DATA DETOX KIT

تحكَّم في بيانات هاتفك الذكي

لزيادة خصوصيتك على الإنترنت

٤. قلِّل من آثارك

يُخزِّن المتصفح على جهازك كثيرًا من المعلومات عنك؛ موقعك، الأشياء التي تبحث عنها، أي المواقع تستخدم، وقد يقدّم تلك المعلومات إلى أحد يومًا ما.

لكن لا يزال بإمكانك أن تستعيد التحكّم في بعض هذه المعلومات، عبر بعض التغييرات.

غالبًا ما تكون الهواتف والتابلت والحواسيب مثبتًا عليها مسبقًا متصفحات لا تبالي بخصوصيتك. يمكنك بدلًا من ذلك تحميل متصفح يجعل من نشاطك على الشبكة أكثر خصوصية بشكل افتراضي، ويحميك من المتعقّبين.

ولمزيد من الخصوصية، يمكنك تحميل إضافات تُعرف بـ"الإضافات والامتدادات" (برامج صغيرة لمتصفحك سهلة التحميل تجعل من نشاطك على الإنترنت أكثر خصوصية).

لحجب الدعايات التجسسية والمتعقبات غير المرئية، حمِّل يوبلوك أوريجن على كروم وسفاري وفايرفوكس أو برايفاسي بادجر على كروم وفايرفوكس وأوبرا.

لضمان اتصال آمن بالمواقع قدر الإمكان، حمّل HTTPSEverywhere: وهو إضافة للمتصفح تضمن تشفير اتصالك مع المواقع الكبرى وحمايتك في أثناء التنقل. إذا كنت تستخدم سفاري وتريد هذه الميزة، فاضبط متصفحك الافتراضي على منتج غير تابع لجوجل، مثل دوك دوك جو DuckDuckGo، الذي يعيد توجيهك إلى الاتصالات المشفّرة تلقائيًا.

٥. لا تستخدم التاج (الإشارة) أنت والآخرون

هل أسهمت في بناء بيانات أصدقائك بذكرهم في تاج الصور والمنشورات في الماضي؟

خفِّف من حمل بياناتهم (وضميرك بالمناسبة) عبر عدم ذكرهم في التاج قدر الإمكان، في الصور والمنشورات.

انشر ذلك! شجِّع أصدقاءك وعائلتك وزملاءك في العمل على مشاركتك التحكم في آثار بياناتنا، إذا ما عملنا سويًا في ذلك، يمكننا مساعدة بعضنا على تنظيف آثار أقدامنا الرقمية.

إذا كنت تفكر ما الذي تخبر به بياناتك الآخرين عنك، فإن ذلك لا يبدو أمرًا صعبًا: من يهتم إذا كنتَ تحب موسيقى بلد معين، أو ترغب في شراء أحذية أكثر مما تريد، أو تبدأ تنظيم عطلتك القادمة مسبقًا.

تكمن المشكلة في ما يحدث لبياناتك، فبجمعها معًا وبمرور الوقت تظهر الأنماط الرقمية الخاصة: فتُكشف عاداتك وتحركاتك وعلاقاتك وتفضيلاتك ومعتقداتك وأسرارك لمن يحللونها ويستفيدون منها، كسماسرة الأعمال التجارية والبيانات.

وباتّباعك عملية تنظيف البيانات هذه، ستحصل على لمحة عن كيفية حدوث كل ذلك ولماذا يحدث، وستتبّع خطوات عملية لـ التحكم في بياناتك وآثارك على الإنترنت.

فلنبدأ!

datadetoxkit.org/ar/home
#datadetox

مدعوم من قبل
Firefox GOETHE INSTITUT

منتج لصالح
TACTICAL TECH

١.

غيِّر اسم جهازك

لربما اخترت اسمًا في وقت ما لجهازك على شبكة واي فاي أو بلوتوث أو كليهما، أو ربما أُنشِئ الاسم أوتوماتيكيًا في أثناء الإعداد.

هذه يعني أن اسم "جهاز أليكس تشنغ" سيظهر لصاحب شبكة الإنترنت، وإذا كان البلوتوث مفعلًا، فسيظهر لكل شخص في المنطقة يفعّل البلوتوث على جهازه.

وفي العادة فإنك لا تُعلن اسمك عندما تدخل إلى المقهى أو المطعم أو المطار، كذلك الأمر بالنسبة لجهازك.

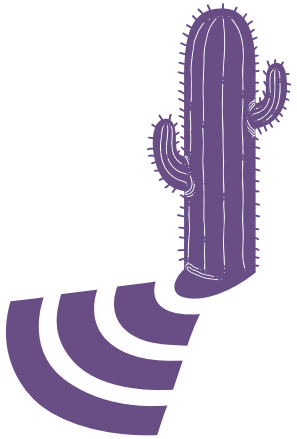
يمكنك تغيير اسم جهازك إلى اسم أقل تحديدًا للهوية الشخصية، لكن يشير إليك بشكل مميز. إليك كيف تفعل ذلك:

آيفون:

غيّر اسم الجهاز:
إعدادات ← عام ← عن الجهاز ← غيّر الاسم

أندرويد:

تغيير اسم الواي فاي:
الضبط ← Wi-Fi ← القائمة ← المزيد / خصائص أخرى ← Wi-Fi Direct ← إعادة تسمية الجهاز
تغيير اسم البلوتوث:
الضبط ← بلوتوث ← تشغِّل البلوتوث
إن كان مطفأ ← القائمة ← إعادة تسمية الجهاز ← تشغيل البلوتوث



٢.

احذف آثار موقعك

في حين تبدو بيانات مكانك على أنها أجزاء عشوائية صغيرة من المعلومات، فعندما تجتمع، فإنها قد تكشف تفاصيل مهمة عنك وعن عاداتك، مثل مكان إقامتك، وعملك، وأين تحب أن تذهب مع أصدقائك، ما يجعل عديدًا من الشركات وسماسرة البيانات يتهافتون عليها.

قد يكون أمرًا عاديا أن يصل تطبيق الخرائط في جهازك إلى موقعك، لكنك ستُفاجأ بكمّ التطبيقات التي أذنت لها بالوصول إلى موقعك.

بإمكانك أن تتفقّد أذونات كل تطبيق وتُوقف خدمات المواقع، وتبحث عن التطبيقات التي لا تحتاج إليها لتقديم الخدمة (هل تحتاج لعبة أن تعرف أين موقعك حقًا؟) وبالنسبة للتطبيقات التي لا تريد أن تأذن لها بذلك:

أندرويد:

الضبط ← التطبيقات ← حدّد خدمة الوصول إلى الموقع بحسب التطبيق

آيفون:

الإعدادات ← الخصوصية ← خدمات الموقع ← حدد خدمة الوصول إلى الموقع بحسب التطبيق

٣.

رتِّب التطبيقات

تهتم تطبيقات وسائل التواصل الاجتماعي والطقس والألعاب ببياناتك، وقد تجمع كثيرًا منها.

قد يكون التخلص من التطبيقات العشوائية التي لا تستخدمها أبدًا على جهازك، وسيلة فعّالة لتنظيف سجلّاتك الرقمية.

بالإضافة إلى ذلك، يُسهم الترتيب في تفريغ بعض المساحة على جهازك، وتقليل استخدام البيانات وإطالة عمر البطارية، ما يسهم في زيادة الأداء العام، بحسب التطبيق.

أندرويد:

الضبط ← التطبيقات ← اختر التطبيق الذي تريد إزالة تثبيته ← إزالة تثبيت

آيفون:

اضغط فترة على التطبيقات حتى تبدأ الاهتزاز، وتظهر قائمة صغيرة أعلى الزاوية اليسرى لكل تطبيق.

لحذف التطبيق، اضغط على حذف من القائمة الصغيرة.

للعودة إلى الوضع العادي، اضغط على زر القائمة.

احم أشياءَك الافتراضية القيمة

تمامًا مثلما تهتم بأشيائك الثمينة في المنزل، كذلك يجب أن تفعل بالنسبة للمعلومات التي تخزنها افتراضيًا، سواء كان ذلك سجلات مالية، أم صور جواز سفرك، أو حتى عنوانك أو رقم هاتفك، إن الأمر يستحق التفكير: أين تخزّن بياناتك الشخصية الأكثر أهمية؟ و كيف يمكنك حمايتها؟

إن أداء عملية تنظيف كاملة أمر رائع إذا أردتَ القيام ببعض التحسينات الخاطفة في أثناء احتسائك كوبًا من القهوة. ابحث عن معلومات محددة موجودة في بريدك الإلكتروني أو حساباتك الأخرى واحذفها؛ صور هويتك، تفاصيلك البنكية أو معلومات تأمينك الصحي، على سبيل المثال لا الحصر. وفي حال كنت ستحتاج إليها في المستقبل، فيمكنك تحميلها على جهازك أو طباعتها قبل حذفها من بريدك الإلكتروني.

أما إجراء عملية تنظيف عميقة فهي أكثر شمولية، ومن الجيد أن تقوم بها مرة في السنة، أرشِف كل شيء في بريدك الإلكتروني أو حسابك على مواقع التواصل الاجتماعي، حمّله على كمبيوترك واحذف محتوى الحساب من أجل بداية جديدة.

ويعود الأمر إليك إذا كنت تريد أن تحتفظ بنسخة احتياطية لأرشيفك ومستنداتك على السحابة، أو حفظها على قرص صلب خارجي أو فلاشة. في كل الأحوال، تأكد من عدم فقدانها، وأن كلمة المرور قوية ومنطقية بالنسبة لك.

مرِّرها

لئن كان النسيان سهلًا، فإن وراء تسمية "الشبكة العنكبوتية" سبب وجيه. نحن جميعًا متصلون عبر الإنترنت من خلال عدة شبكات، ليس فقط "كأصدقاء" على مواقع التواصل الاجتماعي، بل كذلك عبر قائمة الأسماء على حسابات الإيميلات والصور التي نشاركها على الإنترنت.

عندما تؤمّن حساباتك، وتقوّي كلمات المرور، وتنظّف بياناتك، فإنك لست المستفيد الأوحد من ذلك، فكل شخص أنت على اتصال به يصبح في أمان أكبر بفضل جهودك.

عندما تنظف قوم بتنظيف بريدك الإلكتروني وحساباتك على مواقع التواصل الاجتماعي، فكر بالأشياء الأخرى التي تستطيع تحميلها على جهازك وحذفها التي تساعد أصدقاءك وزملاءك في العمل: : التفاصيل البنكية الخاصة بشقيقتك، رمز مفتاح الدخول إلى مكتبك، أو صورة عن الجواز السفر الخاص بابنك، هذهي فقط بعض السجلات التي يمكن أن تسبب المتاعب إذا ما وقعت في الأيدي الخطأ.

منتج لصالح
TACTICAL TECH

مدعوم من قبل
Firefox
GOETHE INSTITUT

datadetoxkit.org/ar/home
#datadetox

DATA DETOX KIT

غيّر إعداداتك

لتأمين بياناتك

إذا كان الإنترنت فقط مكانًا لمشاركة صور كلاب ترتدي زي ديناصورات، فلن تكون هناك حاجة ماسة لكلمات المرور.

إلا أنه من خلال الإنترنت، فإنك أيضًا تدفع فواتيرك، وتعيد شراء وصفاتك الطبية، وتسجّل بياناتك للتصويت.

عندما تفكر في جميع "أشيائك الافتراضية الثمينة" التي تشاركها عبر الإنترنت، والتي تخزّن على أجهزتك، تسأل: لماذا لا تُبقي عليها في مأمن تمامًا مثل محفظتك ومفاتيحك؟

هناك طريقة بسيطة لجعل وصول الآخرين إلى أشيائك الافتراضية الثمينة مهمة أصعب: لا تجعل تكهنهم بكلمات المرور أمرًا سهلاً، لا يحتاج أغلب الناس إلى مهارات تقنية متخصصة للدخول إلى حساباتك، إذ يمكنهم الدخول إليها عبر القيام ببعض التكهنات لكلمات المرور أو بتشغيل برنامج مؤتمت.

وحالما يتمكنون من الدخول إلى حساب واحد، يمكنهم تجريب كلمة المرور المكشوفة هذه للدخول إلى حسابات أخرى، وتجميع معلومات عنك وعن عاداتك، والاستيلاء على الحسابات التي تملكها، أو حتى استخدام هويتك الرقمية.

باتّباعك عملية تنظيف البيانات هذه، ستتعلم خطوات عملية لزيادة أمنك على شبكة الإنترنت.

فلنبدأ!

١.
أقفل بابك الرقمي

أقفال الشاشة: إن كلمات المرور، أو الأنماط، أو البصمات، أو هوية الوجه التي تستخدمها للدخول إلى جهازك، بعض من أفضل الدفاعات التي تستخدمها ضد من يريد الدخول إلى جهازك. إلا أن هناك كثيرًا من الأنواع المتوافرة وقد يكون من الصعب معرفة أي منها يناسبك.

إن وجود أي قفل على جوالك أو التابلت أو الكمبيوتر يعطيك حماية أفضل من عدم وجود قفل على الإطلاق. وتمامًا كأنواع الأقفال المختلفة التي قد تضعها على أبوابك، فإن بعض أقفال الشاشات أقوى من غيره.

من بين جميع الأقفال المتوافرة، فإن كلمات المرور الطويلة والفريدة هي الأقوى. هذا يعني أنك إذا فتحتَ جهازك بكلمة مرور، فإنها ينبغي أن تتضمن أحرفًا وأرقامًا ورموزًا خاصة.

فلنقل إنكم تستخدمون تمريرًا بسيطًا لفتح جهازكم، باستطاعتكم زيادة أمنكم بإنشاء كلمة مرور طويلة، أو هل تستخدمون نمطًا الآن؟ ما رأيكم بجعل النمط أطول؟ هل تستخدمون 1234 رمزًا للدخول إلى جهازكم؟ ما رأيكم برمي حجر النرد سبع مرات وحفظ ذلك الرمز بدلًا من ذلك؟

إن تغييرًا بسيطًا يمكن أن يسهم بشكل كبير في سيطرتكم على أجهزتكم.

٢.
دع الشخص الصحيح يدخل

إن إنشاء كلمات مرور قوية أمر سهل. كل ما عليك فعله هو اتّباع بعض المبادئ الأساسية. ينبغي أن تكون كلمات المرور التي تنشئها:

طويلة: ينبغي أن تكون كلمة المرور مؤلفة من ثمانية رموز على الأقل، هل تريد أفضل من ذلك؟ 16-20 رمزًا.

فريدة: ينبغي أن تكون كل كلمة مرور تستخدمها -لكل موقع- مختلفة عن الأخرى.

عشوائية: لا ينبغي أن تتبع كلمة المرور نمطًا منطقيًا، أو أن تكون سهلة التخمين، هنا يصبح مدير كلمات المرور مفيدًا جدًا.

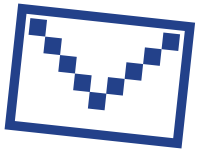
إن أقوى كلمات المرور هي تلك التي تجمع بين الأحرف والأرقام والرموز الخاصة. إن هذه النصيحة الأزلية تجعل من كلمة المرور قوية وصعبة التخمين بشكل أكبر، لسوء الحظ، فإن بعض أنظمة كلمات المرور لا تسمح لك باستخدام رموز خاصة (مثل @#$%-=+)، لكن استخدام مزيج طويل بما فيه الكفاية من الأحرف والأرقام، يبقى أفضل من استخدام كلمة مرور قصيرة.

ولأفضل أدا، ينبغي لك استخدام مدير كلمة مرور مخصص لإنشاء جميع كلمات المرور الخاصة بك وتخزينها. إن مديري كلمات المرور مثل 1Password و KeePassXCمما ينصح به خبراء الأمن، وهي تطبيقات هدفها الأوحد حماية بيانات تسجيل الدخول والبيانات الأخرى الحساسة الخاصة بك.

٣.
أضف مفتاحًا ثانيًا

إن إنشاء تحقق ثنائي العامل "2FA أو تحقق متعدد العوامل "(MFA) يعني أنه حتى إذا حصل أحد على كلمة المرور الخاصة بك، فلن يتوافر لديه على الأرجح العامل الإضافي الذي يحتاج إليه للدخول.

ألق نظرة على إعدادات الأمن الخاصة بالمواقع والتطبيقات الأكثر استخدامًا، لترى ما إذا كان بإمكانك إنشاء هذا المفتاح الإضافي. ابدأ بالمواقع الأكثر أهمية، أي التطبيقات المالية، أو خدمات مثل البريد الإلكتروني التي تستخدمها لاستعادة حسابات أخرى.



فيس بوك:

القائمة ← الإعدادات ← الأمن وتسجيل الدخول ← استعمل التحقق بخطوتين

جوجل:

سجّل الدخول إلى حسابك myaccount.google.com ← الأمن ← 2-Step Verification التحقق بخطوتين ← Get Started ابدأ

ملاحظة: عندما تنشيءتنشئ مرحلة تالية من التحقق، فسيترتب عليك اختيار طريقة ثانية للتحقق من هويتك. حاول تجنب استخدام الرسائل النصية المرسلة إلى رقم جوالك هاتفك كعامل ثانٍ، لأنهك قد تفقد جوالكهاتفك. استخدام البريد الإلكتروني هو خيار أكثر موثوقية.

DATA DETOX KIT

اهرب من الافتراضات

لتقوية سلامتك الرقمية

متى كانت آخر مرة "أطفأتَ" فيها جهازك ولم تقترب من التكنولوجيا ليومٍ، أو حتى لساعة واحدة؟

إذا كنت مداومًا على الاتصال الإنترنت، فلستَ وحدك، ففي المتوسط ينقر الشخص العادي ويمسح شاشة الجوال بيده أكثر من ٢٦٠٠ مرة كل يوم. وإذا كنت تفعل أي شيء بهذه الكثرة، فأنت بحاجة إلى أن تشعر أنه يستحقّ هذا العناء، فكيف لك أن تتأكّد أن الوقت الذي تقضيه على جهازك مفيد وقيّم؟

يبدأ ذلك بمعرفة أن الانجذاب الذي لا يُقاوم نحو جهازك التكنولوجي ليس غلطتكَ! صدق أو لا تصدق ولكن التطبيقات والمواقع الإلكترونية قد حسَّنت كل خاصية ولون وصوت وجعلتها "بالشكل الأمثل"، حتى تجعلك مشدودًا إليها طوال الوقت ومقتنعًا، وتعود دائمًا طلبًا للمزيد.

هل تريد أن تجد توازنًا صحيًا بين حياتك على الإنترنت وحياتك خارجه؟ إنه موضوع هذا الجزء من تنظيف البيانات.

٤.

ارقع صوتك

إذا كنت مستاءً من التصاميم الإدمانية أوالإقناعية أو المعلومات الخاطئة على مواقع الإنترنت التي تزورها، أو التطبيقات التي تستعملها، فيمكنك أن ترسل إيميلات، وتكتب تغريدات، وتُعلِم الشركات أنك غير راضٍ عن ممارساتهم، وعندما يجدون الضغط آتيًا مِنْ أثمن ما يملكون -المستخدمين- فإنهم سيبادرون على الأرجح بالتغيير.

وإذا شعرتَ أن تعليقك لم يلق آذانًا مصغية، فيوجد شيء قوي بوسعك أن تفعله: استعمل موقعًا إلكترونيًا آخر أو تطبيقًا مختلفًا، وإذا نشرتَ بأنك مستاء من شيء يفعله موقع أو تطبيق ما، ومن ثم قررتَ التوقف عن استعماله فعلًا أو أزلتَ تثبيته، وتابعك في ذلك عدد كاف من الناس، فإنهم سيتنبهون.

٥.

انشر الخبر

مرّرها! هذه الملاحظات المفيدة سريعة النسيان، بيد أن أثرها يمكن أن يكون كبيرًا، فأخبر أصدقاءك، وعائلتك، وزملاءك في العمل، عن الأشياء التي تلاحظها، واطلب منهم مشاركتك في عملية التنظيف التي تقوم بها!

الجميع يعاني من أجل إدارة عاداتهم الهاتفية، المهم أن تجد طريقة مناسبة لك ولأسلوب حياتك. جرّب أن تجد ما يناسبك، ثم حدّث عاداتك، لأن حاجاتك تتغير بمرور الزمن، لا يوجد حل واحد يناسب الجميع.

وأخيرًا، أخبر القريبين منك بالخيارات التي تفضّلها وترتاح إليها، مثل أنك لن تكون متاحًا على تطبيق الماسنجر كل يوم بعد الساعة ٨ مساء، لأنك ستخلد فيه إلى الراحة بعيدًا عن الشاشة: أخبر بذلك عائلتك وأصدقاءك، كي يتفهموا موقفك ويختاروا طرقًا بديلة للتواصل معاك تناسبك أكثر. أبقِ النقاش مفتوحًا، اسأل أسئلة، ويمكنك أن تعيش حياة متوازنة تناسبك على الإنترنت.

منتج لصالح TACTICAL TECH

مدعوم من قبل GOETHE INSTITUT Firefox

datadetoxkit.org/ar/home
#datadetox

١.

كن حاضراً في اللحظة الراهنة

ماهذه الملاحظة أقسى مما تبدو عليه، البقاء في اللحظة الحاضرة يتطلب ممارسة يومية، الأمر أشبه بعضلة في دماغك عليك تدريبها دوريًا كي تبني قوتها. يمكنك أن تبدأ ملاحظة علاقتك مع التكنولوجيا التي تستخدمها.

ما الوقت الذي تمضيه على هاتفك؟

إذا كنت مستاء من الجواب، هناك إعدادات واستراتيجيات يمكنك اتّباعها للسيطرة على استخدامك للتكنولوجيا.

إذا كنتَ تهدف إلى تمضية وقت أقل على فيس بوك، أو إنستجرام، أو سناب شات، فغيّر الإعدادات وأذونات تلك التطبيقات لتُحسِّن أداءَها معك. بل إن بعضها مثل إنستجرام لديه خيار يُذكِّرك بكل لطف بأنك وصلت إلى حدودك الزمنية اليومية.

إنستجرام:

الصفحة الشخصية ← قائمة ← الإعدادات ← الحساب ← نشاطك ← اضبط التذكير اليومي

إذا وجدتَ أن هاتفك يُفسد عليك محادثاتك في الحياة الواقعية برنينه، أو أزيزه، أو الومضات التي تصدُر عنه، فيمكنك أن تُسكته مؤقتًا، ضع واجهته للأسفل أو حتى ضعه بعيدًا في جيبك أو حقيبتك كي يبقى بعيدًا عن ناظريك.

٢.

اكشف خدع التصميم

التصاميم المقنعة، المعروفة أيضًا بـ"النماذج السوداء"، تستند في أساسها إلى علم النفس البشري، والهدف منها دفعك إلى الاشتراك في شيء ما، أو شراء شيء ما، أو إفشائك معلومات شخصية أكثر مما كنت تنوي أو تقصد.

إن سبب مشاهدتك لهذه الألاعيب المصممة في كل مكان، أنها لا تتوقف عن العمل، فهي تحملنا على النقر والاشتراك والشراء أكثر من المعتاد، والاستمرار في العودة إليها. وكلما ازداد وعيك بهذه المحفزات الماكرة وصور التلاعب الموجودة في المواقع الإلكترونية التي تستخدمها، زادت معرفتك وعلمك بها.

بوسعك أن تفعل عدة أشياء لتكون أذكى من التطبيقات التي تستعملها. اعرفمتى يدفعونك لشيء ما.

أول شيء يمكنك فعله أن تكون مُدركًا لاستخدام هذه الأساليب.

التقط صورة للشاشة وشاركها: التقط صورًا للشاشة في أي وقت تصادف فيه تصاميم إقناعية على الإنترنت، وشاركها مع أصدقائك (بعد أن تحذف أي تفاصيل تدل على هويتك الشخصية، الخصوصية أولًا). يمكنك أن تطلب من الشركات أيضًا أن يغيّروا ممارساتهم.

حافظ على هدوئك: إذا كانت هناك ساعة للعد التنازلي على صفحة مشتريات، اسأل نفسك: "هل هذا مُلحّ حقًا؟" وإذا وجدت نفسك تنقر على زر عندما لم تكن تقصد ذلك بالفعل، فكّر في صيغ العبارات على الأزرار أو الألوان التي تستعملها الخدمة. وإذا شعرتَ بالتشوش، لا تعتقد فورًا أنك على خطأ، فكّر في الكلمات التي يستعملها الموقع الإلكتروني أو التطبيق، فقد تكون مبهمة.

٣.

ابق ذكيًا إعلاميًا

تمامًا مثلما يمكنك أن تتعلّم أن تكون أكثر ذكاء مع الخصائص والتصاميم المقصود منها إبقاؤك متنقلًا على الشاشة ودائم النقر، يمكنك أيضًا أن تكون ذكيًا بشأن كشفك مواد أو منشورات إخبارية المقصود منها تضليلك.

ربما سمعتَ بمشكلات "المعلومات الخاطئة" و"الأخبار الكاذبة"، وربما يمكنك أن تتصرف بحكمة إزاء المعلومات الخاطئة إذا تعوَّدتَ أن تسأل أسئلة حاسمة بخصوص أي أخبار تتلقاها، لا سيّما إذا بدت مدعاة للاستغراب، أو فاضحة، أو يصعب تصديقها لمغالاتها.

وفي النهاية، ستحتاج إلى تمييز الأخبار الحقيقية من الزائفة، لا سيّما إذا كنت تخطط لمشاركتها مع العائلة أو الأصدقاء، لذا اسأل نفسك دائمًا:

مِن أي موقع إلكتروني جاء هذا؟
مَن كتبه (ومتى)؟
ماذا تقول المقالة في مُجملها، بصرف النظر عن العناوين العريضة؟
أي مصادر يشيرون إليها؟

فإذا اعتقدت أنها معلومات خاطئة وترغب في منع انتشارها، فإن معظم المنصات توفر مكانًا تبلّغ فيه عن هذا المنشور. قد تحتاج أيضًا إلى أن تقرر إذا ما كنت تريد الاستمرار في متابعة الحساب الذي نشر المعلومات أم لا.