وَعي

خطوتك الاولى نحو الامان الرقمي

dPhish

نبذة عن الشركة

شركة دي فيش – dPhish هي شركة عربية تأسست في عام ٢٠٢٢، وتعمل في عدد من الدول العربية والأجنبية لتقديم خدمات اكتشاف التصيّد للشركات ورفع الوعي الأمني لموظفيها. تهدف شركة دي فيش إلى أن تكون أول شركة عربية في مجالها تستطيع التواجد بقوة في الأسواق العربية والأجنبية من خلال توفير عدد من المميزات التي تجعل حلولها فريدة ومتميزة عن منافسيها.

نبذة عن الكُتيب

بناءً على إيماننا بأهمية نشر الوعي الأمني السيبراني في المجتمع وتأثيره على حياة الأفراد، جاءت فكرة هذا الكتيب ليكون دليلاً توجيهياً مجانياً يهدف إلى رفع الوعي الأمني السيبراني في كل منزل، حيث يُمكن لجميع أفراد الأسرة قراءته. هذه مساهمة اجتماعية منا في مجتمع نفتخر بأننا جزء منه.

سيتضمن هذا الكتيب عدة نسخ تتناول مواضيع متنوعة في مجال أمان المعلومات التي تهم الأشخاص غير المتخصصين، بهدف أن يكون دليلهم نحو تصفح آمن على الإنترنت. نتمنى أن يحظى هذا الكتيب بإعجابكم، ونتطلع إلى استقبال تعليقاتكم واقتراحاتكم على موقع شركتنا؛ لنبدأ معكم في رحلة توفير الحماية ضد الاحتيال الإلكتروني.

المحتويات

مقدمة

في هذا الكُتيب نناقش عددا من مواضيع **أمن المعلومات** التي تهمّ كل شخص في عالمنا هذا، ففيه سنعرف ببساطة وبسهولة كيف يُمكن للمُخترقين سرقة بياناتنا وأموالنا واقتحام خصوصيتنا، وسنبيِّن كيفية مواجهة ذلك ومنعه، وكيفية التصدي للخطر الناتج عنه.

في عالم صرنا نتعامل فيه مع هواتفنا وأجهزة الكمبيوتر الخاصة بنا بشكل يومي، أصبح الأشخاص الذين ليس لديهم معلومات تقنية كبيرة في خطرا
فقد انتشر التعرض إلى الاحتيال من كثير من قراصنة الإنترنت في هذه الأيام. فقد تجد نفسك تتساءل من أين تبدأ عندما يتعلق الأمر بحماية بياناتك وخصوصيتك من المخاطر الكامنة في التهديدات السيبرانية ومن مخاطر المتسللين. لذلك سنتناول في هذا الكُتيب مواضيع عدة، مثل: التعاملات البنكية، والشراء من الإنترنت، وكيفية تجنب الاحتيال على مواقع التواصل الاجتماعي، بالإضافة إلى ورود جزء مُخصص لإرشاد الأطفال عن كيفية تعاملهم على الإنترنت لتجنب أي اختراق لخصوصيتهم وبياناتهم.

الاحتيال المالي

عند استخدام **بطاقة الدفع البنكية** الخاصة بك للشراء عبر الإنترنت، ستقوم بإعطاء الموقع بعض البيانات الخاصة، مثل: **الستة عشر رقما** الموجودين على البطاقة، بالإضافة إلى: تاريخ انتهاء البطاقة، واسمك المطبوع عليها، والثلاث أرقام التي في خلف البطاقة.

ولأن هذه البيانات يسهل الوصول إليها، سواء بقراءتها من على بطاقتك، أو بأي طريقة احتيال أخرى، فإن البنوك تقوم بإرسال كلمة السر – التي عادة ما تتكون من **ست أرقام** – في رسالة نصية إلى هاتفك الخاص، وذلك للتأكد من أنك أنت من تحاول القيام بعملية الشراء بشخصك. ولإتمام أي معاملة شراء عبر الانترنت يجب عليك إدخال هذه الأرقام.

وهنا تبدأ محاولة الاحتيال؛ **لذلك فاحذر وتخيل التالي!**

تخيل أنك تلقيت رسالة من البنك الخاص بك تحتوى على **الأرقام الستة**، وبعدها بلحظات جاءت مكالمة من شخص ذو صوت يبدو صادق ويُعَرِّف نفسه أنه من البنك الخاص بك أو ما شابه، ويطلب منك تزوديه بالأرقام المُرسلة في الرّسالة النّصية لإتمام أمر عاجل يخصّ حسابك، كمنع حسابك من التعطل أو إيقاف عملية احتيال تتعرض إليها ... وغيرها.

في هذا الموقف يجب عليك عدم مشاركة هذه الأرقام معه ولا مع أي شخص آخر على وجه العموم، لأن ذلك - ببساطة – سيؤدى لسرقة أموالك. وعلى أي الأحوال لن يطلب منك أي مصرف أو جهة مالية رسمية هذا الرقم لأنه لا يحق له ذلك.

"The OTP for the online purchase of card number 5699 is 98617, and it will expire in 10 minutes. Please do not share this code with anyone for any reason."

"كلمة المرور لمرة واحدة لشراء البطاقة رقم 1234 عبر الإنترنت هي 986179. وستنتهي صلاحيتها خلال 10 دقائق. يرجى عدم مشاركة هذا الرمز مع أي شخص لأي سبب من الأسباب."

في حالة أنك واجهت هذا الموقف فعليك التالي:

أبلغ البنك الخاص بك، واطلب منه إيقاف كارت المدفوعات الخاص بك، وقم باستبداله على الفور

قُم بتعديل كلمة مروك حسابك على منصة الانترنت البنكي

قم بمراجعة معاملتك البنكية في الفترة الماضية بحثا عن أي تحويل لا تعرفه قد يكون حدث

الآن، لنري طريقة أخرى من طرق الاحتيال! تخيل وصول هذه الرسالة لك مذكور فيها أنَّ هناك اختراق لحسابك المصرفي ويجب عليك إصلاحه بشكل عاجل عن طريق الضغط على الرابط التالي.

طبيعيا، ستبدأ بالقلق! فأنت تريد حماية أموالك. ولكن لا تتعجل، **ولاحظ معي التالي:**

١

يسهل على المحتالين ارسال رسائل نصية لهاتفك وكأنها من المصرف الخاص بك، وهذا لا يعني اختراقه، فاطمئن

٢

في حالة وصول مثل هذه الرسالة ، يجب عليك الاتصال بالمصرف للتأكد من مدي صدق الرسالة على الفور. وانتبه لعدم التعامل مع الرابط الموجود فيها بأي شكل من الاشكال

٣

المصرف لن يطلب منك أبدا الدخول لرابط لحل مشكلة اختراق في حسابك

“عاجل : تم اختراق أمان حسابك. مطلوب اتخاذ إجراء فوري. انقر على الرابط أدناه للتحقق من هويتك ومنع الوصول غير المصرح به”

الاحتيال عبر مواقع التواصل الاجتماعي

تعد وسائل التواصل الاجتماعي مكانًا يسيرا لممارسة الاحتيال، حيث يمكننا جميعا مشاركة أفضل لحظاتنا، والتواصل مع الأصدقاء والعائلة والضحك معًا، لكن تعلم كيف تسير الأمور. هناك دائمًا **"لكن"!**

تخيل هذا: أنت تقضي يومك فحسب، وتتصفح رسائل الوسائط الاجتماعية الخاصة بك، فجاة تصلك رسالة مثل هذه :

عاجل : مسابقة لفترة محدودة مع فرصة للفوز بجائزة!

يسعدنا أن نعلن عن فرصة حصرية لك! تصرفوا بسرعة، لأن الوقت ينفد للمشاركة في مسابقتنا المثيرة مع فرصة الفوز بجوائز مذهلة، بما في ذلك أحدث الهواتف الذكية! **أبرز مميزات الجائزة:**

-الهواتف الذكية الجديدة - خصومات وعروض حصرية - قسائم هدايا مثيرة

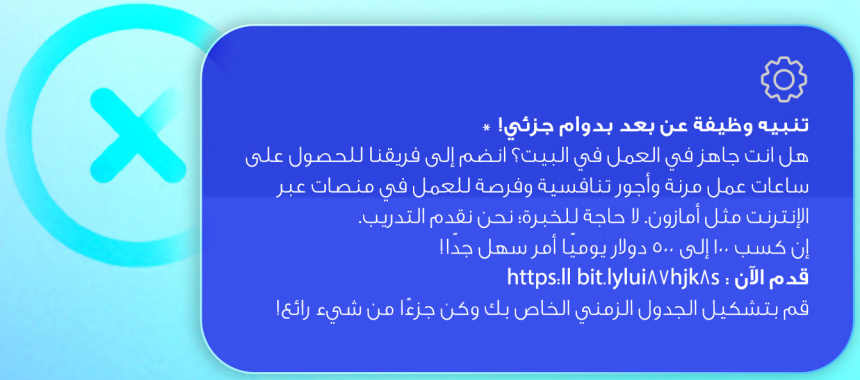
لا تفوت فرصتك في الحصول على هذه المكافآت الرائعة.

هذه المسابقة مفتوحة لفترة محدودة فقط، وقد تؤدي مشاركتك إلى تحقيق مكاسب كبيرة! للدخول وتأمين فرصتك في هذه الجوائز المذهلة، انقر على الرابط أدناه الآن :https:\\bit.ly أسرع، فهذه الفرصة لن تدوم طويلًا! تصرف الآن، وقد تكون الفائز المحظوظ التالي.

تبدو هذه الهدايا جميلة جدًا، أليس كذلك؟ ولكن لنكن واقعيين.

لماذا يقوم شخص ما بالتبرع بمثل هذه الأشياء القيمة مجانًا لأشخاص عشوائيين؟

أولاً وقبل كل شيء، لا ترد على الرسالة أو تتفاعل مع المرسل بأي شكل من الأشكال. تجنب الضغط على أي رابط أو تنزيل أي ملف من الرسالة. فإن فعلت؛ فإن هذا سيؤدي إلى اختراق خصوصيتك و تحميل برمجيات خبيثة على هاتفك او حاسوبك.



ما سبق هو واحد من أشهر طرق الاحتيال المنتشرة عبر مواقع التواصل الاجتماعي، وهناك طرق أخرى كثيرة تشاركه نفس الصفات. رسائل جميلة بشكل غير واقعي، تطلب منك بياناتك أو الضغط على رابط، أو تحميل ملف، أو يقوم باستدراجك لمحادثة أطول ثم يقوم بسرقتك!

هناك أيضا من يستغل رغبتنا في الحصول على وظيفة من المنزل من خلال الانترنت، فهذا شيء رائع لأغلبنا! ولكن – من تجاربنا –أغلب هذه الرسائل مزيفة، فلا ترد عليها إن لم تأتى من شخص موثوق تعرفه جيدا.

احمي نفسك اثناء التسوق عبر الانترنت

يجب أن أعترف أنني من محبي التسوق عبر الإنترنت! فإنه يغيّر قواعد اللعبة في عالمنا سريع الخطى، حيث توفير الراحة بالحصول على ما تحتاجه – فقط – ببضع نقرات!

تخيل أنك تنتظر طردًا، ثم تتلقى بريدًا إلكترونيًا **مثل هذا:**

لقد تغيرت حالة شحنتك :

لقد قمنا بمحاولة تسليم طردك اليوم, ولكن لسوء الحظ, لم تكن متاحًا.
----تفاصيل الشحنة----
الرقم المرجعي: SJFSJFNSLMF
رقم التتبع: GH45OJKLSDN

ونحن نعتذر بصدق عن أي إزعاج تسبب لإعادة جدولة التسليم وتقديم عنوان محدث, يرجى النقر على الرابط التالي:
https:\\bit.ly\dgsf78s

يبدو مألوفا، أليس كذلك؟ لكن - حقيقةً - هذا أحد طرق الاحتيال! وسنتحدث فيما يلي عن بعض طرق التمييز بين البريد الحقيقي والمُزيف:

١ تأكد أنه قادم من اسم الشركة الذي تتوقعه دون أي تغير فإن كنت ستشري من أمازون – مثلا – وجاءك من فيدكس، فهذا احتيال.

٢ إن كنت تشترى من أمازون، وجاءك من أمازون، فتأكد أنها - فعلا– تنتمي لأمازون، وذلك عن طريق قراءة البريد المُرسل بدقة.

٣ إن ضغطت على الرابط، ولاحظت أنه قام بتحميل ملف، فامسحه على الفور، ولا تقم بفتحه. أو لو وجدت أنه يطلب منك اسم المستخدم و كلمة المرور، فلا تقم بإدخالهم.

٤ على أي حال، تستطيع تتبع شحنتك ومعرفة تفاصيلها من خلال فتح حسابك على مواقع الشحن نفسها دون الضغط على أي رابط داخل البريد المُرسل اليك.

اطفالنا أمانة فنوعيهم

اليوم، عندما نتحدث عن هواتفنا الذكية وحياتنا الرقمية، فمن الواضح أنه حتى أطفالنا أصبحوا مرتبطين بحساباتهم على وسائل التواصل الاجتماعي وألعابهم عبر الإنترنت.

لذلك من الضروري التأكد من أن أطفالنا على دراية بقضايا أمن المعلومات والسلامة الرقمية. **وما يلي بعض الارشادات الواجب تعليمهم إياها:**

شجعوهم على إنشاء كلمات سر قوية يصعب تخمينها لحساباتهم

علّموهم أن يتعاملوا مع معلوماتهم الشخصية ككنوز، لا يعطونها لأى أحد عبر الهاتف أو الإنترنت. ومن هذه البيانات: الاسم الكامل، ورقم الهاتف، والعنوان، والمدرسة التي يذهبون إليها، وكلمات السر الخاصة بحاسباتهم.

علّموهم ألّا يتفاعلوا بشكل كبير مع أشخاص لا يعرفونهم بشكل شخصي في الحقيقة عبر الإنترنت.

اجعلوهم مدركين لأهمية تحديثهم للتطبيقات على هواتفهم، فذلك يساعد في حمايتهم، فهناك بعض التحديثات تكون بهدف معالجة ثغرة أمنية في التطبيق.

أكّدوا عليهم ضرورة التحدث لشخص بالغ يعرفونه إن واجهتم أي مشكلة على الانترنت تبدو مريبة.

وأخيرا، الحذر الشديد واجب دائما. فيجب التنبيه على أطفالكم ابلاغكم دائما، والتأكد من موافقتكم قبل مشاركة أي بيانات شخصية على أي منصة عبر الانترنت.