تطبيقات الهاتف الجوال وحماية الخصوصية

الفئة المستهدَفة
طلبة الجامعات

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

تطبيقات الهاتف الجوّال وحمايـــة الخصوصيـــة

الفئة المستهدَفة: طلبة الجامعات

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حقوق الملكية الفكرية

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 663 62
00974 404 663 79
academy@ncsa.gov.qa
www.ncsa.gov.qa/

يناير 2025م
الدوحة، قطر

◆ عزيزي المشارك

في ظلّ التطوُّر التكنولوجي المتسارع، ودخول الإنترنت إلى مختلف مجالات الحياة؛ أصبحت التهديدات السيبرانية تُواجِه مختلف شرائح المجتمع، ما يتطلَّب العمل على تعزيز الوعي بمفاهيم السلامة الرقمية؛ التي تُعدّ الدّرع الذي يحمي المجتمع من هذه التهديدات.

وفي سياق جهود «المبادرة الوطنية للسلامة الرقمية» لتعزيز مؤشرات السلامة الرقمية في المجتمع؛ تُقدِّم الوكالة الوطنية للأمن السيبراني هذا الكُتَيِّب، والذي يتضمَّن مجموعةً من النصائح والإرشادات العامَّة المتعلّقة بالسلامة الرقمية.

الفهـــرس	رقم الصفحـة

مُقدّمـــة

أصبحت تطبيقات الهاتف الجوّال جزءاً لا يتجزّأ من حياتنا اليومية؛ حيث تُتيح لنا الوصول إلى مجموعة متنوعة من الخدمات والمعلومات بسهولة وسرعة؛ من التسوق عبر الإنترنت إلى الخدمات المصرفية، وإدارة الصحة، وغيرها.

وتعتمد التطبيقات على جَمْع بيانات المُستخدِمين لتخصيص الخدمات وتحسين التجربة.

لكن مع هذا الاعتماد المتزايد على التطبيقات، تبرز المخاوف بشأن خصوصية البيانات وحمايتها. وتجمع العديد من التطبيقات معلومات حسّاسة مثل الموقع الجغرافي، البيانات الشخصية، السجلات الصحية، والمعاملات المالية، مما يجعلها أهدافاً محتملةً للهجمات الإلكترونية وسوء الاستخدام.

لمواجهة هذه التحديات؛ أصبحت حماية الخصوصية أولوية قصوى في تطوير التطبيقات؛ حيث يعتمد المُطوِّرون على تقنيات متقدّمة مثل التشفير لضمان أمان البيانات في أثناء نقلها وتخزينها، والتحقق متعدّد العوامل لتعزيز الأمان ومنع الوصول غير المصرَّح به. إضافةً إلى ذلك، تم تعزيز قوانين حماية البيانات حول العالم، مثل اللائحة العامة لحماية البيانات (GDPR)، ما يُلزم الشركات باتباع ممارسات صارمة لحماية خصوصية المُستخدِمين.

كما أن هناك مسؤولية تقع على المُستخدِمين أنفسهم من خلال فهم الأذونات التي تمنح للتطبيقات وإدارة إعدادات الخصوصية بشكلٍ دقيق. وتُوفِّر المتاجر الرقمية مثل Google Play وApple App Store سياسات تشترط على المطوّرين الإفصاح بشكلٍ واضحٍ عن كيفية جَمْع البيانات ومعالجتها، مما يزيد من الشفافية ويُعزّز الثقة بين المُستخدِمين ومقدّمي الخدمات.

01

الفصل الأول

مفهـوم تطبيقـات الهاتـــف الجـــوّال

- أولاً: آليات وأسباب جمع تطبيقات الهاتف الجوّال لبيانات المُستخدِمين.
- ثانياً: أنواع البيانات التي يتم جَمْعها في تطبيقات الأجهزة المحمولة.
- ثالثاً: مخاطر تطبيقات الهواتف المحمولة.

مفهوم تطبيقات الهاتف الجوّال

تطبيقات الهاتف الجوّال هي برامج صُمِّمت للعمل على الهواتف الذكية والأجهزة اللوحية؛ بهدف تقديم مجموعة متنوعة من الخدمات والوظائف للمُستخدِمين.

تشمل هذه التطبيقات العديد من المجالات، مثل التواصل الاجتماعي، الأعمال، التعليم، الصحة، الترفيه، وغيرها.

تعمل هذه التطبيقات على تسهيل الحياة اليومية عبر توفير وصول سريع ومباشر إلى المعلومات والأدوات، مما يُعزّز من الكفاءة والإنتاجية، وبفضل التطور السريع للتكنولوجيا، أصبحت تطبيقات الهاتف جزءاً أساسياً من حياة الأفراد والشركات؛ حيث تُوفّر تجربة تفاعلية وسلسة تعتمد على تكنولوجيا الهواتف المحمولة المتقدّمة.

أولاً: آليات وأسباب جمع تطبيقات الهاتف الجوّال لبيانات المُستخدِمين

أجرى باحثون في جامعة أكسفورد دراسةً حول خصوصية تطبيقات الهواتف المحمولة، ووجدوا أن هذه التطبيقات غالباً ما تُرسل البيانات إلى عدد قليل من الشركات الكبرى، مثل ألفابت (الشركة الأم لجوجل) وفيسبوك وتويتر (إكس حالياً) ومايكروسوفت وأمازون. ويُلاحَظ أن هذه الشركات تعتمد على شبكة من الشركات التابعة لجمع البيانات من التطبيقات، مما يساعد على إخفاء تركيز البيانات في أيدي أكبر شركات التكنولوجيا في العالم.

وبناءً على سلوكيات الاستخدام الخاصة بمُستخدِمي التطبيقات، مثل متوسط وقت الاستخدام والصفحات التي يتابعونها والمكان الذي قاموا بتسجيل الدخول منه إلى التطبيق وما إلى ذلك، فإن تلك الجهات تَعرف ما يكفي لتحديد موقع المُستخدِمين واهتماماتهم الحالية، وخططهم المستقبلية، وحالتهم المالية أيضاً.

ويمكن أن تتضمّن البيانات التي تم جمعها بواسطة أطراف ثالثة من خلال تطبيقات الهواتف المحمولة أي شيء من معلومات الملف الشخصي مثل العمر والجنس، إضافةً إلى تفاصيل الموقع، بما في ذلك البيانات حول أجهزة توجيه Wi-Fi، والمعلومات حول كل تطبيق موجود على الهاتف[1].

إن ما سبق يُثير مخاوف الكثيرين حول خصوصية البيانات الشخصية عند استخدام التطبيقات المختلفة، إلا أنه يُشار إلى إمكانية التحقق من البيانات التي يجمعها التطبيق وإزالة الإذن إذا لزم الأمر؛ حيث يلتزم معظم مُزوّدي التطبيقات بذلك. ومع ذلك، فإن الشعور بالانزعاج والتهديد أمر طبيعي إذا تم تعقُّبهم مِن قِبَل شخص مجهول دون إدراك منهم.

هل تعلم؟

كشفت دراسة أُجريت على نحو مليون تطبيق أندرويد أنّ ما يَقرب من 90% من تطبيقات الهاتف الجوّال تجمع البيانات، وتُعيد نقلها مجدداً إلى أطراف ثالثة؛ بهدف تحسين تجربة العملاء، وللوقوف على مدى جودة المُنتَجات، وتقييم العلاقة بين المستهلك والعلامة التجارية[2].

1. How Mobile Apps Collect Your Data And What You Should Do, December 2022. follow link: https://ready.io/blog/how-mobile-apps-collect-your-data
2. Aliya Ram, et al, How smartphone apps track users and share data, October 2018. follow link: https://ig.ft.com/mobile-app-data-trackers/

احذر!

يساعد جمع البيانات في التعرُّف على سلوك المُستخدِمين وأنماطهم المفضَّلة، لإظهار المحتويات التي تتوافق مع اهتماماتهم، كما يحدث في حالة منصات التواصل الاجتماعي التي تلعب الخوارزميات دوراً مهماً في تحسين جودة تصفُّح المُستخدِم، وإظهار المحتوى المتوافق معه؛ للبقاء مدة أطول على المنصة.

هل تعلم؟

في أبريل 2022م، فرضت جوجل على جميع المطوّرين الذين ينشرون تطبيقات على متجر Google Play الإفصاح عن كيفية جمع ومعالجة بيانات المُستخدِمين في تطبيقاتهم. ويُلزَم المطورون بتقديم تفاصيل حول ممارسات الأمان، مثل التشفير، ويشمل ذلك أيضاً البيانات التي يتم جمعها عبر مكتبات أو حزم تطوير برمجيات تابعة لجهات خارجية مُستخدَمة في التطبيقات. هذه السياسة تهدف إلى زيادة شفافية التطبيقات، وتعزيز حماية بيانات المُستخدِمين[1].

1. https://support.google.com/googleplay/android-developer/answer/10787469?hl=en

ثانياً: أنواع البيانات التي يتم جمعها في تطبيقات الأجهزة المحمولة

يمكن لتطبيقات الهواتف المحمولة جَمْع مجموعة واسعة من البيانات، اعتماداً على وظائفها وميزاتها والأذونات الممنوحة مِن قِبَل المُستخدِمين **وفيما يلي أنواع البيانات التي يتم جمعها:**

المعلومات الشخصية

تتضمَّن هذه البيانات: الأسماء، وعناوين البريد الإلكتروني، وأرقام الهواتف، وأرقام الضمان الاجتماعي... وغيرها من المعلومات التي تُحدّد هوية المُستخدِم.

بيانات الموقع

تجمع العديد من التطبيقات معلومات حول موقع المُستخدِم بواسطة بيانات نظام تحديد المواقع العالمي (GPS)، أو شبكة Wi-Fi، أو شبكة الهاتف؛ وذلك لاستخدامها في أغراض مختلفة مثل تقديم خدمات تعتمد على الموقع أو الإعلانات المستهدَفة أو تحليل سلوك المُستخدِم[1].

1. Mahesh Atapattu, Mobile Application Data Collection and Data Sharing: What You Need to Know, July 2023. follow link: https://www.linkedin.com/pulse/mobile-application-data-collection-sharing-what-you-need-atapattu/

معلومات الجهاز

تجمع بعض التطبيقات بيانات حول جهاز المُستخدِم، بما في ذلك طراز الجهاز، وإصدار نظام التشغيل، ونوع المتصفح، ومُعرّفات الجهاز الفريدة (UDID)، وعنوان IP، واتصالات الشبكة، ومواصفات الأجهزة؛ لأن هذه المعلومات تساعد المُطوّرين على تحسين أداء التطبيق.

بيانات الاستخدام

من البيانات التي تقوم بعض التطبيقات بجمعها: سلوك المُستخدِمين مع التطبيق، بما في ذلك الميزات التي يستخدمونها، والمدة التي يقضونها في استخدام التطبيق، وأنماط التنقل الخاصة بهم؛ لمساعدة المطورين على فهم سلوك المُستخدِم، وتحسين ميزات وآليات استخدام التطبيق بناء عليها.

بيانات المصادقة (أو بيانات تسجيل الدخول)

تلجأ العديد من التطبيقات إلى جمع أسماء المُستخدِمين، وكلمات المرور، أو رموز المصادقة الأخرى؛ للسماح للمُستخدِم بتسجيل الدخول بأمان، والوصول إلى المحتوى أو الخدمات عليها.

بيانات وسائل التواصل الاجتماعي

عادةً تطلب التطبيقات الوصول إلى ملفات تعريف المُستخدِم على وسائل التواصل الاجتماعي، وكذلك قوائم الأصدقاء، وغيرها من المعلومات التي يمكن استخدامها في الإعلانات المستهدَفة.

معلومات الدفع

تتجه تطبيقات التجارة الإلكترونية إلى جمع معلومات الدفع مثل أرقام بطاقات الائتمان، وعناوين الفواتير، وسجل المعاملات لمعالجة المشتريات وإدارة الحسابات.

بيانات الصحة واللياقة البدنية

تجمع تطبيقات الصحة واللياقة البدنية بيانات شخصية، مثل: نمط التمارين الرياضية والعادات الغذائية، وأنماط النوم والقياسات الحيوية لتتبُّع وتحليل المقاييس المتعلقة بالصحة للمُستخدِمين.

هل تعلم؟

وفقاً لدراسة أجراها مركز بيو Pew للأبحاث، فإن 72% من مُستخدِمي الهواتف الذكية أبدوا قَلَقهم من مسألة جمع بياناتهم بواسطة تطبيقات الهواتف. في حين لا يدرك 68% من المُستخدِمين أن بياناتهم يتمّ بَيْعها بواسطة التطبيقات التي يستخدمونها[1].

1. McClain, Colleen,et al, How Americans View Data Privacy, PEW, October 2023, follow link: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

ثالثاً: مخاطر تطبيقات الهواتف المحمولة

تختلف مخاطر أمان الهواتف المحمولة عن أجهزة الحاسوب الشخصية والمكتبية، ولهذا السبب فإن حماية تطبيقات الأجهزة المحمولة مهمة لا سيما مع توفرها مع ما يقرب من 80% من سكان العالم، وارتفاع وتيرة عمليات تنزيل التطبيقات سنوياً؛ **حيث سجَّل عام 2021م وحده نحو 230 مليار عملية تنزيل**، ويختلف تأمين تطبيق الهاتف الجوّال تماماً عن تأمين موقع ويب أو تطبيق ويب أو حتى تطبيق برمجي لأجهزة الحاسوب المحمولة أو المكتبية؛ ولذا فعلى المطورين العمل ضمن قيود كلٍّ من نظام تشغيل الهاتف (iOS أو Android) ومتجر التطبيقات الذي يريدون نشر التطبيق التابع لهذين النظامين عليه.

علماً بأن معظم مشكلات أمان تطبيقات الهاتف الجوّال تبدأ في عملية التطوير، وتمتد إلى الإهمال في الشيفرة، والذي يتسبَّب في تسلُّل مجرمي الإنترنت إلى التطبيق لبدء عملية سرقة البيانات أو الاستيلاء على حساب المُستخدِم.

ومن المخاطر الأمنية لتطبيقات الهاتف الجوّال:

1- الاتصالات غير الآمِنة

في تطبيقات المحمول الشائعة، يتم تبادل البيانات عن طريق قيام التطبيق بنقل البيانات عبر الإنترنت وشبكة شركة الاتصالات الخاصة بالهاتف الجوّال، وهنا قد يستغل المهاجمون ثغرات الأمان في الأجهزة لاعتراض المعلومات الحسّاسة أو بيانات المُستخدِم أثناء انتقالها عبر الشبكة[1].

ومن أسباب التهديد الموجودة في الاتصالات غير الآمنة:

- البرمجيات الضّارَّة على الجهاز المحمول.
- شبكة Wi-Fi غير آمِنَة أو مُخترَقة مِن قِبَل مجرمي الإنترنت.

علماً بأنَّ مُطوّري الأجهزة المحمولة عادةً ما يستخدمون بروتوكول حماية SSL/TLS فقط في أثناء المصادقة، ولكن ليس في أيّ مكان آخر، مما يؤدي إلى طبقة أمان غير كافية، وهو ما يزيد من خطر تعرُّض البيانات الحسّاسة -مثل بيانات تسجيل الدخول، والمعلومات الشخصية، ومعرفات الجلسة، وغيرها من البيانات المهمة- لخطر الاعتراض مِن قِبَل المجرمين؛ إذ لا يعني وجود بروتوكول SSL/TLS أن التطبيق المحمول آمِن تماماً.

احذر!

في تطبيقات المحمول الشائعة، يتم تبادل البيانات عن طريق قيام التطبيق بنقل البيانات عبر الإنترنت وشبكة شركة الاتصالات الخاصة بالهاتف الجوّال، وهنا قد يستغل المهاجمون ثغرات الأمان في الأجهزة لاعتراض المعلومات الحسّاسة أو بيانات المُستخدِم أثناء انتقالها عبر الشبكة.

1. M3: Insecure Communicatio, Clouddefense, follow link: https://www.clouddefense.ai/owasp/2016/3

2- تخزين البيانات الشخصية بشكل غير آمِن

غالباً ما تُخزّن تطبيقات الهواتف المحمولة، وحتى تطبيقات الخدمات المصرفية، البيانات الحسّاسة محلياً، وهذا يعني أن رقم التعريف الشخصي، وأرقام بطاقات الائتمان، وكلمات المرور، وتفاصيل تسجيل الدخول، وغيرها من البيانات يتم تخزينها ببساطة في مكان ما على الهاتف الذكي. والأسوأ أنها غالباً ما يتم تخزينها بشكلٍ غير آمِن، ما يعني إمكانية وصول مجرم الإنترنت عن بُعْد إلى الجهاز، ثم عثوره على هذه البيانات وسرقتها[1].

ويتم تخزين البيانات الحسّاسة بشكلٍ غير آمِن بسبب التشفير غير الصحيح، فبعض تطبيقات الهاتف لا تقوم بعملية تشفير البيانات المحلية تماماً؛ أو قد تقوم بالعملية، لكن لا تُخزّن مفاتيح التشفير بشكل صحيح؛ أو أنها تَستخدم بروتوكولات تشفير مخصَّصة غير آمنة.

احذر!

غالباً ما تُخزّن تطبيقات الهواتف المحمولة، وحتى تطبيقات الخدمات المصرفية، البيانات الحسّاسة محلياً، وهذا يعني أن رقم التعريف الشخصي، وأرقام بطاقات الائتمان، وكلمات المرور، وتفاصيل تسجيل الدخول، وغيرها من البيانات يتم تخزينها ببساطة في مكان ما على الهاتف الذكي.

1. mobile app security risks and how to mitigate them, Cypress Data Defense, July 2020. follow link: https://2u.pw/PKH0B660

3- تسرب البيانات الحسّاسة

قد تتعرَّض البيانات الحسّاسة إلى التسرُّب والاختراق؛ إما عن طريق الخطأ، وإما عن عمد. ومن الأمثلة الشهيرة على ذلك: ما حدث لتطبيق Park mobile الشهير الخاص بمواقف السيارات والتنقل على الهاتف الجوّال عندما تسبَّبت ثغرة أمنية في برنامج تابع لجهة خارجية في تسرُّب البيانات عام 2021م، ما أدَّى إلى الكشف عن رسائل البريد الإلكتروني، وتواريخ الميلاد، وأرقام لوحات الترخيص، وأرقام الهواتف، وغيرها من بيانات شخصية لنحو 21 مليون مُستخدِم[1].

وفي بعض الأحيان، تحدث هذه التسريبات عن غير قَصْد، فمثلاً يُعدّ Firebase أحد أكثر حلول تخزين البيانات شيوعاً لتطبيقات أندرويد An-droid؛ إلا أنه غالباً ما يتمّ تكوينه بشكل خاطئ ما يعني إمكانية وصول أيّ شخص يعرف عنوان URL الصحيح لتطبيق ما تمَّ إنشاؤه باستخدام Firebase بسهولة إلى قواعد بيانات هذا التطبيق، وبالتالي إمكانية تسرُّب بيانات المُستخدِم.

ولمنع تسرُّب البيانات الحسّاسة، يمكن منع تخزين البيانات في ذاكرة التخزين المؤقَّت؛ لأن المجرمين يمكنهم استخدام هذه البيانات لمحاولة اختراق حساب المُستخدِم. كما على المُستخدِمين تنظيف ذاكرة التخزين المؤقَّت يدوياً؛ فهذا يجعل التطبيق أكثر أماناً.

1. Twingate Team, what happened in the park mobile data breach?. Twingate, may 2024, follow link: https://www.twingate.com/blog/tips/park-mobile-data-breach

4- البرمجيات الخبيثة

البرمجيات الخبيثة للأجهزة المحمولة هي برمجيات ضارَّة مُصمَّمة خصيصاً لاستهداف الهواتف الذكية والأجهزة اللوحية، بهدف الوصول إلى البيانات الخاصة بالمستخدِمين. وهي تُشكِّل تهديداً متزايداً؛ لأن العديد من الشركات تسمح الآن للموظفين بالوصول إلى شبكات الشركات باستخدام أجهزتهم الشخصية، مما قد يؤدي إلى زيادة فُرَص تهديد بيئة العمل.

وبالفعل شهدت السنوات الأخيرة العديد من مشكلات أمان الأجهزة المحمولة التي تعمل بنظام أندرويد Android، ومع ذلك فإن شركة أبل Apple ليست مُحصَّنة تمامًا ضد البرمجيات الضَّارَّة.

02

الفصل الثاني

حمايـــة بيـانـــات التـطـبـيـقـــــات

- أولاً: **أساليب خرق التطبيقات.**
- ثانياً: **أضرار استخدام التطبيقات المجانية.**
- ثالثاً: **مخاطر إساءة استخدام بيانات الهاتف الجوّال.**
- رابعاً: **علامات وجود برمجيات خبيثة على أجهزة الهواتف.**
- خامساً: **كيفية الحد من مخاطر انتهاك الخصوصية عند استخدام تطبيقات الهواتف المحمولة.**

حماية بيانات التطبيقات

تُعدّ حماية بيانات المُستخدِمين في التطبيقات من أهمّ الأولويات في عالم التكنولوجيا اليوم؛ حيث تتزايد التهديدات الأمنية والهجمات الإلكترونية.

وتتضمَّن إستراتيجيات حماية البيانات مجموعة من الممارسات والتقنيات التي تهدف إلى تأمين المعلومات الشخصية والحسّاسة التي يجمعها التطبيق من مُستخدِميه.

وتشمل هذه الإستراتيجيات ما يلي:

- استخدام تقنيات التشفير؛ لضمان حماية البيانات أثناء نقلها وتخزينها.
- ضبط إدارة الوصول، لتحديد مَن يمكنه الوصول إلى البيانات.
- تفعيل التحقُّق مُتعدّد العوامل؛ لتعزيز الأمان.
- تقديم ضمانات لالتزام التطبيقات بالقوانين والتشريعات المعمول بها.

أولاً: أساليب خرق التطبيقات

يستخدم مجرمو الإنترنت تكتيكات مختلفة لإصابة الأجهزة المحمولة، ومن الأنواع الأكثر شيوعاً:

أدوات الوصول عن بُعد Remote Access Tools

هي أدوات تُوفّر وصولاً واسع النطاق إلى البيانات في الأجهزة المصابة، وغالباً ما تُستخدَم لجمع المعلومات الاستخباراتية، كما يمكنها غالباً الوصول إلى معلومات، مثل: التطبيقات المثبتة، وسجل المكالمات، ودفاتر العناوين، وسجل تصفح الويب، وبيانات الرسائل القصيرة. وكذلك قد تستخدم تلك الأدوات في إرسال رسائل SMS، وتمكين الكاميرا في الأجهزة، وتسجيل بيانات نظام تحديد المواقع العالمي[1].

برمجيات الفدية Ransomware

هي نوع من البرمجيات الخبيثة التي تُستخدَم لمنع المُستخدِم من الوصول إلى بيانات جهازه والمطالبة بدفع فدية، والتي غالباً ما يتم طلب دفعها بعملة البيتكوين المشفّرة لصعوبة تعقُّبها، وبمجرد أن يدفع الضحية الفدية، قد يتم توفير رموز الوصول للسماح له بإلغاء قفل جهازه.

1. Ben Forster, why hackers like your remote access and what you can do about it, Paloalto Networks, Jun 2021. follow link: https://www.paloaltonetworks.com/blog/2021/06/why-hackers-like-your-remote-access/

أحصنة طروادة المصرفية Bank trojans

تأتي في صورة تطبيقات شرعية، وتهدف إلى اختراق المُستخدِمين الذين يقومون بأعمالهم المالية بما في ذلك التحويلات المالية ودفع الفواتير من خلال أجهزتهم المحمولة؛ حيث يسرق هذا النوع من البرمجيات الخبيثة تفاصيل تسجيل الدخول وكلمة المرور[1].

هل تعلم؟

يعود مفهوم حصان طروادة إلى حرب طروادة (1260 - 1180 قبل الميلاد)؛ حيث استخدم اليونانيون حصاناً خشبياً مليئاً بالمقاتلين للوصول إلى مدينة طروادة التركية. واليوم، يُستخدَم نفس الاسم مجازاً لوصف مجموعة متنوّعة من التكتيكات الخبيثة للحصول على حقّ الوصول إلى بيانات المُستخدِمين الآمِنة.

1. Adam Hayes, Banker Trojan: What it Means, How it Works, July 2022. follow link: https://2u.pw/Ys1Bc3lq

برمجيات التعدين المشفرة Cryptomining Malware

تُتيح لمجرمي الإنترنت تنفيذ عمليات حسابية خفية على جهاز الضحية، مما يسمح لهم بإنشاء عملة مشفرة، بواسطة أكواد حصان طروادة مخفية في تطبيقات تبدو شرعية[1].

الاحتيال بالنقرات الإعلانية Advertising Click Fraud Ransomware

هو نوع من البرمجيات الضّارّة التي تسمح لمجرمي الإنترنت بتحقيق دخل مالي من خلال نقرات الإعلانات المزيفة[2].

هل تعلم؟

كشف تقرير عن حالة الاحتيال بالنقرات لعام 2023م، أن الاحتيال بالنقرات كلّف المعلنين ما يقرب من 35.7 مليار دولار في عام 2022م[3].

1. Kurt Baker, What is Mobile Malware?, CROWDSTRIKE, November 2023. Follow link: https: //www.crowdstrike.com/en-us/cybersecurity-101/malware/mobile-malware/
2. Sanja Trajcheva, et al, What is Click Fraud? how it works, examples, and red flags, Cheq, January 2024. follow link: https://cheq.ai/blog/what-is-click-fraud/
3. The State of Fake Traffic 2023. Cheq, follow link: https://cheq.ai/state-of-fake-traffic-2023/

ثانياً: أضرار استخدام التطبيقات المجانية

يدفع مُستخدِمو التطبيقات المجانية على الهواتف المحمولة ثمن استخدامهم لتلك التطبيقات التي تبدو مجانية؛ إلا أن فاتورة الاستخدام باهظة، فقد كشف باحثون أن هناك أعراضاً صحية ونفسية تنتج عن استخدام التطبيقات المجانية، منها: تسويف المهام، والحرمان من النوم، وقلة التركيز؛ حيث تعتمد شركات التكنولوجيا الكبرى على تحليل أنماط السلوك الرقمي للمُستخدِمين لتوجيه الإعلانات المخصَّصة لهم مباشرةً، ما يعني أن انتباه المُستخدِمين هو السلعة التي تستغلها تلك الشركات، فعلى سبيل المثال نجح مُستخدِمو موقع يوتيوب YouTube البالغ عددهم ثلاثة مليارات شخص، في تحقيق عائدات تُقدَّر بنحو 30 مليار يورو شهرياً، من خدمات يُنظَر إليها على أنها مجانية.

احذر!

يدفع مُستخدِمو التطبيقات المجانية على الهواتف المحمولة ثمن استخدامهم لها، فهناك أعراض صحية ونفسية تنتج عن استخدامها؛ منها: تسويف المهام، والحرمان من النوم، وقلة التركيز.

في كثير من الأحيان، يتم جمع البيانات الشخصية للمُستخدِمين من خلال تطبيقات الهاتف الجوّال التي لا تُكلّف المال للتنزيل والتثبيت، لكن أكَّد الباحثون وجود تكاليف مرتبطة بالتطبيقات المجانية، مهما ظهر خلاف هذا. وهي الظاهرة التي أطلق عليها الباحثون اسم "اقتصاد السعر الصفري"، بمعنى أن مُزوّد الخدمة (أو مُقدّم التطبيق المجاني) يُقدّم خدماته في مقابل بيانات المُستخدِم واهتماماته دون تبادل الأموال؛ حيث تستنزف تلك التطبيقات وقت المُستخدِمين[1].

ونأتي إلى تساؤل حول: إلى أين تذهب البيانات الشخصية للمُستخدِمين؟ ومن يمكنه رؤيتها؟

لقد تغيَّر عالَم خصوصية البيانات بشكلٍ كبير؛ فقد تفاقَم الخلاف حول خصوصية التطبيقات، وظهرت مخاوف مشروعة من عدم قدرة العديد من مالكي الهواتف على تحديد التهديدات الحقيقية. وفي تطبيقات الهاتف الجوّال بصفة عامة، تميل الإعلانات إلى اتباع آلية عمل معينة؛ حيث يقوم مُطوّر التطبيق بتضمين جزء من التعليمات البرمجية من مجموعة معينة مختصة بمسألة تطوير البرامج، والتي يمكنها جَمْع جميع أنواع المعلومات، مثل موقع المُستخدِم وبيانات استخدام التطبيق.

1. Linköping University, The hidden costs of free apps – more than personal data, Alpha Galileo, October 2024. follow link: https://www.alphagalileo.org/en-gb/Item-Display/ItemId/250905?returnurl

وطالما لم يقم المُستخدِم بقراءة تفاصيل سياسة الخصوصية، أو بيان شروط الخدمة؛ فإنه لن يُدرك مسألة حدوث عملية جمع البيانات وإرسالها إلى أطراف ثالثة من عدمها.

فمُطوّر التطبيق الذي يسعى لجَنْي الأموال من تطبيقه؛ يقوم بوضع مجموعة من حزم تطوير البرامج الإعلانية المختلفة للاستفادة من أكبر عدد ممكن من الشبكات، دون التحقُّق من ممارسات الخصوصية الخاصة بتلك الشبكات الإعلانية، ما يتسبَّب في أخذ حزم تطوير البرامج جميع البيانات التي تمرّ عبرها عند استخدام التطبيق، وتقوم بجمع البيانات المارَّة، ثم بيعها. ومن خلال استمرارية قيام هذه الكيانات في تمرير بيانات المُستخدِمين ودمجها مع بيانات من شركات أخرى يتم تشكيل صورة واضحة لسلوك المُستخدِم.

احذر!

تؤدي إساءة استخدام بيانات الهاتف الجوّال إلى تغذية الإعلانات المستهدَفة، من خلال جمع وتحليل سلوك المُستخدِمين وأبرز تفضيلاتهم وتفاعلاتهم.

من أكبر المخاطر المحتملة لعملية نقل البيانات هو مَن الذي يمكنه رؤية تلك البيانات، ولسوء الحظ، فإن تحديد هوية تلك الأطراف ليس بالأمر السهل؛ حيث يمكن لأيّ شخص يعمل في الشركة التي تصنع تطبيقاً ما، أو أيّ من الأطراف الثالثة التي يُرسِل إليها التطبيق البيانات، أو حتى الموظفين في الشركة التي تستضيف الخادم الذي يُخزّن البيانات، الوصول إلى بعض أو كل البيانات[1].

ويُعدّ الوضع الوحيد الذي يكون فيه وصول تلك الأطراف الخارجية إلى البيانات مستحيلاً هو عندما يُنفّذ التطبيق عملية التشفير من البداية إلى النهاية بشكل صحيح.

1. Thorin Klosowski, how mobile phones became a privacy battleground, September 2022. follow link: https://www.nytimes.com/wirecutter/blog/protect-your-privacy-in-mobile-phones/

ثالثاً: مخاطر إساءة استخدام بيانات الهاتف الجوّال

من أبرز المخاطر الشائعة التي قد يواجهها المُستخدِمون في حالة إساءة استخدام بيانات الهاتف الجوّال:

سرقة الهوية:

تؤدي إساءة استخدام بيانات الهاتف الجوّال إلى سرقة الهوية؛ حيث يستخدم المجرمون المعلومات الشخصية المسروقة مثل الأسماء والعناوين وغيرها في انتحال هوية الأفراد؛ أو فتح حسابات احتيالية؛ أو إجراء معاملات غير مصرَّح بها.

الاحتيال المالي:

من المخاطر المترتبة على تسرب بيانات الهاتف الجوّال تنفيذ عمليات احتيال مالية بما في ذلك الوصول غير المصرَّح به إلى الحسابات المصرفية والاحتيال على بطاقات الائتمان والقروض؛ حيث يمكن للمجرمين استغلال المعلومات المالية المسروقة في إجراء عمليات شراء غير مصرَّح بها أو استنزاف الحسابات المصرفية.

احذر!

من المخاطر المترتبة على تسرُّب بيانات الهاتف الجوّال: تنفيذ عمليات احتيال مالية، بما في ذلك الوصول غير المصرَّح به إلى الحسابات المصرفية، واستغلال المعلومات المالية المسروقة في إجراء عمليات شراء غير مصرَّح بها أو استنزاف الحسابات المصرفية.

انتهاكات الخصوصية:

تُعدّ أحد أبرز المخاطر الناتجة عن إساءة استخدام بيانات الهواتف مِن قِبَل المجرمين، ويتم ذلك عن طريق جمع المعلومات الحسّاسة دون موافقة المُستخدِم، وتتبُّع مواقعه، ومراقبة أنشطته عبر الإنترنت، والوصول إلى اتصالاته؛ ما يعني وقوع المُستخدِم تحت المراقبة طول الوقت.

الإضرار بالسُّمعة:

تصل المخاطر في بعض الأحيان إلى حدّ الكشف عن بيانات حساسة غير مصرَّح بنشرها، ما يتسبَّب في الإضرار بسُمعة الأفراد، مثل: نشر محتوى الرسائل الخاصة أو الصور الشخصية أو مقاطع الفيديو، ما يُعرِّض المُستخدِمين إلى خطر الإساءة والابتزاز الإلكتروني.

احذر!

تصل المخاطر في بعض الأحيان إلى حد الكشف عن بيانات حساسة غير مصرَّح بنشرها؛ ما يتسبَّب في الإضرار بسُمْعة الأفراد، مثل: نشر محتوى الرسائل الخاصة، أو الصور الشخصية، أو مقاطع الفيديو.

الإعلان المستهدف والتلاعب بالمُستخدِم:

تؤدي إساءة استخدام بيانات الهاتف الجوّال إلى تغذية الإعلانات المستهدفة وتكتيكات التلاعب بالمُستخدِمين؛ من خلال جمع وتحليل سلوكهم وأبرز تفضيلاتهم وتفاعلاتهم، وهو ما يُمكِّن المجرمين أو المعلنين غير الأخلاقيين من إنشاء إعلانات مخصَّصة مُوجَّهة لفئة معينة من المُستخدِمين، ما يعني التلاعب بخيارات المُستخدِمين وقراراتهم.

هجمات الهندسة الاجتماعية:

فيما يُعرَف باسم "التصيد الاحتيالي"، أو "الهندسة الاجتماعية"؛ يقوم مجرمو الإنترنت بصياغة وإرسال رسائل خادعة إلى ضحاياهم، لدفعهم إلى الكشف عن البيانات الحسّاسة، مثل أسماء المُستخدِمين، وكلمات المرور، وتفاصيل بطاقات الائتمان. وعندما يكون هناك تصوُّر حول المُستخدِم فإنه يُمكن لمجرمي الإنترنت تخصيص رسائل التصيد الاحتيالي لجذب المزيد من الاهتمام أو الإشارة بشكل مخادع لنيل ثقة المُستخدِمين، وبالتالي زيادة فعالية الهجوم. علماً بأن هجمات التصيد الاحتيالي لا تصيب الأفراد فحسب، بل يمكن أن تصيب الشركات الكبرى من خلال موظفيها، وكذلك المؤسسات الحكومية. وقد صنَّف الإنتربول الهندسة الاجتماعية واحدة من اتجاهات الاحتيال الناشئة في العالم[1].

احذر!

يقوم مجرمو الإنترنت بصياغة وإرسال رسائل خادعة إلى ضحاياهم؛ لدفعهم إلى الكشف عن البيانات الحسّاسة، مثل: أسماء المُستخدِمين، وكلمات المرور، وتفاصيل بطاقات الائتمان.

1. Jacob Leon Kröger, how data can beused against people:a classification of personal data misuses, December 2021. follow link: https://linksshortcut.com/KGJvq

رابعاً: علامات وجود برمجيات خبيثة على أجهزة الهواتف

- رؤية إعلانات منبثقة عشوائية أو تطبيقات جديدة؛ فأغلب الإعلانات المنبثقة لا تحمل برمجيات خبيثة، ولكنها تُستخدَم فقط كأدوات تسويقية. ومع ذلك، إذا وجد المُستخدِم أنه يُغلق نوافذ الإعلانات المنبثقة أكثر من المعتاد؛ فهذا يشير إلى وجود برمجية ضارَّة على الهاتف[1].
- في حالة وجود تطبيقات على الجهاز لم يقم المُستخدِم بتنزيلها أو تثبيتها، ينبغي على الفور إلغاء تثبيتها، واستخدام برامج مكافحة الفيروسات لفحص الجهاز.
- ارتفاع حرارة الهاتف، فأجهزة الهواتف المحمولة لم تُصمَّم لدعم البرمجيات الضّارَّة، وعند تنزيل تطبيق يتضمَّن برمجية ضارَّة عن طريق الخطأ؛ فإن الجهاز يعمل بجهد أكبر لمواصلة عمله مما يتسبَّب في رفع درجة حرارته.
- إرسال رسائل بريد عشوائية أو رسائل عبر وسائل التواصل الاجتماعي تتضمَّن روابط أو ملفات مجهولة إلى جهات اتصال المُستخدِم. ومن الأفضل إخبار جميع المستلمين بأن الهاتف تم اختراقه حتى لا يقوموا بتنزيل أيّ برمجيات ضارَّة بأنفسهم أو إعادة توجيه هذه الروابط إلى أيّ شخص آخر.

1. 7 Signs Your Phone Has a Virus and What You Can Do, Mcafee, August 2022. follow link: https: //www.mcafee.com/blogs/mobile-security/7-signs-your-phone-has-a-virus-and-what-you-can-do/

- بطء استجابة الهاتف بشكلٍ غير عادي، والسبب أن الجهاز يحتاج إلى العمل بجهد أكبر لدعم الفيروس الذي تم تنزيله. كما أن التطبيقات غير المألوفة تشغل مساحة تخزين وتشغل مهامّ في الخلفية؛ مما يتسبَّب في بطء تشغيل الهاتف.
- وجود رسوم احتيالية على الحسابات، مما يستدعي متابعة المُستخدِم لحساباته المصرفية بانتظام ومراجعة كشوف الحساب لرصد أيّ عمليات شراء تمَّت دون عِلْمه.
- استخدام بيانات الهاتف بشكلٍ لافتٍ؛ فالارتفاع المفاجئ في استخدام البيانات أو فاتورة الهاتف هو مُؤشِّر على وجود برمجيات ضارَّة تقوم بتشغيل عمليات في الخلفية أو استخدام اتصال الإنترنت لنقل البيانات خارج جهاز المُستخدِم لأغراض ضارَّة.
- استنزاف البطارية بسرعة غير عادية.

احذر!

استنزاف البطارية بسرعة غير عادية، وارتفاع حرارة الهاتف، ووجود رسوم احتيالية على الحسابات؛ جميعها علامات على وجود برمجيات ضارَّة على أجهزة الهواتف.

خامساً: كيفية الحدّ من مخاطر انتهاك الخصوصية عند استخدام تطبيقات الهواتف المحمولة

لا يمكن منع التطبيق من جمع بيانات المُستخدِمين طالما أنها موجودة على هواتفهم.

ومع ذلك، يمكن تقليل المخاطر الناجمة عن ذلك من خلال اتباع ما يلي:

- الالتزام بتنزيل التطبيقات من مصادر موثوقة مثل متجر أبل App Store، ومتجر جوجل Google Play.
- التحقُّق من المراجعات أولاً قبل تنزيل التطبيقات، وفي حال وجد تقييمات سلبية حول أذونات الوصول، ينبغي التراجع عن قرار تنزيل التطبيق.
- الانتقال إلى الإعدادات والتحقُّق من أذونات التطبيق جيداً، وإزالة الأذونات التي تُهدِّد خصوصية البيانات.
- التفكير جيداً قبل مَنْح أيّ مُوافقة عند استخدام التطبيقات.
- عدم ربط التطبيق بالحساب الشخصي مثل البريد الإلكتروني، أو رقم الهاتف، أو حساب المنصات الاجتماعية لتجنُّب مشاركة البيانات الشخصية بين الأطراف.
- استخدام الشبكات الافتراضية الخاصة (VPN) يساعد في حماية البيانات من خلال تشفير اتصال الإنترنت، وإخفاء عنوان IP الخاص بالمُستخدِم.

- تجنُّب استخدام شبكات Wi-Fi العامَّة للوصول إلى المعلومات الحسّاسة، فقد لا تكون آمِنَة.
- استخدام متصفّح آمِن يحظر أدوات التتبُّع والإعلانات، مما يساعد في حماية البيانات.
- من أبسط احتياطات السلامة الرقمية: تفعيل قفل الشاشة الرئيسية، فقد أظهر تقرير صادر عن مركز بيو عام 2017م، أن ما يقرب من 30% من مالكي الهواتف الذكية لا يستخدمون قفل الشاشة أو ميزات الأمان الأخرى للوصول إلى هواتفهم. رغم أن مثل هذه الأخطاء تؤدي إلى جعل المُستخدِمين فريسة لانتهاكات الأمن السيبراني، ومن بينها سرقة بيانات شخصية وكلمات المرور[1].

احذر!

يُعدّ غَلْق نوافذ الإعلانات المنبثقة أكثر من المعتاد مؤشراً على وجود برمجية ضارَّة على الهاتف.

هل تعلم؟

كشفت صحيفة فايننشال تايمز Financial Times أن سياسة الخصوصية التي انتهجتها شركة أبل Apple للتأكد من شفافية تتبُّع التطبيقات لبيانات المُستخدِمين تتسبَّب في خسارة المنصات الاجتماعية حوالي 10 مليارات دولار سنوياً[2].

1. Stephanie Taylor, 10 ways to make your phone safer, September 2011. follow link: https://linksshortcut.com/fUmGE
2. Anna Yaskiv, App Tracking Transparency: what Data do Apps Collect and why?, January 2022. follow link: https://linksshortcut.com/xXsmi

التمارين تعتمد على المادة العلمية المقدَّمة في سياق هذا الكتيب، وهي مذكورة هنا بدون حلّ، وتم إرفاق الحل في نهاية الكُتَيِّب.

التمرين الأول

ما هــي؟

1. نوع من البرمجيات الخبيثة التي تُستخدَم لمنع المُستخدِم من الوصول إلى جهازه مقابل مبلغ مالي، غالباً ما يتم دَفْعه بعملة البيتكوين المشفرة.

2. هي برمجيات تتيح لمجرمي الإنترنت تنفيذ عمليات حسابية خفية على جهاز الضحية بواسطة أكواد حصان طروادة مخفية في تطبيقات تبدو شرعية.

3. نوع من البرمجيات الضّارَّة التي تسمح لمجرمي الإنترنت بتحقيق دخل مالي من خلال نقرات المُستخدِمين.

4. هجمات تعتمد على تسرُّب بيانات الهاتف الجوّال للوصول غير المصرَّح به إلى الحسابات المصرفية وإجراء عمليات شراء غير مُصرَّح بها.

5. من خلال تقنيات احتيالية يقوم مجرمو الإنترنت بصياغة وإرسال رسائل خادعة إلى ضحاياهم؛ لدفعهم إلى الكشف عن البيانات الحسّاسة. علماً بأن هذه الهجمات لا تصيب الأفراد فحسب، بل يمكن أن تصيب الشركات الكبرى من خلال موظفيها.

التمرين الثاني

اكتب كلمة (صحيح) أمام العبارات الصحيحة، وكلمة (خطأ) أمام العبارات الخاطئة، وصحح الخطأ إن وجد:

1. بناءً على سلوكيات مُستخدِمي التطبيقات فإن جهات نقل البيانات يمكنها تحديد موقع المُستخدِم واهتماماته. (.....)

.....

2. بعض تطبيقات الهواتف تجمع بيانات المُستخدِمين لعرض إعلانات الشركات الراغبة في الإعلان عن منتجاتها أو خدماتها. (.....)

.....

3. ليس من بين البيانات التي تجمعها تطبيقات الهاتف: بيانات طراز جهاز المُستخدِم وإصدار نظام التشغيل ونوع المتصفّح. (.....)

.....

4. تحظر تطبيقات التجارة الإلكترونية جمع معلومات مثل أرقام بطاقات الائتمان وعناوين الفواتير. (.....)

.....

5 تتضمَّن البيانات التي يتم جمعها بواسطة أطراف ثالثة من خلال تطبيقات الهواتف المحمولة أي شيء من معلومات الملف الشخصي مثل العمر وتفاصيل الموقع. (.....)

.....

6 بعض مُطوّري التطبيقات قد يقومون ببيع بيانات مُستخدِمي تطبيقاتهم إلى شركات أبحاث السوق. (.....)

.....

7 بيانات تصفُّح التطبيقات تُساعد المؤسسات على تحديد العملاء المستهدَفين بشكلٍ أفضل، والتواصل معهم، والتعرُّف على مطالبهم، وإيجاد حلول لها. (.....)

.....

8 تتجنّب التطبيقات الوصول إلى ملفات تعريف المُستخدِم على وسائل التواصل الاجتماعي، بما في ذلك قوائم الأصدقاء. (.....)

.....

التمرين الثالث

أكمل العبارات التالية

1. ..... يُقصَد بها الشركات التي تشتري وتبيع البيانات الشخصية، والذين بدَوْرهم يبيعونها إلى شركات أخرى.
2. ..... من وظائفها الاستفادة من بيانات مُستخدِمي التطبيقات من أجل فهم سلوكهم وتحسين ميزات التطبيق وكفاءته.
3. من عوامل التهديد الموجودة في الاتصالات غير الآمِنَة ..... ، ..... ، .....
4. ..... هي برمجيات متطفّلة مصمَّمة خصيصاً لاستهداف الهواتف الذكية والأجهزة اللوحية، بهدف الوصول إلى البيانات الخاصَّة.
5. ..... تستخدم تلك الأدوات في إرسال رسائل SMS، وتمكين الكاميرا في الأجهزة، وتسجيل بيانات نظام تحديد المواقع العالمي (GPS).

حلّ التمارين والتدريبات

السؤال

التمرين الأول: ما هي؟

الإجابة

1. برمجيات الفدية.
2. برمجيات التعدين المشفرة.
3. الاحتيال بالنقرات الإعلانية.
4. الاحتيال المالي.
5. هجمات الهندسة الاجتماعية.

السؤال

اكتب كلمة (صحيح) أمام العبارات الصحيحة، وكلمة (خطأ) أمام العبارات الخاطئة، وصحح الخطأ إن وجد:

الإجابة

1. صحيح.
2. صحيح.
3. خطأ؛ بل تُعدّ من البيانات التي يتم جمعها.
4. خطأ؛ تتّجه تطبيقات التجارة الإلكترونية إلى جمع معلومات الدفع، مثل أرقام بطاقات الائتمان، وعناوين الفواتير، وسجل المعاملات لمعالجة المشتريات وإدارة الحسابات.
5. صحيح.
6. صحيح.
7. صحيح.
8. خطأ؛ عادة تطلب التطبيقات الوصول إلى ملفات تعريف المُستخدِم على وسائل التواصل الاجتماعي، وكذلك قوائم الأصدقاء، وغيرها من معلومات يمكن استخدامها في الإعلانات المستهدَفة.

السؤال

التمرين الثالث: أكمل العبارات التالية

الإجابة

1. سماسرة البيانات Data Brokers.
2. شركات أبحاث السوق.
3.
   - البرمجيات الضّارَّة على الجهاز المحمول.
   - شبكة Wi-Fi غير آمِنَة أو مخترقة مِن قِبَل مجرمي الإنترنت.
   - شركة الاتصالات أو أجهزة الشبكة.
4. البرمجيات الخبيثة للأجهزة المحمولة.
5. أدوات الوصول عن بُعْد.

المراجع

1. How Mobile Apps Collect Your Data And What You Should Do, December 2022. follow link: https://ready.io/blog/how-mobile-apps-collect-your-data
2. Aliya Ram, et al, How smartphone apps track users and share data, October 2018. follow link: https://ig.ft.com/mobile-app-data-trackers/
3. https://support.google.com/googleplay/android-developer/answer/10787469?hl=en
4. Mahesh Atapattu, Mobile Application Data Collection and Data Sharing: What You Need to Know, July 2023. follow link: https://www.linkedin.com/pulse/mobile-application-data-collection-sharing-what-you-need-atapattu/
5. McClain, Colleen,et al, How Americans View Data Privacy, PEW, October 2023, follow link: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

6. M3: Insecure Communicatio, Clouddefense, follow link: https://www.clouddefense.ai/owasp/2016/3

7. mobile app security risks and how to mitigate them, Cypress Data Defense, July 2020. follow link: https://2u.pw/PKH0B660

8. Twingate Team, what happened in the park mobile data breach?. Twingate, may 2024, follow link: https://www.twingate.com/blog/tips/park-mobile-data-breach

9. Ben Forster, why hackers like your remote access and what you can do about it, Paloalto Networks, Jun 2021. follow link: https://www.paloaltonetworks.com/blog/2021/06/why-hackers-like-your-remote-access/

10. Adam Hayes, Banker Trojan: What it Means, How it Works, July 2022. follow link: https://2u.pw/Ys1Bc3Iq

11. Kurt Baker, What is Mobile Malware?, CROWDSTRIKE, November 2023. Follow link: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/mobile-malware/

12. Sanja Trajcheva, et al, What is Click Fraud? how it works, examples, and red flags, Cheq, January 2024. follow link: https://cheq.ai/blog/what-is-click-fraud/

13. The State of Fake Traffic 2023. Cheq, follow link: https://cheq.ai/state-of-fake-traffic-2023/

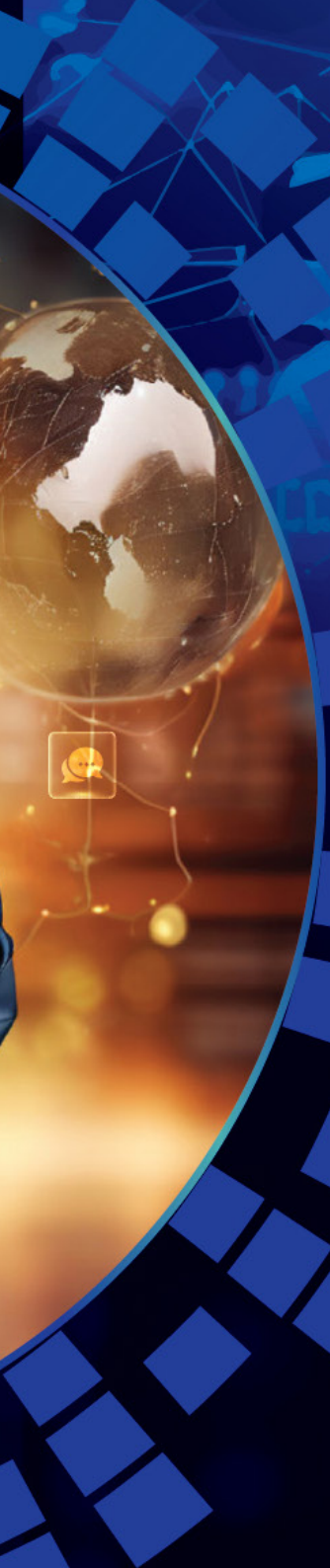
14. Linköping University, The hidden costs of free apps – more than personal data, Alpha Galileo, October 2024. follow link:https://www.alphagalileo.org/en-gb/Item-Display/ItemId/250905?returnurl

15. Jacob Leon Kröger, how data can beused against people:a classification of personal data misuses, December 2021. follow link: https://linksshortcut.com/KGJvq

16. 7 Signs Your Phone Has a Virus and What You Can Do, Mcafee, August 2022. follow link: https://www.mcafee.com/blogs/mobile-security/7-signs-your-phone-has-a-virus-and-what-you-can-do/

17. Stephanie Taylor, 10 ways to make your phone safer, September 2011. follow link: https://linksshortcut.com/fUmGE

18. Anna Yaskiv, App Tracking Transparency: what Data do Apps Collect and why?, January 2022. follow link: https://linksshortcut.com/xXsmi



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنية للسلامة الرقمية
Digital Safety National Initiative