secdev.foundation

المديرية الإقليمية بمكناس
ⵜⴰⵔⴰⵎⵜ ⵜⴰⵏⴰⵎⵓⵔⵜ ⵏ ⵎⴽⵏⴰⵙ
Direction Provinciale Meknès

PROPER THOUGHT FOR DEVELOPMENT
الفكر السليم للتنمية

سلام@
Salam@

جمعية الفكر السليم للتنمية

دليل السلامة الرقمية في التعلم عن بعد

محتويات الدليل

سياق الدليل:

يأتي هذا الدليل في إطار مشروع وقاية-نت المنظم من طرف جمعية الفكر السليم للتنمية، بشراكة مع كل من المديرية الإقليمية لوزارة التربية الوطنية والتعليم الأولي والرياضة بمكناس و مؤسسة SECDEV ضمن برنامج سلامات المغرب، كما أنه يأتي في سياق التزايد غير المسبوق في الزمن الذي يمضيه الأطفال أمام شاشات الأجهزة الإلكترونية، نتيجة التحول الذي فرضته الثورة الرقمية وضاعفت من وثيرته جائحة كورونا التي غيرت بشكل ملحوظ أنماط تفاعلاتنا اليومية بما فيها تلك التي تنتمي لحقل التربية والتكوين ونخص بالذكر نمط التعليم والتعلم. ما دفع عدداً كبيرا من الأسر إلى اعتماد التقنيات والحلول الرقمية لمواصلة تعليم أطفالهم وترفيههم وربطهم بالعالم الخارجي، الشيء الذي نتج عنه آثار نفسية واجتماعية لها انعكاساتها الخاصة على هاته الشريحة التي باتت رهينة لأجهزتها الذكية وشبكات التواصل الاجتماعي، والتي يتم استخدامها دون ضوابط أو قيود في كثير من الأحيان. ويعتبر هذا الدليل حصيلة للعديد من التدخلات التي قامت بها الجمعية (مجموعات تركيز، استطلاعات رأي، و استشارات مع الأستاذات والأساتذة تم من خلالها جمع العديد من المعطيات المهمة في مجال السلامة الرقمية الخاصة بالتعليم عن بعد بالمغرب. ونهدف من خلال هذا الدليل إلى المساهمة في زيادة الوعي بالاستعمال الآمن للانترنيت للتلميذات والتلاميذ خلال عملية التعلم عن بعد، من أجل تجنب المخاطر التقنية والنفسية والقانونية التي قد تواجههم أثناء تبحرهم للأنترنيت.

كلمة الدكتورة: وفاء شاكر
المديرة الاقليمية لوزارة التربية الوطنية والتعليم الأولي والرياضة بمكناس

يعيش عالمنا اليوم تحولات جذرية بفعل التسارع المهول لآليات الثورة الرقمية باعتبارها إحدى أبرز تجليات التطور التقني-العلمي الذي يشهده عصرنا الحالي، وأحد أكبر العوامل المؤثرة في الحياة الخاصة والعامة للأفراد والمجتمعات. فبالرغم من العمر القصير لهذه الطفرة المعلوماتية إلا أنها استطاعت أن تجتاح كل مناحي الحياة الإنسانية وأن تتمدد داخل جل الأوساط المجتمعية ومجالات النشاط الإنساني. الشيء الذي مكنها من أن تعدل وتوجه الكثير من سلوكاتنا وعلاقاتنا في مختلف أبعادها: الأسرية، الاجتماعية، الاقتصادية، التربوية... وعليه يمكن القول إن الإنسانية برمتها وعلى امتداد الجغرافيا البشرية قد أصبحت متأثرة بشكل أو بأخر بهذه الثورة التي تخترق دون توقف كل الحدود والعقول معا.

صحيح أن من الإيجابيات الكبرى لهذه الثورة الرقمية أنها سهلت التواصل وعززت من قيمته بين الأفراد والمجتمعات، كما اختزلت المسافات بين الدول والثقافات حتى بات العالم بحق قرية صغيرة؛ لكنها في المقابل أيضا عدلت من نمط وجودنا وأشكال تفاعلاتنا الموروثة عن الثورات التكنولوجية السابقة فاسحة بذلك المجال لأنماط عيش و لأشكال جديدة من التفاعلات الإنسانية. لكن، فكما للثورة الرقمية وجهها المبشر بالإنجازات والفتوحات ثمة مخاطر وتهديدات وراء هذا التحول المذهل الذي تتسارع خطواته يوما بعد يوم.
ضمن هذا السياق لم تسلم منظومات التربية والتكوين من هذا التحول العميق في مجتمعات اليوم، إذ أن الثورة الرقمية لم تستثني أي مجال من مجالات الفاعلية البشرية من تأثيراتها وآثارها، بل إن الظهور المفاجئ لجائحة كورونا خلال السنتين الماضيتين عمق من ضرورة التحول نحو بدائل للتعليم والتعلم ضمن منظومات التربية والتكوين. وفي هذا السياق لم يتأخر المغرب في التعاطي مع وضع طارئ كان على المدرسة أن تتكيف معه بشكل سريع وإيجابي.
من هنا كان لزاما على مؤسسات التربية والتكون الانتقال من نمط كلاسيكي للتعليم والتعلم لنمط غير مألوف، التعليم عن بعد، يستثمر مكتسبات الثورة الرقمية ومعه الإمكانات التي يتيحها الأنترنيت؛ ويعيد تحديد شكل علاقة المتعلمات والمتعلمين بتعلماتهم وبالمعرفة عموما. لكن هذا التحول ينطوي على مخاطر عديدة فهو يضع الناشئة أمام العديد من المخاطر المرتبطة باستعمال هاته التقنيات الحديثة. لذلك بات من الضروري على منظومتنا التربوية مواكبة هذه التحولات عبر تسليح المتعلمات والمتعلمين بآليات ومهارات الحماية من كل أشكال المخاطر المحتملة التي تتهدد مستقبلهم وشخصياتهم جراء الإستخدام غير الآمن للتكنولوجيا والأنترنيت.
في هذا السياق بالذات يأتي "دليل السلامة الرقمية في التعلم عن بعد" الذي نضعه بين أيدي الأطر الإدارية والتربوية وكذا الأسر والتلاميذ، دليل نتغيا من ورائه استخداما آمنا وفعالا للأنترنيت، وتوجيها للمتعلمات والمتعلمين نحو حماية أنفسهم من كل المخاطر المحتملة.

حقائق من الضروري معرفتها:

من التلاميذ لا يعرفون ماذا نعني بالسلامة الرقمية.

من المشاركين في الدراسة لم يسبق لهم البحث عن طرق استخدام الأنترنيت بأمان.

من المشاركين في الدراسة معرضون للخطر خلال استخدام الأنترنيت.

قالوا إنهم لا يشعرون بالأمان أثناء تصفح الإنترنت أو استخدام الشبكات الاجتماعية.

من المشاركين كانوا ضحايا لجرائم إلكترونية، والتي تشمل استخدام الصور والمعلومات الشخصية دون إذن ،التهديد باستخدام البيانات الشخصية واختراق الحسابات، أغلبية الضحايا تكلموا عن المشكل مع أحد المعارف ولكن إثنين من عشرة فقط من بلغوا الجهات الأمنية.

إن لم يكونوا ضحايا، فإنهم يعرفون شخصا على الأقل تعرض لجريمة إلكترونية.

المصدر : دراسة لبرنامج سلامات في المغرب خلال الموسم الدراسي 2020 /2021
استهدفت تلاميذ الإعدادي والثانوي التأهيلي من 8 مدن مغربية

على المستوى العالمي:

خلال كل 15 ثانية شخص بالغ يكون ضحية لجريمة إلكترونية.

خلال كل 18 ثانية يتم تنفيذ هجوم الكتروني ببرمجيات الفدية.

فقط هي نسبة الجرائم الإلكترونية التي يتم التبليغ عنها كل عام في الولايات المتحدة.

المصدر : دراسة لمجلة CPO Magazine https://www.cpomagazine.com/

ما هي السلامة الرقمية؟

يمكن اعتبار السلامة الرقمية أسلوب عيش في الفضاء الرقمي، بحيث تشمل مجموعة الممارسات السليمة، غايتها حماية حساباتنا ومعطياتنا من الأخطار الرقمية كالاختراق أو التسلل أو التدخل والتطفل من طرف أشخاص يمكن أن يشكلو خطرا على سلامتنا النفسية والجسدية. ويمكن لهذ النوع من المخاطر أن يكون نتيجة تدخلات بشرية أو تحديات تقنية وتكنولوجيا، وهي كثيرة ومتنوعة وكل خطر ولديه طريقة تعامل خاصة به.

- لهذا اخترنا في برنامج سلامات مجموعة من الأخطار الرقمية الأكثر انتشارا وحاولنا من خلالها تقديم بعض الطرق والإجراءات التي من شأنها أن تحمي سلامتكم الرقمية.

ملاحظات مهمة:

1. هذا الدليل يحتوي على روابط لمواقع وتطبيقات، استخدموا تقنية Scan ل Code Barres للتمكن من الدخول لهذه المواقع.

2. نحن لانحتضن أو نقوم بالإشهار أو التسويق لأي تطبيق أو برنامج مذكور في هذا الدليل.

تعرفوا على أنواع الأخطار الرقمية

في العالم الرقمي هناك العديد من المخاطر ومن بينها:

- الهندسة الإجتماعية
- التصيد
- التنمر
- التحرش الرقمي
- الاختراقات
- الإبتزاز الرقمي
- التشهير
- أضرار نفسية
- التعرض لمحتوى عنيف أو جنسي

ماذا نعني بالهندسة الإجتماعية؟

بعد أن وثقت ببعض
الأصدقاء الجدد
وأعطيتهم كل المعلومات...
الآن اخترقوا كل حساباتي.

ماذا نعني بالهندسة الإجتماعية؟

هناك طرق عديدة لاختراق الحسابات الشخصية وسرقة المعلومات على الأنترنيت ومن بينها ما يسمى"بالهندسة الإجتماعية".
وهي وسيلة للإختراق يستخدم فيها المخترقون تقنيات وحيل لتجميع المعلومات الشخصية لاستخدامها في عملية الاختراق المباشر، أو لاستدراج الضحايا للضغط على روابط تحتوي على برمجيات خبيثة.
هذه المعلومات غالبا ما يتم تجميعها من حسابات مواقع التواصل الإجتماعي من خلال المنشورات التي يتم مشاركتها بعفوية لكنها قد تكشف عن بعض المعلومات الحساسة مثل: أماكن إقامتنا، أو رقم جواز السفر، أو رقم البطاقة الوطنية... وهي معلومات حساسة تسمح للمخترقين دراسة الشخصية، أو تجميع المعلومات من أجل اختيار الطرق المناسبة للإختراق واستدراج الضحايا.

5 أساليب للهندسة الإجتماعية

1. استغلال عواطف الضحايا وطباعهم الشخصية من خلال دراسة ما يقومون بمشاركته في مواقع التواصل الإجتماعي سواء في الحائط أو الخاص.
2. استغلال الشائعات لاستدراج الضحايا للضغط على الروابط المغلفة بالبرمجيات الخبيثة.
3. انتحال الشخصية لصديق مقرب أو شخص من العائلة من أجل الحصول على معلومات حساسة.
4. استغلال ضعف الخبرة التقنية في مجال السلامة الرقمية للضحية.
5. اصطياد كلمات السر (الشرح المفصل في المحور القادم).

بالإطلاع الدائم على
جديد السلامة الرقمية، وعدم مشاركة
المعلومات الحساسة والشخصية على
مواقع التواصل الإجتماعي.
لا تثق في الأشخاص الذين يسألونك عن معلومات حساسة
وشخصية للغاية،
استخدم مضاد الفيروسات Anti Virus
والتحديث المستمر للتطبيقات والبرامج
وتأكد من الروابط قبل الضغط عليها.

عليكم أن تعلموا أن الرسائل أو المكالمات التي تخبركم بأنكم فزتم بشيء ما، 99,99% منهم مجرد نصب واحتيال.

نصيحة سريعة

إحذروا من التصيد

ما المقصود بالتصيد؟

هو مجموعة من الأساليب الخداعية والتقنيات المستخدمة من طرف المخترقين للسيطرة على الحسابات الشخصية، سواء في مواقع التواصل الإجتماعي أو الحسابات البنكية أو البريد الإلكتروني...
وغالبا ما يتم فيه الإعتماد على ما يعرف بالهندسة الإجتماعية، وبعض طرق الإحتيال لسرقة كلمات السر، أو للسيطرة على الحواسيب.
ومن الطرق الشائعة للتصيد هناك الصفحات المزورة الشبيهة بصفحات المواقع المراد سرقة كلمة السر الخاصة بها، مثل صفحة الدخول لفيسبوك أو Gmail إذ أنها تخفي بداخلها برمجيات أو تقنيات تتيح إظهار كلمات السر "للهاكرز" الذي يستخدم طرقا جذابة لإغواء الضحية للدخول لهذه الروابط.

أبرز 6 طرق للتصيد

1. إستغلال ضعف الخبرة في مجال السلامة الرقمية للضحايا.
2. تزوير صفحات الدخول (تقنية الصفحات المزورة).
3. استغلال الأخبار الكاذبة وفترات إنتشار الشائعات.
4. استغلال العواطف والطباع الشخصية للضحايا (الهندسة الإجتماعية).
5. انتحال الشخصية.
6. استغلال المواضيع الساخنة أو الجنسية.

ما هي طرق الحماية من التصيد؟

1. تأكدوا من الروابط قبل الدخول لها أو الضغط عليها.

2. لا تقوموا بإعطاء معلومات عنكم لأي شخص غريب.

3. لا تنسوا أن تقوموا بالتحديث Mise à jour بصفة دائمة لكل البرامج والتطبيقات، لإغلاق الثغرات في البرامج لكي لا يتم إستغلالها من المخترقين لتثبيث البرمجيات الخبيثة في أجهزتكم.

4. عند التوصل برسالة إلكترونية تحتوي على رابط، لا تضغطوا عليه بل قوموا بنسخ الرابط ولصقه في المتصفح حتى لا يتم اختراق بريدكم الإلكتروني بالروابط الملغومة.

5. لا تقوموا بتحميل أي ملف مرفق من الرسائل الورادة من أشخاص مجهولين أو من رسائل تضم نوع من الإغراء المادي أو المعنوي.

6. استخدموا موقع Virus Total لفحص الملفات والروابط والتأكد من عدم احتوائها على برمجيات خبيثة.

فحص الملفات

فحص الروابط

اختبروا معلوماتكم عن التصيد

هذا الموقع عبارة عن أداة للتأكد من المعارف والمهارات المتعلقة بالحماية من التصيد.
يوفر مجموعة من الأسئلة التفاعلية، الهدف منها التنبيه ببعض طرق التصيد، وكذلك تدريبكم على الممارسات السليمة لحماية حساباتكم.
ادخلوا للموقع وجربوا إن كان بالإمكان الإيقاع بكم بالتصيد!

الرابط: https://phishingquiz.withgoogle.com/?hl=ar


علاش فينما نحط
شي صورة ولا شي تعليق
فمواقع التواصل الإجتماعي
كيبقاو صحابي
يتنمروا عليا ؟؟!!
كون غير
سكتي حسن
&$!#%
راسو
مربع

ما هو التنمر الإلكتروني؟

التنمر هو أحد أشكال العنف الذي يمارسه شخص أو مجموعة من الأشخاص ضد شخص أخر أو إزعاجه بطريقة متعمدة ومتكررة. وقد يأخذ التنمر أشكالًا متعددة كنشر الإشاعات، أو التهديد، أو مهاجمة الشخص المُتنمَّر عليه بدنيًا أو لفظيًا، أو عزل شخص ما بقصد الإيذاء أو حركات وأفعال أخرى تحدث بشكل غير ملحوظ.

unicef

فيما يلي تعرفوا على 8 علامات

للتنمر الإلكتروني

8 علامات للتعرف على التنمر الإلكتروني

1. التقليل من قيمة الشخص.

2. النعت بصفة إو إسم مسيء في مجموعات الدردشة أو وسائل التواصل الاجتماعي.

3. استخدام صور الأشخاص في محتوى ساخر (Memes).

4. نشر معلومات سواء حقيقية أو إشاعات ومحتوى كاذب بغرض تشويه سمعة الأفراد.

5. النشر في صفحات الأشخاص بغرض التضييق عليهم أو الإيقاع بهم.

6. تهديد الأشخاص بنشر صورهم أو محتوى عنهم لغرض يضر بهم.

7. إستغلال محتوى شخصي أو صور شخصية.

8. تذكروا أن كلمة كنت أمزح معك لا تمحي أثار التنمر.

غالبية هذه الأفعال تعرض أصحابها للمساءلة القانونية والمتابعة القضائية.


يجب أن تعطيني مبلغ مالي
وإلا سأقوم بنشر معلوماتك
اختراق

ماذا يعني الإبتزاز الإلكتروني؟

يعرف الإبتزاز الإلكتروني بكونه عملية تهديد بنشر صور أو فيديو أو معلومات شخصية و حساسة إذا لم يتم الرضوخ لطلبات المبتز، ومعظم الطلبات تكون على الشكل التالي:

1. دفع مبالغ مالية للمبتزين.
2. تصوير فيديوهات أو صور مخلة.
3. القيام بأعمال غير مشروعة.
4. الإفصاح عن معلومات سرية.

كيف يتم الإبتزاز؟

غالبا ما يقوم المبتزين بعمليات وطرق للإيقاع بالضحايا ومن بين الطرق الشائعة هناك:

- استدراج الضحايا إلى المحادثات الجنسية.
- الإيقاع بالضحايا بمحادثات مرئية مفبركة من أجل تصويرهم في وضعيات مخلة.
- سرقة الصور والمحادثات من أجهزة الضحايا عبر اختراق الحسابات بالتقنيات التي تحدثنا عنها سابقا مثل (التصيد، الهندسة الإجتماعية)
- إتصالات هاتفية خداعية.
- هجومات فيروسية (هجوم الفدية).

(وهي عبارة عن اختراقات تقوم بإغلاق أجهزة الضحايا وتقوم بتشفير كل الملفات وتطلب من الضحية أن يدفع مبلغ مالي لفتح الجهاز في أجال محددة وإذا ما لم يتم الرضوخ سيتم حذف كل الملفات من الجهاز.

ماذا يمكننا فعله للحماية من الإبتزاز الإلكتروني؟

حاولوا الإبتعاد عن المحادثات التي يمكن أن تسبب لكم المخاطر، سواء مع الأشخاص المجهولين وحتى مع المقربين، فالمبتز ليس بالضرورة شخصا مجهولا بل يمكنه أن يكون شخصا تثقون به.

لا تقوموا بتحميل ملفات أو تطبيقات من مواقع مجهولة.

احذروا من تفعيل خاصية المزامنة Synchronisation للصور والفيديو مع حساب Icloud أو Drive أو Google Photos يحيث إذا تم اختراق أي حساب منهم فصوركم وفيديوهاتكم كلها ستكون بين يدي المخترق.

لا تصدقوا رسائل SPAM أو الرسائل التي تحتوي على معلومات الربح أو الإغواء.

إذا تعرضتم للإبتزاز حاولوا التكلم مع شخص قريب وشاركوا معه المشكل ربما تتوصلون للحل معا، خصوصا أن المبتزين يخلقون حالة من الصدمة تشتت تفكير الضحايا.

تواصلوا مع خبير في مجال السلامة الرقمية.

اتصلوا بالأمن الوطني ولا تترددوا في طلب المساعدة.

يجب أن تعلموا

خلال عمليات الإبتزاز الإلكتروني، المبتزون يقومون بجمع معلومات مهمة حول حسابات عائلات وأصدقاء ضحاياهم، حيث يقوم المبتز/ة بتهديد الضحية بأنه سوف يتم تشويه سمعته/ها مع العائلة والأصدقاء.

وهو ما يخلق حالة من الصدمة للضحايا والخوف من الفضيحة..

المبتز غالبا حينما يصل للمبتغى لا يتوقف عن التهديد، بل يعاود الإبتزاز ويطلب المزيد.

لهذا فالتبليغ وطلب المساعدة هو أحسن حل وعدم البقاء وحيدا أمام المشكل قد يساعدكم.

ماذا أفعل إذا تعرضت للتشهير عبر الأنترنيت؟

لا تتجاوبوا مع المعتدي

احتفظوا بلقطة الشاشة Capture d’écrane

تواصلوا مع شخص مقرب وثقة
لتقديم المساعدة

تواصلوا مع خبير في السلامة الرقمية وفي كل
الأحوال تواصلوا مع برنامج سلامات

بلغوا السلطات المختصة


ما هي الأضرار النفسية للعنف الرقمي
؟

ما هي الأضرار النفسية للعنف الرقمي؟

تشير بعض الدراسات إلى أن ضحايا العنف إلكتروني من الممكن أي يعانوا من:

- اضطراب في الشهية.
- اضطراب في النوم، (من الممكن أن تكون أعراض إكتئاب).
- القلق المستمر.
- فقدان الإحساس بالآمان.
- الخوف من إما الجاني أو من نظرة المجتمع.
- إضطراب في الصورة الذاتية.
- إنخفاض في الثقة بالنفس.
- الإنعزال وعدم الرغبة في قضاء الوقت مع الآخرين (أو أداء أدوارهم الاجتماعية أو الذهاب إلى العمل، المدرسة).
- الإحساس بالوحدة (عدم القدرة على الإفصاح عن العنف من الممكن أن يسبب ذلك).
- ظهور اضطرابات في الصفات الشخصية (مثال، يصبح الضحايا أكثر عصبية، إنطوائية، خوف...

المصدر : موقع PSYCOM
www.psycom.net/iadcriteria.html

في حال التعرض للعنف الرقمي
هناك قانون 13-103
الذي يحمي النساء من العنف

العنف عبر الإنترنت أو العنف الرقمي

يشير العنف الرقمي أو عبر الإنترنت ضد المرأة إلى أي عمل من أعمال العنف التي يتم ارتكابها أو المساعدة عليها أو تفاقمها باستخدام تكنولوجيا المعلومات والاتصالات (الهواتف المحمولة والإنترنت ووسائل التواصل الاجتماعي وألعاب الحاسوب والرسائل النصية والبريد الإلكتروني وما إلى ذلك) ضد امرأة فقط لأنها امرأة.

يمكن أن يشمل العنف عبر الإنترنت ما يلي:

التنمر الإلكتروني، ويتضمن التنمر الإلكتروني إرسال رسائل تخويف أو تهديد.

الرسائل الجنسية غير الرضائية، وتتضمن الرسائل الجنسية غير الرضائية إرسال رسائل أو صور صريحة دون موافقة المستلم/ة.

الإفصاح عن المعلومات الشخصية، يتضمن هذا النوع الكشف العلني عن معلومات خاصة أو تعريفية للضحية.

هيئة الأمم المتحدة للمرأة

العنف الرقمي المسلط على النساء والفتيات

تسجيلات أو صور
ذات طبيعة جنسية
أو لأغراض جنسية

DOXING
نشر معلومات
شخصية عن الفتاة
أونلاين

التحرش
الجنسي

السب
والشتم

الإستغلال
والإبتزاز
الجنسي

التمييز
المبني على
النوع الإجتماعي

واحدة من كل أربع نساء تعرَّضَت للعنف عبر الأنترنيت،
في حين أن واحدة فقط من كل عشر نساء، تعرّضن للعنف الرّقمي، بادرت إلى
تبليغ السلطات العمومية عنه.

منظمة « MRA »

أهم العقوبات التي جاءت في قانون 103 - 13 لحماية النساء من العنف الرقمي

الفصل 447-1

يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 2.000 إلى 20.000 درهم، كل من قام عمدا، وبأي وسيلة بما في ذلك الأنظمة المعلوماتية، بالتقاط أو تسجيل أو بث أو توزيع أقوال أو معلومات صادرة بشكل خاص أو سري، دون موافقة أصحابها.

يعاقب بنفس العقوبة، من قام عمدا وبأي وسيلة، بتثبيت أو تسجيل أو بث أو توزيع صورة شخص أثناء تواجده في مكان خاص، دون موافقته.

الفصل 447-2

يعاقب بالحبس من سنة واحدة إلى ثلاث سنوات وغرامة من 2.000 إلى 20.000 درهم، كل من قام بأي وسيلة بما في ذلك الأنظمة المعلوماتية، ببث أو توزيع تركيبة مكونة من أقوال شخص أو صورته، دون موافقته، أو قام ببث أو توزيع ادعاءات أو وقائع كاذبة، بقصد المس بالحياة الخاصة للأشخاص أو التشهير بهم.

الفصل 503-1-1

يعتبر مرتكبا لجريمة التحرش الجنسي ويعاقب بالحبس من شهر واحد إلى ستة أشهر وغرامة من 2.000 إلى 10.000 درهم أو بإحدى هاتين العقوبتين كل من أمعن في مضايقة الغير في الحالات التالية:

1. في الفضاءات العمومية أو غيرها، بأفعال أو أقوال أو إشارات ذات طبيعة جنسية أو لأغراض جنسية؛
2. بواسطة رسائل مكتوبة أو هاتفية أو إلكترونية أو تسجيلات أو صور ذات طبيعة جنسية أو لأغراض جنسية.

تضاعف العقوبة إذا كان مرتكب الفعل زميلا في العمل أو من الأشخاص المكلفين بحفظ النظام والأمن في الفضاءات العمومية أو غيرها.

إذا تعرضتن للعنف الرقمي احتفظن بدليل مادي مثل تسجيل أو لقطة شاشة حتى يتبقى لديكن إثبات على الإعتداء.

نصيحة سريعة

لا تنسوا أنه هناك العديد من القوانين المغربية لحمايتكم في الفضاء الرقمي

لكل شخص الحق في حماية حياته الخاصة

الفصل 24 من الدستور

المادة 1

المعلوميات في خدمة المواطن، وتتطور في إطار التعاون الدولي. ويجب ألا تمس بالهوية والحقوق والحريات الجماعية أو الفردية الإنسان. وينبغي ألا تكون أداة الإفشاء أسرار الحياة الخاصة للمواطنين.

المادة 57

يعاقب بالحبس من 6 أشهر إلى سنتين وبغرامة من 50.000درهم إلى 300.000درهم أو بإحدى هاتين العقوبتين فقط،

كل من قام، دون الموافقة الصريحة للأشخاص المعنيين، بمعالجة معطيات ذات طابع شخصي تبين بشكل مباشر أو غير مباشر الأصول العرقية أو الاثنية، أو الآراء السياسية أو الفلسفية أو الدينية، أو الانتماءات النقابية للأشخاص المعنيين أو المتعلقة بصحة هؤلاء.

لقد تمت سرقة كلمات المرور
الخاصة بحساباتي الشخصية،
أود أن أعرف الوسائل
لحماية نفسي!

كلمة المرور Mot De Pass

كلنا لدينا العديد من الحسابات على الأنترنيت، وربما نستخدم نفس كلمة المرور Mot de pass لكل الحسابات بحيث تكون نفس كلمة المرور المستخدمة للفيسبوك هي نفسها في Gmail أو في حسابات أخرى.
هذه الطريقة قد تسهل علينا تذكر كلمة المرور، ولكن في نفس الوقت قد تشكل خطرا، بحيث إذا تم اختراق حساب واحد يمكن اختراق كل الحسابات الأخرى بسهولة.
كما أنه العديد منا يستخدمون إما تاريخ الميلاد أو إسم الأم أو تاريخ ولادة شخص مقرب ككلمة مرور، وهناك من يستخدمون تسلسلات عددية سهلة وهذه الطرق تسهل على المخترقين الذين يعتمدون على الهندسة الإجتماعية الوصول لكلمات المرور الحاصة بنا سواء عن طريق التخمين العقلي أو باستخدام بعض البرامج التي تقوم بهذه العملية أوتوماتيكيا وبسرعة كبيرة.

كلمات السر لا تستخدموها أبدا

123456 | 123456789 | azerty

password | azerty123 | 12345678 | 000000

iloveyou | adminadmin | 123123

كيف أقوي كلمة المرور؟

- المزج بين الأحرف الكبيرة والصغيرة.
- كلما زاد عدد الأحرف، كلما كان أفضل.
- المزج بين الأحرف والأرقام.
- إظافة رمز خاص واحد على الأقل، مثل! @ #؟]،
- كلما زدنا من الخصائص السابقة في كلمة المرور الخاصة بنا، كلما كانت أقوى.
- استخدموا تطبيق بتوليد وتخزين كلمات السر القوية.

أمور يجب أن نتجنبها؟

- أي كلمة من السهل إيجادها في القاموس مثل: (...salam1، maroc2021)
- كلمات مرور من حروف متكررة أو سلسلة من الأحرف مثل (، AAAAA أو 12345).
- لا تستخدموا نفس كلمة السر لكل الحسابات.
- سلسلة من الأحرف متجاورة في لوحة المفاتيح مثل (azerty أوqwerty).
- أن لا تكون كلمة السر عبارة عن معلومات شخصية مثل (أعياد الميلاد، أسماء الحيوانات الأليفة أو الأصدقاء، رقم الهاتق، العناوين، إسم الأم أو الأب، مكان الميلاد...إلخ).
- احفضوا كلمة السر في مكان آمن، ولا تكتبوه أمام أي شخص.

نصائح مهمة جدا

غيروا كلمة المرور بانتظام - تقريبا مرة بين ثلاثة إلى ستة أشهر.

غيروا كلمة المرور إذا كان لديكم أدنى شك في أن كلمة المرور معروفة لدي شخص ما أو موقع ما.

خصصوا لكل موقع كلمة سر خاصة به.

حاولوا ما أمكن أن لا تكتبوا كلمة المرور في أجهزة الكمبيوتر أو الهواتف غير الخاصة بكم خصوصا في مقاهي الإنترنت.

لا تقوموا بحفظ كلمات المرور أبدًا في متصفح الويب على جهاز الكمبيوتر وخصوصاً إذا كان الجهاز في مكان عام أو يتم استخدامه من طرف أشخاص أخرين.

استخدموا مدير لكلمات السر لحفظها بشكل آمن.

مواقع مهمة

جربوا إن سبق وتم اختراق كلمة المرور الخاصة بكم

https://monitor.firefox.com/

موقع لإنشاء كلمة مرور قوية

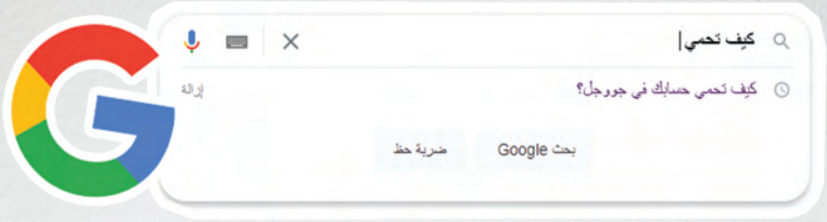
https://keepass.info

تم اختراق بريدي الإلكتروني
وقاموا باختراق حساباتي في فيسبوك
وإنستاغرام.. كيف أحمي حساباتي
في مواقع التواصل الإجتماعي؟

تعلموا معنا

كيفية حماية حساباتكم

في مواقع التواصل الإجتماعي



تعتبر خدمات Google من أكثر الخدمات على الأنترنيت التي يحتاجها رواد الأنترنيت، ويرى البعض أنه من المستحيل استخدام الأنترنيت بدون الإعتماد على خدمات مثل Youtube، Gmail و Drive وغيرهم.
الشيء الذي يجعل من شركة ALPHABET، الشركة الأم لGoogle ، من أكبر شركات التكنولوجيا عالميا التي تتوفر على معلومات مهمة عن مستخدمي الأنترنيت، إذ يعتقد الخبراء في المجال أن بإمكان Google أن تعرف عنا أكثر مما نعرفه عن أنفسنا.

وعليه باستطاعة شركة Google التعرف على كل أماكن تواجدنا بالضبط منذ استخدامنا لخدمتها Google Maps، كما يمكنها أن تتعرف على كل أرقام الهواتف لمعارفكم، ومع من تتواصلوان أكثر، من خلال خدمة Google Contact، وبإمكانها أيضا الوصول لكل صوركم وفيديوهاتكم والتعرف على كل أفراد عائلتك بتقنيات الذكاء الإصطناعي من خلال خدمة Google Image، بل إن معرفة الشركة بالأفراد قد تمتد لأبسط أنشطة الحياة اليومية بحيث تستطيع معرفة كم خطوة تخطوها يوميا وحالتكم الصحية من خلال خدمة FIT ، وكذا نوع عملكم وطبيعة علاقاتكم المهنية والمواقع، والمواقع التي تقومون بالتسجيل فيها من خلال Gmail، ناهيك عن قدرتهم على تحديد اهتمامتكم الفنية والثقافية وأنواع الموسيقى المفضلة لديكم، أو نوعية البرامج اللي تحبون مشاهدتها من خلال موقع Youtube، وكل التطبيقات التي تقومون بتنزيلها على أجهزتكم الذكية بالنسبة لمستخدمي نظام Android، وهو الأمر ذاته الذي ينطبق على المواقع التي تتصفحونها والأمور التي تبحثون عنها من خلال خدمة محرك البحث google أو من خلال متصفح Chrome.
لهذا من الضروري حماية أنفسنا سواء من الشركة أو من الأشخاص الذين قد يخترقون حساباتنا في google وقد تمكنهم من الوصول لكل هذه المعلومات ، إذا لم يتم اتخاد الإجراءات اللازمة.

كيف أحمي حسابي في GOOGLE ؟

كيفية تفعيل خاصية التحقق بخطوتين؟

01 إضغطوا على صورتكم الشخصية

02 وادخلوا لقائمة إدارة حسابكم على Google

03 بعد ذلك أدخلوا لقائمة الأمان

04 من هناك فعلوا خاصية التحقق بخطوتين

05 سيطلب منكم إدخال كلمة المرور لحساباتكم

06 اختاروا طريقة التوصل بالرمز السري (مكالمة أو تطبيق المصادقة، أو SMS)

07 أدخلوا الرمز المتوصل به بعد ذلك اختاروا تفعيل

معلومات مهمة جد

- انتبهوا للصلاحيات التي تمنحونها ل Google مثل مزامنة أرقام الهواتف والصور والملفات
- ألغوا خاصية مزامنة رفع الصور والفيديوهات أوتوماتيكيا ل Google Image أو DRIVE
- ألغوا خاصية تتبع GPS
- يمكن لكم معرفة كل المعلومات التي جمعها عنكمGoogle وبإمكانكم مسح السجل من خلال هاد الرابط:
https://myactivity.google.com/myactivity

نصائح مهمة

- لا تشاركوا كلمة المرور مع أي شخص.
- لا تدخلوا للروابط المشبوهة حتى وإن توصلتم بها من أصدقائكم المقربين.
- الرسائل التي تتوصلون بها على Gmail وتخبركم بالفوز بأموال أو الرسائل التي تضم ابتزاز أو نخبركم بأن لديهم صوركم لا تصدقوها وقوموا بمسحها مباشرة.
- إذا تعرضتم لابتزاز حقيقي، بلغوا السلطات وتواصلوا معنا أو مع خبير متخصص في الأمن الرقمي.
- حاولوا دائما أنلا تفتحوا حساباتكم من حاسوب أو هاتف ليس خاصا بكم، وإذا كنتم مضطرين،كونوا حذرين وأغلقوا حسابكتم بعد الإنتهاء وغيروا كلمة المرور.

إعدادات الخصوصية
ل Youtube من الحاسوب

1. ادخلوا إلى موقع Youtube من خلال الحاسوب و اتصلوا بحسابكم

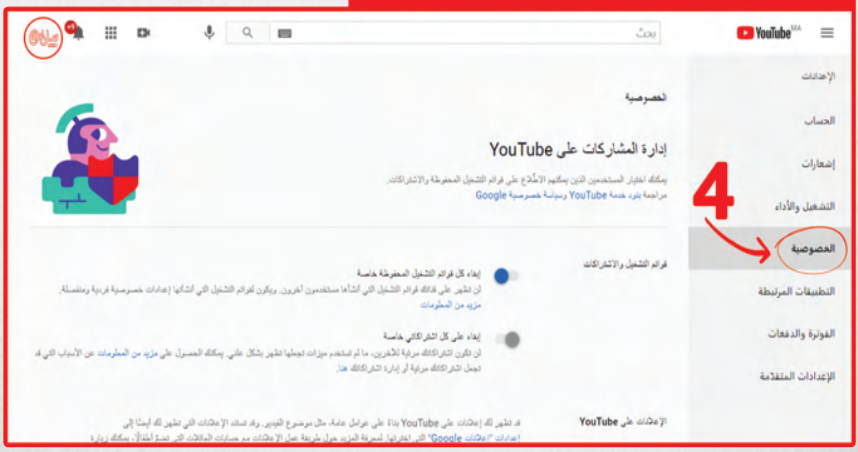
2. اضغطوا على الصورة الشخصية لإظهار القائمة كما هو مبين في الصورة

4. من صفحة الإعدادات، ادخلوا إلى إعدادات الخصوصية

5. من الصورة الأخيرة ستجدون اختياران

- تعديل خصوصية قوائم التشغيل التي يعدها المستخدم وعدم إظهارها للعموم.

- تعديل خصوصية لائحة القنوات التي يتم الإشتراك فيها المستخدم وعدم إظهارها للعموم.



إعدادات الخصوصية في Youtube من الهاتف

أدخلوا لقسم الإعدادات في تطبيق اليوتوب

"التذكير بالإستراحة من المشاهدة هذه الخاصية تذكركم بالتوقف عن المشاهدة بعد مدة معينة

"التذكير بموعد النوم للتوقف عن استعمال التطبيق بعد وقت معين

خاصية "الوضع المقيد"
و هي خاصية تخفي المحتوى الغير ملائم لعمر الأطفال

كيف أحمي حسابي في Facebook ؟

تتجسد قوة شركة Meta في كونها تمتلك المنصة الإجتماعية الأولى عالميا، واستحواذها على مجموعة من الخدمات الاخرى مثل واتساب وإنستاغرام، جعلت من الشبكة التي كانت تسمى سابقا بشركة فيسبوك تتبوء الصدارة في التوفر على بيانات المستخدمين على المستوى العالمي، وهذه البيانات جعلت من فيسبوك أكبر سوق للإعلانات في العالم والتي تشكل أكثر من 90 % من مداخيل الشركة. وبالرغم من جائحة كورونا وتدهور الإقتصاد العالمي إلا أن مداخيل الشركة من الإعلانات ارتفعت بأكثر من 22% في الربع الثالث من 2020 ووصلت لأزيد من 21.5 مليار دولار.

حسب الدراسة التي قمنا بها، وجدنا أن موقع وتطبيق فيسبوك لشركة Meta هو أكثر مواقع التواصل الإجتماعي استخداما سواء من طرف الطلبة أو الأساتذة، وهذا الأمر ينطبق على المستوى العالمي كذلك، كما جاء في التقرير العالمي المسمى " ديجيتال 2021 الذي ذكر أن عدد مستخدمي الشبكة وصل في بداية عام 2021 إلى قرابة 2.8 مليار مستخدم نشط في جميع أرجاء العالم.

أي ما يعادل تقريبا 36 % من إجمالي عدد سكان العالم المقدر عددهم بحوالي 7.8 مليار نسمة. الشيء الذي جعل من فيسبوك يحتل الرتبة الأولى عالميا من حيث عدد المستخدمين.

ويعرف أن شركة META الشركة الأم لفيسبوك تعمل دائما على تطوير تقنيات جديدة أو الإستثمار في التقنيات التي يتزايد عليها الطلب وهو ما قاموا به عند الإقبال على التعليم والعمل عن بعد خلال فترة جائحة كورونا وقاموا بإظافة غرف للدردشة الجماعية سواء عبرMessenger أو من خلال تطبيق Whatsapp. وذلك من أجل عدم فقدان المستخدمين لصالح لمنصات أخرى،

وأمام هذه السيطرة الكبيرة لشركة Meta يجب أن نكون واعيين بحقوقنا والأمور التي يجب الإحتياط منها من أجل حماية خصوصيتنا خلال استخدامنا لخدمات شركة META ومن بينها فيسبوك ذو التاريخ الكبير في انتهاك خصوصية المستخدمين .

كيف أحمي حسابي في Facebook ؟

كيف أقوم بتفعيل خاصية التحقق بخطوتين؟

01 أدخلوا إلى قائمة الإعدادات

02 ستجدون قائمة الأمان
اختاروا الأمان وتسجيل الدخول

03 اختاروا تفعيل خاصية
التحقق بخطوتين

04 بعد ذلك اختاروا الوسيلة
المناسبة لكم للتحقق بخطوتين
رقم الهاتف، أو تطبيق المصادقة، أو 10 رموز احتياطية)

05 ستتوصلون برمز سري
إما في SMS أو Email

06 أدخلوا الرمز السري
المتوصل به

كيف أحمي حسابي في Facebook ؟

كيف تعرف إذا تم الدخول لحسابك في Facebook من طرف شخص مجهول؟

01 أدخلوا لقائمة الإعدادات

02 اختاروا قائمة الإعدادات والخصوصية

03 ستجدون قائمة الأمان وتسجيل الدخول

04 اختاروا التوصل بتنبيهات إذا حاول شخص ما الدخول لحسابك فيسبوك

05 اختاروا طريقة التوصل بالتنبيهات عبر SMS و البريد الإلكتروني

اختيار قائمة الأصدقاء الموثوقين للمساعدة في استرجاع الحساب إذا تمت سرقته

01 أدخلوا لقائمة الإعدادات

02 إختاروا قائمة الإعدادات والخصوصية

03 ستجدون قائمة الأمان وتسجيل الدخول

04 حددوا بين 3 و 5 من الأصدقاء الموثوقين للمساعدة في حال سرقة حسابكم

كيف أحمي حسابي في Facebook ؟

نصائح مهمة

- استعملوا كلمة مرور قوية غير مكررة في موقع أخر
- لا تضغطوا على الروابط المشبوهة أو المجهولة حتى وإن توصلتم بها من أصدقائكم الموثوقين.
- انتبهوا لإعدادات الخصوصية، وتحكموا في من يستطيع رؤية منشوراتكم.
- أوقفوا خاصية GPS في الفيسبوك.
- حاولوا دائما أن لا تستخدموا حسابكم فيسبوك من كمبيوتر أو هاتف ليس خاصا بكم، وإذا كنتم مضطرين سجلوا الخروج، بعد الإنتهاء وغيروا كلمات السر

طرق التبليغ على المنشورات المخالفة في فايسبوك؟

للتبليغ عن أي انتهاكات للخصوصية أو أي شكل من أشكال العنف الرقمي اتبعوا هذه الخطوات :

للتبليغ عن حساب :
ادخلوا إلى الحساب المعني بالأمر
إضغطوا على ثلاث نقط بجانب الصورة الشخصية وبعد ذلك اختاروا إما الدعم أو الإبلاغ عن ملف شخصي.

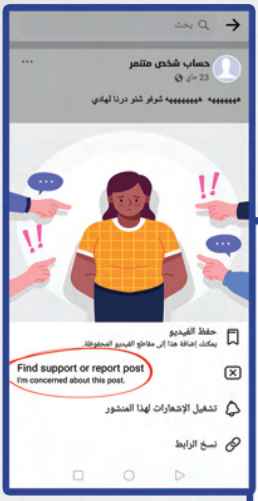
توفر المنصة العديد من الخيارات منها: (انتحال الصفة ، الحساب تم اختراقه، نشر محتوى غير ملائم) كلما كان بلاغك محددا وواضحا كلما زادت الفرص في الحد من نشاط الحساب أو إزالته.

خيار "انتحال صفة" من هناك يمكن اختيار إذا كنتم تبلغون لأنفسكم ، أو من أجل صديق أو لشخصية معروفة.
إذ اخترتم "من أجل صديق" سيطلب منكم تحديد الصديق المعني بالأمر .
وبعد ذلك اضغطوا على إرسال لتأكيد بلاغكم.
بعد الإرسال ، لكم الخيار أن تمنعوا الحساب أو كتمه (لعدم تلقي الرسائل منه).

طرق التبليغ على المنشورات المخالفة في فايسبوك؟

بإمكانكم التبليغ عن محتوى ضار أو يشكل تهديد (صورة أو منشور)، من خلال الضغط على الثلاث نقاط بجانب المنشور المعني بالبلاغ

و من هناك بإمكانكم اختيار نوع البلاغ.
تتوفر خيارات أخرى تحت "أخرى" مثل 'مشاركة صور خاصة '
بعد تحديد البلاغ إضغط على زر إرسال.



بإمكانكم أيضا التبليغ عن محادثة تحتوي على رسائل عنف أو تهديد... عبر الخطوات التالية :
الضغط على إسم المعني بالبلاغ في أعلى المحادثة.
واختاروا "هنالك مشكلة"
ستجدون عدة خيارات مثل "التحرش ، العنف اللفظي ، انتحال صفة" . بعد الإختيار، لك خيارات إيقاف التوصل بالرسائل من هذا الشخص أو منع الشخص القائم بالعنف.

حتى تأكدوا على البلاغ ، يجب الضغط على زر "تبليغ عن المحادثة" حتى يتم إرسال المحادثة إلى فريق فايسبوك للمراجعة.

في جميع الحالات أو الأمثلة المقدمة، سيتم فحص بلاغك و إرسال إخطار حينما تتم المراجعة.
في حال الخطر الكبير أو التهديد ينصح الإستعانة بأصدقاء أو منصات دعم مثل سلامات لاتباع نفس الخطوات و مساعدتك في الإبلاغ.

كيف أحمي حسابي في WHATSAPP؟

كيف أحمي حسابي في WHATSAPP؟

01 أدخلوا لقائمة الإعدادات واختاروا "الحساب"

02 ستجدون في القائمة "التحقق بخطوتين"

03 إضغطوا على تفعيل الخاصية

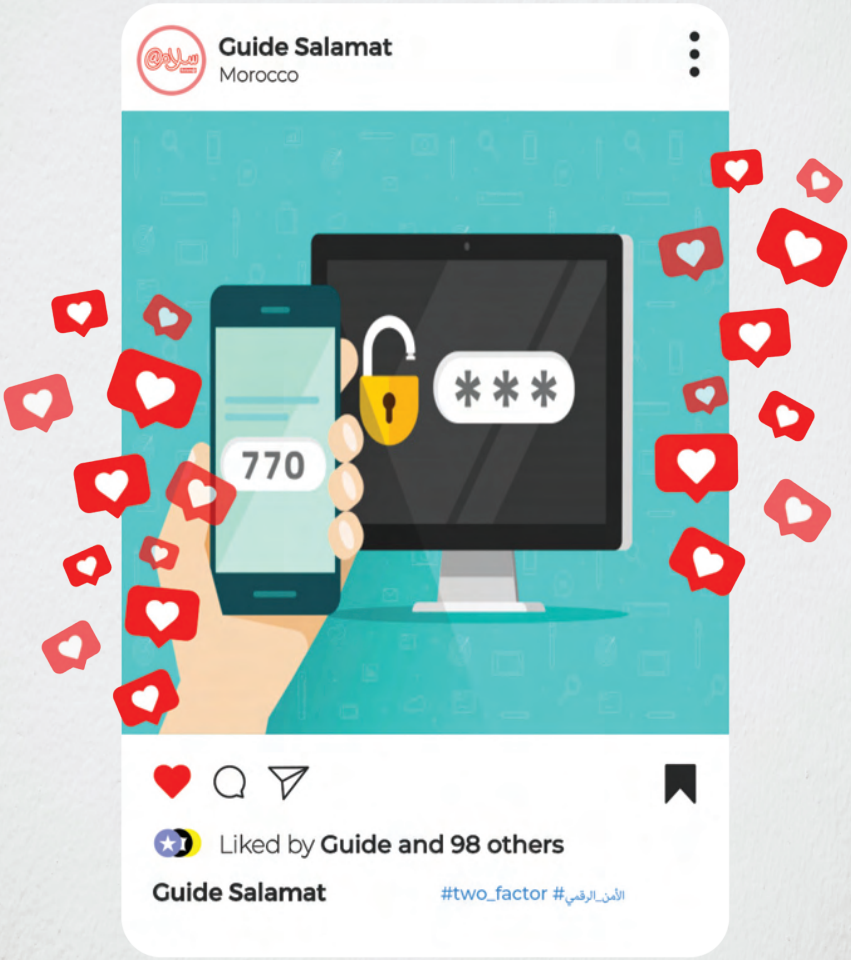
04 أدخلوا رقما سريا قويا وتذكروه جيدا

05 أدخلوا البريد الإلكتروني وسيتم تفعيل الخاصية

نصائح مهمة

- لا تشاركوا كلمة السر الخاصة بالتحقق بخطوتين مع أي شخص.
- لا تضغطوا على الروابط المشبوهة أو المجهولة أبدا.
- عدلوا إعدادات الخصوصية، للتحكم في من يستطيع رؤية stories والصورة الشخصية.
- حاولوا دائما أن لا تفتحوا حساب الواتساب من حاسوب أو هاتف ليس خاصا بكم وإن كنتم مضطرين، كونوا حذرين وأغلقوا حسابكم بعد الإنتهاء.
- إذا توصلتم برسالة أو صورة أو فيديو أو PDF... من رقم لا يتواجد بقائمة معارفكم أو رقم مشبوه لا تفتحو الملف المرفق وقوموا بمسحه مباشرة والتبليغ عن الحساب.

كيف أحمي حسابي في INSTAGRAM ؟



كيف أحمي حسابي في INSTAGRAM ؟

تفعيل خاصية التحقق بخطوتين

01. أدخلوا لقائمة الإعدادات
02. بعد ذلك اختاروا قائمة الأمان
03. من هناك فعلوا خاصية التحقق بخطوتين
04. ثم اختاروا الوسيلة المناسبة لكم للتحقق بخطوتين
(رقم الهاتف، أو تطبيق المصادقة، أو 10 رموز احتياطية)
05. ستتوصلون برمز سري في الوسيلة التي اخترتم
06. أدخلوا الرمز المتوصل به واغلقوا الصفحة

نصائح مهمة

- استعملوا كلمة مرور قوية وغير مكررة في موقع أخر.
- لا تدخلوا للروابط المشبوهة أو المجهولة.
- انتبهوا لإعدادات الخصوصية، وتحكموا فمن يستطيع رؤية stories و المنشورات الخاصة بكم.
- حاولوا دائما أن لا تستخدموا حساب إنستاغرام من جهاز ليس خاصا بكم، إذا كنتم مضطرين لذلك، لا تنسوا إغلاق الحساب وتغيير كلمة المرور.
- للتأكد بأن حسابكم لا يستخدمه أحد غيركم، جربوا هذه الخطوات: الإعدادات > الأمان > نشاط تسجيل الدخول

كيف أحمي حسابي في TIKTOK؟

ضبط إعدادات الخصوصية للحساب

- اضغطوا على خيار "الأمان" ومن ثم "أجهزتك" ستظهر لكم التنبيهات الأمنية والأجهزة المستخدمة للدخول على حساباتكم (راجعوها باستمرار لتتأكدوا من عدم دخول شخص مجهول).

- اختاروا "الخصوصية" وراجعوا الخصوصية حسب رغبتكم، أخذاً بعين الإعتبار الآثار المتوقعة، مثل قدرة المستخدمين على تنزيل مقاطع الفيديو الخاصة بكم واقتراح حسابكم للآخرين والقدرة على متابعتكم ومشاهدة مقاطعكم من العموم.

نصائح مهمة

- ☑ قوموا بتعيين كلمة مرور قوية وغير مكررة
- ☑ لا تشاركوا رمز التحقق المرسل إلى رقم هاتفكم أو بريدكم الإلكتروني مع أي شخص
- ☑ إذا لاحظتم شيئا غير اعتيادي في حسابكم قوموا بمراسلة الشركة مباشرة
- ☑ تجنبوا التجاوب مع الغرباء خصوصا عند طلبهم لإفشاء عن معلوماتكم الشخصية الحساسة

تعرفوا على أخطار رسائل SPAM؟

رسائل Spam تعرف بكونها رسائل جد مزعجة يتم إرسالها لأغراض تجارية بدرجة أولى ثم لأغراض خبيثة منها التصيد والإبتزاز وغيرهما...

يوميا يتم إرسال الملايين من الرسائل من هذا النوع، وغالبا حتى أنتم استلمتم على الأقل رسالة تخبركم بفوزكم بمبلغ كبير، أو شخص يطلب مساعدتكم لاستخراج مبلغ مالي من البنك...

وبالتالي فكل هذه الرسائل هدفها إما سرقة أموالكم أو اختراق الأجهزة من خلال الملفات الخبيثة المرفقة.

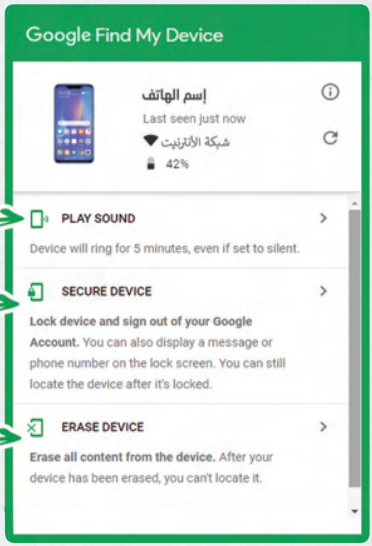
نصائح للتعامل مع رسائل SPAM؟

إذا توصلتم برسائل Spam:

- لا تضغطوا على الروابط المرفقة في هذه الرسائل.
- لا تردوا حتى تتأكدوا من المرسل.
- إذا شككتم في كونها رسالة نصب من عنوانها إمسحوا الرسالة ولا تفتحوها.
- لاتحملوا الملفات المرفقة مثل PDF أو صور من رسائل SPAM.
- إذا طلب منكم إرسال معلومات شخصية أو معلومات الحساب البنكي لا ترسلوهم ولا تردوا.

ماذا أفعل إذا ضاع أو سرق هاتفي؟

في حالة ضياع جهاز يشتغل بنظام أندرويد أو سرقته أول خطوة هي التوجه لموقع: www.google.com/android/find
الذي يمنح إمكانيات مهمة من بينها:
تتبع مكان الهاتف من خلال Google Maps.



إطلاق صوت إذا كان الهاتف قريب منكم

حماية الجهاز و وإغلاقه عن بعد
(وبامكانكم كتابة رسالة فيها رقم الهاتف)

مسح البيانات عن بعد

من الضروري التحقق من تفعيل خاصية الجهاز المفقود في الهاتف. بالنسبة لمستخدمي أندرويد يمكن تفعيل الخاصية من إعدادات حساب Google من قسم الحماية الذي تتواجد فيه خاصية إيجاد الهاتف.

ومن هناك يمكنكم تفعيل الخاصيات الآتية :

* التحكم عن بعد في الهاتف
* معرفة الموقع
* إرسال آخر معلومة عن مكان تواجد الجهاز قبل انطفائه.

ماذا أفعل إذا ضاع أو سرق هاتفي؟

بالنسبة للأجهزة اللي تعمل بنظام IOS الخاص ب Apple يتم تفعيل الخاصية من خلال موقع:www.icloud.com/find
وبعدها يتم إدخال Apple id و كلمة السر
لتفعيل خاصية إيجاد الهاتف وميزات أخرى :

ومهما كان نوع الجهاز فنحن ننصح بحذف كل البيانات إذا ضاع أو سرق منكم ، مع التركيز على حذف اتصال مواقع التواصل الإجتماعي والبريد الإلكتروني وتبليغ الأمن في حالة السرقة من أجل حماية أنفسكم من أي خطر أو استخدام غير قانوني لأجهزتكم أو البيانات التي تتواجد فيه.

هل مضادات الفيروسات مهمة ؟

بالطبع مضادات الفيروسات مهمة جدا لاسكتشاف وحماية الحواسيب والهواتف من البرمجيات الضارة التي يمكن أن تكون برمجيات هدفها التجسس أو سرقة البيانات أو الإضرار بالأجهزة وتعطيلها.

هناك أنواع كثيرة للبرمحيات الخبيثة التي لا يمكن أن نعرف بتواجدها في أجهزتنا بدون استخدام على الأقل برنامجا واحدا مضادا للفيروسات أو مضادات برمجيات التجسس.

لا يوجد برنامج واحد فعال لكل الفيروسات ولكن نستطيع كمثال استخدام برنامج Avira كمضاد للفيروسات وMalwarebytes كمضاد لبرمجيات التجسس و CCleaner كمنظف للأجهزة وتسريعها.

لماذا يجب علينا تفعيل حاصية التحديث Mise à Jour

التحديث المستمر للأجهزة وللتطبيقات المثبّتة وأنظمة التشغيل يساعد على توفير أحدث المميزات التي تأتي مع التحديثات، من بينها تحسين درجة الأمان وإغلاق بعض الثغرات التي يستخدمها الهاكرز لاختراق الأجهزة، غالبا حينما ترسل الشركة التحديث توضح الغرض منه والجديد الذي يحتويه.
لهذا لا يجب تجاهل تحديث الأجهزة وكل التطبيقات والبرامج التي نستخدمها ، مع قراءة الوصف الذي يكون مرفقا مع التحديث لمعرفة الجديد الذي جاء به.

ماذا يحدث حينما لا نقوم بالتحديث للأجهزة والتطبيقات؟

- تصبحون عرضة للقرصنة عن طريق الثغرات التي تظهر في بعض أنظمة التشغيل أو التطبيقات.
- ضعف الجهاز وعدم ثباته.
- عدم مواكبة تطور بعض البرامج والتطبيقات.
- توقف الدعم حيث أن بعض الشركات تخبر المستخدمين للنسخ القديمة بأنهم غير مسؤولين على أي مشكل أو قرصنة في حال الإستمرار بالعمل بالنسخ القديمة.

إحذروا مما تنشرون في حساباتكم على مواقع التواصل الإجتماعي !

من الواجب أن يكون كل مستخدم لمواقع التواصل الإجتماعي واعيا بما ينشر ، بحيث يجب الحذر من نشر المعلومات الكاذبة، والتشهير بالأشخاص.. إذ هناك معلومات قد تشكل خطرا إذا لم نأخذ بعين الإعتبار العواقب المترتبة عنها، وفيما يلي بعض الأمثلة:

راجعوا ما يلي:

من سيتطيع مشاهدة منشوراتكم،
فكروا ما إذ نشرتم معلومة ما هل قد تسبب لكم مشكلا ؟
لا تنشروا المعلومات الحساسة مثل تاريخ ومكان الميلاد ، التوجه الجنسي. المكان الجغرافي؟؟

لا تنشروا

محتوى عنيف أوجنسي بحيث يمكن أن يتسبب في إغلاق حساباتكم أو حتى في متابعات قضائية بتهم مثل التشهير...

معلومات مهمة

بعض المنشورات التي تحرض على الإرهاب أو عصيان القانون يمكن أن تتسبب في سجن صاحبها، لهذا من الضروري الإبتعاد عن هذا النوع من المنشورات.

إحذروا من WIFI وشحن الأجهزة في الأماكن العمومية

Wifi Public

غير أمن بتاتا، بحيث أنه عندما ترتبطون بشبكة WIFI من مقهى أو مطار فأنتم تكونون معرضين لخطر الإختراق والتجسس من طرف الأشخاص المتواجدين معكم في نفس الشبكة.

شحن الأجهزة في الأماكن العمومية

غير أمن خصوصا إذا كان يحتوي على منفذ Port USB، حيث يمكن أن يكون ذلك المنفذ مرتبطا مع جهاز يمكن الهاكرز من اختراق أجهزتكم.


5+
TEST

تعلموا معنا
طرق استخدام
منصات
التعليم عن بعد

غيرت أزمة كورونا التي عرفها العالم أنماط العيش لدى المجتمعات والأفراد، كما أثرت على جميع القطاعات، كما هو الحال مع قطاع التربية والتكوين. فانتشار الوباء دفع المدارس والجامعات والمؤسسات التعليمية لإغلاق أبوابها من أجل محاصرة انتشار الوباء .

ومع هذا التغيير المفاجئ ظهر الإحتياج الكبير للتحول إلى التعلم الإلكتروني (E-Learning)، كبديل كان قبل كورونا ولكن ليس بالشكل والإنتشار الحالي.

وفي المغرب وكسائر بلدان العالم توجهت غالبية المؤسسات التعليمية نحو التعليم عن بعد كبديل أنسب لضمان استمرارية العملية التعليمية.

الشيء الذي أدى لزيادة كبيرة في عدد المستخدمين للأنترنيت وسط الأساتذة والأستاذات وهو الأمر الذي وازاه ارتفاع ملحوظ في استخدام تطبيقات محادثات الفيديو عبر الأنترنيت مثل "Zoom" و"Microsoft Teams" وغيرهم.

هذه المتغيرات كلها طرحت تساؤلات حول الجاهزية لهذا الإنتقال السريـــع نحو رقمنة العملية التعلمية التعليمية عبر استخدام التكنولوجيا الحديثة في عملية التعلم،

واستشعارا منا لأهمية المساهمة في تقوية قدرات الفاعلين في هذا المجالات، نقدم لكم شروحات لأكثر المنصات استخداما في عملية التعليم عن بعد وهما:

Zoom و Microsoft Teams.

خطوات التسجيل وتحميل منصة TEAMS

أدخلوا لموقع Microsoft.com/ar-ww/microsoft-teams

إذا سبق لكم التسجيل أدخلوا من هنا

حملوا البرنامج للحاسوب أو التطبيق للأندرويد أو IOS

تسجيل حساب جديد

بعد التسجيل بالبريد الإلكتروني وتفعيل الحساب فعلوا خيار "للمؤسسة التعليمية" لتحصلوا على مميزات تسهل عملية التعليم عن بعد:

الإختيارات المتاحة في منصة Microsoft Teams

تعرفوا على مميزات منصة Teams

الدردشة
مع المجموعة

الفرق
والفصول الدراسية

الواجبات
الدراسية

الحصول على المزيد
من أدوات العمل مثل
WORD و EXCEL
ومشاركة الملفات

إنشاء فريق جديد
للعمل جماعياً

إذا كنتم أعضاء في فريق
يمكن لكم الدحول من هنا

إسم الفريق
أو المجموعة

وصف الفريق
أو الغرض من المجموعة

تحديد الخصوصية للفريق
(عام أو خاص)

هذه الخاصية تساعد في الحماية من دخول المتطفلين لفريقكم
وكذلك للأقسام الإفتراضية، لهذا فنحن نوصي بتفعيل وضع - خاص -

3 موارد مهمة لتعلم طرق استخدام Teams

1. دلائل إرشادية للطلاب وعائلاتهم والمعلمين والمؤسسات التعليمية للإنتقال للتعلم عن بعد.

https://www.microsoft.com/fr-FR/education/remote-learning

2. موارد مخصصة للمعلمين والمسؤولين عن عملية التعليم عن بعد في المدارس والجامعات.

https://www.microsoft.com/fr-FR/education/products/teams

3. موارد مخصصة للآباء والأمهات وأولياء الأمور.

https://education.microsoft.com/fr-FR/resource/V00e0aΛb

طريقة تفعيل التحقق بخطوتين

للتحقق باستخدام رقم الهاتف

01 اختاروا من القائمة هاتف المصادقة

02 اختاروا بلدكم وادخلوا رقم هاتفكم

03 حددوا خيارات إرسال رمز حسب الرسالة النصية

04 ستتوصلون برسالة SMS ادخلوا رمز التحقق

05 ثم انقروا على التحقق من صحة الرمز

06 ستصلكم رسالة تعلمكم بتسجيل رقم الهاتف بنجاح

يمكنكم أيضا الإستعانة بتطبيق Microsoft Authenticator
وهو متوفر في APP Store و Play Store

يمكنكم الوصول للتطبيق من هذا الرابط :

https://www.microsoft.com/en-us/security/mobile-authenticator-app

بالنسبة للشرح المفصل لاستخدام تطبيق المصادقة لميكروسوفت تقدم لكن هذا الرابط:

https://youtu.be/PaSaq99c9n8

نصائح للحماية في Microsoft Teams

- لا تشاركوا بيانات حساباتكم Teams أبدًا!
- لا تنسوا تفعيل كلمة مرور للإجتماعات والفصول
- فعلوا تخصيص حضور الإجتماعات فقط بالدعوات
- إحذروا من التصيد بالصفحات المزيفة ل Teams
- فعلو خاصية التحقق بخطوتين لحساباتكم

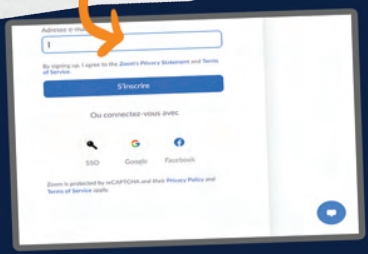
5 خطوات للتسجيل في zoom

1

تسجلوا من هنا

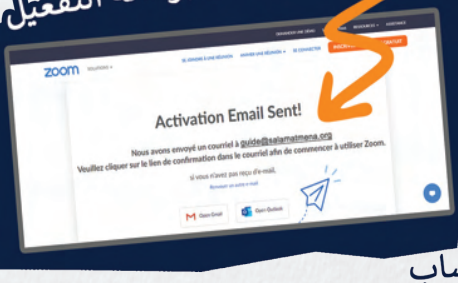
2

أدخلوا البريد الإلكتروني



3

التوصل برسالة التفعيل



4

تفعيل الحساب
من البريد الإلكتروني

*كلمة السر يجب أن تكون قوية

5

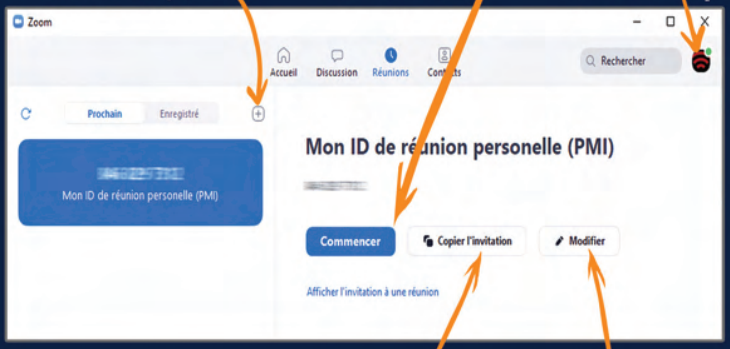
أدخلوا المعلومات الشخصية

إعداد حصة تعليمية أو لقاء في ZOOM

1 لتحميل برنامج ZOOM في الحاسوب

2 أدخلوا لحسابكم في ZOOM

3 الخطوات الأساسية لإعداد لقاء في zoom



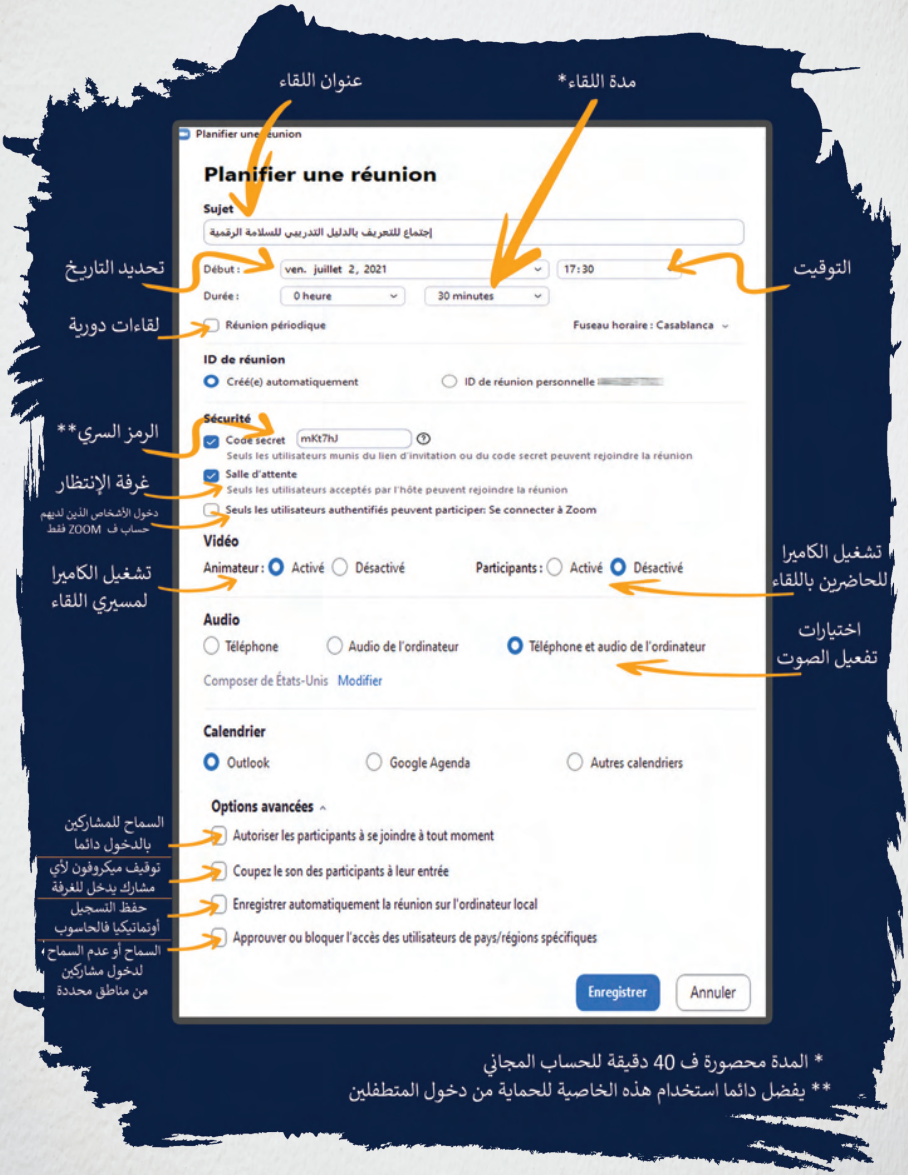
*شرح مفصل في الصفحة التالية:

مميزات ZOOM

الجيد في منصة ZOOM أن كل الحسابات سواء المجانية أو المدفوعة توفر إمكانيات التواصل كتابيا وصوتيا وكذلك إمكانية عرض الشاشة لتقديم الدروس بعروض Powerpoint أو PDF أو فيديو أو بأي صيغة تفضلونها، وهذه الإمكانيات تتوفر لكل الحاضرين في الفصل التعليمي أو في اللقاء لتقديم عروضهم هم كذلك، بشرط الحصول على موافقة مدير الغرفة لاستخدام هذه الإمكانية، ويمكن كذلك للمسؤول عن إدارة الغرفة إيقاف الميكروفون أو الكاميرا لأي فرد، وإخراج أو إيقاف أي مشارك متطفل أو فوضوي، وهذه الإمكانيات مهمة جدا لتنظيم عملية التعلم عن بعد واستكمال الدروس بشكل عملي سلس.

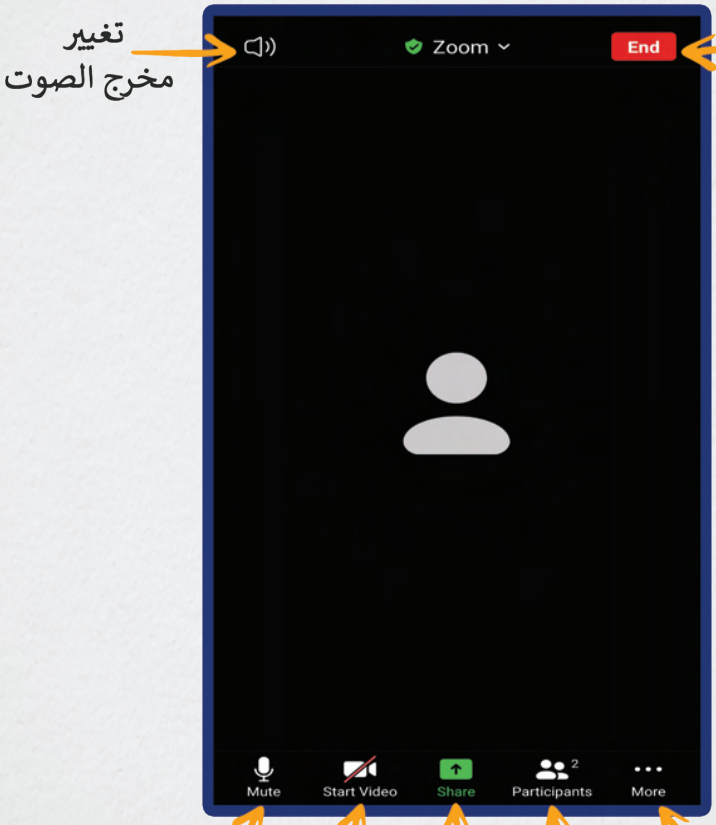
ولاستخدام بعض هذه الإمكانيات، نقدم لكم بعضا منها في الشروحات التالية:

إعداد حصة تعليمية أو لقاء بمواصفات محددة

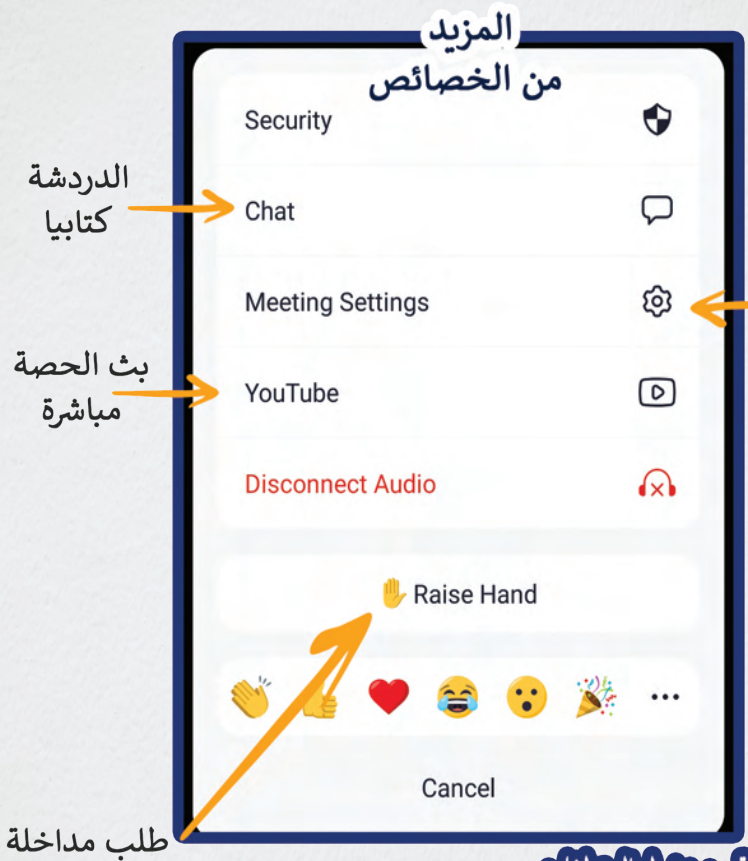


* المدة محصورة ف 40 دقيقة للحساب المجاني
** يفضل دائما استخدام هذه الخاصية للحماية من دخول المتطفلين

إدارة حصة تعليمية على منصة zoom



إدارة حصة تعليمية على منصة zoom



نصائح للحماية من دخول المتطفلين

في الحصص التعليمية تأكدوا من أن الحاضرين هم فقط من التلاميذ والأطر التربوية وكونوا حذرين من نشر رابط الحصص مع أشخاص مجهولين.

ودائما فعلوا خاصية الإجتماعات المغلقة بكلمة المرور، وقوموا بتفعيل غرفة الإنتظار لتتحكموا في الأشخاص الذين لديهم الحق في الدخول للغرفة.

وبذلك ستعملون على حماية حصصكم التعليمية ولقاءاتكم من دخول المتطفلين.

نصائح للحماية في ZOOM

- لا تشاركوا بيانات حساباتكم ل ZOOM أبدًا!
- لا تنسوا تفعيل كلمة مرور للإجتماعات يدويًا
- غيروا معرف الإجتماع (Meeting ID)
- فعلوا خاصية غرفة الإنتظار Waiting Room
- أوقفوا خاصية تعقب الانتباه (Attention Tracking)
- احذروا من تطبيقات ZOOM المزيفة
- استخدموا نسخة الويب من ZOOM لأنها أكثر أماناً
- فعلو خاصية التحقق بخطوتين لحساباتكم في ZOOM

تذكروا دائما

- التعلم المستمر والتعرف على الجديد في مجال السلامة الرقمية
- استخدام تقنيات التحقق بخطوتين ونفعيلها لحماية حساباتكم من القرصنة.
- أن تكونوا حذرين من الروابط والمرفقات والملفات الموجودة على البريد الإلكتروني وتطبيقات الدردشة.
- الحذر من المحتالين الذين يطلبون معلومات شخصية عنكم ، وأن لا تقدموا أبدًا معلومات شخصية خاصة عبر الإنترنت
- الحذر من المواقع المزيفة أو غير الرسمية
- الحذر من أجهزة الكمبيوتر العامة وUSB
- أن تستخدموا كلمات مرور / كلمات سر قوية
- أن تستخدموا تطبيقات إدارة كلمات المرور
- أن تستخدموا برامج مكافحة الفيروسات وجدار الحماية
- حافظوا على تحديث أنظمة التشغيل والبرامج والتطبيقات
- احتفظوا بنسخ احتياطية لملفاتكم في أماكن آمنة
- اهتموا أكثر بموضوع الخصوصية وحماية المعطيات الشخصية
- التعرف على القوانين الي تحمي خصوصيتكم في الفضاء الرقمي
- إذا تعرضتم للعنف الرقمي أو قرصنة لا تترددوا في التواصل مع خبراء في المجال الرقمي أو مع الأمن الوطني.

دراستين حول استخدام الإنترنت والشبكات الاجتماعية من قبل الشباب والأطفال

دراسة قامت بها جمعية الفكر السليم للتنمية

https://drive.google.com/file/d/١٣ltW٣t٥zByJSq٥gPJgjeL١Sve٦WGwnJh/view?usp=sharing

دراسة لجمعية سمسم مشاركة مواطنة ومؤسسة Happy Samala

https://drive.google.com/file/d/١SNnngq٠KmtsPDPebVssMa٦ZΛBgTrLjxO/view?usp=sharing

المصادر:

سلامات المغرب

سلامتك

سلامتك ويكي

CPOMAGAZINE

فريق العمل

الدليل من إعداد وإنجاز: سفيان السعودي

إشراف وتنسيق: منير النايلي - مؤسسة SecDev

الصور والمرئيات: بسنت عاطف

المراجعة والتدقيق: جمعية الفكر السليم للتنمية

مراجعة محتوى السلامة الرقمية: أحمد حجاب - مؤسسة SecDev

المراجعة السيكولوجية: فرح شاش- مؤسسة SecDev

تدقيق ومراجعة نهائية:

محمد التوزاني: مفتش تربوي بمديرية مكناس

عبد الحق متال: رئيس مصلحة الشؤون التربوية - مديرية مكناس

عبد الجليل الغزوي : رئيس CPSI - مديرية مكناس

كل الشكر للمركز الجهوي لمنظومة الإعلام - المديرية الجهوية لوزارة التربية الوطنية والتعليم الأولي والرياضة بمكناس، ولكل للأستاذات والأساتذة الذين ساهموا في مراجعة الدليل.

إذا كانت لديكم أية استفسارات أو واجهتم مشكلا متعلقا بالسلامة الرقمية تواصلوا مع صفحة سلامات

https://www.facebook.com/salamatMOROCCO

SALAMAT_MOROCCO

instagram

facebook

تواصلوا مع برنامج سلامات في الشرق الأوسط وشمال إفريقيا

http://portal.salamatmena.org/

Website

مؤسسة سكديف The secDev Foundation

https://secdev-foundation.org/

Website

جمعية الفكر السليم للتنمية

زورونا على صفحتنا

Proper Thought for Development
N 671, App 2 Marjane 3 Meknes. Tél.: 0660933864 – 0626671129
Mail: info@propertd.com/ www.propertd.com

دليل السلامة الرقمية في التعلم عن بعد

تحميل الدليل

هذا الدليل يوزع مجانا