أمن المعلومات والأمن السيبراني

شعبة الموقع الإلكتروني
رئاسة جامعة بغداد

عرض توعوي وسياسات وإجراءات عملية

لماذا التدريب على الوعي الأمني مهم

- الاعتماد المتزايد على الإنترنت يرفع مخاطر الهجمات
- حماية سرية البيانات وسلامتها وتوافرها
- ارتفاع الحوادث السيبرانية يستدعي ممارسات آمنة
- الوعي والتدريب يقللان فرص الاختراق

الأمان السيبراني هو مسؤولية مشتركة للجميع

تعريف الأمن السيبراني

مجموعة ممارسات وتقنيات لحماية الأنظمة والشبكات والأجهزة والبرمجيات والبيانات من الوصول أو الاستخدام أو التعديل غير المصرّح به أو التدمير.

مقولة مشهورة في الأمن السيبراني

"

"لتكون بأمان تام، يجب أن تكون غير متصل بالإنترنت"

To be 100% secure, you need to be offline

هذه المقولة تعبر عن أن أي جهاز متصل بالإنترنت معرض لتهديدات أمنية بشكل أو بآخر، وأن الأمان الكامل لا يمكن تحقيقه إلا بفصل الاتصال بالشبكات، وهذا نادرًا ما يكون عمليًا في الحياة الحديثة.

الاستخدام المقبول لموارد تكنولوجيا المعلومات

الهدف: حماية المستخدمين والجامعة من المخاطر القانونية والتقنية عبر تحديد الاستخدام المهني والمسؤول للموارد.

الإجراءات الأساسية

- استخدام الموارد لأغراض العمل فقط وبطريقة خاضعة للمساءلة
- استخدام برمجيات مرخّصة قانونياً
- الالتزام بضوابط المهام الموكلة

الإجراءات الأساسية

- حماية المعلومات التي تصل إليها حساباتك الجامعية
- الكشف غير المصرّح/الفقد/الإبلاغ الفوري عن السرقة
- فريق الاستجابة/تبليغ نقاط الضعف والحوادث لعضو الارتباط

الإجراءات الأساسية

- عدم الوصول لبيانات دون تصريح مكتوب
- عدم نسخ البيانات السرية إلى وسائط متنقلة إلا بموافقات أصولية
- استخدام البريد الجامعي للأغراض العلمية فقط
- إنشاء كلمة مرور قوية وعدم مشاركة الموارد لأغراض ترفيهية

أمان الأجهزة والحواسيب

الهدف: توفير بيئة حوسبة آمنة لكل أجهزة الجامعة ومستخدميها عبر ضوابط استخدام وصيانة وحماية متسقة.

الحماية الشخصية والممتلكات

- إغلاق الجهاز عند المغادرة وإيقافه بنهاية اليوم
- تجنّب المواقع والبرامج المشبوهة
- التأكد من HTTPS عند إدخال معلومات حساسة
- تفعيل كلمة مرور للجهاز وفحص الوسائط قبل الاستخدام

الفايروسات وبرامج الحماية

- فريق تقنية المعلومات يدير وينشر مضادات الفيروسات
- أبلغ فوراً عن أي نشاط مريب
- يُمنع تعطيل الحماية
- عند الإصابة :افصل الجهاز وامسح التهديدات بمساندة الفريق

الحماية المستمرة هي أفضل دفاع ضد التهديدات الإلكترونية

أمان البريد الالكتروني

الهدف: تحديد أفضل الممارسات لاستخدام نظام البريد الإلكتروني والتأكد من أن المستخدمين على دراية بالاستخدامات المقبولة وغير المقبولة لنظام البريد الإلكتروني الخاص بهم من الناحية الأمنية، وتسليط الضوء على الحد الأدنى من متطلبات الاستخدام الآمن للبريد الإلكتروني

أفضل الممارسات -البريد الإلكتروني

- تجنب النقر على الروابط أو فتح الملفات من مصادر مجهولة أو مشبوهة
- افحص المرفقات ببرامج الحماية
- تأكد من فحص جميع المرفقات قبل فتحها باستخدام برامج مكافحة الفيروسات

البريد الإلكتروني هو من أكثر الوسائل المستخدمة للهجمات السيبرانية - كن حذراً دائماً

سؤال: عادة عندما تقوم بالدخول الى حسابك في نظام معين، سيتوجب ذلك كتابة كلمة المرور، وعنما تقوم بكتابتها تظهر بشكل رمز النجمة عادة(*)، فلماذا تتوقع سبب هذا الاجراء بدلا من ضهور كلمة المرور؟

- للتأكد من كونك صاحب الحساب الحقيقي
- للتأكد من صعوبة كلمة المرور
- لمنع إطلاع الاشخاص الذين بقربك على كلمة المرور
- لمنع صاحب الحساب من تغيير كلمة المرور

كلمات المرور

الهدف: منع الدخول غير المشروع بوضع معايير قوية للاختيار والحماية والتغيير الدوري، حيث تصنف كلمات المرور على انها معلومات سرية.

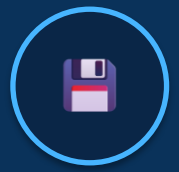
اختيار كلمات المرور القوية

- ألا تكون سهلة التخمين (أسماء/تواريخ/تسلسلات)
- مزيج من أحرف وأرقام ورموز
- طول كافٍ وفق النظام
- تغييرها بشكل دوري وعدم إعادة الاستخدام عبر الأنظمة المختلفة

مقترحات لكلمات المرور

استخدام مولّد كلمات المرور في Chrome/Google

ينشئ كلمات مرور عشوائية قوية ويحفظها تلقائياً



تفعيل التعبئة التلقائية بأمان مع إشعارات الاختراق

تنبيهات فورية عند تسريب كلمات المرور مع اقتراحات للتغيير

الاعتماد على مدير كلمات المرور للتخزين الآمن

تخزين مشفر ومزامنة بين الأجهزة وإدارة سهلة

استخدم كلمة مرور فريدة لكل حساب ولا تكررها أبداً

حوادث أمن المعلومات

الهدف: إدارة مهنية للحوادث لتقليل الضرر على المستخدمين والأنظمة والبيانات

أنواع حوادث أمن البيانات

- محاولات الوصول غير المصرح بها الناجحة
- تغييرات الأنظمة غير المصرح بها
- استخدام غير المصرح به للموارد
- ظروف غير متوقعة
- فقدان المعلومات والمعدات أو سرقتها
- الأخطاء البشرية
- الحرمان من الخدمة
- هجمات الخصم

التحديد الدقيق لنوع الحادث يساعد في تطبيق إجراءات الاستجابة المناسبة

تصنيف البيانات والمعلومات

التصنيف

- **البيانات العامة**

المعلومات التي يمكن تقديمها للعامة أو المخصصة للاستخدام العام دون أن يكون لها أي تأثير سلبي

- **البيانات المحدودة**

معلومات ذات طبيعة أكثر حساسية للجامعة وتتطلب وصول محدود

- **البيانات السرية**

معلومات تسبب ضرراً كبيراً إذا تم انتهاكها أو الكشف عنها

مستوى الوصول

- **عامة**

متاحة للجميع بلا قيود، ولا تسبب ضرراً في حال إعلانها

- **محدودة**

للموظفين الذين يحتاجون إليها كجزء من أدوارهم داخل الجامعة

- **سرية**

وصول مقيّد للغاية ومحدود بأشخاص معينين فقط

التصنيف المناسب للبيانات يساعد في تطبيق إجراءات الحماية المناسبة وتقليل مخاطر الوصول غير المصرح به

الإجراءات عند حدوث الحوادث

- أبلغ عضو الارتباط/فريق الاستجابة فوراً
- يحدد الفريق إجراءات الاستجابة بعد الموافقات
- ساعد في التحقيق ووفّر التفاصيل اللازمة
- الحفاظ على السرية وإبلاغ المعنيين فقط

الاستجابة السريعة للحوادث تقلل الضرر على الأنظمة والبيانات

تعزيز أمان حسابك على Google

الهدف: استخدام أدوات Google لدعم الأمان مثل فحص الأمان، تنبيهات النشاط غير المعتاد، المصادقة الثنائية، مدير كلمات المرور.

أداة فحص الأمان

- مراجعة الأجهزة المتصلة وطرق الاسترداد
- فحص كلمات المرور الضعيفة/المخترَقة
- مراجعة التطبيقات الموصولة
- توصيات تحسينية فورية

تفقد أداة فحص الأمان من Google بشكل دوري للحفاظ على أعلى مستويات الحماية

التحقق بخطوتين

- إضافة عامل ثانٍ لتسجيل الدخول يزيد من أمان حسابك بشكل كبير
- افتح حساب Google ثم الأمان
- اختر التحقق بخطوتين ثم البدء واتبع التعليمات واختر طريقة الرمز/الإشعار
- استخدم إشعارات Google للسماح/الحظر

المصادقة الثنائية تقلل مخاطر الاختراق بنسبة تزيد عن 99%

مدير كلمات المرور من Google

- حفظ ومزامنة كلمات المرور بأمان عبر جميع الأجهزة
- إنشاء كلمات قوية والتعبئة التلقائية للنماذج
- فحص كلمات المرور والتنبيه عند الاختراق أو الضعف
- تقليل الحاجة للحفظ اليدوي لكلمات المرور المعقدة

استخدم مدير كلمات المرور للحصول على تجربة تصفح آمنة ومريحة

البحث عن هاتفي

تحديد الموقع على الخريطة

يمكنك تحديد آخر موقع معروف للهاتف الضائع بدقة على خرائط Google

قفل الجهاز برسالة ورقم تواصل

إغلاق الهاتف عن بُعد مع إظهار رسالة وطريقة الاتصال بك لمن يجده

مسح البيانات عن بُعد عند الضرورة

في حالات الفقدان النهائي، يمكنك مسح جميع البيانات الشخصية من الجهاز لحماية خصوصيتك

لتفعيل هذه الخدمة، تأكد من تسجيل الدخول إلى حساب Google على جهازك وتفعيل خدمة "البحث عن هاتفي" مسبقاً

الحسابات والمزامنة مع المتصفح

الهدف: تنظيم وتخصيص تجارب التصفح بشكل أفضل للحسابات

الحسابات والمزامنة مع المتصفح

ملفات تعريف كروم

- فصل العمل عن الشخصي
- سياسات وإضافات مخصصة لكل ملف
- إدارة مختلفة للإشارات المرجعية والتاريخ
- سهولة التبديل بين الحسابات المختلفة

الفوائد

- مزامنة كلمات المرور والمفضلات
- استرجاع البيانات بعد الفقد
- تسجيل دخول أسرع لخدمات Google
- نقل البيانات بسهولة بين الأجهزة

يساعدك الاستخدام المنظّم للحسابات وميزة المزامنة في تحسين الإنتاجية وزيادة مستوى الأمان

تذكير :الأمان السيبراني مسؤولية مشتركة تبدأ بك

شكرًا لحسن استماعكم

للمزيد من المعلومات، يرجى زيارة منصة جامعة بغداد للتدريب الإلكتروني ووثيقة سياسات استخدام الأنظمة والخدمات الالكترونية

منصة جامعة بغداد للتدريب الإلكتروني

وثيقة سياسات استخدام الأنظمة والخدمات الالكترونية

رابط ورشة العمل