الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

سابك
sabic

البرنامج الوطني للتوعية بالأمن السيبراني

آمن

إرشادات الممارسات الصحيحة للأمن السيبرانى

كيمياء وتواصل™

الفهرس

سابك
sabic

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

إبقى امناً

حصن أجهزتك

قم بتحديث البرامج الخاصة بك

يجب فحص وتحديث جميع البرامج الخاصة بك الى أحدث إصدار.

قم بتثبيت برامج مكافحة الفيروسات

تقوم برامج مكافحة الفيروسات باكتشاف وإزالة البرامج الضارة التي يمكن أن تؤثر على الجهاز الخاص بك لذا يجب تثبيت برنامج مكافحة الفيروسات وتحديثه بشكل دوري.

قم بتفعيل برنامج جدار الحماية

يقوم جدار الحماية بإنشاء حاجز بين جهاز الكمبيوتر الخاص بك والشبكة الخارجية الذي بدوره يمنع الدخول الغير مصرح به.

احرص على تثبيت التطبيقات من المصادر الموثوقة

التأكد من تثبيت التطبيقات من المتجر الخاص بجهازك. قبل تثبيتك لأي من التطبيقات, تحقق من التطبيق عن طريق قراءة الوصف الخاص به والاطلاع على تعليقات المستخدمين. بالإضافة الى ذلك تحقق من صلاحيات التطبيق والسماح فقط بما يناسب احتياجك.

قم بعمل نسخة احتياطية لبياناتك

قم بحماية بياناتك عن طريق إجراء نسخ احتياطي بشكل دوري لحفظ نسخة الكترونية وتخزينها بأمان في جهازك.

الحسابات وكلمات المرور

1. تفعيل المصادقة الثنائية:

قم باستخدام خاصية إضافية من الأمان لتسجيل الدخول الخاص بك, مثل القياسات الحيوية (بصمة الاصبع وبصمة الوجه.. الخ), مفاتيح الأمان أو كلمة المرور لمره واحدة التي يتم إرسالها إلى جهازك المحمول, اجعل كلمة مرورك قوية قدر الإمكان.

لضمان أن تكون كلمات المرور قوية اتبع النقاط التالية:

- اجعل كلمة المرور طويلة بقدر 12 حرفًا على الأقل.
- اجعل كلمة مرورك مكونة من الكلمات والعبارات بشكل عشوائي.
- احرص على ان تشمل الأرقام والرموز والأحرف الكبيرة والصغيرة.
- تجنب استخدام المعلومات الشخصية الواضحة.
- لا تقم بتكرار استخدام كلمة المرور لأكثر من حساب او تطبيق لديك.
- احرص على تغيير كلمة المرور بانتظام.

2. لا تقم باختيار ميزة "تذكرني":

تجنب استخدام ميزة تذكرني على متصفح الويب لتسجيل الدخول إلى الحسابات.

افصل بين حساب العمل وحساباتك الشخصية وتأكد من استخدام كلمات مرور قوية ومختلفة لكل حساب.

3. قم بحماية معلوماتك الشخصية:

كن حذراً من المواقع التي تقوم بزيارتها وتأكد من أنك تتصفح موقع موثوق قبل إدخال أي معلومات شخصية. بالإضافة الى ذلك كن حذرًا من الاتصالات والرسائل التي تدعوك إلى التصرف فوراً أو تطلب معلومات شخصية منك.

4. قم بحماية معاملاتك المصرفية:

- حافظ على بطاقة الائتمان الخاصة بك بأمان
- تذكر رقم التعريف الشخصي لبطاقة الصراف الآلي والائتمان الخاصة بك
- قم بتغيير الرقم السري / كلمة المرور الخاصة بالخدمات المصرفية عبر الإنترنت بشكل دوري
- كن حذرًا عند إجراء المعاملات في مراكز الصراف الآلي
- تحقق من المعاملات في حسابك بانتظام وأبلغ البنك في حال لاحظت معاملات غير مصرح بها
- قم بإخفاء وتغطية الرقم السري CVV الذي يكون خلف البطاقة
- احذر من طرق الدفع الغير معتادة مثل: بطاقات الهدايا, العملات الرقمية
- ضع في اعتبارك بطاقة ائتمان ذات حد منخفض اثناء تسوقك عبر الانترنت

الأمن السيبراني في الأماكن العامة

1. كن حذرا من شبكات الاتصال اللاسلكية العامة (Wi-Fi)

- تعتبر الشبكات اللاسلكية العامة ونقاط الاتصال بالإنترنت كالتي في المطارات والمقاهي ليست امنة, مما يعني انه من الممكن لأي شخص ان يقوم باختراق الشبكة العامة والاطلاع على ما تقوم بتصفحه او أي عمليات أخرى.
- لا تقم بأجراء أي من العمليات المالية أو الحساسة اثناء الاتصال بالشبكات اللاسلكية العامة. وفي حال الضرورة لذلك, قم بالتأكد بأن صفحة الويب آمنة ومشفرة وتتضمن بروتوكول (HTTPs).

2. كن حذرا من الأجهزة العامة

تعتبر الأجهزة العامة التي تتواجد في المطارات او المقاهي او الفنادق غير آمنة او تحتوي على برمجيات خبيثة. لذلك لا تقم بإيصال أي من اجهزتك الخاصة بها, مثل هاتفك المحمول.

3. كن حذرا من محطات إعادة الشحن العامة

المحطات العامة المستخدمة لإعادة شحن الأجهزة الذكية كالمستخدمة في المطارات يمكن التلاعب بها ليتم استخدامها بطرق خبيثة لسرقة البيانات من الأجهزة الذكية. للمحافظة على أمن بياناتك قم باستخدام وحدة الشحن المتنقلة الخاصة بك. وفي حال الضرورة لاستخدام محطات الشحن العامة قم بأغلاق الجهاز كليا قبل توصيله.

4. تعطيل ميزات الشبكة الغير ضرورية

في حال كونك متواجد في أحد الأماكن العامة قم بإيقاف ميزات الشبكة كالبلوتوث او الواي فاي عند عدم الحاجة لها لحمايتك أمنياً من هجمات التنصت.

5. كن حذرا من اختلاس النظر

عند استخدام اجهزتك الذكية في الأماكن العامة كن حذرا من ان يتم اختلاس النظر اليك من قبل الأشخاص الاخرين في حال ادخالك لأي من المعلومات الشخصية.

التصيّد وانتحال الشخصية

أنواع التصيّد

التصيّد يأتي بعدة أشكال اما عن طريق رسائل البريد الالكتروني والرسائل النصية أو عن طريق منصات التواصل الاجتماعي.

من العلامات الدالة على وجود التصيّد

يتم استقبال الرسائل من جهات مجهولة أو من جهات غير رسمية.

أمثلة شائعة

يمكن أن تأتي عمليات الاحتيال على شكل عروض مزيفه, أو رسائل تهديد (على سبيل المثال: سيتم قفل حسابك إذا لم تقم بالتحديث).

مؤشرات رسائل التصيّد

- **المحفزات العاطفية**

يستغل المهاجمون المشاعر من خلال توليد شعور زائف بالإلحاح أو الخوف أو الفضول للحث على اتخاذ إجراء بشأن الرابط المشبوه.

- **أخطاء نحوية أو إملائية**

الأخطاء النحوية والإملائية مؤشرات مهمة لهجمات التصيّد الإلكتروني وخاصة البريد الإلكتروني.

- **المحتوى**

العروض المزيفة والمكافآت غير المتوقعة والتي تتطلب معلومات سرية ومحتوى وسياق غير ذي صلة, بالإضافة إلى الرسائل من مصدر غير معروف تعتبر مؤشرات للتصيّد الإلكتروني.

- **المرفقات**

يمكن استخدام الصور أو المرفقات في مثل هذه الرسائل لتجنب اكتشاف البرامج الضارة المضمنة.

نصائح لحماية نفسك من هجمات التصيّد

- تأكد من هوية الأشخاص الذين يتواصلون معك عبر مواقع التواصل الاجتماعي
- كن حذراً أثناء الاتصال بشبكة الإنترنت, لأن التصيّد الإلكتروني يعتمد بشكل أساسي على إقناع المستخدمين بأساليب مختلفة مما يسهل عليهم عملية الاختراق.
- يجب عليك قراءة محتوى الرسالة الواردة بشكل جيد وأخذ مؤشرات التصيّد بعين الاعتبار عندما تصلك رسالة إلكترونية من أشخاص مجهولين.
- احرص دائمًا على قراءة الرابط الخاص بالموقع الإلكتروني او رسالة البريد الإلكتروني بشكل جيد قبل الضغط عليه من خلال مقارنته مع الرابط الذي يظهر لك عند تمرير المؤشر عليه
- احرص على فحص الروابط قبل الضغط عليها حيث يمكنك الاستعانة ببعض الأدوات الأمنية المتاحة الموثوقة لفحص الروابط الخبيثة.
- تذكر أن الاختراقات السيبرانية انتشرت بشكل واسع على شبكة الإنترنت, لذلك لا تجري المعاملات المصرفية عبر الشبكات اللاسلكية العامة غير المعروفة, لأن المعاملات المصرفية تصبح غير آمنة في ظل هذا التهديد.
- احرص على التحقق من الموقع عبر إدخال كلمة مرور وهمية فإذا تم رفض هذه الكلمة فذلك يدل على موثوقية الموقع, وذلك لوجود قاعدة بيانات يتم من خلالها التحقق من المعلومات المدخلة.
- عند اشتباهك بعملية تصيد, قم بالتأكد عن طريق الاتصال بالشركة او التأكد من موقع الشركة.

سابك
sabic

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الرقابة الأبوية

أجهزة iOS

يتحول استخدام الهواتف الذكية للأطفال، إلى مصدر قلق وخطر كبير لعدد كبير من الاباء، وهو ما يتسبب في إبعادنا لأي أجهزة ذكية عنهم. هناك مجموعة من الضوابط التي وضعتها شركة "أبل" لجعل استخدام الأجهزة الذكية "آمنا" للأطفال. ولتفعيل أدوات "المراقبة الأبوية" يمكن اتباع تلك الخطوات التالية:

- اذهب إلى إعدادات الجهاز أو الحاسب اللوحي, ثم توجه إلى أيقونة **"عام"**, وانتقل إلى أيقونة **"القيود"**, وادخل رمز المرور الخاص بتلك الأيقونة, حتى لا يتمكن طفلك من الدخول إليها وتغيير اعداداتها.

- عند الدخول إلى أيقونة القيود, سيمكنك تعطيل عمل عدد من التطبيقات, التي لا ترغب أن يستخدمها طفلك, مثل استخدام الكاميرا على تطبيق **"فيس تايم"** أو غيرها من التطبيقات. ومنع طفلك من تثبيت أو حذف أي تطبيق أو إجراء عمليات شراء داخل التطبيقات أيضا.

- بعد الانتهاء من تقييد التطبيقات, تبدأ في تقييد المحتوى الذي يسمح لطفلك بالدخول إليه, مثل شراء الأفلام وتصفحها, ونوعية الموسيقى والكتب والتطبيقات ومواقع الإنترنت, التي يمكن أن يتم الدخول إليها, مثل المواقع التي تحتوي على محتوى خاص بالبالغين.

- وفي نفس الأيقونة سيدخل المستخدم إلى خيار الخصوصية لمنع الطفل من إجراء أي تغييرات على التطبيقات, وخاصة تلك التطبيقات التي تسمح بالوصول إلى الصور الخاصة بالجهاز والطفل ومشاركتها في الشبكات الاجتماعية, وعدم السماح بالقيام بالتغييرات الجذرية في الجهاز الذكي.

- انتقل بعد ذلك إلى إعدادات الجهاز, واذهب إلى قسم **"إعدادات الألعاب"**, وانتقل بعدها إلى قسم **"القيود"**. عطل خاصية الدخول إلى الألعاب الجماعية, والتي قد تفتح الباب أمام بعض مخاطر الانترنت مثل التحرش والتنمر.

وللمزيد من المعلومات بإمكانك الضغط هنا

تطبيق سامسونج جلاكسي"Kids Home"

المميزات الرئيسية:

- **هاتفي:** يمكن للأطفال الاتصال بجهات الاتصال الخاصة بهم بناءً على قائمة محددة مسبقًا يسمح بها الآباء.
- **الكاميرا الخاصة بي:** كاميرا للأطفال لالتقاط الصور, وتشمل أيضا ملصقات.
- **الاستوديو الخاص بي:** للصور أو الرسومات التي يتم إنشاؤها في Kids Home أو المسموح بها من قبل الوالدين
- **المتصفح الخاص بي:** للتصفح الآمن داخل بعض المواقع المسموح بها من قبل الوالدين.

اعدادات الرقابة الأبوية:

من الصفحة الرئيسية اضغط على ايقونة **الاعدادات > التحكم الأبوي >ادخل رمز المرور.**

اهم المميزات:

- **إعداد وقت اللعب اليومي:** قم بتعيين وقت اللعب اليومي لأيام الأسبوع وعطلات نهاية الأسبوع.
- **الاستخدام اليومي:** يعرض الاستخدام اليومي حسب اليوم والتاريخ لكل ملف تعريف.
- **النشاط:** يعرض التطبيقات التي تم استخدامها.
- **محتوى مسموح:** يعرض كل المحتوى المسموح به من قبل الوالدين.

تطبيق الرقابة الأبوية "Google Family Link"

- حمل "Google Family Link" على جهاز أحد الوالدين
- قم بتسجيل الدخول عن طريق حساب أحد الابوين **"حساب قوقل"**
- سجل كـ **"أب"**
- إذا كان طفلك لا يملك حساب قوقل يجب عليك ان تنشئ واحد له, وتدخل عمره الصحيح
- حمل "Google Family Link" على جهاز طفلك, ثم قم بتسجيل الدخول باستخدام البريد الالكتروني الخاص بالطفل
- سيطلب منك البرنامج في جهاز الطفل بتسجيل الدخول بحساب الوالدين
- يمكنك التحكم في الإعدادات, الموقع, التطبيقات, وقت النوم, والاستعمال اليومي
- لتقييد المحتوى على جهاز الطفل: افتح تطبيق Google Family Link على **جهاز أحد الوالدين > اذهب الى جهاز الطفل > قيود المحتوى> اختر التطبيق> قم بضبط القيود وفقاً للتطبيقات المتوفرة**

أجهزة اندرويد وGoogle Play

إعداد أدوات الرقابة الأبوية علىGoogle Play

عند تفعيل أدوات الرقابة الأبوية, تستطيع تقييد المحتوى الذي يمكن تنزيله أو شراؤه من Google Play بحسب مستوى النضج.

إعداد أدوات الرقابة الأبوية:

- على الجهاز الذي تريد تفعيل أدوات الرقابة الأبوية عليه, افتح تطبيق **متجر"Play"**
- انقر على **القائمة > الإعدادات > العائلة > أدوات الرقابة الأبوية > تفعيل**
- أنشئ رقمًا تعريفيًا شخصيًا, وسيؤدي هذا إلى منع الأشخاص الذين لا يعرفون رقم التعريف الشخصي من تغيير إعدادات أدوات الرقابة الأبوية. وفي حال إعداد أدوات الرقابة الأبوية على جهاز طفلك, اختر رقم تعريف شخصي لا يعرفه
- انقر على التطبيقات والألعاب
- اختر التقييد المناسب لعمر طفلك

يوتيوب

- تفعيل وضع تقييد المحتوى في اليوتيوب.
- كيف يتم التفعيل:
  - **اذهب الى اليوتيوب > الإعدادات > وضع تقييد المحتوى > تفعيل.**

بلايستيشن 5

معلومات عامة يجب اخذها بعين الاعتبار قبل البدء بضبط الإعدادات:

- تأكد من وجود حساب منفصل لك عن طفلك ليسهل لك إدارة جميع الحسابات
- تأكد أن يكون حسابك محمي بكلمة سر لا يعرفها طفلك
- يمكنك تقييد المحتوى الذي يتعرض له طفلك من المتاجر الالكترونية الموجودة في أجهزة الألعاب كما يمكنك تحديد الأشخاص الذي يلعب معهم طفلك او منع صلاحيات المحادثات الصوتية بالكامل

ضبط الرقابة الابوية:

تسمح لك إدارة العائلة والرقابة الأبوية على جهاز PS5 بتقييد وصول حساب الطفل إلى ميزات الشبكة والتطبيقات والأجهزة

- تسجيل الدخول حساب أحد الوالدين.
- انتقل إلى **الإعدادات > العائلة والرقابة الأبوية > إدارة العائلة وحدد حساب الطفل**.
- تسمح لك إدارة العائلة بجدولة وقت اللعب المخصص لطفلك وإعادة ضبط كلمة المرور لحسابه والمزيد من الخيارات.
- حدد الرقابة الأبوية لإختيار مستوى رقابة أبوية مضبوط مسبقًا لطفلك, أو أنشئ رقابة أبوية
- مخصصة من خلال ضبط الاعدادات بشكل منفصل.

كيفية إجراء استثناء للعبة على أجهزة PS5

إذا حاول طفلك بدء تشغيل لعبة مقيدة, فيتم حظر اللعبة, ويمكن لطفلك أن يرسل إليك طلبًا لإجراء استثناء للعبة. بعد إرسال الطلب, تتلقى بصفتك مدير العائلة رسالة عن طريق البريد إلكتروني.

بصفتك مدير العائلة, **يمكنك** السماح بالطلب المستلم من خلال **الطرق التالية:**

1. باستخدام جهاز الجوال أو جهاز الكمبيوتر الخاص بك:

- بصفتك مدير العائلة قم بزيارة الموقع الإلكتروني المحدد في البريد الإلكتروني وسجل الدخول إلى حسابك.
- حدد طفلك من قائمة أعضاء العائلة, ثم حدد الألعاب المسموحة لعرض طلبه.

2. باستخدام جهاز PS5 الخاص بك:

سجل الدخول بصفتك مدير العائلة.

اضغط على زرPS للانتقال إلى مركز التحكم ثم حدد التنبيهات.

حدد طلب طفلك, ثم **انتقل إلى [الألعاب المسموحة]**

يمكنك أيضًا إدارة طلب طفلك من خلال الانتقال إلى **الإعدادات > العائلة والرقابة الأبوية > إدارة العائلة**, وتحديد طفلك ثم الانتقال إلى الألعاب المسموحة

- إذا قمت بتغيير مستوى قيود الرقابة الأبوية, فسيتمكن طفلك من متابعة لعب الألعاب المسموحة

كيفية تقييد التواصل والمحتوى الذي ينشئه المستخدم على أجهزة PS5

عندما تحدد **إعداد الرقابة الأبوية للتواصل والمحتوى الذي ينشئه المستخدم > تقييد**، يتم تعطيل ما يلي:

- إرسال الرسائل النصية والمحادثة الصوتية مع اللاعبين الآخرين.
- يُسمح بإرسال الرسائل المكتوبة مسبقًا في اللعبة.
- مشاركة المحتوى الذي ينشئه المستخدم.
- رؤية المحتوى الذي ينشئه المستخدمون من اللاعبين الآخرين.
- يمكنك منع رؤية المحتوى غير المناسب لعمر طفلك, كما يمكنك منع تبادل المعلومات مع الآخرين

يشمل المحتوى الذي ينشئه المستخدم والذي يمكن حظره ما يلي:

- لقطات الشاشة.
- مقاطع الفيديو (فيديو طريقة اللعب).
- عمليات البث الخاصة بطريقة اللعب.
- المحتوى الذي ينشئه مستخدم يكون لاعبًا آخر في اللعبة.
- الوصف الشخصي للاعب آخر على ملف التعريف الخاص به

الرقابة الأبوية على جهاز PlayStation 5

1. **مراقبة إدارة العائلة:**

- عندما تقوم بضبط مدة وقت اللعب لليوم, يتم عرض وقت اللعب المتبقي. يمكنك تمديد وقت اللعب المخصص لطفلك وتقليصه من هنا.
- يمكنك تحديد الأيام التي يمكن لطفلك فيها تشغيل الألعاب, بالإضافة إلى المدة المسموح بها عندما ينتهي وقت اللعب المخصص لطفلك, يمكنك اختيار إما حصوله على رسالة تنبيه أو تسجيل خروجه تلقائيًا. تشمل مدة اللعب لليوم وقت اللعب على جهاز PS4 او PS5 الخاص بك.
- تتم إعادة ضبط وقت اللعب المخصص لطفلك عند الساعة 12:00 في منتصف الليل في
- المنطقة الزمنية المحددة.
- اعرض الطلبات للسماح بألعاب محددة وقائمة الألعاب التي سبق أن تم السماح بها.
- اعرض معرّف تسجيل الدخول (عنوان بريد إلكتروني) ومعرّف الاتصال على الإنترنت والاسم المخصص لطفلك. إن الاسم المعروض هنا هو الاسم الذي تم إدخاله عند إنشاء حساب طفلك, وهو غير مرئي للاعبين الآخرين. يظهر هذا الاسم في رسائل
- البريد الإلكتروني التي تتلقاها من PlayStation لهذا الحساب.
- إعادة تعيين كلمة المرور.

2. الرقابة الأبوية:

- ضبط مستويات تقييم السن لبدء تشغيل ألعاب وتطبيقاتPS5
- ضبط مستويات تقييم السن لبدء تشغيل ألعاب وتطبيقات PS4/PS3
- ضبط مستويات تقييم السن لبدء تشغيل Blu-ray
- ضبط مستويات تقييم السن لبدء تشغيل قرصDVD
- تقييد استخدامPlayStation VR
- تقييد تصفح الويب
- تقييد التواصل والمحتوى الذي ينشئه المستخدم تصفية محتوى الإنترنت على أساس السن
- تعيين حد الإنفاق الشهري
- بصفتك مدير العائلة, يمكنك أن تقرر المبلغ الشهري الذي يمكن أن ينفقه طفلك. وبشكل افتراضي, يتم تعيين حد الإنفاق الشهري إلى صفر. إذا كان طفلك سيشتري محتوى على حسابه, فتأكد من تغيير هذا الإعداد .
- إذا عيّنت حدًا للإنفاق على حساب طفل, فسنتيح لهذا الطفل إنفاق هذا المبلغ كل شهر على PlayStation Store يتم خصم هذه الأموال من محفظة مدير العائلة.
- يُرجى العلم أنه إذا كنت "وصيًا" وليس مديرًا للعائلة, فعليك إعلام مدير العائلة في حال أجريت أي تغيرات على حدود الإنفاق.
إذا كنت مدير العائلة, فاعلم ان أي شخص تعيّنه كوصي يمكنه تغيير حدود الإنفاق التي وضعتها

ملاحظة: كلمة المرور الافتراضية هي: 0000. تذكر ان تُغيّر هذا الرمز.

أجهزة ويندوز:

يعتبر استخدام اجهزة الكمبيوتر امرا مفيداً لتنمية مواهب أطفالك ومواكبة مستجدات التقنية الحديثة وتطوراتها, ولكن يجب التأكد من وجود رقابة صارمة على المحتوى الذي يتعرض له طفلك خاصة إذا كان الكمبيوتر متصلا بالإنترنت, لهذا السبب وفرت مايكروسوفت أداة الرقابة الأبوية (Parental Controls) في نظام ويندوز 10 للمساعدة في الحفاظ على أمان الأطفال. من خلال تفعيل هذه الأداة يمكن للوالدين تقييد أنواع التطبيقات والمحتوى الذي يمكن لأطفالهم الوصول له, فيما يلي بعض الخطوات لضبط **اعدادات الرقابة:**

ملاحظة: تأكد من وجود حساب مايكروسوفت لك ولطفلك (وليس حسابًا على جهاز ويندوز), ويمكنك إنشاء الحساب أثناء عملية إعداد الرقابة الأبوية أو قبلها, إلا أنه من الأفضل إنشاؤه أثناء عملية الإعداد.

1. اضغط على قائمة **ابدأ** / Start واختر **الإعدادات** / Settings.
2. اضغط على **الحسابات** / Accounts .
3. اضغط على خيار **العائلة ومستخدمين آخرين** / Family & Other Users.
4. اختر **إضافة عضو في العائلة** / Add a Family Member.
5. اضغط على **إضافة طفل** / Add a Child , ثم اختر الشخص الذي ترغب في إضافته وليس لديه عنوان بريد إلكتروني, أما إذا كان لديه عنوان بريد إلكتروني, فاكتبه في الخانة المخصصة ثم اضغط على **التالي** / Next.

6. اضغط على **لنقم بإنشاء حساب / Let's Create An Account**, اكتب المعلومات المطلوبة بما في ذلك حساب البريد الإلكتروني وكلمة المرور والبلد وتاريخ الميلاد.
7. اضغط على التالي, واخر **تأكيد / Confirm** إذا طُلب منك ذلك.
8. اقرأ المعلومات المقدمة, واختر **إغلاق / Close.**

يمكنك مراجعة الإعدادات وتغييرها أو تعطيلها، باتباع الخطوات التالية:

1. في مربع البحث بجوار قائمة ابدأ Start, أكتب عبارة **عائلة / Family**, ثم اضغط على **خيارات العائلة**, ثم اختر **إظهار إعدادات العائلة**.
2. قم بتسجيل الدخول إذا طُلب منك ذلك, ثم حدد موقع الحساب الفرعي من قائمة الحسابات المضمنة مع عائلتك.
3. اضغط على خيار **وقت الشاشة / Screen Time** أسفل اسم طفلك, ثم قم بإجراء تغييرات على إعدادات وقت الشاشة الافتراضية باستخدام القوائم المنسدلة والجداول الزمنية اليومية.
4. اضغط على **المزيد من الخيارات / More Options** تحت اسم طفلك واختر **قيود المحتوى/ Content Restrictions**.
5. تأكد من تفعيل حظر التطبيقات والألعاب ومواقع الويب غير الملائمة, وإضافة أي تطبيقات أو مواقع ويب ترغب في حظرها أو السماح بتحديد تصنيف عمري مناسب لها.

وللمزيد من المعلومات بإمكانك الضغط هنا

سابك
sabic

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الخصوصية

سناب شات

تشير الاعدادات الافتراضية في تطبيق سناب شات الى أنه لا يستطيع أحد ان يتصل بك مباشرة او يشاهد قصتك الا إذا كان صديقاً قد اضفته بالفعل على التطبيق.

1. اضغط على علامة الاعدادات في الملف التعريفي الخاص بك.
2. مرر للأسفل الى قسم أدوات التحكم في الخصوصية
3. اذهب الى قسم **من يمكنه رؤية موقعي** واختر من يمكنه رؤية موقعك على خريطة السناب, لن تتم مشاركة موقعك على الخريطة حتى تفتحه لأول مرة.
4. اذهب الى قسم من **يمكنه مشاهدة قصتي** وحدد من يمكنه مشاهدة قصتك عن طريق الضغط على **تخصيص**, إذا كنت تود أصدقاء محددين من مشاهدة قصتك. **ملاحظة**: إذا اضفت **"القصة"** ثم غيرت المشاهدة الى **"أصدقائي"** قد يمكن للأخرين مشاهدة القصة المضافة مسبقاً.
5. اذهب الى قسم رؤيتي **في إضافة سريعة** والغاء هذه الخاصية, وبذلك لن تظهر في قائمة "الإضافات السريعة" عند أصدقاء اصدقائك.
6. اذهب الى قسم **من يُمكنه الاتصال بي** وحدّد من يُمكنه الاتصال بك مباشرة من خلال مقاطع Snap ودردشات ومكالمات وغيرها.
7. اذهب الى قسم أرسل إشعارات إلي: اختر أن تتلقى إشعارات من جميع الأشخاص أو أصدقاءك فقط. تعرّف على المزيد عن إعدادات الإشعارات لنظام تشغيل iOS ونظام تشغيل Android.
8. اذهب الى قسم من الذي يُمكنه استخدام سيلفي الأشرطة الخاص بي: اختر الشخص الذي يمكنه استخدام سيلفي الأشرطة الخاص بك في الأشرطة الثنائية.

إليك بعض الأشياء التي يتعيّن عليك تذكّرها:

حتى إذا اخترت **"أصدقائي"**, فإن أي شخص يوجد في مجموعة معه يستطيع التواصل معك في الدردشة الجماعية. إذا كنت تريد أن تشاهد من الموجود في مجموعة ما قبل الدخول فيها, اضغط باستمرار على اسم المجموعة في شاشة الدردشة!

إذا اخترت **"أصدقائي"**, فلن ترى مقاطع Snap التي يُرسلها إليك غير الأصدقاء, بل ستستقبل إشعاراً بأنهم أضافوك كصديق. إذا قبلت إضافتهم وأضفتهم, ستتمكّن من مشاهدة مقطع Snap الذي يُرسلوه إليك.

إذا اخترت **"الجميع"** في **"الاتصال بي"**, فإن مُستخدمي سناب شات الذين لم تضفهم سيتمكّنون من التواصل معك.

إذا كنت تود استقبال مقاطع Snap من **"الجميع"** ولكن تُريد فقط استقبال الإشعارات عند قيام الأصدقاء بإرسال مقطع Snap إليك, يُمكنك تغيير إعدادات الإشعار في إعدادات الإشعارات لنظام تشغيل iOS أو Android في **إعدادات سناب شات > الإشعارات**.

الإبلاغ عن محتوى: يمكن الإبلاغ عن محتوى بالضغط مطولا على **المحتوى > الضغط على ايقونة "العلم" الموجودة في أسفل يسار المحتوى "ابلاغ" > اختيار سبب الإبلاغ على المحتوى.**

حظر الأصدقاء او ازالتهم من القائمة: تحت صفحتك الشخصية, اختار **"أصدقائي"**. اضغط مطولاً على الحساب ثم اختار **"حظر"** او **"ازالة الصديق"**

تذكر دائماً, حتى لو حفظت صورك الشخصية او الفيديوهات الخاصة في تطبيق السناب شات, هذا لا يعني انها محمية تماماً. لأنه من المحتمل ان يتم اختراق التطبيق ويتم سرقة كل ما حفظته.

تسجيل الدخول بخطوتين: اضغط على علامة الاعدادات ثم **"حسابي"** ثم **"تسجيل الدخول بخطوتين"** وقم بتفعيل الخاصية.

تطبيق الواتساب

تتيح الإعدادات الافتراضية للخصوصية في واتساب ما يلي:

- يمكن لأي مستخدم رؤية صورة الملف الشخصي, ومعلومات قسم الأخبار, ومؤشرات قراءة الرسائل
- يمكن لجهات الاتصال رؤية حالاتك الجديدة
- يمكن لأي مستخدم إضافتك إلى المجموعات

ملاحظة: قد يتمكن المستخدمون الذين حفظتهم كجهة اتصال أو الذين راسلتهم من قبل من رؤية آخر ظهور ومتصل الآن.

تغيير إعدادات الخصوصية

1. على أجهزة Android: انقر على **خيارات إضافية > الإعدادات > الخصوصية.**
2. أجهزة iPhone: انقر على **الإعدادات > الخصوصية.**
3. **واتساب للكمبيوتر:** انقر على **القائمة > الإعدادات > الخصوصية.**
4. تستطيع تغيير من يمكنه:
   - رؤية آخر ظهور ومتصل الآن
   - رؤية صورة ملفك الشخصي
   - رؤية معلومات الأخبار الخاصة بك
   - رؤية الحالات الجديدة
   - رؤية مؤشرات قراءة الرسائل
   - إضافتك إلى المجموعات

ملاحظة: إذا لم تشارك وقت آخر ظهور لك أو متصل الآن, فلن تتمكن أيضًا من رؤية وقت آخر ظهور أو متصل الآن الخاص بالمستخدمين الآخرين.

إذا أوقفت مؤشرات قراءة الرسائل لديك، فلن تتمكن من رؤية تلك المؤشرات عندما يقرأ الآخرون رسائلك. وفي الدردشات الجماعية, يتم دائمًا إرسال مؤشرات قراءة الرسائل, ولا يمكن تعطيلها.

إذا أوقفت جهةُ اتصال ما مؤشرات قراءة الرسائل لديها، فلن تتمكن أنت من معرفة ما إذا كانت تلك الجهة قد شاهدت حالاتك الجديدة.

يمكن للأشخاص المتصلين الآن في سلسلة دردشة معك رؤية أنك تكتب.

بإمكانك أيضا حظر او الإبلاغ عن جهة اتصال بالذهاب الى صفحته الشخصية والضغط على **"حظر جهة الاتصال"** او **"الإبلاغ عن جهة الاتصال"**

لمنع التنزيل التلقائي للوسائط القادمة من التطبيق على الجهاز, اذهب الى **الاعدادات > حجم البيانات والتخزين للمستخدم, ووضع كل الاختيارات تحت "التنزيل التلقائي للوسائط" الى "أبداً"**.

خطوات التحقق الثنائي لبرنامج WhatsApp

1. اضغط على **الاعدادات** في الأسفل.
2. اختر **الحساب**
3. ثم اختر **التحقق بخطوتين**
4. قم بتفعيل الخاصية عن طريق الضغط على **(تفعيل)**
5. يتم ادخال الرقم السري للبرنامج
6. ادخل البريد الإلكتروني الخاص بك

أجهزة iOS

تستطيع التحكم في أي تطبيق يمكن الوصول اليه من خلال الاعدادات. في اعدادات اختر خيار الخصوصية. ستظهر لك قائمة من التطبيقات التي من خلالها يمكنك الاختيار على أي منها والتحكم في خيارات الخصوصية فيها.

1. الموقع:

كيف يمكنك ان تحدد أي من التطبيقات يمكنه الوصول الى موقعك:

من خلال **الاعدادات > الخصوصية** يوجد خيار خدمات المواقع. من هنا تستطيع التحكم في كل تطبيق ما إذا يسمح له بمعرفة موقعك او لا. يوجد عددا من الخيارات يمكنك الاختبار من خلالها بشأن تحديد الموقع وهم:

1. **مطلقا:** لا يسمح للتطبيق الوصول الى موقعك بشكل نهائي.

2. **السؤال في المرة القادمة:** تستطيع من خلالها التحكم في حال متى يجب الوصول الى موقعك من خلال إعطائه الفرصة للوصول الى موقعك مره واحده فقط بعد السماح له بذلك.

3. **اثناء استخدام التطبيق:** يسمح للتطبيق في الوصول الى موقعك في حال فقط تواجد في التطبيق نفسه.

كيف يمكنك ان تحدد أي من جهات الاتصال لديك يمكنه الوصول الى موقعك: من السهولة ان يتم نسيان الأشخاص الذين قد شاركت موقعك معهم. لذلك يمكنك الذهاب الى **الاعدادات > الخصوصية > مشاركة موقعي**, وستظهر لك قائمة من جهات الاتصال الذين يمكنهم تتبع موقعك عبر الخرائط. تستطيع أيضا تعطيل هذه الخدمة من خلال الضغط على خانة **"مشاركة موقعي"** وتعطيلها ان لم تكن معطلة من الأساس.

إذا كنت قد منحت شخص ما مشاركة موقعك يمكنك سحب ذلك من خلال الضغط على جهة الاتصال واختيار "توقف مشاركة موقعي."

كيف يمكنك ان تحدد أي من الأنظمة الخدمية تستطيع الوصول الى موقعك: الاعدادات > الخصوصية **> خدمات النظام**, سوف تظهر لك قائمة من الخدمات التي تستخدم موقعك. يمكنك تعطيل أي منها, ولكن معظم المستخدمين يبقونها مفعله, كما اننا ننصح بإبقاء بعضها مفعله مثل مكالمات الطوارئ وغيرها من الخدمات المهمة .في نفس الخانة توجد **"المواقع المهمة", الاعدادات > الخصوصية > خدمات النظام > المواقع المهمة**, في هذه الخانة سوف تجد قائمة من المواقع المهمة التي قام جهازك بحفظها بناءً على **"الخرائط, الصور, التقويم, وغيرها"**

هذه المعلومات مشفرة وغير متاحة لشركة أبل, ولكن جهازك يتخذ قرارات فيما يتعلق بتحركاتك, رحلاتك, واستخدامات أخرى.

2. الاشعارات:

يمكنك ان تحدد أي من التطبيقات يسمح لها ارسال اشعارات لك: الاشعارات ليست مسألة خصوصية بشكل كبير, ولكن في بعض الأحيان من الممكن ان تسبب نوع من الازعاج. لتحديد الاشعارات يمكنك الذهاب الى **الاعدادات > الاشعارات** ومن خلالها يمكنك تحديد أي من التطبيقات يسمح له ان يرسل اليك اشعارات.

ظهور الاشعارات على شاشة الجهاز

الاعدادات > الاشعارات, من خلالها يمكنك ان تحدد كيفية ظهور الاشعارات على شاشة الجهاز الرئيسية, من خلال الدخول على التطبيق ومن ثم الضغط على اظهار المعاينات, وأفضل خيار يمكن اختياره هو **"في حال فتح القفل"** لذلك سوف تظهر المعاينات حال فتح قفل الجهاز فقط.

3. سيري/Siri :

الاعدادات > Siri > السماح بـSiri عند القفل, من خلالها يمكنك تعطيل السماح لـ Siri للوصول الى شاشة القفل.

4. متصفح سفاري/Safari:

متصفح سفاري هو المتصفح الرئيسي في أجهزة أبل. تستطيع التحكم في خصوصية المتصفح من خلال الذهاب الى **الاعدادات > Safari**. الاعدادات المضبطة من المصنع تكون غالبا متناسبة مع معظم المستخدمين. علما بأن متصفح سفاري يحد من **"التتبع اثناء تصفح المواقع"** التي تأخذ بعض بيانات زوارها بغرض الإعلانات وغيرها.

في هذا السياق يمكنك اتخاذ خطوة للأمام, للحد من اخذ بعض المواقع بياناتك من خلال الضغط على خيار **"حظر كل الكوكيز"**. في حال تعطيل هذه الخدمة سوف تتعطل بعض الخدمات الأخرى.

وبالإمكان أيضا تعطيل الوصول الى **"الكاميرا والميكروفون"** مع العلم ان بعض المواقع سوف تطلب منك السماح لها للوصول إليهم .

تذكر: في حال استخدامك متصفح اخر مثل "Chrome" فان هذه الاعدادات لن تكون متطابقة.

5. ارقام الهاتف:

في بعض الأحيان من اشكال التحكم في جهازك حظر شخص ما. بالإمكان حظر جهة اتصال معينة بحيث لا يمكن لجهة الاتصال هذه الاتصال بك او ارسال أي رسالة اليك, وبالتزامن سوف يحظر أيضا من برنامج Face Timeولن يستطيع الاتصال بك من خلاله. ولكن يجب عليك أيضا حظر البريد الالكتروني المتزامن مع ذلك الرقم في بعض الحالات.

لحظر الأرقام غير المحفوظة في جهات الاتصال, افتح تطبيق **"الهاتف"** في خيار **"الحديثة"** اختر جهة الاتصال واضغط على علامة "i" من ثم **"حظر هذا المتصل"**. وأيضا بالإمكان حظر الجهات الاتصال المحفوظة بنفس الطريقة.

يمكنك التأكد من قائمة المحظورين لديك من خلال: الإعدادات > الهاتف > جهات الاتصال المحظورة.
وأيضا يمكنك الذهاب الى **FaceTime> جهات الاتصال المحظورة.**

6. تتبع الإعلانات:

كيف يمكنك الحد من تتبع البيانات في تطبيقات أبل: الإعدادات > الخصوصية > الإعلانات, عند تعطيلك لهذه الخدمة سوف تقوم أبل بتعطيل الإعلانات ذات العلاقة, بمعنى أنك لن تستقبل إعلانات تتعلق باهتمامات التي تجمعها أبل من خلال محرك البحث لديك, او التطبيقات التي تحملها, او الاخبار التي تقرئها وغيرها. للأسف لا يمكن الغاء هذه الخاصية بشكل كامل.

تستطيع أيضا تعطيل خدمة الإعلانات حسب موقعك من خلال: الإعدادات > الخصوصية > خدمات النظام > إعلانات Apple بحسب الموقع

7. المصادقة الثنائية:

كيف يمكنك ان تفعل مصادقة ثنائية: الإعدادات > حساب أبل **"اسمك وصورة العرض" > كلمة السر والامن > المصادقة ذات العاملين**

8. استخدام رقم سري قوي:

الإعدادات >Touch ID ورمز الدخول. عندما تنشأ رمز دخول جديد سوف تظهر لك عدت خيارات في كيفية الرقم السري الذي ترغب فيه:

- **تخصيص رمز رقمي ابجدي:** وهو عبارة عن رمز دخول يتكون من ارقام وحروف *ويعتبر هذا الخيار الأفضل *
- **تخصيص رمز رقمي:** وهو عبارة عن رمز دخول يتكون من ست ارقام
- **اعداد رمز رقمي:** وهو عبارة عن رمز دخول مكون من أربعة ارقام
- لتأكيد ان رمز الدخول المستخدم قوي بما فيه الكفاية استخدم Touch ID / Face ID مع رقم سري قوي.

9. العثور على الiPhone : الإعدادات > تحديد الوقع > العثور على ال iPhone

بلايستيشن 5

انتقل إلى **الإعدادات > المستخدمون والحسابات > الخصوصية**. اختر عرض وتخصيص إعدادات خصوصيتك. اختر مستوى إعدادات خصوصية مضبوطًا مسبقًا أو اختر ميزة لتغيير إعدادات الخصوصية.

ما هي إعدادات الخصوصية على PlayStation Network (PSN)؟

يمكنك الحد من ظهورك إلى مستخدمين آخرين على **PlayStation Network** باستخدام إعدادات الخصوصية. يمكنك تخصيص الميزات التالية:

1. اللعب | الوسائط

اختر من يمكنه رؤية الوسائط المشتركة الخاصة بك وأنشطتك الحديثة.

2. الأصدقاء | المعارف

تحكّم بهوية الذين يمكنهم إرسال طلبات صداقة لك ومتابعة حسابك ورؤية اصدقائك.

3. المعلومات الشخصية | المراسلة

اختر من يمكنه رؤية اسمك الحقيقي والتواصل معك

ماهي إعدادات الخصوصية المضبوطة مسبقًا على أجهزة PS5؟

يمكن للّاعبين البالغين الاختيار من بين ملفات التعريف المضبوطة مسبقًا.

1. اجتماعي

يمكن لأي لاعب أن يرى معلومات ملف التعريف الخاص بك, والتواصل معك.

2. لاعب متعاون

يمكن لأي لاعب أن يرى معظم معلومات ملف التعريف الخاص بك لكن يجب على الأقل أن يكون صديق أحد أصدقائك لدعوتك إلى المحادثة.

3. التركيز على الأصدقاء

يمكن فقط لأصدقائك رؤية معلوماتك ودعوتك إلى المحادثة.

4. منفرد ومركّز

لا يمكن لأي لاعب أن يرى معلوماتك ملف التعريف الخاص بك أو دعوتك إلى المحادثة حتى إن قمت بإضافته كصديق.

يمكن للأطفال تحديد ملف تعريف خاص بالخصوصية عند إنشاء حساب مع مدير العائلة, إلا أنّه لا يمكنهم الاختيار من ملفات التعريف هذه الخاصة بالخصوصية بعد إنشاء حساب ما

كيفية ضبط من يمكنه تغيير إعدادات الخصوصية لطفلك:

يمكنك ضبط من يمكنه تغيير إعدادات الخصوصية لطفلك من خلال زيارة إدارة الحساب.

حدد أحد حسابات الاطفال من بين أعضاء العائلة ثم اذهب إلى الخصوصية.

حدد تعيين بواسطة ثم حدد النمط الخاص بك من القائمة الموجودة.

إعدادات الخصوصية التي تم تعيينها بواسطة ولي الأمر:

إذا اخترت تعيين بواسطة ولي الأمر, فيمكن لمدير العائلة تغيير إعدادات خصوصية الطفل.

يمكنك أيضًا تحديد الإعدادات التي تريد السماح لطفلك بتغييرها. إذا سمحت لطفلك بتغيير الإعدادات, فيمكنك أيضًا تحديد الخيارات التي يمكنه الاختيار من بينها.

يتم إعلامك في كل مرة يغير فيها الطفل إعداداته

انستقرام

جعل حسابك على الانستقرام خاصاً

ملاحظة: إذا كان عمرك أقل من 16 عامًا عند التسجيل للحصول على حساب الانستقرام, سيكون لديك خيار للاختيار بين حساب عام أو خاص, ولكن يتم تحديد خاص افتراضيًا.

إذا كان عمرك أكثر من 16 عامًا, يظهر حسابك على الانستقرام للعامة بشكل افتراضي ويمكنك اختيار تعيين حسابك إلى خاص في أي وقت. تعرَّف فيما يلي على المزيد عن كيفية تعيين حسابك إلى خاص

لتعيين حسابك إلى خاص:

1. اضغط على الاعدادات
2. انقر على **الخصوصية والأمان > خصوصية الحساب > اضغط للتفعيل لحساب خاص**

يرجى العلم أن الملفات الشخصية للأنشطة التجارية لا يمكنها تعيين حساباتها إلى حسابات خاصة. وإذا أردت جعل حساب نشاطك التجاري حسابًا خاصًا, فيجب أولاً إعادة تحويل الحساب إلى حساب شخصي.

سابك
sabic

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

استرجاع الحساب

استرجاع الحساب

خطوات استرجاع حساب Snap Chat الخاص بك

اذهب الى صفحة الدعم عبر الرابط التالي: https://support.snapchat.com

اختر **حسابي والأمان**

اختر **امان حسابي**

اختر **تعرض حسابي للاختراق**

سيقوم فريق الدعم بتوجيهك أولاً إلى القيام **بتغيير كلمة المرور**. على افتراض أنك قد جربت ذلك بالفعل ولم تنجح, اختر **نعم** التي بجانب **هل تحتاج مساعدة بخصوص شيء اخر؟**

املأ النموذج الذي يظهر لك بأكبر قدر ممكن من الدقة ثم أرسله, قد يمنحك فريق الدعم في Snapchat إمكانية الوصول إلى الحساب مرة أخرى, مما يسمح لك بإنشاء كلمة مرور جديدة.

إذا لم يمنحك تطبيق Snapchat حق الوصول إلى حسابك, فستحتاج إلى إنشاء حساب جديد إذا كنت تريد الاستمرار في استخدام التطبيق.

خطوات استرجاع حساب WhatsApp

في حال كان الحساب مخترق او تم سرقته قم بحذف التطبيق من جهازك وإعادة تثبيته بنفس الرقم. عندها سيتفعل الحساب لديك ويتعطل عند المخترق.

قم فورا بتفعيل خاصية التحقق بخطوتين.

اما في حال كان المخترق قد فعل خاصية التحقق بخطوتين على حسابك فعندها لن تتمكن من استرجاع حسابك بالطريقة السابقة. ويجب حينها مراسلة الشركة بالبريد الإلكتروني على العنوان support@whatsapp.com .

اذكر بعض التفاصيل الضرورية عما حصل او عما يفعله المخترق على سبيل المثال: ابتزاز او سرقات ... الخ. بعد الارسال ستصلك رسالة رد الي من نفس الشركة تحتوي على معلومات عامه وتوجيهات. وفي نهاية الرسالة يوجد رقم بلاغ خاص بالحادثة.

خطوات استرجاع حساب Twitter

1. **اطلب إعادة ضبط كلمة مرورك.**
   - ادخل اسم المستخدم وعنوان البريد الإلكتروني.
   - تحقق من ان البريد الإلكتروني هو البريد المرتبط بحسابك على Twitter.

2. **اتصل بالدعم الفنّي إذا كنت بحاجة إلى مساعدة.**
   - اختر **"حساب مُخترق"** من قائمة الخيارات عبر هذا الرابط https://help.twitter.com/forms
   - تأكد من استخدام عنوان البريد الإلكتروني المرتبط بحسابك المخترق على Twitter, وارفق كل من اسم المستخدم وآخر تاريخ سجلت فيه الدخول. سيتم ارسال المزيد من المعلومات والإرشادات الى بريد الالكتروني عن طريق Twitter.

سابك
sabic

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

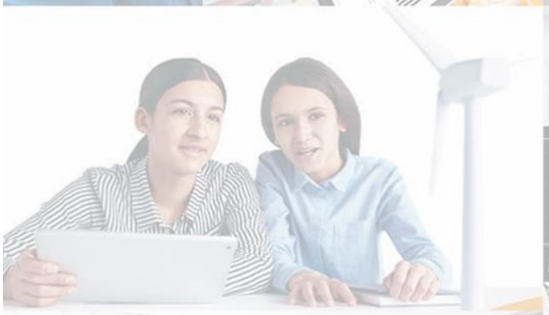
سابك
sabic

شكراً لكم

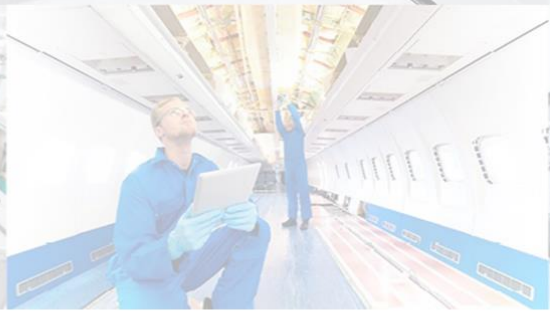










كيمياء وتواصل™