اختراق المواقع الإلكترونية
و الحماية السيبرانية

مقدم الدورة

م. عبدالغني الخطيب

مهندس أمن سيبراني معتمد, يعمل في شركة كلاود زون التقنية .

حاصل على اعتمادات وخبرات متعددة في الأمن السيبراني

CEH, ECSA, Microaoft, Offensive Security

#خلك_واعي

الهندسة الإجتماعية

(Social Engineering)

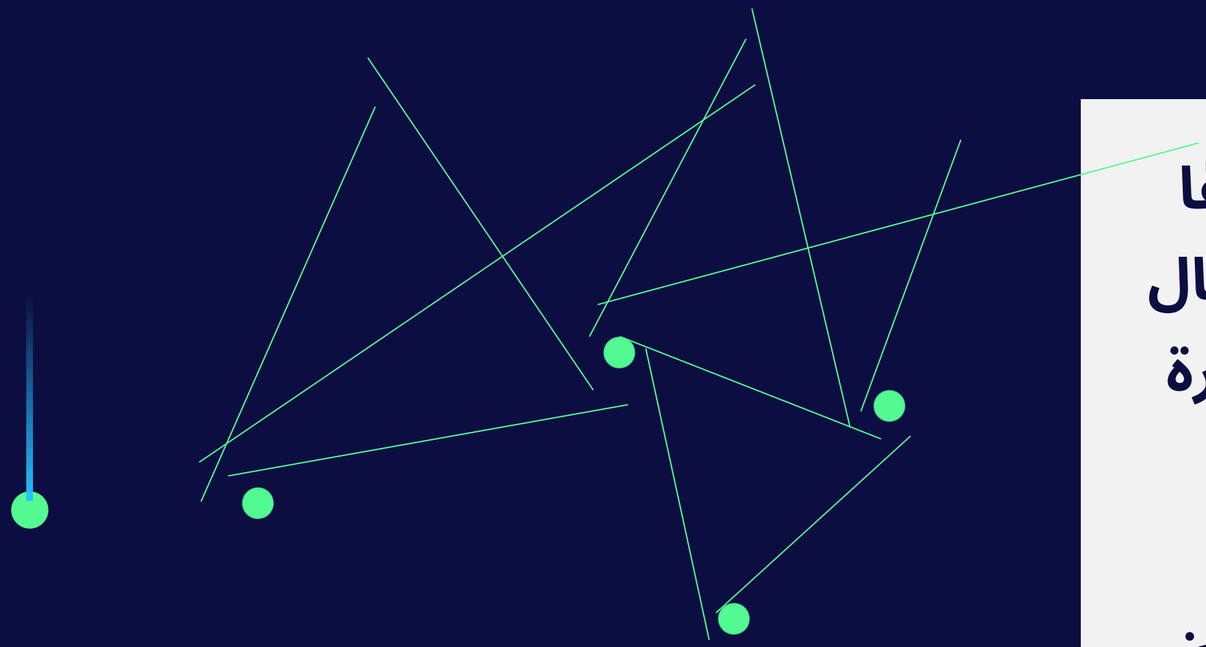
الهندسة الاجتماعية هي التلاعب بالبشر وخداعهم بهدف الحصول على بيانات أو معلومات، كانت ستظل خاصة وآمنة ولا يمكن الوصول إليها، بهدف اختراق النظام. ومن هنا يستخدم المخترِق "المهندس الاجتماعي" مهاراته لإستهداف نقاط الضعف البشرية في محاولة للتحايل على الضوابط والإجراءات التي من شأنها أن تمنعه من الحصول على المعلومات التي يحتاجها

#خلك_واعي

ما نوعية المعلومات التي يمكن خسارتها؟

كل شيء، ففي عصر المعلومات يمكن أن يكون لأي معلومة قيمة، فالشخص الذي يستهدفك له دوافع معينة، وبالتالي لا يمكن الاستهتار بأي معلومة تخسرها.

#خلك_واعي



حماية البريد الإلكتروني

يُعتبر البريد الإلكتروني أكثر الطرق شيوعًا للمراسلات على الإنترنت، وخاصة للأعمال التجارية. ولكن بنفس الوقت، نسبة كبيرة من البرمجيات الضارة على الشبكات المعرضة للخطر يكون مصدرها البريد الإلكتروني، إذ تُشير إحصاءات أنّ أكثر من 90٪ من الهجمات الإلكترونية تبدأ برسائل بريدية ضارة. هذا يعني أنك إذا كنت تستخدم البريد الإلكتروني في أعمالك، فأنت في خطر ما لم تبذل جهد في توفير أفضل الحلول لـ حماية البريد الإلكتروني من الاختراق.

#خلك_واعي

يمكن أن يؤدي ضعف أمان البريد الإلكتروني إلى تسرب المعلومات السرية، مثل: البيانات المالية للشركة وأوراق الملكية الفكرية ومعلومات الموظفين والعملاء. مما يؤدّي إلى خسارات فادحة في الإيرادات والحصة السوقية، بالإضافة إلى الغرامات والعقوبات القانونية ومخاطر الإضرار بالسمعة.

#خلك_واعي

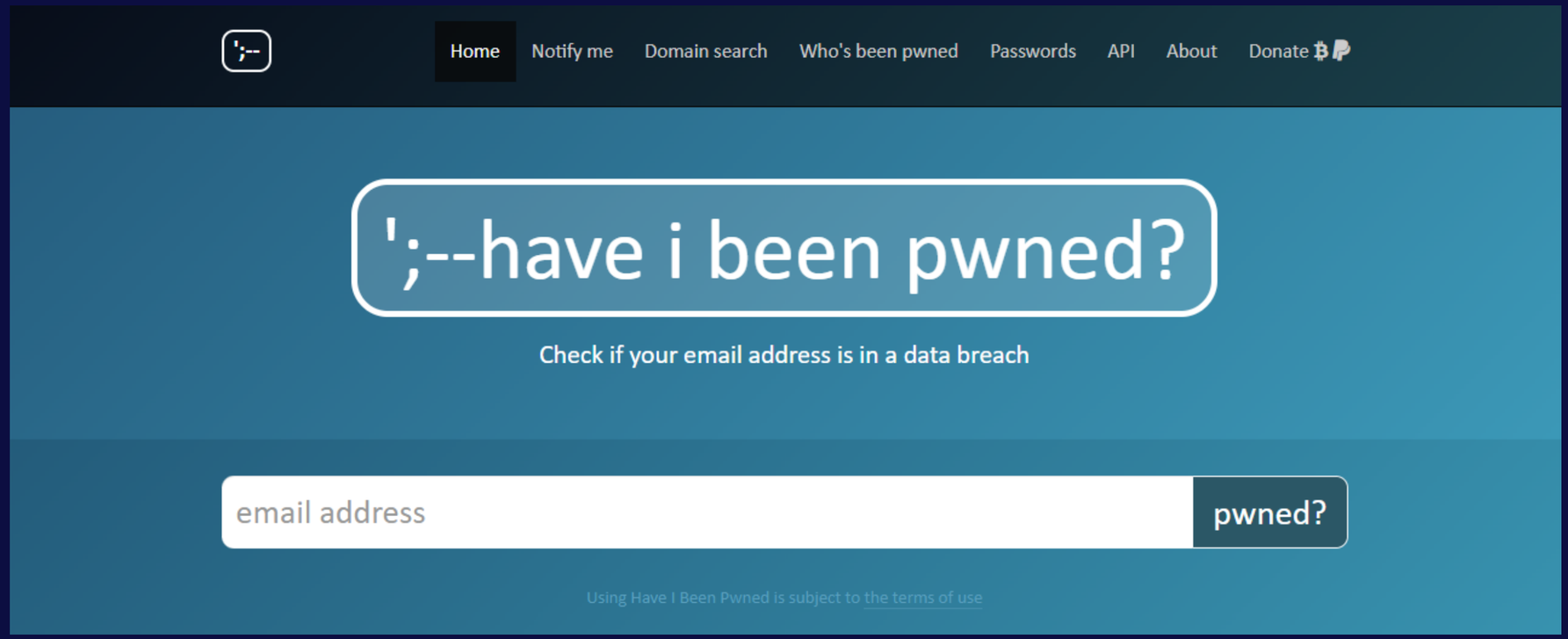
لماذا تعتبر حماية البريد الالكتروني من الاختراق مهمّة؟

حماية المعلومات الحساسة والحفاظ على سرية الاتصالات

ثغرة صغيرة يمكن أن تُؤثّر على المنظمة بأكملها

دائمًا ما يستخدم المجرمون البريد الإلكتروني كوسيلة لاختراق الأنظمة

#خلك_واعي



https://haveibeenpwned.com

#خلك_واعي

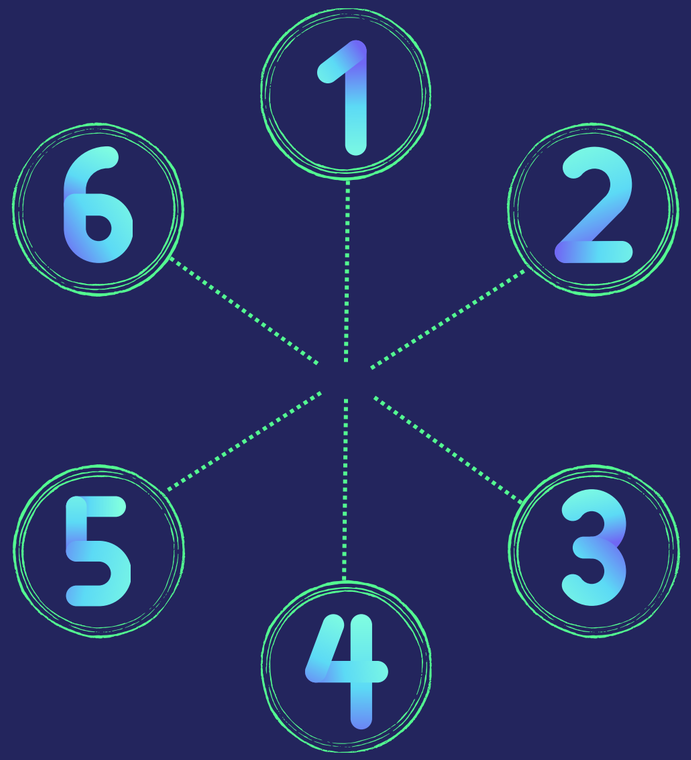
انتحال البريد الإلكتروني

ينتحل المهاجمون شخصية شركة أو مؤسسة مالية معروفة، مثل بنك أو خدمة دفع عبر الإنترنت. يرسلون رسائل بريد إلكتروني تحاكي العلامة التجارية للمؤسسة وتصميمها، مما يجعل من الصعب على المستلمين التمييز بين رسائل البريد الإلكتروني الأصلية والمزيفة.

غالباً ما تحتوي هذه الرسائل الاحتيالية على طلبات عاجلة للحصول على معلومات شخصية أو تفاصيل الحساب أو تحويلات الدفع، مما يستغل ثقة المستلم وشعوره بالإلحاح .

#خلك_واعي

بريد إلكتوني يبدو أنه من مصدر موثوق ، مثل زميل موثوق به أو شركة من خلال
التلاعب بمعلومات رأس البريد الإلكتروني يأتي من عنوان مختلف عما هو عليه في الواقع



تحتوي رسالة البريد الإلكتروني على شعور بالإلحاح،
وتحث المستلم على اتخاذ إجراء فوري،
مثل التحقق من تفاصيل حسابه أو تحديث كلمة المرور الخاصة به

يملئ الضحية بياناته الشخصية او كلمة السر
او معلوماته البنكية .

عندما يكمل الضحية ارسال البيانات
تصل البيانات للمخترق

يستخدم المخترق تلك بيانات البطاقة البنكية
لسحب الأموال او للشراء من مواقع من خلال
بطاقة الضحية

يمكن للمخترق استخدام بياناتك لإنتحال شخصيتك
و الاحتيال على الأشخاص المقربين و الأصدقاء

#خلك_واعي

اختراق الواتساب

1. ينتحل المخترق شخصية صديق أو قريب لك
2. يطلب منك فيه دفع قيمة طلب له على ان يعطيك ايها لاحقاَ
3. يرسل لك رابط الدفع أو الموقع و يملئ الضحية بياناته البنكية و الشخصية

4 ترسل تلك البيانات التي كتبها الضحية في الموقع للمخترق

5 يستخدم المخترق تلك البيانات البنكية للشراء أو لسحب الأموال

6 أو قد يستخدم المخترق بياناتك الشخصية لإختراق اصدقائك أو أقاربك بإنتحال شخصيتك

اختراق الحسابات البنكية

1 يتصل المخترق منتحل كيان البنك للضحية

2 يطلب المخترق من الضحية بياناته البنكية لتحديث حسابه

3 يعطي الضحية المخترق بياناته لتحديث بياناته

4 خلال ساعات يكتشف الضحية سحب مفاجئ للأموال نتيجة اعطاء البيانات

#خلك_واعي

لا تفتح مجال على حساباتك في منصات التواصل الاجتماعي

#خلك_واعي

كيف أحمي نفسي؟

أولاً تجنب مشاركة أي معلومات أو بيانات شخصية مع أي جهة كانت، وعلى الرغم من سهولة القيام بهذا الأمر فإن الكثير من المستخدمين يغفلون عن هذه النصيحة

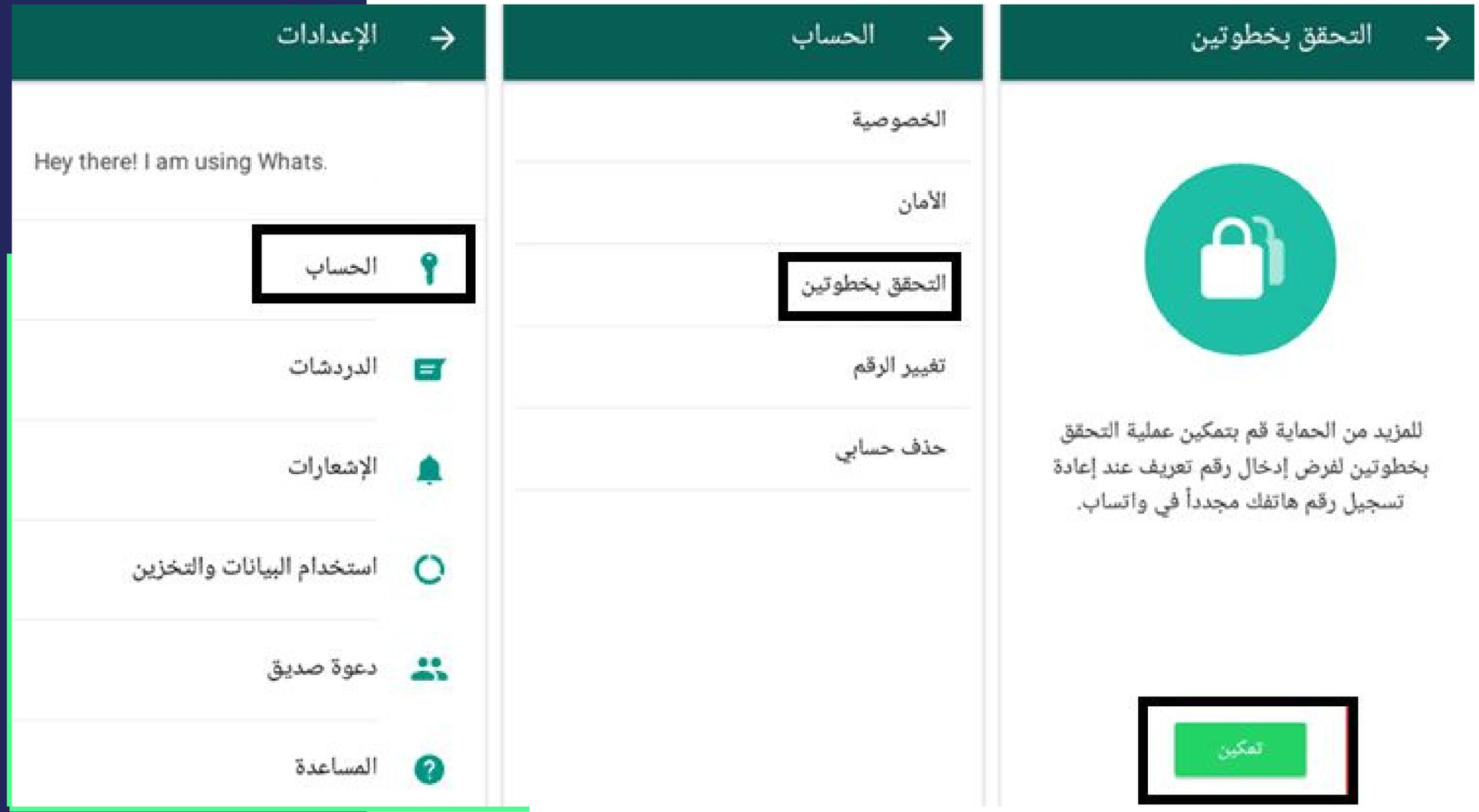
ثانيا، تحقق دائما من الأشخاص الذين تتحدث إليهم سواء عبر الهاتف أو البريد الإلكتروني أو خدمات التواصل الفوري وغيرها، مثلا لو كان المتصل من شركة رسمية فلا تجد حرجاً في أن تطلب منه معلوماته الكاملة وأن يقوم بالاتصال من رقم هاتف رسمي يمكن التحقق منه

ثالثا، لا تفتح مرفقات البريد الإلكتروني من أشخاص غير معروفين، فلغاية الآن يتم استخدام هذه الطريقة على نطاق واسع لنشر البرمجيات الخبيثة والحصول على المعلومات الشخصية، وذلك من خلال انتحال هوية شركات كبرى وإرفاق بعض الملفات في البريد

رابعا، اعمل على تأمين هاتفك الذكي أو حاسوبك المحمول، يمكن أن تعتمد على فلترة البريد المزعج بالاعتماد على أدوات خاصة، كذلك اعتمد على برامج قوية لمكافحة الفيروسات تتضمن أدوات لمكافحة رسائل وصفحات التصيد

#خلك_واعي

حماية حسابك على واتساب (WhatsApp)



#خلك_واعي

لتفعيل إشعارات الأمان:

- من الإعدادات **اختر الحساب** ثم إشعارات الأمان
- **فعّل إظهار** إشعارات الأمان على هذا الهاتف

لتتلقى الإشعارات عندما
يتغير رمز الأمان الخاص بأي جهة
من جهات اتصالك

#خلك_واعي

كيف تسترجع حسابك على واتساب؟

أكّد رقم هاتفك بإدخال رمز يصلك في رسالة نصية

بعد إدخال الرمز, سيتم تسجيل خروج الشخص الذي اخترق حسابك تلقائياً

حذف الأجهزة المرتبطة بالحساب

من الأعدادات اختر
الأجهزة المرتبطة

ستظهر لك كل الأجهزة التي تستخدم
حسابك, قم بتسجيل الخروج منها فورا

#خلك_واعي

انتهت الدورة

شكراً لحضوركم

#خلك_واعي