إرشادات لحمايتك من التصيد Phishing

إعداد : محمد المسقطي

Mohammed Al-Maskati

Twitter:@mohdmaskati

المقدمة :

التعريف : هو محاولة الحصول على المعلومات الخاصة بمستخدمي الأنترنت سواء أكانت معلومات شخصية أو مالية، عن طريق الرسائل الإلكترونية أومواقع الأنترنت التي تبدو وكأنها مبعوثة من شركات موثوقة أو مؤسسات مالية وحكومية، كالبنوك و غيرها و هي في الحقيقة مواقع وهمية و زائفة .

العديد من الأشخاص وقعوا ضحايا إلى الهجمات التي تسمى بالتصيد Phishing و مما أدى إلى أن يمنعوا من الوصول إلى حساباتهم و خصوصا على وسائل التواصل الاجتماعي .

ليس الغرض من هذا الدليل الحماية الكاملة بل هو لتقليل المخاطر المتعلقة بأستخدام الأنترنت .

١- كن حذرا من مشاركة المعلومات :

احذر من أي رسالة على البريد الإلكتروني او على وسائل التواصل الاجتماعي او في المحادثات الخاصة تطلب منك مشاركة معلوماتك الخاصة مع أطراف حتى ان كانوا معروفين بالنسبة لك .

جميع المؤسسات و البنوك لن يطلبوا معلوماتك الشخصية أو الحساسة عن طريق رسالة في البريد الالكتروني أو عن طريق اتصال هاتفي أو عن طريق محادثات خاصة .

٢- لا تستجب إلى الضغوط :

يستغل المتطفلين و الأشرار بعض الحيل للضغط عليك من أجل الاستجابة في مشاركة معلوماتك معهم و يستخدمون في ذلك "إستراتيجية التخويف " .

حيث يخبرونك كذبا بأن الحساب سوف يتوقف / يتعطل أو أن لن يتم تفعيل الخدمة حتى تقوم بتحديث معلوماتك الشخصية و الحساسة .

أن هذه الاستراتيجية الغرض منها استغلال خوفك من توقف حسابك أو الخدمة ، لا تشارك معلوماتك معهم و قم بالاتصال بالقائمين على الموقع الإلكتروني أو الخدمة مباشرة للتأكد من صحة هذه الرسالة .

٣- لا تثق في الروابط / الوصلات :

بعض الأحيان يصلك رابط / وصلة تطلب منك الدخول إليها من أجل تسجيل الدخول على الموقع :

الملاحظات :

١- شكل الموقع : هذا هو الشكل الخاص لموقع Facebook و لم يتغير شئ .
٢- الرابط / الوصلة : هذه الوصلة / الرابط ليست تابعة لموقع Facebook .

الوصلة المزيفة / الوهمية : /http://facceboooook.site50.net
الوصلة الحقيقة : /https://www.facebook.com

تذكر : دائما قم بكتابة اسم الموقع بنفسك و لا تنقر على أي رابط / وصلة .

٤- شهادة الأمان Security certificate

تأكد دائما بأن الموقع الإلكتروني الذي قمت بالدخول إليه يحتوي على SSL/TLS و هي شهادات الأمان و التي تقوم بتعمية (تشفير) الاتصال بينك و بين الموقع الإلكتروني الذي انت تستخدمه .

مثال : عندما تدخل على موقع https://twitter.com

سوف يحتوي الموقع على شهادة الأمان و هي حرف (S) بعد البروتوكول HTTP

المزيد : فيديو يشرح عن الشهادة الرقمية / الأمان (اضغط هنا)

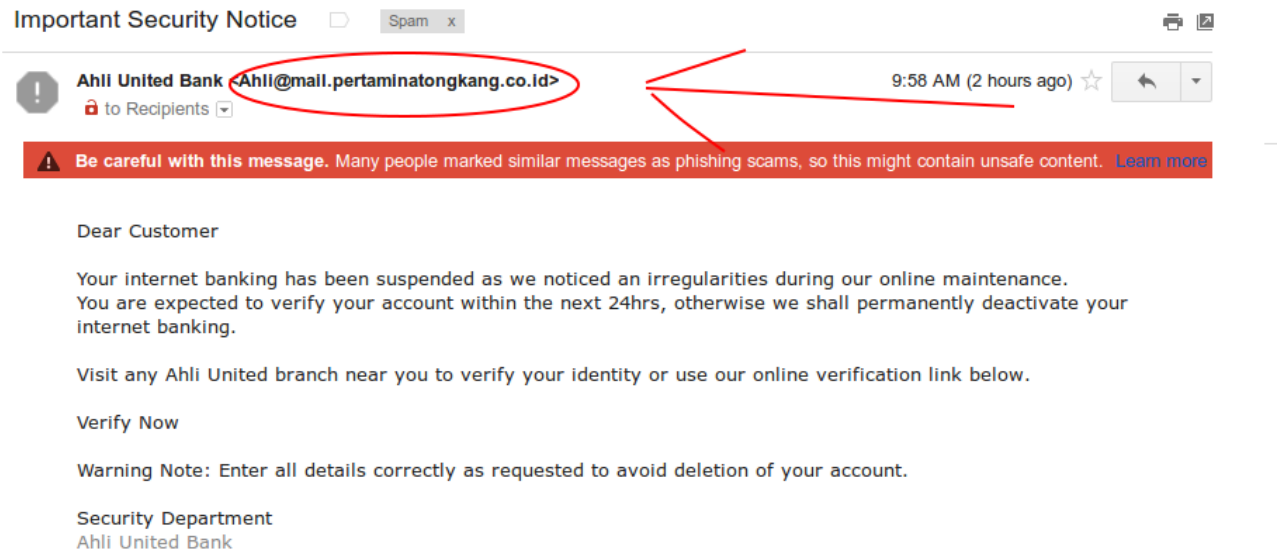
٥- مصدر الرسالة البريدية :

تأكد دائما من مصدر الرسالة ، حيث أن شركة الفيسبوك و غيرها من الشركات لديها عنوانين محدده يتم استخدامها في إرسال الرسائل .

مثال : Info@twitter.com أو security@facebookmail.com

حيث أن الرسائل الوهمية تحاول أن تستخدم عنوانين وهمية

مثال : رسالة وهمية مفترضة من بنك تجاري

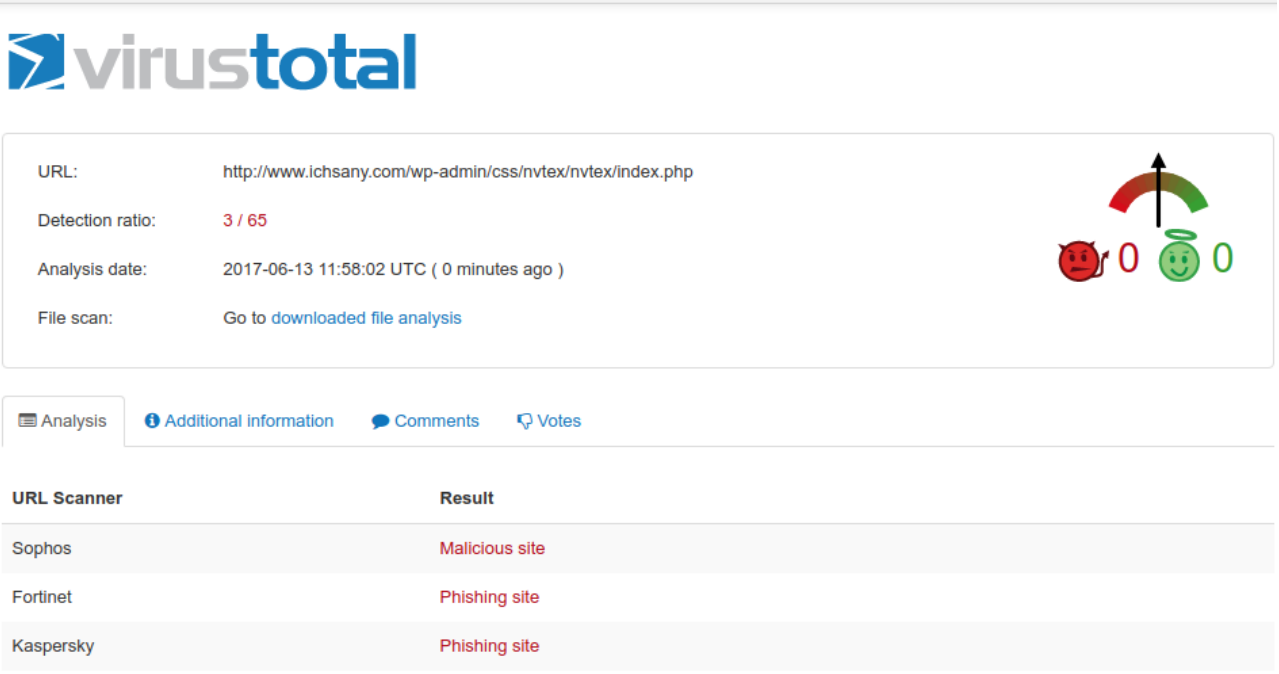


٦- فحص الروابط / الوصلات :

العديد من هذه الروابط / الوصلات تم كشفها مسبقا و بالامكان استخدام موقع Virus total و الذي يحتوي على العديد من التطبيقات المتعلقة بالبرمجيات الخبيثة و غيرها .

الموقع : https://www.virustotal.com/

مثال : http://www.ichsany.com/wp-admin/css/nvtex/nvtex/index.php



إذا ترغب بأستخدام الموقع ، في الصفحة الأولى أنقر على URL و من ثم قم بوضع اسم الرابط/ الوصلة التي ترغب في فحصها .

٧- الخدمة أو الموقع يعلمون بأسمك :

العديد من هذه الرسائل الوهمية / الزائفة يستخدمون كلمة السيد / السيدة أو Dear Customer حيث ان أغلب هذه الرسائل توجه إلى عديد كبير من الضحايا و ليس إلى أشخاص محددين .

إذا كنت مستهدف ، سوف توجه لك رسالة خاصة بأسمك و أن الأشخاص الذين استهدفوك لديهم معلومات كافية عنك .

Dear Customer

Your internet banking has been suspended as we noticed an irregularities during our online maintenance.
You are expected to verify your account within the next 24hrs, otherwise we shall permanently deactivate your internet banking.

Visit any Ahli United branch near you to verify your identity or use our online verification link below.

Verify Now

Warning Note: Enter all details correctly as requested to avoid deletion of your account.

٨- انتحال الشخصية :

قد تكون هذه الرسائل تم إرسالها عن طريق بريد إلكتروني معروف لديك (صديقك ، مديرك في العمل ، زوجتك و غيرهم) و لكن بعض الأحيان يتم استخدام طريقة انتحال الشخصية و هي طريقة عن طريقها تم استغلال بريد إلكتروني لأشخاص انت تعرفهم من اجل التواصل معك .

إذا تم طلب معلومات حساسة أو شخصية أو غيرها ، قبل إرسالها تأكد بأن الشخص الذي اتصل بك لم يتم اختراق بريده الإلكتروني أو لم يتم انتحال شخصيته .

٩- أبقي جهازك محمي :

ان البرمجيات الخبيثة Malware قد تؤدي وظائف عديدة في جهازك و منها تدمير الجهاز او سرقة المعلومات او الربح المالي أو التحكم بالجهاز عن بعد .

ان العديد من المستخدمين لا يقومون بـ تثبيت / تنصيب تحارب هذه البرمجيات الخبيثة و أيضا العديد من المستخدمين يستخدمون تطبيقات غير مجانية أو غير آمنة أو تم كسر حمايتها بأستخدام الكراك Crack .

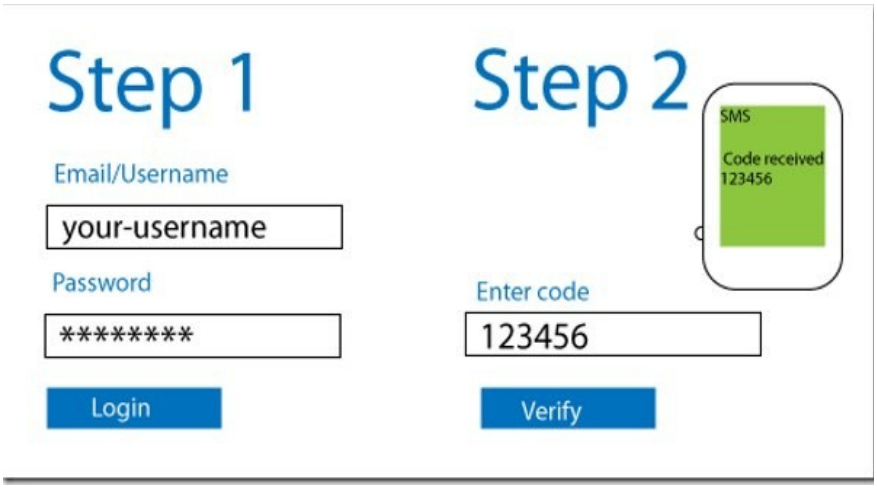
أن استخدام تطبيقات / برمجيات لم يتم تفعليها بشكل صحيح لن يساهم في تأدية الوظيفة التي من أجلها تم تثبيت / تنصيب هذا التطبيق من أجله و هي "مكافحة البرمجيات الخبيثة " .

ننصح بأستخدام التطبيقات/ البرمجيات المجانية التي تكافح الفيروسات التالية :

- أفاست Avast (اضغط هنا)

-أفيرا Avira (اضغط هنا)

لا يجب تثبيت / تنصيب أكثر من تطبيق مع بعض لان سوف يؤدي إلى تضرر الجهاز ، و لكن بالامكان تثبيت / تنصيب هذا التطبيق مع البرمجيات في الاعلى من دون ان يتضرر جهازك – Malwarebytes



١٠ – تفعل خاصية "التحقق بخطوتين "

تأكد دائما أن تقوم بتفعيل خاصية " التحقق بخطوتين " Two Step Verification و حيث ان هذه الخاصية سوف تمنع الاستيلاء على حسابك حتى إذا انكشفت كلمة السر الخاصة بك .

بالإمكان الاطلاع على الدليل التدريبي المتعلق بتفعيل خاصية "التحقق بخطوتين " - أضغط هنا

ماذا تفعل إذا كنت ضحية "التصيد" Phishing ؟

١- قم بتغيير كلمة السر حالا.

٢- أبلاغ جميع الأصدقاء على وسائل التواصل الاجتماعي بهذه الحادثة و الطلب منهم التوقف عن التواصل مع حسابك حتى يتم حمايته .

٣-أطلب المساعدة من إدارة المواقع أو أتصل بالبنك لوقف الخدمة أو لإبلاغهم بالحادثة .

٤- حاول تحذير الآخرين حول الموقع أو الخدمة أو البريد الإلكتروني الوهمي / الزائف الذي وصلك أو الذي قمت بالدخول إليه .