سلامة
SALAMA
شركة سلامة للتأمين التعاوني
Salama Cooperative Insurance Company

إدارة الأمن
السيبراني

تعاريف الأسبوع

الإخوة/الزملاء

١. البرامج الضارة – أي جزء من البرامج تم كتابته بقصد الإضرار بالبيانات أو الأجهزة أو الأشخاص

٢. أحصنة طروادة – وهي برامج خبيثة تتنكر على أنها برمجيات شرعية. "يعمل بشكل مستقل ويخلق الخلفية في أمانك للسماح لبرامج ضارة أخرى بالدخول"

٣. فيروس الإعلانات – برنامج يقوم بعرض أو تنزيل المواد الإعلانية تلقائيًا مثل إعلانات بانر أو النوافذ المنبثقة عندما يكون المستخدم متصلاً بالإنترنت

٤. الرسائل غير المرغوب فيها – الرسائل غير المرغوب فيها التي يتم إرسالها عبر الإنترنت ، عادةً إلى عدد كبير من المستخدمين ، لأغراض الإعلان والتصيد الاحتيالي ونشر البرامج الضارة

٥. فيروس الفدية – هذه الغاية من البرامج الخبيثة هي اختطاف الملفات التي تشفرها ، وتتطلب المال من الضحية مقابل مفتاح فك التشفير

SALAMTEQ
Cybersecurity Dept.

سلامة
SALAMA
شركة سلامة للتأمين التعاوني
Salama Cooperative Insurance Company

إدارة الأمن
السيبراني

نصائح لأمان الهاتف المحمول

الإخوة/الزملاء

١. استخدم كلمة مرور قوية. تجنب استخدام الأفكار الشائعة لكلمات المرور ، مثل تاريخ الميلاد ، اسمك الاول او الاخير. بدلاً من ذلك ، قم بإنشاء كلمة مرور عشوائية ولكن يمكن تذكرها.

٢. لا تثق في الرسائل التي تحاول إقناعك بالكشف عن أي معلومات شخصية. تعامل مع الرسائل بالطريقة نفسها التي تتعامل بها مع البريد الإلكتروني ، فكر دائمًا قبل الضغط على أي رابط! (التصيّد عبر الرسائل النصية القصيرة).

٣. استخدم فقط التطبيقات المتاحة في المتجر الرسمي لجهازك – لا تقم بتنزيل التطبيقات من المتصفح. كن حذرا من التطبيقات من مطورين غير معروفين أو من لديهم تقييمات محدودة / سيئة. احرص على تحديث التطبيقات دائما من اجل تحسين مستوى الأمان.

٤. كن حذرا من أي روابط تتلقاها في وسائل التواصل الإجتماعية. يمكن استخدامها لتثبيت البرامج الضارة على جهازك المحمول من أجل سرقة المعلومات الشخصية.

٥. احرص دائمًا على استخدام المواقع الإلكترونية (https) أثناء إجراء المعاملات المالية عبر الإنترنت. توفر هذه المواقع اتصالًا آمنًا يضمن عدم اطلاع اي طرف خارجي على المعلومات التي تدخلها في هذه المواقع.

٦. عام أو غير معروف ، خصوصا عند العمل Wi-Fi لا تستخدم اتصال إنترنت على بيانات حساسة ومهمة في هاتفك. حتى الشخص الذي ليس لديه خبرة كافية في البرمجة يمكنه اختراق الكمبيوتر اللوحي أو الهاتف بسهولة وسرقة المعلومات منه.

٧. لا تنقر على الروابط التي تتلقاها عبر البريد الإلكتروني – حتى وان كان الشخص المرسل من جهة موثوقة. يمكن للمخترقين إنشاء شعارات ومواقع ويب مشابهة للشركات المعروفة – وبالتالي ، يمكنهم جذب المستخدمين لمشاركة كلمات المرور الخاصة بهم عن غير قصد.

٨. قم بتحديث نظام تشغيل هاتفك المحمول. أحدث إصدار من نظام التشغيل هو الأكثر حماية

SALAMTEQ
Cybersecurity Dept.

salamacic
www.salama.com.sa/

فيروس الفدية

إدارة الأمن
السيبراني

الإخوة/الزملاء

فيروس الفدية: هو برنامج ضار يمنع المستخدم من الوصول الى النظام بتشفير جميع البيانات المخزنة بجهاز الكمبيوتر، تابلت او الجوال.

اول هجمة كانت عام ١٩٨٩ م , من اقوى الهجمات التي هددت WannaCry شركات عالمية منها سكايب وذلك في عام م٢٠١٧

انواع هجمات فيروس الفدية:

(WannaCry) يهدد اجهزة الويندوز ويقوم بتشفير بياناتك وملفاتك

(KillDisk) يقوم الفايروس بحذف كل المعلومات المجودة على جهاز الضحية

(Locky) يكون الفيروس مخبأ داخل ملف مايكروسوفت ورد وعندتفعيله يقوم بتشفير بيانات جهازك

كيف تحمي نفسك:

- قم بنسخ احتياطي لجميع المعلومات بجهازك بشكل دوري
- احذف الايميلات المشبوهة
- نشر الوعي بين الزملاء

SALAMTEQ
Cybersecurity Dept.

salamacic
www.salama.com.sa/

سلامة
SALAMA
شركة سلامة للتأمين التعاوني
Salama Cooperative Insurance Company

إدارة الأمن
السيبراني

الهندسة الاجتماعية

الإخوة/الزملاء

استخدام الخداع للتلاعب بالأفراد للكشف عن معلومات غاية بالسرية التي من الممكن ان تسخدم في عمليات الأحتيال.

هجمات الهندسة الاجتماعية الشائعة:

شخصيا: استخدام المهارات الشخصية لجمع المعلومات

-مقابلة الضحية
-التحدث للضحيه عبر الهاتف
-مراقبة الضحية من حيث الشخصيه والتصرفات

رقمي:استخدام التكنولوجيا لجمع المعلومات

-ايميل او رسالة وسائط
-إعلانات مزيفة
-مواقع مزيفة لماركات عالمية

معلومات تعرفها وسائل التواصل الاجتماعي عنك:

الأسم
اللقب
رقم الجوال
الإيميل
صور
فيديو
معلومات الموقع
تاريخ الميلاد
معلومات حساب البنك
عنوان المراسلات
ضبط الأجهزة
معلومات ضبط الجهاز

ما الذي يمكن أن تستخدم فيه هذه المعلومات:

-سرقة الهوية
-تخمين كلمة المرور
-سرقة المال

SALAMTEQ
Cybersecurity Dept.

salamacic
www.salama.com.sa/