

ضد شنود دیجیتال

شنود دیجیتال به مجموعه‌ای از روش‌ها گفته می‌شود که از طریق آن‌ها، داده‌ها، صدا، تصویر، موقعیت مکانی و الگوهای رفتاری فرد از طریق ابزارهای دیجیتال جمع‌آوری می‌شوند.

برخلاف تصور عمومی، شنود دیجیتال فقط مخصوص تماس تلفنی نیست؛ بلکه گوشی هوشمند، به‌تنهایی یک پلتفرم کامل شنود است.



دفتر راهبردی نجات ایران

www.dornairan.com 

اگر دستگاهی به اینترنت وصل میشود قابل نفوذ است. امنیت ۱۰۰٪ وجود ندارد، فقط مدیریت ریسک وجود دارد.



این بخش مهم‌ترین و ترسناک‌ترین قسمت تریدکرافت مدرن است. در دنیای امروز، گوشی هوشمند شما بزرگترین جاسوس جیبی است که ۲۴ ساعته مکان، صدا و تصویر شما را مخابره می‌کند. این جزوه بر روی تشخیص و دفاع (Defense & Detection) تمرکز دارد.





چک‌لیست امنیت و پاکسازی

بازرسی ادمین‌ها (Device Admin Apps)

بدافزارها برای اینکه حذف نشوند، دسترسی "ادمین" می‌گیرند.

مسیر:

Settings > Security > Device Admin Apps

اقدام: هر برنامه‌ای غیر از "Find My Device" (گوگل/اپل) را که تیک خورده و نمی‌شناسید، غیرفعال کنید.

۱

کدهای دستوری (USSD) - افسانه و واقعیت

بسیاری از کدها در اینترنت شایعه هستند، اما این کد برای بررسی "دایورت تماس" (Call Forwarding) مفید است:

کد: *#21#

کاربرد: نشان می‌دهد آیا تماس‌ها یا پیام‌های شما به شماره دیگری دایورت شده است یا خیر. (اگر دایورت بود، با ##002 معمولاً لغو می‌شود.)

۲

مجوزهای دسترسی (Permissions Audit)

خطرناک‌ترین دسترسی‌ها میکروفون، دوربین و موقعیت مکانی هستند.

اقدام: به لیست مجوزها بروید. چرا یک اپلیکیشن "چراغ قوه" یا "ماشین حساب" باید به میکروفون دسترسی داشته باشد؟ بلافاصله قطع کنید.

۳



دفتر راهبردی نجات ایران

www.dornairan.com



ارتباطات امن

سیگنال (Signal) به جای واتساپ/تلگرام
چرا؟ سیگنال کمترین "متادیتا" (Metadata) را ذخیره می‌کند.

یعنی شاید محتوای پیام شما در واتساپ رمزگذاری شده باشد، اما واتساپ می‌داند "چه کسی، به چه کسی، در چه ساعتی" پیام داده است. سیگنال این را هم نمی‌داند.



احراز هویت دو مرحله‌ای (2FA)

قانون: هرگز از SMS برای دریافت کد تایید استفاده نکنید (قابل شنود است).
حتماً از اپلیکیشن‌های Authenticator (مثل Google Auth) استفاده کنید.

تمرین عملی: «قرنطینه دیجیتال» Digital Quarantine

برای درک میزان وابستگی و نفوذپذیری خود، این تمرین را انجام دهید:

روز اول:

تمام دسترسی‌های (Permissions) غیرضروری اپلیکیشن‌ها را ببندید. (لوکیشن اینستاگرام، میکروفون اسنپ و...) ببینید کدام اپلیکیشن‌ها از کار می‌افتند.

شب:

قبل از خواب، وای‌فای و دیتای گوشی را خاموش کنید. صبح چک کنید باتری چند درصد کم شده. اگر بیش از ۲-۳٪ بود، مشکوک است.

تست مکان:

در گوگل مپس خود به بخش "Your Timeline" بروید. ببینید گوگل با چه دقتی تمام حرکات سال‌های گذشته شما را ضبط کرده است. این همان چیزی است که باید حذف شود.