نصائح عامة لتعزيز أمن المعلومات لمستخدمي الحاسب الآلي

General Tips to Enhance Information Security

عمادة تقنية المعلومات والإتصالات

Deanship of Information and Communication Technology

جامعة نجران
NAJRAN UNIVERSITY

مرحبا بكم في النشرة الأولى لأمن المعلومات!
هدفنا هو اطلاعكم على الطرق المناسبة لمعالجة المعلومات بجميع أشكالها , الالكترونية وغير ذلك.

أنت مستهدف

تشكل معلوماتك الشخصية وجهاز الكمبيوتر الخاص بك صيدا ثمينا للمجرمين الذين يعملون على الانترنت وغيرهم من الفضوليين. وقد أظهرت الإحصاءات أن البشر هم الحلقة الأضعف في تأمين المعلومات. لذلك، سيحاول مجرمو الإنترنت الإيقاع بك لاتخاذ الإجراءات التي من شأنها أن تفتح أمامهم الأبواب. فهم يستهدفونك من أجل:

- الوصول إلى معلومات مالية أو غيرها من المعلومات الحساسة
- استخدام جهاز الكمبيوتر الخاص بك لمهاجمة أنظمة حاسوبية أخرى
- سرقة هويتك
- الإضرار بسمعتك
- اكتساب ميزة تنافسية (عن طريق سرقة الأبحاث)

التكنولوجيا وحدها ليست كافية لتأمين المعلومات. قد يكون لديك معلومات حساسة ملقاة على مكتبك أو تجري مناقشتها في الغرفة المجاورة. ضع في الاعتبار أن تسرب المعلومات غالبا يبدأ من داخل المؤسسة وليس من المهاجمين على شبكة الإنترنت. اتبع مبادئ توجيهية بسيطة بديهية، وسوف تساعدنا على إبقاء جميع المعلومات التي لدينا آمنة.

مبادئ بديهية وبسيطة

- لا تكشف عن أي معلومات شخصية أو سرية ما لم يكن ذلك ضروريا للغاية وإلى الطرف المناسب
- لا تترك معلومات حساسة متناثرة في مكان عملك
- لا تثبت تطبيقات غير مصرح بها أو غير مرخصة
- اقفل جهازك دائما قبل تركه
- تأكد دائما أن برامج مكافحة البرامج الضارة مثبتة بنظام التشغيل
- تحقق دائما قبل السماح بوصول شخص إلى منطقة عمل حيث تتم معالجة معلومات حساسة.

كلمات السر: مفاتيح مملكتك

اجعل كلمة السر كإبرة في كومة قش يصعب على القراصنة العثور عليها.

اتبع هذه الإرشادات عند اختيار واستخدام كلمات السر الخاصة بك:

- لا تستخدم كلمات السر التي يسهل تخمينها
- استخدم كلمات سر صعبة وسهلة التذكر. كلمات السر الصعبة تحتوي حروف علوية وسفلية الحالة بالإضافة إلى أرقام ورموز أخرى
- لا تشارك كلمة السر الخاصة بك مع أي شخص، حتى المشرف أو أفضل صديق
- لا تستخدم نفس كلمة السر للعمل والحسابات الشخصية
- لا تكتب كلمة السر الخاصة بك وتتركها حيث يمكن للآخرين العثور عليها
- لا تستخدم جهاز كمبيوتر عام لتسجيل الدخول إلى مواقع ذات معلومات حساسة (مثل البنك)

البريد الإلكتروني، «التصيد»، والهندسةالاجتماعية

إذا تلقيت رسالة بريد إلكتروني تطلب منك النقر على رابط أو إرسال معلومات شخصية عن طريق البريد الإلكتروني، فهذه على الأرجح محاولة خادعة تهدف إلى الحصول على معلومات شخصية. ويسمى هذا النوع من الهجوم "تصيد". موظفو الدعم التقني لا يطلبون هذه المعلومات عن طريق البريد الإلكتروني. الرجاء الإبلاغ عن مثل هذه الطلبات. استخدم الحس السليم: إذا كان البريد الإلكتروني يبدو غريبا أو مختلفا عن النمط العام، فإنه على الأرجح محاولة خبيثة للوصول إلى المعلومات الخاصة بك وبحساباتك.

- لا تضغط على الروابط التي تتلقاها في رسائل البريد الإلكتروني إلا إذا كنت متأكدا تماما من أنها آمنة.
- لا تستجب لرسائل البريد الإلكتروني أو المكالمات الهاتفية التي تطلب معلومات شخصية أو سرية قبل التحقق من هوية الطالب والغرض الذي من أجله يطلبونها.
- لا ترسل معلومات سرية عن العمل عن طريق البريد الإلكتروني دون الحصول على إذن مناسب.
- لا ترسل المعلومات السرية إلى حسابات البريد الإلكتروني الشخصية مثل Gmail أو Yahoo!

سلامة الشبكات الاجتماعية

تكشف الشبكات الاجتماعية المعلومات الشخصية الخاصة بك إذا لم تكن حذرا، يمكن أن تكشف المعلومات التي تسعى إلى المحافظةعليها.

- القاعدة الذهبية رقم ١: إذا كنت لا تريد العالم أن يراه، فلا تنشره!
- القاعدة الذهبية رقم ٢: لا تسمح للآخرين بكسر القاعدة الأولى بالنسبة لك. لا تشاركهم ما لا تريد للعالم أن يراه!
- إذا كنت في مركز وظيفي مرموق، فأنت هدف رئيسي للمهاجمين. اتبع القاعدتين رقم ١ ورقم ٢ بكل حرص وانتباه.
- لا تستخدم نفس كلمة السر لحسابات البنك الذي تتعامل معه أو العمل والحسابات الشخصية.
- فكر قبل أن تنشر! ليس هناك ضمان للخصوصية على شبكة الإنترنت.
- تحكم بإعدادات الخصوصية على الموقع الخاص بك في الشبكات الاجتماعية.
- كن حذرا من طلبات صداقات جديدة ". هل هم حقا من يزعمون؟
- كن مشككا في كل ما يصل إليك أو يطلب منك، مثلا:
  - لا تضغط على الروابط المنشورة على صفحات الفيسبوك
  - احترس عند تثبيت تطبيقات من أطراف أخرى

اتصل بنا

- إذا كنت غير متأكد من أنه تم تثبيت برامج مكافحة البرامج الضارة في جهاز الكمبيوتر الخاص بك في العمل وأنها تعمل بشكل صحيح؛
- إذا كنت تعتقد أن معلومات حساسة تعرضت للتسريب؛
- إذا كنت غير متأكد من سلامة رسالة تلقيتها؛
- إذا كنت تعتقد أنه تم انتهاك خصوصية جهاز الكمبيوتر الخاص بك أو اختراقه؛
- إذا تلقيت رسالة جيدة الصياغة من أي شخص في جامعة قطر تطلب منك معلومات شخصية بما في ذلك كلمات مرور حسابك والحسابات المصرفية وما إلى ذلك؛
- إذا كان لديك أسئلة أخرى تتعلق بحماية المعلومات؛

يرجى الاتصال بمكتب المساعدة

من خلال الهاتف 017542-2000

أو عن طريق البريد الإلكتروني: helpdesk@nu.edu.sa