



NUB

NAHDA UNIVERSTY IN BENI SUEF
جامعة النهضة - بني سويف



الاجندة

- ✓ التعرف 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 حقلك ؟
- ✓ المخاطر على العمل التجاري اثر الهجمات الالكترونية والاختراقات .
- ✓ امن المعلومات واهميته واعتباره امن قومي
- ✓ التعرف 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 رقمياً 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 تشبيهه على انه بصمتك الالكترونية التي تحدد هويتك الحقيقية 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 اولى خطوات التحول الرقمي الذي لا بد 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 طويلةٍ 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



Free

إيجابيات التحول الرقمي

تحليل البيانات

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



إيجابيات التحول الرقمي

صديقة للبيئة



المعاملات الإلكترونية لا تتطلب 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

سليات 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

سليات التحول الرقمي

التجسس او الاختراق



حيث يستطيع بعض المخترقين اعتراض المعاملات الإلكترونية، 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

سليات 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 لتم حمايتها من كل ما يمكن أن يُهددها من مخاطر مختلفة، ولا شك أن اختلاف تلك المخاطر المتعددة وتطورها المستمر يتطلب العمل المستمر على تطوير ذلك العلم، ليتمكن من تفادي ومواجهة كل ما قد يُستجد 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 لأي شخص بالعبث بها بأي طريقة كانت سواء بالحذف أو بالتعديل عليها، كان هذا بقصد أو دون قصد. ومنع الأشخاص من القيام بعمل إي إجراء دون إذن مالكيها.

التوافر

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

السرية

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

صداقة

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 الآخرين عنوه ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية او أجهزة مؤسساتهم او بنفسياتهم عند سحبه ملفات وصور، او مستندات، او رسائل بحثية او وثائق سرية.



الاختراق

هل الاختراق امر حديث مرتبط بالإنترنت

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 غير 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 القبة 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 القبة 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 امني 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 **Hacktivism** ومعناها 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 سلبي في اغلب الاحيان).



ترتيب الخطورة

المستخدم العادي معرض للهجمات المخترقين علي النحو التالي

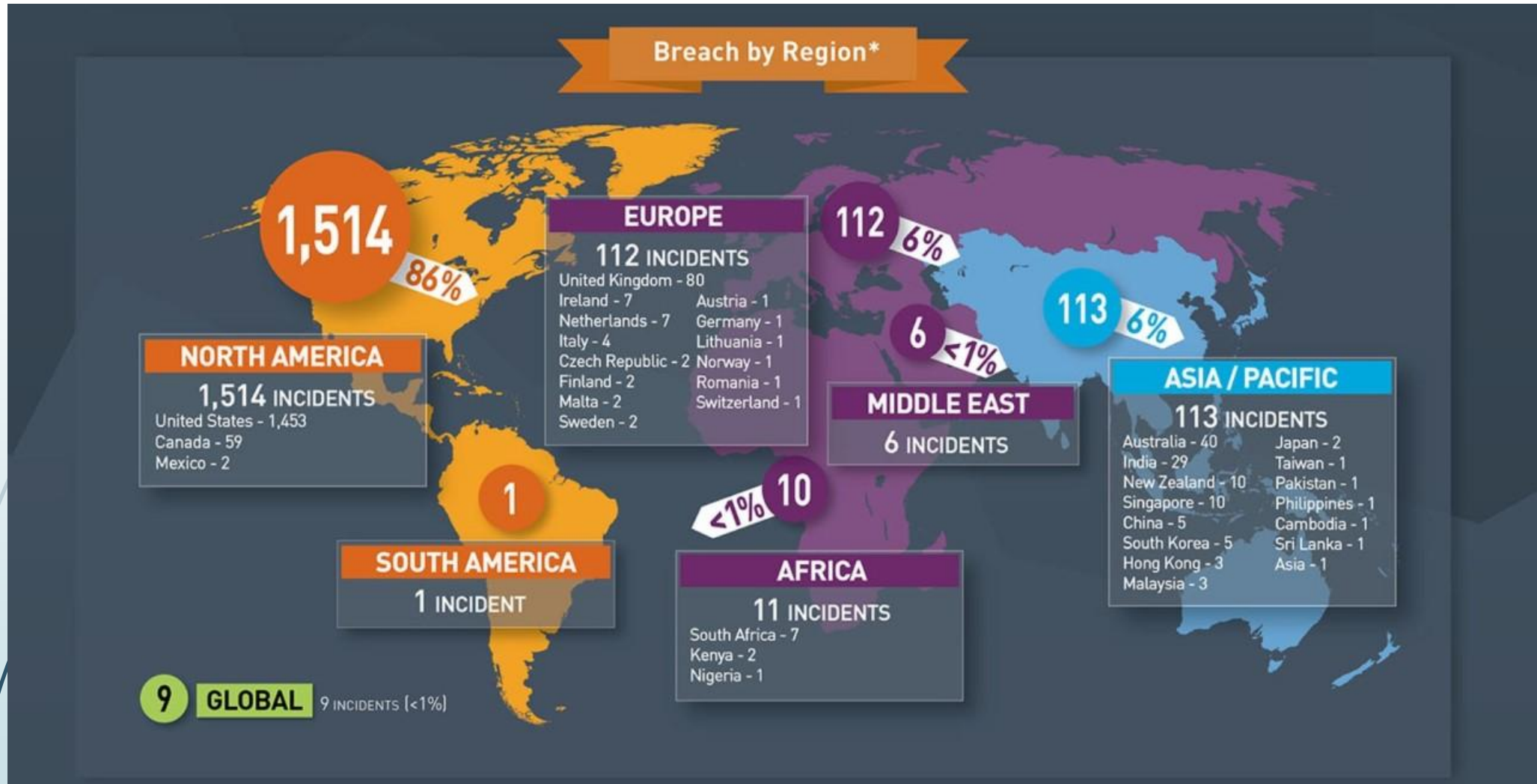


- أطفال الهاكرز Script Kiddies
- الهاكرز ذو القبة السوداء Black Hat Hackers
- الهاكرز ذو القبة الرمادية Grey Hat Hackers
- الهاكرز ذو القبة الحمراء Red Hat Hackers

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

Number of Breach Incidents by Industry



أكثر الفئات اختراقاً عالمياً

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 WPS للاتصال السريع
- وجود أجهزة مصابة على الشبكة

أشهر أسباب الاختراق

عدم تحديث أنظمة التشغيل والتطبيقات



عدم الاهتمام بتحديث أنظمة التشغيل والتطبيقات من أكثر الأسباب التي تؤدي إلى الاختراق وتقوم الشركات بإضافة التحديثات الإلزامية، ولكن تكون بدون فائدة إذا لم يقوم المستخدم بأجراء التحديث بشكل مستمر

اشهر أسباب الاختراق

Wi-fi بنفس اسم شبكتك



- وقوع قيام المخترق بعمل شبكة Wi-Fi مماثلة تماما لنوع شبكتك بنفس الإعدادات (التردد ونوع التشفير، ولكن بكلمة سر مختلفة)
- وعندها يتم خدعك 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 انتهاء عملك
- قد لا يهتم غيرك بتأمين 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 بتحليلها 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 تخمينها 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 مستوى 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 موجودة 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 المهمة، ومنها كلمة السر.



اشهر أسباب الاختراق

الرسائل الاحتيالية المرتبطة بالهندسة الاجتماعية



تعتبر واحداً من أكثر الهجمات الالكترونية شيوعاً وتتم من خلال ارسال رسالة عبر البريد الإلكتروني 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 للاختراق 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 أصلية وغير تابعة للشركة المصنعة .
- 2- استخدام برامج غير أصلية تكون محملة بالعديد من الفيروسات والروابط الملغمة.
- 3- استخدام برامج مفعلة بطرق غير شرعية **Cracks** وتمثل حوالي **70%** من أسباب الاختراق وتشفير البيانات

أشهر أسباب الاختراق

استخدام الخدمات العامة

استخدام خدمات مجانية دون التأكد من سلامتها



FREE
Wi-Fi

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 ضرراً كبيراً في الأجهزة المستهدفة، 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 للخيل والأحصنة، فقد قبلوا هذه الهدية بدون تفكير. وفي الليل، خرج اليونانيون من الحصان وهاجموا المدينة من الداخل. تتلخص فكرة عمل أحصنة طروادة في أنها تتخفي 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

تعد البرامج الآلية شكلاً متقدماً 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 انتهاكاً 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 يرمج 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 كلياً أو جزئياً، 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.

الروت (Rootkits)

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

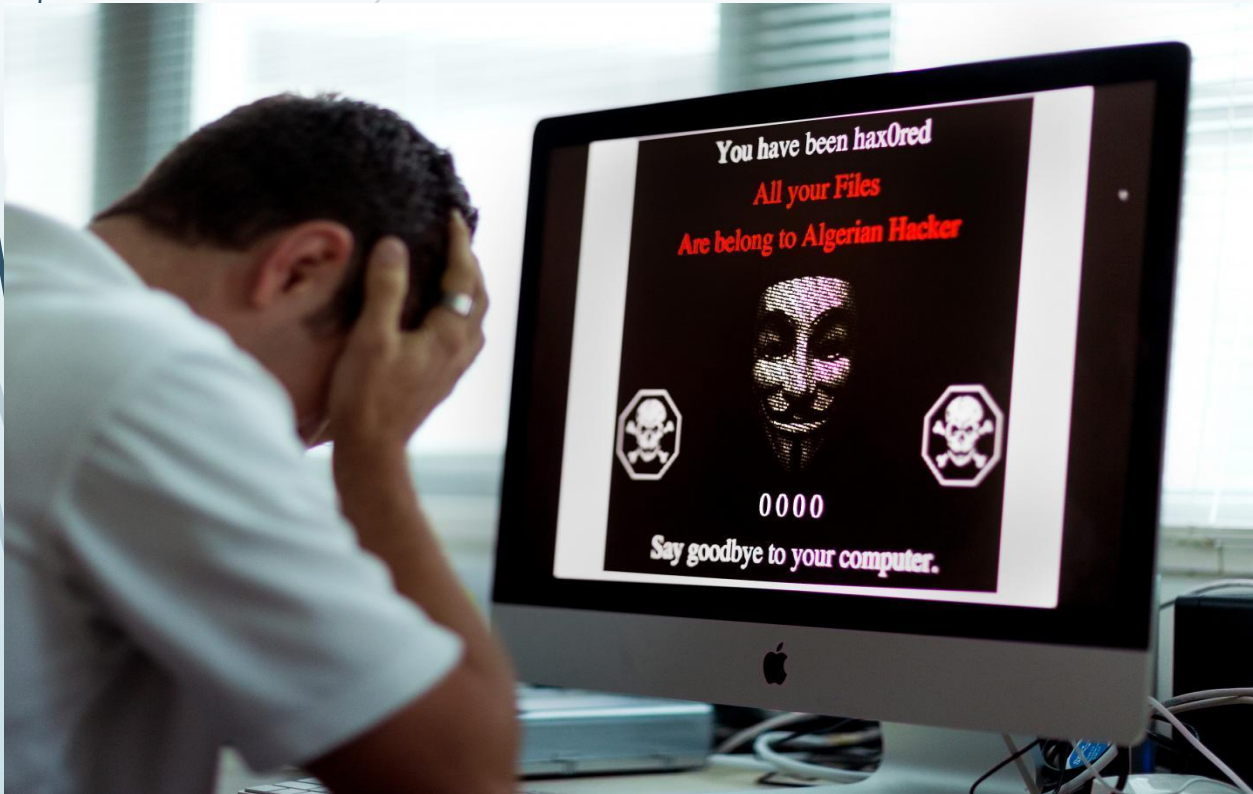
الزومبي

هي برمجيات مشاهدة للبرمجيات التجسسية، وآلية دخولها مشاهدة أيضاً، 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
تعذر فتح بعض التطبيقات , وخاصة تطبيقات الأمان .
تفعيل خاصية تحميل التطبيقات من مصادر غير معروفة .
ظهور الإعلانات المزعجة بشكل مُتكرر.
تغير 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 المكالمات
إبقاء الهاتف قيد التشغيل وعدم القدرة على إغلاقه نهائياً
ظهور فاتورة مُشتریات عبر البطاقة الائتمانية لأشياء لم يتم 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

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 يتم 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

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
تعذر فتح بعض البرامج
وجود برامج غريبة لم تقم بتحميلها
ظهور الإعلانات المزعجة بشكل مُتكرر
تغيير طريقة عرض بعض المواقع الإلكترونية
عدم استقرار خدمة الانترنت
استهلاك موارد الجهاز بدون سبب

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 كورونا و استخدام التكنولوجيا في تزايد مستمر مما جعل عدد الأشخاص الذين يرغبون في الحماية من التهديدات الأمنية يتزايد بشكل مستمر وكذلك جميع المؤسسات وحتى الأشخاص يحتاجون الى نظام امن معلومات قوى يقوم بحمايتهم

هل تثبت حقلك 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 حقلك 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 استخراجہ
- عدم مشاركة تلك البيانات مع أي جهة غير الجهات المختصة للتحقيق
- 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 دائماً.

إجراءات مادية

- التأمين المادي للأجهزة والمعدات
- تقييد الوصول إلى المكاتب، وخصوصاً مراكز تخزين البيانات
- تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.
- تركيب أنظمة Firewall وأنظمة 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 نظراً 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 الأقسام 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

A person wearing a dark hoodie is shown from the chest up, centered in the frame. The background is a dark green color with a pattern of glowing white binary code (0s and 1s) and faint white lines, suggesting a digital or data environment. A semi-transparent dark grey horizontal bar is overlaid across the middle of the image, containing the text.

أكبر 10 عمليات اختراق الكتروني في 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 وخبرته، 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 شيء.



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 Ransomware كوسيلة 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 حساسيتها اتجاه Ransomware.

يتم تشفير الملفات بطريقتين :-

Offline

وهناك امل ضعيف في استعادة الملفات بطرق فنية معقدة بعض الشيء

Online

ولم يتم اكتشاف أي حلول حتى 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 تقدّم خدمات تكنولوجيا المعلومات للشركات، وانخفضت الأرباح 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 دولار 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 Inc واحدة 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 المتحدث 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 طالبت به بأكثر من 20 مليون دولار!

نوفمبر 2020

- محكمة العدل العليا البرازيلية
- نادي مانشستر يونايتد لكرة القدم

ديسمبر 2020

- GenRx Pharmacy هي 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 كلياً مثل توقف كامل لبث القنوات الفضائية كما حدث لوكالات أنباء تعرضت لهذا الهجوم، وتقديم خدمات ومعلومات مزيفة من جهات وهمية مثل السيطرة على شبكة أحد البنوك وتقديم معلومات كاذبة للعملاء، وصلت خطورة هذه الهجمات وفي عام 2015، إلى حد إيقاف بث قناة فرنسية.

لماذا حساب الكتروني باسم الجامعة؟؟



NAHDA UNIVERSITY
IN BENI SUEF
جامعة النهضة . بني سويف



التسويق و إدارة الأعمال
نماذج محاكاة للبنوك والمصارف
القومية والأجنبية بجانب
المحاسبة و إدارة الأعمال



علوم الحاسب
معامل تطبيقية
متميزة
لأكبر شركات
البرمجة في العالم



**الإعلام
والعلاقات العامة**
استديو تلفزيوني و آخر
اذاعي على أحدث
مستوى تقني



الهندسة
ميكاترونيك -
إنتاج - مدني -
إتصالات - عمارة -
طاقة متجددة



الصيدلة
مصنع لصناعة
الأدوية
و مركز للأبحاث
العلمية



**طب الفم
والأسنان**
مستشفى فم
و أسنان
مجهزة على
أعلى مستوى

خطوة أكبر
#جيل . جاهز . لبحره

19206
www.nub.edu.eg

nub.edu.eg

لماذا حساب الكتروني باسم الجامعة؟

@nub.edu.eg



ربما يظن البعض أن الحساب الإلكتروني الذي تهيئه 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 الخارجيين بعكس البريد الإلكتروني المجاني 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 سرقة
فليس لديك سوى القليل جدا الخيارات الصعبة
لتنمكّن من استرجاعه لأن هذا البريد ليس ملكاً لك
في الأساس، ولكن السؤال الأصعب، هل يمكنك أن
تتعامل وتتأقلم مع فقدان بريدك الإلكتروني للأبد
وفقدان كافة الرسائل؟

ACCESS

INFORMATION
PRIVACY

CYBER
SECURITY



DATA
PROTECTION

MOBILE
DEVICES

اجراءات الامان

الارشادات الحماية والسرية

اجراءات الامان



✓ احرص دائما على تفعيل جميع اجراءات الامان ولا تحمل 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 لحمايةك من اي متطفل يمكن ان يطلع على خصوصياتك قد قام بتحميل برنامج ليقوم بحفظ كلمات السر به دون ان تعرف **(Key logger)**.



الارشادات الحماية والسرية

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.

الارشادات الحماية والسرية

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

الارشادات الحماية والسرية

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.

الارشادات الحماية والسرية

التأكد من سلامة الروابط

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



الارشادات الحماية والسرية

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 يرجى 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 .

الارشادات الحماية والسرية

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 يرجى فقط ارسال طلب الي قسم الشبكات وامن المعلومات علي

noc@nub.edu.eg

الارشادات الحماية والسرية

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 **OPT** للتأكيد 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 الهاتف
- استخدم وضع المتصفح الامن اثناء عملية الشراء



امور اضافية يجب تطبيقها بشكل دقيق جدا

بالنسبة لجهاز الكمبيوتر



- تحميل نظام حماية **Internet Security** والتحديث 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 مشبووه
- استخدم متصفح امن مثل **Google** او **Firefox**
- لا تقم بحفظ كلمة السر علي المتصفح .
- الحرص علي عمل نسخ احتياطية من البيانات كل فترة علي وسيلة 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 الائتمان علي التليفون .



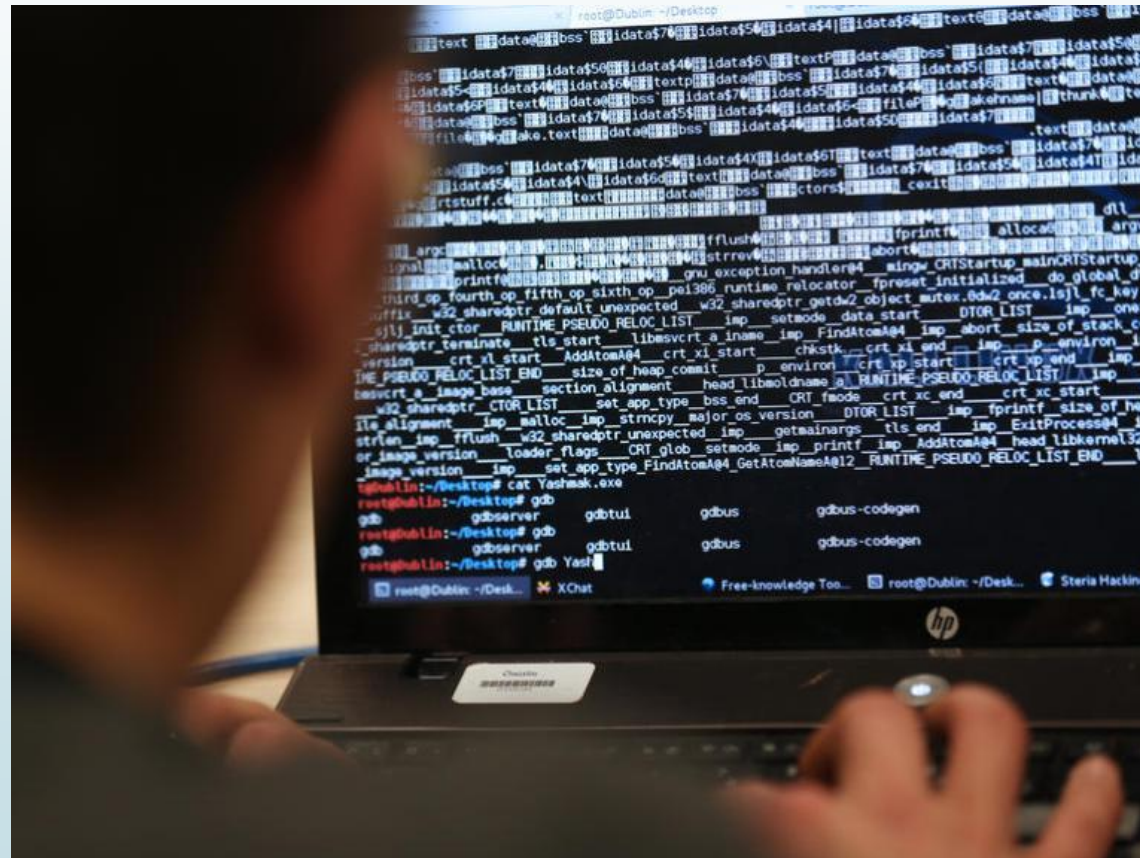
امور اضافية يجب تطبيقها بشكل دقيق جدا

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 تغيير كلمة السر في الحال مع ضرورة مراعاة الآتي:

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

Keepass Password Safe



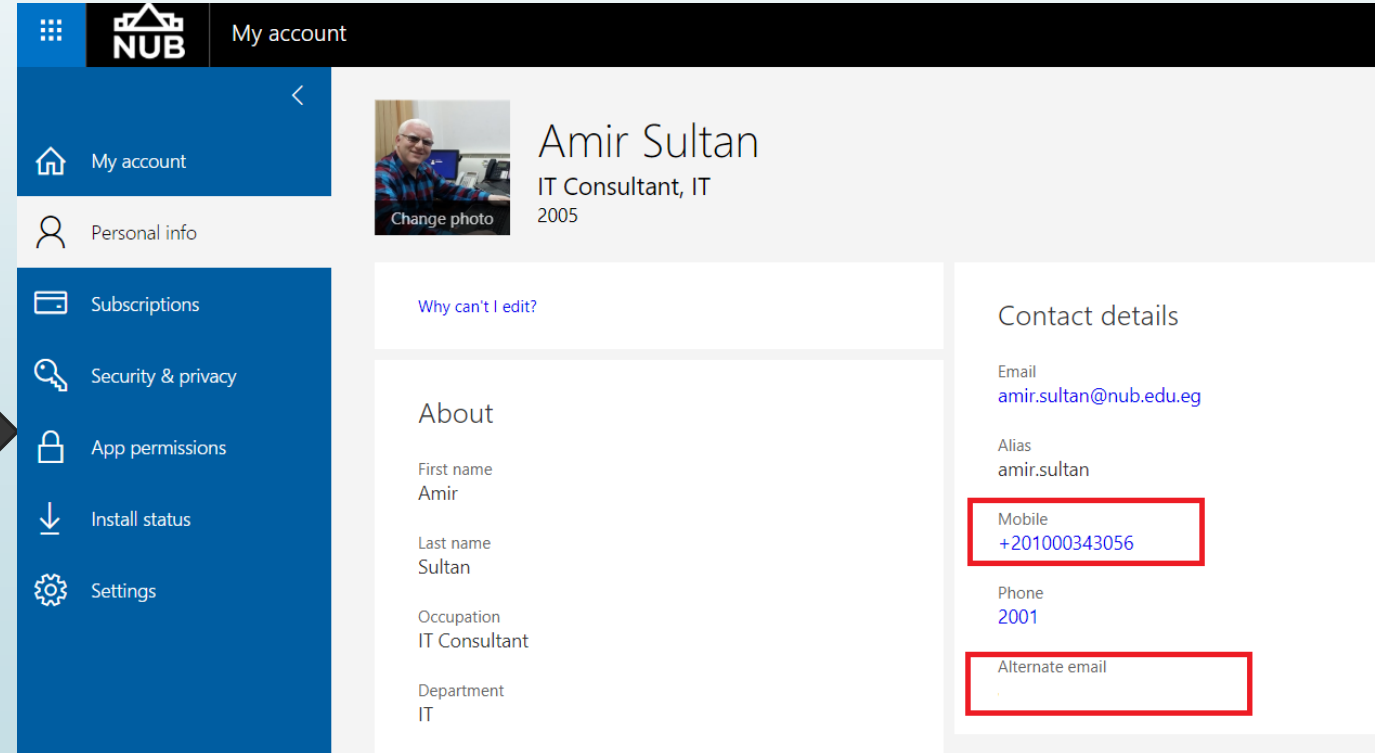
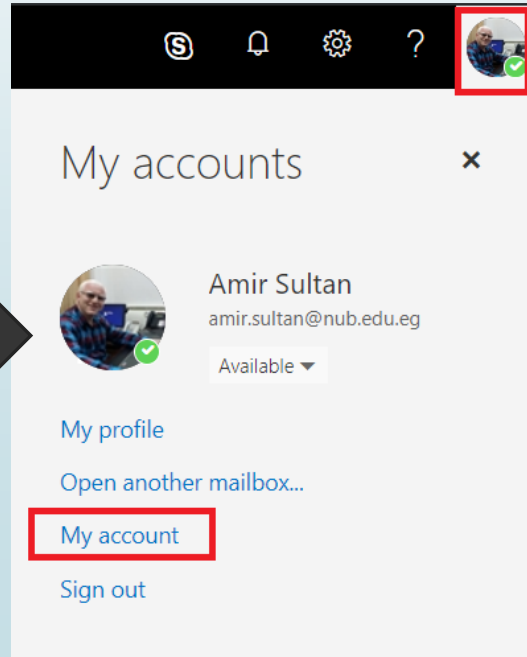
Change
Password

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 تركيب **Hard Disk** في 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 **Scan** للجهاز 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 موثوق بها لعدم تفاقم 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

طلب المساعدة

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 القرصنة هو “الانقضاء 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 المرجح أن يكون مرفق معه برامج ضارة.





Attachments

Technical Attachment

Step By Step



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

حماية Router من الاختراق

حماية Router



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

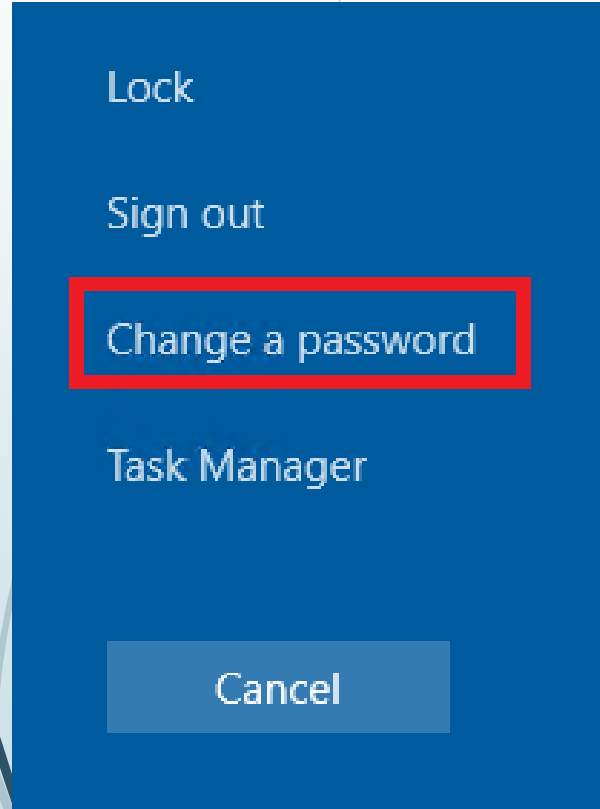
في حالة الاختراق

طريقة تغيير كلمة السر

بعد الدخول علي جهاز الكمبيوتر الخاص بك قم علي الثلاث مفاتيح الثالثة التالية مرة

Ctrl + Alt + Del واحدة مع بعضها البعض

ثم اختار **Change Password**



كيف تعرف ان جهاز به برنامج غير معروف المصدر

Task Manger

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	Publisher	Status	Startup impact
AvLaunch component	AVAST Software	Enabled	Not measured
Microsoft OneDrive	Microsoft Corporation	Enabled	High
Windows Security notification icon	Microsoft Corporation	Enabled	Low

Fewer details Disable

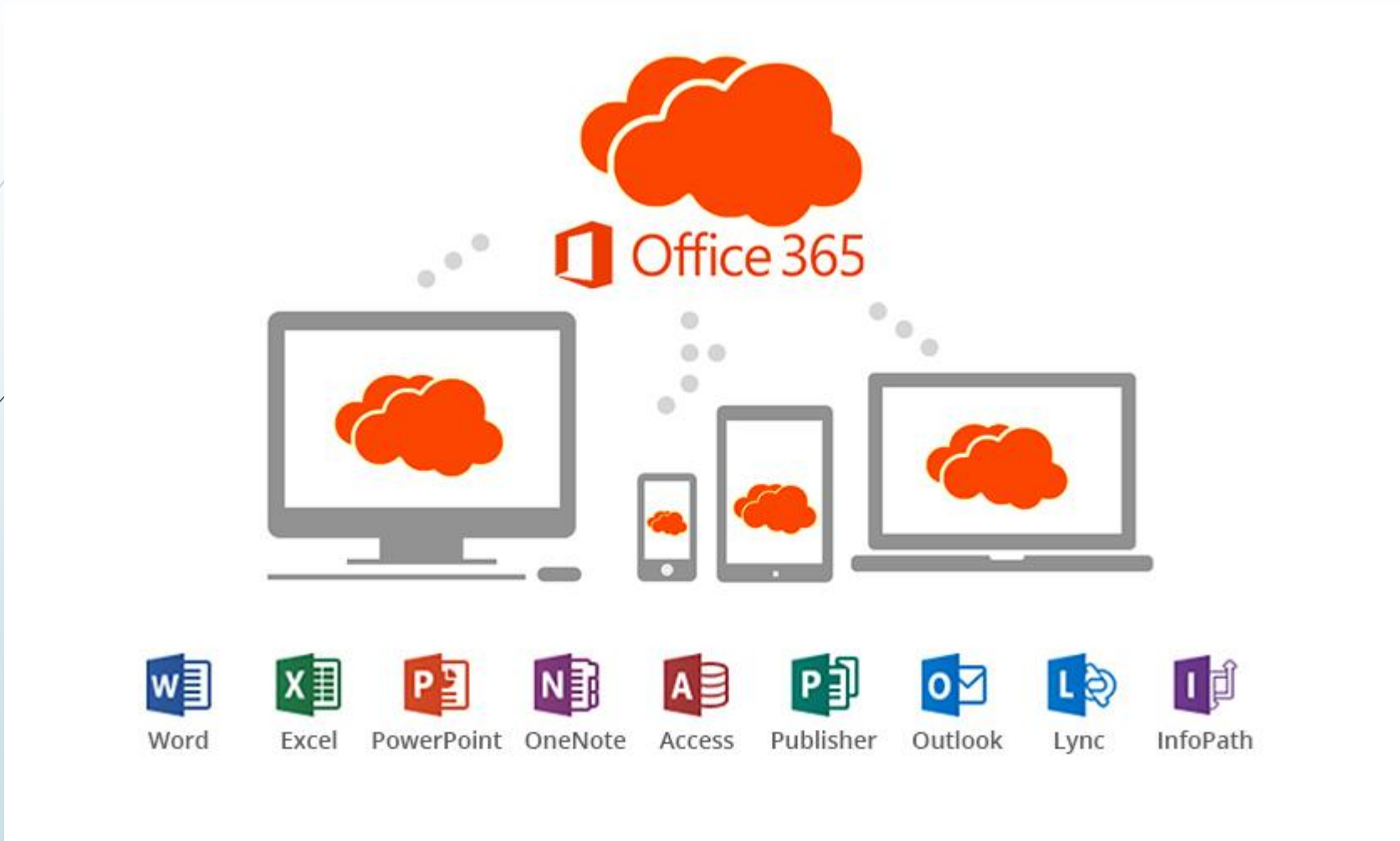
Task Manager

File Options View

Processes Performance App history Startup Users Details Services

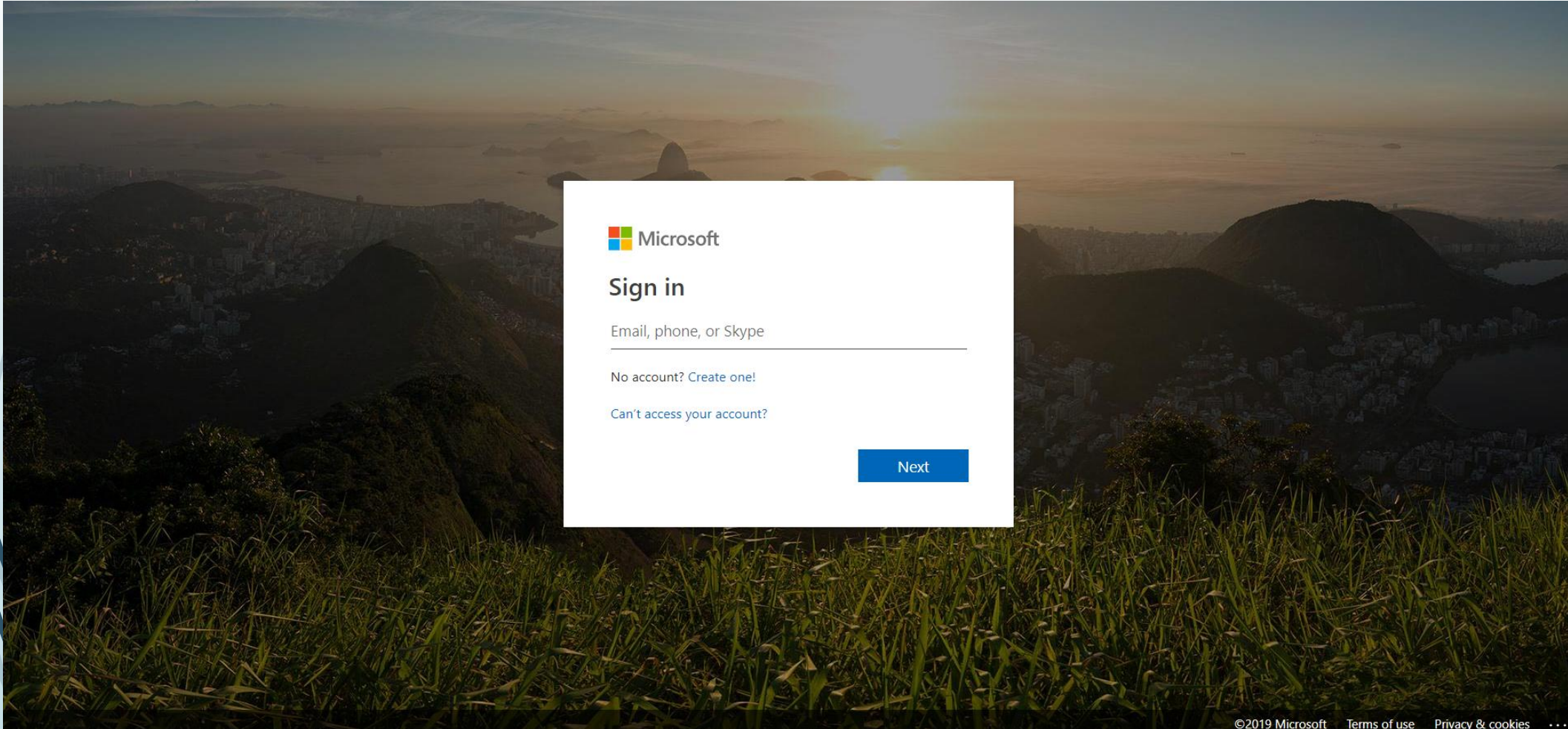
Name	Status	85% CPU	71% Memory	44% Disk	0% Network	Power usage	Power usage tr...
Apps (2)							
> Avast Antivirus (32 bit) (2)		0.5%	38.5 MB	0 MB/s	0 Mbps	Very low	Very low
> Task Manager		3.7%	21.6 MB	0 MB/s	0 Mbps	Very low	Very low
Background processes (37)							
Application Frame Host		0%	4.4 MB	0 MB/s	0 Mbps	Very low	Very low
Avast Antivirus (32 bit)		0%	27.7 MB	0 MB/s	0 Mbps	Very low	Very low
Avast Antivirus Installer (32 bit)		0%	2.3 MB	0 MB/s	0 Mbps	Very low	Very low
Avast Antivirus Installer (32 bit)		0%	9.8 MB	0.1 MB/s	0 Mbps	Very low	Very low
> Avast Behavior Shield		0%	14.9 MB	0 MB/s	0 Mbps	Very low	Very low
> Avast firewall service (32 bit)		0%	9.2 MB	0 MB/s	0 Mbps	Very low	Very low
> Avast Service (32 bit)		24.7%	29.6 MB	13.9 MB/s	0 Mbps	Low	Very low
COM Surrogate		0%	1.7 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate		0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
> Cortana (2)		0%	3.6 MB	0 MB/s	0 Mbps	Very low	Very low
CTF Loader		0%	3.8 MB	0 MB/s	0 Mbps	Very low	Very low
Google Installer (32 bit)		0%	1.9 MB	0 MB/s	0 Mbps	Very low	Very low
Google Installer (32 bit)		0%	0.7 MB	0 MB/s	0 Mbps	Very low	Very low
> Google Installer (32 bit)		0%	3.1 MB	0 MB/s	0 Mbps	Very low	Very low
Host Process for Windows Tasks		0.5%	2.4 MB	0.1 MB/s	0 Mbps	Very low	Very low
> Microsoft Edge (5)		0%	2.7 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft OneDrive Setup (32 bi...		0%	0.8 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft OneDrive Setup (32 bi...		50.8%	68.9 MB	0.1 MB/s	0 Mbps	Moderate	Moderate

Fewer details End task



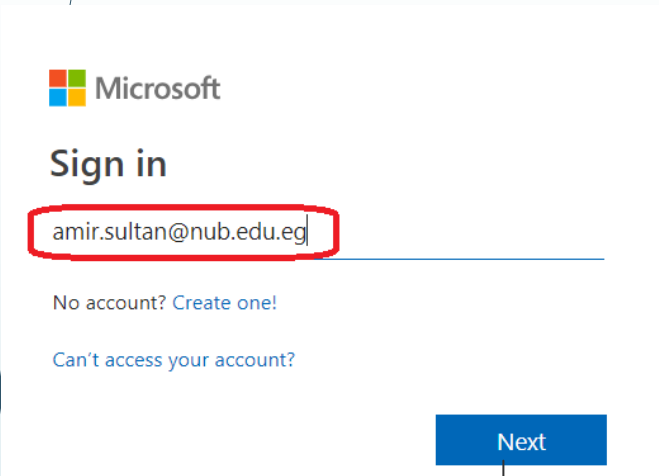
Office 365

1- قم بفتح متصفح الانترنت [Google Chrome](#) او [Firefox](#) لزيارة الرابط التالي
[Portal.office365.com](https://portal.office365.com)

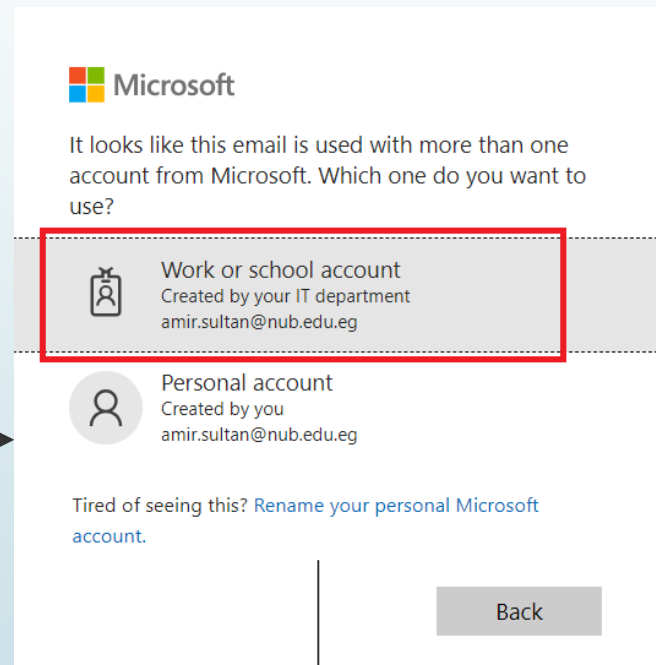


Office 365

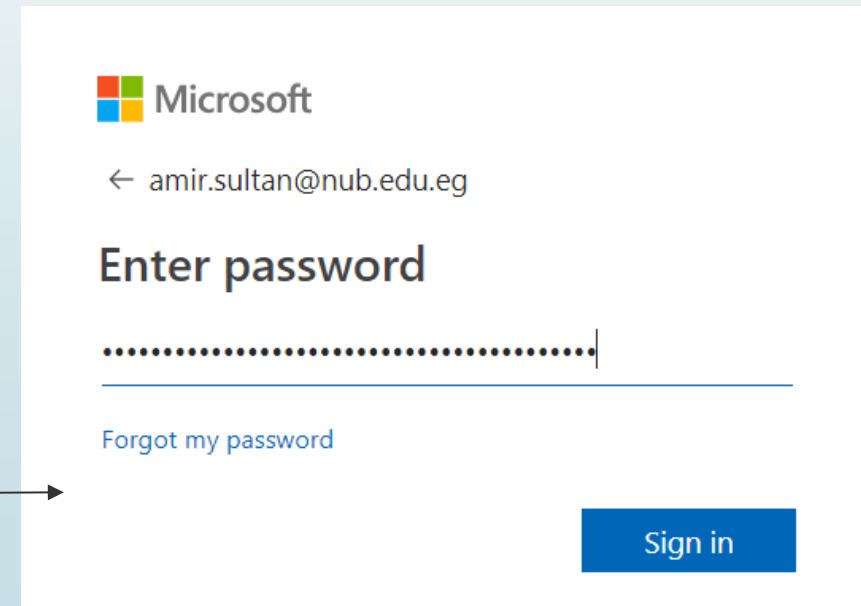
2- قم بكتابة الحساب الخاص بك بشكل كامل



Microsoft
Sign in
amir.sultan@nub.edu.eg
No account? [Create one!](#)
Can't access your account?
Next



Microsoft
It looks like this email is used with more than one account from Microsoft. Which one do you want to use?
Work or school account
Created by your IT department
amir.sultan@nub.edu.eg
Personal account
Created by you
amir.sultan@nub.edu.eg
Tired of seeing this? [Rename your personal Microsoft account.](#)
Back



Microsoft
← amir.sultan@nub.edu.eg
Enter password
.....
[Forgot my password](#)
Sign in

Office 365

3- استكمال باقي البيانات لتأمين الحساب



abrar.amir@nub.edu.eg

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

don't lose access to your account!

To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. You'll need to set up at least 2 of the options below.

- Authentication Phone is not configured. Set it up now
- Authentication Email is not configured. Set it up now

finish cancel

don't lose access to your account!

Please verify your authentication phone number below.

Authentication phone

Egypt (+20)

text me

call me

back

Office 365

تابع استكمال باقي البيانات لتأمين الحساب

don't lose access to your account!

Please verify your authentication phone number below.

Authentication phone

Egypt (+20) [Redacted]

text me

call me

We've sent a text message containing a verification code to your phone.

[Redacted]

verify

try again

back

don't lose access to your account!

To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. **You'll need to set up at least 2 of the options below.**

✔ Authentication Phone is set to +20 1000347128. [Change](#)

❗ Authentication Email is not configured. [Set it up now](#)

finish

cancel

don't lose access to your account!

Please verify your authentication email address below. Don't use your primary work or school email.

Authentication Email

[Redacted].com

email me

Office 365

تابع استكمال باقي البيانات لتأمين الحساب

don't lose access to your account!

Please verify your authentication email address below. Don't use your primary work or school email.

Authentication Email

email me

We've sent an email message containing a verification code to your inbox.

verify

try again

back

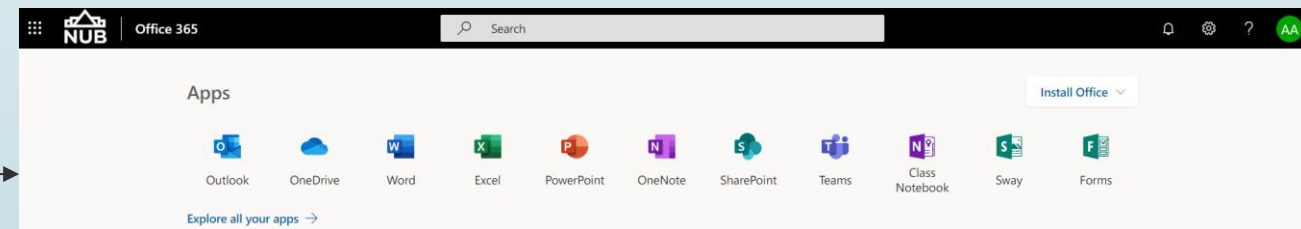
don't lose access to your account!

Thanks! We'll use the info below to recover your account if you forget your password. Click "finish" to close this page.

- ✔ Authentication Phone is set to +20 1000347128. [Change](#)
- ✔ Authentication Email is set to dramir2001@gmail.com. [Change](#)

finish

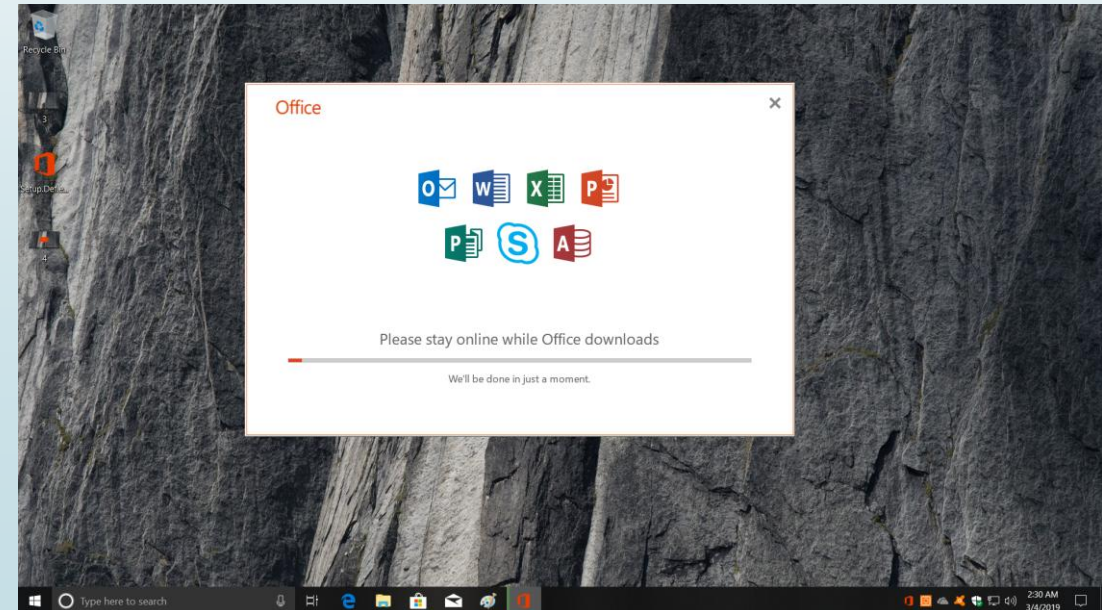
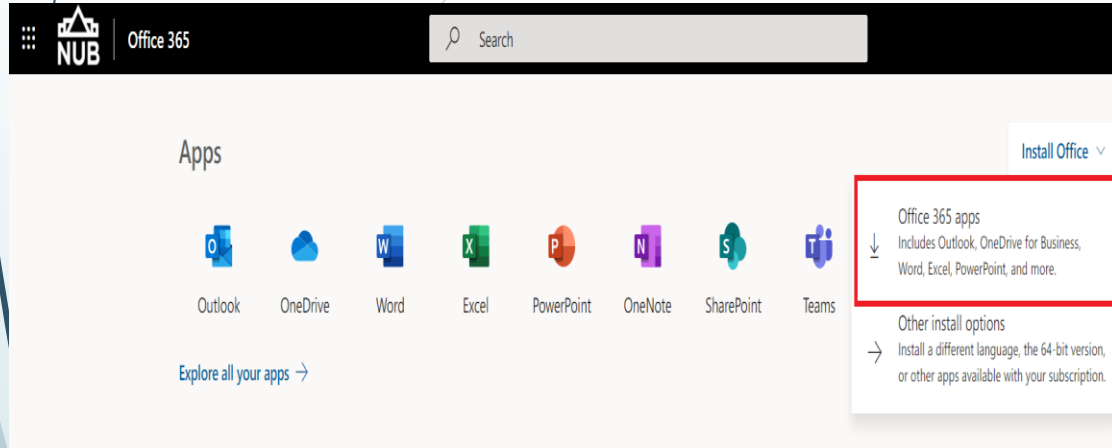
cancel



Office 365 Home Page showing the Apps section with icons for Outlook, OneDrive, Word, Excel, PowerPoint, OneNote, SharePoint, Teams, Class Notebook, Sway, and Forms. A search bar and an "Install Office" button are also visible.

Office 365

الحصول علي احدث اصدار من ميكروسوفت اوفيس



طريقة تفعيل التحقق بخطوتين



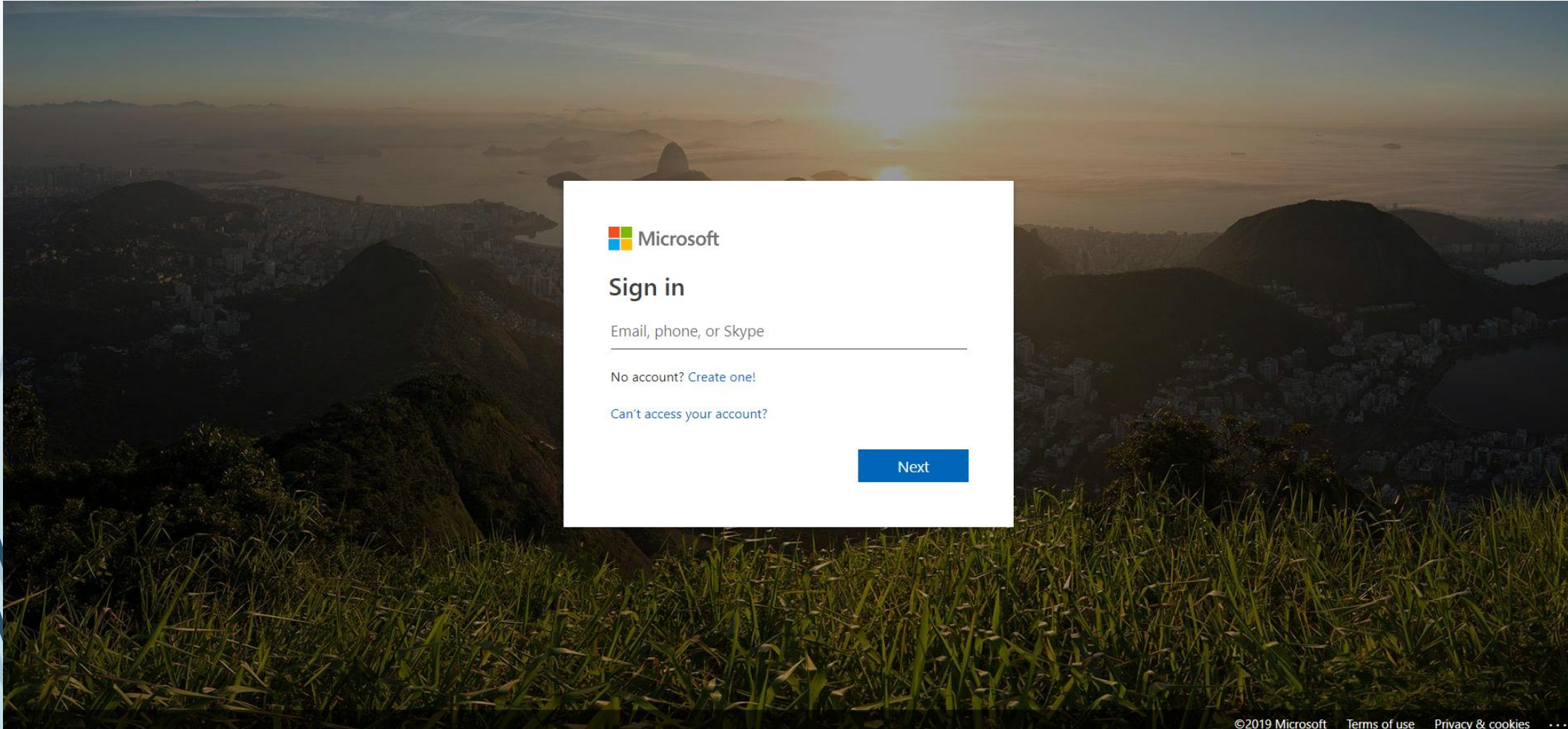
طريقة تفعيل التحقق بخطوتين

في البداية يجب تحميل برنامج Microsoft Authenticator by Microsoft Corporation



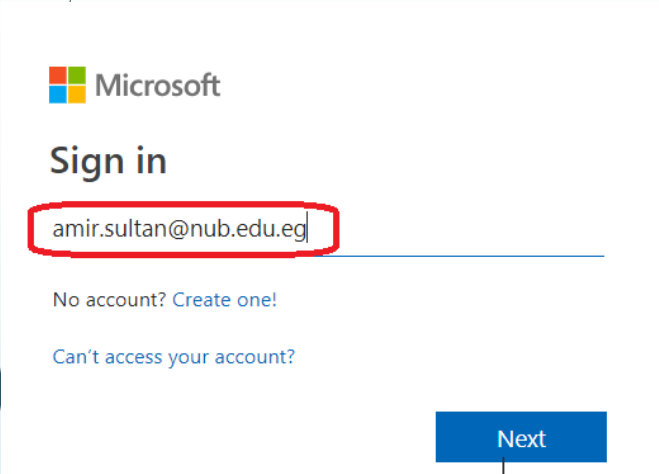
تفعيل التحقق بخطوتين

1- قم بفتح متصفح الانترنت [Google Chrome](#) او [Firefox](#) لزيارة الرابط التالي
[Portal.office365.com](https://portal.office365.com)

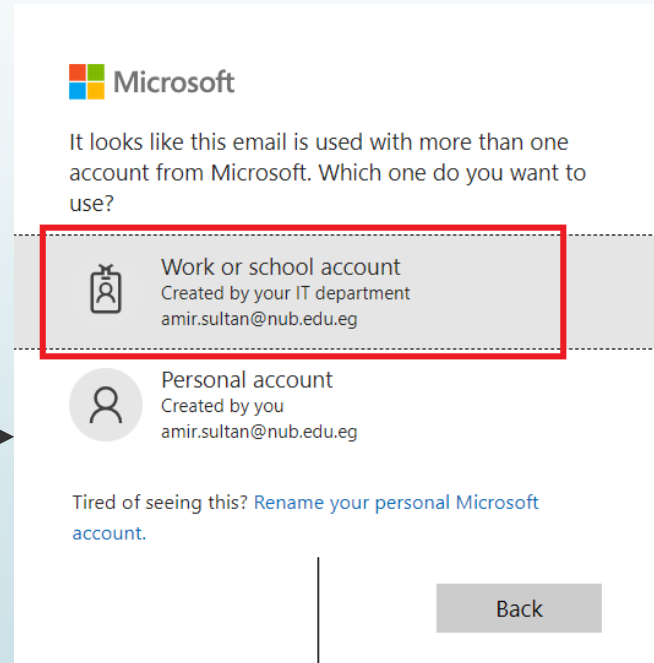


تفعيل التحقق بخطوتين

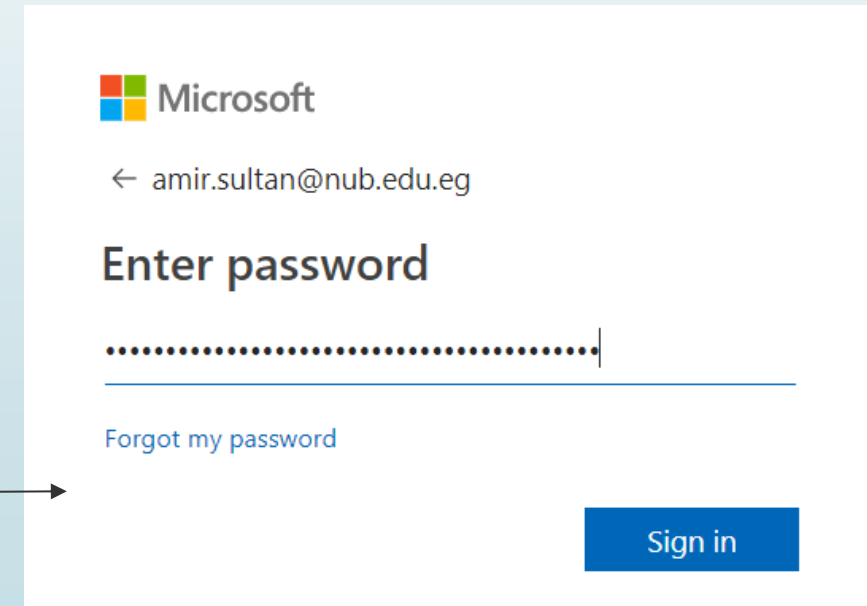
2- قم بكتابة الحساب الخاص بك بشكل كامل



Microsoft
Sign in
amir.sultan@nub.edu.eg
No account? [Create one!](#)
Can't access your account?
Next



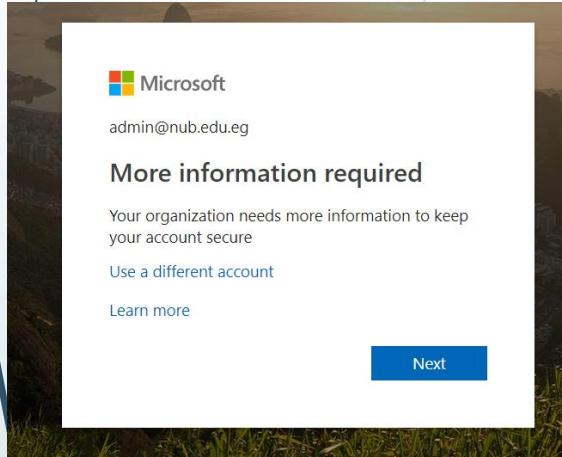
Microsoft
It looks like this email is used with more than one account from Microsoft. Which one do you want to use?
Work or school account
Created by your IT department
amir.sultan@nub.edu.eg
Personal account
Created by you
amir.sultan@nub.edu.eg
Tired of seeing this? [Rename your personal Microsoft account.](#)
Back



Microsoft
← amir.sultan@nub.edu.eg
Enter password
.....
[Forgot my password](#)
Sign in

تفعيل التحقق بخطوتين

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



Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Authentication phone

Egypt (+20) 1000343056

Method

Send me a code by text message

Call me

Next

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

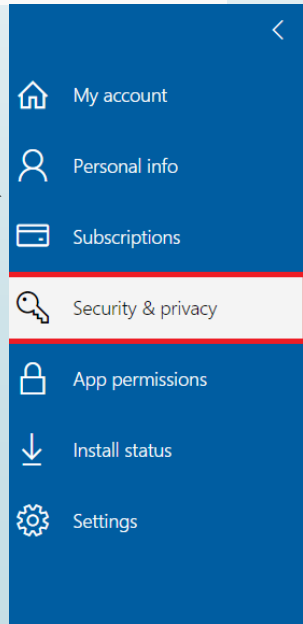
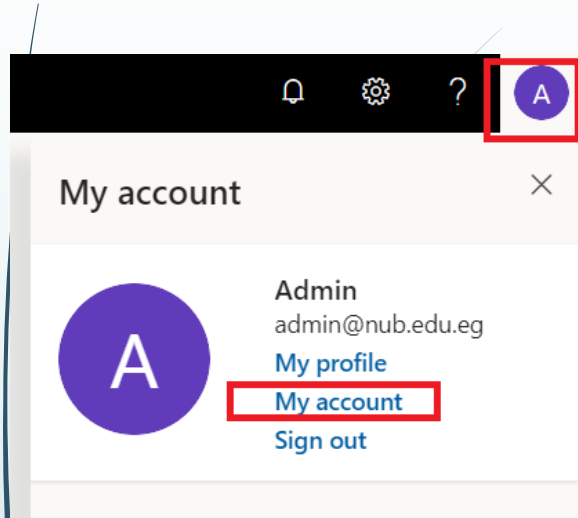
Step 2: We've sent a text message to your phone at +912186888

When you receive the verification code, enter it here

000000

Cancel Verify

طريقة تفعيل التحقق بخطوتين



Security & privacy

Password
Change your password.

Contact preferences
Manage how and why you are contacted.

Your settings aren't available right now. Please try again later.

Organization Privacy Statement
View your organization's Privacy Statement

Additional security verification
Your admin has turned on additional security verification to better secure your account.

To sign in to Office 365, you need to enter a password and reply back to the security message that is sent to your phone.
[Update your phone numbers used for account security.](#)

To sign into some apps installed on your computer or smart phone, you'll need to create an app password. When prompted by the app, enter the app password instead of your work or school account password.
[Create and manage app passwords](#)

طريقة تفعيل التحقق بخطوتين

Additional security verification App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
[View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Text code to my authentication p ▼

how would you like to respond?

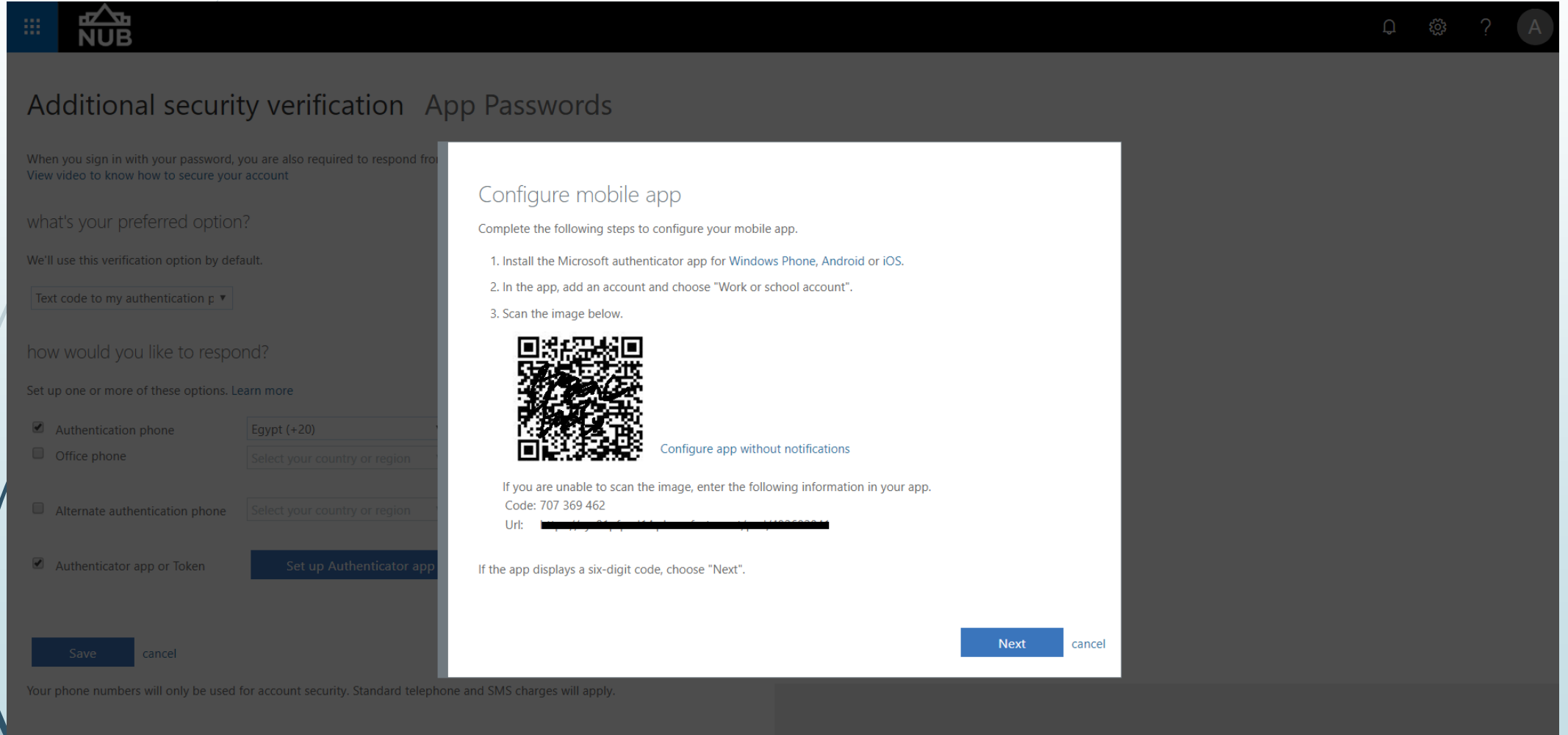
Set up one or more of these options. [Learn more](#)

<input checked="" type="checkbox"/>	Authentication phone	Egypt (+20) ▼	11 ٢٠٠٨٨٤
<input type="checkbox"/>	Office phone	Select your country or region ▼	Extension
<input type="checkbox"/>	Alternate authentication phone	Select your country or region ▼	
<input checked="" type="checkbox"/>	Authenticator app or Token	Set up Authenticator app	

Save cancel

طريقة تفعيل التحقق بخطوتين

قم بفتح التطبيق الذي تم تحميله على الموبايل
وجعل التطبيق QR-Code



Additional security verification App Passwords

When you sign in with your password, you are also required to respond from your phone. [View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Text code to my authentication p ▼

how would you like to respond?

Set up one or more of these options. [Learn more](#)

- Authentication phone Egypt (+20)
- Office phone Select your country or region
- Alternate authentication phone Select your country or region
- Authenticator app or Token **Set up Authenticator app**


Save cancel

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



[Configure app without notifications](#)

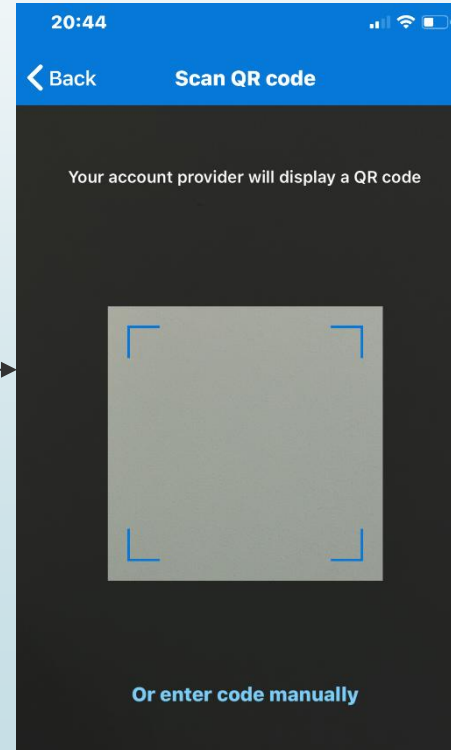
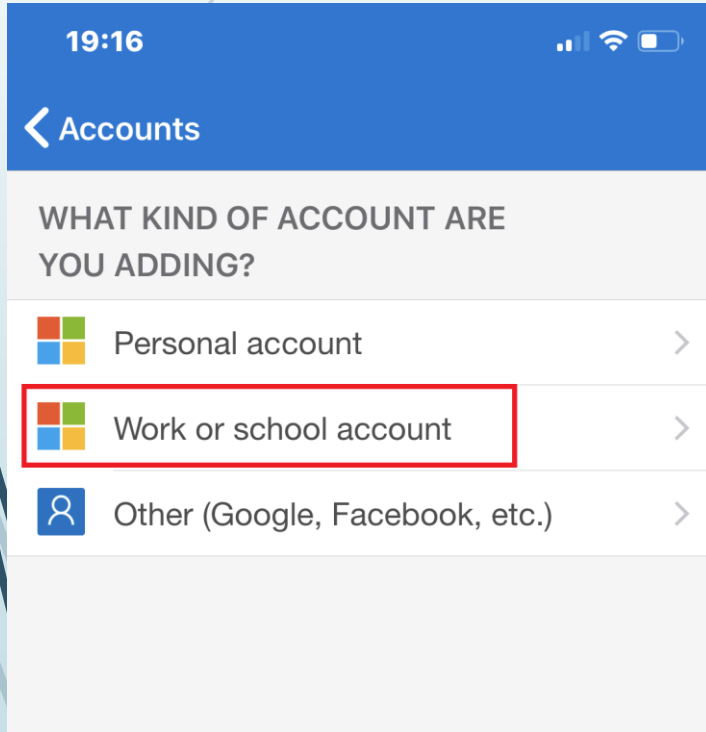
If you are unable to scan the image, enter the following information in your app.
Code: 707 369 462
Url: _____

If the app displays a six-digit code, choose "Next".

Next cancel

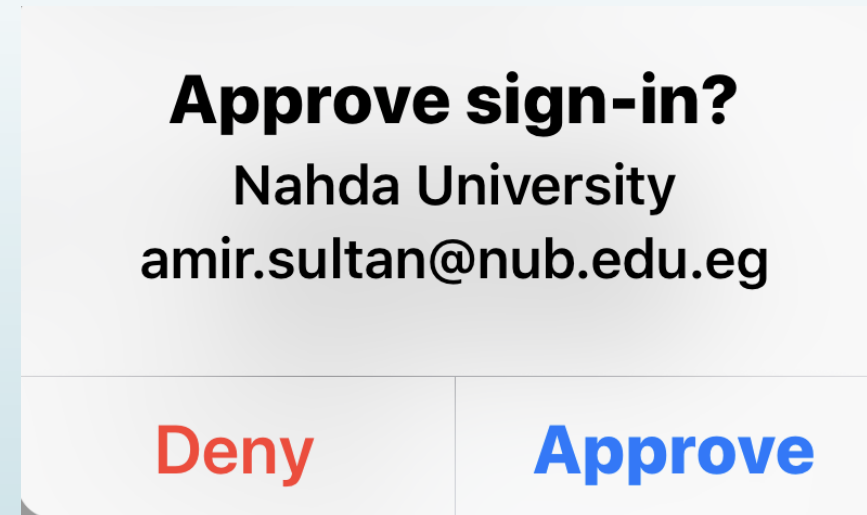
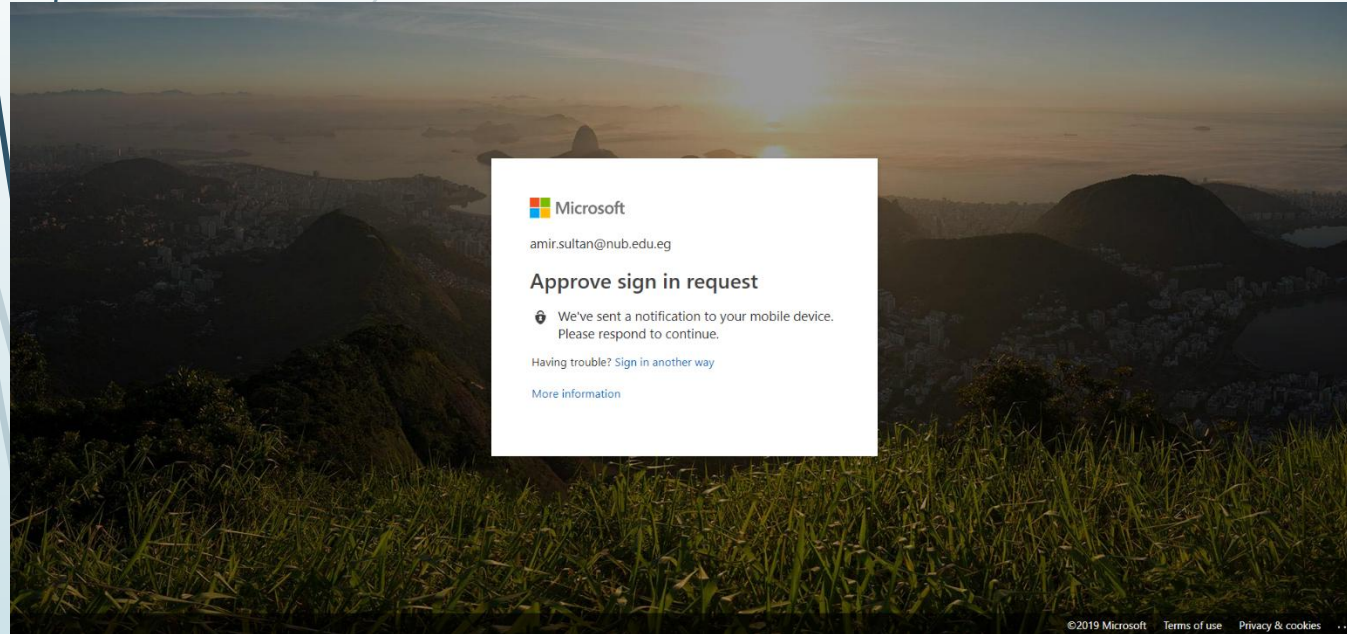
طريقة تفعيل التحقق بخطوتين

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



طريقة تفعيل التحقق بخطوتين

- بمجرد انتهاء 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)



My accounts

Amir Sultan
amir.sultan@nub.edu.eg
Available

My profile
Open another mailbox...
My account
Sign out

My account

Amir Sultan
IT Consultant, IT
2005

Personal info

Subscriptions

Security & privacy

App permissions

Install status

Settings

Why can't I edit?

About

First name
Amir

Last name
Sultan

Occupation
IT Consultant

Department
IT

Contact details

Email
amir.sultan@nub.edu.eg

Alias
amir.sultan

Mobile
+201000343056

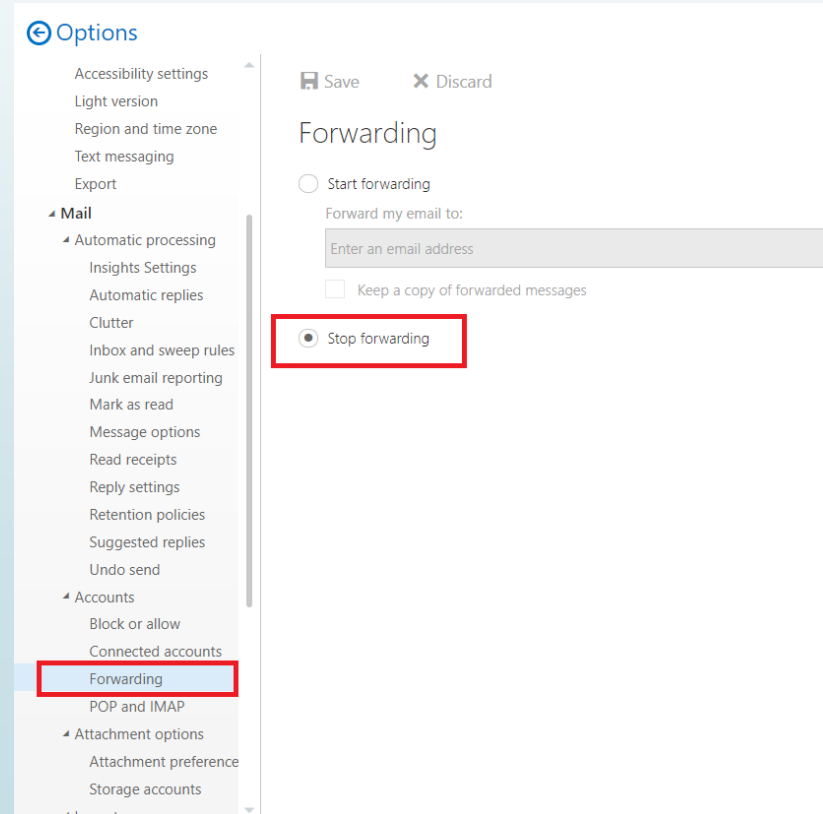
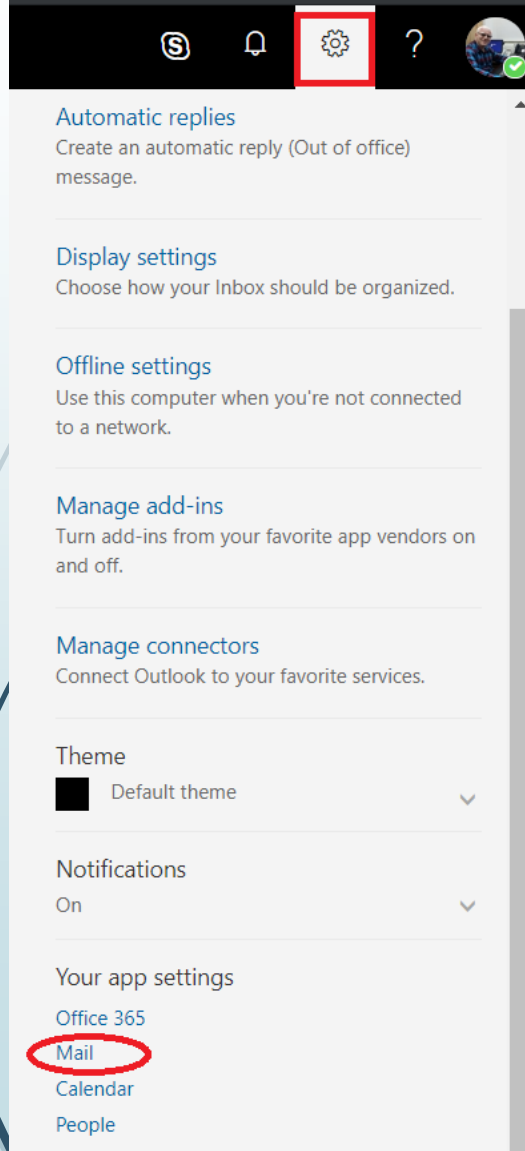
Phone
2001

Alternate email

مراجعة إعدادات حسابك

تفقد إعدادات حسابك

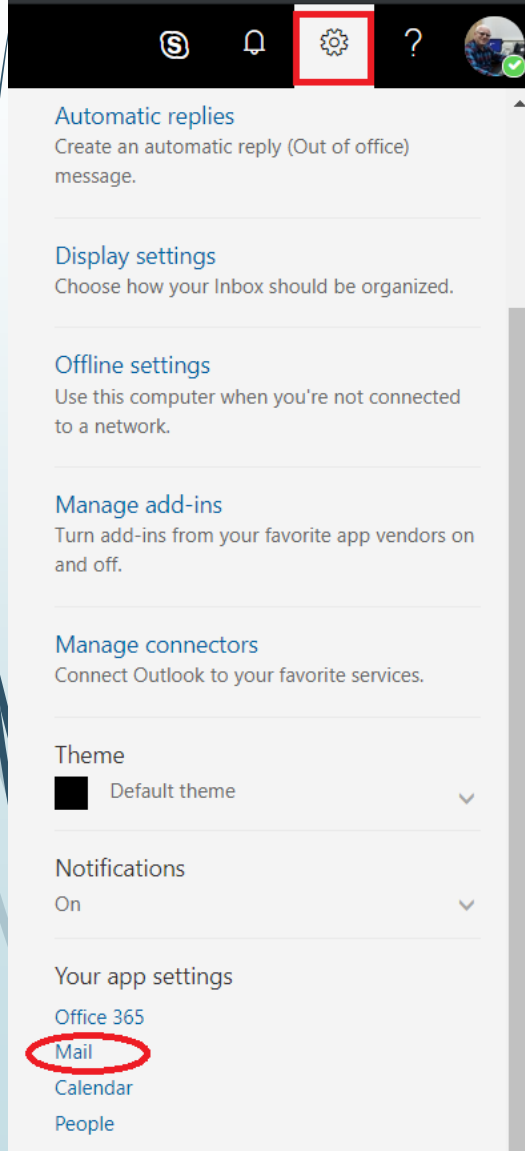
التأكيد علي عدم وجود Auto forwarding



مراجعة إعدادات حسابك

تفقد إعدادات حسابك

مراجعة الأجهزة المتصلة بحسابك وحذف أي جهاز غير معروف



Automatic replies
Create an automatic reply (Out of office) message.

Display settings
Choose how your Inbox should be organized.

Offline settings
Use this computer when you're not connected to a network.

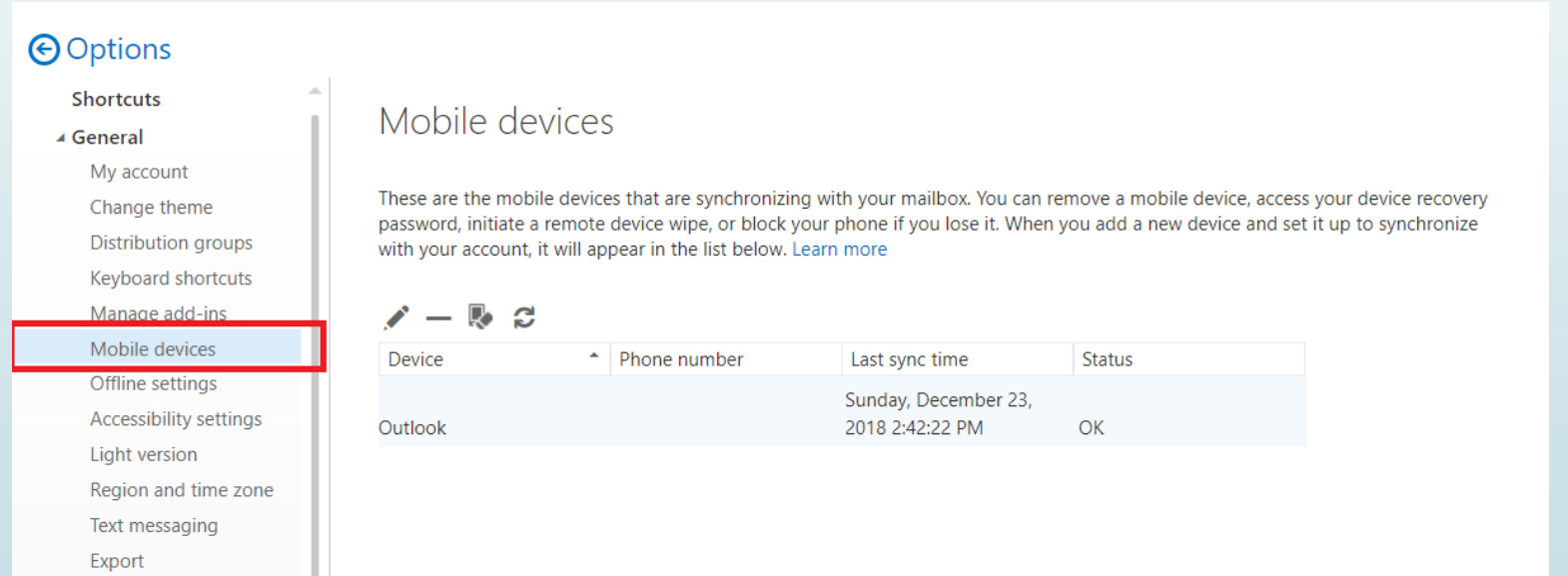
Manage add-ins
Turn add-ins from your favorite app vendors on and off.

Manage connectors
Connect Outlook to your favorite services.

Theme
Default theme

Notifications
On

Your app settings
Office 365
Mail
Calendar
People



Options

Shortcuts

General

- My account
- Change theme
- Distribution groups
- Keyboard shortcuts
- Manage add-ins
- Mobile devices
- Offline settings
- Accessibility settings
- Light version
- Region and time zone
- Text messaging
- Export

Mobile devices

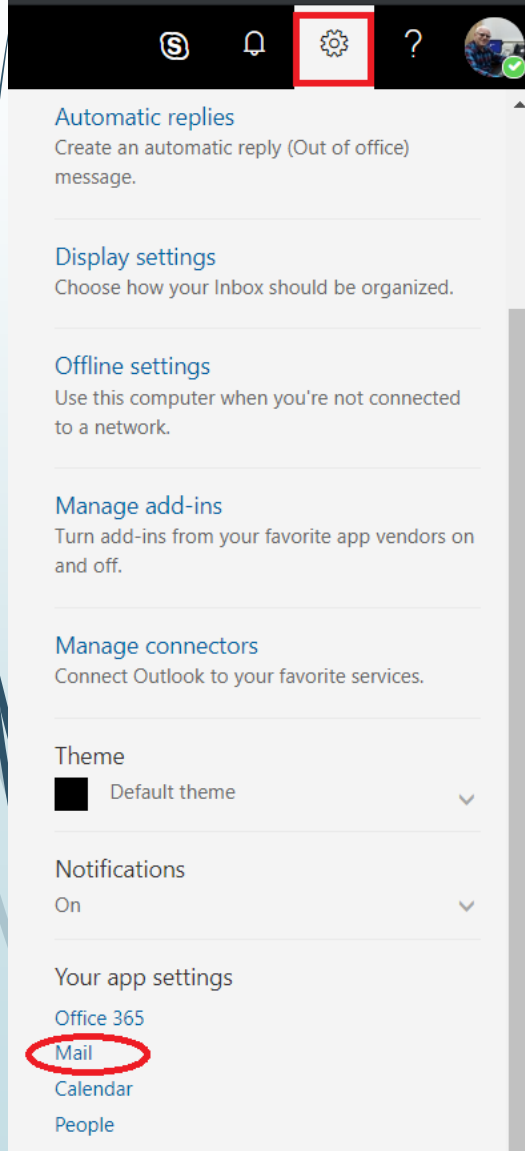
These are the mobile devices that are synchronizing with your mailbox. You can remove a mobile device, access your device recovery password, initiate a remote device wipe, or block your phone if you lose it. When you add a new device and set it up to synchronize with your account, it will appear in the list below. [Learn more](#)

Device	Phone number	Last sync time	Status
Outlook		Sunday, December 23, 2018 2:42:22 PM	OK

مراجعة إعدادات حسابك

تفقد إعدادات حسابك

مراجعة الجهات الممنوعة



Automatic replies
Create an automatic reply (Out of office) message.

Display settings
Choose how your Inbox should be organized.

Offline settings
Use this computer when you're not connected to a network.

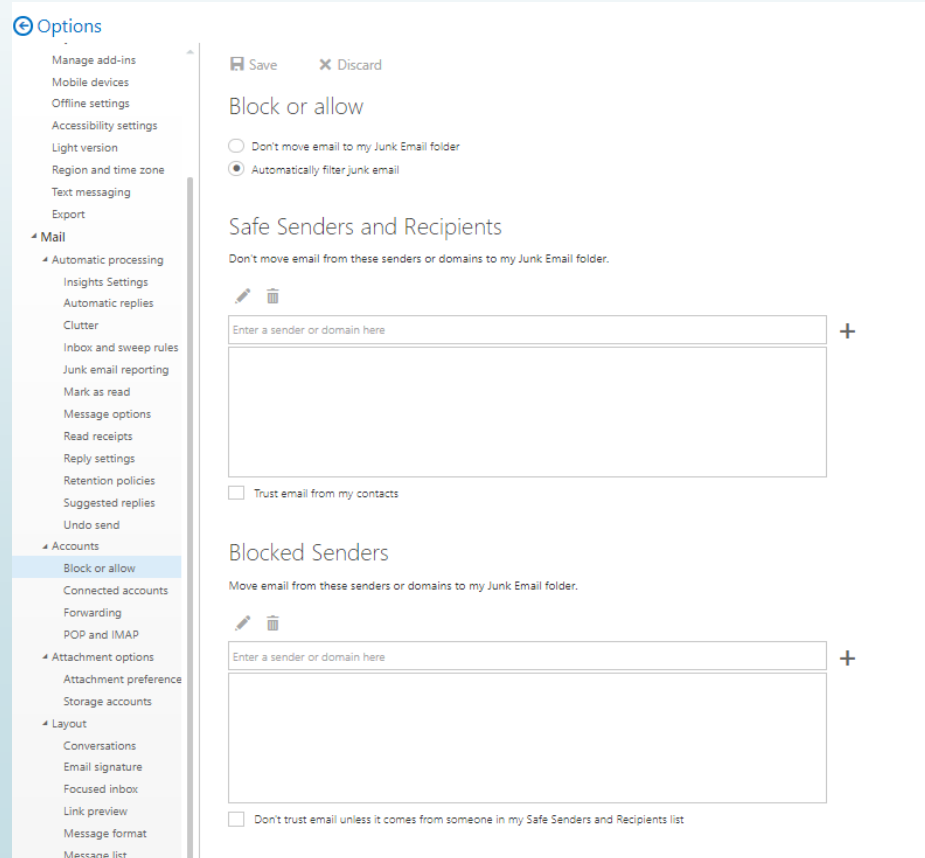
Manage add-ins
Turn add-ins from your favorite app vendors on and off.

Manage connectors
Connect Outlook to your favorite services.

Theme
Default theme

Notifications
On

Your app settings
Office 365
Mail
Calendar
People



Options

Manage add-ins
Mobile devices
Offline settings
Accessibility settings
Light version
Region and time zone
Text messaging
Export
Mail

Block or allow

Don't move email to my Junk Email folder
 Automatically filter junk email

Safe Senders and Recipients

Don't move email from these senders or domains to my Junk Email folder.

Enter a sender or domain here

Blocked Senders

Move email from these senders or domains to my Junk Email folder.

Enter a sender or domain here

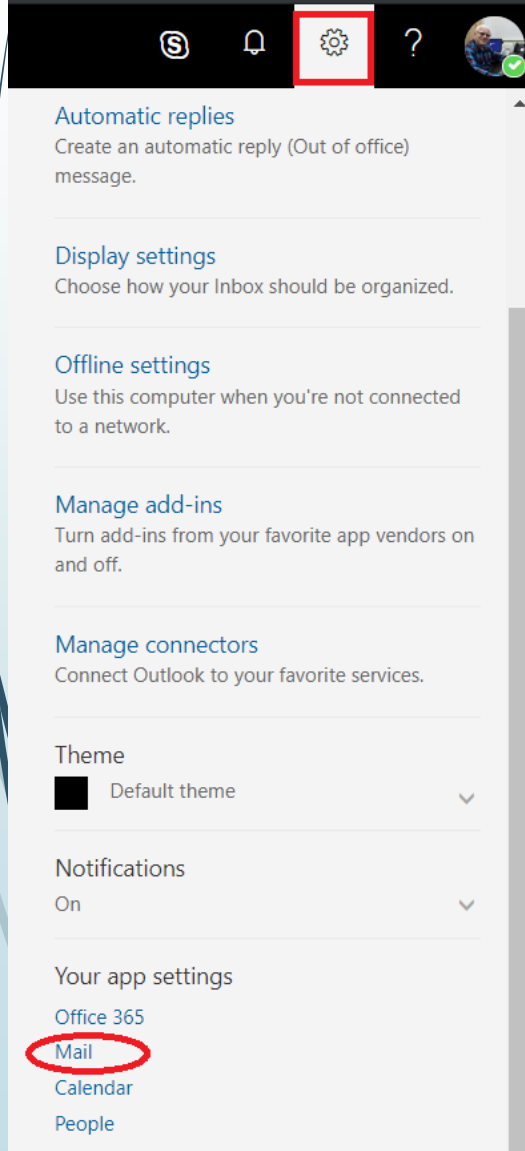
Trust email from my contacts

Don't trust email unless it comes from someone in my Safe Senders and Recipients list

في حالة الاختراق

تفقد إعدادات حسابك

مراجعة القواعد والإجراءات



Automatic replies
Create an automatic reply (Out of office) message.

Display settings
Choose how your Inbox should be organized.

Offline settings
Use this computer when you're not connected to a network.

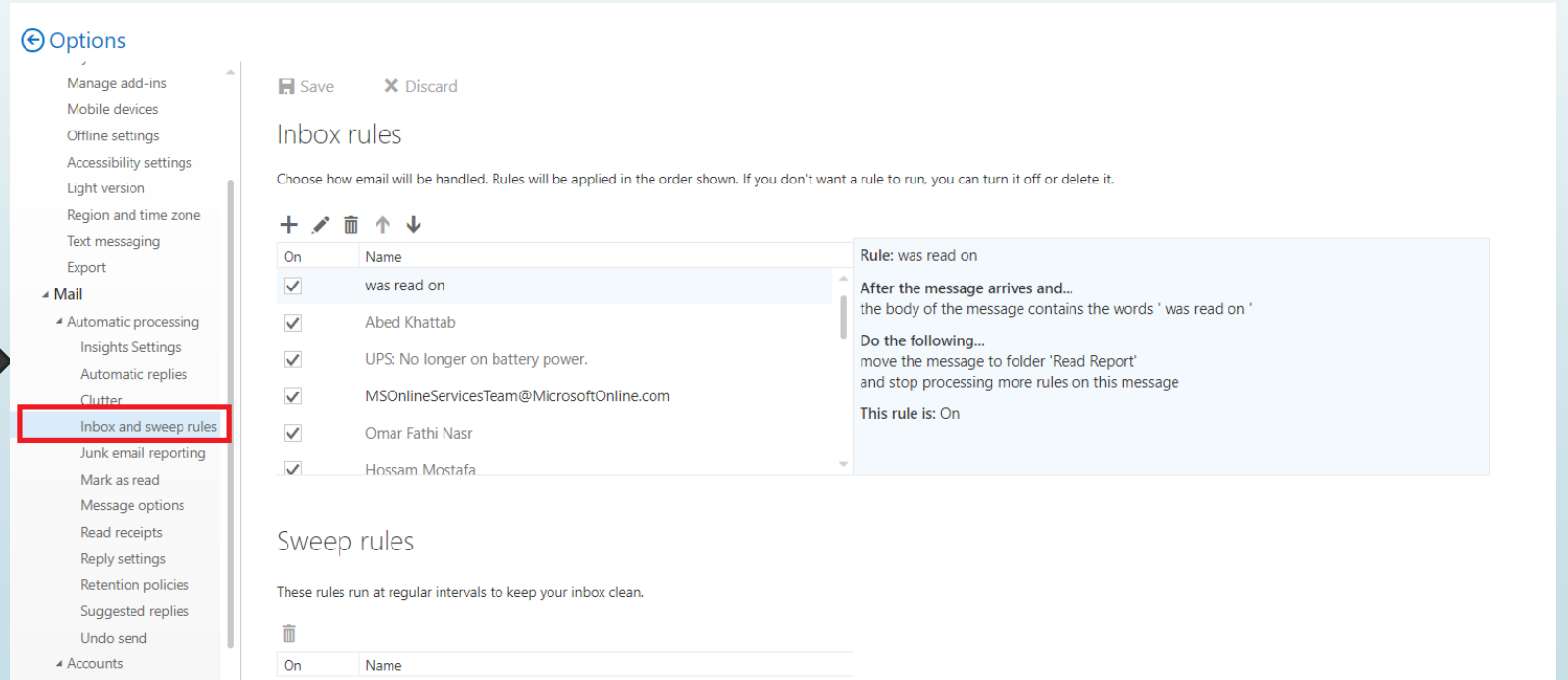
Manage add-ins
Turn add-ins from your favorite app vendors on and off.

Manage connectors
Connect Outlook to your favorite services.

Theme
Default theme

Notifications
On

Your app settings
Office 365
Mail
Calendar
People



Options

Manage add-ins
Mobile devices
Offline settings
Accessibility settings
Light version
Region and time zone
Text messaging
Export

Mail

Automatic processing
Insights Settings
Automatic replies
Clutter
Inbox and sweep rules
Junk email reporting
Mark as read
Message options
Read receipts
Reply settings
Retention policies
Suggested replies
Undo send

Accounts

Save Discard

Inbox rules

Choose how email will be handled. Rules will be applied in the order shown. If you don't want a rule to run, you can turn it off or delete it.

On	Name
<input checked="" type="checkbox"/>	was read on
<input checked="" type="checkbox"/>	Abed Khattab
<input checked="" type="checkbox"/>	UPS: No longer on battery power.
<input checked="" type="checkbox"/>	MSONlineServicesTeam@MicrosoftOnline.com
<input checked="" type="checkbox"/>	Omar Fathi Nasr
<input checked="" type="checkbox"/>	Hossam Mostafa

Rule: was read on

After the message arrives and...
the body of the message contains the words ' was read on '

Do the following...
move the message to folder 'Read Report'
and stop processing more rules on this message

This rule is: On

Sweep rules

These rules run at regular intervals to keep your inbox clean.

On	Name
----	------

في حالة الاختراق

مراجعة تسجيل الدخول والابلاغ عن وجود نشاط غير معروف

Recent activity

You should recognize each of these recent activities. If one looks unfamiliar, you should review your [security info](#).

Time	Location	IP	App	Account	Status
Today at 9:30:57 PM EET	Jawa Timur, ID	118.█.█.22	Office 365 Exchange Online	amir.sultan@nub.edu.eg	Unsuccessful sign-in
Today at 9:07:05 PM EET	New Jersey, US		Office 365 Exchange Online		Unsuccessful sign-in
Today at 8:45:29 PM EET	Kyiv Misto, UA		Office 365 Exchange Online		Unsuccessful sign-in
Today at 12:51:10 PM EET	Al Jizah, EG		Microsoft Teams Web Client		Successful sign-in
Yesterday at 9:13:47 AM EET	Florida, US		Office 365 Exchange Online		Unsuccessful sign-in
Yesterday at 8:58:54 AM EET	Seoul Teukbyeolsi, KR		Office 365 Exchange Online		Unsuccessful sign-in
Yesterday at 7:30:41 AM EET	Punjab, PK		Office 365 Exchange Online		Unsuccessful sign-in

[Look unfamiliar? Secure your account](#)



تأمين حساب فيسبوك

- General**
- Security and Login
- Your Facebook Information
- Privacy
- Timeline and Tagging
- Location
- Blocking
- Language
- Face Recognition
- Notifications
- Mobile
- Public Posts

General Account Settings

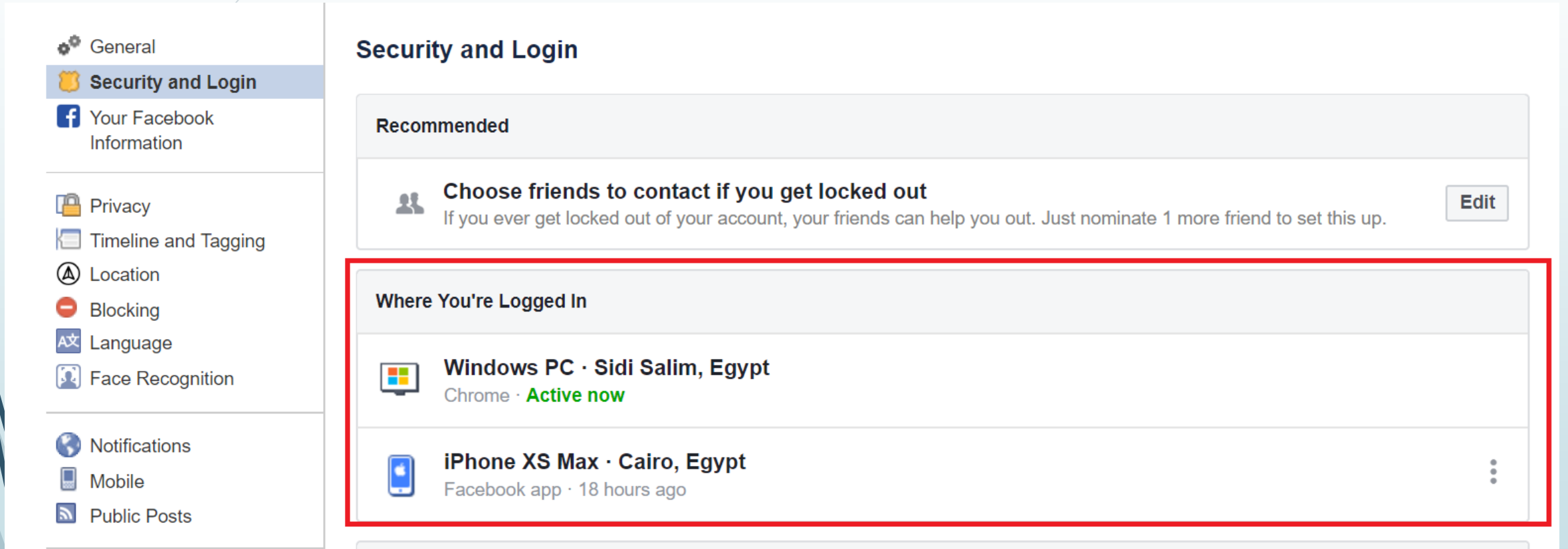
Name	Amir Sultan	Edit
Username	https://www.facebook.com/amirsultan79	Edit
Contact	Primary Contact	

Add another email or mobile number

Allow friends to include my email address in [Download Your Information](#)

Save Changes Cancel

تأمين حساب فيسبوك



The image shows a screenshot of the Facebook 'Security and Login' settings page. The left sidebar contains navigation options: General, Security and Login (selected), Your Facebook Information, Privacy, Timeline and Tagging, Location, Blocking, Language, Face Recognition, Notifications, Mobile, and Public Posts. The main content area is titled 'Security and Login' and includes a 'Recommended' section with a prompt to 'Choose friends to contact if you get locked out' and an 'Edit' button. Below this is a section titled 'Where You're Logged In', which is highlighted with a red border. This section lists two active sessions: 'Windows PC · Sidi Salim, Egypt' using Chrome, marked as 'Active now', and 'iPhone XS Max · Cairo, Egypt' using the Facebook app, marked as '18 hours ago'. A three-dot menu icon is visible next to the iPhone session.

General

Security and Login

Your Facebook Information

Privacy

Timeline and Tagging

Location

Blocking

Language

Face Recognition

Notifications

Mobile

Public Posts

Security and Login

Recommended

Choose friends to contact if you get locked out [Edit](#)

If you ever get locked out of your account, your friends can help you out. Just nominate 1 more friend to set this up.

Where You're Logged In

Windows PC · Sidi Salim, Egypt
Chrome · **Active now**

iPhone XS Max · Cairo, Egypt
Facebook app · 18 hours ago

تأمين حساب فيسبوك

General

Security and Login

Your Facebook Information

Privacy

Timeline and Tagging

Location

Blocking

Language

Face Recognition

Notifications

Mobile

Public Posts

Login



Change password

It's a good idea to use a strong password that you're not using elsewhere

Edit



Log in with your profile picture

On • Tap or click your profile picture to log in, instead of using a password

Close

THIS BROWSER

Remember password

Just click your profile picture to log in

Turn off profile picture login

Use email or phone number to log in

OTHER DEVICES & BROWSERS

Remove profile picture login from Facebook for iOS on iOS 12

Last used Today at 12:14 PM

No passcode

تأمين حساب فيسبوك

General

Security and Login

Your Facebook
Information

Privacy

Timeline and Tagging

Location

Blocking

Language

Face Recognition

Notifications

Mobile

Public Posts

Two-Factor Authentication



Use two-factor authentication

On • We'll ask for a security code if we notice a login from an unusual device

Edit

تأمين حساب فيسبوك

General

Security and Login

Your Facebook
Information

Privacy

Timeline and Tagging

Location

Blocking

Language

Face Recognition

Notifications

Mobile

Public Posts

Authorized Logins

Review a list of devices where you won't have to use a login code

Close

This device:

Chrome on Windows January 28, 2019

Other devices:

Facebook for iPhone March 3, 2019

Remove

تأمين حساب فيسبوك

General

Security and Login

Your Facebook Information

Privacy

Timeline and Tagging

Location

Blocking

Language

Face Recognition

Notifications

Mobile

Public Posts

Setting Up Extra Security



Get alerts about unrecognized logins

On • We'll let you know if anyone logs in from a device or browser you don't usually use

Close

Get an alert when anyone logs into your account from an unrecognized device or browser.

Notifications

Get notifications

Don't get notifications

Messenger

Get notifications

Don't get notifications

Email

Email login alerts to [redacted]

Don't get email alerts

Add another email or mobile number

Save Changes

تأمين حساب فيسبوك




Privacy







- Timeline and Tagging
- Location
- Blocking
- Language
- Face Recognition




How People Find and Contact You








Who can send you friend requests?	Everyone	Edit
Who can see your friends list? Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends.	Only me	Edit
Who can look you up using the email address you provided?	Friends	Edit
Who can look you up using the phone number you provided?	Friends	Edit
Do you want search engines outside of Facebook to link to your profile?	Yes	Edit

تأمين حساب فيسبوك


-  General
-  Security and Login
-  Your Facebook Information

-  Privacy
-  **Timeline and Tagging**
-  Location
-  Blocking
-  Language
-  Face Recognition

-  Notifications
-  Mobile
-  Public Posts

-  Apps and Websites
-  Instant Games
-  Business Integrations
-  Ads
-  Payments
-  Support Inbox
-  Videos

Timeline and Tagging Settings

Timeline	Who can post on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends of friends	Edit
	Allow post sharing to stories?	On	Edit
	Hide comments containing certain words from your timeline	On	Edit
Tagging	Who can see posts you're tagged in on your timeline?	Friends of friends	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Friends	 Edit
Review	Review posts you're tagged in before the post appears on your timeline?	On	Edit
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

تأمين حساب فيسبوك

Timeline ▾ About Friends 771 Photos Archive More ▾

About


Overview
Work and Education
Places You've Lived
Contact and Basic Info
Family and Relationships
Details About You
Life Events

CONTACT INFORMATION

Mobile Phones

Address 30 Borhan st
Helwan, Egypt

Neighborhood Helwan

Email 

[+ Add / Remove Emails](#)

[Save Changes](#) [Cancel](#)

WEBSITES AND SOCIAL LINKS

Social Links amirsultan79 (Skype)

[+ Add a website](#)

BASIC INFORMATION

Birth Date July 10

Birth Year 1979

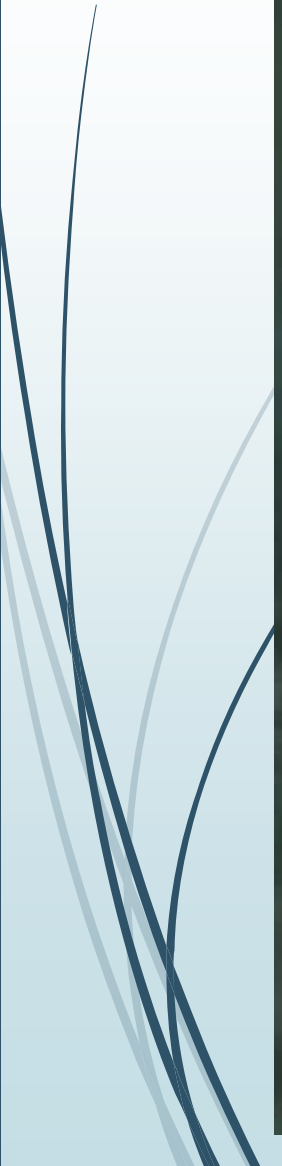
Gender Male

Languages **Arabic** English language

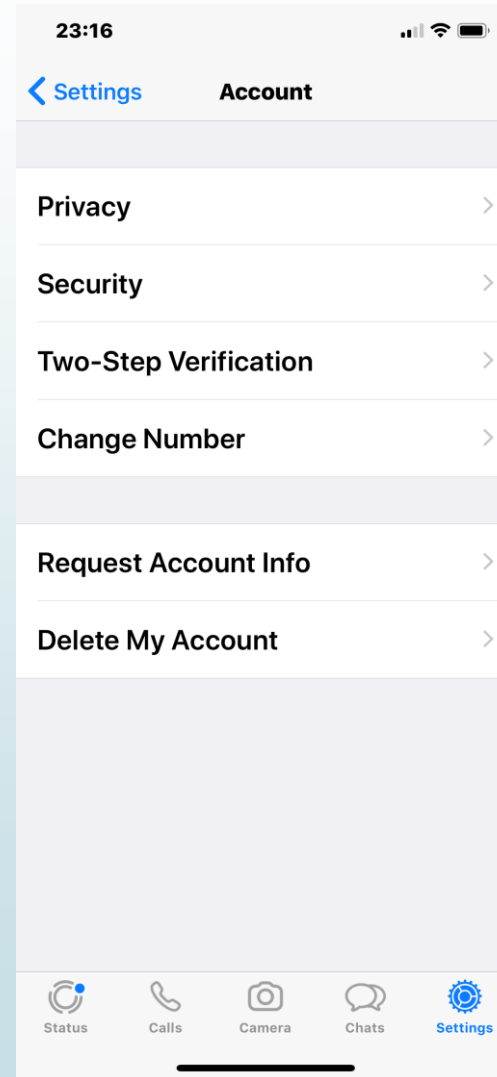
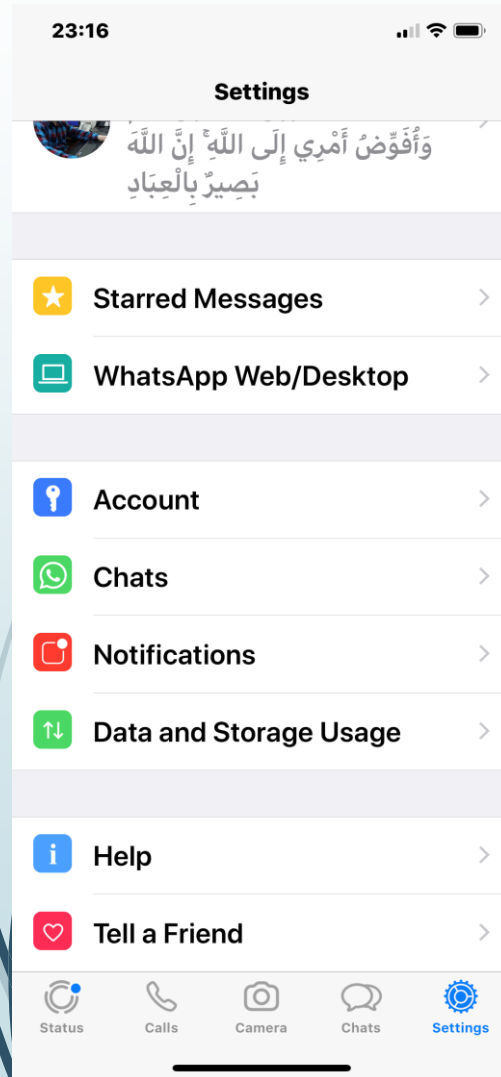
Religious Views **Lslam**
لا اله الا الله محمد رسول الله

[+ Add who you're interested in](#)

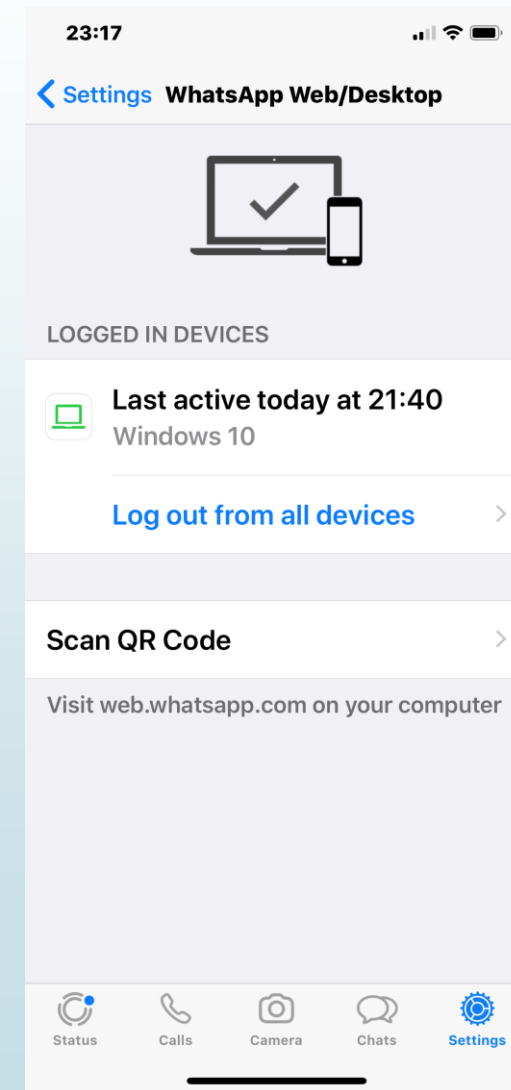
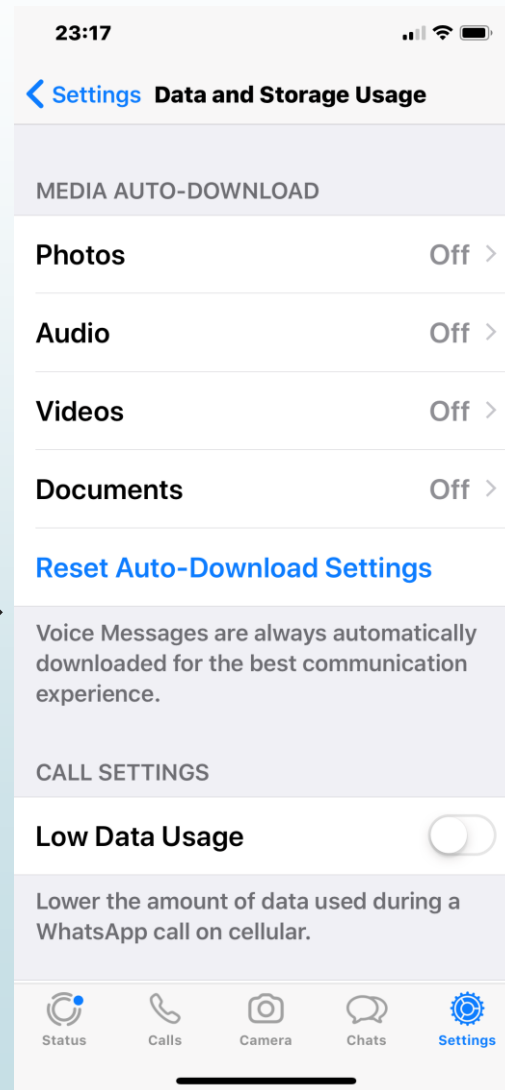
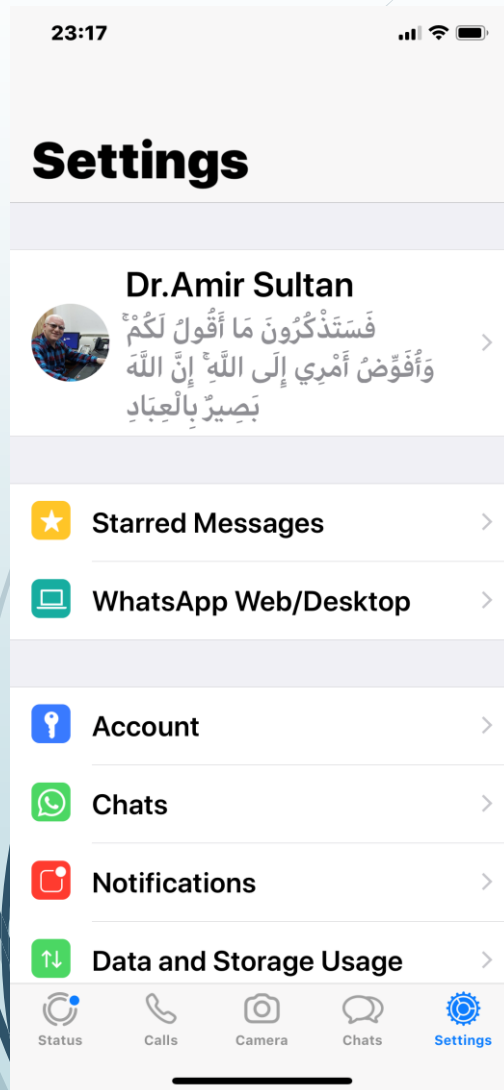
[+ Add your political views](#)



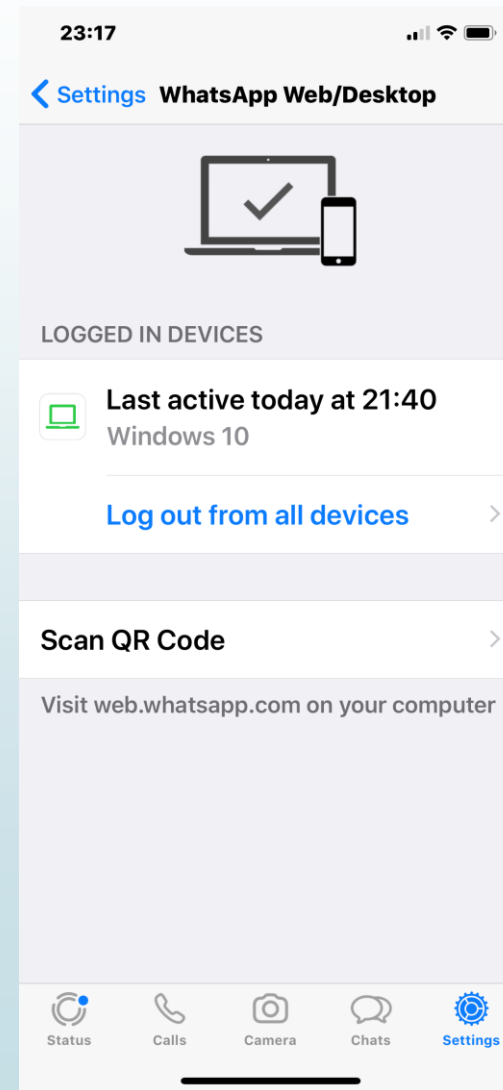
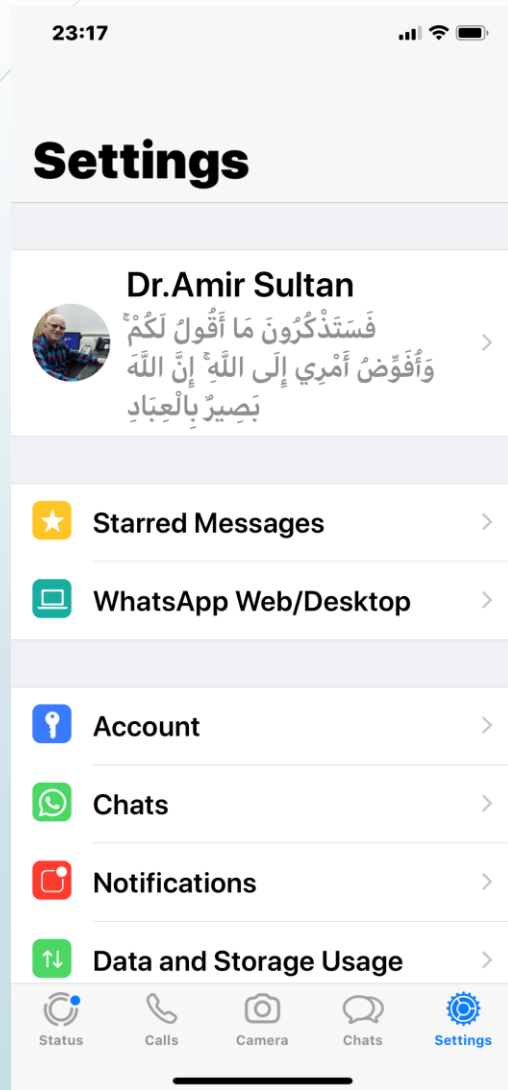
WhatsApp Security



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](https://www.linkedin.com/in/amirsultan79)

