
# تخلص من هاتفك المحمول بأمان

## نظرة عامة

تستمر الأجهزة المحمولة، كالهواتف الذكية والساعات الذكية والأجهزة اللوحية، في التطور والابتكار بمعدلات مذهلة. ونتيجةً لذلك، يستبدل بعض الأشخاص أجهزة المحمول الخاصة بهم بشكل متكرر كل عام او نحوه. ولكن للأسف هناك الكثير من الأشخاص لا يدركون مقدار البيانات الشخصية الموجودة على هذه الأجهزة. فيما يلي سنستعرض ما قد يكون على جهازك المحمول وكيف يجب عليك مسحه بشكل آمن قبل التخلص منه. إذا كان جهاز الهاتف المحمول الخاص بك قد تم منحه من قبل صاحب العمل الخاص بك، أو كان يحتوي أي بيانات عمل مخزنة عليه، قم بالتأكد انت ومديرك المباشر من إجراءات النسخ الاحتياطي والاتلاف المناسب للمعلومات.

## معلوماتك

تخزن أجهزة المحمول بيانات أكثر خطورة وحساسية مما يدركه الكثيرون، وغالبًا أكثر بكثير من حاسوبك الشخصي.

قد تشمل مثلا:

- **المكان الذي تعيش فيه ومكان العمل والأماكن التي تزورها.**
- **تفاصيل جهات الاتصال لجميع معارفك في دفتر العناوين الخاص بك، بما في ذلك العائلة والأصدقاء وزملاء العمل.**
- **سجل المكالمات الهاتفية بما في ذلك المكالمات الواردة والصادرة والبريد الصوتي والمكالمات التي لم يرد عليها.**
- **المراسلات النصية أو جلسات الدردشة داخل تطبيقات مثل: الدردشة الآمنة والألعاب ووسائل التواصل الاجتماعية.**
- **سجل تصفح الويب وسجل البحث وملفات تعريف الارتباط والصفحات المخبأة.**
- **الصور الشخصية ومقاطع الفيديو والتسجيلات الصوتية.**
- **كلمات المرور المخزنة والوصول إلى حساباتك، مثل البنك أو وسائل التواصل الاجتماعي أو البريد الإلكتروني.**
- **المعلومات المتعلقة بالصحة، بما في ذلك عمرك أو معدل ضربات القلب أو تاريخ التمرين أو ضغط الدم.**

## آليه مسح وتهيئه جهازك

الخدعة التي تكمن هنا أنه في أغلب المواقف لم يتمكن مجرمي الانترنت من اختراق جهازك وهم لا يعرفون الكثير عنك ولا يعرفون أنشطتك على الانترنت، ببساطة يحاولون استخدام التفاصيل الشخصية القليلة التي لديهم عنك لإخافتك لتصديق أنهم اخترقوا حاسوبك

أو جهازك ويجبروك على أن تدفع لهم مقابل عدم نشر هذه البيانات للحفاظ على خصوصيتك. تذكّر، مجرمو الانترنت يمكن أن يستعملوا نفس تقنيات الاحتيال من خلال مكالمة هاتفية أيضا لابتزازك.

- **أجهزة Apple IOS: الإعدادات | عام | إعادة تعيين | محو كل المحتوى والإعدادات.**
- **أجهزة Android: إعدادات | الخصوصية | الاعادة لضبط المصنع.**

## بطاقات الذاكرة الخارجية

بالإضافة إلى جهازك، تحتاج أيضًا إلى التفكير فيما يجب فعله ببطاقة SIM (وحدة تعريف المشترك). بطاقة SIM هي ما يستخدمه الجهاز المحمول لإجراء اتصال خلوي أو اتصال بيانات. عندما تقوم بمسح جهازك، تحتفظ بطاقة SIM بمعلومات حول حسابك وبيانات مرتبطة بك. إذا كنت تحتفظ برقم هاتفك وتريد الانتقال إلى جهاز جديد، فتحدث إلى مزود خدمة الهاتف الخاص بك حول نقل بطاقة SIM الخاصة بك. إذا لم يكن ذلك ممكنًا، فاحتفظ ببطاقة SIM القديمة وقم بتدميرها يدوياً لمنع أي شخص آخر من إعادة استخدامها لانتحال هويتك والوصول إلى معلوماتك أو حساباتك. وأخيرًا، تستخدم بعض أجهزة Android المحمولة بطاقة SD قابلة للإزالة للتخزين الإضافي. قم بإزالة بطاقات التخزين الخارجية هذه من جهازك المحمول قبل التخلص منه. وفي كثير من الأحيان يمكنك إعادة استخدام هذه البطاقات في الأجهزة المحمولة الجديدة، أو يمكن استخدامها كمخزن عام على الكمبيوتر الخاص بك باستخدام محول USB. أما إذا لم يكن من الممكن إعادة استخدام بطاقة SD، مثل بطاقة SIM القديمة، فإننا ننصحك بتدميرها يدوياً.

إذا لم تكن متأكدًا من أي من الخطوات الموضحة أعلاه، أو إذا كانت خيارات إعادة تعيين الجهاز مختلفة، فخذ جهازك المحمول إلى المتجر الذي اشتريته منه واحصل على المساعدة من فني مُؤَهَل لذلك. أخيرًا، إذا كنت ترمي جهازك بعيدًا، ففكر في التبرع به بدلاً من ذلك. هناك العديد من المنظمات الخيرية الممتازة التي تقبل الأجهزة المحمولة المستعملة، والعديد من مزودي خدمات الهاتف المحمول لديهم صناديق تسليم في متاجرهم.

## الضيف المحرر

ريستوفر كرولي مستشار مستقل في ضواحي واشنطن متخصص بالعمليات الامن والحماية. ينشر تويتات ومقالات من حين لأخر(@CCrowMontance). ترقبوا كتابه القادم حول مراكز العمليات الأمنية. أيضا هو مدرس اول في معهد SANS

## مصادر إضافية

SANS Course: Pen Testing Mobile Devices: https://sans.org/sec575
SANS Course: Advanced Smartphone Forensics Course: https://sans.org/for585
كيف تتخلص من هاتفك من FTC: https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device