



دليل حماية بصمتك الرقمية

يقصد بالبصمة الرقمية جميع المعلومات الموجودة عبر الإنترنت نتيجة ممارسة أنشطة إلكترونية أونلاين. ويشمل ذلك - على سبيل المثال لا الحصر - منشوراتك على وسائل التواصل الاجتماعي، والدرشات، والرسائل النصية، وسجل التصفح، ورسائل البريد الإلكتروني وعمليات الشراء عبر الإنترنت، وبيانات الموقع الجغرافي. ويمكن استغلال بصمتك الرقمية بما يعرضك لمخاطر عديدة، منها:

- **زيادة خطر تعرضك للاحتيال.** يمكن للمحتالين والمزورين استغلال بصمتك الرقمية لاستهدافك أو انتحال هويتك أو سرقة معلوماتك الشخصية.
 - **وضعك تحت المراقبة، سواء من جانب جهات حكومية أو أفراد يسيئون استخدام السلطة أو يسعون للتحكم فيك.** يتضمن ذلك إمكانية معرفة موقعك إذا كنت تُفعل خاصية تحديد الموقع الجغرافي أو تستخدم خاصية "تسجيل الدخول" عبر وسائل التواصل الاجتماعي.
 - **زيادة احتمالية تعرضك للاستغلال أو الإيقاع بك.** يستغل المجرمون البصمة الرقمية للأشخاص لاستهدافهم واستدراجهم إلى أوضاع عمل قسرية أو ظروف استغلالية. كما يمكن للمتطرفين وغيرهم من ذوي النوايا السيئة أيضاً استغلال البصمة الرقمية للأشخاص
- **التأثير سلبيًا على قبول طلبك للهجرة.** بات من المطلوب الآن الإفصاح عن الحسابات عبر وسائل التواصل الاجتماعي، وأسماء المستخدمين، وغيرها من المعلومات الرقمية، عند التقدم إلى العديد من طلبات الهجرة الشائعة. كما يمكن تفتيش الأجهزة الإلكترونية عند محاولة دخول الولايات المتحدة أو عند احتجاز الشخص من جانب وزارة الأمن الداخلي. يمكن استخدام أنشطة الأفراد عبر الإنترنت للتأثير على قرارات مهمة مثل: الاحتجاز أو الترحيل أو تعديل الوضع القانوني أو التجنيس أو منح حق اللجوء أو غيرها من أشكال المساعدات المقدمة للمهاجرين.

إدارة بصمتك الرقمية أمر بالغ الأهمية لسلامتك وأمنك وسمعتك!

12 نصيحة أساسية نقدمها لك لإدارة بصمتك الرقمية بحكمة وذكاء

1. **احمِ أجهزتك وحساباتك.** تأكد من أن جميع أجهزتك محمية بكلمات مرور قوية، ويُفضل استخدام المصادقة الثنائية. وتعني المصادقة الثنائية وجود طريقتين للتحقق من الهوية، مثل: إدخال كلمة المرور بالإضافة إلى إدخال رمز تستقبله على هاتفك المحمول.
2. **لا تشارك معلوماتك الخاصة.** تجنب نشر اسمك الكامل وعنوانك أو رقم هاتفك أو أي معلومات خاصة أخرى عبر الإنترنت، وينطبق ذلك على جميع وسائل التواصل الاجتماعي.
3. **اجعل حساباتك خاصة** إذا كنت تستخدم حسابات على وسائل التواصل الاجتماعي، فتأكد من ضبطها على وضع "خاص". عادةً يمكنك تنفيذ ذلك من خلال الدخول إلى إعدادات الحساب أو الخصوصية، والتأكد من تحديد خيار "خاص" لنوع حسابك.
4. **احذف حساباتك القديمة** إذا لم تعد تستخدم حسابًا، فبادر بحذفه. وبالمثل، لا تنس إيقاف أو تعطيل خدمات التخزين السحابي أو الحسابات المرتبطة بأجهزة قديمة ما زلت تملكها ولكنك نادرًا ما تستخدمها.
5. **تأكد من إلغاء تفعيل خاصية تتبع الموقع.** لإلغاء تفعيل خاصية تتبع الموقع على الجهاز، انتقل إلى إعدادات الجهاز، والتي توجد عادة تحت تبويب "الخصوصية" أو "الأمان" أو "الموقع". ثم، تأكد من إلغاء تفعيل خدمات الموقع لمنع التطبيقات والخدمات من معرفة مكانك الجغرافي.
6. **قلل من المحتوى الذي تنشره.** حاول نشر أقل قدر ممكن من المعلومات عبر الإنترنت.
7. **لا تقبل طلبات الصداقة من أشخاص لا تعرفهم.** تأكد من أنك لا تقبل طلبات الصداقة إلا من الأشخاص الذين تعرفهم. احذر! فقد يخفي البعض هويتهم خلف ملفات شخصية مزيفة، مثل المحتالين أو المتاجرين بالبشر أو من يحاولون مراقبتك.
8. **احذف المواد الحساسة والتطبيقات التي قد يساء فهمها من هواتفك وأجهزتك الأخرى.** في حالة السفر دوليًا، يجوز لممثلي وزارة الأمن الداخلي تفتيش الأجهزة الإلكترونية عند نقاط الدخول في طريق العودة إلى الولايات المتحدة. لذا، بادر بحذف جميع النصوص والصور والتطبيقات والمواد الأخرى التي قد يساء فهمها.

9. تأكد من التواصل بأمان. استخدم تطبيقات التواصل التي توفر خاصية التشفير التام من طرف إلى آخر مثل واتساب وسيجنال وتيليجرام.

ملاحظة: رغم أن هذه التطبيقات أكثر أمانًا، إلا أن منصات الرسائل المشفرة قد تساهم في تكوين بصمتك الرقمية من خلال تخزين البيانات الوصفية مثل: من تتواصل معه، ومتى، بالإضافة إلى المحتوى المشترك كالصور والفيديوهات ومعلومات الملف الشخصي. لذا، كن حذرًا فيما تتواصل بشأنه.

10. توخ الحذر عند تصفح الويب. لا تنقر على الروابط المشبوهة من المرسلين الذين لا تعرفهم أو تزور مواقع إلكترونية غير موثوقة لأنها قد تعرض جهازك للفيروسات أو تستخدم في مراقبتك.

لا تشارك إلا المعلومات الضرورية. واحذر من المواقع أو التطبيقات التي تطلب معلومات شخصية أكثر مما هو مطلوب فعليًا.

امسح ملفات تعريف الارتباط وذاكرة التخزين

المؤقت للمتصفح بانتظام. يمكنك عادة تطبيق ذلك بالانتقال إلى تبويب إعدادات المتصفح، ثم إعدادات الخصوصية، ثم البحث عن خيار "مسح بيانات التصفح" أو خيار مماثل.

11. استخدم هاتفًا محمولاً مؤقتًا أو يمكن التخلص منه.

مثل هذه الهواتف غالبًا ما تكون مدفوعة مسبقًا وغير مرتبطة بعقد، مما يسهل استخدامها لعدم الكشف عن هوية مستخدمها وتجنب التتبع. ومع ذلك، حال استخدامك لهاتف محمول مؤقت، يجب أن تتأكد من إبلاغ الأشخاص المهمين (مثل الأخصائي المسؤول عن حالتك أو محاميك) برقمك الجديد. أحيانًا، يختار بعض الأشخاص امتلاك هاتفين؛ هاتف مؤقت لأنشطتهم عبر الإنترنت وآخر دائم للتواصل المهم والمستقر مع الأشخاص الأساسيين في حياتهم.

12. احرص على استخدام أغطية الكاميرا. احرص على

استخدام أغطية الكاميرا على الهواتف وأجهزة الكمبيوتر المحمولة لحجب العدسة عندما لا تكون قيد الاستخدام. فهذا يمكن أن يمنع انتهاكات الخصوصية عبر الكاميرا.