خبراء يكشفون عن 3 ميزات في هواتف أندرويد يجب تجنبها لردع الاختراق

حذر خبراء أمن الإنترنت من ثلاث ميزات متوفرة على أجهزة "أندرويد"، يجب تجنبها للحفاظ على جهازك آمنا من المجرمين.

وميزات "أندرويد" هذه متاحة للجميع، لكن تطبيقها متروك لمالك الجهاز. وتم تسليط الضوء على الميزات الثلاث الخطيرة من قبل خبراء التكنولوجيا في شركة أمن الكمبيوتر "كاسبرسكي" (Kaspersky).

ولتجنب اختراق جهاز "أندرويد"، ستحتاج إلى تجنب استخدام ميزة إمكانية الوصول، وعدم تنزيل تطبيقات غير معروفة، وعدم منح حقوق المستخدم المتميز لجهازك.

وفيما يلي تفصيل للميزات الثلاث الخطيرة:

أولا، تم إنشاء ميزة إمكانية الوصول (feature accessibility) لمساعدة الأشخاص الذين يعانون من إعاقات بصرية شديدة في التنقل بشكل أفضل على أجهزة "أندرويد" الخاصة بهم.

وتستخدم هذه الميزة تطبيقا خاصا يقرأ النص بصوت عال ويستجيب للأوامر الصوتية. ويمكنها أيضا التحكم في الأقسام أو النقر عليها.

ولكن هذا قد يكون خطيرا، لأن التطبيقات الضارة يمكنها أن تطلب إذنا للوصول إلى هذه الميزة والتحكم في الجهاز.

ثانيا، عدم تثبيت تطبيقات غير معروفة (apps unknown installing) يمكن أن تأتي من جهات خارجية أو تم تغييرها من الإصدار الأصلي.

ويمكن أن تأتي هذه التطبيقات مع عدد كبير من المشكلات، لأنه يمكن ترميزها بأي شيء بما في ذلك البرامج الضارة.

وإذا قمت بتنزيل تطبيق غير رسمي، فقد يأتي مع ميزات غير رسمية والتي يمكن أن تمنح المحتالين على الإنترنت إمكانية الوصول المباشر إلى جهازك.

ويمكن للمجرم الإلكتروني عادة إرسال برامج ضارة إلى جهازك من خلال التطبيق أو محاولة الوصول إلى بياناتك من خلال التطبيق أيضا.

ثالثا، الحصول على حقوق المستخدم المتميز (rights superuser) على جهاز "أندرويد" التي تمنح المستخدم امتيازات فريدة للغاية في التحكم الكامل في النظام.

وبمعنى آخر، فإن الحصول على حقوق المستخدم المتميز هو عملية اختراق يقوم بها الشخص بنفسه لنظام التشغيل الخاص بهاتفه الذكي.

وسيحتوي جهاز "أندرويد" من خلال هذه الميزة على حسابات مميزة للغاية يتم استخدامها بشكل أساسي للإدارة من قبل موظفي تكنولوجيا المعلومات المتخصصين. ولكن يمكن أيضا أن يؤدي ذلك إلى التخلص من الضمان والتسبب في تلف الجهاز.