تقنية المعلومات
Information Technology

أمن المعلومات
Information Security

#وعيك_يحمينا

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

عن أمن المعلومات

يعمل أمن المعلومات بجامعة الملك خالد تحت إدارة تقنية المعلومات، ويهدف للتطوير والمحافظة على أمن وحماية المعلومات وإدارة المخاطر وتدقيق البرامج، ونطمح من خلال هذه العمليات إلى التأكد من سرية وسلامة وتوافر المعلومات للموظفين وأعضاء هيئة التدريس والطلاب.

أهداف أمن المعلومات بالجامعة

- تطوير السياسات و الإجراءات الأمنية اللازمة.
- تحديد المخاطر التي تهدد أمن ونظم المعلومات.
- تحديد متطلبات أمن المعلومات، وإنشاء الحد الأدنى والأساسي لأمن المعلومات على أساس القوانين واللوائح المعترف بها، وأفضل الممارسات الأمنية.
- التأكد من تطوير خطط الإستجابة للحوادث وضمان تنفيذها.
- زيادة الوعي لدى منسوبي الجامعة في أمن المعلومات.
- حماية أصول المعلومات من الوصول الغير مصرح به، أو تعديلها، أو الكشف عنها أو اتلافها.
- إدارة أنظمة وبرامج أمن المعلومات.
- إجراء إختبارات ضمان الأمان لحماية الشبكة والأنظمة.
- التأكد من فاعلية برامج الحماية على أجهزة جميع المستخدمين.

مبادرة #وعيك_يحمينا

- تحقيقاً لقرار مجلس الوزراء رقم (81) وتاريخ 1430/3/19هـ البند الخامس الفقرة الثالثة، القاضي بتوجيه كل جهة حكومية بإعداد برامج توعوية للمستخدمين في مجال أمن المعلومات. قام قسم أمن المعلومات بالإدارة العامة لتقنية المعلومات بمبادرة "وعيك يحمينا" التي تتماشى مع إرشادات وأطر هيئة الاتصالات وتقنية المعلومات.

- تهدف مبادرة "وعيك يحمينا" إلى تعزيز ونشر ثقافة الوعي بأمن المعلومات في المجتمع الجامعي ، وإعطاء فكرة أساسية عن مفاهيم أمن المعلومات ، وزيادة الرصيد المعرفي ، والإرتقاء بمستوى أمن المعلومات ، وإيضاح المخاطر المعلوماتية ومدى تأثيرها.

- تقدم مبادرة "وعيك يحمينا" خدمات توعوية موجهة ، من خلال إقامة ورش عمل حول أساسيات ومفاهيم أمن المعلومات والمخاطر المعلوماتية ، كما يتم عبر صفحة المبادرة تقديم عدد من الفيديوهات التي تحتوي على معلومات ومفاهيم تم استقاؤها من الكتب والمصادر العالمية وفق أعلى معايير الجودة والنجاح في مجال أمن المعلومات.

احم بريدك الالكتروني من السرقة

طرق سرقته؟

- وجود برامج أو أجهزة تجسسية في حاسوبك.
- الدخول لبريدك الإلكتروني من خلال مقاهي الإنترنت أو الشبكات العامة.
- إختيار كلمة مرور ضعيفة مثل أسماء معروفة أو أرقام.
- أجوبة الأسئلة الخاصة عند فقدان كلمة المرور سهلة التخمين.
- التسجيل في منتديات أو مواقع بنفس كلمة المرور الخاصة ببريدك الإلكتروني.
- السماح للبرامج بالاحتفاظ بكلمة المرور وتذكرها بدلاً عنك.
- كشف كلمة المرور لشخص آخر.
- كتابة كلمة المرور في مكان غير آمن.
- بقاء كلمة المرور لفترات طويلة دون تغيير.

طرق الحماية؟

- حدّث أنظمة التشغيل والبرامج بشكل مستمر.
- قم بتشغيل مكافح الفيروسات وحدّثه باستمرار.
- تجنب الدخول لحسابك البريدي من مقاهي الإنترنت والشبكات العامة.
- تجنب الدخول لبريدك الإلكتروني من أي نافذة منبثقة.
- إختر كلمة مرور قوية وخاصة للبريد الإلكتروني، وحدثها دورياً.
- لا تكتب أجوبة سهلة التخمين للأسئلة المطلوبة عند فقدان كلمة المرور.
- تجنب استخدام نفس كلمة المرور في أكثر من حساب.
- لا تسمح للبرامج بالاحتفاظ بكلمة المرور.
- لا تكشف كلمة المرور لأحد ولا تحتفظ بها في مكان غير آمن.

اجعل تصفحك للإنترنت آمن

لجعل متصفح الإنترنت آمن:

1. قم بتحديث متصفح الإنترنت باستمرار.
2. إحرص على عدم حفظ كلمات المرور من خلال برنامج المتصفح (باختيار "تذكرني") ، لأنه يمكن للمخترقين الحصول عليها عند اختراق الجهاز.
3. إحرص على مسح المحفوظات والملفات المؤقتة والكوكيز من برنامج المتصفح بشكل مستمر، خاصة بعد زيارة المواقع الحساسة مثل البنوك.
4. إضبط إعدادات المتصفح لتحديد المواقع التي يُسمح لها باستخدام الكوكيز.
5. إمنع النوافذ المنبثقة، فبعضها ربما يشكل هجمات خبيثة أو خفية.
6. لا تحاول التخلص من النوافذ المنبثقة عند ظهورها بالضغط على زر "موافق" بل أغلقها فوراً.
7. تأكد من ضبط إعدادات الأمان والخصوصية والمحتوى لمتصفح الإنترنت. يجب أن يكون مستوى الأمان "متوسط" على أقل تقدير.
8. قم بتعطيل مكونات JavaScript و Java و ActiveX في حال رغبتك بتصفح مواقع غير موثوق بها.

تعامل مع مواقع التواصل الاجتماعي بأمان

التعامل الآمن داخل مواقع التواصل الإجتماعية :

1. اعلم أنه بتسجل بياناتك الشخصية على مواقع التواصل الإجتماعية ، فإنك قد قمت بعرضها للجميع؛ لذلك احرص على ضبط "إعدادات الخصوصية" وذلك لإنتقاء الأشخاص الذين تود أن تشاركهم هذه المعلومات دون الآخرين.
2. إستخدم الكنية عوضاً عن اسمك الحقيقي.
3. تجنب عرض عنوان السكن أو العمل أو أرقام الهاتف لأن مثل هذه المعلومات يمكن أن تُستَغل من قبل الآخرين.
4. لا تقم بعرض بيانات قد تدل على كلمة المرور الخاصة بك.
5. إحذر من عرض صور خاصة بك يمكن استغلالها من قبل ضعاف النفوس.
6. لا تنشر معلومات تخص بيئة عملك كأنواع الأنظمة والأجهزة والشركات المصنعة لها.
7. إحذر من قبول طلبات الإضافة من أشخاص لا تعرفهم، واحرص على معرفة سبب طلبهم لإضافتك (مثل إرسال بريد إلكتروني لهم قبل قبول الإضافة..ماهو سبب إضافتك لي؟).
8. راجع سياسات الخصوصية للموقع الذي تتعامل معه.

هل أنت على وعي بمخاطر أمن المعلومات!!

تعرف على مخاطر أمن المعلومات :

(Trojan) برمجية خبيثة تستطيع التحكم بجهازك عن طريق الشبكة.

(Virus) برنامج خبيث قد يؤدي إلى تعطيل جهازك أو حذف ملفاتك.

(Spam) بريد إلكتروني يحتوي على إعلانات تصلك من مصدر مجهول.

(Spyware) برمجية خبيثة تهدف إلى التجسس على بياناتك الشخصية .

(Phishing) موقع إلكتروني للتصيد يوهمك بأنه موقع ترتاده ويهدف لسرقة حسابك.

(Vulnerability) ثغرة أمنية متواجدة يمكن استغلالها من قبل المخربين.

(Worm) برنامج خبيث مثل الفايرس ولكن له المقدرة على الإنتشار بين الحواسيب.

متى يكون استخدامك للأجهزة العامة آمن؟

الإستخدام الآمن للأجهزة العامة:

1. لا تسمح بخيار التخزين التلقائي لبيانات الدخول الخاصة بك.
2. لا تبتعد عن الجهاز أثناء عرض معلومات حساسة خاصة بك.
3. امسح الملفات المؤقتة التي قمت بفتحها أثناء العمل على الجهاز (مثل ملفات الإنترنت المؤقتة و الكوكيز وغيرها).
4. انتبه من الأشخاص الذين يقفون حولك لأنهم قد يراقبوا ما تقوم بعمله.
6. لا تستخدم الأجهزة العامة للدخول إلى الحسابات البنكية أو إلى معلومات حساسة.
5. لا تسجل معلومات حساسة في الأجهزة العامة.
7. تأكد من الخروج بالشكل الصحيح عند الرغبة في المغادرة (مثل الضغط على زر تسجيل الخروج الموجود في الموقع).

إحذر من برامج التجسس !!

كيف تكتشف إصابة حاسوبك ببرنامج تجسس؟

- عن طريق فحص جهازك باستخدام البرامج المضادة للتجسس بشكل دوري.
- تغير صفحة البداية في متصفح الإنترنت بشكل مفاجئ.
- يصبح جهاز الحاسوب فجأة بطيئاً جداً عند فتح برامج أو تنفيذ المهام.
- ظهور رسائل خطأ بشكل عشوائي.

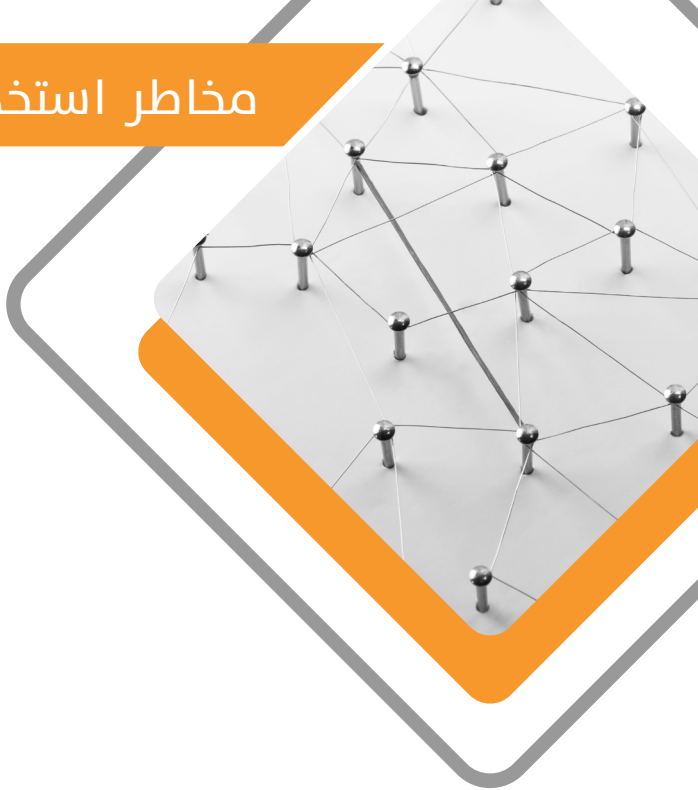
كيف تحصن حاسوبك ضد برامج التجسس؟

- كن حذرا عند تحميل البرامج المجانية الغير موثوقة.
- لا تقم بتنصيب البرامج المقرصنة وغير الأصلية.
- إحرص على قراءة "اتفاقية الإستخدام" للتأكد من خلو البرنامج من محاولة تجميع معلومات خاصة لأغراض دعائية.
- لا تستجب لروابط البريد الإلكتروني التي تدعي تقديم برامج لمكافحة التجسس.

كيف تزيل برامج التجسس؟

- شغل البرامج المضادة للفيروسات مع فحص كامل لجهازك.
- استخدم البرامج الأصلية المصممة خصيصاً لإزالة برامج التجسس.
- تأكد من عدم وجود تعارض بين برنامج مكافحة الفيروسات وبرنامج مكافحة التجسس.

مخاطر استخدام مواقع التورنت (Torrent)



توفر مواقع التورنت طريقة سريعة وسهلى وفعالة لتحميل الملفات من الإنترنت خصوصا ذات الحجم الكبير ، غير أنه يمكن أن تعرضك للكثير من المخاطر ، مثل :

• إمكانية تحميل ملفات خبيثة.

• بناءً على إحصائيات نشرتها شركة (InfoArmor) في آواخر 2016 اتضح أن الملفات الخبيثة التي يتم تحميلها من مواقع التورنت هي السبب في تضرر ما يزيد عن 12 مليون مستخدم شهرياً.

• الدخول غير المصرح به للجهاز.

• عند تحميلك لملفات بإستخدام التورنت والتي قد تبدو سليمة في ظاهرها إلا أنها قد تستخدم لفتح منافذ للوصول لبيانات الجهاز أو التحكم فيه عن بعد.

• المساءلة القاونية.

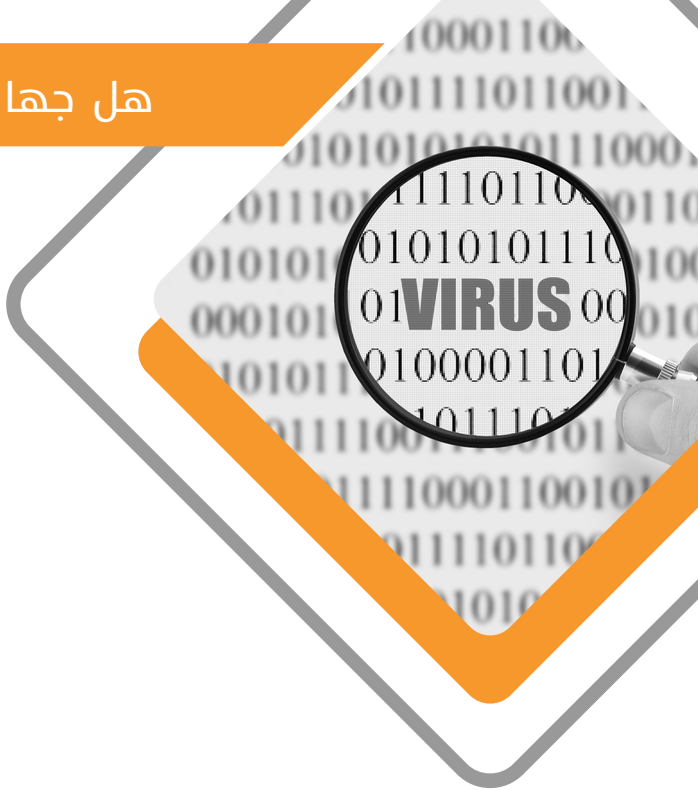
• استخدامك لمواقع التورنت لتحميل الأفلام ، الملفات الصوتية أو البرامج محمية الحقوق، تعتبر جريمة معلوماتية في بعض الدول يعاقب عليها القانون بالسجن والغرامات المالية.

هل هناك تهديد أمني أثناء استخدامك للمحادثات الفورية ؟

الإستخدام الآمن للمحادثات الفورية :

- لا تفتح أي صورة أو تحمل ملفاً أو تضغط رابط إلا إذا تأكدت تماماً من هوية المرسل وأن مصدره موثوق.
- لا ترسل معلومات حساسة أو خاصة عبر المحادثات الفورية.
- لا تستخدم أسماء مستعارة تدل على معلومات شخصية مثل دولتك أو مدينتك أو عائلتك.
- إحذر من قبول طلبات الإضافة من أشخاص لا تعرفهم.
- إستخدم خاصية الحجب لمنع الأشخاص غير المرغوب بهم من الإتصال بك.
- لا تستخدم خاصية "الدخول التلقائي" خصوصاً إذا كنت تستخدم جهازاً عاماً.
- تأكد دائماً من استخدام النسخة الأحدث من برنامج المحادثة الفورية.

هل جهازك مصاب ببرمجيات خبيثة ؟



مؤشرات تدل على إصابة جهازك ببرمجية خبيثة :

1. بطء ملحوظ في أداء الجهاز مقارنة بالوضع الطبيعي.
2. التوقف عن الإستجابة بشكل متكرر (مثل جمود الشاشة أو مؤشر الفأرة).
3. إعادة التشغيل تلقائياً دون تدخلك.
4. البرامج والتطبيقات المثبتة على جهازك لا تعمل بشكل صحيح.
5. عدم القدرة على الوصول إلى الأقراص الصلبة أو ذاكرة الفلاش.
6. ظهور رسائل غير متوقعة من حين إلى آخر.
7. ظهور القوائم ومربعات الحوار بشكل مشوه وغير منتظم.
8. ظهور رسائل تحذيرية بعدم توفر مساحة كافية للتخزين على خلاف الواقع.

احذر من استخدام شبكات WiFi العامة

تتوفر شبكات الواي فاي العامة والمجانية في كل مكان تقريباً، حيث تستطيع الاتصال بالإنترنت من المقاهي والمطاعم والفنادق وغيرها.

وفي الأغلب لا تحتاج حتى إلى كلمة مرور للاتصال بالإنترنت، ورغم أنه أمر رائع إلا أنه للأسف يستغله المجرمون الإلكترونيون.

وبسبب ذلك فإن أفضل نصيحة هي تجنب استخدام شبكات الواي فاي العامة مطلقاً.

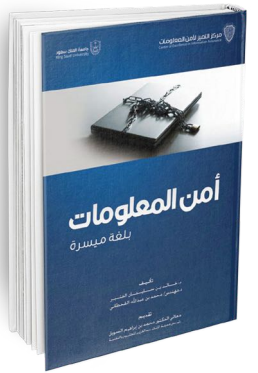
لذا جمعنا لكم مجموعة من النصائح للحماية من تهديدات استخدام شبكات الواي فاي العامة:

- لا تثق أبداً بشبكات الواي فاي المفتوحة التي لا تطلب كلمة مرور.
- عند اضطرارك لاستخدام شبكة عامة، فاستخدمها فقط لإحتياجاتك الأساسية، فلا تفتح حسابك المصرفي أو أي خدمة أخرى مهمة.
- تأكد من شبكة الواي فاي العامة ليست شبكة وهمية تابعة للمخترقين.
- ضع بعين الإعتبار استخدام الشبكة الخاصة الإفتراضية (VPN) لتشفير وحماية بياناتك، واحذر من استخدام هذه التقنية لأعمال غير مشروعة حيث سيعرضك ذلك لعقوبات نظام مكافحة جرائم المعلوماتية.
- ثبت برنامج أمنياً موثوقاً على جهازك حيث يتم تحذيرك عندما تتصل بشبكة غير موثوقة ولا يسمح بتسريب معلوماتك الحساسة إلى المجرمين الإلكترونيين.
- أغلق خاصية الواي فاي في جهازك عندما لا تستخدمها، حيث سيساعد ذلك في حماية بياناتك كما يوفر من شحن بطارية الجهاز.
- تأكد من استخدام خاصية نسيان الشبكة وأن جهازك ليس معد للإتصال تلقائياً بأي شبكة واي فاي غير معروفة، حيث سيحميك هذا الإجراء من مخاطر عديدة، أيضاً من وسائل التعقب التي تستخدمها منظمات مختلفة.

إليك مجموعة من الكتب التي تقدم شرح مبسط للمفاهيم الأساسية لأمن المعلومات، وبيان الأسباب الرئيسية وراء الحاجة الملحة لهذا العلم .

هل يمكن لقرصان التسلل بسهولة إلى نظام معلومات مصرف ما؟ هل من الخطر ترك رقم بطاقة ائتمان على موقع في شبكة الانترنت؟ كيف يمكن التأكد من أن أحداً لن يتمكن من قراءة وثيقة سرية محفوظة على حاسوب؟ ماهي التدابير القانونية في حال وقوع مشكلة ما؟ كلما تزود مجتمعنا بالحواسيب الآلية ووسائل الإتصال الرقمي، تنامت أهمية مسألة أمن المعلومات. يُطلع هذا الكتاب القارئ على المخاطر التي ينطوي عليها استعمال الحاسوب، مقوماً التكاليف المترتبة على الأخطار المعلوماتية، ومسلطاً الضوء على الإطار القانوني الراهن في مجال أمن المعلومات، وعارضاً وسائل الحماية التقنية المتوافرة اليوم والمتوقعة في آفاق المستقبل.

هذا الكتاب أراد مؤلفه أن يكون مرجعاً رئيسياً لأمن المعلومات، يستهدف المبتدئين والمتخصصين؛ فيجد المبتدئ فيه ما يساعده على البدء في دراسة أمن المعلومات، ويجد المتخصص فيه ما يشرح له أساس ومفاهيم وموضوعات أمن المعلومات، وعلاقتها ببعضها بعضاً ليتسنى له البحث فيها وتطويرها.
يحوي هذا الكتاب بين دفّتيه عشرة فصول، تغطي علم أمن المعلومات من عشرة جوانب...



هذا الكتاب يهدف إلى نشر الوعي بأهمية أمن المعلومات بلغة مبسطة، مع تقديم الحد الأدنى من المعلومات المفيدة لكل مستخدم عن أمن المعلومات. كما يقدم الكتاب أمثلة واقعية وموثقة تعطي القارئ تصوراً عن الموضوع بعيدا عن التهويل. كما يخاطب الكتاب شرائح مختلفة من المجتمع بسبب سعة المواضيع، وتدرج الطرح من التبسط إلى التعمق، حتى يجد معظم القراء بغيتهم.

هذا الكتاب أراد مؤلفه أن يكون مرجعاً رئيسياً لأمن المعلومات، يستهدف المبتدئين والمتخصصين؛ فيجد المبتدئ فيه ما يساعده على البدء في دراسة أمن المعلومات، ويجد المتخصص فيه ما يشرح له أساس ومفاهيم وموضوعات أمن المعلومات، وعلاقتها ببعضها بعضاً ليتسنى له البحث فيها وتطويرها.
يحوي هذا الكتاب بين دفّتيه عشرة فصول، تغطي علم أمن المعلومات من عشرة جوانب...

أمن المعلومات
Information Security

الإصدار الأول (2017 - 2018)

infosec.kku.edu.sa