#أمنك_مسؤوليتك

# الهندسة الاجتماعية...

# انتبه بياناتك في خطر!

"نحن مخترقون ومراقبون طالما أننا متصلون بالإنترنت"

## الهندسة الاجتماعية.. انتبه بياناتك في خطر!
## "نحن مخترقون ومراقبون طالما أننا متصلون بالإنترنت"

لا مفرّ من العيون التي تراقبنا حتى وإن ابتعدنا عن الجميع واعتكفنا في غرفتنا.. فحواسيبنا، وهواتفنا الذكية، ومتصفحات الإنترنت، يعلمون الكثير عنّا وعن حياتنا وأسرارنا بأدق تفاصيلها، هذا فضلاً عن أناس امتهنوا مهمّة رصد ومراقبة الآخرين وجمع معلوماتهم وبياناتهم الشخصية للاستيلاء عليها، وهو ما يعود عليهم بالكثير من الأموال.

ليس من الضروري أن تكون مشهوراً، أو من أصحاب الملايين، أو تمتلك معلومات أو شركات ضخمة ليتمّ اختراقك، ولا يكفي اعتمادك على برامج قوية للحماية من القرصنة ومكافحة الفيروسات لتحصين أجهزتك الإلكترونية، فمع كل ما يمكن لمطوّري النظم الأمنية ابتكاره في هذا المجال، يبقى لجانب آخر -**ربما يكون أكثر أهمية**- دوراً في ذلك وهو العنصر البشري المتمثل بالمستخدم. فكثيراً ما يعتمد المخترقون على الخطأ البشري وجهل البعض بالتكنولوجيا، للوصول إلى ما يريدونه من معلومات سرية، مستخدمين أساليب الحنكة والمكر، وهو ما بات يعرف بفن "اختراق العقول" أو "الهندسة الاجتماعية".

يعمد "المهندس الاجتماعي" إلى مراقبة حسابات مواقع التواصل الاجتماعي للضحية، يجمع عنه الكثير من المعلومات، يدرس شخصيته ويعرف الكثير عنها رغم أنه لم يلتقيه، ومن ثم يصنع شخصية افتراضية ينتحلها ويتحدث إلى الضحية عبرها مستخدماً المعلومات التي جمعها عن حياته الشخصية بطريقة مدروسة، فيتقرب منه حتى يثق فيه، ثم يُملي عليه ما يريد للوصول إلى غاياته بسهولة، كأن يقنعه بالضغط على رابط مفخخ، أو بتحميل ملف يحتوي على برمجية خبيثة، أو ربما قد يخترق حاسوب الضحية ويستخدمه لنشر فيروس في أجهزة الشركة التي يعمل بها.

**يمكن تعريف "الهندسة الاجتماعي" في سياق أمن المعلومات على أنها استخدام الخداع للتلاعب بالأفراد من أجل الكشف عن معلوماتهم السرية أو الشخصية والتي يمكن استخدامها لأغراض احتيالية.**

يُطوّر "المهندسون الاجتماعيون" بشكل مستمر أساليب جديدة لخداع ضحاياهم، فإلى جانب انتحال الشخصية، وخيانة الثقة التي يمنحها له الضحية والذي قد يكون صديقاً أو مقرباً، يعمد المخترقون إلى استغلال فضول الضحية وعواطفه وطباعه الشخصية، بالإضافة إلى استغلال المواضيع الجديدة والساخنة التي قد تكون محطّ اهتمام الكثيرين، للوصول لغاياتهم الاحتيالية.

فكثيراً ما نصادف على وسائل التواصل الاجتماعي منشورات من قبيل: "شارك المنشور مع 10 من أصدقائك لتدخل السحب على سيارة"، أو "اضغط على الصورة لتتحرك"، أو "املأ الاستمارة للدخول في سحب للفوز بجوائز قيّمة"، أو "حمّل ملف نسخة محدّثة عن تطبيق معين موثوق" بينما يكون الرابط خبيثاً، وبذلك تكون قد أهديت المخترق

بياناتك الشخصية بكامل إرادتك، ليستخدم تلك المعلومات بسرقة حساباتك عن طريق تخمين كلمات السر، أو بيع تلك المعلومات إلى شركات المعلنين.
كما قد يعمد المخترق لاصطياد كلمة سر الضحية، من خلال إرسال صفحة من تصميمه تشبه صفحة تسجيل الدخول لأحد المواقع الشهيرة من حيث الشكل، لكنها تحمل عنوانًا مختلفًا عن العنوان الأصلي، وعندما يُدخل الضحية كلمة السر للولوج في حسابه تصل بكل بساطة إلى المخترق ويكون الضحية قد وقع بالفخ دون أن يشعر بالخداع.

أما عن المعلومات التي قد يستهدفها المخترقون فهي تشمل كل ما يساعدهم في الحصول على الأموال، ورغم أنهم يركزون بشكل أساسي على الخدمات المالية كالحسابات البنكية وغيرها، إلا أنّ أي معلومة قد يتمكنون من الحصول عليها سيكون لها قيمة وتوظيف للوصول إلى غاياتهم.

ومن الأمثلة على استخدام أساليب الهندسة الاجتماعية للاختراق ما حدث في الانتخابات الأمريكية الأخيرة التي جرت عام 2016، إذ اتهم مكتب التحقيقات الفيدرالية "إف بي آي" الحكومة الروسية بالتدخل في الانتخابات الأمريكية، عبر اختراق تسبب في التلاعب بنتائج الانتخابات الرئاسية التي انتهت بفوز دونالد ترامب بالرئاسة على منافسته هيلاري كلينتون.[1]

وأظهرت التحقيقات أن مخترقين روس أنشؤوا آلاف الحسابات الوهمية على موقعي "فيس بوك" و "تويتر"، ليمرروا بواسطتها عدداً كبيراً من الأخبار المضللة والشائعات، من خلال الدخول في نقاشات مع مواطنين أمريكيين وكسب ثقتهم.
كما كشفت شركة "غوغل"، أن عملاء روس أنفقوا عشرات الآلاف من الدولارات على نشر إعلانات على عدد من المواقع منها "يوتيوب"، و"جيميل"، ومحرك بحث "غوغل" وغيرها، في إطار حملة تضليل، مهمتها التأثير على نتائج الانتخابات الأمريكية.[2]

**ربما يظن البعض أن أساليب الهندسة الاجتماعية لن تنطلي عليهم وأنهم حذرون بالقدر الكافي، ولكن الوقائع تقول أن مسؤولين في كبرى الشركات العالمية قد وقعوا في فخها، لما يمتلكه المخترقون من درجة عالية من الاحترافية، واعتمادهم على استهداف الناحية النفسية للإنسان والمحفزات الأساسية للسلوك البشري.**

## كيف ننجو من الهجمات ونحمي أنفسنا من مخاطر الهندسة الاجتماعية؟

[1] "قبيل قمة بوتين وترامب: واشنطن تتهم 12 روسيا باختراق الانتخابات الرئاسية الأمريكية"، بي بي سي عربي. ١٤ يوليو/تموز ٢٠١٨. (آخر زيارة ١٨ تشرين الثاني/نوفمبر ٢٠١٨). http://www.bbc.com/arabic/world-44830314.
انظر أيضاً: "الكونجرس الأمريكي يبدأ تحقيقا في مزاعم الاختراق الإلكتروني الروسي"، وكالة رويترز للأنباء. ٥ كانون الثاني/يناير ٢٠١٧. (آخر زيارة ١٨ تشرين الثاني/نوفمبر ٢٠١٨). https://ara.reuters.com/article/worldNews/idARAKBN14P0ML.
[2] "غوغل: عملاء روس أثروا على الانتخابات الأمريكية"، بي بي سي عربي. ٢٠ تشرين الأول/أكتوبر ٢٠١٧. (آخر زيارة ١٨ تشرين الثاني/نوفمبر ٢٠١٨). http://www.bbc.com/arabic/science-and-tech-41562084.

ينصحنا الخبراء بـ:

- ✓ التثقيف في مجال الأمن الرقمي وأساليب الاختراق المتجددة.
- ✓ تجنب إعطاء أي معلومات سرية أو بيانات شخصية إلا بعد التأكد من هوية الشخص المتحدث، وأن الاتصال تمّ من جهة رسمية أو معروفة.
- ✓ تجنب الحديث في الأسرار الشخصية مع الأصدقاء المجهولين عبر وسائل التواصل الاجتماعي.
- ✓ عدم فتح ملفات أو مرفقات البريد الإلكتروني المُرسَل من أشخاص غير معروفين. والتأكد من الروابط المرسلة بأنّها ليست روابط خبيثة من خلال فتحها عبر استخدام موقع فيروس توتال.
- ✓ العمل على تأمين هواتفنا أو حواسيبنا واستخدام برامج لمكافحة الفيروسات.

فقد أظهرت دراسة أجرتها "شركة فيرايزون الأميركية" أن أكثر هجمات الاحتيال والتصيد تستهدف موظفي الإدارات المالية كونهم يتولون الإشراف على عمليات تحويل الأموال.[3]

**وإلى جانب تلك الإجراءات يتوجب على الشركات تدريب الموظفين لديها على اتخاذ التدابير الأمنية اللازمة للحماية من الهندسة الاجتماعية، وخصوصًا الأكثر عرضة منهم للاختراق كموظفي القطاع المالي.**

**أما عند الوقوع ضحية للهندسة الاجتماعية فعليك القيام بالخطوات التالية:**

1. اللجوء للشخص المسؤول عن الأمن الرقمي في المؤسسة أو لأصحاب الاختصاص في هذا المجال.
2. العمل على إزالة آثار الهجوم بحسب نوعه.
3. معرفة الأشخاص أو الجهات المتضررة من الهجوم وإعلامهم بما حدث.

ويبقى الأخذ بالأسباب أهم أنواع الحماية، فبياناتك الشخصية كتاريخ ميلادك ورقم هاتفك وأسماء أفراد عائلتك وكل ما يُعرّف بهويتك يجب أن تبقى محمية ومحفوظة عن المشاركة مع الآخرين في الفضاء الإلكتروني، حيث لا يمكننا التنبؤ بنيات الجميع تجاهنا، أو مهاراتهم وقدراتهم على توظيفها لاختراقنا.

---

[3] الاختراق بالهندسة الاجتماعية.. ماذا تعرف عنه؟، الجزيرة نت، ١ أيار/مايو ٢٠١٧.(آخر زيارة ١٤ تشرين الثاني/نوفمبر ٢٠١٨).
http://www.aljazeera.net/news/scienceandtechnology/2017/5/1/%D8%A7%D9%84%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D8%A8%D8%A7%D8%B3%D8%AA%D8%AE%D8%AF%D8%A7%D9%85-%D8%A7%D9%84%D9%87%D9%86%D8%AF%D8%B3%D8%A9-%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9.

# المؤسسات المشاركة بالحملة:

**منظمة سوريون من أجل الحقيقة والعدالة:** منظمة سورية مستقلة، تأسست عام 2015، تعمل على توثيق انتهاكات حقوق الإنسان في سوريا، وقضايا المناصرة في المحافل الدولية.

**جريدة عنب بلدي:** مؤسسة إعلامية سورية مستقلة تأسست عام 2011 في مدينة داريا بريف دمشق، وتصدر مطبوعة أسبوعية، سياسية، اجتماعية، منوعة.

**راديو روزنة:** إذاعة سورية انطلقت عام 2013، تقدم نشرات ومواجز إخبارية متعددة وبرامج ثقافية وتوعوية وخدمية متنوعة، وتنشط أيضاً عبر موقعها الإلكتروني.

**الشبكة السورية للإعلام المطبوع:** تأسست عام 2014، وهي تجمّع لصحف ومجلات سورية مستقلة، تعمل على تنسيق الجهود فيما بينها من خلال تبادل الخبرات الصحفية والمهنية.

**منظمة آرتا للإعلام والتنمية:** وهي منظمة غير حكومية غير ربحية، مقرها في مدينة عامودا بمحافظة الحسكة، تعمل على تطوير مشاريع إعلامية مستقلة وتدريب ودعم صحفيين.

**مشروع سلامتك:** تأسس عام 2012، يهدف لنشر التوعية والمساعدة حول الأمن الرقمي، عبر تقديم الدعم التقني للمنظمات السورية، والمساعدة التقنية عبر الإنترنت، والتدريب الميداني.

**موقع أنا إنسان:** يركز على نشر القصص الإنسانية، وبشكل خاص قصص السوريين، بهدف طرح ومعالجة قضايا متعددة، وتوثيق معاناتهم والانتهاكات التي ارتُكبت بحقهم، إلى جانب عرض تجارب نجاحهم وإنجازاتهم.

#أمنك_مسؤوليتك