禪

لزوم توجه به نکات پایه امنیت در سیستمعاملهای همراه

10 نکته امنیتی برای محافظت از حریم خصوصی گوشیهای اندرویدی

کاربران از گوشیهای اندرویدی بیشتر از لپتاپها استفاده میکنند، با این وجود در شرایطی که کاربران به خوبی نکات امنیتی لپتاپها را رعایت میکنند، در مورد گوشیهای اندرویدی چندان به مبحث امنیت توجهی ندارند و بیشتر آنها یک جمله آشنا به زبان میآورند : «مگر فرد مهمی هستم که هکرها بخواهند گوشی اندرویدی من را هک کنند !» برخی دیگر نیز به دلیل اینکه تولیدکنندگان گوشیهای همراه در بازههای زمانی مختلف وصلههای امنیتی را برای اندروید ارائه میکنند نسبت به رعایت نکات امنیتی چندان حساس نیستند. هکرها از همین غفلت کاربران سوء استفاده میکنند تا روزنهای در گوشیهای اندرویدی برای دسترسی به اطلاعات حساس پیدا کنند . برای آنکه از گزند هکرها در امان بمانید و شانس هکرها برای دسترسی به اطلاعات شخصی ذخیره شده روی گوشی را کم کنید لازم است به یکسری نکات امنیتی ساده و ابتدایی دقت کنید .

1. از یک برنامه مدیریت گذرواژهها استفاده کنید

Dashlane 1Password Enpass .

2.

[illegible] iOS [illegible] «apk» [illegible] SlideMe [illegible] Getjar [illegible].

3. [illegible] 1234 [illegible]





استدلالهای مختلفی در ارتباط با استفاده یا عدم استفاده از حسگر اثر انگشت به عنوان اصلیترین مکانیزم امنیتی وجود دارد . برخی مدعی هستند که اثرانگشت به اندازه گذرواژه یا پینکد ایمن نیست و شما میتوانید یک حسگر اثرانگشت را به سادگی شکست دهید. اگر قصد دارید از پینکدهای دیجیتالی روی گوشی خود استفاده کنید، نباید از یک پینکد ساده همچون 1111 یا 1234 استفاده کنید . در مورد قفلهای الگوی تصویری نیز همین مسئله صادق است. اگر بیش از اندازه ساده باشند، قدرتمند نیستند . باید میان پیچیدگی و سهولت در تایپ و یادآوری تعادلی برقرار کنید تا هر زمان که نیاز داشتید با کمترین زحمت ممکن به گوشی دسترسی داشته باشید.

مطلب پیشنهادی

عکسبرداری حرفهای با بهترین کیفیت ممکن

12 ترفند چالب و کاربردی دوربین گوشیهای اندرویدی

4. از وایفای عمومی برای انتقال دادههای حساس استفاده نکنید

در شهرهای بزرگ، ارائهدهندگان خدمات اینترنتی اقدام به ارائه وایفای عمومی میکنند که به سختی میتوان در مقابل دسترسی به یک انتخاب رایگان مقاومت کرد . بیشتر کارشناسان امنیتی توصیه میکنند برای حفظ امنیت بهتر است تحت هیچ شرایطی به وایفای عمومی متصل نشوید. در یک شبکه وایفای عمومی انواع مختلفی از حملات در کمین کاربران هستند تا دادههای ذخیره شده در گوشی و اطلاعات مالی را به سرقت ببرند. یک هکر برای حمله به یک گوشی همراه از طریق یک وایفای عمومی به نبوغ چندان خاصی نیاز ندارد . اگر هنوز هم دوست دارید از وایفای عمومی برای وبگردی استفاده کنید، مطمئن شوید که از سایتهایی که با پروتکل https محافظت شدهاند بازدید میکنید . تحت هیچ شرایطی جزئیات کارت اعتباری یا بانکی خود را با وایفای عمومی ارسال نکنید . ممکن است تمامی وبسایتهای بانکی ایمن باشند، اما در یک شبکه وایفای عمومی این مکانیسمهای امنیتی نمیتواند از شما در برابر حمله مرد میانی محافظت کنند .

مطلب پیشنهادی

Wi-Fi

ارتباط بهتر گوشیهای اندرویدی با وایفای

15 تکنیک و ترفند چالب وایفای برای گوشیهای اندرویدی

5- از یک شبکه خصوصی مجازی استفاده کنید

یک شبکه خصوصی مجازی در زمان ورود به اینترنت یک لایه محافظ اضافی پیرامون وبگردی قرار میدهد و تمامی اطلاعات ارسالی را میان گوشی و سرور مربوطه رمزگذاری میکند . عملکرد یک شبکه خصوصی مجازی ساده است. شبکه خصوصی مجازی به ویژه زمانی که قصد استفاده از یک وایفای عمومی را دارید از اطلاعات شخصی در برابر شنود محافظت میکند.

6. [illegible]

[illegible] Settings > Security & Lock Screen > Security Update [illegible]

7. [illegible]

[illegible] My Apps & Games [illegible] Updates [illegible] (Auto updates) [illegible] Settings > [illegible] Auto Update [illegible] update Apps [illegible].

[illegible]

[illegible]

8- حذف جميع البيانات من الجهاز عن بعد

حذف جميع البيانات من الجهاز عن بعد هي ميزة مهمة تتيح للمستخدمين حماية بياناتهم الشخصية في حالة فقدان الجهاز أو سرقته. تعمل هذه الميزة عن طريق إرسال أمر إلى الجهاز عبر الإنترنت، مما يؤدي إلى مسح جميع البيانات المخزنة عليه، بما في ذلك الصور والرسائل وجهات الاتصال والتطبيقات. يمكن تفعيل هذه الميزة من خلال إعدادات الجهاز أو من خلال تطبيقات خاصة مثل Find My Device. من المهم تفعيل هذه الميزة مسبقًا قبل فقدان الجهاز، حيث لا يمكن تفعيلها بعد ذلك. بعد تفعيل هذه الميزة، يمكن للمستخدم إرسال أمر الحذف من أي جهاز آخر متصل بالإنترنت، مثل جهاز كمبيوتر أو جهاز لوحي آخر. يجب أن يكون المستخدم على دراية بأن هذه العملية لا رجعة فيها، وأن جميع البيانات المحذوفة لا يمكن استعادتها.

9. تتبع الجهاز عن بعد على خرائط جوجل

يتيح تطبيق Find My Phone على أجهزة أندرويد تتبع موقع الجهاز على خرائط جوجل في حالة فقدانه أو سرقته. يمكن للمستخدم تسجيل الدخول إلى حسابه على Google من أي جهاز آخر، ثم عرض موقع الجهاز على الخريطة. يمكن أيضًا تشغيل صوت على الجهاز لمدة 5 دقائق حتى لو كان على وضع الصامت، مما يساعد في العثور عليه إذا كان قريبًا. بالإضافة إلى ذلك، يمكن قفل الجهاز عن بعد وتسجيل الخروج من حساب Google، أو مسح جميع البيانات الموجودة على الجهاز. يمكن العثور على هذه الخيارات في قسم Security & Lock screen في إعدادات الجهاز. من المهم تفعيل Find My Phone مسبقًا.

تطبيقات مفيدة

تطبيقات مفيدة يمكن أن تساعد في حل بعض المشكلات

10. [illegible]

[illegible] Kaspersky Internet Security [illegible]

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]
[illegible]
[illegible]:
06:25 - 13/10/1398
[illegible]:
[illegible]

[illegible]
[illegible]:https://www.shabakeh-mag.com/mobile-tricks/android-tricks/16429/10-%D9%86%DA%A9%D8%AA%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AD%D8%B1%DB%8C%D9%85-%D8%AE%D8%B5%D9%88%D8%B5%DB%8C-%DA%AF%D9%88%D8%B4%DB%8C%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C