول الرقمي

ويتم تعريف البريد الإلكتروني على انه رسالة تحتوي على نصوص، أو ملفات، أو صور، أو مرفقات يتم تبادلها عبر شبكة المعلومات من جهة معينة إلى شخص واحد أو مجموعة أشخاص

إيجابيات التحول الرقمي

إيجابيات التحول الرقمي

السرعة

سرعة أداء الإجراءات الرقمية تفوق الإجراءات بالطرق التقليدية، وبالتالي سوف تكون هذه الإجراءات سهلة وسريعة على المستفيدين

إيجابيات التحول الرقمي

أكثر سرية

نظرا لانتقال المعاملات الالكترونية بدون شخص وسيط مثل التعاملات العادية مما يجعلها أكثر سرية

إيجابيات التحول الرقمي

التخزين على المدى الطويل

يُمكن أرشفة مليارات المعاملات لفتراتٍ طويلة من الزمن وبكل سهولة عكس الاحتفاظ بالأوراق

إيجابيات التحول الرقمي

معدوم التكلفة

تعتبر الخدمات الالكترونية من الخدمات المجانية التي يتم تقديمها للأشخاص بصرف النظر عن تكلفة الاتصال بالإنترنت وتكلفة الخوادم ، حيث يستطيع الإنسان اجراء العديد من المعاملات والأنشطة من أي مكان في جميع أنحاء العالم، والى أي بلد

إيجابيات التحول الرقمي

الانتشار

سرعة الانتشار والتوسع للشركات والمؤسسات ووصولهم إلى أعداد كبيرة من الجمهور بالإضافة الي تنظيم وتحسين الكفاءات التشغيلية وتسهيل كيفية مراقبة المسؤولين لسير العمل . لفتح مجال للإبداع في كيفية تقديم الخدمات التي يتم تقديمها للعملاء

إيجابيات التحول الرقمي

تحليل البيانات

إمكانية تتبع ومراقبة وتحليل المقاييس والبيانات التي سوف تحصل عليها وسوف يمكّنك من استخدام هذه البيانات في تحسين وتطوير جودة العمل للحصول على نتائج أفضل.

إيجابيات التحول الرقمي

صديقةٌ للبيئة

المعاملات الإلكترونية لا تتطلبُ الورق وبالتالي الحفاظ على الموارد الورقية وعدم الحاجة الي مصاريف اهلاك.

إيجابيات التحول الرقمي

سرعة البحث

يمكنك البحث عن أي معاملة منذ سنوات بخطوات بسيطة جدا واسترجعها في لحظات

سلبيات التحول الرقمي

سلبيات التحول الرقمي

سرقة الهوية الرقمية

حيث يستطيع بعض المخترقين انتحال شخصية من خلال معرفة بعض المعلومات الأساسية المنتشرة بصفحات التواصل الاجتماعي وانتحال شخصية بالعديد من الجهات الحكومية

سلبيات التحول الرقمي

التجسس او الاختراق

حيث يستطيع بعض المخترقين اعتراض المعاملات الإلكتروني، وفتح الرسائل الخاصة بك في حالة عدم تأمين الحساب بالشكل الكافي.

سلبيات التحول الرقمي

الرسائل غير المرغوبة او المزعجة

الذي يُعرف باسم البريد العشوائي حيث تتمثل المشكلة في إمكانية فقدان رسالة بسبب وجود مئات الرسائل غير المرغوب فيها في صندوق الوارد.

وتقدر عدد رسائل المزعجة التي يتم إرسالها يوميًا بحوالي 306 مليار رسالة، وهو ما يبلغ 6 أضعاف رسائل البريد الإلكتروني السليمة التي يتم إرسالها يوميًا والتي تبلغ 52.6 مليار رسالة

سلبيات التحول الرقمي

المرفقات الضارة

يتم ترميز البرامج الضارة بهدف إلحاق الضرر بمستخدميها المستهدفين. مما يؤثر على المستخدمين من الأفراد والشركات على حد سواء، حيث يمكنها سرقة المعلومات وإتلاف البيانات، وسرقة زيارات الموقع والتجسس على نشاط الإنترنت ؛البرمجيات الخبيثة برامج لا تبدو مؤذية كما يمكن أن تكون مصممة خصيصا للتهرب من الدفاعات وتنفيذ مهام محددة. وبمجرد تثبيتها دون قصد، يمكن للبرمجيات الخبيثة تنفيذ العديد من الأنشطة غير المرئية.

أمن المعلومات
Information Security

مفهوم أمن المعلومات:

هو علم قائم بذاته يهتم بتقنيات الحماية للمعلومات التي يتم تداولها عبر شبكة الإنترنت أو حفظها على أجهزة الكمبيوتر والهواتف الذكية والأجهزة الإلكترونية كافةً لتتم حمايتها من كل ما يمكن أن يُهددها من مخاطر مختلفة، ولا شك أنَّ اختلاف تلك المخاطر المتعددة وتطورها المستمر يتطلَّب العمل المستمر على تطوير ذلك العلم، ليتمكن من تفادي ومواجهة كل ما قد يُستَجَد من أساليب المبتكرة في خرق الحماية ومقدرة على الوصول إلى المعلومات غير المُصرحة لهم بها .

مكونات أمن المعلومات

أمان المعلومات

الحرص على المحافظة على البيانات كاملة بصورتها الأصلية، دون السماح لأيِّ شخص بالعبث بها بأي طريقة كانت سواء بالحذف أو بالتعديل عليها، كان هذا بقصد أو دون قصد. ومنع الاشخاص من القيام بعمل إي اجراء دون اذن مالكها.

التوافر

الحرص على الوصول للبيانات بسهولة وسرعة عند حاجة المستخدم لها، وعدم السماح لأي فرد أو جهة بقطع هذه الخدمة بشكل مُفاجئ.

السرية

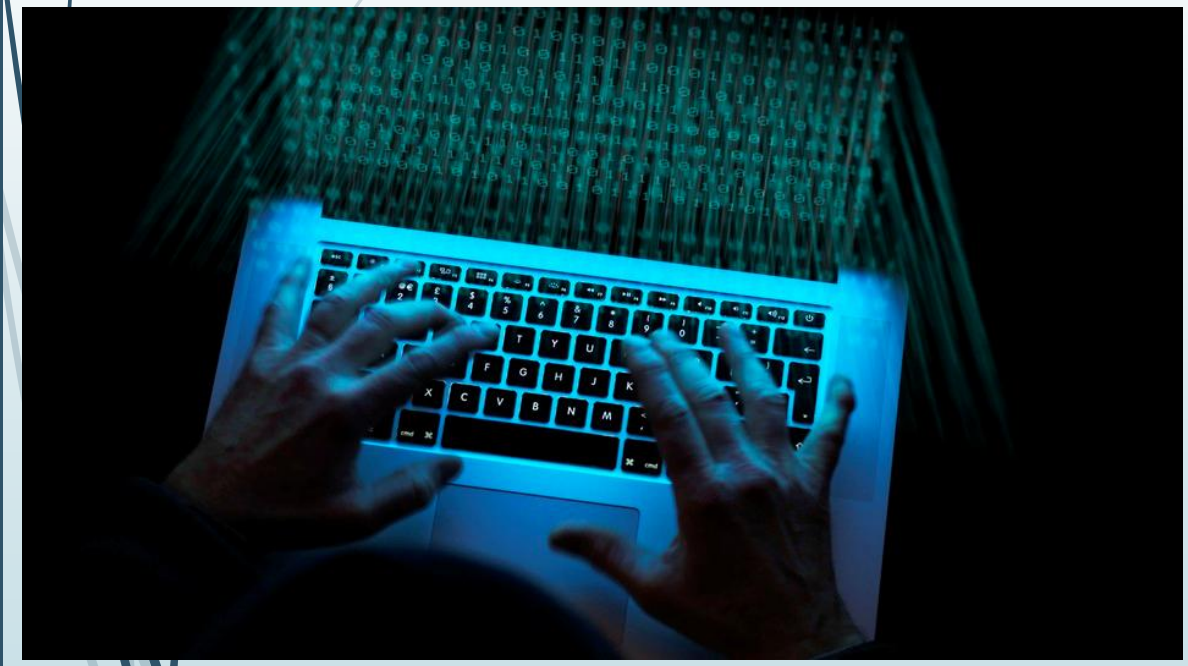
عدم الإفصاح عن أيِّ معلومات لأيِّ شخص من الأشخاص غير المُصرَّح لهم بذلك، حيث يتم منع أي شخص من اختراق الجهاز الخاص بشخص آخر وإمكانية وصوله وحصوله على ما يوجد بها من ملفات ومعلومات خاصَّة.

صادقة

تعني الحرص على عدم إطلاع أي طرف ثالث على أي مُحادثة طرفين، شفافية كاملة عن البيانات التي يتم تحليلها

الاختراق

تعريف الاختراق



الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الأخرين عنوه ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية او أجهزة مؤسستاهم او بنفسياتهم عند سحبه ملفات وصور، او مستندات، او رسائل بحثية او وثائق سرية.

الاختراق

هل الاختراق امر حديث مرتبط بالأنترنت

في عام 1903 كان الفيزيائي جون أمبروز يستعد لعرض إحدى العجائب التكنولوجية المستجدة وهي نظام تلغراف لاسلكي بعيد المدى في محاولة لإثبات أن رسائل شفرة مورس يمكن إرسالها لاسلكيا عبر مسافات طويلة، وكان ذلك أمام جمهور غفير في قاعة محاضرات المعهد الملكي بلندن.

وقبل بدء العرض بدأ الجهاز ينقر مكونا رسالة، كانت في البداية كلمة واحدة ثم تحولت إلى قصيدة ساخرة بشكل غير لائق تتهمه "بخداع الجمهور"، فقد تم اختراق العرض وكان المخترق هو المخترع البريطاني نيفيل ماسكيلين الذي قال لصحيفة تايمز إن هدفه كان كشف الثغرات الأمنية من أجل الصالح العام.

أنواع المخترقين او الهاكرز

1. الهاكرز ذو القبعة البيضاء White Hat Hackers

- او ما يسمى ايضا بالهاكرز الأخلاقي Ethical Hackers
- هو شخص يقوم بتوجيه مهاراته من اجل اكتشاف الثغرات ونقاط الضعف في انظمة الشركات لحمايتها.
- ويحمل هذا الشخص شهادات متخصصة لكي يمارس عمله بشكل قانوني .
- ويقوم ايضا بالتوقيع على تعهدات دولية مختلفة (ميثاق شرف) أي ان دوره إيجابي ومفيد.

أنواع المخترقين او الهاكرز

2- الهاكرز ذو القبعة السوداء Black Hat Hackers

- ويسمى هذا الشخص الكراكر
- هم المخترقين الذين يستهدفون المصارف والبنوك والشركات الكبرى للحصول على المال،
- دورهم سلبي وعملهم خطير ويؤدى الى اضرار كبيرة جدا عالميا.
- يتم محاربتهم بشكل دولي وعملهم يشبه عمل العصابات

أنواع المخترقين او الهاكرز

3- الهاكرز ذو القبعة الرمادية Grey Hat Hackers

- يطلق عليهم اصحاب المزاج المتقلب، بمعنى انهم خليط ما بين الهاكرز ذو القبعة البيضاء (المفيدين) والهاكرز ذو القبعة السوداء (المخربين)
- بتوضيح أكثر يقومون احيانا بمساعدة الشركات في اكتشاف نقاط الضعف والثغرات واغلاقها (أي دورهم هنا إيجابي ومفيد) وأحيانا اخرى يقوم باكتشاف هذه الثغرات واستغلالها بشكل سيء وممارسة عملية الابتزاز (دورهم هنا سيء وخطير جدا) .
- وفي الاغلب هم يعانون من امراض نفسية شديدة.

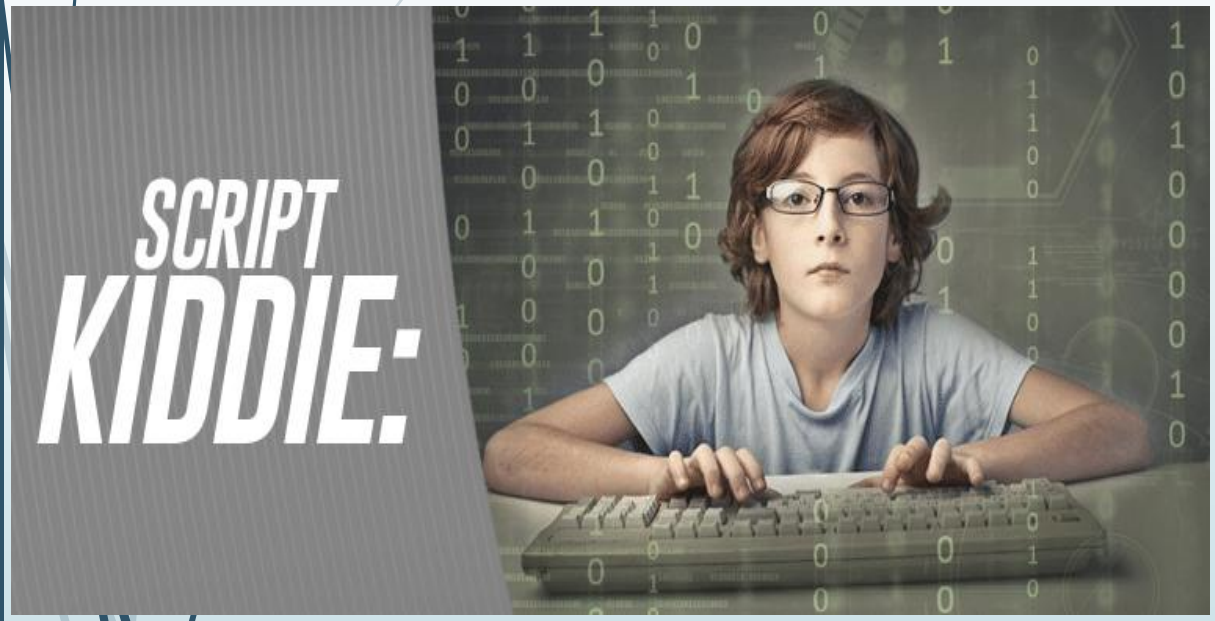
أنواع المخترقين او الهاكرز

4- الهاكرز ذو القبعة الحمراء Red Hat Hackers

- أخطر أنواع الهاكرز او حراس عالم الاختراق مع التركيز على ان معظمهم يعمل في جهات أمنية وحكومية وعسكرية.
- تابعين للدول بشكل رسمي ويعملون تحت مظلتها ورعايتها.
- ونظراً لخطورتهم ومهارتهم المتميزة ودورهم الخطير فهم خبراء ومختصين في علوم الكمبيوتر و يطلق عليهم مصطلح الوحوش البشرية فعليا حيث يقومون باختراق الهاكرز والمختصين الاخرين وأجهزة التحكم والسيطرة وتدمير اجهزة الهدف وايقافه عن العمل نهائيا.
- يقومون بشن هجمات على بعض الدول بدعم امنى وعسكري من دولهم.
- لهم ارقام هوية عالمية للتصنيف الدولي لتخفي ورائها .

أنواع المخترقين او الهاكرز

5- أطفال الهاكرز Script Kiddies



- وهم الأشخاص اللذين يبحثون عن كيفية اختراق الأنظمة الالكترونية ومنصات التواصل الاجتماعي والتجسس علي التطبيقات واستخدام برامج ليست من صنعهم منتشرة علي الانترنت وبالطبع هذه التطبيقات ملوثة وضارة وخطيرة جدا (دورهم سلبي وخطير)
- لديهم هوس بتعلم الاختراق .

أشهر مجموعات المخترقين

Anonymous

- هم مجموعة من الهاكرز موجودين في كل دول العالم تقريبا
- ويقومون بتنفيذ هجمات إلكترونية اما بهدف سيأسى او إنساني ويصنفون على انهم Hacktivismومعناها بالعربية الجهاد او النضال الإلكتروني ويقومون بذلك ضد نظام دول معينة بهدف تسريب معلومات سرية او حساسة عن هذه الدول لفضحها وتسريب معلومات ووثائق عنه او فضح مؤسسة مالية او بنكية دون التأثير على حسابات الاشخاص نفسها (أي دورهم هنا إيجابي وليس سلبى في اغلب الاحيان).

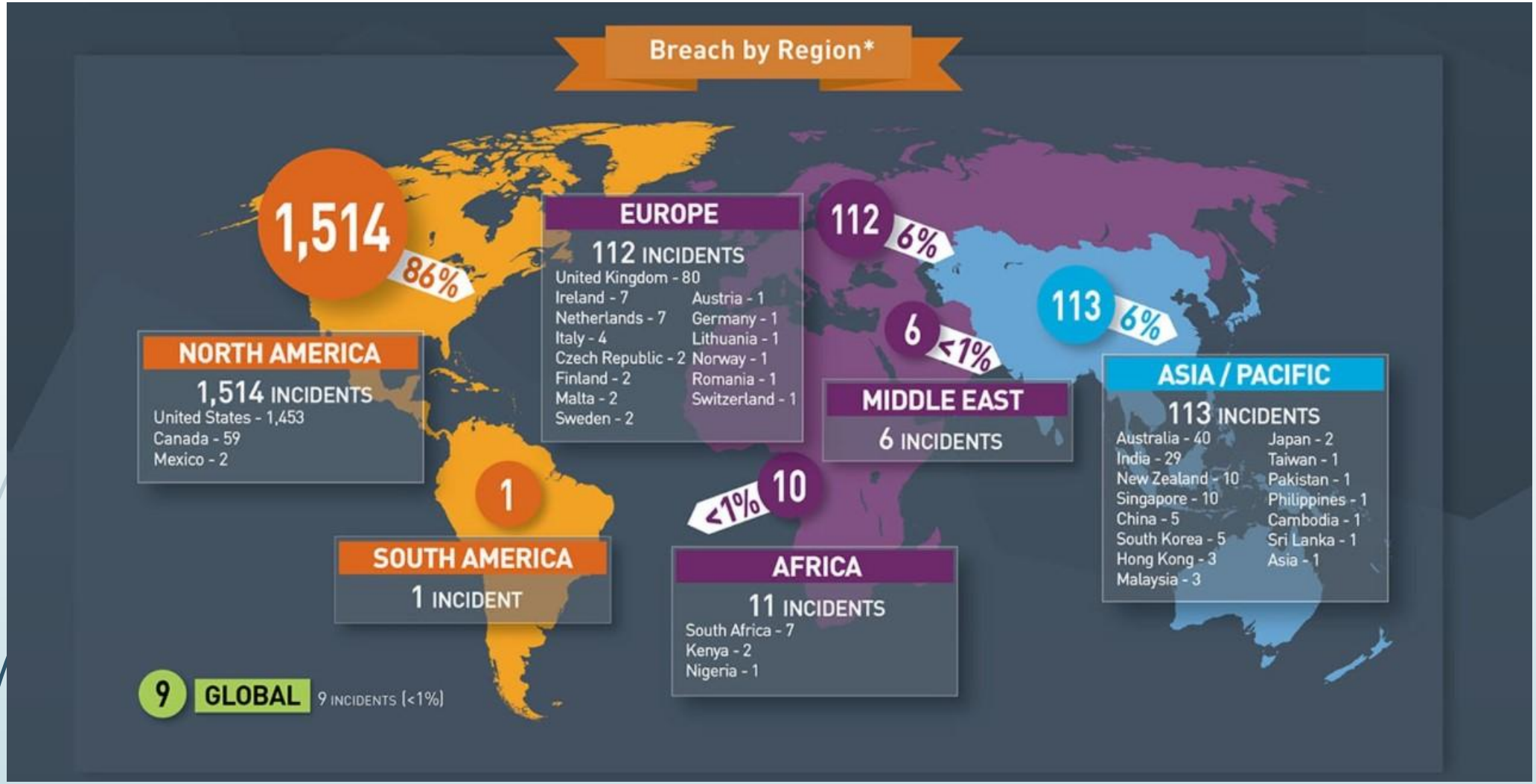
ترتيب الخطورة

المستخدم العادي معرض للهجمات المخترقين علي النحو التالي

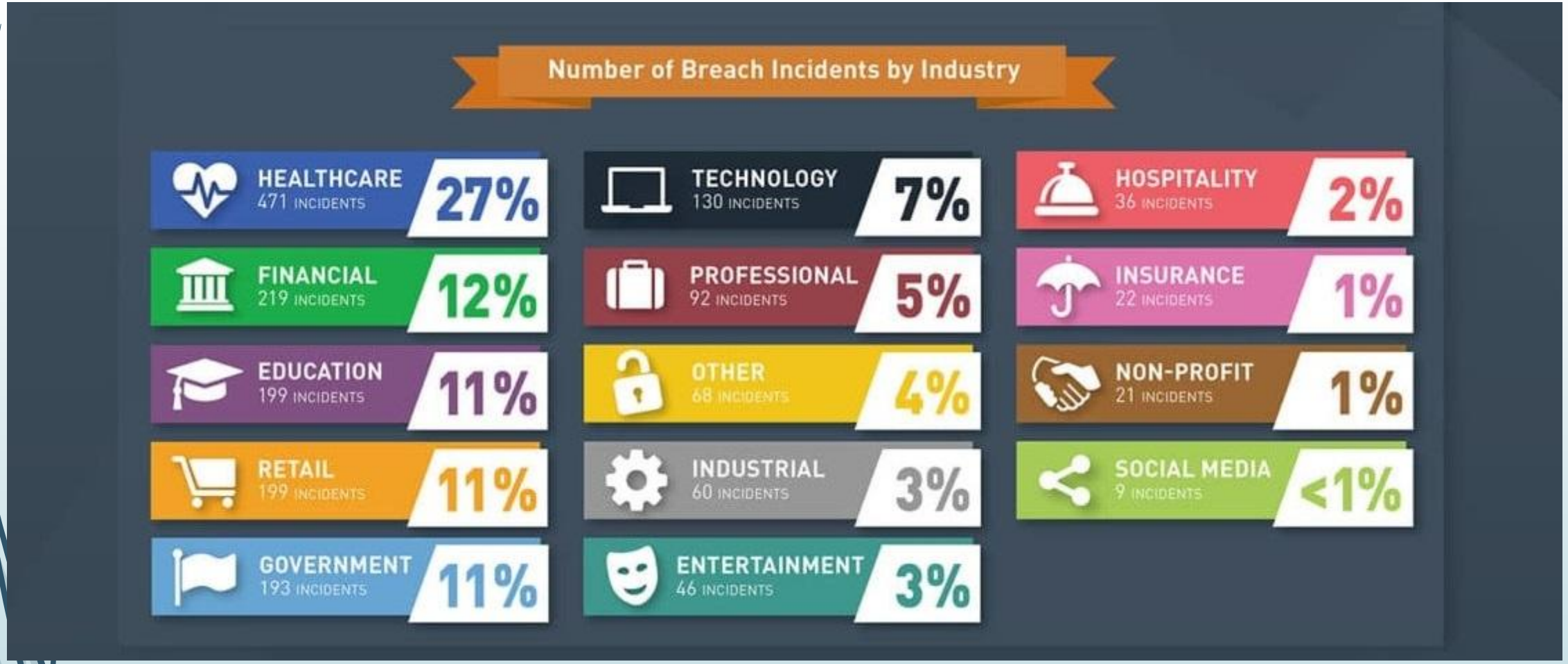
- أطفال الهاكرز Script Kiddies
- الهاكرز ذو القبعة السوداء Black Hat Hackers
- الهاكرز ذو القبعة الرمادية Grey Hat Hackers
- الهاكرز ذو القبعة الحمراء Red Hat Hackers

الهدف من الاختراق

1. المعرفة
2. التعديل
3. التخريب
4. الحصول على المال
5. التخفي وراء ضحايا منعا للمحاسبة القانونية
6. أغراض سياسة
7. الاضرار بالسمعة.
8. حروب الكترونية



الدول الاكثر اختراقاً على مستوي العالم وبمعدل زيادة 1.5% سنويا



أكثر الفئات اختراقاً عالميا

أشهر اسباب الاختراق

أشهر أسباب الاختراق

عدم حماية Router

- عدم الاهتمام بتغير كلمة المرور الافتراضية Router
- ضعف كلمة مرور الشبكة اللاسلكية Wi-Fi
- استخدام نظام تشفير ضعيف
- تفعيل خاصية WPSللاتصال السريع
- وجود أجهزة مصابة على الشبكة

أشهر أسباب الاختراق

عدم تحديث أنظمة التشغيل والتطبيقات

عدم الاهتمام بتحديث أنظمة التشغيل التطبيقات من أكثر الأسباب التي تودي الي الاختراق وتقوم الشركات بإضافة التحديثات الازمة، ولكن تكون بدون فائدة إذا لم يقوم المستخدم بأجراء التحديث بشكل مستمر

اشهر أسباب الاختراق

Wi-fi بنفس اسم شبكتك

- وقو قيام المخترق بعمل شبكة Wi-Fi مماثلة تماما لنوع شبكتك بنفس الإعدادات (التردد ونوع التشفير، ولكن بكلمة سر مختلفة)
- وعندها يتم خدعاك ويطلب منك كتابة الباسورد مرة خري
- وعندها يتم سرقة كلمة السر الأساسية واختراق شبكتك وكل اجهزتك المتصلة بها بكل سهولة .

أشهر أسباب الاختراق

استخدام اجهزة الاخرين

- عدم تسجيل الخروج بعد انهاء عملك
- قد لا يهتم غيرك بتامين جهازه بالشكل الكامل واحتمالية وجود برامج ضارة عليه شكل محتمل
- استخدام جهاز طفلك لإنجاز عمل طارق تم طلبه منك وانت خارج العمل .

اشهر أسباب الاختراق

واصلات الانترنت

- استخدام واصلات الانترنت لتقليل تكلفة الاشتراك الشهري او عدم توفر بدائل بتكلفة مناسبة في بعض الإمكان السكنية الجديدة او الريفية

أشهر أسباب الاختراق

استخدام وسيط

- Proxy or VPN استخدام أنظمة وسيطة غير موثوق بها للحصول علي خدمات وزيارة مواقع محجوبة طبقا لسياسة الاستخدام الخاصة ببلدك او مؤسستك
- حيث يقوم مزود الخدمة بالاحتفاظ بجميع بياناتك ويقوم بتحليها ويتجسس عليك بكل سهولة .

أشهر أسباب الاختراق

عدم تأمين حسابك بصورة جيدة

- ترك كلمة المرور مع أكثر من شخص ليقوم بالنيابة عنك في بعض الأمور .
- عدم الاهتمام بإجراءات الحماية والسرية .
- الثقة الزائدة في بعض الأشخاص عند كتابة كلمة المرور.

أشهر أسباب الاختراق

تصفح الرسائل الغير معروفة والعشوائية

عادة ما تكون الرسائل الغير معروفة والعشوائية بها العديد من الإعلانات والبرامج الضارة

أشهر أسباب الاختراق

كلمات مرور سهلة

وهي من أشهر الأسباب حيث يمكن تخمنيها بسهولة مثل
رقم الموبايل او تاريخ الميلاد او اسم أحد ابنائك

00000000	0000	123	1234	12345
123456	12345678	123456789	Password	P@ssw0rd
qwerty	letmein	football	iloveyou	admin
welcome	monkey	login	abc123	starwars
123123	dragon	passw0rd	master	trustno1
hello	freedom	whatever	qazwsx	Co@123
asd@123	101010	2019	100100	mypass
user	hacker	superadmin	mymail	I&you

أشهر كلمات المرور اختراقنا على مستوي العالم

أشهر أسباب الاختراق

الاختراق بالصفحات المزورة

زيارة الصفحات المزورة أو الملغمة والروابط المختصرة والمصغرة مثل **bit.ly** أو **goo.gl** دون التأكد من سلامتها والامثلة على ذلك كثيرة جدا

وهي طرق جديدة دائما وتنتشر بشكل غير طبيعي اثناء الاحداث التي الموجودة على الساحة

أشهر أسباب الاختراق

الرسائل الاحتيالية

هي إحدى الطرق المفضلة لدى المخترق حتى يتمكن من سرقة بريدك الإلكتروني أو معلوماتك الحساسة، والأمثلة على ذلك كثيرة ومتجددة، منها أن تصلك رسالة بنفس شكل البنك الذي تتعامل معه، ويطلب منك تعديل بياناتك الخاصة لوجود مشكلة فنية، ويضع رابط موقع إلكتروني مزيفًا شبيهًا بموقع البنك، وهنا قد لا يستطيع المستخدم تمييز الموقع المزيف، ويضع جميع معلوماته المهمّة، ومنها كلمة السر.

اشهر أسباب الاختراق

الرسائل الاحتيالية المرتبطة بالهندسة الاجتماعية

تعتبر واحداً من أكثر الهجمات الالكترونية شيوعاً وتتم من خلال اراسل رسالة عبر البريد الإلكترونية التي غالباً ما تكون مقنعة وتبدو أنها من مرسلين شرعيين. وتهدف هذه الرسائل إلى إغراء مستلميها المستهدفين للنقر على الروابط

تستهدف عمليات التصيد الاحتيالي أكبر عدد من مستلمي الرسائل بحيث تنطلي الخدعة على نسبة ضئيلة منهم لتحقيق النجاح المحتمل.

كما يمكن استخدام الفواتير الوهمية، وإشعارات التسليم والإيصالات والتحديثات المصرفية كوسيلة للخداع في هذه المحاولات.

أشهر أسباب الاختراق

استخدام برامج لاختراق الاخرين

وهو قيام الضحية باستخدام برامج مخصصة للاختراق الشبكات اللاسلكية للحصول على انترنت مجاني وتعتمد على مشاركة كلمات المرور بين المستخدمين وبين مصمم البرنامج نفسه بالإضافة الي زرع برمجيات خبيثة داخل جهازك وبموافقتك.

أشهر أسباب الاختراق

استخدام خط تليفون لا تملكه

استخدام خط تليفون محمول او شريحة بيانات غير مسجلة لدي مزود الخدمة باسمك ممكن يجعل من السهل استبدال الشريحة بكل سهولة واختراق جميع حساباتك الالكترونية في اقل من 7 دقائق.

أشهر أسباب الاختراق

شريحة غير موثوق من مصدرها

أحدث طرق الاختراق وهي عرض أحد الأشخاص عليك شريحة تتضمن العديد من الميزات والخدمات التي لا تقاوم مكالمات دولية مجانية , انترنت بدون حدود وبدون أي مصاريف

أشهر أسباب الاختراق

برامج غير معروفة المصدر

1- استخدام أنظمة تشغيل غير اصلية وغير تابعة للشركة المصنعة .
2- استخدام برامج غير اصلية تكون محملة بالعديد من الفيروسات والروابط الملغمة.
3- استخدام برامج مفعلة بطرق غير شرعية Cracksوتمثل حوالي 70% من أسباب الاختراق وتشفير البيانات

أشهر أسباب الاختراق

استخدام الخدمات العامة

استخدام خدمات مجانية دون التأكد من سلامتها

البرمجيات الخبيثة

الفيروسات

تمتلك الفيروسات القدرة على نسخ نفسها من خلال الارتباط بملفات معينة في الجهاز مثل الأغاني ومقاطع الفيديو. ومن أمثلة الفيروسات، فيروسات الملفات، وفيروسات الماكرو، وفيروسات قطاع الإقلاع

الديدان

تنسخ الديدان نفسها، ولكنها لا ترتبط بالملفات كما تفعل الفيروسات. ولعل الفارق الأكبر بين الفيروسات والديدان هو أن الأخيرة عبارة عن برمجيات مخصصة للشبكات، فهي تستطيع الانتقال بسهولة من جهاز إلى آخر عند توفر الشبكة، كما أنها لا تحدث ضررًا كبيرًا في الاجهزة المستهدف، فقد تعمل مثلاً على استهلاك مساحة القرص الصلب، وبالتالي تقلل من سرعة الكمبيوتر.

حصان طروادة

تختلف أحصنة طروادة بصورة كبيرة عن الفيروسات والديدان من ناحية المفهوم. وقد اشتقت أحصنة طروادة اسمها من الأسطورة اليونانية القديمة حول دخول اليونانيين إلى مدينة طروادة المحصنة. فقد أخفى اليونانيون جنودهم في داخل حصان خشبي عملاق وقدموه لسكان طروادة على أنه هدية، وبسبب حب سكان طروادة الشديد للخيول والأحصنة، فقد قبلوا هذه الهدية بدون تفكير. وفي الليل، خرج اليونانيون من الحصان وهاجموا المدينة من الداخل.

تتلخص فكرة عمل أحصنة طروادة في أنها تتخفى في داخل برامج تبدو سليمة من الظاهر، وعند تشغيل هذه البرامج تنفذ أحصنة طروادة عملها إما بسرقة المعلومات أو غيرها من المهمات التي صُممت من أجلها.

البرامج الآلية

تُعد البرامج الآلية شكلاً متقدمًا من الديدان، وهي عبارة عن عمليات آلية مصممة للتفاعل عبر الإنترنت دون الحاجة إلى تدخل بشري. ويمكن للبرامج الآلية أن تكون جيدة أو سيئة. أما البرامج الآلية الخبيثة فهي تصيب الجهاز المضيف، وتتصل بعد ذلك بسيرفر مركزي يعطي الأوامر لجميع البرامج الآلية المرتبطة، والتي ترتبط بالسيرفر المركزي من خلال شبكة الروبوت أو البوت نت.

طريقة عمل البرمجيات الخبيثة

الإعلانات الخبيثة

الإعلانات الخبيثة ليست ضارة للغاية، ولكنها تمثل انتهاكًا لخصوصية المستخدمين، فهي تعرض الإعلانات على سطح المكتب أو في داخل البرامج. وتأتي هذه الإعلانات عادةً مرتبطة بالبرامج المجانية، فهي تمثل مصدر الدخل الرئيسي لمطوري هذه البرامج. وتراقب هذه الإعلانات اهتماماتك وتعرض إعلانات مرتبطة بها. ويمكن للمهاجم أن يبرمج الإعلانات على نحو يمكنها من التجسس على نشاطات حاسوبك، أو تعطيله.

برامج التجسس

هي برامج تراقب نشاطاتك على جهاز الحاسوب وتنقلها إلى الجهة المعنية. وتدخل برامج التجسس إلى الجهاز عادةً بواسطة أحصنة طروادة أو الفيروسات أو الديدان، وبمجرد دخولها تثبت نفسها على الجهاز، وتبقى في حالة سكون حتى لا تُكتشف.

ومن أشهر هذه البرامج برنامج KEYLOGGER والذي يسجل عمل لوحة المفاتيح، وبالتالي يمكن الهاكرز من الحصول على معلومات مهمة مثل اسم المستخدم، وكلمة المرور، ومعلومات بطاقة الائتمان، وغير ذلك.

برامج الفدية

هي برامج تشفر ملفاتك، أو تقفل حاسوبك كليًا أو جزئيًا، بعد ذلك تظهر شاشة تطلب منك دفع فدية مقابل فك التشفير أو الإغلاق.

(Scareware)

تتخفي هذه البرمجيات على أنها أدوات تساعدك على إصلاح النظام، ولكن بمجرد تشغيلها تصيب نظامك وتدمره بالكامل، كما أنها قد تعرض رسالة لتخويفك وإجبارك على اتخاذ بعض الإجراءات مثل الدفع من أجل إصلاح نظامك.

الرووت (Rootkits)

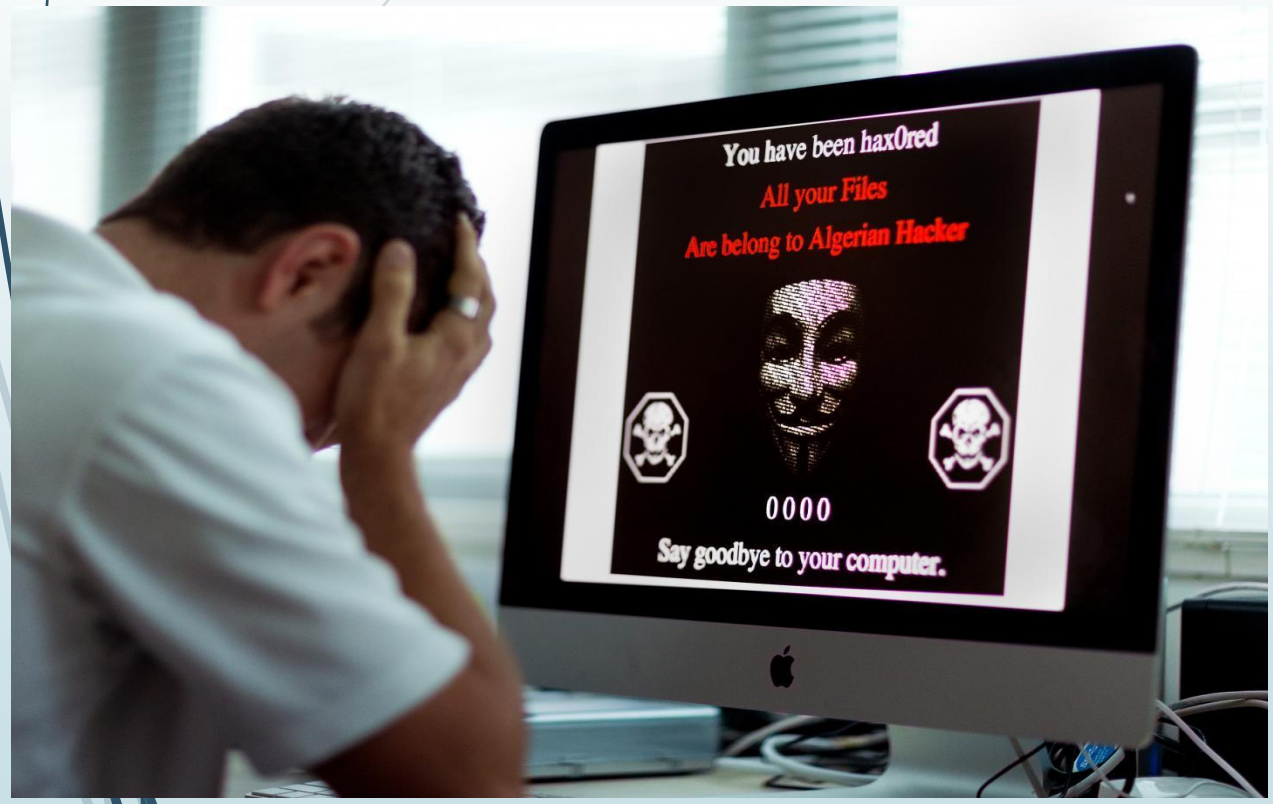
هي برمجيات مصممة للحصول على امتيازات إدارية في نظام المستخدم، وذلك بهدف سرقة الملفات أو البيانات الخاصة.

الزومبي

هي برمجيات مشابهة للبرمجيات التجسسية، وآلية دخولها مشابهة أيضًا، ولكنها لا تتجسس ولا تسرق المعلومات، وإنما تدخل إلى الجهاز وتظل منتظرة لأوامر الهاكرز للتخفي وراء الضحية

كيف تعرف أنك مخترق ؟؟

كيف تعرف أنك مخترق ؟؟



Computer

Phone

كيف تعرف انه تم اختراق هاتفك

كيف تعرف أن هاتفك مخترق

انخفاض نسبة الشحن في البطارية رغم الاستخدام العادي.
ظهور النوافذ المنبثقة واعلانات بشكل مستمر
زيادة استهلاك حزم البيانات ودقائق المكالمات
تشغيل البلوتوث رغم عدم تفعيله
تشغيل الكاميرا والتقاط الصور
تشغيل ضوء الفلاش رغم عدم تفعيله
إعادة تشغيل الهاتف دون سبب
تعذّر فتح بعض التطبيقات , وخاصة تطبيقات الأمان .
تفعيل خاصية تحميل التطبيقات من مصادر غير معروفة .
ظهور الإعلانات المُزعجة بشكل مُتكرر.
تغيّر طريقة عرض بعض المواقع الإلكترونية
مواجهة انقطاعات غير عادية في بعض الخدمات؛ كفقدان الشبكة

تثبيت عشوائي للتطبيقات
مطالبات بإعادة تعيين كلمات المرور
تغيير إعدادات الهاتف وحذف الملفات
ظهور رسائل نصية ورسائل بريد إلكتروني لم تُرسل
تسجيل مقاطع الفيديو
سماع صوت غريب أثناء إجراء المُكالمات
إبقاء الهاتف قيد التشغيل وعدم القدرة على إغلاقه نهائياً
ظهور فاتورة مُشتريات عبر البطاقة الائتمانية لأشياء لم يتمّ شراؤها
تحميل صفحات إنترنت ومواقع إلكترونية بشكل عشوائي
استقبال أو إرسال رسائل نصية غريبة
فتح مواقع ذات محتوى سيئ بشكل تلقائي
بطء شديد في استجابة الجهاز , بالضافة الي ارتفاع درجة الحرارة

كيف تعرف انه تم اختراق جهازك

كيف تعرف أن جهاز الكمبيوتر

انخفاض نسبة الشحن في البطارية (Laptop)
ظهور النوافذ المنبثقة واعلانات بشكل مستمر
تعطل نظام الحماية
عدم القدرة على تحميل مضاد للفيروسات
تشغيل الكاميرا والتقاط الصور
حذف وتشفير الملفات
إعادة تشغيل الجهاز دون سبب
تعذّر فتح بعض البرامج
وجود برامج غريبة لم تقم بتحمليها
ظهور الإعلانات المُزعجة بشكل مُتكرر
تغيّر طريقة عرض بعض المواقع الإلكترونية
عدم استقرار خدمة الانترنت
استهلاك موارد الجهاز بدون سبب

تثبيت عشوائي للتطبيقات
مطالبات بإعادة تعيين كلمات المرور
تغيير إعدادات الجهاز
ظهور رسائل بريد إلكتروني لم تُرسل
تسجيل مقاطع الفيديو
عدم القدرة علي تحديث نظام التشغيل يدويا.
إبقاء الجهاز قيد التشغيل وعدم القدرة على إغلاقه نهائياً
ظهور فاتورة مُشتريات عبر البطاقة الائتمانية لأشياء لم يتمّ شراؤها
تحميل صفحات إنترنت ومواقع إلكترونية بشكل عشوائي
ظهور ملفات بامتدادات غريبة
فتح مواقع ذات محتوى سيئ بشكل تلقائي
ظهور ملفات كثيرة مخفية بأسماء غريبة

هل تم اختراق حسابك الالكتروني من قبل؟؟

هل يمكن معرفة المخترق من قبل المحققين؟؟

الجرائم الإلكترونية

يؤدي الاستخدام المتزايد للتقنيات الرقمية في قطاع الأعمال دوراً حيوياً في نمو الأعمال التجارية. غير أن هذا الاستخدام له أخطار أيضاً.

تستهدف الجرائم الإلكترونية الضحايا من الأفراد وحتى الشركات الكبيرة، وذلك عبر طرق مختلفة مثل التصيد الاحتيالي والتثبيت غير المشروع للبرامج الضارة. الأمر الذي يؤدي إلى خسارة فادحة.

الهجمات الرقمية تشهد تزايداً في استخدام الأدوات المتطورة المتاحة في السوق الاجرامي الافتراضي على الانترنت. ومع تطوير بعض الجماعات الإجرامية لأنشطتها، فإن الجرائم الإلكترونية تتطور أيضاً وتنمو بسرعة.

في الفترة الأخيرة وخاصة بعد انتشار فيروس كرونا و استخدام التكنولوجيا في تزايد مستمر مما جعل عدد الأشخاص الذين يرغبون في الحماية من التهديدات الأمنية يتزايد بشكل مستمر وكذلك جميع المؤسسات وحتي الأشخاص يحتاجون الى نظام امن معلومات قوى يقوم بحمايتهم

هل تثبت حقك في حالة الاختراق؟

قانون الجريمة الالكترونية

زاح قانون مكافحة جرائم الإنترنت في مصر الستار عن العديد من الجرائم التي ترتكب عبر مواقع التواصل الاجتماعي وتتنافى مع الآداب العامة، وتنتهك سلوكيات المجتمع المصري. ويتضمن قانون مكافحة جرائم الإنترنت عددا من العقوبات لمواجهة الاستخدام غير المشروع للحواسيب وشبكات المعلومات، وحماية البيانات والمعلومات الحكومية والأنظمة والشبكات المعلوماتية الخاصة بالدولة أو أحد الأشخاص الاعتبارية العامة من الاعتراض أو الاختراق أو العبث بها أو إتلافها أو تعطيلها بأي صورة، والحماية الجنائية لحرمة الحياة الخاصة التي كفلها الدستور للمراسلات الإلكترونية، وعدم إفشائها أو التنصت عليها إلا بأمر قضائي مسبب، بالإضافة لضبط الأحكام الخاصة بجمع الأدلة الإلكترونية، كما نظم المشروع إجراءات حجب المواقع الإلكترونية.

هل تثبت حقك في حالة الاختراق؟

الأدلة الإلكترونية

ليتم النظر في طلبك امام الجهات القانونية يجب ان يتم تدعيم الطلب بالآتي

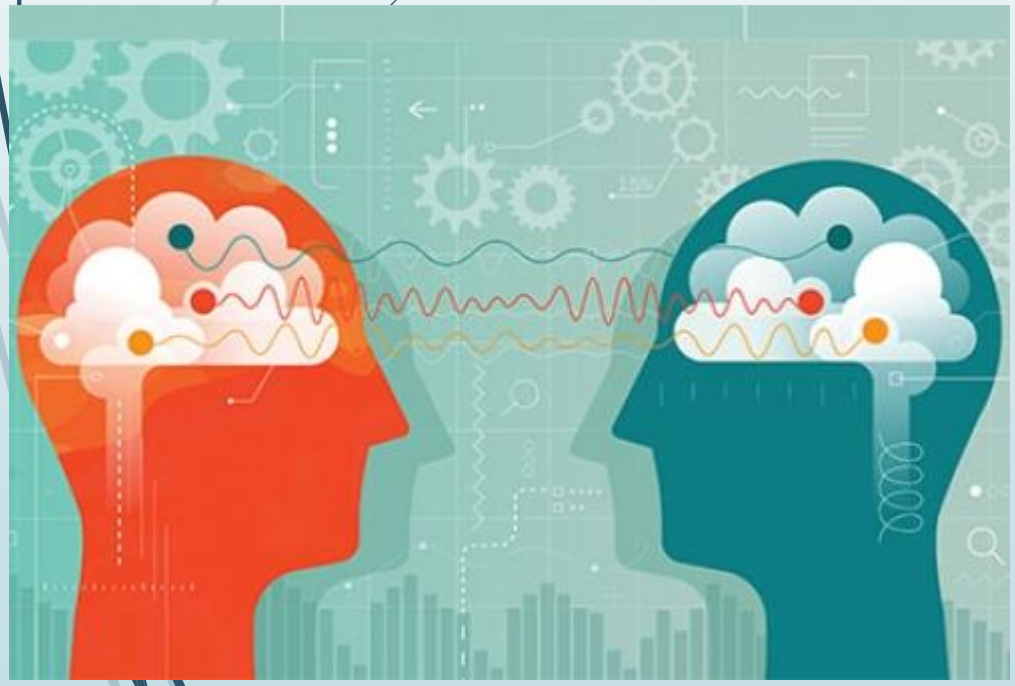
- التقاط فيديو للمطلوب الإبلاغ عنه (فيديو امر ضروري ويمكن التدعيم بالصور)
- ضروه ارفاق جميع المعلومات وليس جزء من الشاشة
- استخدام الكمبيوتر بقدر المستطاع في عمل التوثيق وليس التليفون المحمول .
- اخذ نسخة من المطلوب الإبلاغ عنه (منشور، ايميل .الخ) بدون اجراء أي تعديل باي برنامج
- اخذ نسخة من URL في ملف TXT وان يكون واضح ضمن الفيديو اثناء استخراجه
- عدم مشاركة تلك البيانات مع أي جهة غير الجهات المختصة للحقيق
- تحميل الأدلة الرقمية على أسطوانة يتم تسليمها ضمن مستندات الطلب.

إجراءات المحافظة على أمن المعلومات داخل المؤسسات

إجراءات المحافظة على أمن المعلومات داخل المؤسسات

توظيف المؤهلين

لحماية المعلومات السرية وتأمينها بشكل جيد، يجب على أي مؤسسة توظيف الأشخاص المؤهلين لحماية بيانات المؤسسة هذا للتأكد من أن الموظف يعرف ما يجب فعله في حالة حدوث مشكلة. إلى جانب ذلك، يتمتع الموظفون المؤهلون بفهم أفضل لأمن المعلومات ويعرفون الخطوات اللازمة حتى يتأكدوا من عدم تسريب معلومات المؤسسة دائمًا.



إجراءات مادية

- التأمين المادي للأجهزة والمعدات
- تقييد الوصول إلى المكاتب، وخصوصًا مراكز تخزين البيانات
- تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.
- تركيب أنظمة Firewallوأنظمة كشف الاختراق وتحديثها.
- تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.
- عمل سياسة للنسخ الاحتياطي.
- استخدام أنظمة قوية لتشفير المعلومات المرسلة.
- التواصل المستمر مع فريق امن المعلومات.
- نشر التعليم والوعي الأمني كل فترة نظرا لتغير طرق الاختراق

إجراءات المحافظة على أمن المعلومات داخل المؤسسات

لا تخلط بين حياة الشركة والحياة الشخصية

يجب أن يعرف الموظفون حدودهم. يجب أن يعرفوا كيف يفرقون بين حياتهم الشخصية وعملهم ويجب ألا يستفيدوا من مرافق المؤسسة المستخدمة لأغراضهم الشخصية هذا لأنها يمكن أن تجعل معلومات المؤسسة في خطر و يجب أن تشرح المنظمة هذا الأمر للموظفين لإعلامهم بما هو مقبول وغير مقبول

الالتزام بالسياسات

يجب على المؤسسة وضع وتنفيذ السياسات المتعلقة بأمن المعلومات لضمان اتباع الموظفين لهذه السياسات وتعتبر سياسات أمن المعلومات مهمة جدًا في المنظمة لأنها ستحدد متطلبات أمن المعلومات. لذلك يجب على المنظمة مراجعة السياسة بشكل منتظم من أجل تلبية متطلبات امن المعلومات.

زيادة مستوى وعي الموظفين بأمن المعلومات

من أجل زيادة الوعي بقضايا الامن بين الموظفين يجب على المؤسسة اتخاذ عدة خطوات لتحسين وعي الموظفين وفهمهم لأمن المعلومات والطريقة التي يمكن أن تتخذها المؤسسة من خلال توفير التعليم لموظفيها حول حماية البيانات و التدريب المكثف للموظفين حول طريقة حماية البيانات.

المخاطر

يمثل أمن المعلومات لأى مكان الجهاز العصبي لها حيث ان وجود إي عطل به يتسبب في العديد من الأضرار الخاصة بمختلف الاقسام فهو عبارة عن اداة تضمن سرية العديد من المعلومات الخاصة بالمؤسسة وتعمل على توافرها وتضمن مصداقيتها وهذا يقلل من حدوث ازمات في المؤسسة.

- سرقة البيانات
- التشفير البيانات للحصول على فدية
- إتلاف الأجهزة
- إعادة توجيه خدمات المصرفية عبر الإنترنت
- فقدان البيانات
- سرقة الأموال.
- تزوير الهوية (انتحال الشخصية).
- تعطل النشاط التجاري
- تضرر السمعة
- تقييد الوصول إلى الإنترنت


أكبر 10 عمليات اختراق الكتروني فى العالم

الحروب الالكترونية

مع عصر التقنية حيث أصبحت أغلب الأشياء تعتمد على التقنية في سيرها وتسييرها، وما دام هناك أنظمة تشغيل، فدوما يرافقها قضية مهمة وهي: الأمان والحماية المتعلقة بهذه الأنظمة.

أصبحت أجهزة التلفزيون ذكية، السيارات ذكية وذاتية القيادة، الثلاجة أصبحت ذكية، المنازل أصبحت ذكية حتى وصل الأمر إلى أحذية ذكية ويوجد مدن كاملة مرتبطة بشبكة الانترنت وغيرها من الأشياء الخاصة بالأفراد

والمقصود بالذكية أنه أصبح من السهل التحكم بها أو تعمل بنظام تشغيل يسهل استخدامها ويبسطه، وبشكل خاص أصبحت مرتبطة بشبكات داخلية أو شبكة انترنت، فبالتالي القاعدة تنطبق عليها، أي شيء مرتبط بالشبكة فهو قابل للاختراق مع تفاوت في قدرة الهاكرز على اختراقها، وفقا لخبرتهم، ووفقا لقوة نظام التشغيل المستخدم أو طرق التشفير المعتمدة.

هل كل شيء قابل للاختراق؟

الجواب باختصار: **نعم** كل شيء قابل للاختراق، لكن على درجات متفاوتة، وكما ذكرنا سابقا، إمكانية الاختراق راجعة أولا لقدرة المخترق أو وخبرنه ، والأمر الثاني راجع لقوة نظام التشغيل أو تشفير الشيء المراد اختراقه مهما كان، وبشكل عام الجماعات أو المنظمات التابعة للدولة لها قدرة أكبر في اختراق أي شي.


RANSOMWARE

RANSOMWARE

هجمات الفدية أكبر تهديد على الإنترنت

عبارة عن هجوم إلكتروني (فيروس) يُستخدم لابتزاز المستخدم وتحريضه على دفع المال. كان المجرمون في البداية يستخدمون Ransomware كوسيلة ابتزاز لجني الأموال من الأفراد الذين يريدون استرداد معلوماتهم الشخصية. واليوم يستخدم المجرمون Ransomwareكوسيلة ابتزاز لجني الأموال من الشركات التي تريد استرداد معلوماتها الحساسة. لا يوجد جهاز محصّن من Ransomware. فقد ابتز المجرمون الأفراد لتحريضهم على دفع الأموال مقابل استرداد معلوماتهم الشخصية أو الطبية من مزوّدي الرعاية الصحية ومنعوا الضيوف من الدخول إلى غرفهم في الفنادق. حتى أن الأنظمة الصناعية أثبتت حساسيّتها اتجاه Ransomware.

يتم تشفير الملفات بطريقتين :-

Offline

وهناك امل ضعيف في استعادة الملفات بطرق فنية معقدة بعض الشيء

Online

ولم يتم اكتشاف أي حلول حتي الان نظرا للتعقيد الشديد لمفاتيح التشفير

اشهر ضحايا الفدية المعلن عنها

ابريل 2020

- عملاقة الطاقة البرتغالية (EDP) وتم بتشفير أنظمة الشركة وطالب بفدية قدرها 10 مليون
- شركة Cognizant ضمن قائمة أعلى 500 شركة مساهمة أمريكية من حيث الإيرادات، وهي شركة تقدِّم خدمات تكنولوجيا المعلومات للشركات، وانخفضت الارباح بنسبة 3.4٪ بسبب هجوم الفدية

مايو 2020

- شركة محاماة Grubman Shire Meiselas بنيويورك ولديها مجموعة من العملاء المشهورين وطلب فدية 21 مليون دولار، بل تضاعفت الفدية المطلوبة إلى 42 مليون دولار عندما رفضت الشركة أن تدفع
- جامعة ولاية ميشيغان – 10 مليون دولار

يونيو 2020

- شركة السيارات العملاقة هوندا، واستهدف هذا الهجوم مكاتب الشركة في الولايات المتحدة الأمريكية وأوروبا واليابان
- كلية Columbia College Chicago

يوليو 2020

- شركة الاتصالات الفرنسية Orange أكبر مشغل للهاتف المحمول في أوروبا
- مدينة لافاييت في كولورادو في 45 ألف دولار

اشهر ضحايا الفدية المعلن عنها

أغسطس 2020

- جامعة يوتا 457 ألف دولا ولأن البيانات المسروقة احتوت على معلومات خاصة بالطلاب والموظفين، قررت الجامعة سداد الفدية لتجنب تسريب المعلومات، كما نصحت الجامعة جميع الطلاب والموظفين في الكلية المتضررة بمراقبة تاريخ استخدام بطاقاتهم الائتمانية لرؤية أي نشاط احتيالي فور وقوعه، وكذلك تغيير أي كلمات مرور يستخدمونها على الإنترنت.
- شركة Accretive Health Incواحدة من أكبر شركات تحصيل الديون الطبية في الولايات المتحدة الأمريكية، وهي متعاقدة مع أكثر من 750 مؤسسة رعاية صحية في الولايات المتحدة سبتمبر 2020
- شركة K-Electric، الموزع الوحيد للطاقة في مدينة كراتشي بباكستان 7.7 مليون دولار.
- مكاتب الهجرة في الأرجنتين والعديد من الوكالات الحكومية الأمريكية وجامعة كاليفورنيا في سان فرانسيسكو (التي دفعت أكثر من مليون دولار كفدية).

اشهر الضحايا المعلن عنها

أكتوبر 2020

- وكالة أنباء India (PTI)، مما أدى إلى شل خدماتها لساعات. وصف متحدث باسم الشركة الحادث بأنه هجوم فدية هائل تسبب في تعطيل العمليات وتوصيل الأخبار إلى المشتركين في جميع أنحاء الهند.
- Software AG واحدة من أكبر شركات **البرمجيات** في العالم تعرضت لهجوم من عصابة برنامج الفدية Clop، والتي طالبته بأكثر من 20 مليون دولار!

نوفمبر 2020

- محكمة العدل العليا البرازيلية
- نادي مانشستر يونايتد لكرة القدم

ديسمبر 2020

- GenRx Pharmacyهي منظمة رعاية صحية مقرها أريزونا الأمريكية
- شركة الأجهزة المنزلية العملاقة Whirlpool

الحروب السيبرانية

الحروب السيبرانية هي هجمات على شبكات الكمبيوتر، عن طريق اختراق الشبكات وإضافة معلومات كاذبة، ونشر فيروسات بهدف تعطيل الشبكات، أو الحصول على بيانات معينة بدون إتلافها، مثل البيانات العسكرية والاستخباراتية لبعض الدول.

ومن نتائج الحرب السيبرانية ضعف وضرر الخدمة بشكل جزئي مثل انقطاع التيار الكهربائي، أو توقف الخدمة كليًا مثل توقف كامل لبث القنوات الفضائية كما حدث لوكالات أنباء تعرضت لهذا الهجوم، وتقديم خدمات ومعولمات مزيفة من جهات وهمية مثل السيطرة على شبكة أحد البنوك وتقديم معلومات كاذبة للعملاء، وصلت خطورة هذه الهجمات وفى عام 2015، إلى حد إيقاف بث قناة فرنسية.

لماذا حساب الكتروني باسم الجامعة؟؟

لماذا حساب الكتروني باسم الجامعة؟

@nub.edu.eg

ربما يظن البعض أن الحساب الإلكتروني الذي تهديه لك الجامعة بلا فائدة لكن الحقيقة أن لهذا الحساب الإلكتروني المقدم من ميكروسوفت العالمية فوائد عديدة حيث تستخدمه الشركات للتأكد من كونك منتمي لجامعة النهضة لتقدم لك بعض العروض أو التخفيضات الخاصة بالجهات التعليمية والبحثية فقط .

لماذا حساب الكتروني باسم الجامعة؟

خدمات Microsoft office 365 for education

خدمات تساهم بشكل في رفع كفاءة العملية التعليمية إذا استغلت الاستغلال الامثل، حيث يستطيع المستخدم الحصول على العديد من الخدمات السحابية المميزة والتي تتمتع بمستوي امان عالي جدا كما يمكنه تثبيت هذه الخدمات على جميع أنواع الأجهزة والأجهزة اللوحية والتليفون المحمول بصورة قانونية

- Office APP
- Outlook
- One Drive
- Team
- Planner
- Power Automate
- Power Bi
- Calendar
- Kaizala
- OneNote Class Notebook
- Stream
- To Do
- whiteboard
- Yammer
- Windows 10

لماذا بريد الكتروني باسم الجامعة؟؟

المصداقية والثقة

عنوان بريدك الإلكتروني الرسمي يخلق شعورًا من الثقة لدى جمهورك وعملائك الخارجين بعكس البريد الإلكتروني المجّاني حيث يبحث العملاء دائمًا على الإنترنت عن دلائل تشير إلى أن هذه الجهة شرعية قبل التعامل معها

لماذا بريد الكتروني باسم الجامعة؟؟

الملكية

إذا تم إيقاف بريدك الإلكتروني المجاني أو سرقته فليس لديك سوى القليل جدا الخيارات الصعبة لتتمكّن من استرجاعه لأن هذا البريد ليس ملكًا لك في الأساس، ولكن السؤال الأصعب، هل يُمكنك أن تتعامل وتتأقلم مع فقدان بريدك الإلكتروني للأبد وفقدان كافة الرسائل؟

اجراءات الامان

اجراءات الامان

- ✓ احرص دائما على تفعيل جميع اجراءات الامان ولا تهمل اي اجراء مهما كان بسيطا بالنسبة لك حتى تضمن حماية حسابك من اي مخاطر يمكن ان يتعرض لها.

استخدم جهاز خاص بك

- ✓ احرص دائما على استخدام جهاز خاص بك وغير مشترك مع الاخرين وذلك لحمايتك من اي متطفل يمكن ان يطلع على خصوصياتك قد قام بتجميل برنامج ليقوم بحفظ كلمات السر به دون ان تعرف (Key logger).

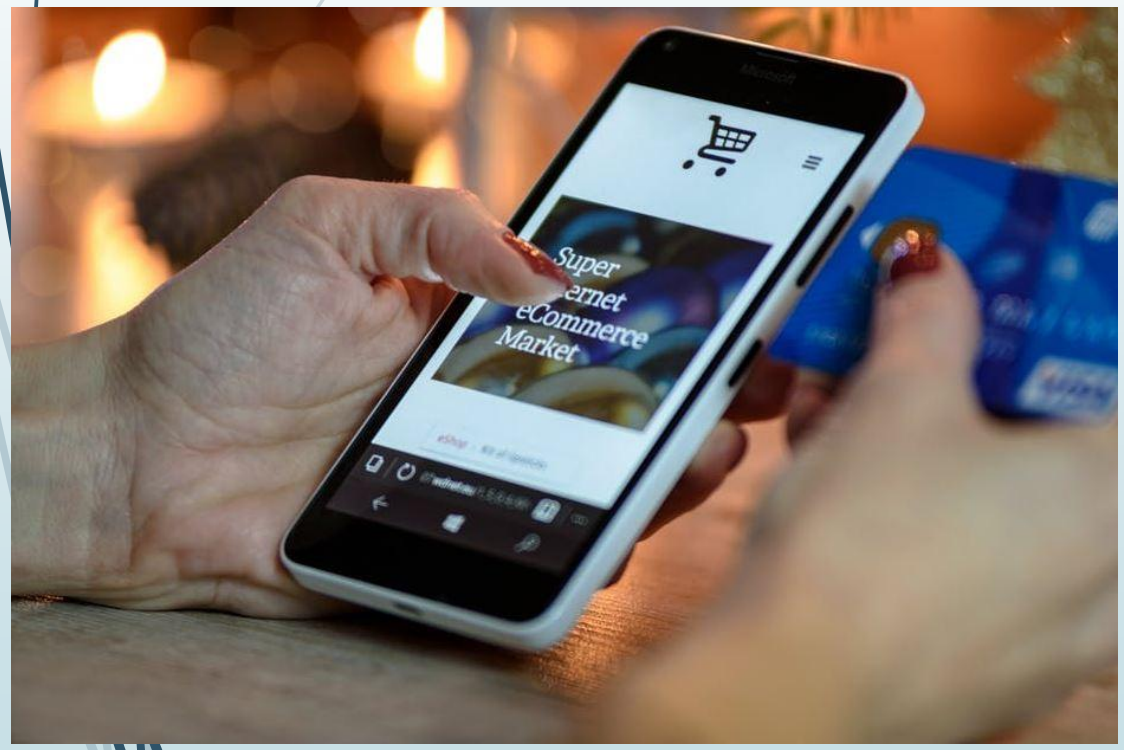
التحقق قبل الرد

- ✓ لا تقوم ابدا بالرد على اي رسالة لا تعلم معلومات عن مرسلها والتأكيد علي اسم الدومين المرسل منه الرسالة .

الاتصال المشفر

- ✓ تأكد من تشغيل الاتصال الامن HTTPS الخاص بمتصفحك فهو يعمل على تشفير بياناتك ويضمن عدم كشفها للمتطفلين.

لا تسجل في المواقع لا تخص العمل



- ✓ لا تقوم باستخدام بريدك الالكتروني للتسجيل في اي موقع لا يتبع للجامعة مثل مواقع التسوق او المنتديات او خدمة غير موثوقة

عنوان الرسالة

- ✓ لقاء نظرة على عنوان الرسالة، وهل هي مكتوبة بأسلوب مألوف لديك مقارنة بالرسائل التي تستلمها من هذا الشخص، على افتراض أنه شخص تعرفه بالفعل.

التأكد من سلامة الروابط

في حالة استلام رابط وتريد التأكد من سلامته نظرا لحاجتك
الشديدة الي فتحه والتعامل معه لحاجة العمل
يرجي استخدام احد المواقع التالية(URL Check)

Norton by Symantec

VirusTotal

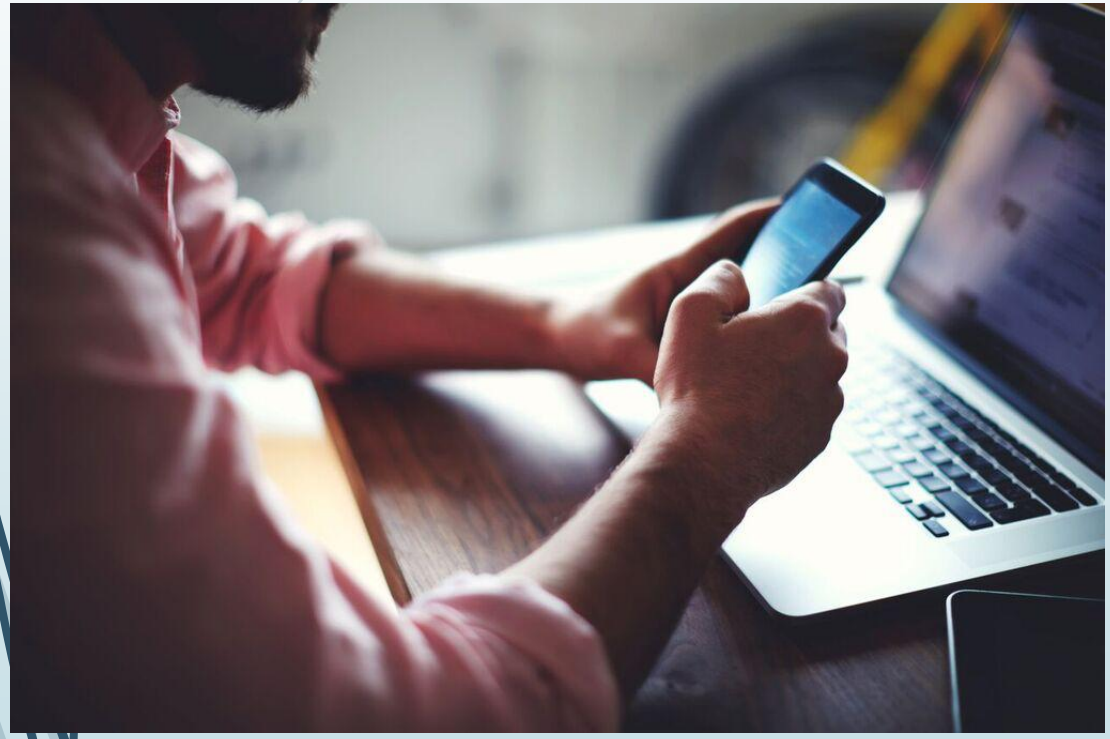
التأكد من سلامة QR Code

في حالة استلام صور في شكل QR-Code وتريد التأكد من سلامته
نظرا لحاجتك الشديدة الي فتحه والتعامل معه لحاجة العمل
يرجي استخدام احد المواقع التالية(QR Code Scanner)
والمقدم من شركة Kaspersky العالمية المتخصصة في امن المعلومات

الشبكات الانترنت العامة

- ✓ لا تقم باستخدام شبكات الانترنت اللاسلكية في الأماكن العامة (النوادي، الاستراحات العامة , الفنادق البسيطة , المطاعم ...) في عمل شيء مهم .

تفعيل التحقق بخطوتين



وتعتبر من اهم الخطوات للحفاظ علي سرية حسابك حيث لا يمكن الدخول علي حسابك الالكتروني الا بعد استقبال رمز حماية علي التليفون المحمول للتأكد من انك الذي تقوم باستخدام الحساب

ولتفعيل تلك الميزة يرجي فقط ارسال طلب الي قسم الشبكات وامن المعلومات علي

noc@nub.edu.eg

تنظيف وفحص جهازك

يجب فحص الجهاز جيدا من الفيروسات والبرامج الضارة باستخدام البرامج والادوات المتخصصة ولا تقم بإيقاف برامج الحماية لاي سبب من الاسباب

الارشادات الحماية والسرية

استخدام برامج مخصصة وتعمل علي تشفير المراسلات

احرص دائما على استخدام Microsoft Outlook وهو متاح علي الموبايل والكمبيوتر بشكل مجاني تماما

استخدام بطاقات الائتمان

- استخدم بطاقات الائتمان الافتراضية او PayPal في تعاملات الانترنت والتي أصبحت متاحة من جميع البنوك
- لا تقم باستخدام بطاقات الائتمان الشراء من خلال غير موثوق بها بشكل كبير
- حاول دائما عدم الاحتفاظ بأرقام بطاقات الائتمان على المواقع الالكترونية
- يجب تفعيل خاصة OPTللتأكيد قبل اتمام عملية السداد
- أوقف خدمات التجديد التلقائي للخدمات
- لا تشارك ارقام بطاقات الائتمان (مكتوبة مصورة) عبر تطبيقات التواصل الاجتماعي او الرسائل القصيرة او عبر التليفون
- استخدم وضع المتصفح الامن اثناء عملية الشراء

امور اضافية يجب تطبيقها بشكل دقيق جدا

بالنسبة لجهاز الكمبيوتر

- تحميل نظام حماية Internet Securityوالتحديث الدوري
- فحص الملفات من وقت لأخر مرة كل شهر على الاقل
- لا تقم بتحميل برنامج من شخص لا تثق بخبرته الفنية بشكل كبير
- لا تقم بتحميل برامج او الأفلام من مواقع مشبوهه
- استخدم متصفح امن مثل Googleاو Firefox
- لا تقم بحفظ كلمة السر علي المتصفح .
- الحرص علي عمل نسخ احتياطية من البيانات كل فترة علي وسبلة خارجية

امور اضافية يجب تطبيقها بشكل دقيق جدا

التليفون المحمول

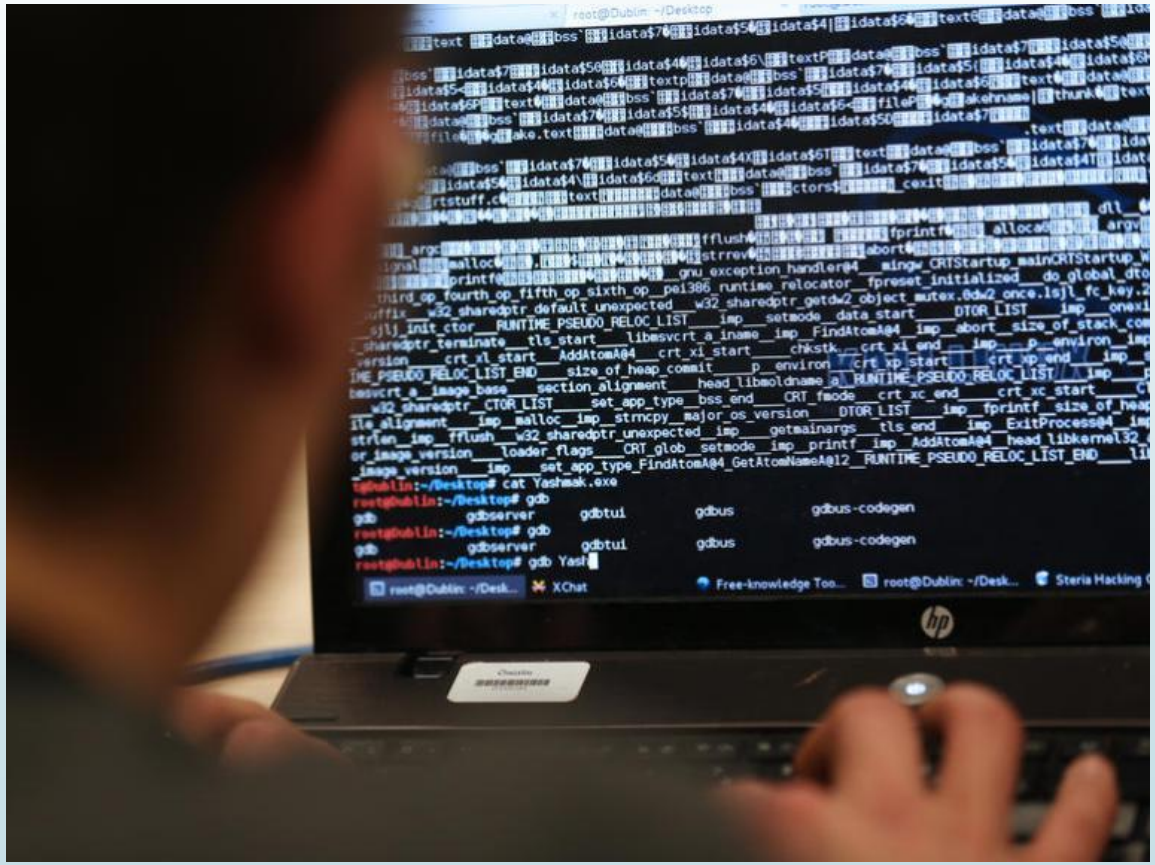
1. تحديث نظام التشغيل بشكل دوري
2. تفعيل خيار Google Protect
3. تحميل برامج حماية مناسبة
4. تشفير الجهاز
5. عدم ترك جهاز لأي شخص لا تعرفه علي الرغم من وجود رمز حماية
6. عدم استخدام برامج وسيطة لتنظيم الرسائل القصيرة عدا برامج الحماية
7. الغاء الاشعارات من على شاشة القفل .
8. عدم شحن الهاتف من الشواحن العامة .
9. نقل محتويات الجهاز كل فترة الي الكمبيوتر
10. عدم الاحتفاظ ببيانات سرية او ارقام بطاقات الاتمان علي التليفون .

امور اضافية يجب تطبيقها بشكل دقيق جدا

Messenger Application

- الغاء التحميل التلاقي
- تفعيل خاصية التشفير
- تفعيل التحقق بخطوتين
- عدم فتح أي صورة او فيديو او رابط في مجموعة تم اضافتك بها بشكل عشوائي
- إخفاء الايميل الإلكتروني ورقم التليفون اذا كان متاح
- تفعيل Passkey
- عدم مشاركة أي معلومات حساسة مثل كلمات المرور
- عدم ارسال بطاقة الهوية او جواز السفر او بطاقات الفيزا

ماذا تفعل في حالة الاختراق ؟؟



في حالة الاختراق

تغيير كلمة السر

يجب تغير كلمة السر في الحال مع ضرورة مراعاة الاتي:

- ألا تكون كلمة السر مشتركة بين جميع حساباتك الالكترونية من المنصات المختلفة
- عدم استخدام كلمة السر مرتين.
- استخدام كلمة سر معقدة يصعب تخمينها تتضمن حروف كبيرة وصغيرة وأرقام ورموز (P@ss0rd).
- تغير كلمة السر كل 90 يوم.
- الاحتفاظ بجميع كلمات السر في ورقة بعيدة عن الكمبيوتر وفي مكان امن في المنزل او خزينة.
- استخدام تطبيق لحفظ كلمات المرور وعمل كلمة مرور معقدة جدا عليه

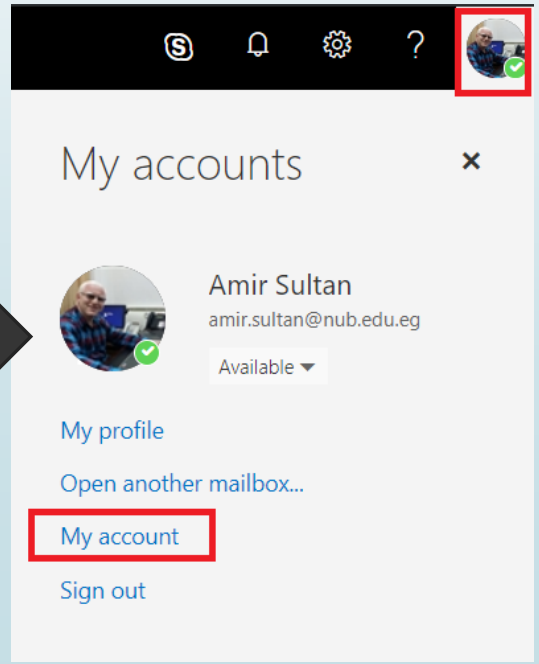
KeePass Password Safe

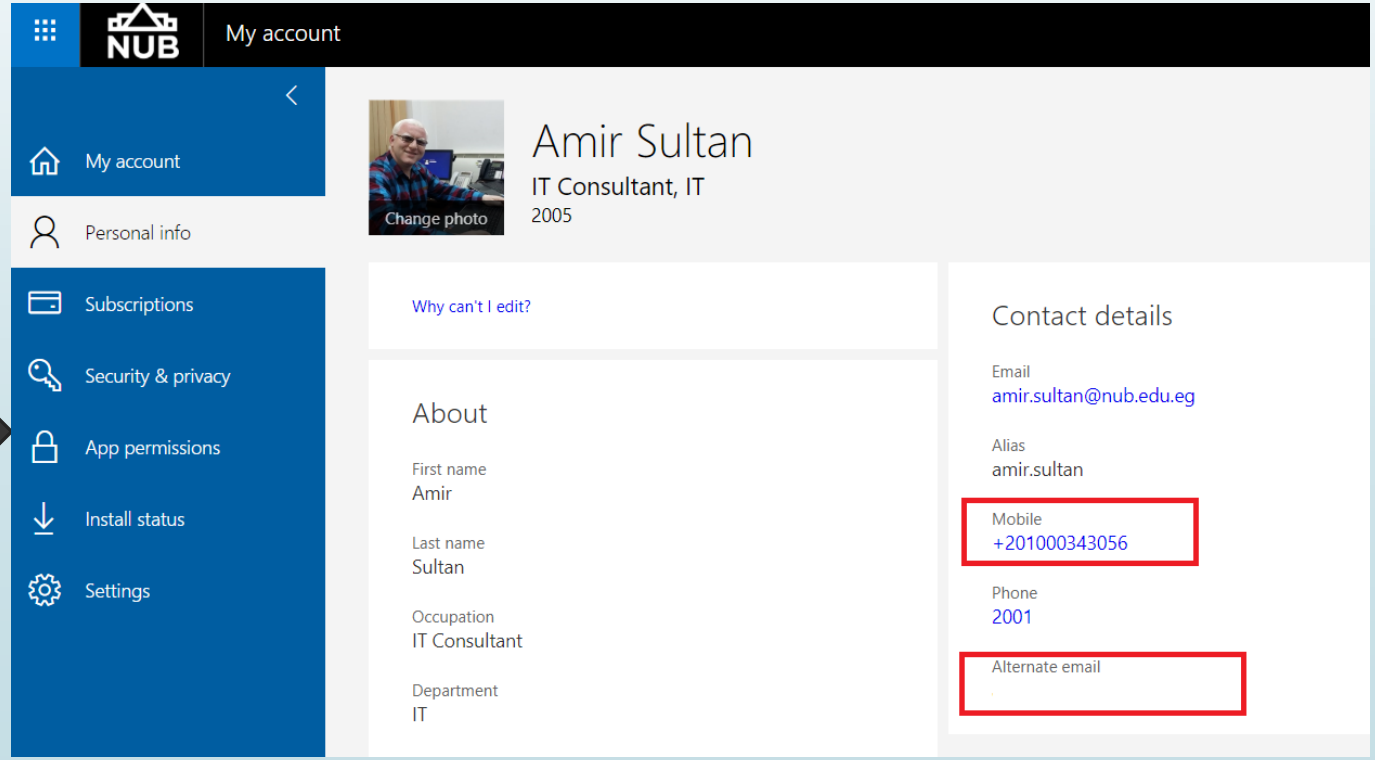
في حالة الاختراق

تفقد إعدادات حسابك

التأكيد علي عدم تغير بياناتك الأساسية مع مراعاة تغير أسئلة الأمان الاحتياطية علي الفور

Personal Info (Alternate Email, Mobile)





في حالة الاختراق

تنظيف وفحص جهازك

- يجب فحص الجهاز جيدا من الفيروسات والبرامج الضارة باستخدام احد برامج الحماية الشهيرة
- إعادة تحميل نظام التشغيل (Windows or Mac or IOS or Android) حسب نوع جهازك

في حالة الاختراق بفيروس الفدية

خطوات هامة جدا

- افصل الجهاز على الفور
- حاول تركب Hard Diskفي جهاز اخر سليم وعليه برنامج حماية مناسب إذا لم يتوافر ذلك قم بتحميل برنامج حماية وقم بتشغيل الجهاز المصاب وحدث برنامج الحماية دون فتح أي موقع او التعامل مع أي رسائل
- يجب عمل Scanللجهاز وتنظيفه بصورة جيدة جدا
- قم بتجميع كافة الملفات المصابات في مكان واحد ويفضل خارج الجهاز المصاب اذا توافر ذلك
- قم بتحميل نظام تشغيل أصلي ويمكنك الحصول عليه مجانا من خلال ايميلك الجامعي
- لا تقم بتجربة أدوات غير معرفة المصدر لحل التشفير ويجب التعامل مع مواقع موثق بها لعدم تفاكم المشكلة مثل NO MORE RANSOM او Kaspersky Free Ransomware Decryptors
- لا تدفع الفدية باي شكل من الاشكال حيث لا يوجد أي ضمانات لإعادة الملفات وإمكانية تعرضك للاختراق مرة اخري بسهولة

لطلب المساعدة

توفر الجامعة فريق للدعم الفني متخصص قد تم تدريبه و مستعد لتلقي الاستفسارات وإجراءات كل الإجراءات الفنية الازمة للتصدي للهجمات الالكترونية وتقديم الدعم الفني

لطلب المساعدة العاجلة

يرجي الرجوع الي مسؤول الدعم الفني او مسؤولي الشبكات وامن المعلومات بقطاع سيادتكم او التواصل علي نظام IT Ticket System عبر الرابط

Ticket.nub.edu.eg

في حالة الاختراق

الاعتذار

الاعتذار في حال إرسال رسائل سيئة من قبل المخترق

جزء كبير من استراتيجية القراصنة هو "الانقضاض بمخالبهم" على جهات الاتصال بك بهدف التواصل مع الآخرين. لذلك قم بإرسال رسالة إلى جميع جهات الاتصال لديك في أقرب وقت ممكن حتى تخبرهم بالذي حصل، وليتجنبوا فتح أي رسالة بريد إلكتروني واردة منك والتي من المرجّح أن يكون مرفق معه برامج ضارة.

Attachments

Technical Attachment
Step By Step

- ✓ حماية Router من الاختراق
- ✓ تغير كلمة السر
- ✓ Task Manger
- ✓ احصل على Office 365
- ✓ Windows 10
- ✓ One Drive
- ✓ طريقة تفعيل التحقق بخطوتين
- ✓ مراجعة إعدادات حسابك
- ✓ تامين حساب Facebook
- ✓ تامين حساب WhatsApp

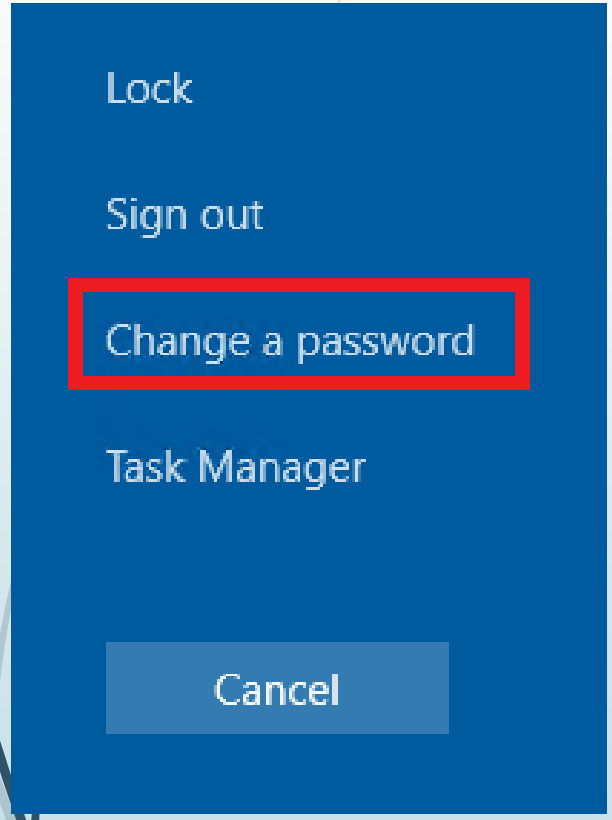
حماية Router من الاختراق

حماية Router

- تغير كلمة المرور الافتراضية
- تغير كلمة مرور Wi-Fi الافتراضية
- تغير اسم Wi-Fi وعدم تسميه باسم Router
- إيقاف خاصية WPS
- إيقاف خاصية Universal plug and play
- تعطيل برتوكول CWMPوالمسؤول عن تحكم مقدم الخدمة
- اختيار نظام تشفير قوي مثل WPA2
- كلمة سر معقدة
- تفعيل Firewall
- تفعيل خاصية MAC Filter
- مراجعة الأجهزة المتصلة كل فترة

في حالة الاختراق

طريقة تغيير كلمة السر

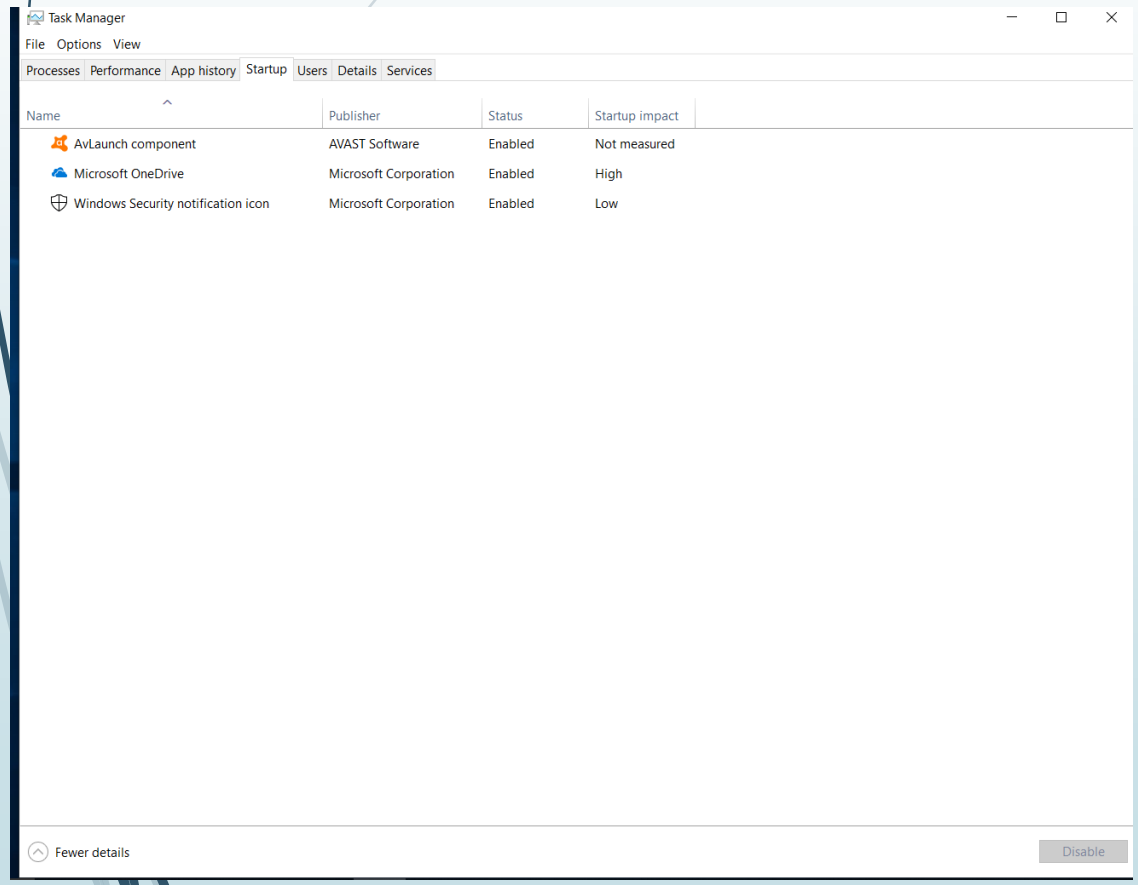


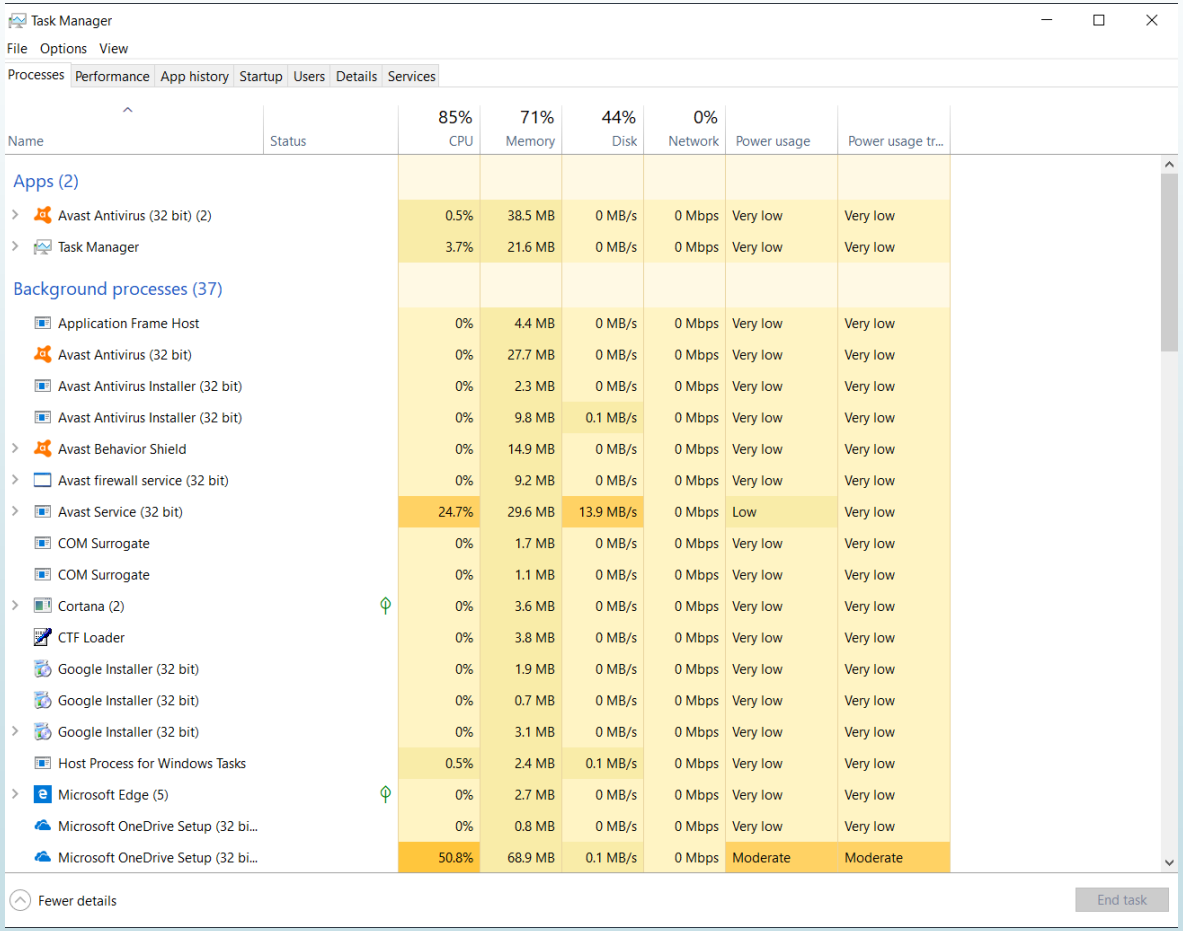
بعد الدخول علي جهاز الكمبيوتر الخاص بك قم علي الثلاث مفاتيح الثالثة التالية مرة واحدة مع بعضها البعض Ctrl + Alt + Del

ثم اختار **Change Password**

كيف تعرف ان جهاز به برنامج غير معروف المصدر

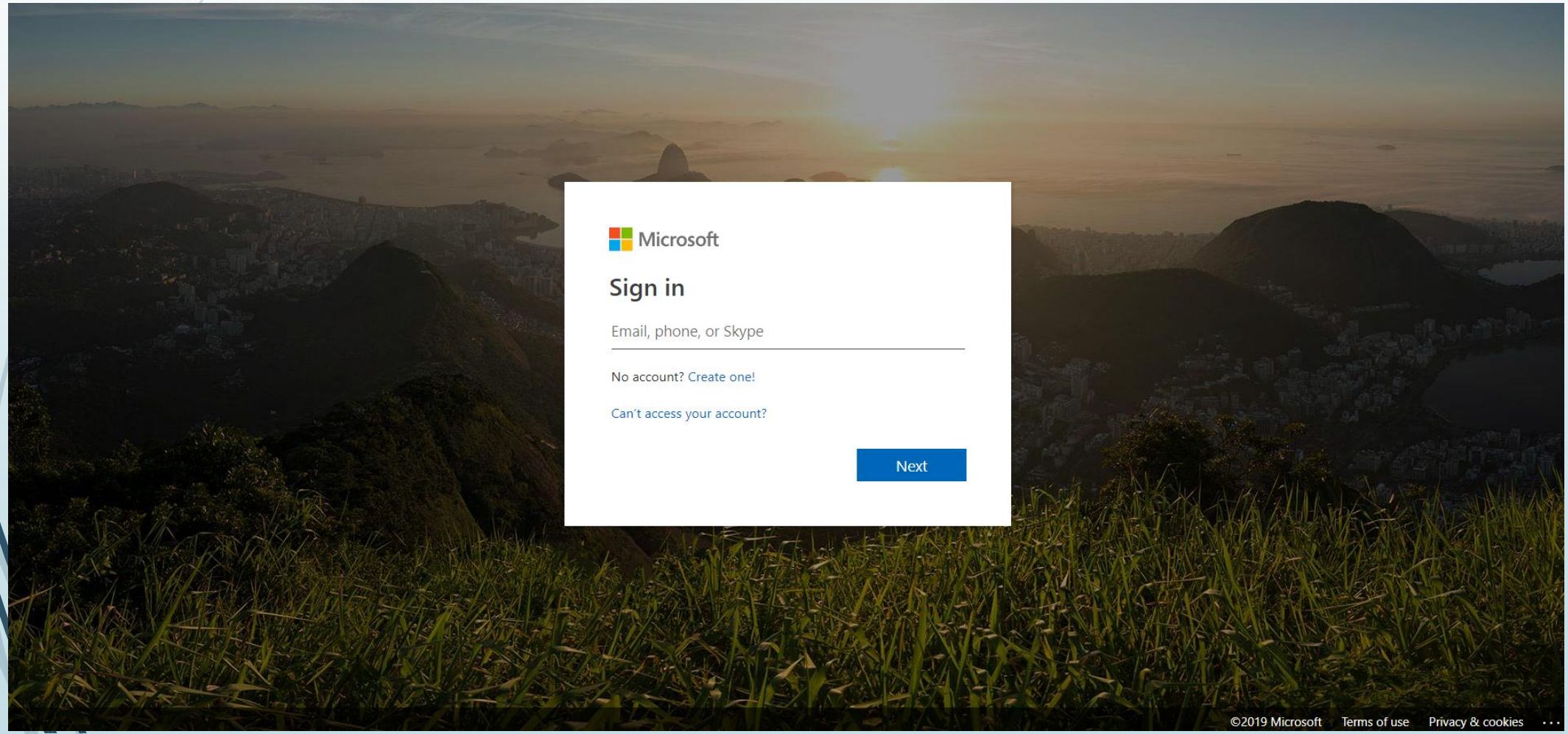
Task Manger





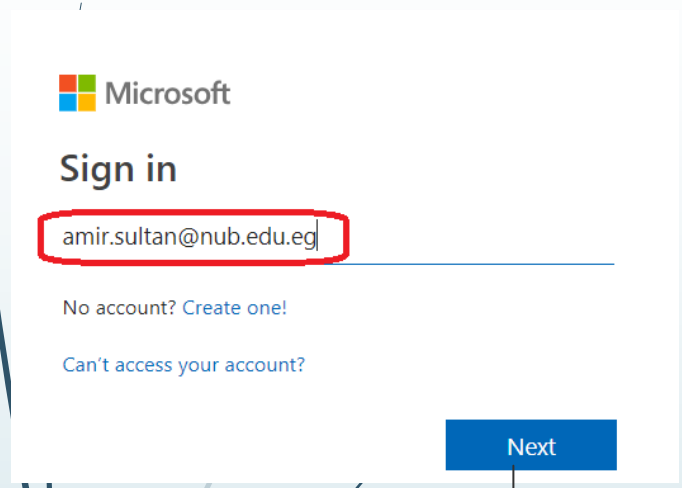
Office 365

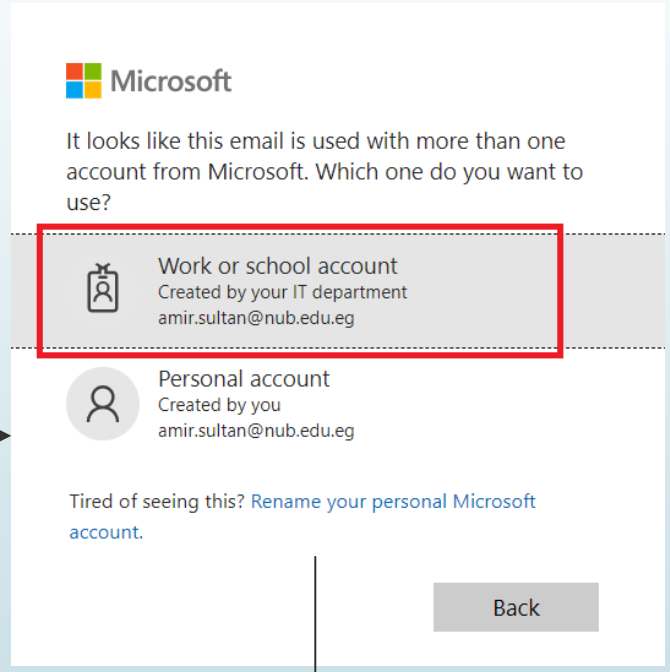
1- قم بفتح متصفح الانترنت Google Chrome او Firefox لزيارة الرابط التالي
Portal.office365.com

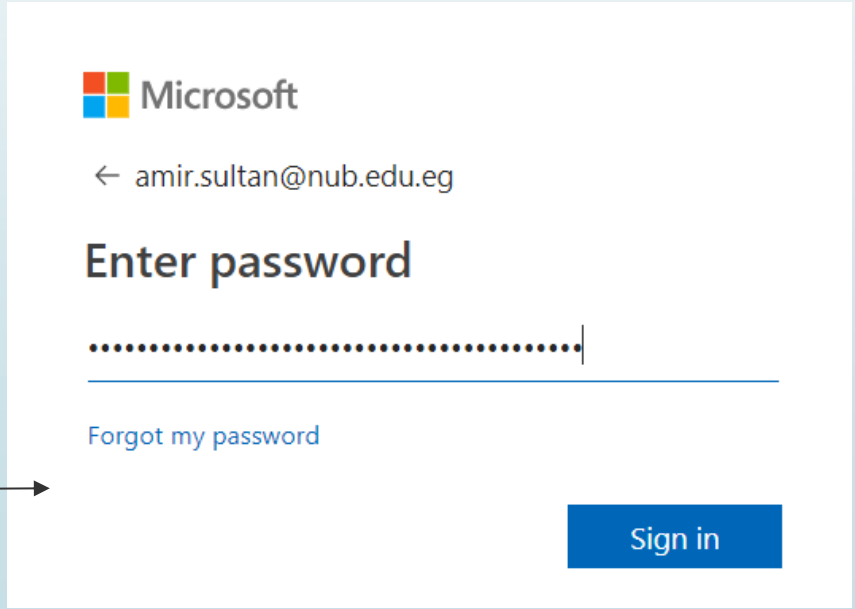


Office 365

2- قم بكتابة الحساب الخاص بك بشكل كامل

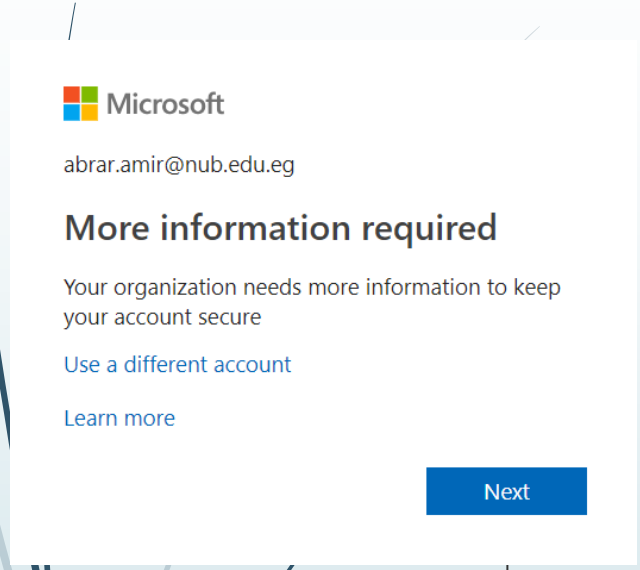


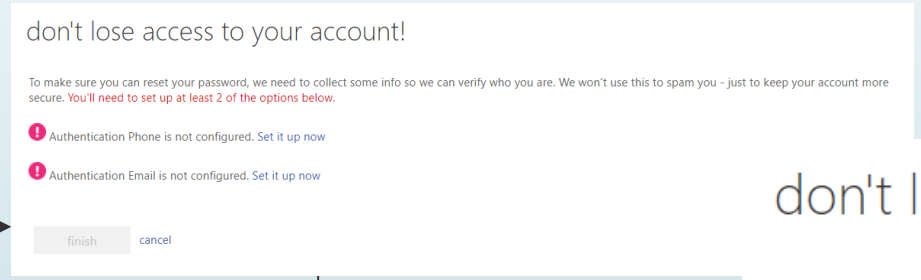


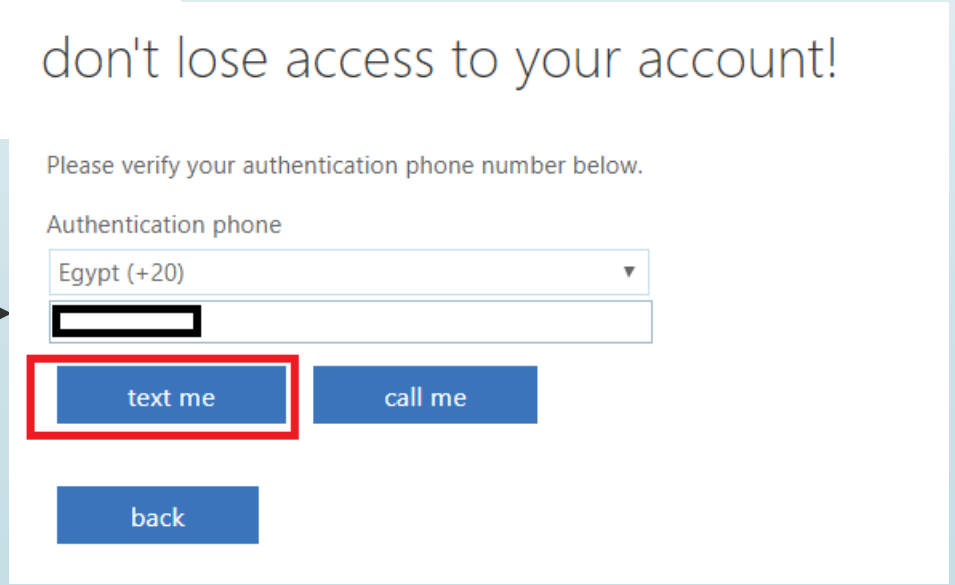


Office 365

3- استكمال باقي البيانات لتامين الحساب

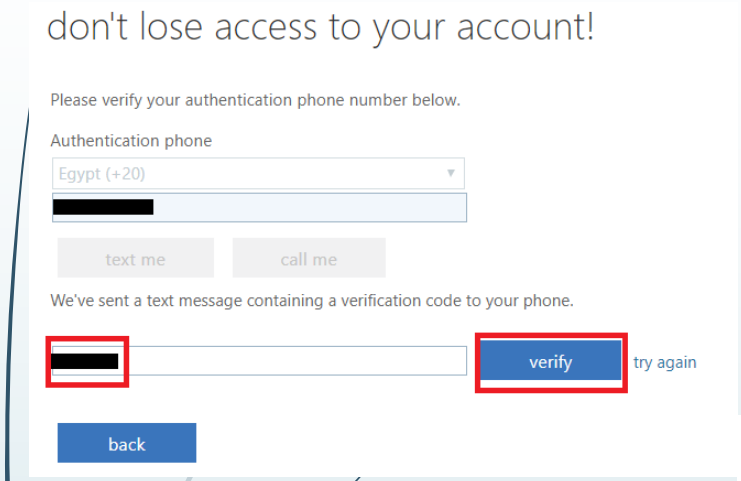


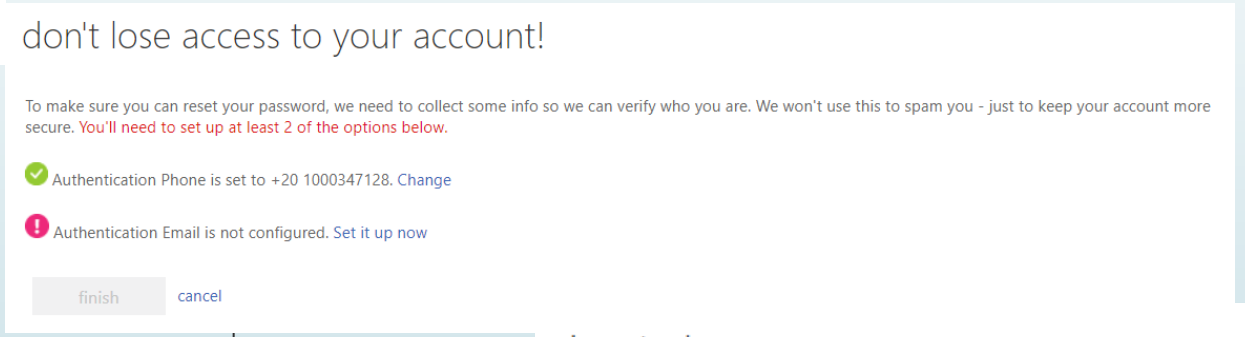


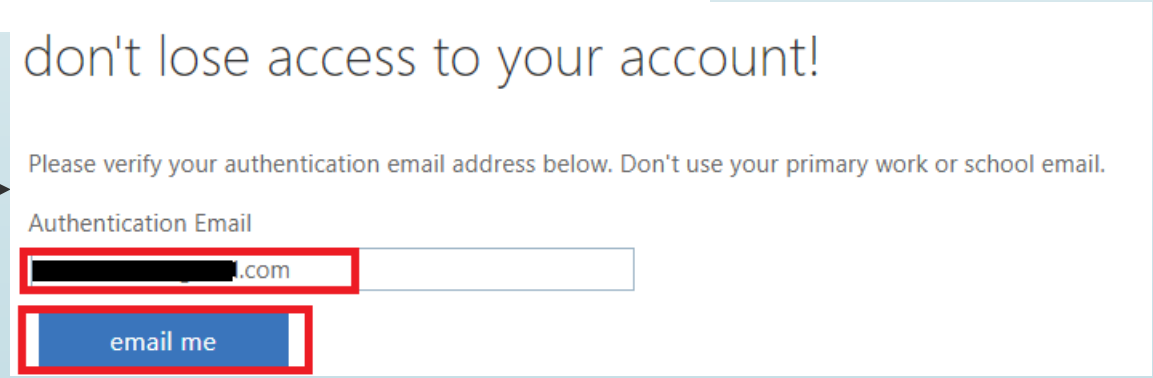


Office 365

تابع استكمال باقي البيانات لتامين الحساب

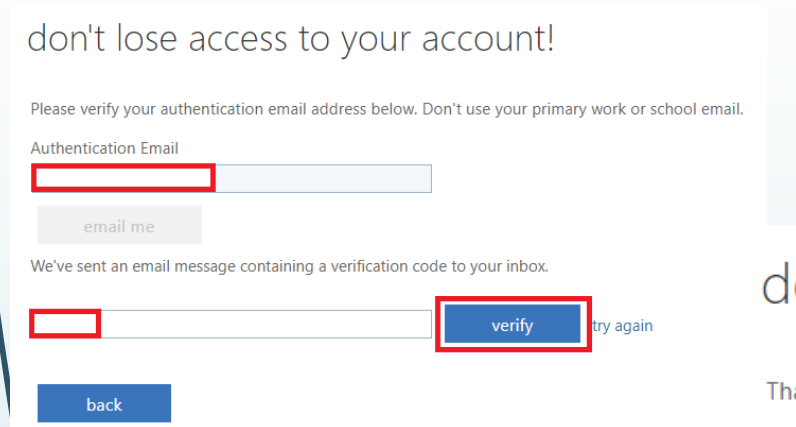


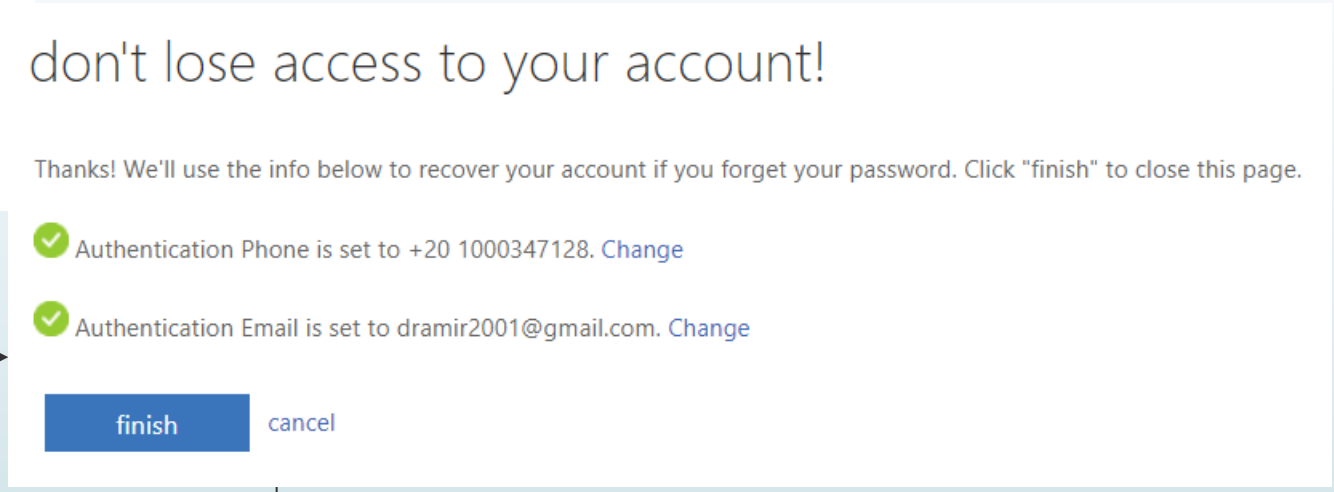


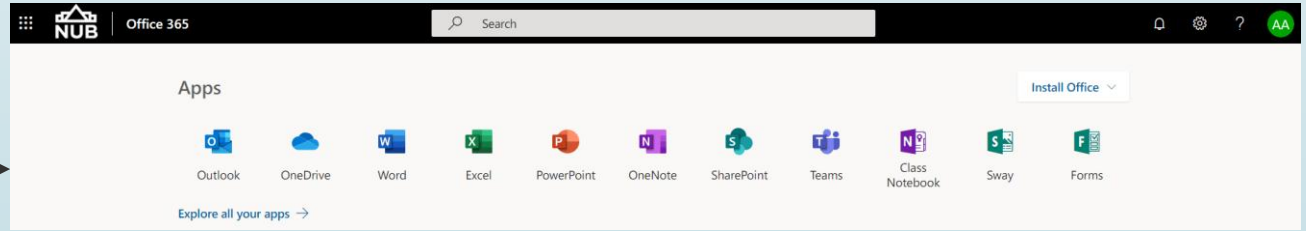


Office 365

تابع استكمال باقي البيانات لتامين الحساب

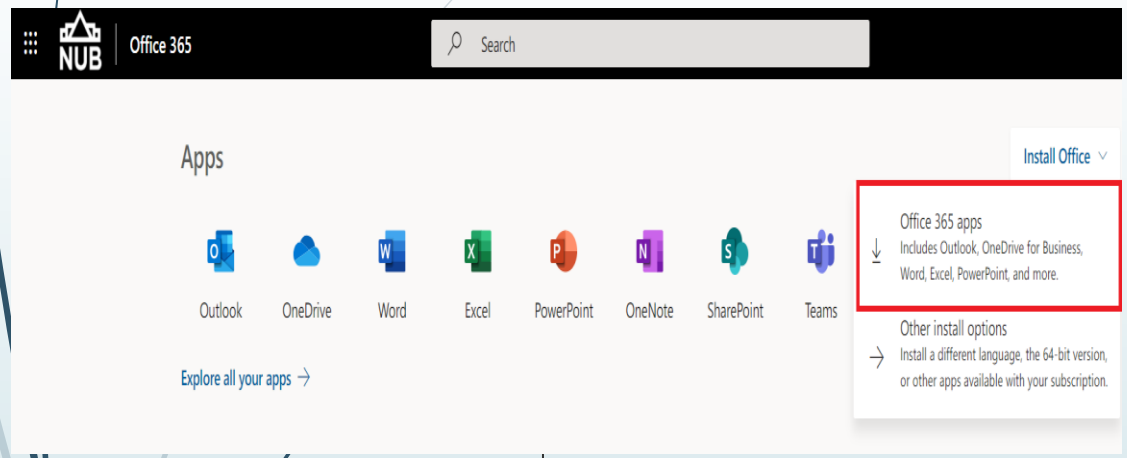


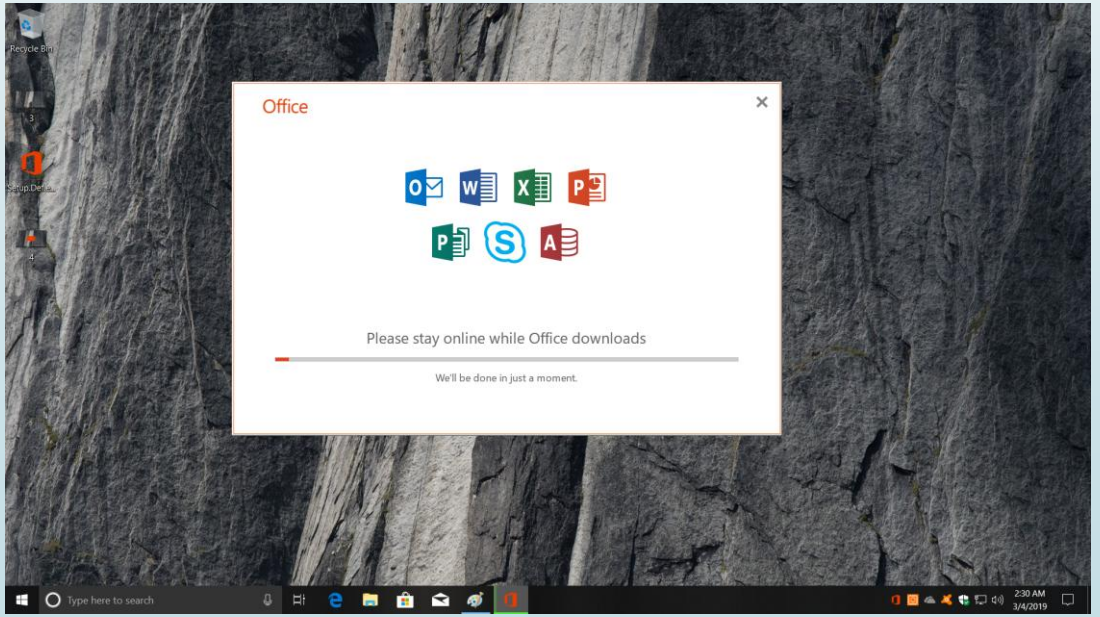




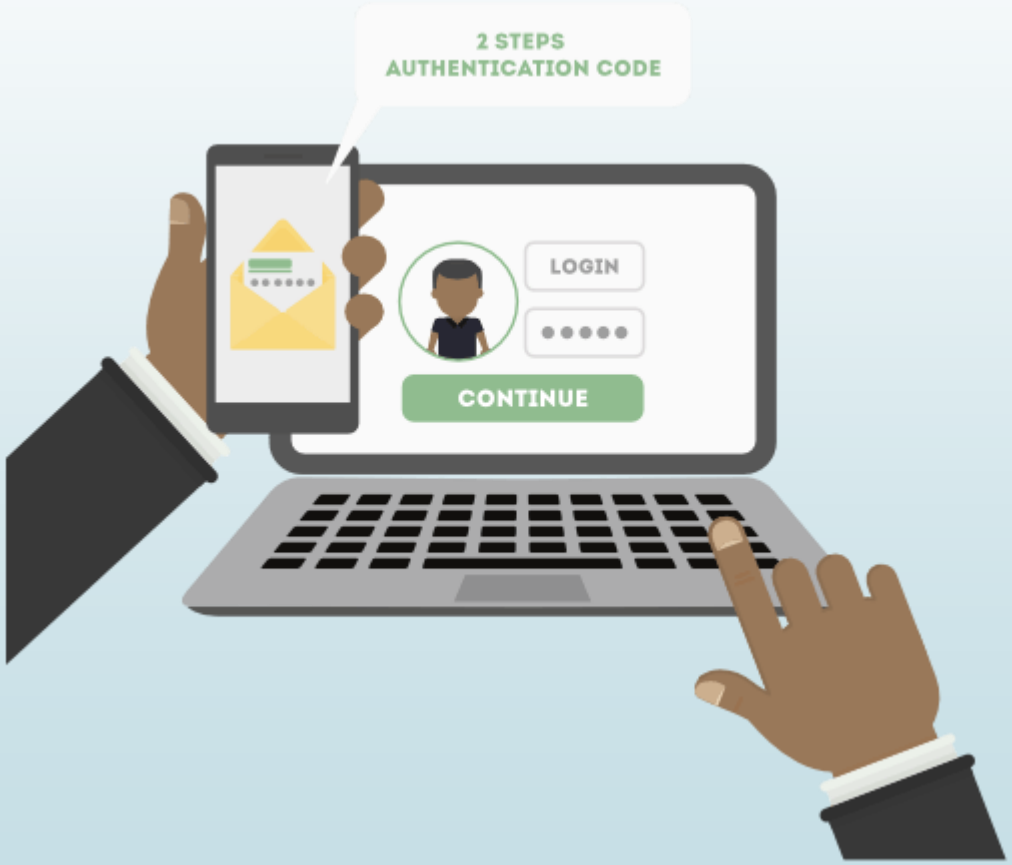
Office 365

الحصول علي احدث اصدار من ميكروسوفت اوفيس





طريقة تفعيل التحقق بخطوتين

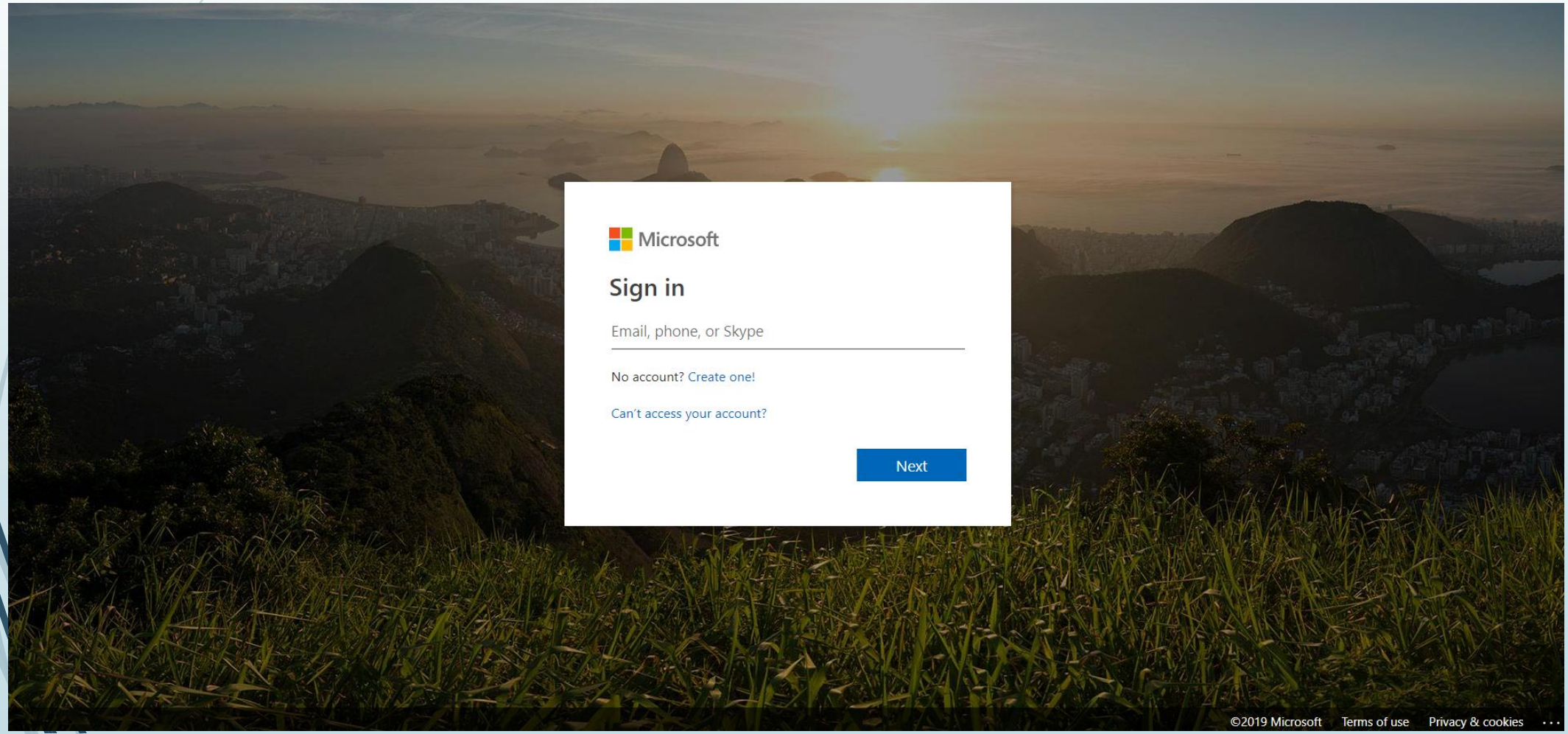


طريقة تفعيل التحقق بخطوتين

في البداية يجب تحميل برنامج Microsoft Authenticator by Microsoft Corporation

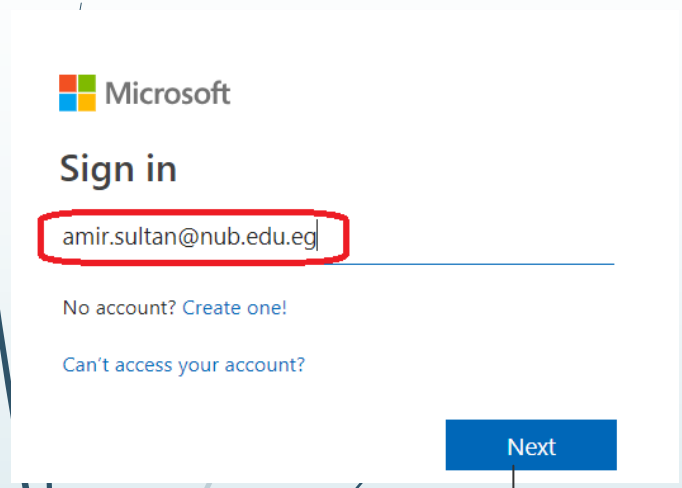
تفعيل التحقق بخطوتين

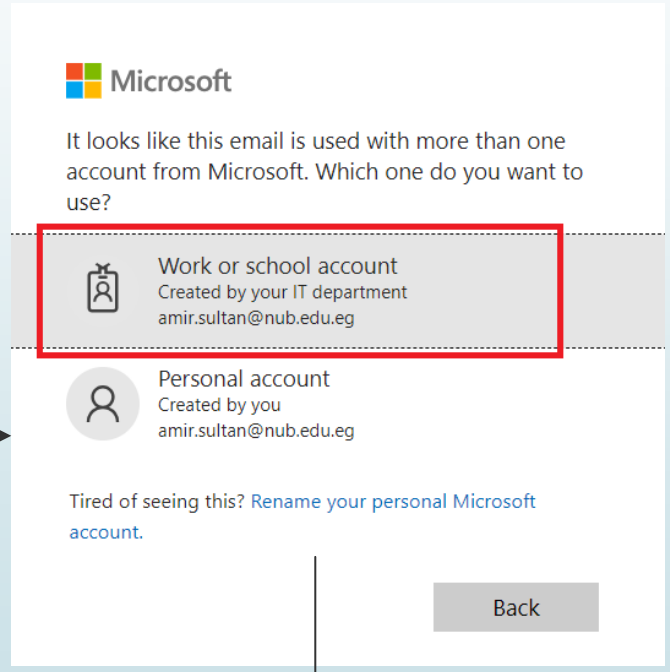
1- قم بفتح متصفح الانترنت Google Chrome او Firefox لزيارة الرابط التالي Portal.office365.com

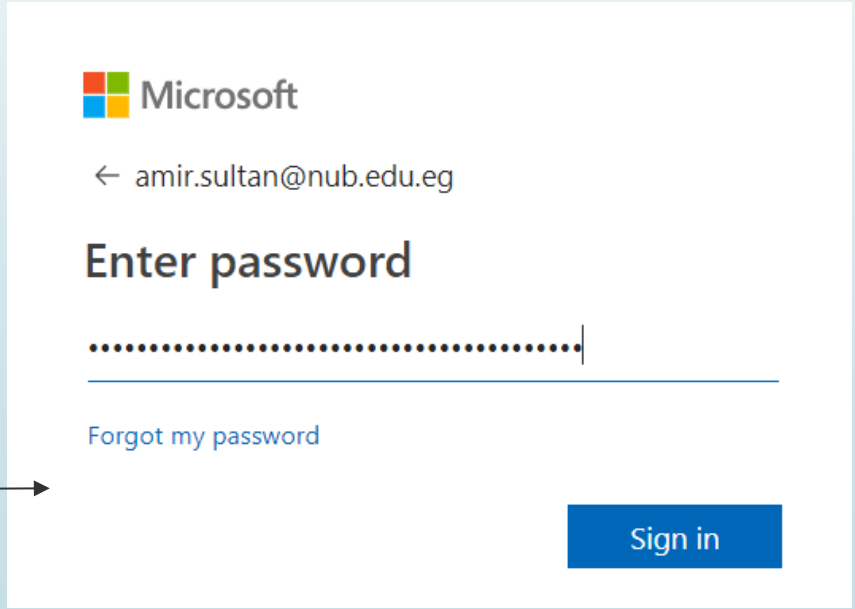


تفعيل التحقق بخطوتين

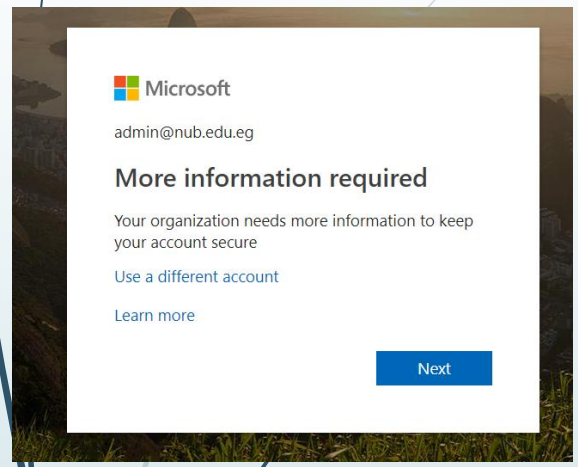
2- قم بكتابة الحساب الخاص بك بشكل كامل



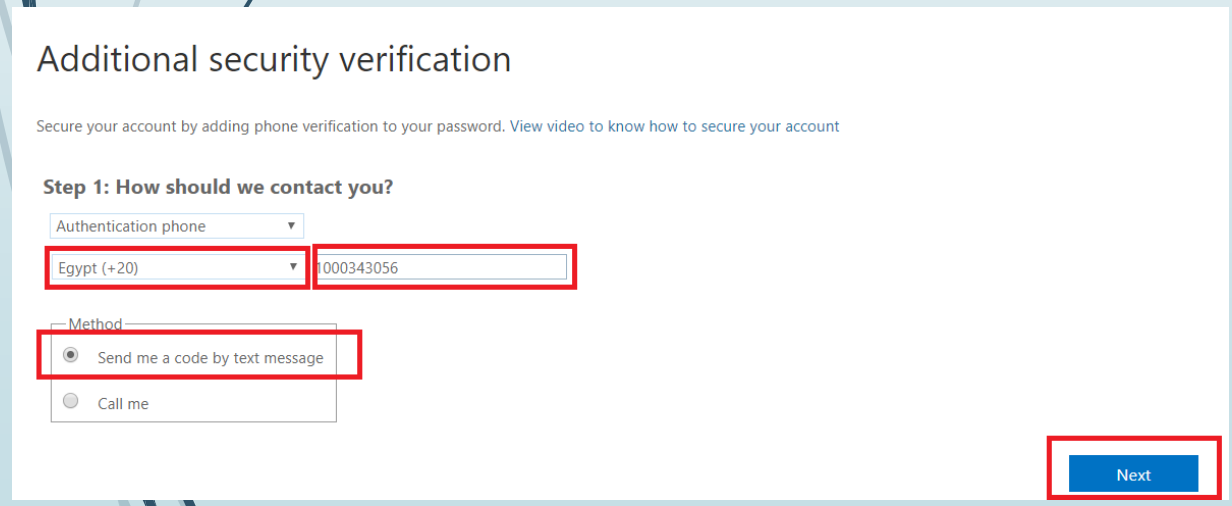


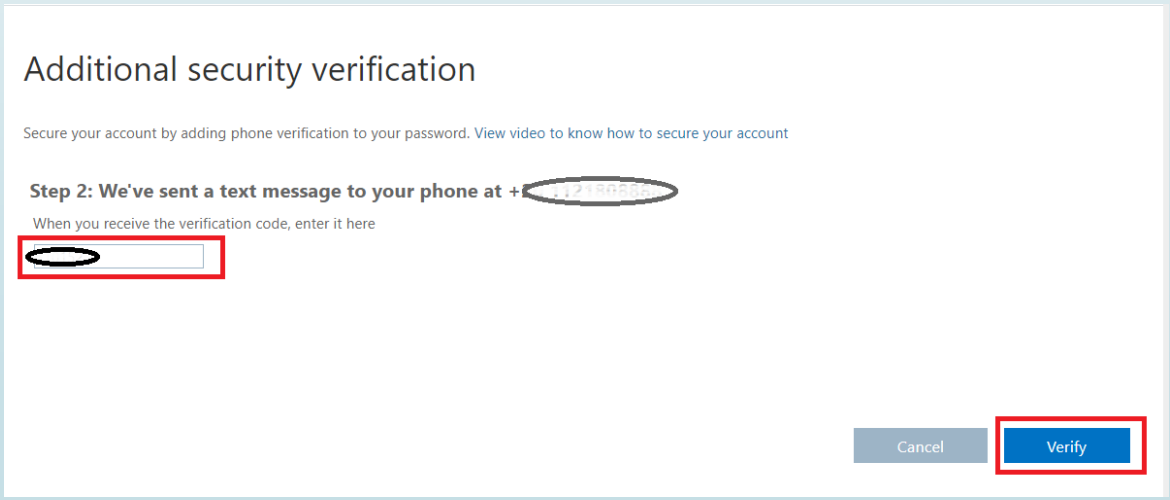


تفعيل التحقق بخطوتين

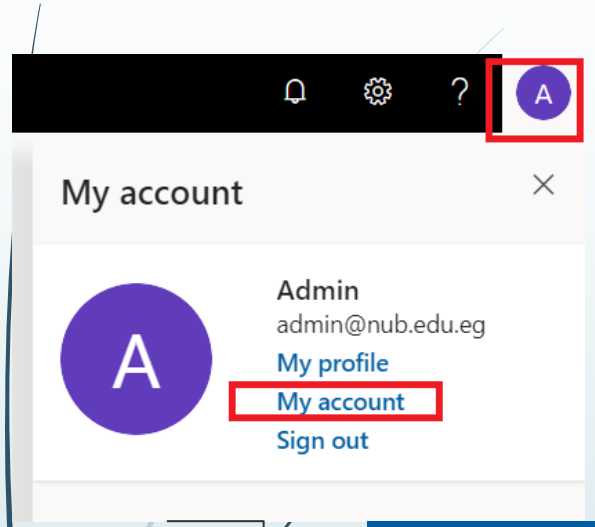


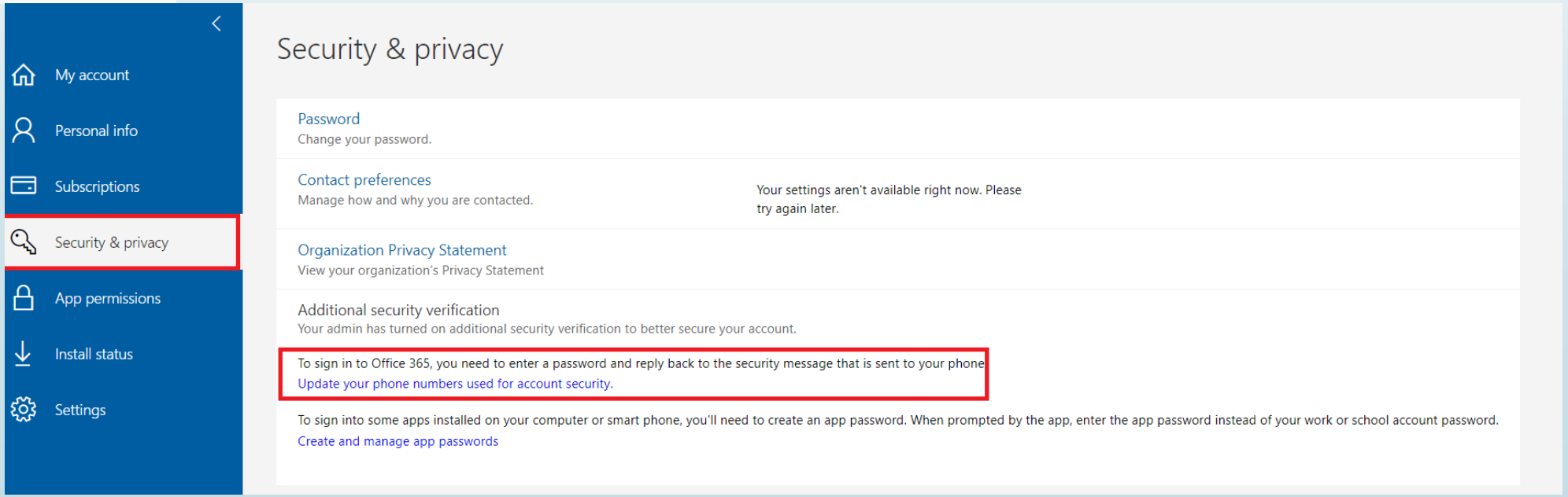
بمجرد قبول الطلب والدخول علي الحساب سوف تظهر تلك الرسالة والتي تتطلب منك استكمال البيانات لتفعيل ميزة التحقق المزدوج



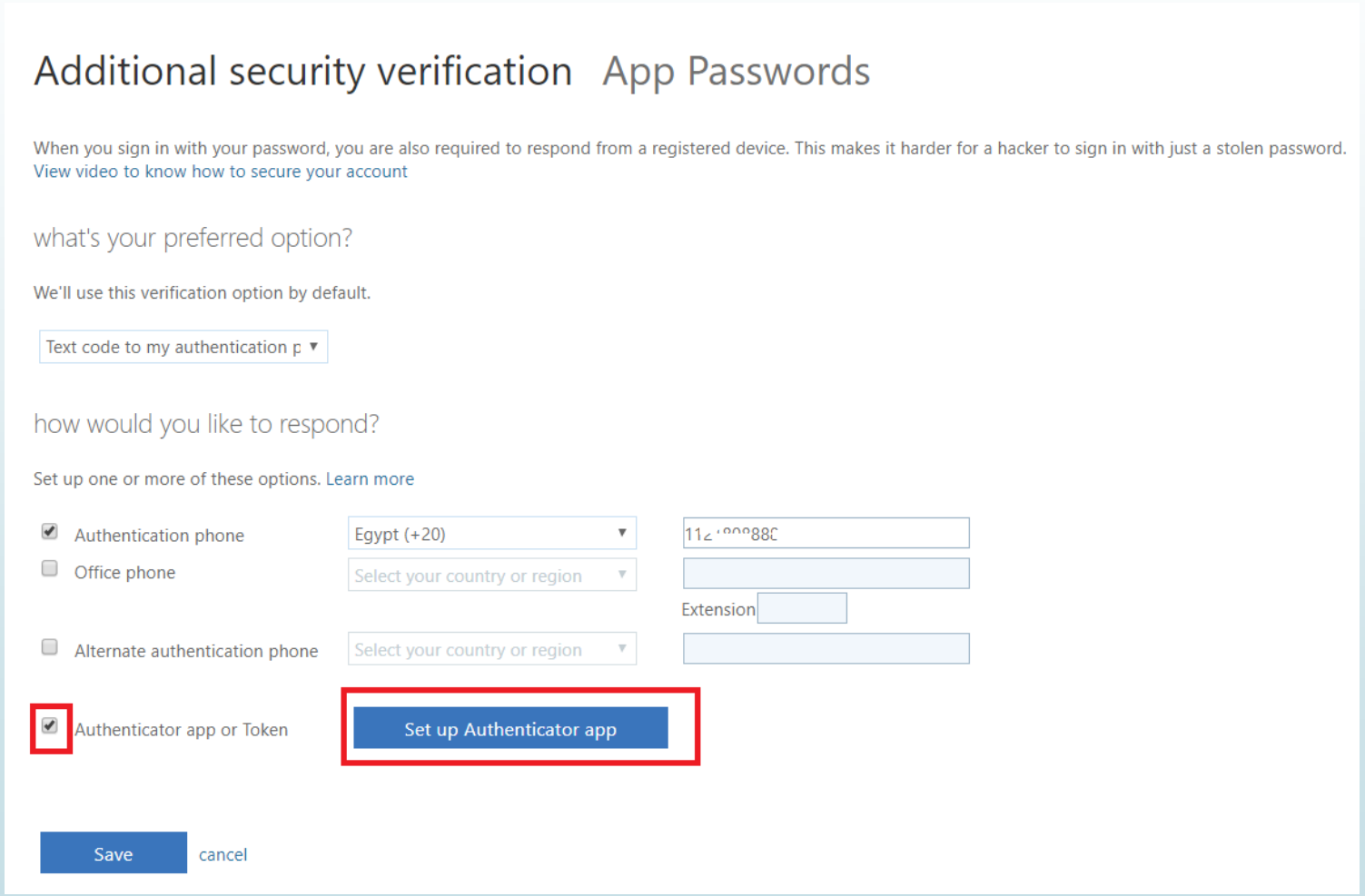


طريقة تفعيل التحقق بخطوتين



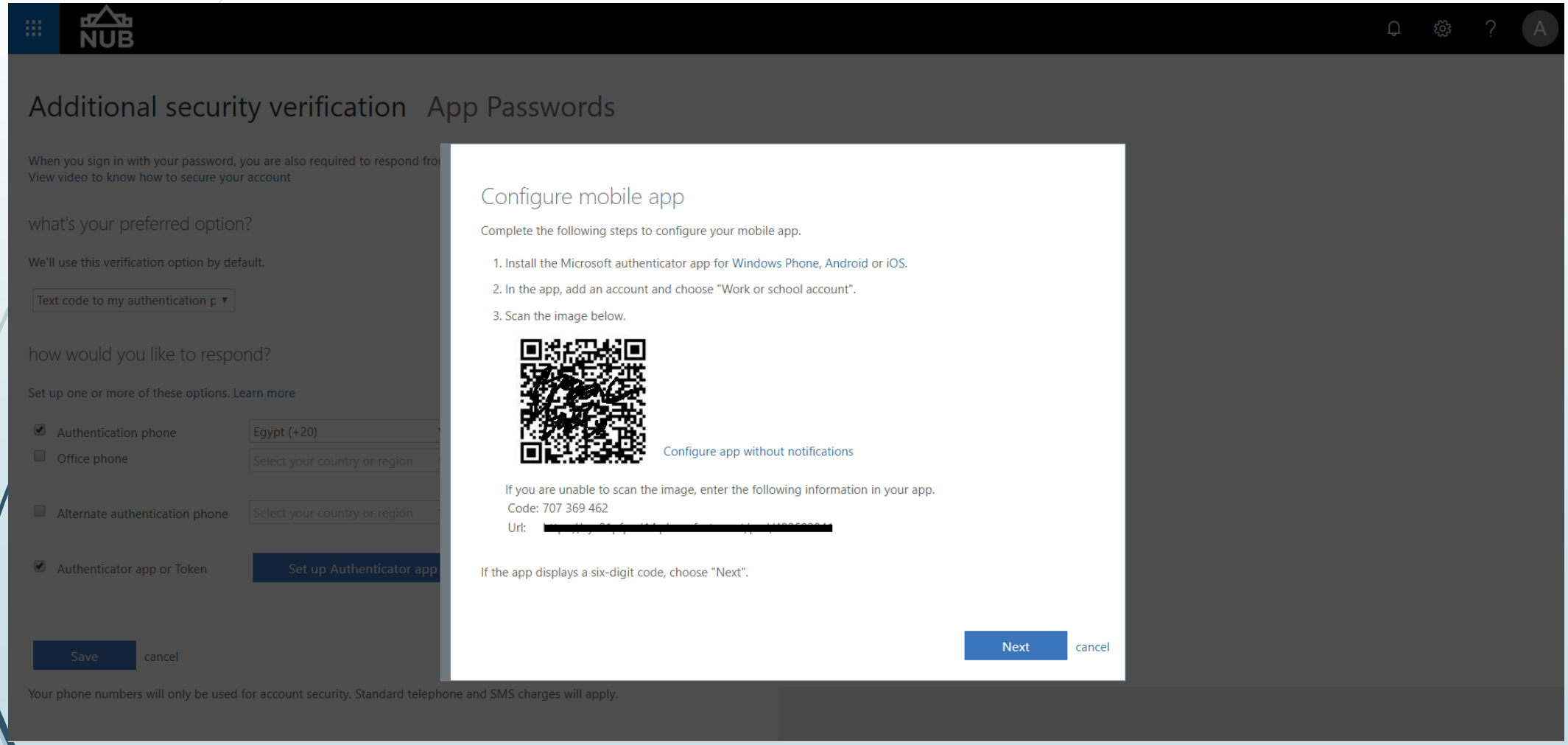


طريقة تفعيل التحقق بخطوتين



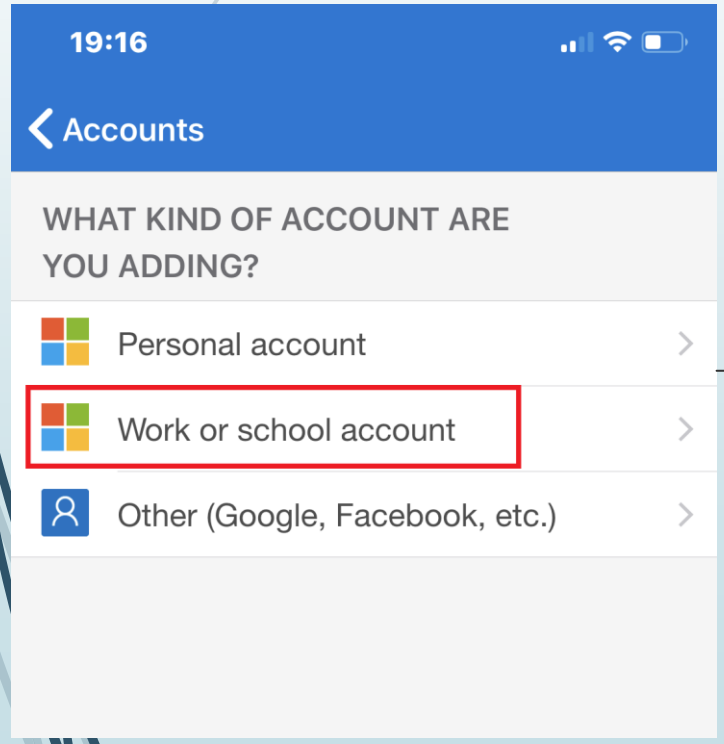
طريقة تفعيل التحقق بخطوتين

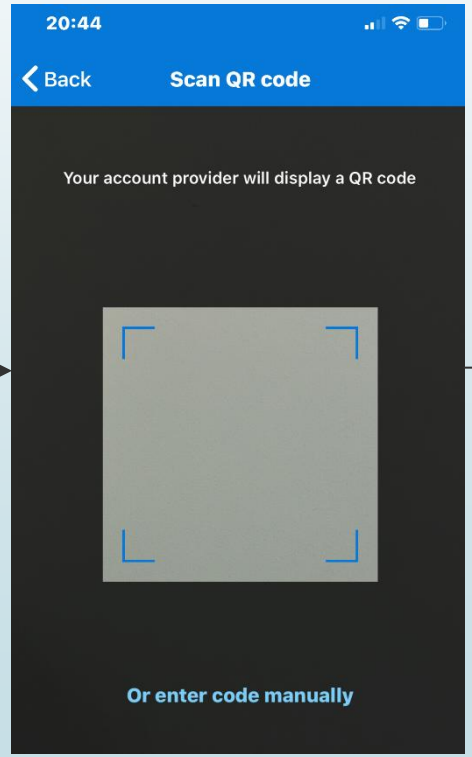
قم بفتح التطبيق الذي تم تحميل علي الموبايل
وجعل التطبيق QR-Code



طريقة تفعيل التحقق بخطوتين

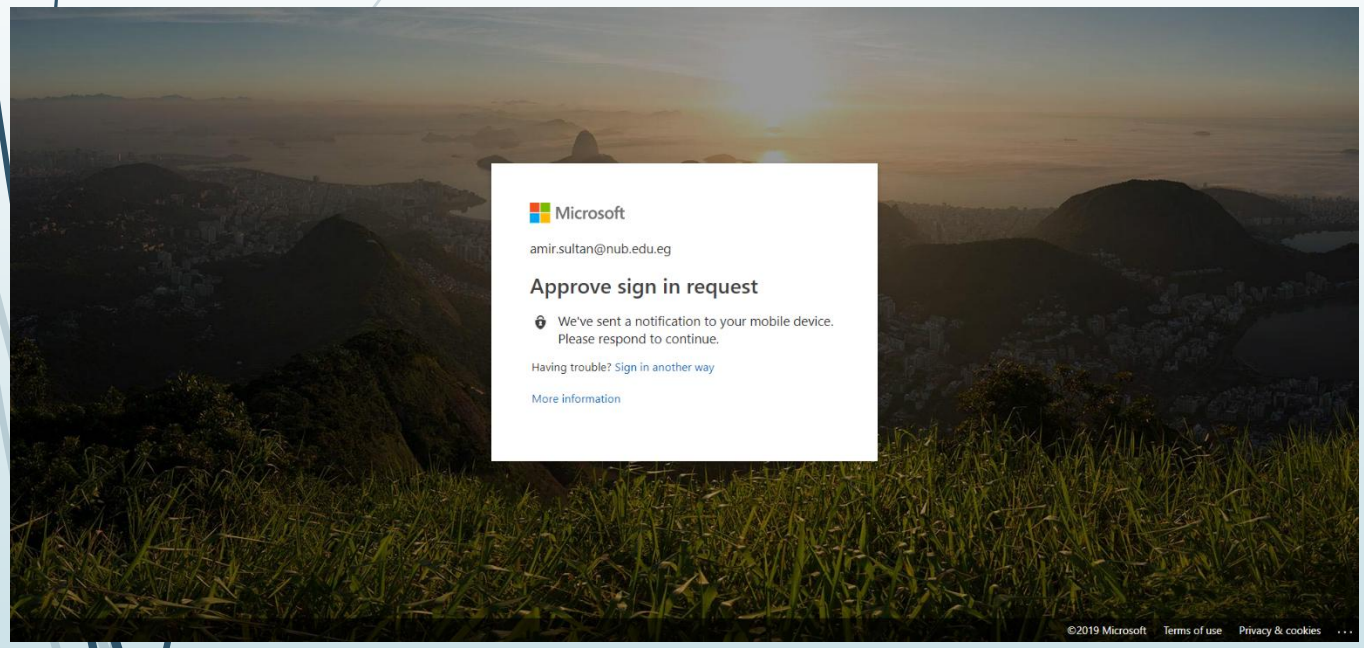
- قم بفتح التطبيق الذي تم تحميل على التليفون Microsoft Authenticator
- ثم اختيار علامة + ثم اختيار Work or School
- قم بتقريب الموبايل من شاشة الكمبيوتر ليقوم بمسح QR-Code الموجود علي شاشة الكمبيوتر



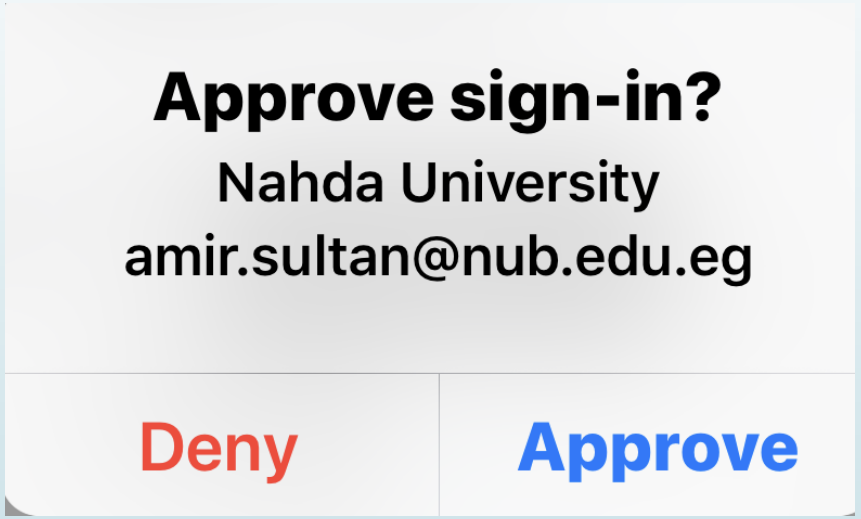


طريقة تفعيل التحقق بخطوتين

- بمجرد انهاء الاعدادات وعن الدخول مرة اخري علي حسابك الالكتروني سوف يصل لك اشعار علي الموبايل لإتمام عملية الدخول ولن يسمح بالدخول الا بعد الضغط علي **Approve**



شاشة الكمبيوتر في انتظار اعتماد الموافقة من علي الموبايل



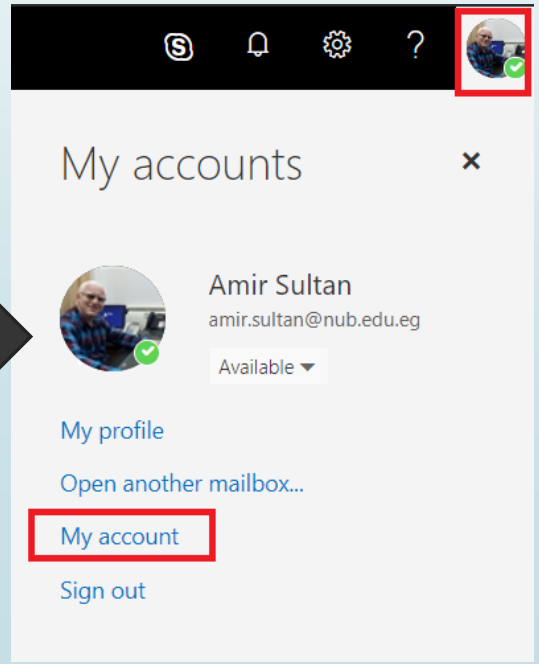
القبول والرفض من شاشة الموبايل

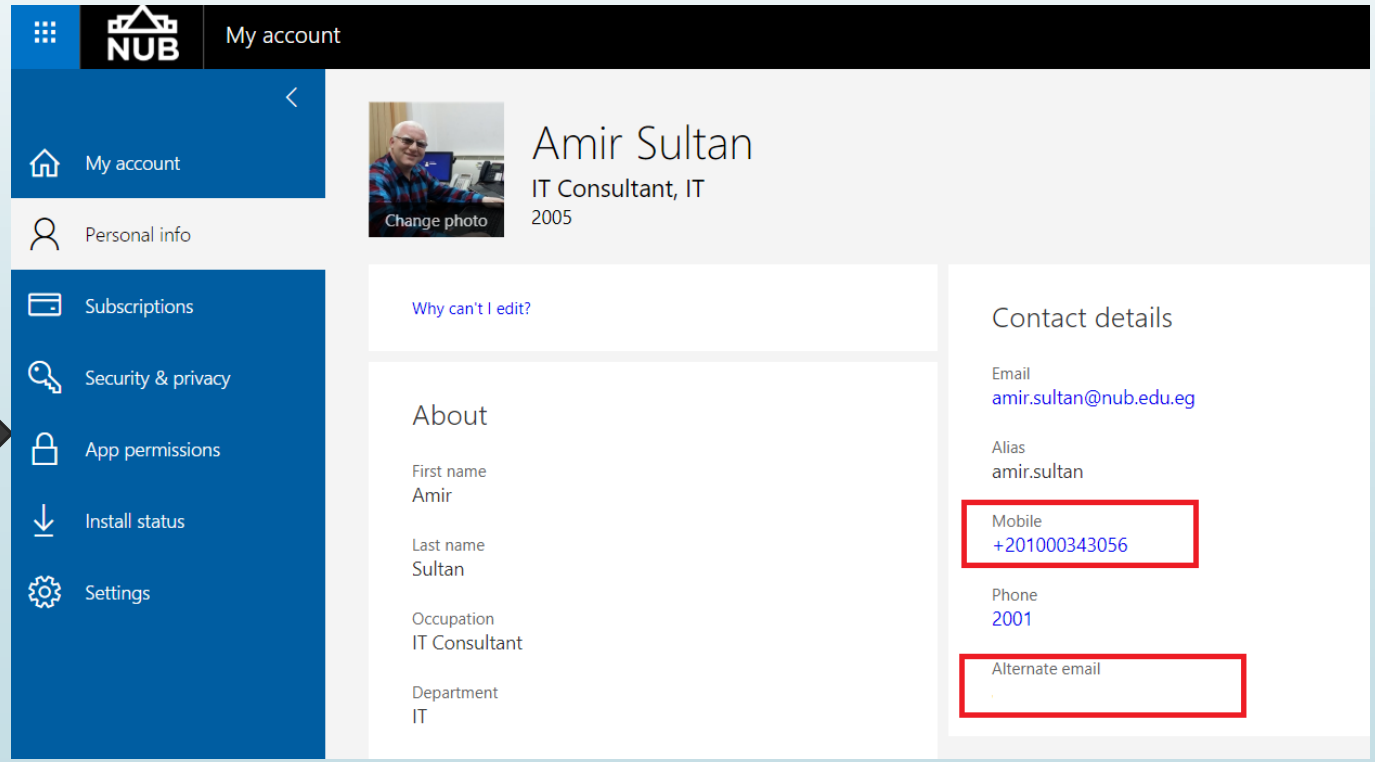
مراجعة إعدادات حسابك

تفقد إعدادات حسابك

التأكيد علي عدم تغير بياناتك الأساسية

Personal Info (Alternate Email, Mobile)

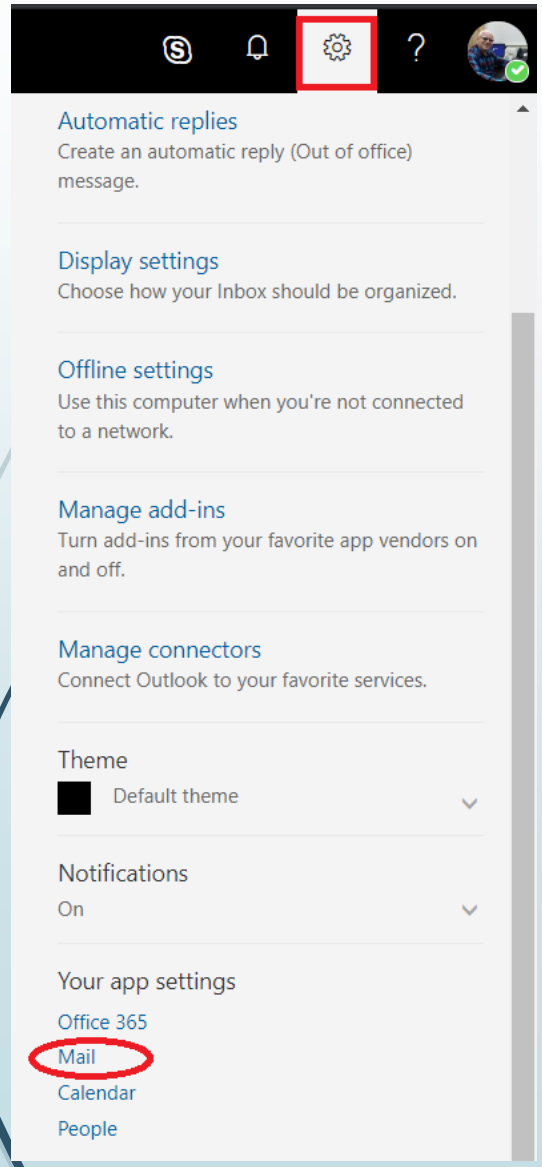


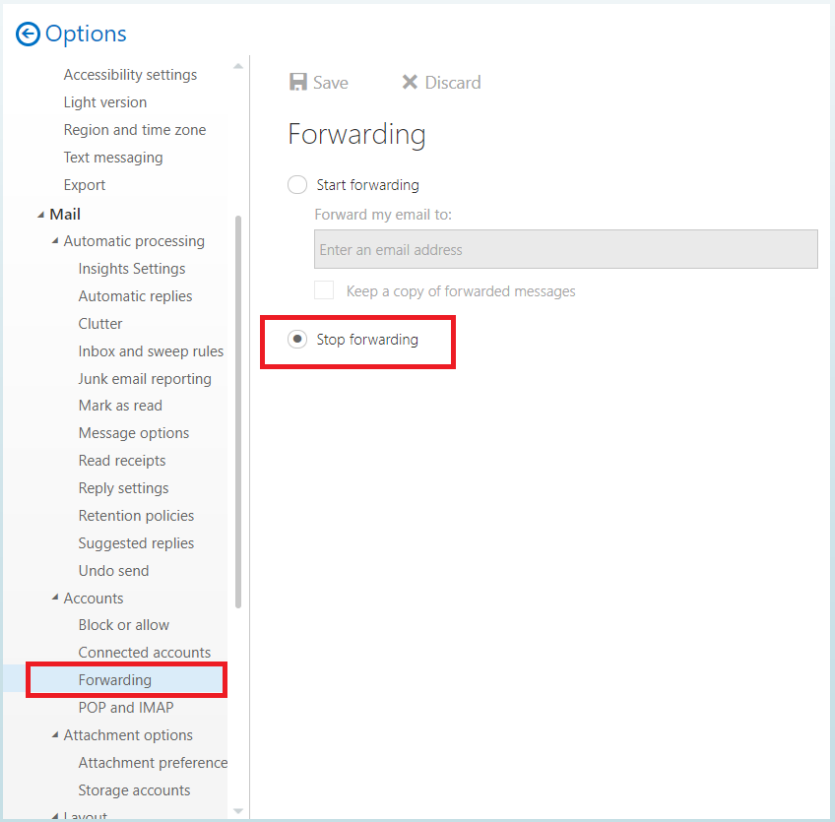


مراجعة إعدادات حسابك

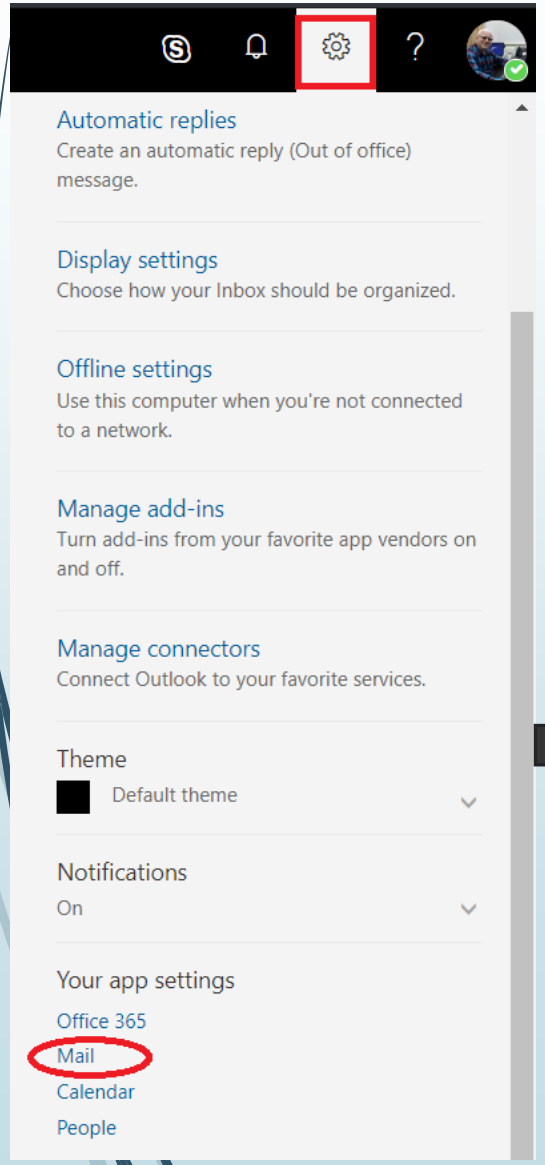
تفقد إعدادات حسابك

التأكيد علي عدم وجود Auto forwarding



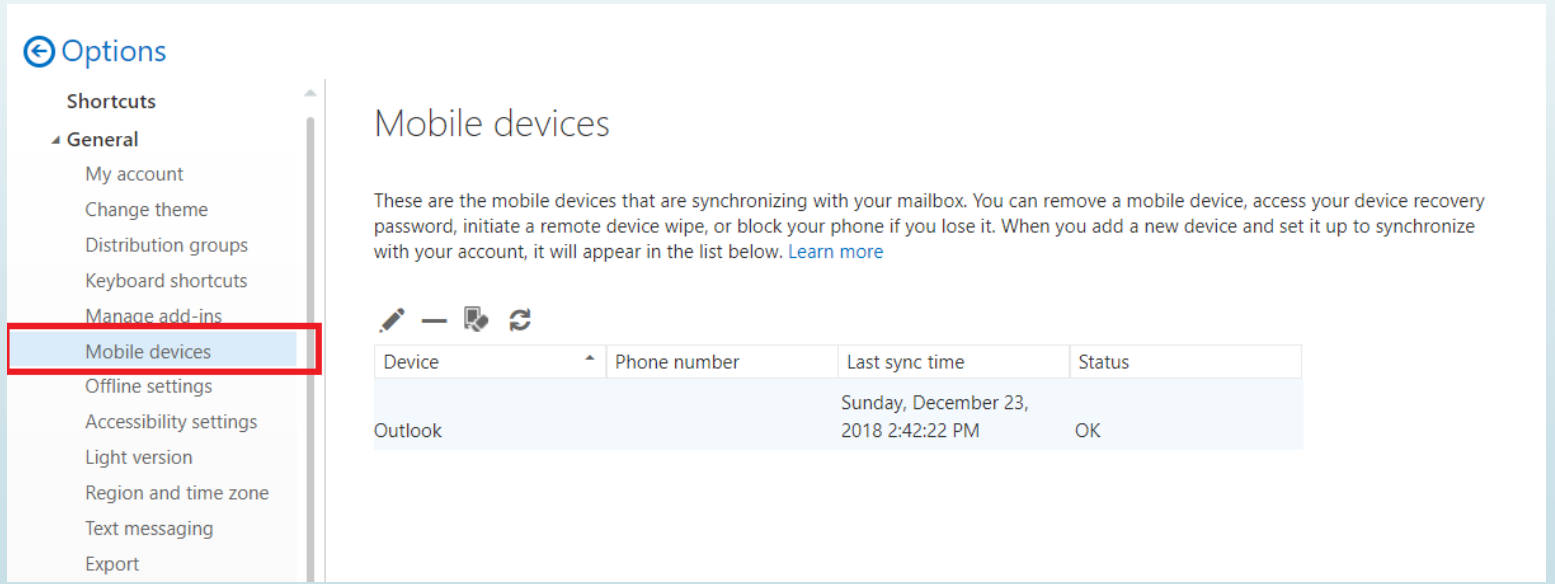


مراجعة إعدادات حسابك



تفقد إعدادات حسابك

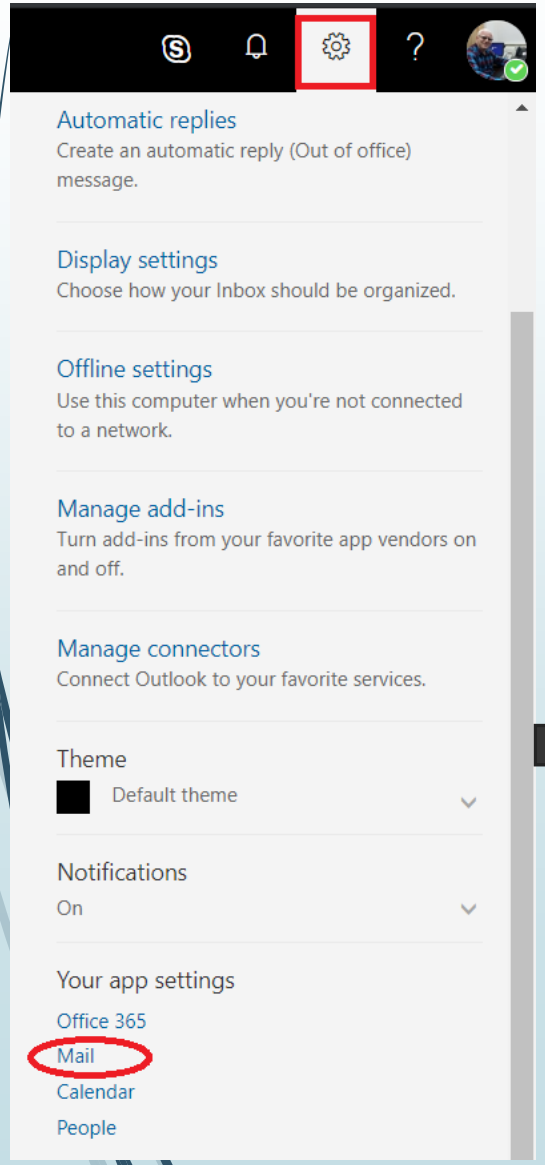
مراجعة الأجهزة المتصلة بحسابك وحذف أي جهاز غير معروف

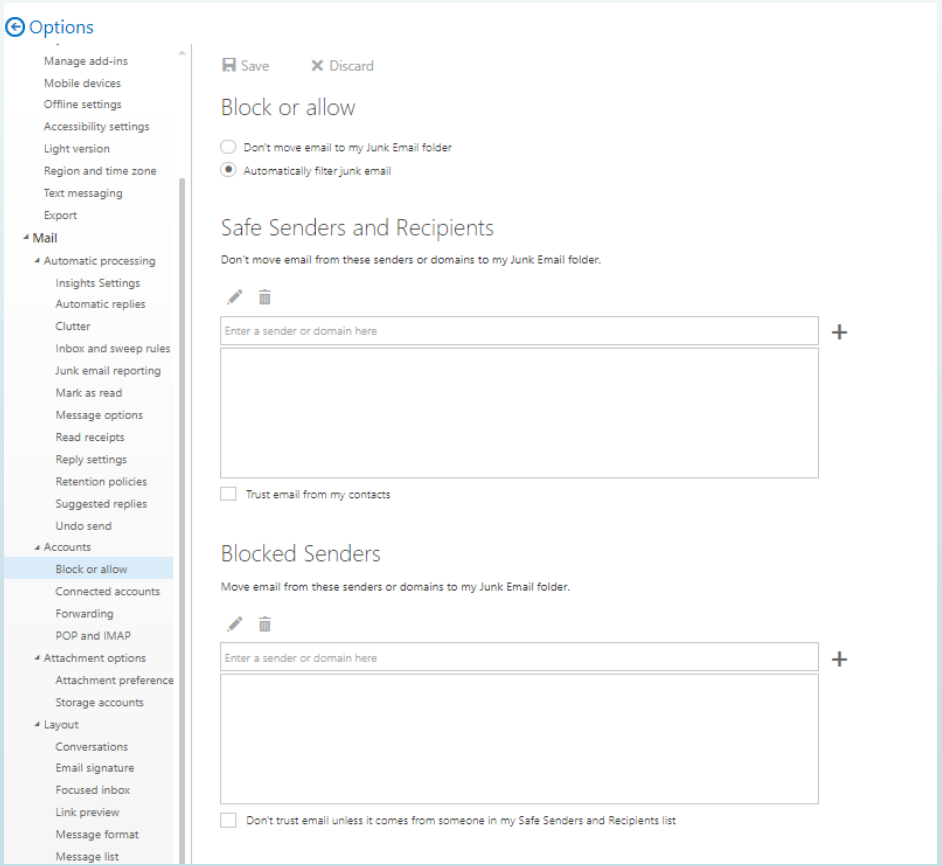


مراجعة إعدادات حسابك

تفقد إعدادات حسابك

مراجعة الجهات الممنوعة

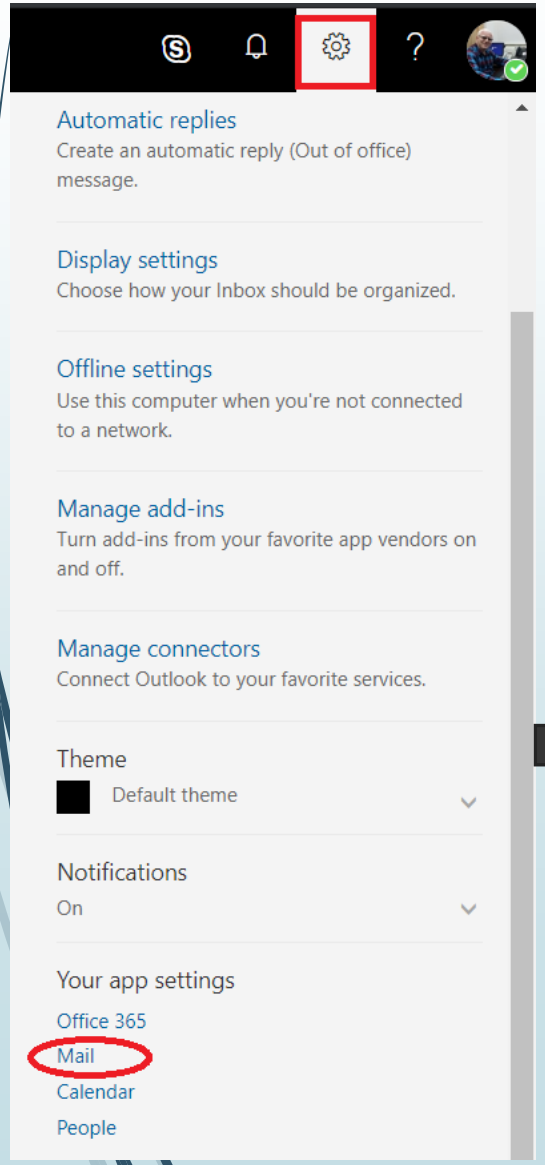


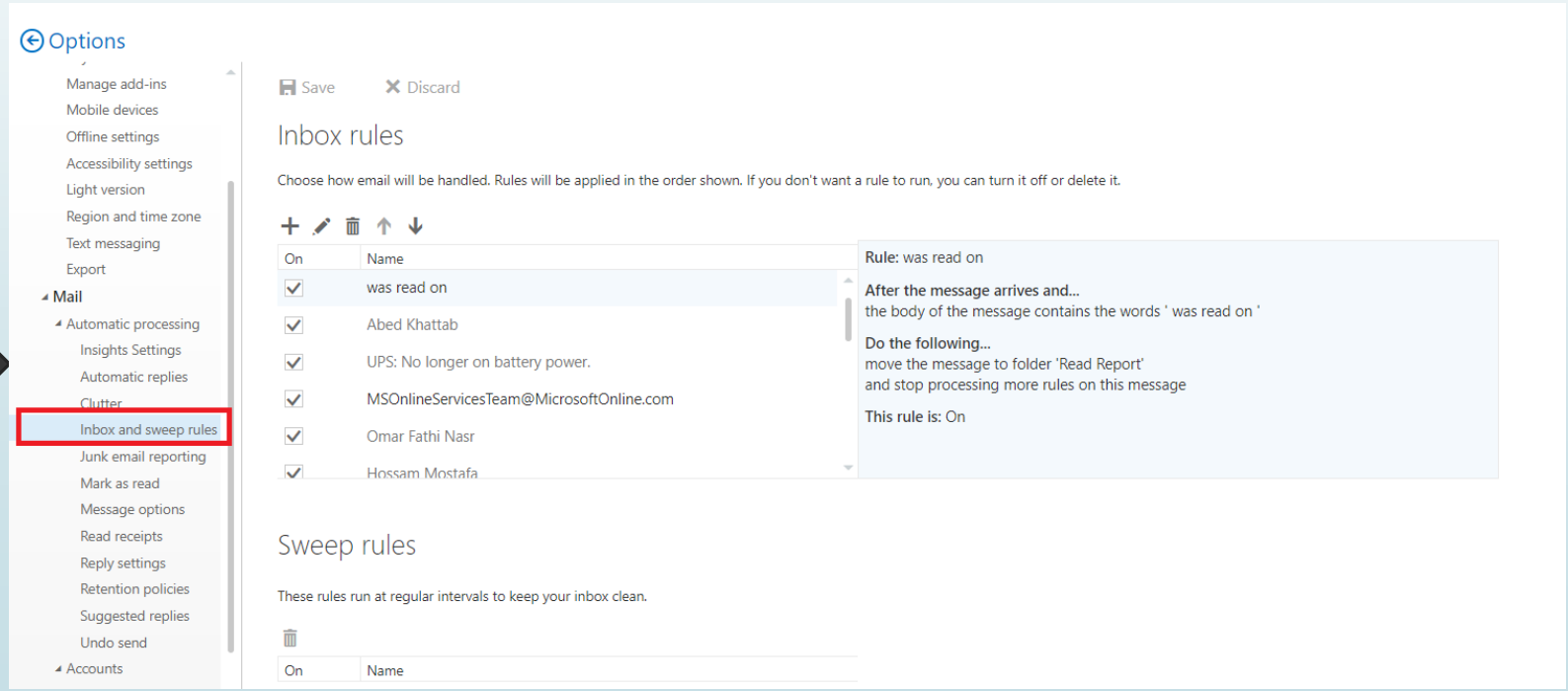


في حالة الاختراق

تفقد إعدادات حسابك

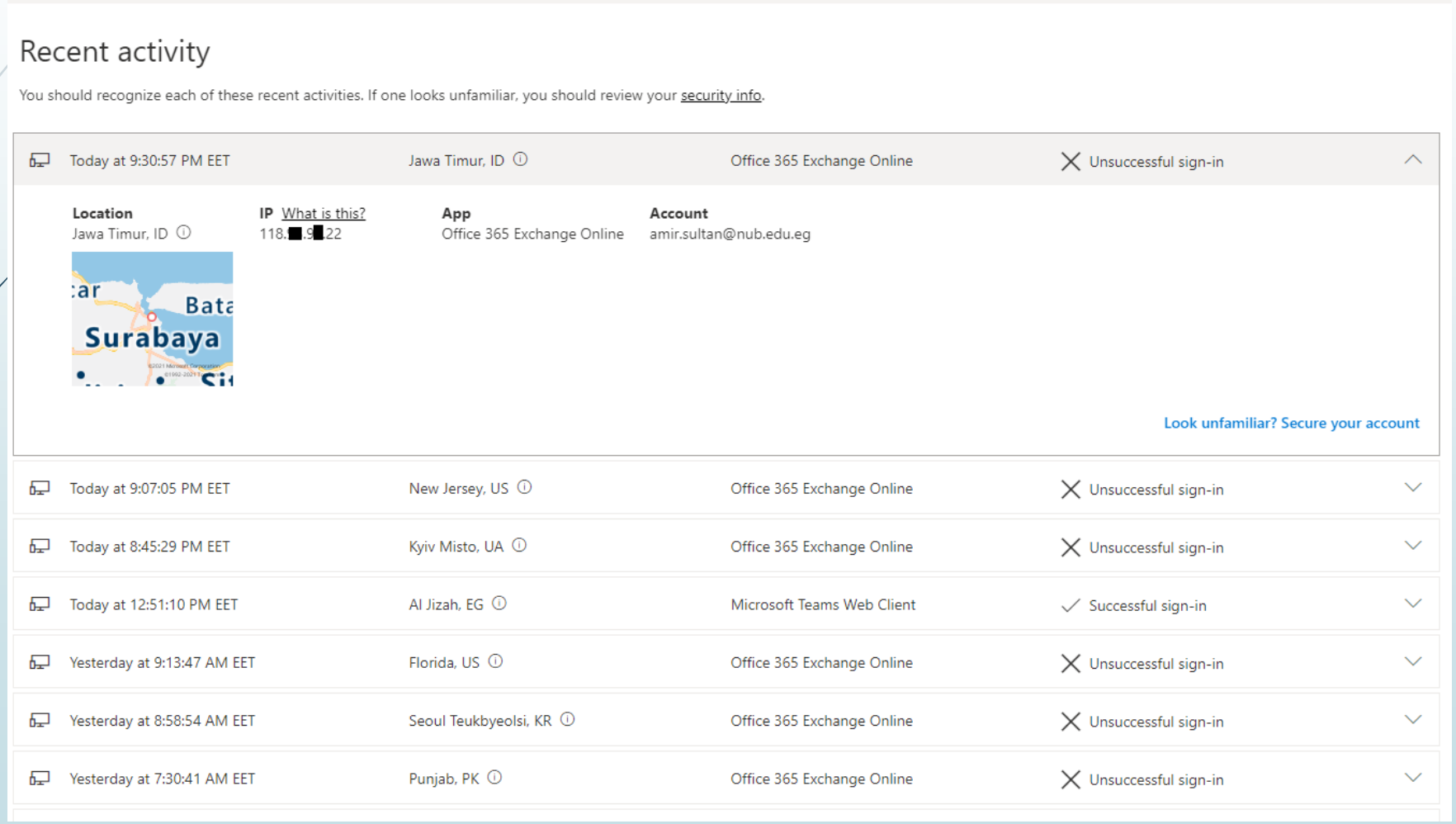
مراجعة القواعد والإجراءات



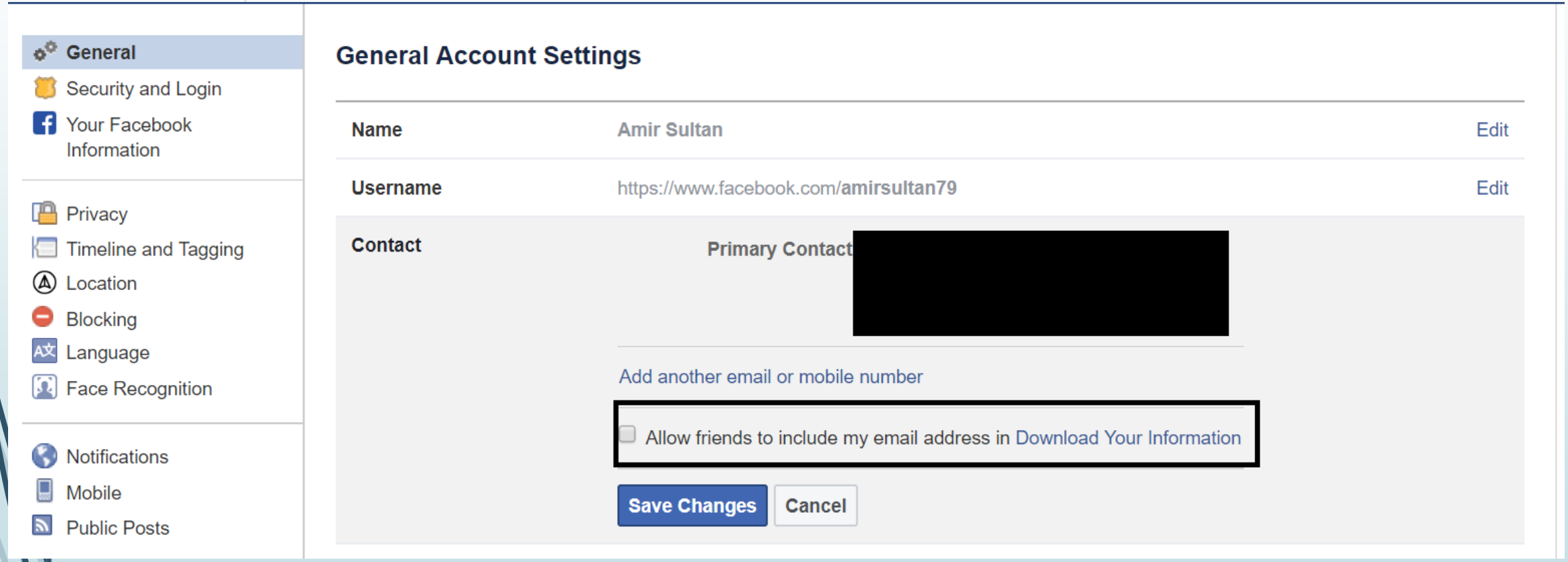


في حالة الاختراق

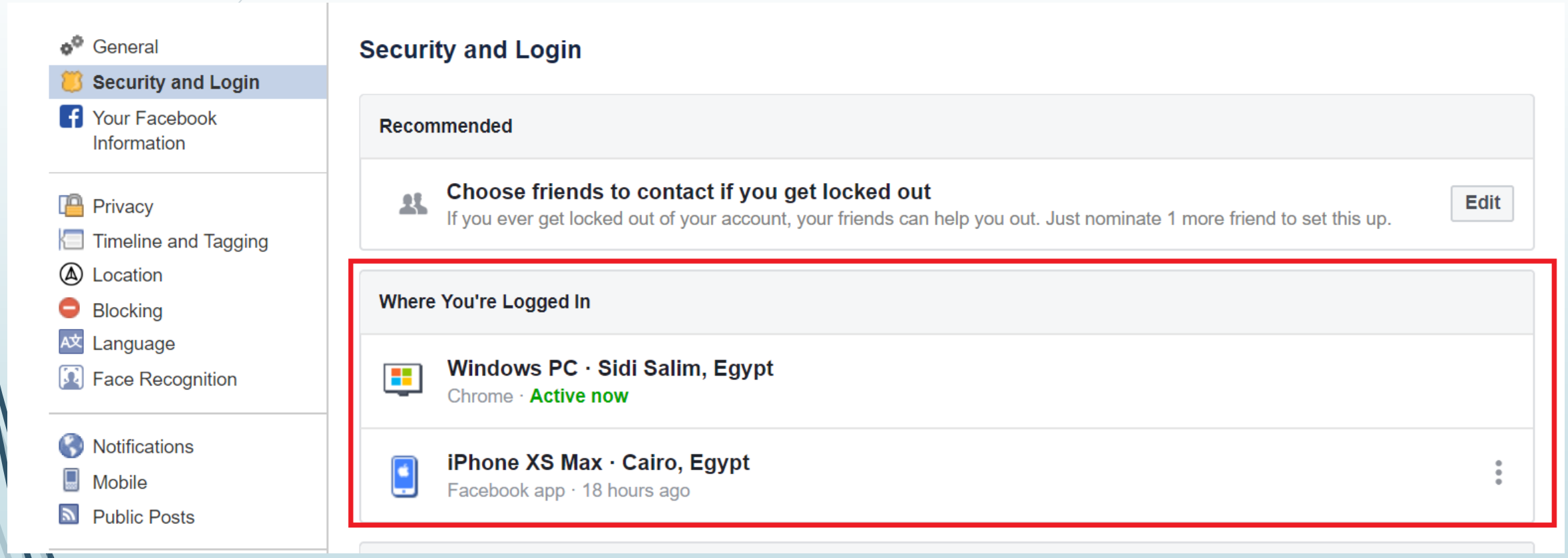
مراجعة تسجيل الدخول والابلاغ عن وجود نشاط غير معروف



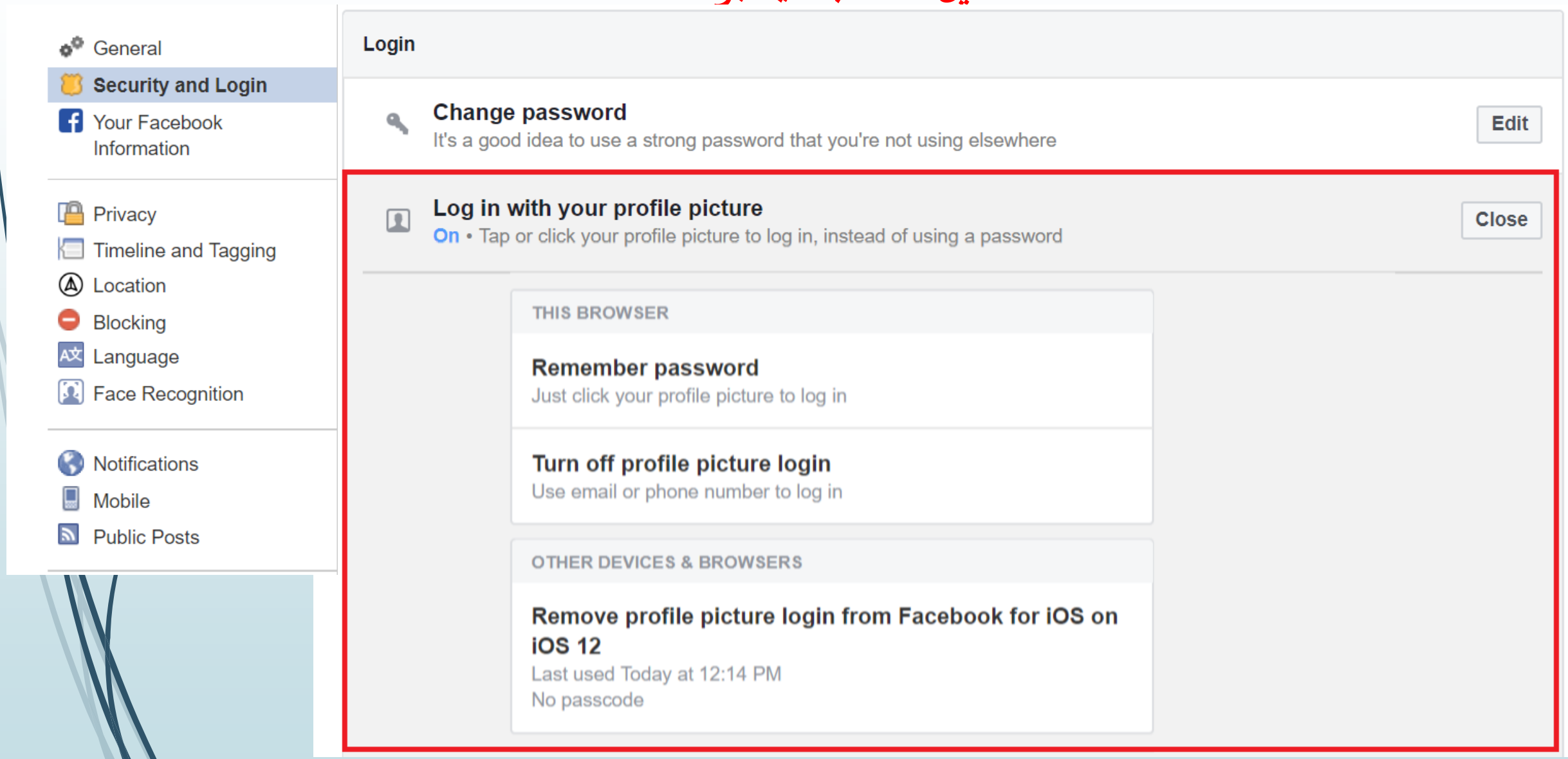
تأمين حساب فيسبوك



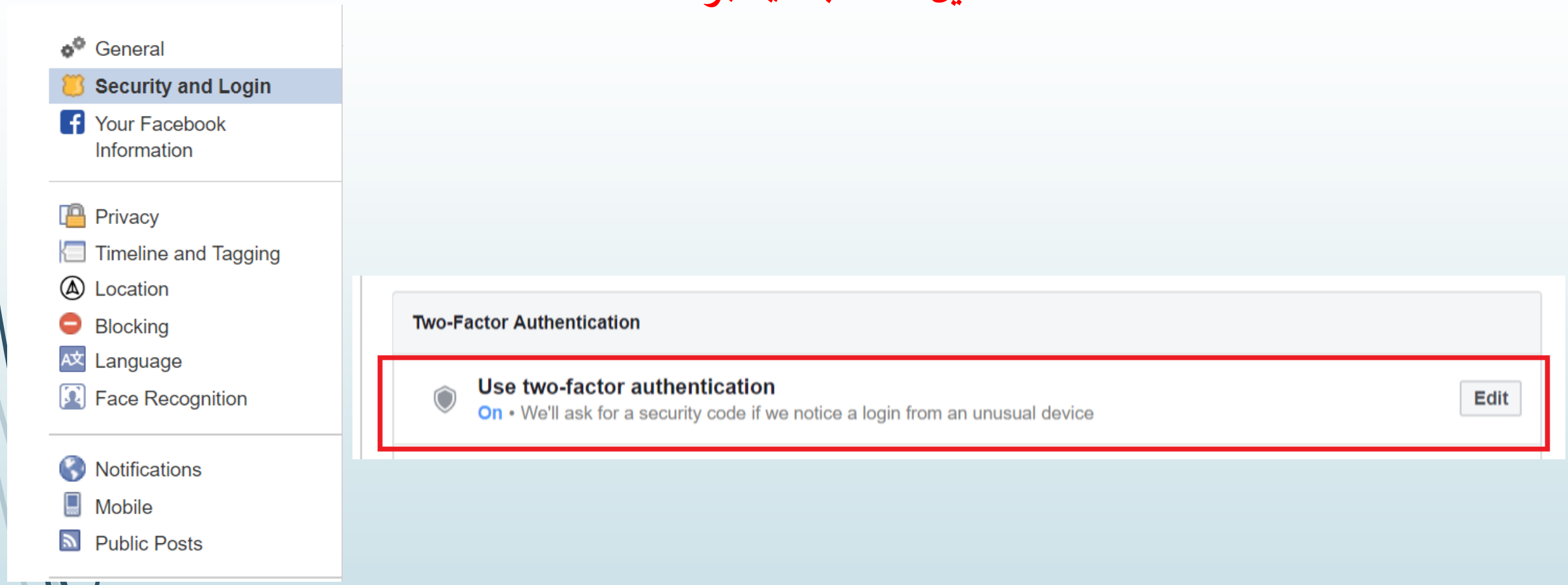
تأمين حساب فيسبوك



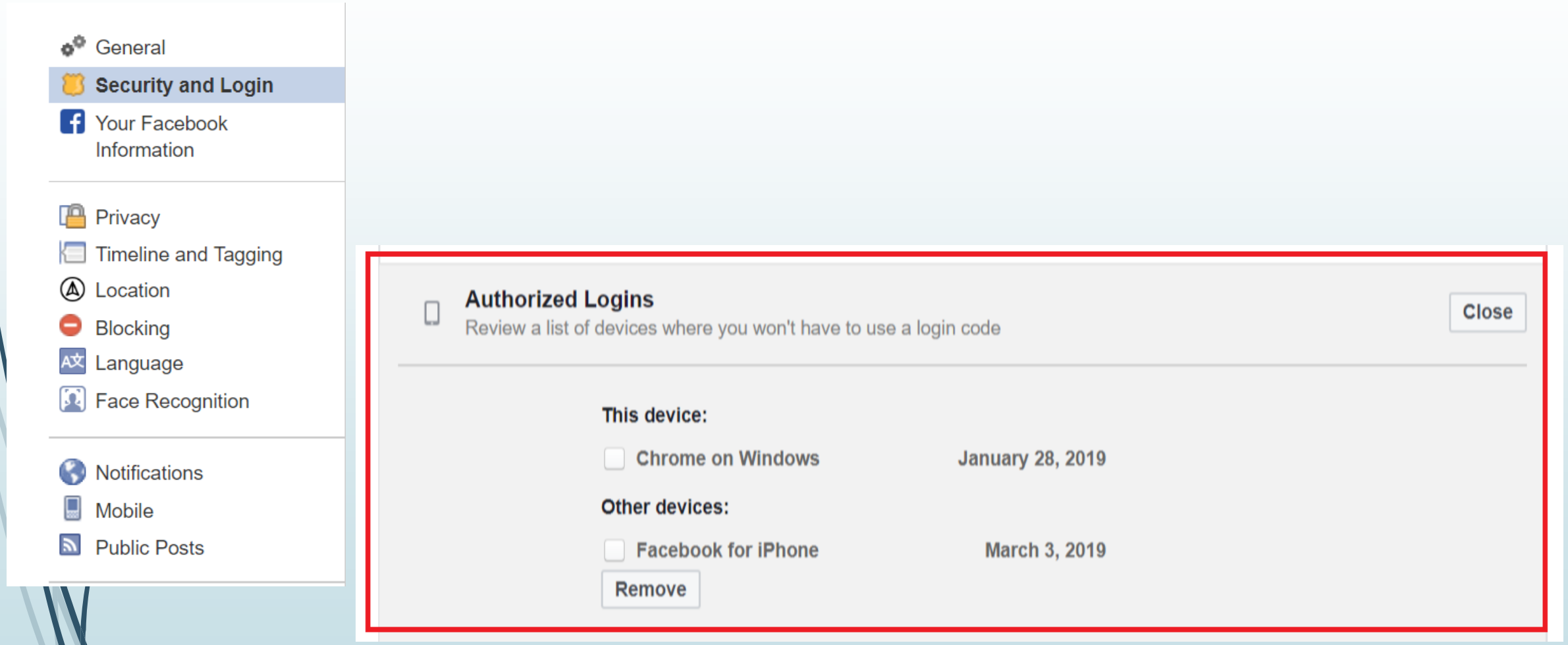
تأمين حساب فيسبوك



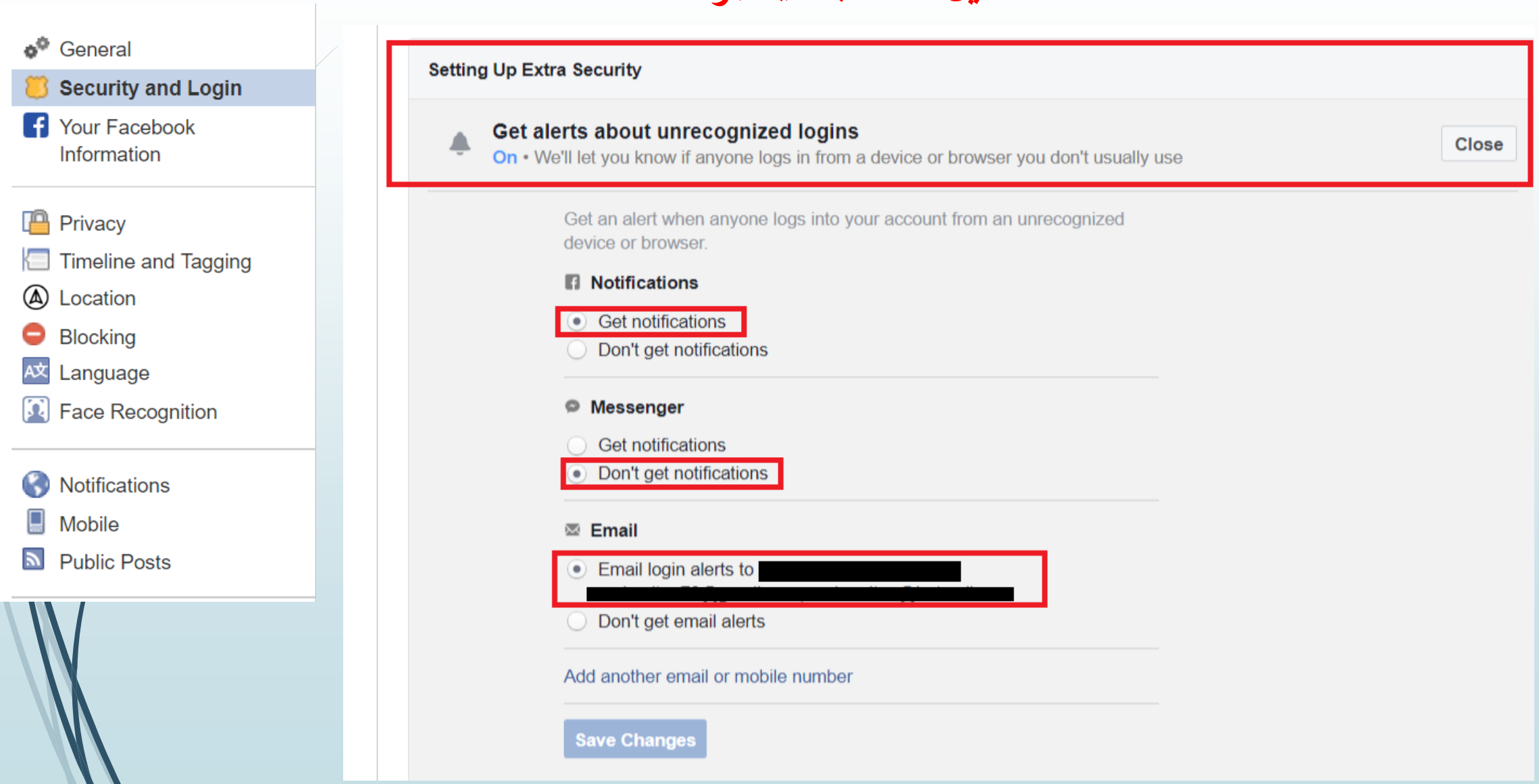
تأمين حساب فيسبوك



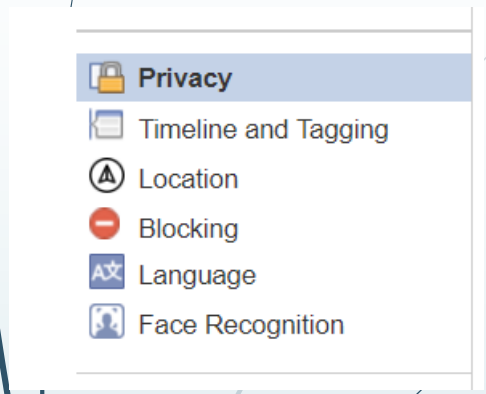
تأمين حساب فيسبوك

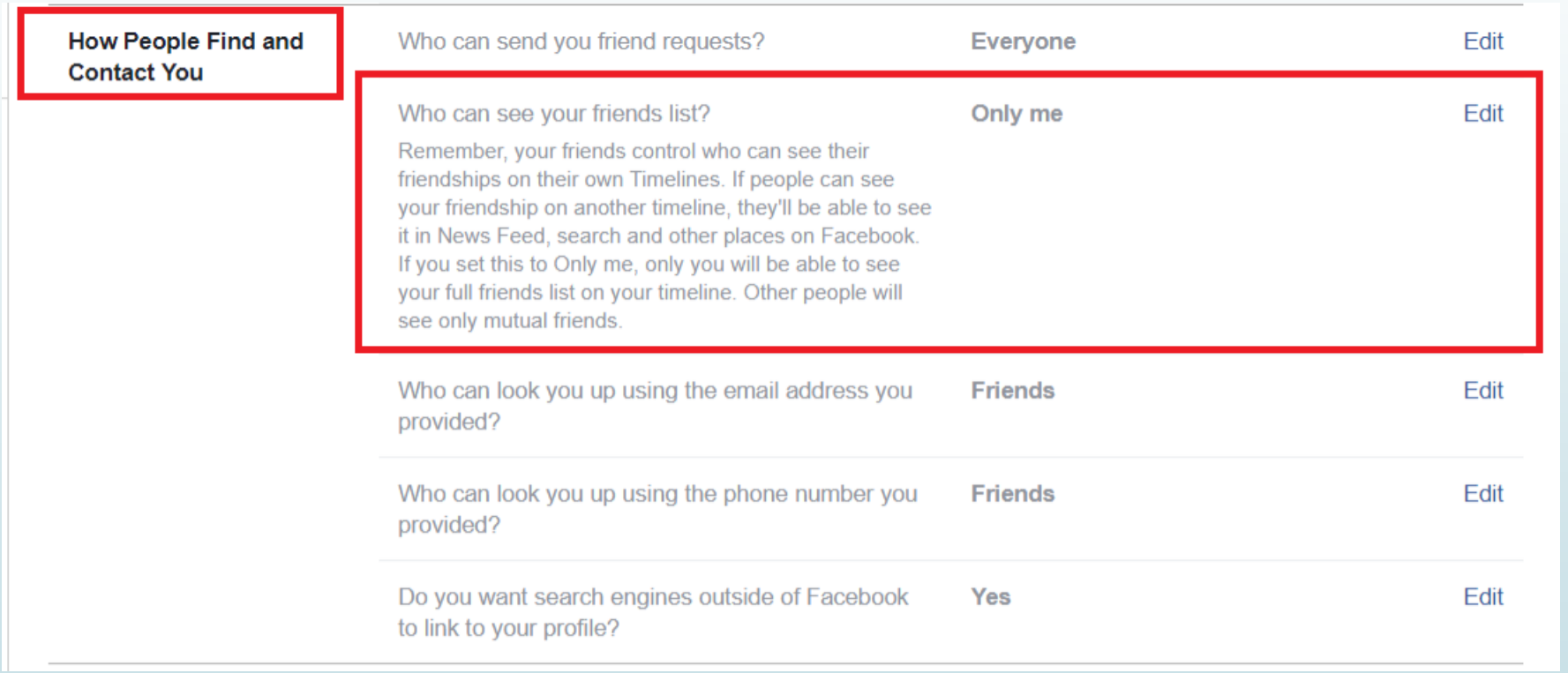


تأمين حساب فيسبوك

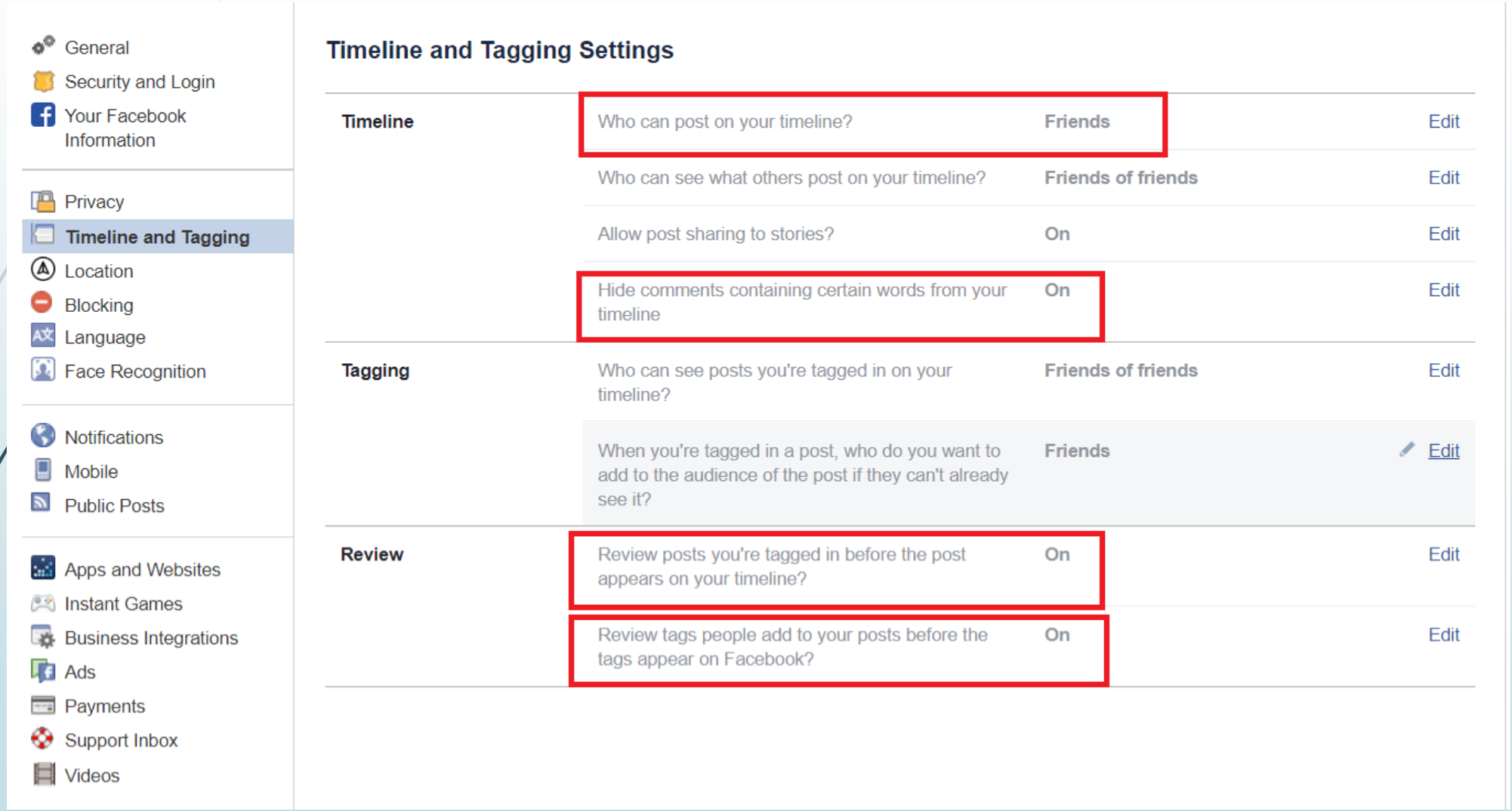


تأمين حساب فيسبوك

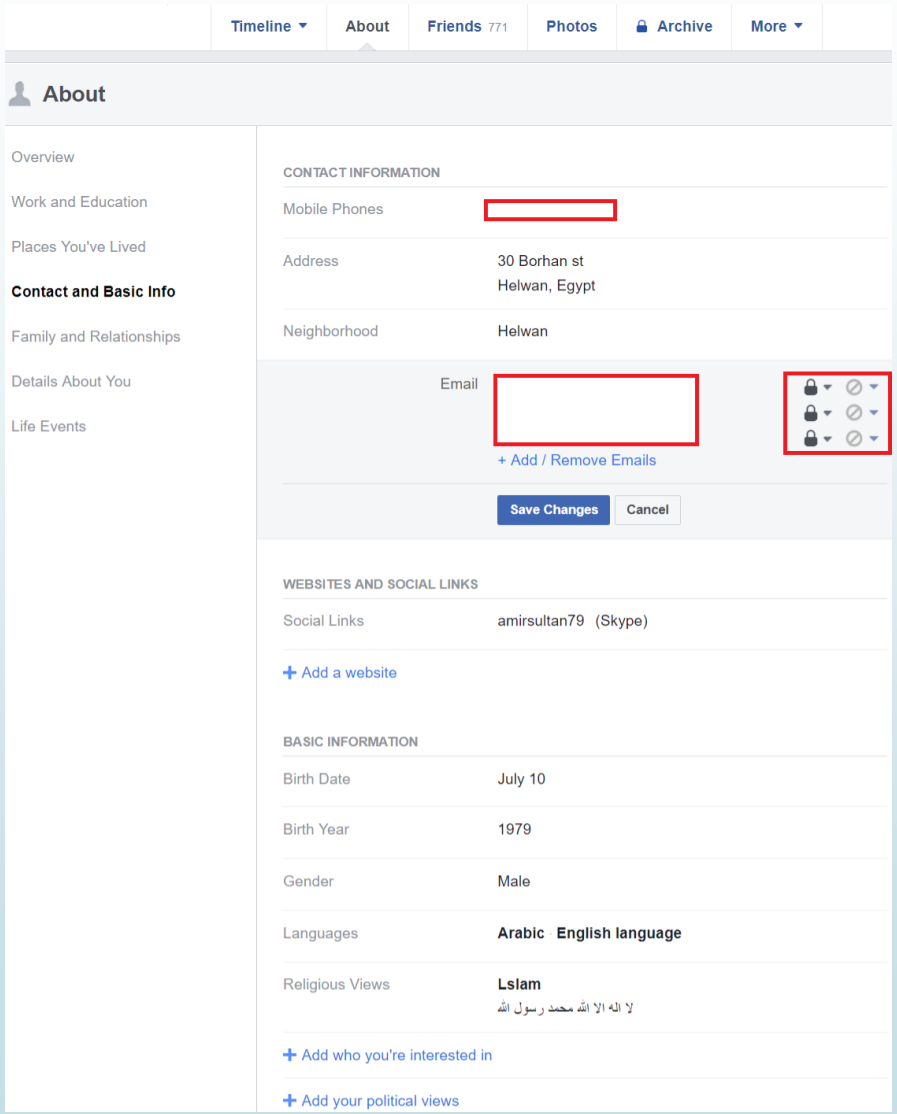




تأمين حساب فيسبوك

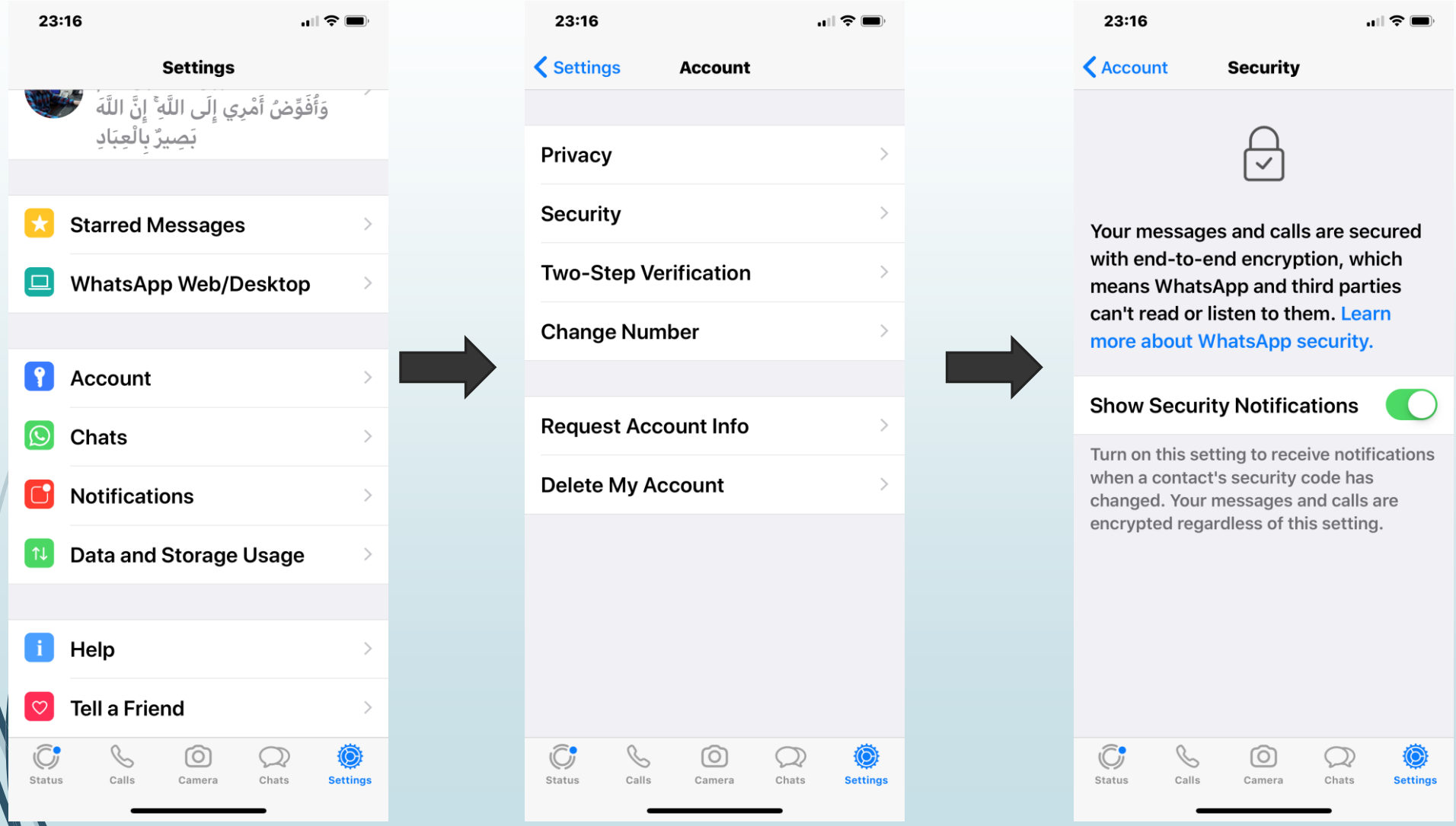


تأمين حساب فيسبوك

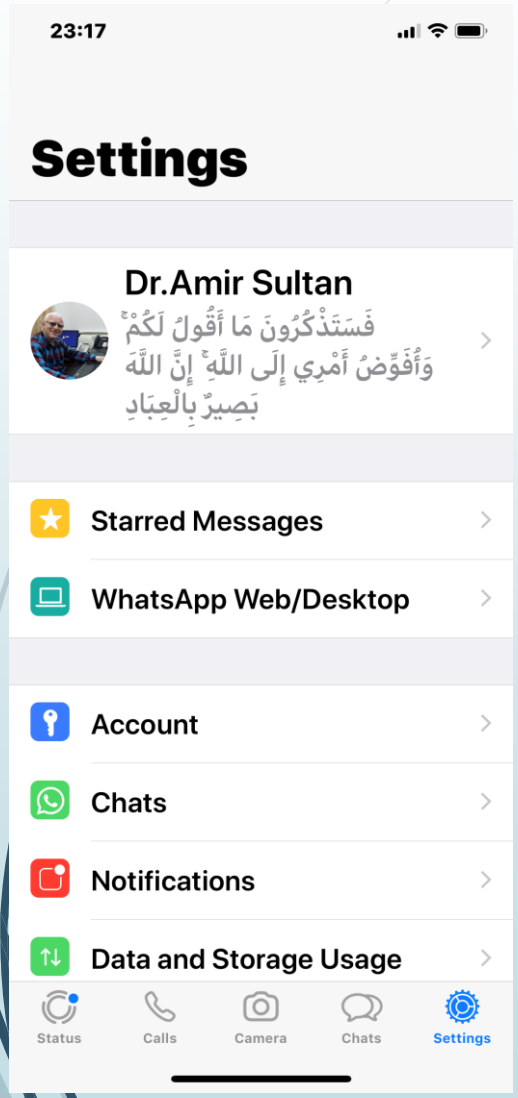


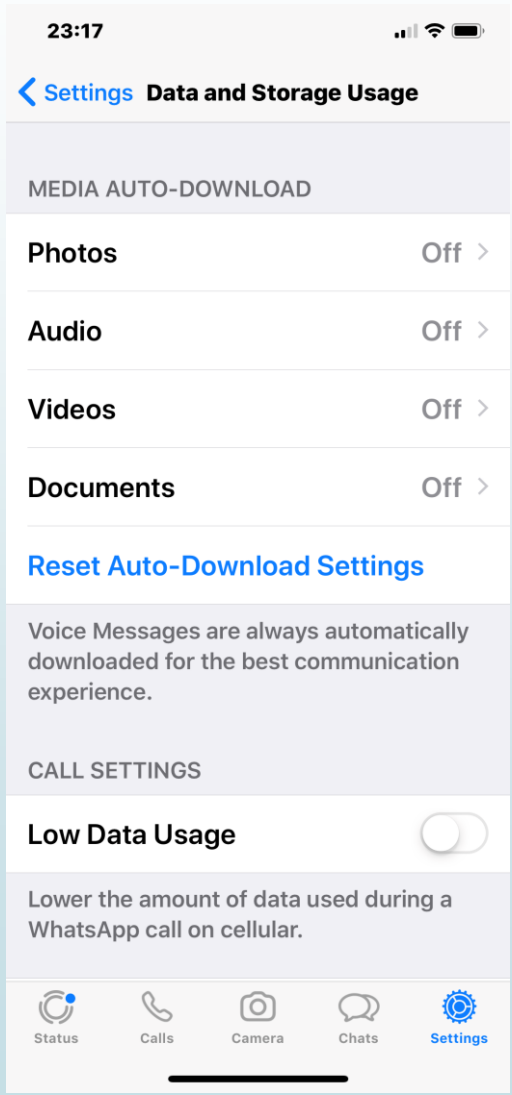

WhatsApp

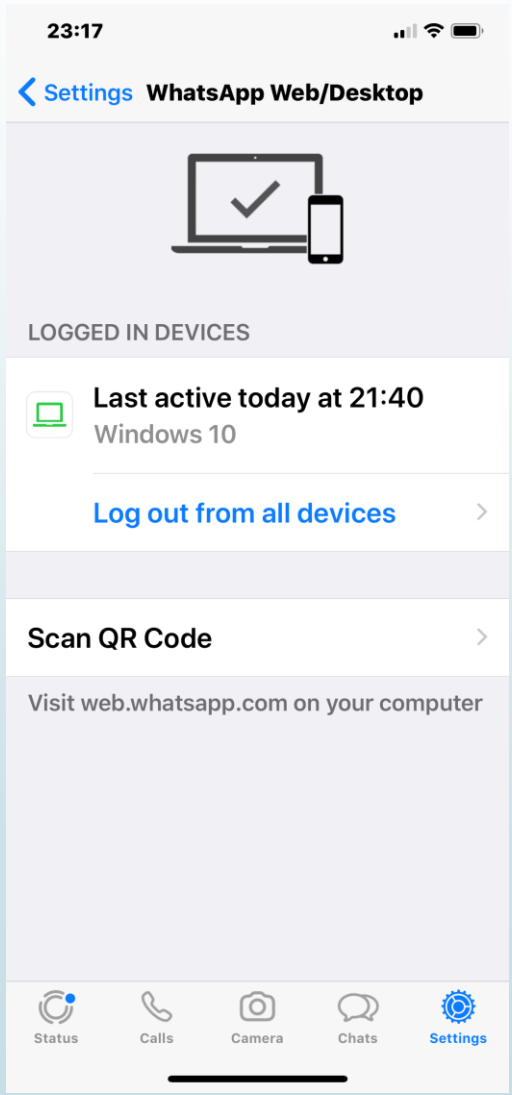
WhatsApp Security



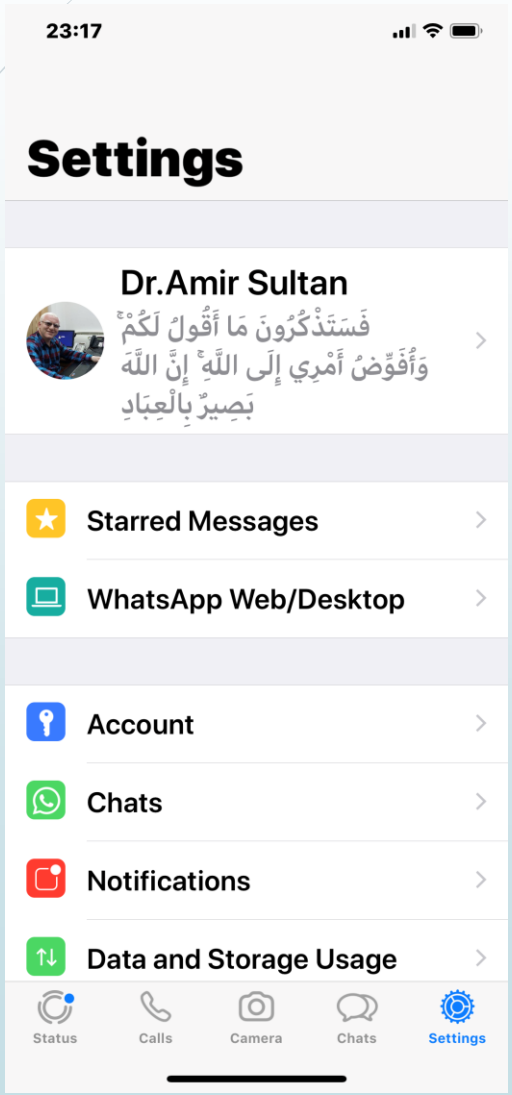
WhatsApp Security

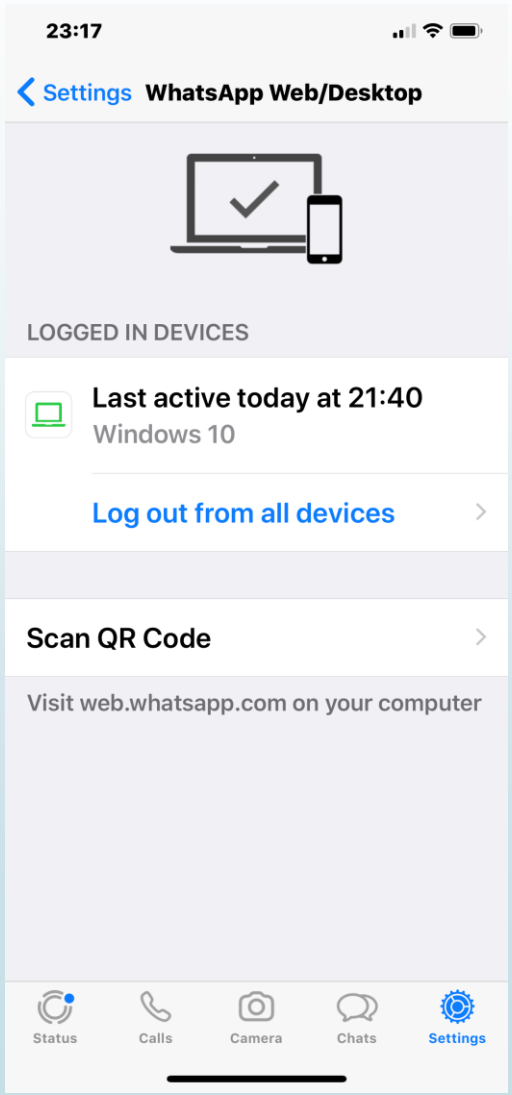






WhatsApp Security





Thank You

Best Regards

Eng *Amir Sultan*

ICT Director

Nahda University Road-New Bani Sweif City, Egypt

Short No: 19206. Ex: 2001

Tel : +2 082- 22 84 68 0-9

Fax : +2 082- 22 84 688

Mob : +2 01000 34 30 56

E-Mai : amir.sultan@nub.edu.eg

Web : www.nub.edu.eg

LinkedIn :linkedin.com/in/amirsultan79