الطقوس والشعوذة الرقمية، والأعشاب الطبيعية لحماية نفسك من العين

إذا كنتِ تعتقدين أن الإنترنت مجرد مكانٍ للاستماع إلى أغنيتكِ المفضلة، فسيكون ذلك سهلاً، وبذلك فلن يكون هناك حاجة ماسة لوضع كلمات المرور. ولكن تذكري بأن الإنترنت هو المكان الذي تحتفظين فيه بصوركِ الخاصة، وتنظمين الأحداث والفعاليات، وتدفعين فواتيركِ.

عند التفكير في كل "الأملاك الافتراضية" الخاصة بكِ التي يتم تبادلها عبر الإنترنت وتخزينها على أجهزتكِ، يتبادر هنا سؤال: لماذا لا تحافظين عليها بنفس حرصكِ على محفظة أموالكِ أو مفاتيح منزلكِ؟

في هذا الدليل، ستجدين خطوات بسيطة يمكنكِ اتباعها للعنايةِ بنفسكِ وبالآخرين على الإنترنت.

لنبدأ!

الطقوس الخاصة بالأجهزة الخاصة

يوفر لكِ أي قفل على جهازكِ المحمول حماية أكبر لبياناتكِ الرقمية. وهي تشبه إلى حدٍ ما أنواع الأقفال المختلفة التي تضعينها على أبواب منزلكِ أو سيارتكِ، والتي تكون غالباً بعضها أقوى من غيرها، وكذلك الحال لأقفال شاشة حاسوبكِ أو هاتفكِ. قد يفاجئكِ الأمر، ولكن كلمات المرور التي تتكون من ثمانية أحرف أو أكثر وتحتوي على أحرف وأرقام ورموز خاصة هي الطريقة الأكثر أمانًا لقفل حاسوبكِ أو هاتفكِ. بشرط، عدم إعادة استخدام كلمات المرور نفسها، أو بنفس أنماط الكلمات السابقة لكيلا يسهل تخمينها.

وكذلك عدم استخدام أسماء شائعة أو كلمات قاموسية أو تواريخ سهلة، والتي من الممكن أن تكون على قوائم كلمات المرور التي يتداولها القراصنة أو المتتبعون على الإنترنت.

نصائح أخرى :

- تفعيل المصادقة الثنائية (2FA) في المواقع والتطبيقات التي تتوفر فيها.
- تقوية كلمات المرور: يجب أن تكون كلمات المرور الخاصة بك طويلة وفريدة وعشوائية.

تعويذات للاتصالات الخاصة

تسمح بعضتطبيقات المراسلة (مثل واتساب وسيجنال) للمستخدمين بتعيين "الرسائل المؤقتة" في الدردشات، وهذا يعني أن التطبيق سوف يمحو الرسائل تلقائيًا بعد فترة محددة من الزمن للمرسل والمستلم.

ولكن مهلاً، يمكن للشخصالآخر أن يقوم بالتقاط صورة لرسالتكِ وإظهارها للآخرين في الفترة الزمنية المحددة، دون علمكِ!

نصائح أخرى:

- إيقاف معاينة الرسائل : عندما يكون هاتفكِ مغلقًا، تأكدي من إخفاء رسائلكِ أيضًا.
- قفل التطبيقات الحساسة - التي يمكن أن تحتوي على بيانات مهمة عنكِ - بكلمات مرور إضافية من خلال المصادقة الثنائية للحفاظ على سلامتها ، في حال تم اختراق هاتفكِ.

لغات سرية للأجهزة

عند النظر في خيارات تطبيقات المراسلة، من المهم أن تدركِ أنها ليست جميعها متساوية. وهنا بعض الأسئلة الرئيسية التي يجب عليك مراعاتها:

- هل يتم تشفيرها من خلال خاصية من النهاية إلى النهاية أو (End to End) ؟

هذا يعني أن الرسالة مشفرة ولا يمكن فك تشفيرها إلا من قبلكِ والشخص الآخر. وعلى الرغم من أن ذلك، قد تساعد هذه الخاصية في منع الرسالة من الوصول إلى طرفٍ ثالثٍ، إلا أنه لا يزال هناك خطر من أن الشخص الآخر والذي يمكنه عرضها لشخص آخر أو التقاط صورة للمحادثة.

- **ماذا تخزن بعض شركات الطرف الثالث عنك؟**

حتى إذا كان تطبيق المراسلة مشفر من النهاية إلى النهاية، إذا تم نسخ رسائلكِ إلى خوادم الشركة، فهذا يعني وجود احتمال لأن يطلب شخص ما سجلات الرسائل. تذكري، كلما جمع التطبيق أقل معلومات عنكِ، كلما كان قلة احتمالية الكشف عنكِ وتتبعكِ على الإنترنت.

نصائح أخرى:

- استخدام تطبيقًا مراسلة آمنًا مثل Wire أو Signal للتواصل مع أصدقائكِ وأفراد عائلتكِ.
- ستخدام أسماء مستعارة خاصة وأسماء مجموعات أقل وضوحًا لبعض دردشاتكِ وجهات الاتصال المحفوظة في هاتفكِ وتطبيقاتكِ، إذا كان ذلك مناسبًا لكِ.

الأعشاب الطبيعية للعلاج : الرعاية الذاتية

المخاطر والسلامة مشتركة، لذلك تذكري أنكِ لستِ وحيدة في هذا العالم المليء بالمخاطر. تحدثي مع الأصدقاء والعائلة الموثوق بهم حول هذه الطقوس الرقمية والشعوذة المناسبة لكل تطبيق. وكذلك، لا تنسي الأعشاب الطبيعية للمساعدة فيالحفاظ على الخصوصية وتجنب العين الشريرة - ربما لديهم بعضالنصائح الرائعة لمشاركتها معكِ أيضًا.

إذا كنتِ ترغبين في معرفة واستكشاف المزيد من النصائح قومي بزيارة :

/datadetoxkit.org/ar

*هذا الدليل هو تكييف ل"داتا ديتوكس كيت"، صُمم خصيصًا للنساء في الخليج في عام 2023 .