Fem Pawer
النسوية من أجل حقوق النساء الاقتصادية

KVINNA KVINNA

PWWSD

دليل الأمان والتحول الرقمي من منظور النوع الاجتماعي

جمعية المرأة العاملة الفلسطينية للتنمية

2025

دليل الأمان والتحول الرقمي من منظور النوع الاجتماعي
منشورات جمعية المرأة العاملة الفلسطينية للتنمية
الموقع الإلكترونيّ: www.pwwsd.org
البريد الإلكترونيّ: pwwsd@pwwsd.org

لمزيد من موارد الأمان الرقمي على منصة حملة
https://dsc.7amleh.org/
البريد الإلكترونيّ: info@7amleh.org
الموقع الإلكترونيّ: www.7amleh.org

إعداد
حملة - المركز العربي لتطوير الإعلام الاجتماعي
حملة - المركز العربي لتطوير الإعلام الاجتماعي
7amleh - The Arab Center For the Advancement of Social Media

تم انجاز هذا الدليل من قبل جمعية المرأة العاملة الفلسطينية للتنمية ضمن برنامج النسوية من اجل حقوق النساء الاقتصادية FemPawer، وبدعم من وزارة الخارجية الهولندية، ولا تعبر الآراء الواردة هنا بالضرورة عن المؤسسات الممولة.

Fem Pawer
النسوية من أجل حقوق النساء الاقتصادية

PWWSD

شكر وتقدير:

تتقدم جمعية المرأة العاملة الفلسطينية للتنمية بخالص الشكر والتقدير إلى فريق مركز حملة - المركز العربي لتطوير الاعلام الاجتماعي على جهوده القيّمة في إعداد هذا الدليل حول«الأمن والتحول الرقمي من منظور النوع الاجتماعي».

يشكل هذا الدليل إضافة نوعية ومهمة في تعزيز الوعي بحقوق النساء عموما وفئة الشابات على وجه الخصوص، في الفضاء الرقمي، ويمثل خارطة طريق نحو تمكين النساء في المجال الرقمي وضمان بيئة رقمية أكثر أمانًا وشمولًا.

نثمّن عاليا تعاون مركز حملة المثمر والتزامه الدائم بدعم قضايا العدالة الرقمية وحقوق الإنسان، آملين أن يستمر هذا العمل والتعاون المشترك من أجل تحقيق مجتمع أكثر مساواة وأمانًا للجميع.

أمال خريشة
المديرة العامة لجمعية المرأة العاملة الفلسطينية للتنمية

الفهرس

أعد مركز حملة هذا الدليل «الامان والتحول الرقمي من من منظور النوع الاجتماعي» لصالح جمعية المرأة العاملة الفلسطينية للتنمية (PWWSD) في إطارمشروع النسوية من أجل حقوق النساء الاقتصادية. بهدف الدليل الى تعزيز الفهم والتطبيق العملي لمبادئ الأمان الرقمي بأسلوب يأخذ بعين الاعتبار التحديات الخاصة التي تواجهها النساء في الفضاء الرقمي. يطمح هذا الدليل إلى خلق بيئة رقمية أكثر شمولية وأمانًا، من خلال تمكين النساء من تطوير قدراتهن في مجال الأمن الرقمي ومواجهة المخاطر المتزايدة التي تعترضهن على الإنترنت، كالتمييز والعنف المبني على النوع الاجتماعي.

يأتي هذا الدليل استجابةً لتزايد الاعتماد على التكنولوجيا في الحياة اليومية وما يرافقه من تحديات جديدة تتطلب استراتيجيات فعالة لحماية حقوق النساء في العالم الرقمي. عبر تقديم أدوات عملية ومعارف متخصصة، يسعى هذا الدليل إلى تمكين النساء من التعامل مع التحديات الرقمية بثقة ومسؤولية، وتعزيز حضورهن الفاعل في الفضاء الإلكتروني.

إننا نطمح من خلال هذا العمل إلى تحقيق تغيير إيجابي يسهم في بناء مجتمعات أكثر شمولية ومساواة، حيث يتمكن الجميع من المشاركة في الفضاء الرقمي بشكل آمن وعادل. نأمل أن يكون هذا الدليل أداة ملهمة ومؤثرة تدعم النساء في رحلتهن نحو تحقيق الأمان الرقمي والتمكين المجتمعي.

الفصل الأول:
الإحصائيات والحقائق

يعرض هذا الفصل مجموعة من الحقائق والإحصائيات التي تسلط الضوء على التحديات التي تواجه النساء في المجال الرقمي على المستويات العالمية، الإقليمية، والمحلية. ويهدف إلى تقديم صورة واضحة عن واقع الأمان الرقمي للنساء، من خلال استعراض معدلات التحرش الإلكتروني، والاختراقات، والفجوات القانونية التي تزيد من تعرض النساء للخطر. كما يقدم الفصل بيانات تدعم الحاجة الملحة لتبني استراتيجيات فعالة لحماية النساء وتعزيز أمنهن الرقمي.

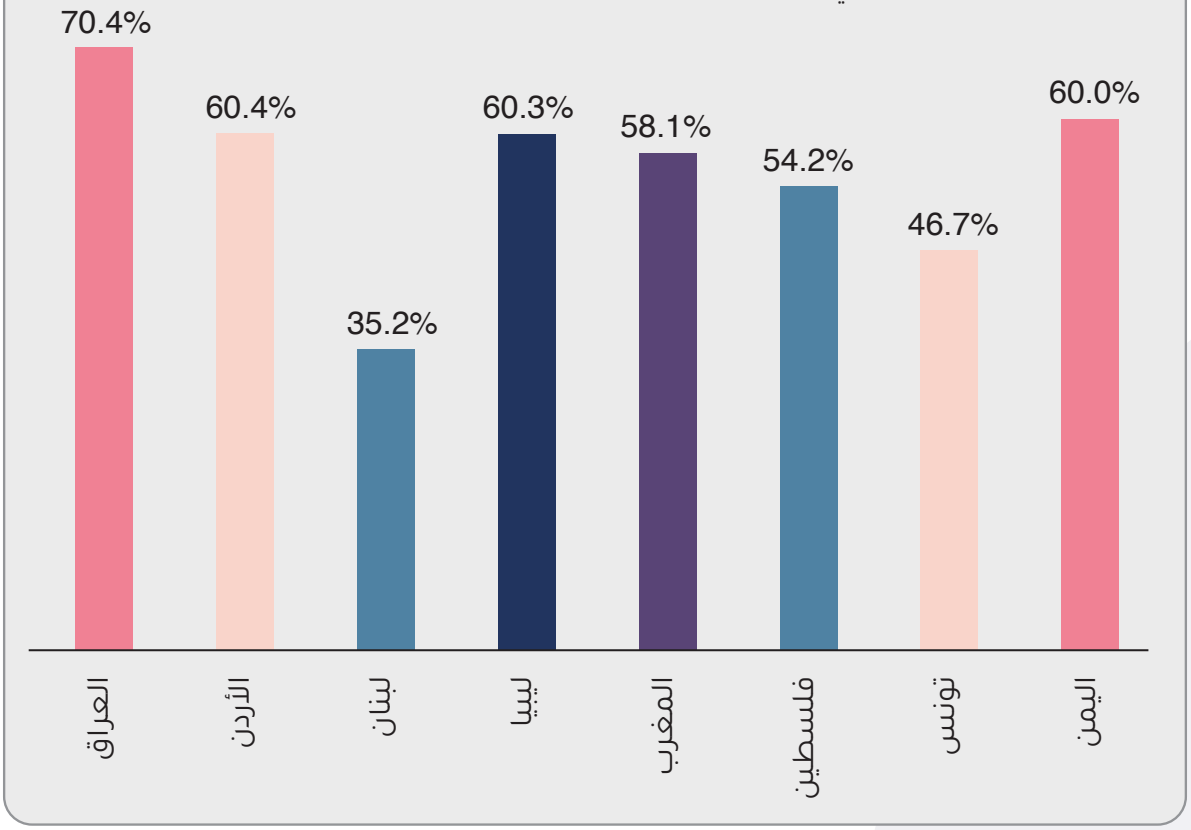
عالمياً

وفق دراسة أجريت من قبل (The Economist Intelligence Unit)و التي تعتبر أحد أبرز المنصات الإعلامية العالمية، 38% من نساء العالم تعرضوا لعنف رقمي من نوع ما، مما يجعل هذه الظاهرة أحد أبرز التحديات الرقمية التي تواجه النساء عالميًا. ورغم غياب إحصائيات دقيقة حول اختراق أجهزة النساء، فإن الهجمات السيبرانية التي تستهدف الأفراد بشكل عام، بما في ذلك النساء، تشهد زيادة مستمرة.

إقليمياً

وفق دراسة بعنوان (العنف ضد المرأة في الفضاء الرقمي) أجريت من قبل هيئة الأمم المتحدة للمرأة، والتي اقتصرت على 11،500 مستطلع من 14 دول عربية (المغرب وليبيا وتونس والأردن وفلسطين ولبنان والعراق واليمن)، 60% من المستطلعات سبق لهن التعرض لعنف عبر الانترنت و أبلغن عنه، للمزيد من المعلومات يرجى مراجعة الدراسة.

رسم بياني 1: نسبة النساء اللاتي سبق لهن التعرض لعنف عبر الانترنت و أبلغن عن ذلك في السنة الماضية، حسب البلد وفق دراسة UNWOMEN



من الجدير بالذكر كذلك أن المنصة ذات الوجود الأكبر لهذه الظاهرة كانت Facebook بنسبة43%، تليها Instagram بنسبة 16%، ثم واتساب بنسبة11%، مما يضع مجموعة Meta في محور هذه المشكلة.

محلياً

في نفس الدراسة الإقليمية، 54.2% من النساء الفلسطينيات قد تعرضن لأشكال مختلفة من العنف عبر الانترنت و قاموا بالتبليغ عن الحادثة، كما و يجب الأخذ بعين الإعتبار أنه وفقاً لنفس الدراسة، 44%من النساء الالتي تعرضن للعنف عبر الانترنت، تعرضن له أكثر من مرة.

المنظومة القانونية والفجوات

تشير التقارير إلى أن هناك تحسنًا في الأطر القانونية لمكافحة العنف الرقمي ضد النساء في بعض الدول العربية حيث تتضمن هذه التحسينات تطوير قوانين تجرّم العنف الإلكتروني بالتحديد، بالإضافة إلى تعزيز التدابير القانونية لضمان حماية خصوصية النساء عبر الإنترنت كإقامة خطوط خاصة بضحايا العنف عبر الانترنت و بوابات الكترونية لتقديم الشكاوي. كما يتم العمل على تحسين آليات الإنفاذ القانونية لضمان استجابة أكثر كفاءة وفعالية لهذه القضايا. لكن هذا لا ينفي استمرارية وجود فجوات قانونية - مجتمعية في عدة دول عربية تمكن بعض الأشخاص من ممارسة العنف المبني على النوع الإجتماعي عبر الانترنت بدون مساءلة.

يقدم هذا الدليل مجموعة من الأدوات والموارد التي تهدف إلى تعزيز القدرات الفنية والمهارات الضرورية للنساء لفهم ومواجهة التحديات الأمنية في العصر الرقمي الحديث حيث يتمحور التوجيه في هذا الدليل حول استخدام أدوات الأمن الرقمي بشكل فعال وآمن، وتحسين التوعية بمخاطر الإنترنت وكيفية التعامل معها بطريقة آمنة ومسؤولة.

لماذا هذا الدليل؟

تم تصميم هذا الدليل لتزويد النساء، وخاصة الناشطات والمدافعات عن حقوق الإنسان، بالأدوات والمعرفة اللازمة لحماية أنفسهن في الفضاء الرقمي حيث أنه مع تزايد الاعتماد على الإنترنت للتعلم والتواصل والتمكين، أصبح التنقل بأمان في العالم الرقمي ضرورة ملحة وليس مجرد خيار.

يحمل الإنترنت فرصًا هائلة، ولكنه في الوقت نفسه يطرح مخاطر فريدة للنساء والفتيات، بما في ذلك التحرش والابتزاز وانتهاك الخصوصية. عبر هذا الدليل، يمكن للنساء استعادة السيطرة على الأدوات الرقمية وتحويلها إلى قوة إيجابية لصالحهن.

لماذا التركيز على النساء؟

الأمان الرقمي ضروري للجميع، ومع ذلك، غالبًا ما تواجه النساء تهديدات محددة يمكن أن تؤثر بشكل كبير على حياتهن، مسيرتهن المهنية، وشعورهن بالأمان من منظور النوع الاجتماعي على الإنترنت. إن التعرف على هذه التحديات الفريدة هو الخطوة الأولى نحو معالجتها، فحسب نتائج مركزية لدراسة بعنوان «شبكة منتهكة: العنف الجندري ضد الفلسطينيات في الفضاء الرقمي» أعدها مركز حملة مع الباحثة د. نجمة علي كانت النتائج المركزية للدراسة كالاتي:

- نحو **65%** من المستطلعات لا يستخدمن صورهن الشخصية كصورة تعريفية (بروفايل).
- نحو **28%** من المستطلعات سبق أن تعرضن لمحاولات اختراق حساباتهن على منصات التواصل الاجتماعي.
- نحو **17%** من المستطلعات سبق أن تعرضن لمحاولات تسريب الصور على منصات التواصل الاجتماعي.
- نحو **16%** من المستطلعات تعرضن لمحاولة ابتزاز على منصات التواصل الاجتماعي.
- نحو **36%** من المستطلعات اللواتي تعرضن للابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي كان ذلك ابتزازًا جنسيًا.
- نحو **50%** من المستطلعات يشعرن بأنهن مراقبات عبر وسائل التواصل الاجتماعي.
- نحو **25%** من المستطلعات تعرضن لتعليقات أو مضايقات (استهزاء أو تحقير) لكونهن نساء.
- نحو **33%** من المستطلعات اللواتي تعرضن لمضايقات عبر وسائل التواصل الاجتماعي فقط حذفن حساب المرسل ولم يتخذن أي إجراء آخر.

لا يسلط هذا الدليل الضوء على هذه القضايا فحسب، بل يقدم أيضًا نصائح مصممة خصيصًا للمساعدة في تقليل المخاطر، مما يجعل الفضاء الرقمي أكثر شمولية وأمانًا للنساء

يغطي هذا الدليل مجموعة من المواضيع الأساسية للتمكين والأمان الرقمي من منظور النوع الاجتماعي:

- فهم المشهد الرقمي: نظرة عامة على أسباب وأهمية الأمان الرقمي أكثر من أي وقت مضى، واهم المخاطر الرقمية خاصةً بالنسبة للنساء والشابات بما يشمل ذوات الإعاقة
- التهديدات: شرح وتبيان لأهم المخاطر المحتملة وطرق حصولها وآليات تخفيف الضرر واهم الاجراءات لأمانك الرقمي.
- إجراءات الأمان الرئيسية: إرشادات لتأمين الأجهزة الشخصية والحسابات .

صُمم كل فصل ليكون متاحًا معلوماتيًا وممكّنًا من حيث التطبيق، بغض النظر عن خلفيتك التقنية. لقد اشتمل الدليل على سيناريوهات واقعية، وأدلة خطوة بخطوة، ونصائح عملية لجعل المعلومات قابلة للتطبيق ومفيدة قدر الإمكان.

مستخدمة/مستخدم الدليل

هذا الدليل مُوجه إلى الفئات التي عملت معها جمعية المرأة العاملة الفلسطينية للتنمية، بما في ذلك المؤسسات النسوية القاعدية الشريكة في برنامج النسوية من أجل حقوق النساء الاقتصادية و/أو موظفيها. كما يستهدف الدليل الفئات المستهدفة أو المستفيدة

من الجنسين كأفراد أو كمجموعات. وبشكل عام، بإمكان أي فرد استخدام هذا الدليل للوقاية من مخاطر الأمن الرقمي وتجنبها.

كيفية استخدام هذا الدليل

لا تترددوا في الغوص في أي فصل يثير اهتمامكم، أو قراءة الدليل من الغلاف إلى الغلاف لفهم شامل. إلى جانب المحتوى الرئيسي، ستجدون قوائم تحقق، نصائح سريعة، وتوصيات بموارد لدعم رحلتكن/رحلتكم في تعزيز الأمان الرقمي.

دوركن/دوركم في العالم الرقمي

من خلال اتخاذ خطوات لحماية أنفسكن/أنفسكم على الإنترنت، أنتن /انتم تساهمن وتساهمون في جعل العالم الرقمي أكثر أمانًا للجميع. المعرفة قوة، ومن خلال تمكين أنفسكن وأنفسكم بمعرفة الأمان الرقمي، أنتم تمهدون الطريق لثقة وأمان أكبر على الإنترنت، ليس فقط لأنفسكن ، بل للنساء الأخريات في مجتمعكم.

الفصل الثاني:
المشهد الرقمي للنساء

الفجوة الجندرية الرقمية

في عالمنا المترابط اليوم، يعتبر الإنترنت موردًا حيويًا يقدم فرصًا للتعليم والتوظيف وبناء المجتمع والتعبير عن الذات. ومع ذلك، الوصول إلى هذه الفضاءات الرقمية والتجارب ليس موحداً، مع استمرار وجود فجوة جندرية رقمية ملحوظة. هذه الفجوة لا تنعكس فقط في الوصول إلى التكنولوجيا والإنترنت، ولكن أيضًا في المهارات والفرص لاستخدام الأدوات الرقمية بفعالية وبشكل آمن. غالبًا ما تواجه النساء والفتيات حواجز اجتماعية وثقافية واقتصادية تحد من وصولهن إلى الموارد الرقمية، وهذه مشكلة أساسية يجب معالجتها لضمان المساواة بين الجنسين في العصر الرقمي.

المخاطر الفريدة للنساء على الإنترنت

يمكن أن تختلف تجارب النساء على الإنترنت بشكل كبير عن تجارب الرجال، حيث غالبًا ما تواجه النساء تهديدات محددة إضافة للتهديدات التقليدية، حيث يمكن أن تؤثر على سلامتهن وخصوصيتهن. تشمل هذه التهديدات التحرش الإلكتروني، والمطاردة الإلكترونية، والفضح (نشر المعلومات الخاصة أو التعريفية علنًا)، والإساءة بناءً على الصور، والابتزاز. يمكن أن تكون لهذه التهديدات تداعيات في العالم الواقعي، بما في ذلك الصدمات النفسية، وتآكل السمعة، أو حتى الخطر الجسدي. التعرف على هذه المخاطر ضروري لتطوير استراتيجيات فعالة لمكافحتها ولإنشاء بيئات رقمية أكثر أمانًا للنساء.

المخاطر الرقمية: تعريفها وأنواعها

المخاطر الرقمية هي التهديدات التي يمكن أن تؤثر على الأفراد والمؤسسات في البيئة الإلكترونية أو عبر الإنترنت.

النساء على الإنترنت يواجهن مجموعة من التهديدات التي قد تؤثر بشكل خاص على سلامتهن وخصوصيتهن ورفاهيتهن النفسية. هذه المخاطر تشمل، ولكن لا تقتصر على:

- التحرش الإلكتروني: يتضمن هذا النوع من التحرش الرسائل العدائية والتهديدات والتعليقات الجنسية غير المرغوب فيها. النساء، وخاصة تلك اللاتي لديهن حضور بارز وناشطات على الإنترنت، غالبًا ما يكن أهدافًا لهذه الأنواع من الهجمات.
- المطاردة الإلكترونية: تشمل متابعة الضحية عبر الإنترنت وجمع معلومات عنها دون موافقتها، مما يؤدي إلى شعور بالخوف والقلق.
- الفضح (Doxing): نشر معلومات خاصة أو حساسة عن الأفراد عبر الإنترنت دون موافقتهم، وهو ما يمكن أن يشمل العناوين الشخصية، وأرقام الهواتف.
- الإساءة بناءً على الصورة: توزيع الصور أو مقاطع الفيديو الخاصة أو الحساسة دون موافقة الشخص المعني، والتي يمكن أن تتضمن الانتقام الإباحي.
- التلاعب العاطفي والاحتيال: العلاقات الزائفة التي يتم بناؤها عبر الإنترنت بغرض الاحتيال المالي أو العاطفي.
- الابتزاز: هو جريمة التهديد بالكشف عن معلومات محرجة أو ضارة عن شخص ما للجمهور او العائلة او الشركاء مالم ت/يخضع الضحية لطلبات المبتز.

- التصيد: هو انتحال شخصية شخص آخر بهدف الحصول على معلومات معينة أو الاختراق.
- البرمجيات الخبيثة: هي أي برنامج يقوم بالتصرف بنية خبيثة على الجهاز مثل:
  - الفيروسات: هي برمجيات خبيثة بمجرد ما أن تدخل على جهاز الكومبيوتر تبدأ بنسخ نفسها لتصل إلى أكبر كم من البرامج النظيفة لتستقر فيها، فتصنف هذه البرامج كبرامج مَعدِية (infected).
  - الديدان: تشبه الفيروسات و لكنها تنسخ نفسها لتصيب الأجهزة الأخرى على الشبكة.
  - برمجيات التجسس: هي برمجيات تقوم بجمع أكبر كم ممكن من البيانات مع الإبقاء على سِريّة وجودها على الجهاز قدر المستطاع.
  - البرمجيات المموهة (حصان طروادة): هي برمجيات تبدو نظيفة و مفيدة من الخارج ولكنها خبيثة من الداخل، مثل برنامج تعديل فيديوهات يقوم بدور برمجية تجسس في الخلفية، و تكون بالغالب إصدارات مقرصنة من برامج معروفة.
  - برامج الفدية: هي برامج تشفير الملفات مقابل ابتزاز مالي.
  - مسجل لوحة المفاتيح (keylogger): هو عبارة عن برنامج يقوم بتسجيل كل ضغطة زر يقوم بها المستخدم، لمشاركتها فيما بعد مع الجهات المنتهِكة.
- الهندسة الاجتماعية: هو استخدام أساليب علم النفس بهدف الوصول إلى معلومات معينة تساعد المخترق في أهدافه.
- ثغرات الساعة صفر: هي الثغرات البرمجية الغير مكتشفة بعد ويقوم باستغلالها المخترقين.

الفصل الثالث:
التهديدات وطرق الوقاية

البرمجيات الخبيثة

- أنواعها (على سبيل الذكر وليس الحصر):
  - الفيروسات.
  - حصان طروادة.
  - برامج الفدية.
  - برمجيات التجسس.
  - الديدان.
  - مسجل لوحة المفاتيح (keylogger).
- كيف تحدث:

غالبًا ما تنتشر البرمجيات الخبيثة من خلال تحميل ملفات مصابة.

النقر على روابط ضارة، أو فتح مرفقات البريد الإلكتروني من مصادر غير معروفة أو من خلال وسائل التواصل الاجتماعي.

استخدام memory flash لأشخاص اخرين او وضعها بأجهزة اشخاص اخرين.

تصفح الويب و مواقع غير آمنة.

الهاتف المحمول.

- نتائجها:
  - يمكن أن تتسبب في تدمير نظام التشغيل، سرقة المعلومات الحساسة، أو حتى السيطرة على جهازك.
- الوقاية: تثبيت وتحديث برنامج مكافحة الفيروسات بانتظام. تجنب تحميل الملفات أو النقر على الروابط من مصادر غير معروفة. تحديث نظام التشغيل وجميع البرامج بانتظام لإصلاح ثغرات الأمان. عدم مشاركة المعلومات الشخصية إلا مع من نثق بهم.
- امتصاص الأضرار: إذا تم الإصابة، قطع الاتصال بالإنترنت لمنع اتصال الفايروس او برمجيات التجسس بالخارج. قم بفحص كامل للنظام ببرنامج مكافحة الفيروسات و اتبع تعليماته لإزالة العدوى.

التصيد الاحتيالي والهندسة الاجتماعية

- كيف يحدث: غالبًا ما تأتي محاولات التصيد الاحتيالي على شكل رسائل بريد إلكتروني أو رسائل تحاول خداعك لتقديم معلومات حساسة من خلال التنكر ككيان موثوق او شخص معروف. وتعتمد الهندسة الاجتماعية على التلاعب بالأفراد لخرق إجراءات الأمان العادية.
- انواعه:
  - التصيد العشوائي (التصيد الغير موجه): حيث تكون هجمات التصيد هنا عشوائية

ولا تستهدف شخص بذاته وتكون بالعادة ابسط وسهلة الانكشاف، و يكون الحافز شيء مرغوب بشكل عام مثل المال أو السيارات.

- التصيد بالرمح (التصيد الموجه): المقصود هنا هو التصيد المستهدف لشخص بحد ذاته وهذا النوع من هجمات التصيد يكون أكثر تعقيداً من الذي سبقه ويستخدم وسائل مختلفة وتقنيات مختلفة و يكون الحافز مصمم ليجذب الهدف بالتحديد مثلاً كأن يدعي الصياد أن بحوزته معلومات مهمة بالنسبة لمقال قيد الإنشاء من قبل صحفي.

- نتائجها:
  - تحميل برمجيات خبيثة على الأجهزة الشخصية.
  - سرقة كلمات المرور.
  - الحصول على معلومات حساسة وشخصية.

- الوقاية:
  - كن متشككًا في الرسائل الإلكترونية التي تطلب معلومات حساسة، حتى لو بدت أنها تأتي من مصدر شرعي.
  - عدم النقر على الروابط ما لم يتم التحقق منها بشكل صحيح عن طريق تمرير الفأرة فوقها.
  - التحقق من: المرسل، الموضوع، وكافة الحقول.
  - مراجعة المحتوى بعناية. هل هو موجه لك شخصيا؟
  - عدم فتح المرفقات بأسماء عامة.
  - عدم قبول الدعوات لحضور اجتماع غير مخطط له.
  - التحقق دائمًا، على قناة أخرى مثل signal، من المصدر الرسمي مباشرة مثل التحقق من مرسل البريد الإلكتروني أو دعوة التقويم.
- امتصاص الأضرار: إذا كنت تشكين/تشك في أنك كنت ضحية للتصيد الاحتيالي:
  - قم بتغيير كلمات المرور الخاصة بك فورًا وراقب حساباتك لأي نشاط غير عادي.
  - قم بفحص أجهزتك الشخصية بمكافح الفيروسات للتأكد من عدم وجود برمجيات خبيثة.
  - تفعيل خاصية التحقق من خطوتين على حساباتك.
  - قم بإبلاغ الجهات المعنية بأسرع وقت خصوصاً إذا كان الضرر مادياً كإبلاغ البنك في حالة تسريب بياناتك المصرفية أو إصدار حوالات إحتيالية.

التحرش الإلكتروني والمطاردة الإلكترونية

- المطاردة عبر الإنترنت هي هجوم رقمي على شخص لأسباب تتعلق بالغضب أو الانتقام أو السيطرة.
- النساء أكثر عرضة من الرجال للتعرض للمطاردة، خاصة من قبل الشريك الحميم. كما

أن معظم الذين يلاحقونهم من قبل شريك حميم يواجهون أيضًا اعتداء جسديًا من هذا الشخص.

- تتيح التكنولوجيا للمطارد أن يحاول البقاء مجهول الهوية.
- اشكالها:
  - تشمل هذه التصرفات الاتصال المتكرر غير المرغوب فيه الذي يسبب الخوف أو الضيق.
  - مضايقة أ/و إهانة أ/و إحراج الشخص المستهدف/ة.
  - مضايقة العائلة أ/و الأصدقاء أ/و أصحاب العمل لعزل الشخص.
  - تكتيكات لجعل الهدف خائفًا.
  - يقوم المطارد بتشجيع رفاقه عبر الإنترنت على المشاركة في المضايقة، مما يزيد من ضائقة الشخص.
- كيف تحدث:
  - يمكن أن يحدث ذلك من خلال وسائل التواصل الاجتماعي، البريد الإلكتروني، وغيرها من منصات التواصل الرقمي.
  - الاتصال بالشبكة: يمكن لنقاط اتصال WIFI والبلوتوث أن تكشف عن موقعك وتسهل على الأشخاص اختراق هاتفك.
  - الرسائل القصيرة / المكالمات: إذا تمكن المطارد من الحصول على رقم هاتفك المحمول، فقد يضايقك من خلال رسائل SMS والمكالمات الهاتفية. قد يستخدمونه مع نظام تحديد المواقع العالمي (GPS) للكشف عن معرفتهم بموقعك. يمكن للمطاردين أيضًا استخدام برامج التجسس لاعتراض رسائلك ومكالماتك.
  - كلمات المرور: إذا لم يكن هاتفك محميًا بكلمة مرور، فيمكن لأي شخص يضع يده عليه الوصول إلى معلوماتك. يعد اختراق كلمة المرور أمرًا شائعًا، وكلما زاد معرفة المطارد عنك ، زادت احتمالية تخمينه لكلمات المرور الخاصة بك. بالإضافة إلى ذلك، من السهل تخمين كلمات المرور الأكثر شيوعًا، مثل «password» و «123456» و «letmein» و جميع كلمات المرور المتعلقة ب «qwerty».
  - GPS: قد يخبرك نظام تحديد المواقع العالمي (GPS) بالمقاهي القريبة ، ولكن يمكنه أيضًا السماح للآخرين بمعرفة مكانك.
  - الصور: تحتوي الصور على معلومات مضمنة في خصائصها تتضمن وقت ومكان التقاطها. يمكن أيضًا معرفة الموقع بناءً على ما هو موجود في الصورة.
  - التطبيقات: قد تحتوي التطبيقات الضارة على برامج تجسس. كلما زادت الإمكانات التي يتمتع بها هاتفك الذكي، مثل GPS، زادت إمكانية استخدام هذه الإضافات للتجسس عليك، وأيضا تطبيقات مثل سناب شات تفعيل خاصية عرض الموقع تسهل على المطاردين معرفة مكانك.
  - المدونات: يحب الملاحقون التسكع في مساحات التعليق ونشر التهديدات والإهانات. هذا شائع بشكل خاص عندما يكون المطارد شخصًا غير معروف لك.

- وسائل التواصل الاجتماعي: من السهل جدًا جمع معلومات حول المكان الذي تعيشين فيه والأماكن التي تزورينها بانتظام والأشخاص الذين تهتمين بهم من المشاركات والصور. قد يكشف أصدقاؤك أيضًا عن معلومات عنك عن غير قصد.
- البريد الإلكتروني: غالبًا ما يتم إرفاق عناوين البريد الإلكتروني بالأسماء والملفات الشخصية الحقيقية ، وقد يستخدمها الملاحقون للاتصال بك مباشرةً. مرة أخرى ، يمكن استخدام برامج التجسس للوصول إلى بريدك الإلكتروني الخاص.

- الوقاية:

- ضبط إعدادات الخصوصية على وسائل التواصل الاجتماعي للتحكم فيمن يمكنه التواصل معك ورؤية منشوراتك حيث يمكنك الوصول الى إعدادات الخصوصية على منصة انستغرام من هنا، والفيسبوك هنا.
- حماية بياناتك وصورك:
- تُفقد الهواتف وتُسرق بسهولة، مما يجعل بياناتها عرضة للخطر. انقلي الصور إلى موقع أكثر أمانًا، في أسرع وقت ممكن. أثناء وجودهم على هاتفك، قومي بتشفيرهم واحتفظي بهم في ملف محمي بكلمة مرور.
- في نظام التشغيل ios قومي بإيقاف تشغيل الحفظ السحابي التلقائي. يتم تحميل كل صورة تلتقطها على iPhone تلقائيًا إلى iCloud من Apple. لإيقاف مشاركة iCloud، انتقلي إلى الإعدادات> iCloud> قومي بالتمرير لأسفل إلى الصور وحركي الخيار لإيقاف التشغيل لتعطيل iCloud تمامًا، انتقلي إلى أسفل القائمة واضغطي على «حذف الحساب».
- على هواتف Android يمكن نسخ الصور احتياطيًا إلى خدمة Google Photos السحابية، ولكن سيتم إيقاف هذا عند إعداد حساب Google لأول مرة. تحقق مرة أخرى من الإعدادات الخاصة بك من خلال الانتقال إلى تطبيق الصور> حدد الإعدادات العامة> مرر النسخ الاحتياطي التلقائي إلى إيقاف. تحقق من السحابة الخاصة بك بشكل متكرر لمعرفة بالضبط ما يتم تخزينه هناك.
- لا تقومي ببيع جهازك القديم أو إعطائه لأحد إلا بعد استبدال وحدات التخزين.
- حماية هاتفك بكلمة مرور. سيؤدي ذلك إلى الحفاظ على أمان بياناتك إذا فقدت هاتفك أو حاول شخص ما استخدامه دون إذنك.
- إستخدام تطبيقات تواصل تقوم بحذف ال metadata من الصور قبل إرسالها مثل signal .
- إخفاء موقعك:
  - قومي بتفعيل إعدادات GPS عندما تحتاج إليها. تحتوي غالبية الهواتف الذكية على شرائح GPS يمكنها تحديد الموقع الجغرافي للهاتف في ثوانٍ. هل تحتاجين هذا في كل وقت؟ عادة ما نقوم بتنشيط GPS في الإعدادات> الخصوصية> الموقع.
  - قومي بتعطيل GPS على كاميرا هاتفك المحمول. يمكن تضمين هذه المعلومات الجغرافية في الصور مع تحديد وقت ومكان التقاط الصورة بالضبط (ميتا داتا). جنبًا إلى جنب مع المحتوى، يمكن أن يكون من السهل تمييز المكان الذي تعيشين فيه أو تعملين أو تلعبين فيه. تحققي من الدليل الخاص بك للحصول

على التعليمات. على سبيل المثال، على جهاز iPhone، انتقلي إلى الإعدادات> الخصوصية> الموقع، وقومي بتعطيل خيار «الكاميرا».

- الممارسات عبر الإنترنت

- لا تنشري تفاصيل الاتصال الشخصية الخاصة بك علنا. ولا تشاركي أي شخص آخر بها. غالبًا ما ينشر الأشخاص أرقام هواتفهم في تعليقات Facebook دون التفكير في أنه يمكن لأي شخص آخر رؤيتها. استخدم المراسلة المباشرة بدلاً من ذلك.
- ابحثي بنفسك. قومي بإجراء بحث منتظم على الإنترنت عن اسمك لمراقبة مكان ظهورك على الإنترنت أو إعداد تنبيه بذلك، يمكن أيضاً استخدام تقنيات الذكاء الإصطناعي للتأكد من البيانات المنشورة المتعلقة بك مثل perplexity.
- حافظي على التكنولوجيا الخاصة بك محدثة وآمنة: قومي بتثبيت (وتحديث!) البرامج ذات الصلة. اختاري المصدر المفتوح عندما تستطيعين ذلك.
- تعرفي على المفاضلة بين الأمان والراحة. هل تحتاجين حقًا إلى تثبيت هذا التطبيق الجديد إذا لم تكوني متأكدًة بنسبة ٪100 أنه لن يجعل جهازك عرضة للخطر؟
- تحركي بسرعة لمنع المطاردة الرقمية. الكثير من الناس لا يتخذون أي إجراء لأنهم يعتقدون أنهم يبالغون في رد فعلهم، لكن تكرار الهجمات قد يشلّك. سجلي الحوادث (الوقت، المكان، الحدث). إذا اتخذت إجراءً سريعًا وحجبت فرص المطارد لمضايقتك، فقد يفقد الاهتمام.
- أوضحي أنك لا تريدين أن يتم الاتصال بك. حذري من أن أي اتصال آخر سينتج عنه تقرير للشرطة. قد يتوقف الاتصال عند هذا الحد. اكتبي هذا مرة واحدة ووثقيها.
- توجهي إلى السلطات: يختار المزيد من النساء اللواتي يتعرضن للتحرش عبر الإنترنت الذهاب إلى السلطات، مما أدى إلى تغييرات في التشريعات. إذا تضمنت المضايقات مجموعات تحض على الكراهية أو تهديدات بالقتل أو الأذى الجسدي و/أو منشورات عامة لموقعك أو معلومات الاتصال الخاصة بك، فيجب عليك الاتصال بسلطات إنفاذ القانون على الفور. كلما جمعت المزيد من الأدلة، زادت قدرتهم على التصرف بشكل أسرع و أكثر فعالية.
- احصلي على الدعم العاطفي. أخبري عائلتك وأصدقائك الموثوق بهم أنك تتعرضين للمطاردة إذا ما أمكنك ذلك. يعد دعمهم أمرًا بالغ الأهمية أثناء المطاردة وفي أعقاب ذلك لمساعدتك على التأقلم.
- أبلغي مديرك/تك في العمل إذا لزم الأمر. إذا كنت تعتقدين أن هذا الشخص قد يضايقك في مكان العمل، فمن المهم إخطار صاحب العمل. من المرجح أن يدعمك رئيسك في العمل إذا تلقى لاحقًا اتصالًا من المطارد، وقد يكون قادرًا على تخفيف الضرر المهني وتقديم الأدلة.
- نظفي الضرر. إذا كشفت عمليات البحث الخاصة بك على الإنترنت أن المطارد نشر معلومات عنك، فقومي بإلقاء نظرة على «كيفية حذف الأشياء من الإنترنت» للحصول على مزيد من المعلومات.

- توثيق جميع حالات التحرش. استخدم ميزات الحظر والتبليغ على المنصات الاجتماعية.
- امتصاص الأضرار:
- إذا تصاعد التحرش، أبلغي/أبلغ عنه لمنصة (حر(وفكر/ي في إشراك الشرطة.
- ابحثي/ابحث عن الدعم من المنظمات المخصصة لمساعدة ضحايا التحرش عبر الإنترنت.

الفضح (Doxing)

- كيف يحدث: ينطوي الفضح على البحث وبث المعلومات الخاصة أو التعريفية عن شخص ما، عادةً بنية ضارة. غالبًا ما ينبع ذلك من قواعد البيانات العامة، وسائل التواصل الاجتماعي، أو البيانات الخاصة المخترقة.
- الحلول:
- قللي/قلل من كمية المعلومات الشخصية التي تشاركها على الإنترنت.
- ابحثي/ابحث بانتظام عن اسمك على الإنترنت للتحقق من المعلومات التي يمكن الوصول إليها بشكل عام. -
- استخدم/ي محركات البحث والخدمات التي تركز على الخصوصية.
- امتصاص الأضرار: -
- إذا كنت ضحية للفضح، اطلب/ي إزالة معلوماتك من المواقع التي نشرتها، يمكن أيضاً إبلاغ منصة حملة عنها.
- زد من إجراءات الخصوصية عبر الإنترنت وفكر في طلب استشارة قانونية.

الابتزاز

الابتزاز هو جريمة التهديد بالكشف عن معلومات محرجة أو ضارة عن شخص ما للجمهور أو العائلة أو الشركاء ما لم ت/يخضع هذا الشخص للمبتز.

نظرًا لأن المعلومات عند المبتز عادة ما تكون صحيحة، فهو يطلب المال - أو خدمات أخرى - مقابل عدم الإفصاح عن المعلومات. يمكن أن يشمل «سعر» الابتزاز أيضًا الخدمات الجنسية أو إبقاء الشخص في علاقة. يمكن أن يحدث الابتزاز بأشكال مختلفة منها العاطفية أو المادية.

- اشكاله:
- يمكن أن يتضمن الابتزاز عبر الإنترنت نشر الصور الحميمة على ما يسمى بمواقع «الانتقام الإباحية/ البورن الانتقامي»، إن البورن الانتقامي هو في الواقع انتهاك صارخ لخصوصية المرأة، حيث يتم نشر مقاطع الفيديو والصور الفوتوغرافية الخاصة والشخصية دون موافقة على الشبكة لأغراض الابتزاز و/أو الإذلال. هذا عمل عنيف ولا يجب الخلط بينه وبين المحتوى الإباحي.
- شكل آخر للابتزاز هو سرقة الصور الحميمة للنساء (غالبًا من خلال القرصنة غير

القانونية) ثم تُنشر على الإنترنت. قد يتم نشر الصور مع معلومات الاتصال بالمنزل والعمل، لتشجيع المشاهدين على التحرش بالمرأة.

- الابتزاز عبر الإنترنت عبارة عن حقيبة مختلطة حيث قد يسرق المبتزون صورًا حميمة أو يزيفونها. قد يكون السعر المطلوب هو المال أو السيطرة الجسدية والعاطفية على الشخص الذي يتم ابتزازه. في حالة «الانتقام الإباحي» بدون دافع مالي، يبدو أن الثمن هو إذلال خالص للمرأة.
- كل حالة مختلفة. قد يكون بعض المبتزين مخادعين أو قد يتلاشى بعد رفض الدفع أو حظرهم، بينما قد يهدف آخرون إلى إحداث ضرر حقيقي. بغض النظر، هذا ليس خطأ المرأة!

- امتصاص الأضرار:

- الإبلاغ عن الحالة لجهات موثوقة (مراكز دعم، شخص من العائلة أو الأصدقاء، شرطة؟)
- ضعي في اعتبارك أنه من غير المرجح أن يوقف الدفع مطالب الابتزاز.
- لا تواجهي الشخص (عبر الإنترنت أو غير ذلك)؛ يجب إنهاء جميع الاتصالات معه على الفور.
- قومي بحظرهم من حسابات الشبكات الاجتماعية الخاصة بك وتغيير إعدادات الخصوصية لمحاولة منعهم من الوصول إلى قائمة أصدقائك.
- قومي بتغيير جميع كلمات المرور الخاصة بك باستخدام رموز أبجدية رقمية قوية وفريدة من نوعها إذا كنت تعتقدين أنك تعرضت للاختراق.
- ضعي في اعتبارك بدء حسابات بريد إلكتروني جديدة. دعي جهات الاتصال تعرف أن حساباتك القديمة قد تم اختراقها ويجب ألا تفتح أي رسالة منها.
- ضعي ملصقًا على كاميرا الإنترنت الخاصة بك.
- قومي بالبحث عن اسمك عبر الإنترنت أو قومي بإعداد تنبيهات لإعلامك بأي شيء جديد يتعلق باسمك.

- حالة دراسية: هذه هي الخطوات التي اتخذتها امرأة ما عند تعرضها للابتزاز بسبب فعل جنسي ادعى المبتزون أنهم التقطوه أمام الكاميرا... في النهاية، لم يستمر المبتزون بمطالبهم.

- أنا ... لم أبذل أي محاولة للدفع لهم.
- لقد حظرتهم من قوائم جهات الاتصال الخاصة بي ... ثم حذفت حساب Messenger الخاص بي.
- لقد ألغيت صفحتي على Facebook ونشرت رسالة إلى أصدقائي تشير إلى أن شخصًا ما اخترق حسابي ويقوم بإرسال الرسائل عشوائيًا وأنني سأبقى بعيدًة لبعض الوقت. أي رسالة يتلقونها مني هي مريبة ويجب حذفها على الفور.
- لقد أنشأت العديد من تنبيهات Google لتنبيهي إذا تم نشر أي شيء يحمل اسمي.
- لقد تحققت من موقع YouTube لمعرفة ما إذا تم نشر أي شيء عني، وتحققت أيضًا من سياسة الخصوصية الخاصة بهم.

- أخيرًا، أبلغت صديقًا مقربًا لي وطلبت منه أن يراقب... ويبلغني إذا اكتشف أي شيء.
- مر يوم أو يومين ولا شيء... ولكن بعد ذلك تلقيت بريدًا إلكترونيًا يُفترض أنه من YouTube يحذرني من انتهاك الخصوصية وأنه يمكن تغريمي 15 ألف يورو. أجبت بحماقة على رسالة «YouTube» الإلكترونية مشيرة إلى أنني أتعرض للابتزاز وسميت الحساب الذي كان يفعل ذلك معي. بعد الرد، أدركت أن العنوان كان عنوان YouTube مزيفًا وأن الرسالة كانت مزيفة أيضًا. مرت بضعة أيام ولا شيء. ثم أفتح بريدي الإلكتروني اليوم للعثور على بريد إلكتروني مزيف آخر هذه المرة من «الإنتربول» ويهدد بأن لدي 48 ساعة للرد أو أنه من الممكن أن ينتهي بي الأمر بالذهاب إلى السجن....

- إذا قام المبتز بنشر صورك، فهناك خطوات يمكنك اتخاذها بالإضافة إلى الإبلاغ عن الجريمة:
  - اطلبي من مواقع الأنترنت إزالة المحتوى الخاص بك.
  - تواصلي مع Google لإزالة المعلومات.
  - التواصل مع جهة موثوقة مثل حملة لتسريع عملية حذف المحتوى عن الانترنت.
  - إعادة بناء سمعة إيجابية على الإنترنت «لدفن» نتائج البحث السلبية.
  - الإبلاغ عن الانتهاكات القانونية لمحركات البحث.
  - قدمي دعوى قانونية بالتشهير.

المراقبة

- وسائل على الإنترنت وخارج الإنترنت تستخدمها السلطات لمراقبة المواطنين والنشطاء وتقييد حرية التعبير.
- برمجيات مستخدمة تجمع البيانات لأغراض الدعاية الموجهة والتنميط.
- برنامج لسرقة بيانات المستخدمين يحتمل أن يؤدي إلى تهديدات ومضايقات عبر الإنترنت.
  - تشمل المراقبة الرقمية مراقبة الاتصالات الإلكترونية ، مثل رسائل البريد الإلكتروني والرسائل النصية ، بالإضافة إلى النشاط عبر الإنترنت ، مثل سجل التصفح و الmetadata.
  - تشمل المراقبة الجسدية استخدام الكاميرات وتتبع نظام تحديد المواقع العالمي وتتبع شرائح الجوال وطرق أخرى لمراقبة تحركات الشخص وأفعاله في العالم المادي.

برامج التجسس

- يصل Pegasus (أشهر برامج التجسس المرتبطة بالحكومة الإسرائيلية) إلى كاميرا الهاتف والميكروفون والرسائل النصية.
- تتجسس برمجيات التجسس الخاصة بشركة Candiru الإسرائيلية غالباً على أجهزة الكمبيوتر والأجهزة المحمولة والحسابات السحابية. يزعم أنه يصل إلى Gmail و Skype و Telegram و Facebook.

- SKYNET هو برنامج تحليل يبحث عن الأنماط والسلوكيات داخل البيانات الوصفية للهواتف المحمولة.

الوقاية من المراقبة

- شراء الأجهزة من مصادر موثوقة فقط.
- بقاء الاجهزة تحت النظر، خاصة عند عبور الحدود / نقاط التفتيش، وعدم ترك الأجهزة على الطاولة في المطاعم والمقاهي.
- عدم إستخدام شبكات الإنترنت العامة، خصوصاً عند التعامل مع بيانات حساسة.
- تحديث البرامج الخاصة بك.
- حافظ على تحديث نظام التشغيل الخاص بك وجميع التطبيقات المثبتة على الفور.
- إزالة الأجهزة المشبوهة.
- تحقق مما إذا كانت برامج المراسلة الفورية والحسابات عبر الإنترنت متصلة بأجهزة غير معروفة.
- استخدام برامج مراسلة تدعم التشفير الثنائي مثل Signal.
- استخدام برامج مكافحة البرامج الضارة.
- لا تستخدم برامج من مصادر غير موثوق بها.
- تغيير كلمات المرور.
- استخدم VPN مثل (PROTON VPN) أو Tor.
- استخدام microphone blocker
- استخدام camera blocker

حالة عملية على موضوع الرقابة

كشف تحقيق لمنظمتي أكسس ناو Access Now وفرونت لاين ديفيندرز Frontline Defenders عن تعرّض اثنتين من المدافعات عن حقوق الإنسان من البحرين والأردن لاختراق أجهزتهن باستخدام برنامج التجسس "بيغاسوس"، وهو برنامج تابع لمجموعة "إن إس أو" الإسرائيلية. ويأتي هذا في أعقاب ما كشف عنه مشروع بيغاسوس من استخدام الحكومات في المنطقة العربية لبرنامج التجسس "بيغاسوس" لانتهاك حقوق الإنسان وقمع الناشطات/ين والصحافيات/ين.

قد تعرّضت الكثير من المدافعات والصحفيات الأخريات مؤخّرا، في المنطقة العربية وشمال أفريقيا وخارجها، إلى الاستهداف من طرف برنامج التجسس "بيغاسوس"، ومن بينهنّ على سبيل المثال الناشطة الإماراتية آلاء الصدّيق والصحفية في قناة العربي رانيا دريدي والصحفية الإذاعية في قناة الجزيرة غادة عويس.

اختراق الحسابات الشخصية

طريقة معرفة اختراق احد الحسابات

المهم هنا هو سرعة الملاحظة والتحقق من سرقة الحساب والتعامل مع الموقف بشكل عملي. يمكن أن يكون أي من المؤشرات التالية دليل على اختراق أحد حساباتك:

1. الموقع الذي تحاولين الدخول إليه لا يقبل كلمة السر المُعتادة.
2. عند محاولة تغيير كلمة السر يرفض الموقع عنوان البريد الإلكتروني أو رقم الهاتف الذي تقومين بكتابته (يكون المُخترِق قد قام بالفعل بتغيير تلك البيانات بحيث يُقلل من فرص استردادك للحساب).
3. ورود رسائل على بريدك الإلكتروني تنبهك لمحاولات الدخول لأحد حساباتك من أجهزة لا تنتمي لك أو مناطق جغرافية لست متواجدة بها. يجب توخي الحذر مع هذه الرسائل لأنها تكون أحيانًا رسائل تصيد مفخخة.
4. ورود رسائل من مواقع تُجارية تنبهك لعمليات شراء قمت بها. يجب توخي الحذر مع هذه الرسائل لأنها تكون أحيانًا رسائل تصيد مفخخة.

كيفية التعامل؟

عادة لا يتوقف المُخترِق عند حسابك الشخصي، بل يستخدمه، بعد السيطرة عليه، في إختراق حسابات أُناس آخرين وعلى رأسهم معارفك المسجلين في عناوين الإتصال. يجب الإعتراف بأن سرقة حسابك هو ناتج خطأ منك أنت أولاً. كما يتوجب عليك فوراً تنبيه ومساعدة الآخرين في قوائمك حتى لا يتم تصيدهم عن طريق حسابك.

1. فور اكتشاف اختراق أحد حساباتك المؤسسية، أو الشخصية المستخدمة في التواصل مع زملاء عمل، قومي فورًا باستخدام وسيلة آمنة كمكالمة سيجنال لإبلاغ المدير التقني لمؤسستك.
2. باشري فورًا بإبلاغ معارفك. أعلميهم بالحسابات التي تم إختراقها وحذريهم من فتح أي رسائل أو محاولات تواصل ترد من حساباتك المخترقة.
3. إذا كان حسابك المخترق من مقدم خدمة بريدية أو على منصة تواصل اجتماعي قومي فورًا بالتواصل مع جهة الدعم الفني المختصة. توقعي أن يتم سؤالك عن بياناتك الخاصة(الاسم، العمر، العنوان، صورة إثبات الشخصية) وكذلك عن مجموعة من البيانات المتعلقة بالحساب المتضرر (متى تم فتحه، آخر كلمة سر مسجلة للحساب، آخر مرة تم الدخول فيها للحساب ومن أي موقع جغرافي) وأي أسئلة أُخرى قد توضح لهم أنك فعليًا صاحبة الحساب.
4. بعد استعادة حسابك تأكدي من تغيير كلمة السر لواحدة جديدة تمامًا، كما يجب التأكد من تغيير جميع البيانات الخاصة بتأمين الحساب مثل الأسئلة السرية والعنوان الثانوي وأرقام الهواتف وأيضًا يجب إعادة ضبط خاصية تحقيق المصادقة الثنائية 2FA.

الفصل الرابع:
إجراءات الأمان الأساسية

في هذا الفصل سنتناول أهم إجراءات الأمان الأساسية التي تساهم بتعزيز امانك الشخصي في الفضاء الإلكتروني.

كلمات المرور

- كلمات المرور هي خط الدفاع الأول.
- أهمية كلمات المرور القوية: تحمي كلمات المرور القوية من محاولات القرصنة.
- أمثلة على كلمات المرور الضعيفة: الكلمات الشائعة مثل «1234» ، «password» ، المعلومات الشخصية مثل «JaneSmith» ، «JohnDoe123» ، تسلسل من الأرقام أو الأحرف مثل «qazwsxedc», «abc123» ، «qwerty».

خطوات انشاء كلمة مرور قوية

- استخدم مزيجًا من الأحرف الكبيرة والصغيرة والأرقام والأحرف الخاصة.
- تجنب استخدام المعلومات الشخصية.
- تجنب استخدام نفس كلمة المرور لحسابات متعددة.

نصائح لاستخدام كلمات المرور

- تدقيق كلمات مرور أجهزتك وحساباتك. قم بتغييرها إذا كانت ضعيفة.
- تفعيل التحقق من خطوتين حيثما أمكن ذلك من دون رسائل SMS ، و استخدم/ي تطبيقات المصادقة مثل AUTHY.

مدير كلمات المرور

مدراء كلمات المرور يمكنهم توليد وتخزين كلمات مرور قوية وفريدة لكل من حساباتك. هذا يقلل من الحاجة لتذكر كل كلمة مرور ويعزز الأمان الرقمي، حيث يتم تشفير قاعدة البيانات بكلمة مرور رئيسية واحدة قوية.

- قوموا بتحميل KeePassXC لنظام لينُكس أو ويندوز أو ماك أو KeePassDX لأندرويد StrongBoxلآي. أو. اِس
- يمكن أيضاً استخدام BitWarden على جميع المنصات.
- لا تكرّروا إستخدام كلمات السرّ أبدًا.
- اجعلوا مدير كلمات السرّ يولّد لكم كلمة سرّ طويلة عشوائية فريدة ويحفظها، لكلٍّ من حساباتكم.

المزيد عن سبب توصيتنا هذه: ليس لأي منّا القدرة على تأليف ما يكفي من كلمات السرِّ الطويلة العشوائية الفريدة لزوم حفظ أمان أجهزتنا وحساباتنا. مدير كلمات السرّ برمجية تُولِّد كلمات السرِّ وتحفظها محميّةً بالتعمية.

بدورنا ننصحكم KeePassXC و KeePassDX و StrongBox و BitWarden ، وجميعها تطبيقات يمكن استخدامها مجّانا، وشهد خبراء متخصّصون بكونها آمنة، كما أنّ تطويرها متواصل.

وهي تحفظ كلمات السرّ لكم في ملف على أجهزتكم لا يوضع على الإنترنت، ما يعني قدرتكم على التحّكم في موضع حفظ بياناتكم وكيفية إدارتها.

سيكون هناك بعض كلمات المرور التي يجب حفظها، بما في ذلك كلمة المرور الرئيسية لمدير كلمات المرور الخاص بنا.

هناك استراتيجيات يمكن أن تساعدنا في إنشاء كلمات مرور سهلة التذكر لكن يصعب تخمينها، حتى بالنسبة للمهرة من المتربصين بنا ممن يستخدمون برامج «اختراق كلمات المرور».

- يمكنكم باستخدام أسلوب النّرد توليد كلمات سرٍّ قوية لمدير كلمات السرٍّ وكلمات السِّر الأخرى التي يتوجّب عليكم حفظها مثل كلمة السرِّ التي تفتح خزنة مدير كلمات السِّر، أو تلِجون بها إلى أجهزتكم:
- جهّزوا قائمة مُرقَّمة من الكلمات (حيث يجب تعيين كلمة لكل رقم من النرد) وقِطَع نَرد.
- دحرجوا النَّرد خمس مرات للحصول على رقم عشوائي من خمس منازل مثلا: 6 و 2 و 5 و 1 و 1.
- استخرجوا الكلمات المقابلة للأرقام مما في القائمة.
- كرّروا هذا خمس مرّات، ثم استخدموا الكلمات التي حصلتم عليها «عبارةَ سرٍّ» لحساب واحد، مثلاً قد تكون كلمة السر «سيارة منزل باب منزل ورقة».
- لا تستخدموا كلمة السرِّ هذه لأي غرض آخر.
- ثم اصنعوا صورة عقلية باستخدام هذه الكلمات لكي تساعدكم على تذّكرها
- وتدرّبوا على إدخال كلمات السرّ تلك دوريًّا، يوميًّا ابتداءً، ثم أسبوعيًّا بعد ذلك. التكرار يساعد على ترسيخ كلمات السرّ في الذهن.

كلمات السرِّ وأكواد الدخول الاحتياطيّة الواجب حفظها خارج مدير كلمات السرِّ

- إذا تعيّنت عليكم كتابة كلمات السرِّ على ورقة فيجب حفظها في مكان آمن موصد، مثل خزانة أو أدراج.
- من المهم ألا تكون كلمة السرّ ظاهرة للعيان، وألّا يسُهلَ العثور عليها.
- لا تحفظوا كلمات السرّ في محفظتكم أبدًا.
- أتلفوا الأوراق التي تحوي كلمات سرٍّ أو أكواد الدخول الاحتياطية فور انتفاء حاجتكم إليها.
- كما يمكن حفظ كلمات السرِّ تلك على جهاز آخر، وإخفائها بين ملاحظات أخرى بلا عنوان و لا وصف.
- و أفضل هذه الطرق هي الربط بين كلمة السر و شيء آخر مثلا كأن تكون كلمة السر هي «كتاب في مكتبة (رقم الصف)(رقم العامود)!» ثم تقوم برسم صورة لمكتبة فيها كتابك المفضل بالاحداثيات التي بكلمة السر، بهذه الطريقة حتى إذا تمكن شخص ما من الوصول لهذه الورقة فلن ي/تستطيع معرفة كلمة المرور.

إذا قرّرنا استخدام مدير كلمات المرور عبر الإنترنت

- تجنّبوا حفظ كلمات السرّ شديدة الحساسية فيه كالتي تخصّ الحسابات المالية أو مسوّغات الدخول إلى الحسابات التي تُستخدم لاسترجاع حسابات أخرى.
- تنبغي حماية خزنة مدير كلمات السرّ على الإنترنت بأسلوب التحقق بخطوتين.
- ننصحكم بتطبيق Bitwarden لإدارات لكلمات مروركم المستخدمة على الإنترنت.

تطبيقات إدارة كلمات السرِّ التي تزامن تلقائيًّا الأجهزة المختلفة المتّصلة بها قد تكون أيسر في الاستخدام، فهي تحفظ كلمات السرّ في خزنة مدير مركزية معمّاة على الخادم، إلا أن استخدامها يشكّل خطرًا إضافيًا يمكن للمهاجم استغلاله بتظهير الخزنة مدير واستخراج كلمات السرّ منها دون علمك.

بدورنا نوصي KeePassXC و KeePassDX و StrongBox لأنها لا تحفظ كلمات السرّ في أي موضع على الإنترنت. إذا فضّلت استعمال مدير كلمات سرٍّ على الإنترنت فإنّنا نوصي باتّباع الخطوات التالية لحماية كلمات سرّكم.

- تجنّبوا مشاركة كلمات السّر ما أمكنكم ذلك:
  - إذا اضطررتم إلى مشاركة كلمة سرٍّ مع آخرين فاعمدوا قبل مشاركتها إلى استبدالها بأخرى مؤقتّة، ثمّ استبدلوا تلك المؤقتة مجدّدًا بكلمة آمنة عقَب انتفاء الحاجة إلى مشاركتها.
  - تفّكروا كذلك في إنشاء حسابات منفصلة لكل شخص يلزمه النفاذ إلى المعلومات والوظائف، كثير من الخدمات تتيح ذلك، كما يمكن أحيانا تحديد الأفعال التي يمكن لتلك الحسابات فعلها، والمعلومات التي يمكنهم النفاذ إليها

إيّاك ومشاركة كلمة السّر مع شخص راسلك عبر البريد الإلكتروني أو هاتفك أو بعث لك برسالة نصيّة ينتحل المهاجمون هويّات أخرى، مثل موظّفي الدعم التقني في البنك، لإقناع ضحاياهم بالإفصاح عن بيانات حسّاسة. كما أنهم يتلاعبون عاطفيًّا بضحاياهم لأجل ذلك.

إذا تلقيّتم مكالمة أو رسالة بريد إلكترونياً أو رسالة قصيرة تطلب كلمة سرٍّ أو بيانات حسّاسة أخرى، أو إذا أوصلكم رابط إلى صفحة تطلب معلومات كهذه، فهي على الأرجح محاولة تصيُّد.

- افتح صفحة الخدمة أو التطبيق الرسمية التي تظنّ أنها أرسلت إليك الرسالة للتحقُّق من ذلك الطلب.
- إذا بدا أن الرسالة وردت من شخص ما من معارفكم أو من جهة ما تربطكم بها علاقة، فتواصلوا معهم عبر قناة اتّصال أخرى للتحقُّق من أنهم أرسلوها.
  - على سبيل المثال، إذا وصلتك الرسالة بالبريد الإلكتروني، فاطلبهم بمكالمة صوتية.
  - تجنّبوا اتّباع الروابط الواردة في رسالة البريد الإلكتروني، وكذلك إرسال ردٍّ.
- انتبهوا لمحاولات بعض الرسائل إخافتكم، أو إثارة فضولكم أو إيهامكم بوجود فرصة ستضيع ما لم تستجيبوا بسرعة. تريّثوا وفكّروا في كيفية التحقُّق من صحة الرسالة.

فحص كلمة المرور

لمعرفة اذا كان هناك تسريب لكلمات المرور الخاصة بك قوموا بزيارة هذا الموقع ، وادخل بريدك الإلكتروني أو رقم هاتفك واذا كان هناك تسريب بيانات مرتبطة بالبريد الالكتروني أو الهاتف سيظهرها ، في حالة وجودها عليكم بتغيير كلمة السر بسرعة.

مكافح الفايروسات

- تعد برامج مكافحة الفيروسات والبرامج الضارة أدوات أساسية لحماية الكمبيوتر والشبكة.
- تكمن أهمية برامج مكافحة الفيروسات في تقليل المخاطر الرقمية التي قد تتعرضين لها، من التجسس على أجهزتك الشخصية، سرقة الحسابات وكلمات المرور.
- أنواع برامج مكافحة الفيروسات ومكافحة البرامج الضارة: تتوفر أنواع مختلفة من برامج مكافحة الفيروسات وبرامج مكافحة البرامج الضارة ، بما في ذلك الخيارات المجانية والمدفوعة. تشمل بعض الخيارات الشائعة ما يلي:
  - Windows defender مدمج في نظام التشغيل ويندوز.
  - Kaspersky
  - برنامج McAfee
- يجب عدم إيقاف تشغيل مكافح الفايروسات.
- يجب تفعيل خيار التحديث التلقائي.

التحايل على الرقابة

استخدام متصفّح تور TOR

Tor هو تطبيق مجاني ومفتوح المصدر يستخدم شبكة من المرحلات التطوعية لإخفاء نشاطك عبر الإنترنت مع توفير الوصول إلى بعض المواقع المحجوبة. قد تكون شبكة Tor محظورة في بعض المناطق، وقد يؤدي استخدامها إلى جعل اتصالك يبدو مريبًا لأي شخص قد يراقب نشاطك عبر الإنترنت.

متصفّح التّوجيه البصيلي The Router Onion أو ما يُعرف اختصارًا بتور TOR– هو تطبيق مجاني مفتوح المصدر يستخدم شبكة من الخوادم التّطوعية الّتي تعمل على إخفاء هويتنا ونشاطنا على الإنترنت وتتيح لنا الوصول إلى بعض المواقع المحظورة. تحظر بعض الدّول استخدام شبكة تور، مما قد يجعل استخدامنا لها موضع ريبة بالنّسبة للجهات المُحدَوْدِبة.

يعمل متصفح تور بمنهجيّة تُشبه عمل الشّبكات الافتراضيّة الخاصّة، لكن بدلاً من توجيه تحرّكاتك على الإنترنت إلى مزود خدمة واحد، يوزّعها على ثلاثة خوادم، وبذلك يُخفي من طلب زيارة ماذا ويعزّز خصوصيتنا. يُذكر أنّ لتور ألوف مؤلّفة من الخوادم الّتي يديرها متطوعون ومتطوعات في مختلف أرجاء العالم. وإن كنّا في أحد البلدان الّتي تحظر متصفّح تور أو تُدرجه ضمن الممنوعات أو المواقع غير الآمنة، يُمكننا استخدام نسخة تور برِدج TOR Bridge

يعمل متصفّح تور على حل ثلاثة من إشكاليّات الخصوصيّة:

- يمنع تور المواقع الإلكترونيّة والخدمات الأخرى ذات الصِّلة من تحديد موقعنا–هذه البيانات الّتي يُمكن يتمخّض عن تجميعها قواعد بيانات عن عاداتنا واهتماماتنا. ب باستخدام تور، لن تُقدَّم بياناتنا كمسلّمة من مسلّمات استخدامنا للشبكة، بحيث يسلّمنا تور زمام التّحكم بكل اتصال لنا مع مكوّنات الإنترنت وما المعلومات الّتي نوافق على مشاركتها بملء اختيارنا.
- يمنع تور الأشخاص المتربصين بتحرّكاتك على الشّبكات المحليّة لمعرفة المعلومات الّتي تجمعها ومن أين تجلبونها، ويشمل ذلك مزودي خدمات الإنترنت أو أي شخص لديه إمكانية الوصول إلى شبكة الواي-فاي المنزليّة أو جهاز التّوجيه الخاص بنا، كما يمنعهم من تحديد ما يُسمح لنا معرفته ونشره، فمتى نصل إلى أي جزء من شبكة تور، نستطيع أن نصل لأي موقع إلكتروني على الشّبكة العنكبوتيّة.
- ينقل متصفح تور اتصالك من خلال أكثر من مُرحِّل كي لا يحول دون تمكّن أي مرحل من تفصيل نشاطك على الإنترنت، ويتحقّق ذلك نتيجة أنّ كل مرحل تُديره منظّمات أو أفراد مختلفون، هكذا يُحقّق توزيع الثّقة أمانًا أوثق من نهج وكيل المرحلة الواحدة.

الشبكات الافتراضية VPN

- بفضل الشّبكات الافتراضيّة الخاصّة يمكن جعل اتصالنا بالإنترنت وكأنه يتم من منطقة أو بلدٍ غير منطقتك وبلدك الفعليين، كما يُمكن لهذه الشّبكات أن تحمي اتصالك بالإنترنت من التّطفل على شبكة الواي-فاي الخاصّة بنا. لو كان اتصالنا بالإنترنت يشبه نفقًا، تكون الشّبكة الافتراضيّة الخاصّة جداره الخارج الحامي. تعتمد بعض خدمات الشّبكات الافتراضيّة الخاصّة على خصائص مضمّنة في أنظمة التّشغيل– ويندوز، ولِنُكس، وماك، والآي. أو. اِس –، فيما يتطلّب البعض الآخر تثبيت برامج إضافيّة وتكوينها، مثل تطبيقاتTunnelbear أو ProtonVPN. يوفّر بعض مزودي خدمات الشبكات الافتراضيّة الخاصّة أدوات تثبيت مُحاكة خصيصًا للتعامل مع كل شيء هذه الجبهة بالنيابة عنّا. في هذا السّياق، من المفيد الإبقاء على جُعبة من تطبيقات الشبكات الافتراضيّة، فإن حُظِر أحدها،نستخدم آخرًا، كون هذه التّطبيقات تفتقر لخاصيّة اجتياز الحظر، إن حُظرت.

استخدام خدمة الوكيل البروكسي

إن كانت إحدى خواص تنخيل النّشاط على الإنترنت تمنع الوصول إلى موقع ما، أو تحجب الوصول إليه من منطقة ما، يُمكن لبرمجيات البروكسي أن تجعل طلب الوصول لسين أو صاد من المواقع المحجوبة كأنه من مكان آخر يُتاح فيه الوصول لتلك المواقع واجتياز الحجب.

- يمكن تجريب برنامج لانترن لهذا الغرض https://lantern.io/ar. يناسب هذا التّطبيق أنظمة تشغيل أندرويد، آي. أو. اِس، ولِنُكس، وماك، وويندوز، يعد أداة آمنة ومفتوحة المصدر تمكّننا تجاوز الحجوبات العامّة باستخدام بروكسات بروتوكول ال HTTPS لتأمين وصول لا رقابة عليه للمضامين والمحتويات المتاحة على الشّبكة العنكبوتيّة.

التحديثات

- أنواع تحديثات البرامج : يمكن أن تتضمن تحديثات البرامج :تحديث نظام التشغيل مثل

windows , macos , IOS, Android

- تحديثات التطبيقات سواء البرامج الحاسوبية أو التطبيقات على الهواتف الذكية.
- تحديثات برامج الأمان مثل مكافح الفيروسات والجدران النارية.

التحقق من التحديثات

Windows: Go to Start>Settings>Update & Security>Windows Update

MacOS: Go to the Apple menu and choose «Software Update»

Mobile devices: Check the Settings and App Store or Play Store for updates.

أمان أجهزة الحاسوب

نظام تشغيل ويندوز

لتعزيز أمان نظام ويندوز وحماية بياناتك، يمكنك اتباع عدة إجراءات واستخدام ميزات أمان مدمجة في النظام. فيما يلي بعض النصائح المفصلة مع روابط لمصادر تعليمية من مايكروسوفت توفر معلومات إضافية:

1. استخدام مايكروسوفت ديفندر أنتي فيروس او أي مكافح فيروسات آخر مدفوع

مايكروسوفت ديفندر يوفر حماية فعالة ضد البرمجيات الخبيثة والتهديدات الأمنية عن طريق الفحص المستمر للمحتوى ومراقبة سلوكيات الملفات والعمليات. يمكنك تشغيل فحوصات أمان وتحديث برنامج الحماية بانتظام للتأكد من توفر أحدث الحمايات ضد التهديدات للمزيد هنا.

2. تشفير القرص الصلب باستخدام برنامج bitlocker

3. التحكم في الوصول إلى المجلدات: يمكن تحديد التطبيقات التي يُسمح لها بالوصول إلى مجلدات محددة لحماية بياناتك من التطبيقات الضارة والتهديدات مثل برمجيات الفدية للمزيد هنا.

4. استخدام جدار الحماية ويندوز: جدار الحماية الخاص بويندوز يساعد في حماية جهازك عن طريق تصفية حركة مرور البيانات على الشبكة الداخلة والخارجة. يمكن تكوينه لحظر أو السماح بحركة المرور بناءً على الخدمات والتطبيقات المثبتة على جهازك. يدعم جدار الحماية بروتوكول أمان الإنترنت IPsec لتطلب التوثيق من أي جهاز يحاول التواصل مع جهازك، ما يوفر طبقة حماية تحميك من المخاطر التي تحيط بك.

5. عدم ترك الأجهزة مفتوحة في المقاهي أو الأماكن العامة.

6. انشاء نسخة احتياطية من البيانات المهمة.

7. زيارة موقع VIRUSTOTAL للتحقق من الروابط والملفات.

8. ضبط وقت إقفال الشاشة.
9. إنشاء كلمة مرور.
10. تفعيل الجدار الناري.
11. إيقاف عرض الاشعارات عند إقفال الشاشة.
12. لمحو البيانات :

- من غير الممكن للجهاز أن يمحو جميع بياناته بالكامل، لا بدّ لنا من تشغيل حاسوبنا من محرك أقراص خارجي للقيام بذلك. ثمّ عدّة خيارات اخرى أحدها إزالة محرك الأقراص الصّلبة من حاسوبنا، والتّعامل معه باعتباره محرك أقراص خارجي، وتنظيفه باستخدام حاسوب آخر. للحصول على إرشادات حيال كيفيّة فك القرص الصّلب، يُمكننا البحث على «إزالة القرص الصّلب» ثُمّ نتوجه إلى طِراز ونموذج الحاسوب على موقع iFixit ثُم نضع محُرّك الأقراص المُزَال في حاضنة الأقراص الصّلبة المخصّصة لتخزين ونقل البيانات.
- يُمكننا التّفكير بخيار برمجية ال DBAN ، للكتابة فوق القرص بأكمله. قد يستغرق ذلك بعض الوقت، كما سنحتاج لتنزيل DBAN وتشغيله من محرك أقراص نقل وتخزين بيانات فارغ. لسوء الحظ، من الصّعب ضمان مسح محرك الأقراص بالكامل على الحواسيب الأحدث الّتي تستخدم الأقراص الصّلبة الثّابتةSolid State Drives. مع ذلك لا يزال بإمكاننا بمحو المستطاع باتباع الخطوات التّالية.
  - بمجرد مسح القرص بأكمله، علينا التّفكير في إعادة تثبيت نظام التشغيل.
  - في خضم ذلك، لا بدّ ألّا ننسى ضبط الإعدادات بما يضمن التّشفير للقرص كاملًا.

نظام macOS

لتعزيز أمان نظام macOS وحماية بياناتك، يقدم نظام التشغيل هذا عدة ميزات وإجراءات أمان مدمجة تساعد على حماية جهازك ومعلوماتك الشخصية. إليك بعض النقاط الرئيسية المتعلقة بأمان نظام macOS مع روابط لمصادر تعليمية من Apple توفر معلومات إضافية:

1. الحماية من البرمجيات الخبيثة على macOS: Gatekeeper يضمن أن جميع التطبيقات التي تم تثبيتها من الإنترنت تم التحقق منها للبحث عن البرمجيات الخبيثة وأنها موثوقة قبل أن يتم تشغيلها لأول مرة، مما يقلل من خطر البرمجيات الخبيثة هنا.
2. جدار الحماية المدمج والأمان الشبكي: macOS يتضمن جدار حماية مدمج يمكن تكوينه للتحكم في الاتصالات الواردة والصادرة عبر الشبكة، مما يساعد في منع الوصول غير المصرح به إلى جهازك هنا.
3. ضبط وقت إقفال الشاشة
4. إنشاء كلمة مرور.
5. تفعيل الجدار الناري (Firewall).

6. حذف البيانات:

- في أجهزة Mac القديمة التي تحتوي على شرائح Intel يمكننا مسح محرك الأقراص الثابتة لدينا بأمان باستخدام أداة القرص أو مساعد المسح.
- أمّا على أجهزة الماك المدعمة برقاقات الأقراص الصّلبة الثّابتة، فعلينا بالتّالي:
- أولًا نفعّل التّشفير الكامل للقرص المُراد حذفه (رابط(لكي نضمن أن تبدو محتوياته بلا معنى لأي شخص لا يملك كلمة مرور الجهاز.
- ثانيًا نتبع الإرشادات التّالية لمسح القرص الصّلب الثّابت باستخدام أداة القرص

لمعرفة المزيد عن كل ميزة وكيفية تفعيلها أو استخدامها، يمكنك زيارة الروابط المرفقة التي توفر دليلًا شاملًا لأمان نظام macOS والخدمات المرتبطة به من Apple.

أمن الهاتف المحمول

- تحديثات تلقائية لنظام التشغيل وللتطبيقات.
- وضع كلمات مرور
- ضبط قفل الشاشة بعد دقيقة واحدة.
- تقليل عدد التطبيقات بحسب الحاجة.
- تعطيل خاصية تحديد المواقع وايقافه من نظام التشغيل والتطبيقات التي تطلبها.
- التحقق من أذونات التطبيقات مثل الموقع والكاميرا والميكروفون.
- تقليل الإخطارات على شاشة القفل بقدر الإمكان وحجب محتواها.
- تثبيت التطبيقات المرخصة فقط ومن المتاجر الرسمية ، جماعة Android انتبهوا!
- اختيار مضاد فيروسات مثل Avast على Android.
- التشفير الكامل: يتيح نظام ios التشفير الكامل برمز PIN ، يسمح نظام Android10+ فقط بتشفير الملفات.
- فقدان الجهاز أو السرقة/ يتضمن برنامج Remote Wipe ، وهو برنامج إدارة الأجهزة المحمولة الذي يوفر المسح عن بُعد: Icloud ، ومدير جهاز Android ، و Airwatch ، و MobileIron ، و Intune.
- عدم استخدام شبكات الانترنت اللاسلكي العامة.
- استخدام protonvpn.
- إخفاء البيانات الوصفية من الصور، لحذفها من الايفون :

- Open the Settings app.
- Tap on Privacy > Location Services.
- Scroll down and tap on Camera.
- Select Never.

الاندرويد:

- Open the ‹Gallery› app.
- Locate the image you wish to remove metadata from.
- Select it and click the ‹share› button, which is a three-pointed figure.
- Underneath the photo, click ‹remove location data›

إزالة المعلومات التّعريفيّة من صورنا وسائر ملفاتنا

قد تبدو مسألة حماية معلوماتنا التّعريفيّة أمرًا بسيطًا ينقضي بتمويه للوجوه الظّاهرة في الصّورة أو تغطية التّفاصيل الحسّاسة أو الأماكن الظّاهرة. إلّا أنّ الأمر ليس بهذه السّهولة، فمن لديه الملف قد يستطيع إكتشاف ما نحاول إخفاءه إن لم نُحكِم التمويه بطريقة محدّدة، وهذا يسوقنا إلى تطبيق Obscuracam الّذي يساعدنا على إحكام تمويه صورنا بأمان. تحتوي الصور على معلومات أكثر ممّا نراه، إذ تحتوي كافة الملفات على كمية صغيرة من المعلومات عن كيفية إنشائها ومكانه. تسمى هذه المعلومات البيانات الوصفية. يمكننا عادةً إلقاء نظرة على بعض البيانات التّعريفيّة للملف على حاسوبنا بالنّقر بزر الفأرة الأيمن على الملف واختيار «خصائص» أو «الحصول على معلومات.» قد تتضمن بعض البيانات التعريفيّة موقعنا أو الجهاز الذي تم إنشاء الملف به: معلومات يمكن أن يستخدمها شخص يعاين الملف للتعرف علينا. لتفادي ذلك يُمكننا الاستعانة ببرامج Scrambled Exif ، و MetaX ، و Exifcleaner لمسح البيانات التعريفية بأمان.

محو بيانات الجهاز بالكامل

اندرويد

- أولًا نبدأ بإعادة ضبط المصنع
- ثُم نُثبّت تطبيق Extirpater ، لمباشرة محو كل أثر متبق في شريحة الذّاكرة.

آي أو أس

- لمحو البيانات الخاصة بالايفون يرجى اتباع الخطوات في الرابط.

لنقم بعمل فحص سريع والإجابة عن الأسئلة التالية لمعرفة ما هي حالة جهازنا المحمول ونطبق التعليمات والارشادات المذكورة في الدليل في حال كانت ليست مطبقة على هواتفكم المحمولة

- ما هي التطبيقات الموجودة على هاتفك؟
- هل تم تحديثها؟
- ما هي الصلاحيات التي تم منحها لهم؟

التصفح الآمن

فايرفوكس كمتصفح افتراضي

نوصي بشدة باستخدام متصفح فايرفوكس من موزيلا، لما له من خصائص أمان ، كما أنّه مجاني ومفتوح المصدر.

التّأكد من تحديث نسخة المتصفح الّتي نستخدمها

من المفترض أن يتم تحديث فايرفوكس تلقائيًا، لكن يمكننا التحقق مما إذا كان لدينا أحدث إصدار من المتصفح عبر الرّابط.

إيقاف تشغيل مدير كلمات المرور المدمج في المتصفح

- يستطيع فايرفوكس حفظ كلمات المرور وتشفيرها لك، إلّا أنّنا نوصي بعدم تفعيل هذه الميزة واستخدام مدير كلمات مرور منفصل مثل KeePassXC أو BitWarden بدلاً من ذلك.
- يُذكر في هذا السّياق أنّ ملحقات إدارة كلمات المرور الموجودة في المتصفح تعرضنا لخطر أكبر من خلال قيام مهاجم بخداع متصفحك وبالتّالي الوصول لكافّة كلمات المرور الخاصة بك.
- ينبغي إزالة كافّة عمليات تسجيل الدخول المحفوظة وتعطيل خاصيّة إدارة كلمات المرور على المتصفّح.

التّحقّق من سائر الأذونات الّتي تطلبها المواقع

يمكن تشبيه الأذونات بابٍ أو نافذة مشرّعة إلى بيتنا: بعبارة أخرى إن كان بإمكان سين من المواقع الويب الدخول، فقد يتمكن آخرون من ذلك أيضًا. لذا لا بد من التحقق أن مواقع الويب التي تستخدمها وتثق بها هي فقط التي لديها الإذن باستخدام الخصائص الحساسة مثل الكاميرا أو الميكروفون. قد تستخدم البرامج الضارة هذه الأذونات للسماح لشخص ما برؤية مكانك أو التّنصت عليك.

- وعليه علينا إدارة الأذونات التي لربما سبق وأن منحناها لسين وصاد من مواقع الويب المختلفة.

التّحقّق من إعدادات حماية التتبع المطوّرة

تقوم ملفات تعريف الارتباط وأجهزة التتبع الأخرى بجمع تفاصيل عن هويتك ومكان تواجدك وما تصفحته عبر الإنترنت. لذا عليك التّفكير فيما قد يحدث إذا وقعت هذه الأشياء في أيدي خصومك، واتخذ هذه الخطوات للحد من احتمالات التّعقّب والتّتبع عبر الإنترنت.

- تحقق من الإعدادات الخاصة بك، على الأقل بتفعيل إعدادات الحمايّة المطوّرة من التّعقب والتّتبع: رابط، كما عليك التفكير بخيار تشديد هذه الإعدادات وما قد ينشأ عن ذلك من عدم تمكنك من الدّخول على الكثير من المواقع.

تعيين محرك البحث الافتراضي

تقوم محركات البحث مثل غوغل Google وبينغ Bing بإنشاء ملفات تعريف لمستخدميها، وتتبع جهازك على وجه التحديد، بل وتشارك معلوماتك الشخصية مع أطراف ثالثة. بتعيين

محرّك بحث افتراضي سيستخدم متصفحك محرك بحث واحد في كل مرّة تبحث فيها عن شيء عبر الإنترنت ما لم تُحدّد محرّك بحث آخر.

- وعليه علينا استخدام القوائم المنسدلة المُدرجة ضمن خيار «تخصيص هذه الأداة» للعثور على الإرشادات المناسبة لأجهزتنا على هذه الصفحات، بحيث:
- نعين محرك البحث الافتراضي الذي نرتضيه مثل محرك بحث duck duck go.

استخدام أدوات إضافيّة (Extensions) لتعزيز الحماية على المتصفح

بتصفحنا الإنترنت فإنّنا نتعرض لطيف من الأكواد البرمجية من مصادر مجهولة، وهذا هو أحد الأسباب التي تجعل صفحات الويب مرتعًا للغالبية العظمى من أفخاخ البرامج الخبيثة وبرامج التجسس. بالإضافة إلى ذلك، يستخدم الأشخاص الذين لديهم مواقع إلكترونيّة أو يعلنون عبر صفحات الويب «ملفات تعريف الارتباط»، وهي عبارة عن أجزاء صغيرة من المعلومات التي تتعقبنا أثناء التصفح. الأهم من ذلك، أن مواقع الويب لا تشفر كل ما ترسله أو تستقبله منّا؛ حيث لا يستخدم بعضها بروتوكول نقل النص التشعبي الآمن HTTPS. وعليه، فإنّنا نوصي بتثبيت الأدوات والخصائص الإضافية للمتصفح للحماية من مشكلات الأمان والخصوصية.

- يمكننا اختيار الخصائص الإضافية التي نريد تثبيتها وتحديد كيفية تكوينها، وفقًا لظروفنا واحتياجاتنا.
- في حال كنّا نستخدم حاسوب يديره شخص آخر مثل في مكان عام أو في مكان العمل فقد يتعين علينا إجراء هذه التعديلات بوتيرة متكرّرة
- التثبيت والتكوين:
  - https://privacybadger.org/ :

لماذا علينا تسليح متصفحنا به؟ يحظر هذا البرنامج أجهزة التتبع التي تجمع البيانات عن المكان الذي كنّا فيه عند اتصالنا بالإنترنت.

- برنامج uBlock Origin

لماذا؟ يحظر الإعلانات وأجهزة التتبع، التي قد يكون بعضها ضارًا.

- برنامج Cookie AutoDelete

لماذا؟ يحذف أدوات التتبع التي تجمع البيانات عن المكان الذي كنّا فيه عند اتصالنا بالإنترنت.

- فيسبوك كونتينر Facebook Container

لماذا؟ يمنع منصّة فيسبوك من جمع البيانات عن المكان الذي كنّا فيه عند اتصالنا بالإنترنت وربطها بملفاتنا الشّخصيّة.

- Zoom Redirector

لماذا؟ من خلال فتح روابط Zoom في متصفحك، تحافظ هذه الوظيفة الإضافية على المكالمة ضمن وسائل حماية متصفحك.

- الخيار المتقدم: NoScript

تجدر الإشارة إلى أنّ خاصيّة NoScript كثيرًا ما تتسبب بأن تظهر الصّفحات الّتي نزورها فارغة أو معطّلة؛ لذا ينبغي التعرف على كيفية تكوين هذه الخاصيّة بدقّة لتقليل مثل هذه الأمور. لماذا؟

من الممكن أن يتمكن خصومنا من الوصول إلى أجهزة باستخدام أكوادٍ برمجية ضارة في برنامج نصي تم تنزيله مع صفحة الويب التي نتصفحها؛ في هذه الحالة، يعمل برنامج NoScript على حظر كل الأكواد البرمجية من مواقع الويب غير المعروفة، ما يحمي جهازك من التقاط برمجيات خبيثة وما شابهها.

إدارة الوظائف الإضافيّة والنوافذ المنبثقة عنها

قد يحاول المتربصون بنا خداعنا لتثبيت برامج خبيثة في شكل خصائص إضافية تُضاف على المتصفح. يمكنهم القيام بذلك باستخدام النّوافذ المنبثقة. لذا لا بدّ لنا من ضبط المتصفح لتفادي هذه الحيل والأشراك. بالإضافة إلى ذلك، علينا التّثبّت من تحديث الوظائف الإضافية التي نريدها، وإزالة تلك التي لا نستخدمها، فكما يفسد الطعام القديم، يمكن للأكواد القديمة أن تُضحي ثغرات وخلل برمجي ضار وخطِر. وعليه علينا:

- التّأكد من ضبط المتصفح لحظر النوافذ المنبثقة وتحذيرنا بشأن أي خاصيّة أو برنامج يُراد تثبيته نتيجة لهذه النوافذ.
- تحديث الوظائف الإضافية بوتيرة تلقائية كلما توفّرت تحديثات لها و إزالة الإضافات غير المستخدمة.

حذف سجل بيانات ومعلومات التّصفح

سجل التصفح الخاص بك هو قائمة بمواقع الويب التي قمت بزيارتها. الخيار الافتراضي في المتصفح هو «تذكر سجل التصفح والتنزيل»، مما يعني أن المتصفح سيتذكر سجلات ما نتصفح وننزّل ونبحث عنه، كما سيقبل ملفات تعريف الارتباط من مواقع الويب التي تزورها، تلك الجزئيات المعلوماتية التي تتتبع حركاتنا وسكناتنا عبر الإنترنت تسمح للمواقع المُزارة بتسجيل معلومات على أجهزتنا يرسلها المتصفح إليهم وإلى شركائهم من المعلنين. من جهة أخرى، لسجل بيانات التّصفح هذا مزاياه أيضًا، مثلاً ما سيقترح متصفحك الصفحات التي قمت بزيارتها من قبل، لذلك لا يتعين عليك إعادة كتابة العناوين أو نقلك إلى مواقع ضارة. لكن هناك مقايضات، حيث إن تمكّن شخص ما من الوصول إلى سجل ما نتصفح على الإنترنت، فكأنما وقع على منجمٍ من المعلومات عنّا، وعن الأشخاص الذين نعمل معهم، والأشياء التي كنا نقرأ عنها وتهمّنا. وعليه علينا: من خلال الاعدادت في المتصفح

- مسح جميع ملفات تعريف الارتباط.
- تعطيل ملفات تعريف الارتباط للجهات الخارجية.
- إعداد زر أو خيار واحد بالنّقر عليه نمحي كل ملفات تعريف الارتباط وسجّل التّصفح، بكبسةَ زر كما يقال.
- ضبط المتصفح بحيث لا يتذكّر شيء من سجلات تصفحنا أو تخصيص ما يتذكره وما ينساه
- كذلك يمكننا حذف سجل التّصفح يدويًا: كيفيّة حذف سجل التّصفح: رابط
- في ذات السّياق، من الجدير أن نفكّر إذا ما كنّا نريد تغيير ما يقترحه المتصفح عند الكتابة في شريط العناوين؛ فذلك أيضًا بمقدورنا.

استخدام التصفح الخاص

يشير «التصفح الخاص» إلى وضعيّة تحول دون تتبع المتصفح لملفات تعريف الارتباط أو حفظ سجل التّصفح الخاص بنا، ويعد استخدامه طريقة سريعة لإخفاء بعض أنشطتنا إذا ضبطنا متصفحنا على أنّه من المقبول الاحتفاظ بسجل ما نتصفحه ونبحث عنه عبر الإنترنت. يمكن لهذه الخاصيّة أن تكون مفيدة جدًا إن كنّا نعيش مع شخص يهدّدنا ويمكنه الوصول إلى أجهزتنا، وعليه ينبغي لنا:

- تعميق فهمنا حيال ما لا يُمكن للتصفح الخاص حمايتنا منه: رابط، بما في ذلك منشوراتنا على وسائل التّواصل الاجتماعي، أو الملفات الّتي تقوم بتنزيلها، أو البرامج الخبيثة الّتي قد يضعها المتربصون بنا على أجهزتنا.
- تشغيل التصفح الخاص لجلسة معيّنة.
- التّفكير في خيار التّصفح الخاص في جميع الأوقات.

استخدام متصفح تور أو الشّبكات الافتراضيّة الخاصّة الموثوقة VPN

يتيح لنا استخدام متصفح تور Tor أو عبر الشّبكات الافتراضيّة الخاصّة الموثوقة VPN زيارة الصّفحات الإلكترونيّة دون الكشف عن هويتنا أو موقعنا. في المقابل، إذا سجّلنا في خدمة ما فإنّنا نُشاركها معلومات حساباتنا وربما معلومات شخصية.

المراسلات الآمنة

يُمكن لخدمات الدردشة الوصول إلى المعلومات وجمعها عن موقعك، ونشاطك، ومحتواك، ومن نتحدث معهم؛ لذا حري بنا اختيار التّطبيق أو البرنامج الآمن لحماية سلامتنا.

استخدام تطبيقات المراسلة المشفرة تشفيرًا تامًا

- لا بدّ أن نعلم بأن جهات تقديم خدمات الإنترنت أو الهواتف الخاص بك قد تتمكن من الاطلاع على التطبيقات التي نستخدمها، لتجنب ذلك علينا بالشبكات الافتراضية الخاصة.
- تطبيق سيغنال Signal يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز: تطبيق مجاني و مفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة، والصّوتيّة، والمرئية، لكن يتطلب رقم هاتف صالح للتسجيل فيه.
- تطبيق إيليمنت Element يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز: تطبيق مجاني ومفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة المشفرة تشفيرًا تامًا، ويوفر خاصية مشاركة الملفات للأفراد والمجموعات، يقدّم التّطبيق أيضًا خدمات المراسلة الصّوتية والمرئيّة، يستند إيليمنت على معيار الاتصال المصفوفي(Matrix Communication Standard) .
- تطبيق دلتا Delta يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز: تطبيق مجاني ومفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة بالاعتماد على جهات تقديم خدمات البُريد الإلكترونيّة لنقل البيانات، يُذكر أنّ دلتا لا يتطلّب إدخال رقم هاتف لاستخدامه على عكس تطبيقات واتس-آب، وسيغنال، وتيليجرام.

- تطبيق واير Wire يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز: تطبيق مجاني لكن تجاري ومفتوح المصدر يوفر خدمات آمنة للدردشة النّصيّة بالاعتماد على جهات تقديم خدمات البُريد الإلكترونيّة لنقل البيانات، يُذكر أنّ دلتا لا يتطلّب إدخال رقم هاتف لاستخدامه على عكس تطبيقات واتس-آب، وسيغنال، وتيليجرام.
- إذا لم يكن استخدام التطبيقات المشفرة تشفيرًا تامًا ممكنًا، فحريٌّ بنا استخدام الخدمات الموصى بها والمُستضافة على خوادم موثوقة بواسطة مقدمي خدمات موثوقين مثل Mattermost و RocketChat.

تجنب الاحتفاظ بالمعلومات الحساسة التي لم نعد بحاجة إليها

ينبغي لنا التفكير بتلك الرسائل التي قد يعثر عليها شخص إن وصل إلى حساباتنا على خادم بُردنا الإلكترونية أو أجهزتنا. ما الذي قد تكشفه هذه الرسائل عن حياتنا الشخصية او علاقاتنا او عملنا، أو وجهات نظرك، أينبغي لنا وزن هذه المخاطرة مقابل الاستفادة من إمكانية الوصول إلى بريدك الإلكتروني على أجهزة متعددة. يعد النسخ الاحتياطي لبُردنا الإلكترونية على جهاز مشفر إحدى الطرق للاحتفاظ برسائل البريد وحفظها بأمان، وعليه ينبغي لنا:

- استخدام خاصية الرّسائل المختفية واستخدامها على تطبيقات المراسلة حيثما أمكن ذلك.
- حذف الرسائل حيثما كان ذلك ممكنًا.

مؤتمرات ولقاءات الفيديو الآمنة

- استخدم خدمات الفيديو والصوت والنّص المشفّرة تشفيرًا تامًا، و إذا لم يكن استخدام التطبيقات المشفرة تشفيرًا تامًا ممكنًا، فحريٌّ بنا استخدام الخدمات الموصى بها والمُستضافة على خوادم موثوقة بواسطة مقدمي خدمات موثوقين.
- لا بدّ أن نعلم بأن جهات تقديم خدمات الإنترنت أو الهواتف الخاص بك قد تتمكن من الاطلاع على التطبيقات التي نستخدمها لتجنب ذلك، علينا بالشبكات الافتراضية الخاصة.
- تطبيق جيتسي Jitsi يعمل على أنظمة الأندرويد، والآي. أو. اِس.، ولينكس، والماك، والويندوز: تطبيق مفتوح المصدر بإصدارين أحدهما مجاني والآخر مدفوع، يوفر خدمات آمنة للدردشة الصّوتيّة والمرئية، ويمكن استخدامه على أنظمة لينكس وماك وويندوز عبر المتصفح .
- تطبيق بيغ بلو بَتِن BigBlueButton : تطبيق مفتوح المصدر بإصدارين أحدهما مجاني والآخر مدفوع، يعمل عبر متصفحات الإنترنت يوفر خدمات آمنة للدردشة الصّوتيّة والمرئية، يُذكر أنّه بإمكان الأفراد والمنظمات التي تمتلك الخبرة التقنية المناسبة استضافة خدمات هذا التّطبيق على خوادمها. صُمِّم هذا التّطبيق لغايات الجلسات التّدريبية عبر الإنترنت وضُفِّرَ بالكثير من المزايا الّتي تُحاكي متطلبات هذا السّياق وثّم مقاطع فيديو تعليميّة عن كيفيّة استخدامه للمشاركين في الجلسات المنعقدة من خلاله وعبره كما ولمنسقي هذه الجلسات والمشرفين عليها.

التّحكم في الأشخاص المتصلين بمكالمات الفيديو والمحادثات

لا تمنع الخدمات عبر الإنترنت الأشخاص من تسجيل الدخول إلى المكالمات أو الدردشات باستخدام أسماء غير أسمائهم. للتأكد من أن كل شخص من يدعي، لا بدّ من التّحقّق من هوياتهم قبل الخوض بأي تفاصيل حسّاسة. في خضم جائحة الحمّى التّاجية كوفيد 19 ، اكتشف الكثيرون أن من يسعى لإزعاجهم قد يتسلل إلى مكالمات الفيديو الخاصة بهم. تمنح صلاحيات المشرفين في كتم الصوت أو طرد المشاركين الفرصة لإتمام هذه المكالمات دون تدخل، وعليه ينبغي لنا:

- معرفة من نرسل إليه طلب مكالمة أو دعوة للدردشة، بما في ذلك:
- التّثبّت من أرقام الهواتف أو عناوين البريد الإلكتروني التي نراسلها.
- الإحجام عن مشاركة الدعوات على وسائل التواصل الاجتماعي العامة.
- قبل البدء بأي مكالمة، لا بدّ أن نلم بأدوات المسؤول أو المشرف التي تتيح لنا كتم صوت المشاركين غير المرغوب فيهم أو حظرهم أو إخراجهم. وبتالي علينا تهيئة هذه الأدوات بحيث لا يتمكن سوى المشرفين من كتم صوت مكالمات الفيديو وحظرها.
- عندما تبدأ مكالمة أو محادثة، لا تفترض أنك تعرف المتصل فقط من خلال قراءة اسمه. ليس من الصعب أن يقوم شخص ما بإدخال اسم شخص تعرفه كاسم المستخدم الخاص به، ويتظاهر بأنه هو، وعليه لا بدّ لنا من:
  - التحقق من هويات جميع المشاركين في المكالمة من خلال مطالبتهم بالتحدث أو تشغيل الكاميرا الخاصة بهم.
  - التأكد من هويتهم عبر قناة أخرى مثل الدردشة الآمنة أو البريد الإلكتروني من أن الشخص المشارك في المكالمة هو بالفعل من يظهر اسمه على الشاشة.
  - التقاط لقطات شاشة أو سجل المشاركين غير المرغوب فيهم لجمع الأدلة لتحليلها لاحقًا واتخاذ الإجراءات القانونية.
  - طرد أي شخص لا ترغب في وجوده في المكالمة أو المحادثة.
  - إذا لم ينجح طرد شخص ما أو حظره، فعليك بإنهاء المكالمة وبدء مكالمة جديدة لا وجود للشخص المزعج فيها. كذلك تحقق مرة أخرى من قائمة أرقام الهواتف أو عناوين البريد الإلكتروني التي ترسل إليها، للتأكد من صحة نسبتها للأشخاص الذين تريد محادثتهم، واتصل بكل شخص عبر قناة أخرى للتحقّق من هويتهم على سبيل المثال، عبر مكالمة هاتفية إذا كنت تعتقد أن عنوان بريده الإلكتروني غير صحيح.

تغيير مكالمات الفيديو إلى الميكروفون وتعطيل التفعيل التلقائي للكاميرا

- افترض أنه عند الاتصال، قد يتم تشغيل الكاميرا والميكروفون بشكل تلقائي، لذا تحقق من هذا الإعدادات، وكن حذرًا فيما تظهره وتقوله إلى أن تتثبت من إلغاء تفعيل الكاميرا.
- فكر في تغطية الكاميرا بملصق أو ضمادة لاصقة، وقم بإزالتها فقط عند استخدام الكاميرا.

- فكر في خيار تعطيل الميكروفون والكاميرا من خلال إعدادات الجهاز إن لم نتمكن من إيقاف تشغيلهما خلال استخدام الخدمة قبل الاتصال.

حماية البيانات

مع تزايد كمية البيانات التي نجمعها ونخزنها من صور ومقاطع فيديو ومراسلات، تتعاظم حاجتنا إلى تعزيز حمايتها. ، من الضروري الانتباه لتأثير هذه البيانات علينا في حالة تسربها أو استغلال أشخاص لها ضدّنا.

قد تتمكّن الجهات المُخترقة من الوصول إلى بياناتنا الحساسة عبر الإنترنت أو من الاتصال المباشر معها، هذا يدفعنا لوضع عدّة خطوط دفاع لتفادي هذه الخروقات المُحتملة؛ يسوقنا ذلك لتقنيّة تشفير الملفات المحفوظة على أجهزتنا باعتباره أحد أشكال الحماية الفاعلة.

يُعرّف التّشفير بأنّه وسيلة تستخدمها البرمجيات لتشفير معلوماتنا من خلال عمليات رياضيّة معقّدة، ينشأ عن هذه العمليات مفتاح لفك التّشفير لا يملكه سوانا في شكل كلمة مرور أو شكل آخر. بعبارة أخرى، يُمكننا تشبيه التّشفير بحفظ معلوماتنا في خزانة موصدة بعدّة أقفال لا يملك مفاتيحها سوانا.

فيما يلي بعض الخطوات الّتي يُمكن أن تساعدنا على حماية ما نحفظه من بياناتٍ على أجهزتنا:

خيار حذف البيانات القديمة بدلًا من تخزينها

قد يشكل حفظ الصور ومقاطع الفيديو والمراسلات الشخصية خطرًا علينا. يقلل التّشفير من هذا الخطر؛ لكنه لا يزيله. تتمثّل الخطوة الأولى لحماية هذه البيانات الحساسة بتقليل كمية المعلومات التي نحتفظ بها. ما لم يكن لدينا سبب وجيه لحفظ ملف معين، ، علينا ببساطة حذفه .

خيار التّشفير الكامل لأجهزتنا

في حال سرقة أو استيلاء أشخاص على أجهزتنا بغية الاطلاع على ملفاتنا و اتصالاتنا، فلا بدّ لنا من وسائل حماية إيقافهم، وهذا يسوقنا لخيار التّشفير الكامل لأجهزتنا. قد تحتوي الحواسيب المكتبيّة والمحمولة على خيارات تشفير ضمنيّة. كذلك يمكن أن يوفر برنامج فيرا- كربت VeraCrypt حماية إضافيّة لملفات معيّنة، كذلك الأمر بالنّسبة لمحركات الأقراص الخارجيّة – أو يمكنّنا اللّجوء لتشفير الجهاز كاملًا، إن ارتأينا ذلك.

- تجدر الإشارة هنا إلى أنّ التّشفير الكامل للقرص لا يعمل إلّا إذا كان جهازنا مُطفأ بالكامل، وليس في وضع السكون المعروف أيضًا باسم بالتعليق أو الإسبات. إذ إن كان قيد التّشغيل فقد يجد الشخص المستحوذ على جهازنا سهولة أكبر في اختراق ملفاتنا و اتصالاتنا.

نظام تشغيل Android

يمكن تشفير معظم الهواتف العاملة بنظام تشغيل Android الإصدار السّادس وما تلاه. للتحقّق من ذلك، علينا الذّهاب إلى الإعدادات ثُم إعدادات الأمان، ثم التّشفير وبيانات

الاعتماد، بعد ذلك نبحث عن التّشفير أو تشفير الهاتف. يرجى ملاحظة أنّ خيارات الإعدادات قد تتباين من هاتف لآخر.

نظام تشغيل الآي. أو. اِس iOS

تُشفَّر أجهزة الآي-فون iPhone افتراضيا بمجرّد تعيين رمز الدّخول.

نظام تشغيل ماك Mac

- أولًا نصل حاسبونا بمقبس كهربائي كي نضمن ألّا يكف عن التّشغيل في أثناء التّثبيت.
- اتباع الإرشادات التالية للتشفير باستخدام Filevaul

نظام تشغيل ويندوز

إن كانت حواسيبنا تعمل بنظام ويندوز، يُمكننا تشفير أقراصها كما يلي: التّشفير باستخدام خاصية BitLocker المُضمَّنة لنظام التّشغيل: رابط

إذا قفزت أمامنا رسالة مفادها «لا يمكن لهذا الجهاز استخدام الوحدة النمطية للنظام الأساسي الموثوق به.» فذلك يعني أن حاسبونا يفتقر لوحدة نمطيّة للنظام الأساسي الموثوق به Trusted Platform Module المستخدمة للتشفير. مع ذلك، يمكننا من خلال تعديلات التكوين التّالية، لا يزال من الممكن استخدام BitLocker على الحواسيب الّتي تفتقر لوحدة نمطيّة للنظام الأساسي الموثوق به:

- الخطوة الأولى: نختر ابدأ ثم نتوجه إلى تشغيل (run)، ثم نكتب GPEDIT.MSC في مربع فتح، ثم ننقر فوق موافق. ستظهر لنا نافذة أخرى ننقر على محرّكات نظام التّشغيل.
- الخطوة الثّانية: الآن نختار بنقرتين اثنتين على «المطالبة بخطوات مصادقة إضافيّة عند بدء التّشغيل.» ما سيقودنا إلى نافذة جديدة. ملاحظة: ثمّ خيار للمطالبة بخطوات مصادقة إضافيّة عند بدء التّشغيل لا نريد المطالبة بها خادم ويندوز 2008 و ويندوز فيستا.
- الخطوة الثّالثة: نختار «تفعيل» مع التّثبّت من أنّ الخيار المفعّل هو خيار تفعيل BitLocker دون وحدة نمطيّة للنظام الأساسي الموثوق به متوافقة معه، وهو الخيار الّذي يتطلّب كلمة مرور أو رمز لبدء التّشغيل يُحفظ على وحدة نقل وتخزين البيانات، ثُم ننقر موافق.
- الخطوة الرّابعة: نغلق نافذة محرّر المجموعة.

البريد الالكتروني ووسائل التواصل الاجتماعي

عند الكثيرين تعدت وسائل التواصل الاجتماعي او البريد الالكتروني كونها مجرد وسيلة تواصل أو متابعة للأحداث واخبار الأصدقاء فأصبح البعض يعتبرها مكان لنسخ احتياطية لملفات اعماله او صوره الشخصية أو مراسلاته الشخصية الخاصة ويحتفظ بنسخ منها من خلال إرسالها إلى نفسه، وهذا ما يزيد من الخطر الذي يهدد الخصوصية والأمن وقد يجعل النساء عرضة للابتزاز في حال تم اختراق احد حساباتهم لذلك هناك إجراءات يجب القيام بها عند إنشاء حسابات خاصة بنا.

البريد الالكتروني

- تجنب جعل البريد الإلكتروني الخاص بالعمل نفسه هو المستخدم لانشاء حسابات على وسائل التواصل الاجتماعي او مواقع أخرى على الانترنت.
- عند إنشاء كلمة المرور اتبع إرشادات انشاء كلمة مرور قوية المذكورة في هذا الفصل.
- تفعيل التحقق من خطوتين باستخدام تطبيقات الهاتف المحمولة مثل Authy

حسابات التواصل الاجتماعي

- قم باستخدام بريد الكتروني خاص بك غير معروف للعلن وتجنب مشاركته مع الاخرين او التسجيل بمواقع عامة على الانترنت من خلاله.
- قومي بتسجيل الدخول اليه من فترة لفترة أخرى.
- قومي بإنشاء كلمة مرور قوية.
- فعل التحقق من خطوتين من خلال تطبيق Authy
- بين الفينة والأخرى فحص البريد الإلكتروني إذا كان ضمن بيانات مسربة من خلال هذا الرابط.
- تفعيل إعدادات الخصوصية وإعادة ضبطها حيث ان مشاهدة الحساب والمحتوى تقتصر على الأصدقاء فقط.
- تجنب فتح الروابط او الملفات التي تصلك على وسائل التواصل الاجتماعي واذا كان شخص معروف لديك عليك التواصل معه او معها من خلال وسيلة أخرى للتأكد من كونهم المرسلين فعلا.

منشورات جمعية المرأة العاملة الفلسطينية للتنمية
الموقع الإلكترونيّ: www.pwwsd.org
البريد الإلكترونيّ: pwwsd@pwwsd.org