گوشی شما چقدر ایمن است؟

گوشی هوشمند شما در واقع یک «جاسوس در جیب شما» است که خودتان پولش را داده اید.
این چک لیست کمک میکند تا دهان این جاسوس را تا حد ممکن ببندید. این ۱۲ مورد را بررسی کنید به هر مورد که رعایت شده بود ۱ امتیاز بدهید.

درنا
دفتر راهبردی نجات ایران
www.dornairan.com

قفل صفحه:
خداحافظی با بیومتریک

آیا هنوز از اثر انگشت یا تشخیص چهره FaceD استفاده میکنید؟

خطر: در یک بازداشت یا زورگیری میتوانند به زور انگشت شما را روی گوشی بگذارند یا گوشی را جلوی صورتتان بگیرند اما نمیتوانند ذهن شما را بخوانند. هنوز!

اقدام: بیومتریک را خاموش کنید از یک رمز عبور ترکیبی عدد و حروف حداقل ۶ رقمی استفاده کنید. الگو Pattern هم ناامن است چون رد چربی انگشت روی صفحه میماند.

۲

نمایشگر اعلانها
Lock Screen Previews

آیا وقتی گوشی قفل ،است پیامک ها یا پیام های واتس اپ روی صفحه دیده میشوند؟

خطر: کسی که گوشی شما را بدزدد یا فقط روی میز ببیند، کدهای تایید دو مرحله ای OTP یا پیامهای خصوصی را میخواند.

اقدام: در تنظیمات Notifications گزینه Show Preview را روی Never یا When Unlocked بگذارید.

۳

مجوزهای دسترسی
App Permissions

آیا اپلیکیشن چراغ قوه به مخاطبین یا موقعیت مکانی دسترسی دارد؟

خطر: بدافزارها و آپهای جاسوسی در قالب برنامه های ساده پنهان میشوند.

اقدام: به بخش Privacy > Permission Manager بروید و دسترسی های میکروفون، دوربین و موقعیت مکانی را چک کنید هر چیز غیر منطقی را قطع کنید.

۴

مکانهای مهم
Significant Locations

این ترسناکترین بخش گوشی است.

خطر: گوشی آیفون و اندروید به صورت پیش فرض دقیقاً میدانند شما کجا زندگی میکنید، کجا کار میکنید و ساعت چند به خانه دوستتان میروید.

اقدام آیفون:

Settings > Privacy > Location Services
>System Services > Significant Locations

سپس خاموش کنید و تاریخچه را پاک کنید.

اقدام اندروید:

Google Maps > Settings > Personal Content > Location History سپس خاموش یا Pause کنید.

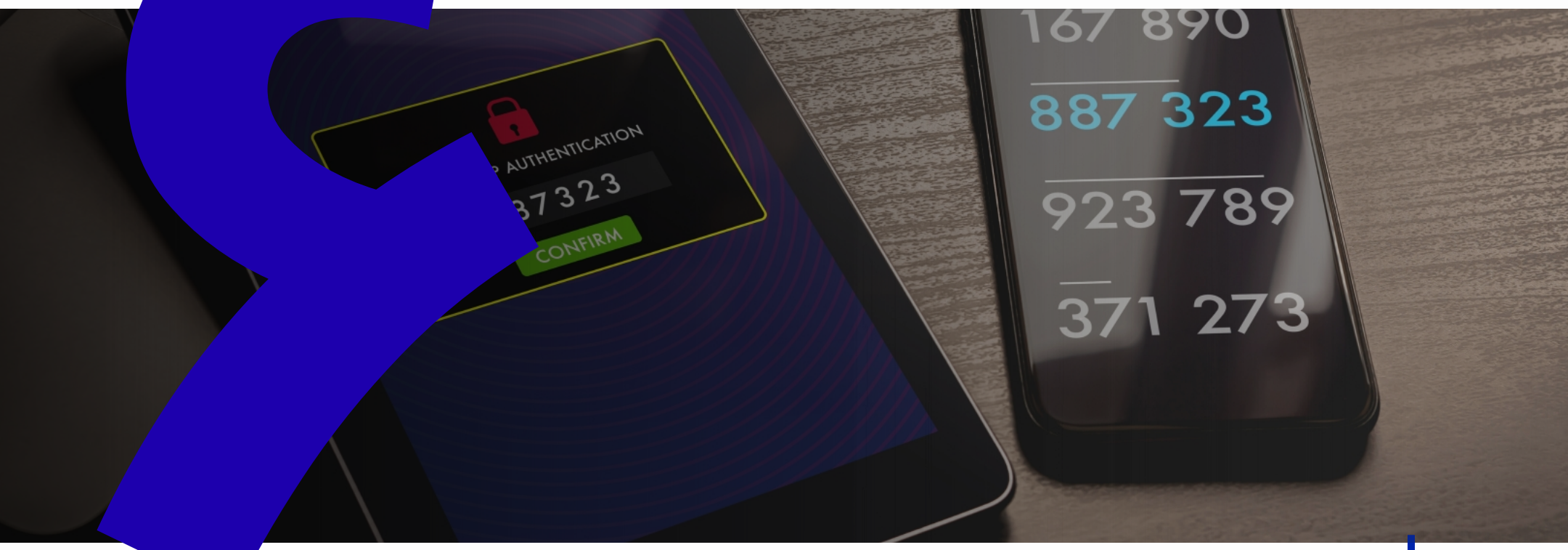
۵

اتصال خودکار وای‌فای
Auto-Join Wi-Fi

آیا وای‌فای شما همیشه روشن است و به شبکه‌های آشنا وصل می‌شود؟

خطر: دستگاه‌های جاسوسی (Pineapple) می‌توانند نام وای‌فای خانه شما را جعل کنند. گوشی شما گول می‌خورد، وصل می‌شود و تمام ترافیکتان شنود می‌شود.

اقدام: گزینه Auto-Join را برای شبکه‌های عمومی خاموش کنید. گزینه Ask to Join Networks را فعال کنید.



احراز هویت دو مرحله‌ای 2FA

آیا برای ورود به اینستاگرام یا جیمیل فقط رمز عبور دارید؟
یا کد را با SMS می‌گیرید؟

خطر: SMS قابل رهگیری است (Sim Swap).

اقدام: SMS را فراموش کنید.
از اپلیکیشن‌های تولید رمز مثل
Google Authenticator یا Raivo (برای آیفون) استفاده کنید.

۷

نام بلوتوث و هات‌اسپات

آیا اسم بلوتوث شما
“Ali’s iPhone” یا “Samsung S22” است؟

خطر: شما در مکان‌های عمومی داد می‌زنید:
«من علی هستم و گوشی گران‌قیمت دارم!»
این کار ردیابی شما را آسان می‌کند.

اقدام: نام دستگاه را به چیزی عمومی و گمراه‌کننده تغییر دهید.
مثلاً: HUAWEI-Y300
(بگذارید دزدها فکر کنند گوشی شما بی‌ارزش است)

مرورگر امن

آیا هنوز از کروم یا سافاری بدون تنظیمات استفاده می‌کنید؟

خطر: آن‌ها تمام رفتار شما را رصد می‌کنند تا تبلیغات نشان دهند.

اقدام: از مرورگر Brave یا Firefox Focus استفاده کنید.
اگر Chrome دارید، موتور جستجو را از Google به DuckDuckGo تغییر دهید.

شناسه تبلیغاتی Advertising ID

هر گوشی یک کد منحصربه‌فرد دارد که شرکت‌های تبلیغاتی با آن شما را می‌شناسند.

خطر: ساخت پروفایل دقیق از علایق و حتی بیماری‌های شما.

اقدام آیفون:
Privacy > Tracking
تیک Allow Apps to Request to Track را بردارید.

اقدام اندروید:
Settings > Google > Ads
گزینه Delete advertising ID را بزنید.

پشتیبان‌گیری ابری
Cloud Backups

آیا عکس‌هایتان خودکار در iCloud یا Google Photos آپلود می‌شود؟

خطر: اگر اکانت شما هک شود یا حکم قضایی برای اپل/گوگل صادر شود،تمام زندگی شما در دسترس است.

اقدام:
برای چیزهای خیلی حساس، بک‌آپ لوکال (روی هارد کامپیوتر) بگیرید.
Sync ابری را برای عکس‌های حساس خاموش کنید.

دکمه وحشت 🚨
Emergency Lockdown

اگر پلیس یا سارق به سمت شما بیاید، چطور در ۱ ثانیه گوشی را غیرقابل نفوذ می‌کنید؟

آیفون:
۵ بار پشت سر هم دکمه پاور را بزنید،(یا پاور + ولوم بالا را نگه دارید). بیومتریک غیرفعال می‌شود و فقط رمز کار می‌کند.
اندروید:
گزینه Show Lockdown Option را در تنظیمات قفل صفحه فعال کنید. با نگه داشتن پاور، گزینه Lockdown می‌آید و اثر انگشت کار نمی‌کند.

۱۲

به‌روزرسانی Updates

آیا آپدیت‌ها را به تعویق می‌اندازید؟

خطر: هکرها از حفره‌های امنیتی قدیمی که پچ نشده‌اند وارد می‌شوند.

اقدام:
بسیستم عامل و اپلیکیشن‌ها را همین الان آپدیت کنید.
گزینه Automatic Updates را روشن بگذارید.

همین الان گوشی خود را دست بگیرید و این ۱۲ مورد را بررسی کنید و به هر مورد که رعایت شده بود ۱ امتیاز بدهید.

۱	🔒 بیومتریک	
۲	👁️ نمایشگر اعلان‌ها	
۳	✋ مجوزهای دسترسی	
۴	📍 مکان‌های مهم	
۵	📡 اتصال خودکار وای‌فای	
۶	🛡️ احراز هویت دو مرحله‌ای	

۷	🏷️ نام بلوتوث و هات‌اسپات	
۸	🌐 مرورگر امن	
۹	🆔 شناسه تبلیغاتی	
۱۰	☁️ پشتیبان‌گیری ابری	
۱۱	🚨 دکمه وحشت	
۱۲	🔄 به‌روزرسانی	

نمره شما چند شد؟

۰ تا ۴: 🔴

گوشی شما یک خانه با درهای باز است.

۵ تا ۸: 🟡

در برابر دزدی معمولی امن هستید، اما نه در برابر جاسوسی.

۹ تا ۱۲: 🟢

«دزد دیجیتال» نفوذ به گوشی شما برای اکثر هکرها دردسر بزرگی است.