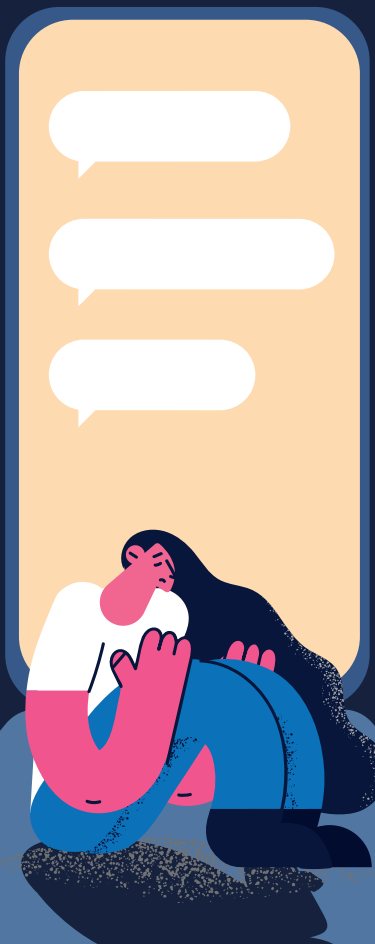
سلام@

Salam@

دليل مواجهة العنف الرقمي

لطالبات الجامعات في الأردن

الإنترنت الآمن حقي



كوني آمنة أونلاين

سلام@ Salam@

دليل مواجهة العنف الرقمي
لطالبات الجامعات في الأردن

I. مقدمة

أسهمت التكنولوجيا الحديثة بانتشار نوع جديد من العنف ضد المرأة و الذي يعرف بالعنف الإلكتروني و الذي يعد من أخطر أنواع العنف و ذلك بسبب آثاره السلبية التي تنعكس عليها سواء من الناحية النفسية أو الصحية أو الاجتماعية، فالمرأة المعنفة إلكترونيا ترفض عادة البوح خوفا على العرض و السمعة من الفضيحة، و في أحيان كثيرة قد تستسلم المرأة فيتم عندئذ ابتزازها .إما بالمال أو بالتحرش الجنسي أو يتم تجنيدها كوسيلة تستخدم بأعمال إجرامية إرهابية.

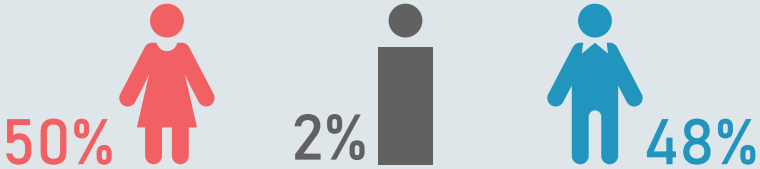
فقد شهد العنف الرقمي ضد النساء وخاصة التحرش وما يصاحبه من إكراه في العلاقات الجنسية، أو الابتزاز أو الاحتيال،، ويكون من أشكال العنف الرقمي استخدام الصور أو مضايقات أو إهانات شخصية أو تهديد من خلال أجهزة إلكترونية أو مقاطع فيديو حميمة لأشخاص آخرين بهدف إبتزازهم وتكون الصيغة التهديد طبعا، وفي نظر المجتمع اللوم على الضحية لا على المذنب.، وهنالك التعليقات السيئة والمحقرة والمهينة وهناك أيضا من تتعرض لرسائل تحمل شتما أو تهديدا صريحا أو صورا خادشة للحياء، ويمتد الأمر إلى اختراق الحسابات الشخصية وانتحال الهوية الإلكترونية للحصول على معلومات أو صور محرجة بغرض نشرها أو ابتزاز صاحباتها.

لا بد لنا ان نعترف بأن ظاهرة العنف ضد المرأة من القضايا المستمرة والمستجدة، اذ لا يخلو مجتمع من هذه الظاهرة . ومع انتشار العولمة الالكترونية التي أصبحت سمة من سمات العصر – لا سيما أثناء جائحة كورونا– فقد أصبح الانترنت نافذة الحرية لكثير من النساء وتزايد استخدام مواقع التواصل الاجتماعي ومختلف التطبيقات الإلكترونية بين مختلف الفئات العمرية ،فقد أتاح لهن مساحة من حرية التعبير والتواصل وكذلك العمل. لكن بالمقابل عزز ذلك العنف ضد المرأة ولكن بشكل غير مباشر.

ومن خلال استبانة تم توزيعها على طالبات الجامعات الاردنية بطريقة عشوائية، أظهرت النتائج أن هناك معرفة خجولة لدى طلبة الجامعات حول العنف الرقمي سواء بتقديم تعريف محدد للعنف الرقمي او الأمور القانونية والنفسية التي تحتاجها الضحية ،أو حتى الجهات التي من الممكن أن تلجأ اليها من تعرضت للعنف الالكتروني بأنواعه وغير ذلك مما سيتم ذكره لاحقًا.

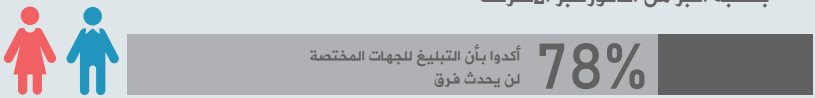
I. مقدمة

أظهرت النتائج أن هناك معرفة خجولة لدى طلبة الجامعات حول العنف الرقمي !

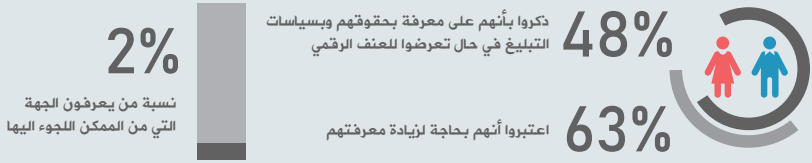


- كانت نسبة من أجاب من الاناث 50٪ والذكور 48٪ فيما فضل 2٪ عدم التصريح عن الجنس

- كانت بعض الإجابات صادمة، فقد صرّح 81٪ أن النساء أو الفتيات هن من يتعرضن للعنف بنسبة أكبر من الذكورعبر الانترنت



- ورغم أن 78٪ أكدوا معرفتهم بوجود جهات مختصة يمكن اللجوء إليها في حال التعرض للعنف الرقمي، إلا أن الغالبية أكدت بأن التبليغ لن يحدث فرق، مع الشعور بالخوف وعدم معرفة الجهات المختصة التي يجب اللجوء إليها بالإضافة أوعدم الثقة في تلك الجهات



- وبالرغم من أن 48٪ ذكروا بأنهم على معرفة بحقوقهم وبسياسات التبليغ في حال تعرضوا للعنف الرقمي، إلا أن 63٪ اعتبروا أنهم بحاجة لزيادة معرفتهم سواء من الناحية التكنولوجية أوالقانونية أو النفسية أو الاجتماعية وأثر هذا النوع من العنف على المجتمعات

سيناريو رقم 1: حوار طالبة مع المدرس

سيناريو رقم 2: حوار طالبه مع زميلها

A. تعريف العنف الرقمي

العنف الرقمي بشكل عام هو سلوك عبر الإنترنت يشكل أو يؤدي إلى الاعتداء على الرفاه الجسدي والنفسي والعاطفي لفرد أو جماعة.
وما يميز العنف الإلكتروني عن أشكال العنف التقليدية خارج الإنترنت هو أنه في الحالة الأولى، يحدث جزء كبير من السلوك عبر الإنترنت، على الرغم من أنه قد ينتقل بعد ذلك إلى سياقات غير متصلة بالإنترنت. وبالتالي ، قد يكون للعنف الرقمي _ولكن ليس من الضروري_ مكون مادي، والكثير من الضرر النفسي و / أو العاطفي.

أما العنف الرقمي القائم على النوع الاجتماعي فهو عبارة عن مضايقات وتحيزات مستهدفة من خلال التكنولوجيا ضد الأشخاص، وبشكل اساسي ضد النساء، على أساس جنسهن. والمصطلح مشابه أيضًا لمضايقات الإنترنت والتسلط عبر الإنترنت والتمييز عبر الإنترنت، لكن المصطلحات الأخيرة ليست خاصة بنوع الجنس[1]

1. ما هي الأفعال التي تصنف عنف رقمي، وكيف نميز أننا تعرضنا له

هنالك عدة افعال تصنف أنها عنف رقمي مثل التحرش والمطاردة الإلكترونية، التنمر والابتزاز الالكتروني فالتحرش الالكتروني هو سلوك متكرر يهدف إلى تهديد وإخافة وفضح وإسكات المستهدفين وقد يكون شبيها بالتحرش الواقعي لكنه أشد أذى منه.

و يمكن أن يشمل العنف القائم على النوع الاجتماعي عبر الإنترنت ملاحظات جنسية غير مرغوب فيها، وتهديدات ، وخداع، ومطاردة ومضايقات عبر الإنترنت، والمشاركات التمييزية القائمة على نوع الجنس.

وقد يحدث العنف القائم على النوع الاجتماعي عبر الإنترنت من خلال طرق مختلفة وتشمل : انتحال الهوية، والقرصنة، والبريد العشوائي، والتتبع والمراقبة، والمشاركة الضارة للرسائل.

[1] https://2u.pw/IreCB

أشكال العنف الرقمي القائم على النوع الإجتماعي

المشاركات التمييزية القائمة على نوع الجنس

ملاحظات جنسية غير مرغوب فيها

القرصنة

تهديدات وخداع

مطاردة ومضايقات عبر الإنترنت

انتحال الهوية

المشاركة الضارة للرسائل

2. ماذا تفعلين عندما تتعرضين للتنمر:

يمكنك أن تواجهي من يتنمر عليك و تخبريه أن ما يفعله جريمة وعليه أن يتوقف

يمكنك أيضًا عدم الرد عليه والتبليغ عن تعليقه أو رسالته على الموقع نفسه او تفعيل خاصية الحظر

ابتعدي عن الصفحات والمجموعات التي يحدث فيها التنمر ولا يقوم المسؤولون عن تلك الصفحات بحظر المتنمرين

تحدثي إلى شخص تثقين به، لا تحتفظي بمشاعرك بالداخل، فإخبار شخص ما يمكن أن يساعدك على تقليل الشعور بالوحدة ومساعدتك في وضع خطة لوقف التنمر

إذا وجدت صفحة لا تحظر المتنمرين او المسيئين قومي بتقليل تقييم الصفحة على الموقع

3. كيفية التبليغ عن العنف الرقمي على وسائل التواصل الإجتماعي:

يتعرض العديد من المستخدمين، خصوصاً النساء إلى حالات عنف لفظي قد يكون ابتزاز أو محاولات تشهير على مختلف منصات التواصل الاجتماعي، في هذا الدليل سنذكر كيفيّة الإبلاغ عن الحسابات أو النشاطات غير المقبولة في منصّة فيسبوك، انستغرام.

متى يجب علينا الإبلاغ عن حساب مخالف؟

يقوم العديد من المهاجمين باستخدام حسابات وهميّة لإخفاء هويتهم وخداع الآخرين، نستطيع التعرف على هذا النوع من الحسابات عن طريق ملاحظة بعض الخصائص فيها، على سبيل المثال قد يحتوي الحساب الوهمي على عدد قليل من المنشورات، الصور أو الاصدقاء، كما من المحتمل أنّ يكون قد تمّ إنشاؤه منذ فترة قصيرة. إذا تواصل معكن أي حساب من هذا النوع وطلب منكن أي بيانات، يجب الإبلاغ عنه حالاً.

بالإضافة إلى ذلك، يمكن أنّ يقوم بعض الأفراد في مواقع التواصل الإجتماعي بانتهاك خصوصيّة الآخرين، مثل نشر صور يظهر فيها وجوه أشخاص من غير موافقتهم على نشرها. كما يمكن أن يتعرّض بعض المستخدمين للتشهير أو الابتزاز بعد جمع معلومات أو صور عنهم وتشكل النساء والفتيات الشريحة الأكبر من ضحايا هذا النوع من العنف. بالإضافة إلى ذلك، يقوم البعض بتهديد الآخرين أو نشر محتوى غير لائق أو محتوى يحث على العنف والكراهية بشكلٍ عام.

كيف نقوم بالإبلاغ عن حساب أو نشاط؟

يمكنكم الإطلاع على الروابط الخاصّة بنماذج الإبلاغ عن معظم خروقات معايير المجتمع والسياسات الخاصّة بمنصّة فيسبوك: عن طريق تبويت المساعدة الخاص بالتطبيق. كما يمكنكم أيضاً النقر على خيارات المنشور أو الحساب ثم الضغط على ابلاغ بعد ذلك اختيار السبب المناسب للإبلاغ.

أما بالنسبة لمنصّة انستغرام، بعد معاينة الحساب أو المحتوى والتأكّد من قيام هذا الشخص بمخالفات للشروط والقواعد المجتمعيّة، يمكنك الإبلاغ عن الحسابات عن طريق زيارتها والنقر على إبلاغ ، ثم اختيار السبب المناسب، فيما يتعلّق بالمراسلات، يمكنك أيضاً الإبلاغ عنها إذا أرسل إليك شخص ما رسائل غير لائقة، عن طريق الضغط بشكل مطوّل على الرسالة، ثم على إبلاغ ، بعدها اختيار سبب الإبلاغ. وأخيراً المنشورات يمكن الإبلاغ عنها عن طريق النقر على خيارات المنشور، ثم على ابلاغ، واختيار السبب المناسب للإبلاغ[2].

[2]Salamtech Wiki

4. الدعم النفسي الإجتماعي

أظهرت الأبحاث أن للعنف السيبراني تأثير كبير على اكتئاب المراهقات ، والقلق وعلى تكوين الصورة الذاتية لهن بالإضافة إلى الاضطرابات العاطفية والسلوك الانتحاري. وعلى عكس المفاهيم الخاطئة السائدة، من الصعب الهروب من العنف السيبراني أو إيقافه.

بسبب النقص في دعم الناجيات والمفاهيم الخاطئة الواسعة الانتشار،يتعين على الضحايا / الناجيات التعامل مع الخسائر النفسية للعنف السيبراني بمفردهن يوميًا تقريبًا. استطلاع رأي عبر الإنترنت شمل 60 مشاركًا من قبل خدمات دعم النساء المعنفات في كولومبيا البريطانية وجد أنه بعد تعرضهن للعنف عبر الإنترنت، فإن ٪48 من النساء اللاتي شملهن الإستطلاع تعرضن لقلق مزمن و (اضطراب ما بعد الصدمة) وذكر ٪43 أن صورتهن الذاتية قد تضررت، و ٪40 أفادوا أنهم انسحبوا من النشاط على الإنترنت، ٪30 شعروا بالخجل والإذلال، ٪28 شعروا بالعزلة من الأصدقاء والعائلة، كما أفاد ٪13 بأن ذلك أثر على عملهم، ٪10 أفادوا أن لديهم أفكارًا انتحارية والانخراط في إيذاء النفس و٪3.3 من النساء قلن إن عليهن تغيير السكن والمجتمع الذي ينتمون إليه.

ولأن التنمر الإلكتروني لا يقل خطورة عن التنمر المباشر أو التقليدي سواء عن طريق الألفاظ المباشرة أو المضايقات باستخدام أساليب و مفردات جارحة قد تكون في أغلب الاوقات مستوحاة من معاناة يمر فيها الشخص او خصائص معينة في شكله الخارجي. ولأن المتنمرين عادة يختبئون وراء شاشة أجهزتهم الإلكترونية، فمن السهل عليهم التلفظ وكتابة كلام جارح قد يؤثر سلبيا على العديد من الأشخاص، وخصوصا النساء. تأكدي ان عالم الانترنت فيه مزايا عدة تساعدك على الحماية من التعرض لمثل هذه المواقف. احم نفسك ولا تستسلمي للاكتئاب والعزلة. حافظي على سلامتك النفسية والرقمية! قومي بالإبلاغ عن التنمر أو العنف الإلكتروني عن طريق وسائل التواصل الإجتماعي أو عن طريق مقدمي الخدمات والجهات المختصة و لا تتردي في طلب الدعم النفسي الإجتماعي.

تقدم جمعية معهد تضامن النساء الأردني، خدمات الدعم النفسي الإجتماعي لضحايا العنف الإلكتروني.

للتواصل:
065543867 | عمان، شارع وصفي التل(الجاردنز) مجمع تطوير العقارات
065543863 | رقم 145 الطابق الرابع

5. ماذا نفعل كأفراد عندما نتابع حالة تشهير مسيئة لشخص ما؟

إذا كانت ضحية التشهير في نطاق معارفنا علينا ان نتواصل معها لنطمئنها دون الخوض في تفاصيل قد تكون ضاغطة عليها.

عدم الرد على من يساعد في نشر المعلومات والتبليغ عن تعليقه أو رسالته على الموقع نفسه او تفعيل خاصية الحظر.

المساعدة في توفير دعم قانوني للضحية لعقاب من يساهم في نشر معلومات مغلوطة أو يساهم في التشهير بها.

إذا وجدت صفحة لا تحظر ناشري أخبار التشهير او المسيئين قومي بتقليل تقييم الصفحة على الموقع و اكتبي لماذا فعلت ذلك.

A. الجانب القانوني

1. نصوص قانون الجرائم الإلكتروني المتعلقة بالعنف الرقمي

ينظم قانون العقوبات الأردني الكثير من المسائل والتعديات والخلافات التي قد تنشأ عن معاملات الأفراد بين بعضهم. ومن الجدير بالذكر أن معظم مواد القانون صيغت قبل ظهور شبكة الإنترنت و نشوء العنف الرقمي المبنية على النوع الاجتماعي، فلا تفترض غالبية نصوصه استخدام الوسائل الرقمية و تتسم بالعمومية بغض النظر عن الوسيلة المستخدمة.

فقد حدد القانون الاردني في مواده التالي:

المادة 3

أ- يعاقب كل من دخل قصداً إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو بكلتا هاتين العقوبتين

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء، أو حذف، أو إضافة، أو تدمير، أو إفشاء، أو إتلاف، أو حجب، أو تعديل، أو تغيير، أو نقل، أو نسخ بيانات، أو معلومات، أو توقيف، أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات الشبكة المعلوماتية فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

ج- يعاقب كل من دخل قصداً إلى موقع الكتروني لتغييره، أو إلغائه، أو إتلافه، أو تعديل محتوياته، أو إشغاله، أو انتحال صفته، أو انتحال شخصية مالكه بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

المادة 4 يعاقب كل من ادخل أو نشر أو استخدم قصداً برنامجا عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو التقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول اليهم أو تغيير موقع الكرتوني أو الغائب أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح بالحبس مدة لا تقل عن ثلاثة اشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) الف دينار.

المادة 5 يعاقب كل من قام قصداً بالتقاط أو باعتراض أو بالتنصت أو أعاق أو حور أو شطب.

A. الجانب القانوني

1. نصوص قانون الجرائم الإلكتروني المتعلقة بالعنف الرقمي

محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار.

المادة 6: يعاقب كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو بالمعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (2000) الفي دينار.

ماذا تفعلي عندما تتعرضي لعملية إبتزاز؟

2. التبليغ قانونيًا عن طريق وحدة الجرائم الإلكترونية أو منظمات المجتمع المدني التي تقدم المساعدة في هذا المجال

الجهات المختصّة بتقديم الدّعم، المساعدة والمشورة لضحايا الجرائم اللاكترونيّة

01 مديريّة الأمن العام، إدارة البحث الجنائيّ – وحدة مُكافحة الجرائم الإلكترونيّة.
للقيام بالتّبليغ عن جريمة إلكترونيّة، نشجّعك بالاتصال بوِحدة مُكافحة الجرائم الإلكترونيّة للقيام بالاجراءات المناسبة التي تضمن لك الخصوصيّة

طريقة تقديم شكوى الجرائم إلكترونية في الأردن يتم من خلال:

التوجه إلى أقرب مركز امني ، ومن ثم يقوم المركز الأمني بتحويلها عن طريق كتاب رسمي وذلك إلى وحدة مكافحة الجرائم الإلكترونية " أو يمكن التوجه إلى المدعي العام القريب من سكن المشتكي " و تقديم استدعاء بالدعوى المراد رفعها ، وطلب تحويلها والانتقال بها إلى وحدة مكافحة الجرائم الإلكترونية في إدارة البحث الجنائي.

أو يمكن التواصل مع وحدة مكافحة الجرائم الإلكترونية

بأي وقت عبر صفحتها على موقع فيسبوك أو من خلال الخط الساخن 065633404 أو رقم واتساب 0770993331

02 الجمعيّة الأُردنيّة للمصدر المفتوح جوسا

الجمعية الأردنية للمصدر المفتوح

يقدّم فريق "جوسا" الدّعم التقني اللّازم للمتضرّرين وبدون أي مُقابل في حالات الطّوارئ وتوفير خدمة الدّعم الفوريّ عبر الرقم: (0770709900) لكل من يتعرض للهجمات الإلكترونيّة.

03 سلامات

فريق من المهتمات والمهتمين بالسلامة الرقمية من عدة دول عربية، هدفهم هو زيادة الوعي العام بالسلامة الرقمية للجميع وبناء قدرات دائمة للنساء والشباب للعمل بأمان عبر الإنترنت من خلال خلق مساحات معرفة متجددة مع الشركاء المحليين، تشمل أنشطتهم حملات توعوية وجلسات التدريب والتوعية والعيادات الرقمية والدعم التقني، فضلاً عن الدعم النفسي والاجتماعي
الموقع للالكتروني: salamatmena.org
البريد الالكتروني: support@salamatmena.org

B. تعريف السلامة الرقمية

السلامة الرقمية:هي كل الطرق والوسائل المتعددة، والمختلفة التي يكون هدفها حماية حسابات الإنترنت وحماية الملفات من المتسللين أو من قبل مستخدمين خارجيين غير مصرح لهم بالدخول إلى هذه الحسابات أو الملفات وبالتالي تهديد الأمن الرقمي، وهي الاستخدام الآمن للأدوات الرقمية و التكنولوجية بشكل يضمن خصوصيتنا وسلامتنا التقنية و القانونية والنفسية عند استخدام شبكة الانترنت.

تبدأ السلامة الرقمية بعدة خطوات أساسية أولها هو استخدام كلمات سر Passwords قوية وآمنة، ولكن حتى لو كانت كلمة السر قوية وكانت أسئلة الأمان الخاصة بها ضعيفة تبقى معرضة للسرقة والإختراق.

لحماية جهازك وحساباتك على الإنترنت يتوجب عليك اتخاذ عدة اجراءات خاصة السلامة الرقمية:

1. خاصية التحقق بخطوتين

التحقق بخطوتين Two Factor Authentication هي إحدى أهم الطرق المستخدمة في يومنا هذا للمصادقة على شخصية مستخدم ما يحاول الوصول إلى حساب له سواء على الانترنت أو على حسابه الشخصي، تعتمد عملية التحقق بخطوتين على أمرين:

شيء تعرفينه: وهو كلمة السرّ.
شيء تملكينه: مثلا هاتفك الجوال المرتبط بالحساب أو مفتاح يو إس بي USB Key يسمى أيضا مفتاح U2F مرتبط بالحساب وهناك أدوات أخرى أقل شيوعا.

إذًا لإتمام عملية المصادقة أي التحقق من شخصية وأهلية المستخدم للدخول إلى حساب يجب على المستخدم أن يدخل كلمة السرّ الصحيحة Password وبعد ذلك عليه أن يستخدم رمزا سريًا يولده الجهاز الذي بحوزة المستخدم والمرتبط بالحساب.

من الممكن أن يتم تفعيل عملية التحقق بخطوتين في حال كانت الشركة أو الموقع يدعم هذه الميزة، لحسن الحظ في يومنا هذا قامت معظم المواقع المعروفة بدعم هذه الميزة مثل غوغل، فيسبوك، مايكروسوفت وغيرها.[3]

[3] Salamtech Wiki

إعدادالتحقق بخطوتين في واتس اب WhatsApp Two-Factor Authentication setup
لتفعيل ميزة التحقق بخطوتين اتبعِ الخطوات التالية:

- من تطبيق واتس أب قومي بالدخول إلى الحساب Account
- من قائمة الحساب إبحثي عن ميزة التحقق بخطوتين Two-step verification
- ثم قومي بتفعيل الميزة Enable
- قومي باختيار رمز من 6 أرقام يمكنك حفظه وقومي بإدخاله
- قومي بادخال الرمز مرة أخرى
- قومي بإدخال عنوان إيميل صحيح لاسترجاع الحساب في حال نسيان الرمز[4]

2.كلمات المرور وكيفية إدارتها وحفظها

تستخدم كلمات السر، Passwords والتي تسمى أيضا كلمات أو عبارات العبور، Pass-phrases لحماية حسابات البريد الإلكتروني والحسابات على مواقع مثل مواقع التواصل الاجتماعي، وأيضا لحماية الحاسب الشخصي، حماية الحاسب المحمول وغيره من الأجهزة الالكترونية الشخصية، وتكون بذلك أسلوبا من أساليب المصادقة Authentication للتحقق من صحة هوية المستخدم الذي يطلب الوصول Access لحساب ما سواء على الحاسب الشخصي أو الانترنت، تستخدم كلمات السرّ أيضا في التشفير Encryption.

- اختيار كلمة سر جيدة Choosing a "Good" Password

عند اختيار كلمة السر اتبعي الشروط التالية لتفادي أي مخاطر:

- اختاري كلمة سرّ من 16 خانة على الأقل
- استخدمي أرقام ورموز مثل _()*&^%$! ضمن كملة السرّ
- امزجي استخدام الأحرف الصغيرة a b c d... والأحرف الكبيرة A B C D...
- تجنبي استخدام الأحرف المتجاورة مثلا تعتبر كلمة qwerty وأيضا 123456 من أسوأ كلمات السر
- تجنبي استخدام معلومات شخصية كالاسم أو العائلة أو رقم الهاتف الشخصي أو رقم هاتف الوالدين
- تجنبي استخدام العبارات الشهيرة أو المستخدمة بكثرة في كلمات السّر
- عدم استخدام كلمة السر على أكثر من حساب واحد

[4]Salamtech Wiki

ادارة كلمات السر Passwords Management

تطلق تسمية إدارة كلمات السرّ على عملية اختيار كلمات السرّ للحسابات المختلفة وحفظها بشكل آمن وتدويرها ، أي استبدالها بكلمات سرّ جديدة كل فترة زمنية.

فعلى الرغم من أن تعليمات اختيار كلمات السرّ الجيدة واضحة، إلّا أن الكثير من المستخدمين يجدون صعوبة في اختيار كلمات سرّ جيدة للحسابات الكثيرة التي يديرونها، ويجدون صعوبة في حفظها ما يضطرهم إلى استخدام كلمات سرّ ضعيفة أو تكرار استخدام كلمة السرّ ذاتها على مواقع مختلفة ما يزيد احتمال اختراق حساباتهم في حال حصول تسرب لبيانات الدخول على أحد المواقع الحل الأنسب هو أن تستخدمي أحد برامج إدارة كلمات السرّ، التي تسمح للمستخدمين إنشاء كلمات سرّ جيدة وحفظها بشكل آمن ضمن ملف أو ملفات خاصة ببرنامج إدارة كلمات السرّ، بهذا الشكل لا يضطر المستخدم لحفظ أي من كلمات السرّ الكثيرة المخزنة ضمن هذه الملفات.

تطبيق LastPass والإصدارات الحديثة منه يمكنك من حفظ كلمات السر الخاصة بك والوصول لها في أي مكان كما هو معتاد، يمكنك الوصول لهذه البيانات بإستخدام عنوان البريد الإلكتروني وكلمة السر الخاصين بك.

A. إدارة البيانات الشخصية والاحتفاظ بها بشكل آمن

بشكل عام، الخصوصية Privacy هي الحد الذي يفصل بين ما يحق وما لا يحق للآخرين أو المجتمع معرفته عن حياتنا الخاصة. بكلمات أخرى تعني الخصوصية قدرة أو حق شخص أو مجموعة من الأشخاص في البت في ما يمكن نشره من معلومات عنهم على العلن وما لا يمكن نشره.

1. كيفية إدارة البيانات وتأمينها ونسخها احتياطيًا، وحذف البيانات / إتلافها بشكل آمن

النسخ الإحتياطي في تكنولوجيا المعلومات يدل على نسخ وأرشفة معلومات الحاسوب حتى يمكن استعادتها في حال تم فقدان المعلومات الأصلية أو العبث به.

يتم النسخ الاحتياطي إلى أجهزة محلية أو أجهزة بعيدة عن طريق الإتصال بالإنترنت (تخزين سحابي) أو كلاهما معاً، وإلى وسائط تخزين أخرى مثل: القرص الصلب الثابت أو المحمول (قرص صلب خارجي)، بطاقات الذاكرة التخزينية.

كي تكون عملية النسخ الاحتياطي ناجحة يجب أن تحقق النقاط التالية:

- يجب أن تكون عملية النسخ الاحتياطي أوتوماتيكية.
- يجب أن تكون عملية النسخ الاحتياطي دوريّة.
- يجب أن تكون النسخ الاحتياطية آمنة، أي أن المعلومات المحفوظة في النسخة الاحتياطية، لا يمكن التلاعب بها، ولا يمكن معاينتها من قبل غير المخولين لهم بذلك
يجب أن تكون النسخ الاحتياطية ذاتها في أمان، أي أنها غير معرضة للتلف، أو الضياع.

حذف الملفات لا يؤدي بالضرورة لاختفائها بشكل نهائي من الحاسب أو الأقراص الصلبة الخارجية أو اليو إس بي ميموري ستيك المعروفة أيضا بالفلاش ميموري USB Memory Stick.

فعلى سبيل المثال في نظام ويندوز يمكن البحث عن الملفات المحذوفة ضمن سلة المحذوفات واستعادتها، عند افراغ سلة المحذوفات Recycle Bin لا يتيح نظام التشغيل ويندوز استعادة هذه الملفات ويبدو أن الملفات وبالتالي البيانات قد حذفت نهائيا. لكن الواقع بعكس ما يتوقعه كثيرون غير ذلك، في الواقع تبقى البيانات موجودة على القرص لكن ما يتم حذفه هو عنوان وجودها في سجل نظام التشغيل.

يمكن تدمير البيانات على الأقراص الصلبة باستخدام برامج خاصة مثل برنامج بليتشبت وسي كلينر Bleachbit CCleaner

3. صلاحيات التطبيقات على الأجهزة

في كل مرة تنصبين تطبيقا على جهاز هاتفك الذكي، فإن هذا التطبيق يطلب أذونات (صلاحيات) للدخول إلى بعض من المعلومات الموجودة على هاتفك، مثل الصور ومقاطع الفيديو وجهات الاتصال، أو بعضا من التقنيات التي يحويها مثل الكاميرا أو المايكروفون، أو تحديد الموقع الجغرافي تعمل التطبيقات الخاصة بالأجهزة الذكية والحواسب اللوحية بطريقة تختلف عن البرامج المصممة لتعمل على أجهزة الحاسب، وهي تقدم خدمات مختلفة، ويتوفر الكثير منها مجانا، لكنها تستفيد من المعلومات التي تجمعها عنك، أو ترسل لك الإعلانات. لا يمكن القول بأن جميع هذه التطبيقات خطرة، وتعرض خصوصيتك للخطر، فمعظمها يقوم بذلك لأهداف تجارية بحتة:
عند تنزيل التطبيق، فإنه يعرض عليك الأذونات التي يطلبها بالتالي، قبل تحميّل اي تطبيق تأكدي مما يلي:

عند تنصيب التطبيق، فإنه يعرض عليك الأذونات التي يطلبها بالتالي، قبل تحميّل اي تطبيق تأكدي مما يلي:

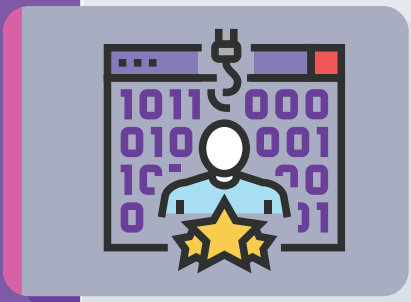
- حملي التطبيقات من متاجر التطبيقات الموثوقة مثل Google Play Store
- لا تقومي بتحميل التطبيقات من متاجر أو مواقع مشبوهة أو دون معرفة مصدرها
- تاكدي من هوية ومصداقية المطور وابحثي بجانب اسم المطور عن علامة زرقاء تعطى للمطورين الموثوقين على المتجر.
- لا تقومي بتحميل التطبيقات التي لا تظهر العلامة الزرقاء بجانب اسم مطورها وأيضا لا تقم بتنصيب التطبيقات غير المعروفة.
- إقرئي المراجعات جيدا لتعرفي أكثر عن التطبيق، حاولي البحث عن المراجعات التي تتناول موضوعي الخصوصية والأمان.
- لا تقومي بتحميل وبتنصيب التطبيقات ذات المراجعات السلبية فيما يتعلق بالخصوصية والأمان.
- راجعي الأذونات التي يطلبها التطبيق جيدا، ولا تقومي بتنصيب أي تطبيق يتطلب أذونات أكثر مما يحتاج لإنجاز عمله، أو الذي يطلب أذونات قد تشكل مصدرا للخطورة على خصوصيتك وأمانك.

B. كيفية تجنب عمليات التصيّد الاحتيالي

ما هو التصيد؟ تعد هجمات التصيد الاحتيالي من بين مخططات الهندسة الاجتماعية الأكثر شيوعًا. تتضمن رسائل البريد الإلكتروني أو الوسائط الاجتماعية أو الرسائل القصيرة أو رسائل الدردشة المصممة لخداع الأشخاص لمشاركة المعلومات التي قد تساعد في ارتكاب جريمة أكثر خطورة أو تثبيت برامج ضارة عن طريق النقر فوق ارتباط أو فتح مرفق.

تتم معظم هجمات التصيد الاحتيالي من خلال رسائل جماعية عامة تبدو شرعية وتأتي من مصدر تثق به عادةً (على سبيل المثال من وكالة حكومية أو بنك أو خدمة وسائط اجتماعية). ولكن هناك أيضًا هجمات تصيد تستهدف أفرادًا أو مجموعات معينة ، وتقوم الجهات الخبيثة باستمرار بابتكار أدواتها وحيلها وتغييرها.

هذه هي الأنواع الأكثر شيوعًا لهجمات التصيد الاحتيالي:



هجمات صيد الحيتان

هي هجمات تصيد بالرمح تستهدف "الأسماك الكبيرة" ، مثل رؤساء المنظمات وأصحاب أو رؤساء تحرير المؤسسات الإعلامية. تتضمن هجمات صيد الحيتان عادةً رسائل بريد إلكتروني احتيالية تبدو وكأنها بريد إلكتروني مهم مُرسَل من مسؤولين حكوميين أو شركاء من منظمات مهمة مثل الوكالات المانحة.

التصيد بالرمح

هو نوع من هجمات الصيد حيث يستهدف ممثل ضار شخصًا معينًا عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي أو الرسائل النصية القصيرة أو رسائل الدردشة التي تبدو مقنعة وكأنها من شخص يعرفه الهدف – مثل زميل أو صديق.

هذه هي الأنواع الأكثر شيوعًا لهجمات التصيد الاحتيالي:

هجمات SMiShing تتضمن رسائل نصوص SMS

قد يقوم المحتالون الذين ينفذون هذه الهجمات بانتحال شخصية شخص تعرفه لطلب المال أو المعلومات الشخصية، يتظاهر الأشخاص الذين يقفون وراء هذه الهجمات أنهم خدمة تستخدمها (مثل شركة البريد السريع أو منصة التسوق عبر الإنترنت) لطلب دفعة أو تقديم تحديث، أو يتظاهرون أنهم فيسبوك أو شركة وسائط اجتماعية أخرى ليطلبوا منك رمز التحقق الذي تتلقاه عبر النظام الأساسي

الروابط المضمنة التي تأخذك عند النقر عليها إلى مواقع ويب مزيفة مصنفة ببرامج ضارةيد الاحتيالي

اكتشاف البريد الإلكتروني المخادع

تتطور أساليب التصيد باستمرار، غالبًا ما تحاكي رسائل التصيد الاحتيالي الأسلوب وتستخدم شعارات حقيقية لمنظمات شرعية لخداعك، ومع ذلك ، تحتوي العديد من رسائل البريد الإلكتروني المخادعة على واحد أو أكثر من الميزات الشائعة المدرجة أدناه والتي يمكن أن تساعدك في اكتشاف مثل هذه الهجمات.

عناوين البريد الإلكتروني المزيفة التي تبدو حقيقية لخداعك، على سبيل المثال، قد يتظاهر المهاجمون بشخصية أمازون لمحاولة سرقة بيانات الاعتماد الخاصة بك عن طريق خداعك من أجل "تحديث" أو "تأكيد" بياناتك، يجب أن تدرك أن هناك خطر ما عندما يأتي هذا البريد الإلكتروني من عنوان ينتهي بـ amazonheadoffice.com @ أو amazzon.com @، بدلاً من amazon.com @ أيضًا ، تجدر الإشارة إلى أنه لن ترسل لك أي مؤسسة شرعية وكبيرة رسائل بريد إلكتروني من عنوان ينتهي بـ gmail.com @ أو mail.ru @ أو أي نظام أساسي آخر للبريد الإلكتروني مصمم لعامة الناس .

الروابط المضمنة التي تأخذك عند النقر عليها إلى مواقع ويب مزيفة مصنفة ببرامج ضارة، لا تنقري أبدًا على الروابط دون التحقق أولاً من المكان الذي تأخذك إليه. يمكنك رؤية عنوان موقع الويب بالكامل عن طريق تمرير مؤشر الماوس فوق ارتباط. قبل النقر فوق الارتباط الذي تجدينه مريبًا إلى حد ما .

قواعد نحوية أو لغة غريبة. غالبًا ما يستهدف المحتالون الذين يستخدمون رسائل البريد الإلكتروني الجماعية لتنفيذ هجمات التصيد الاحتيالي الأشخاص في عشرات البلدان المختلفة. بدلاً من الاستثمار في ترجمة رسائلهم وتخصيصها لاستهداف الجمهور المحلي بشكل أفضل ، يستخدمون خدمات الترجمة المجانية عبر الإنترنت. نتيجة لذلك ، غالبًا ما تستخدم رسائل التصيد الاحتيالي لغة غير طبيعية أو غريبة بشكل واضح وتحتوي على أخطاء نحوية.

تحية عامة بدلا من اسمك، عندما تبدأ رسالة بريد إلكتروني بتحية عامة مثل "عزيزي العميل" أو "عزيزي صاحب الحساب" أو "عزيزي العضو" ، فإن هذا من شأنه أن يجعلك تشعر بالريبة على الفور، غالبًا ما تعرف المنظمات الشرعية التي تتصل بك اسمك.

C. الحماية ضد الفيروسات والبرمجيات الخبيثة

من أكثر الطرق شيوعًا التي يتسبب بها المخترقون والمجرمون في حدوث مشكلات عبر الإنترنت عن طريق نشر البرامج الضارة، لذا اتبعي هذه الإرشادات الأساسية لحماية نفسك من البرامج الضارة بالإضافة إلى استخدام المنطق السليم في التفكير سوف تقي نفسك الكثير.

استخدامي برامج مكافحة الفيروسات

يجب أن يكون لديك دائمًا برنامج لمكافحة الفيروسات يعمل على جميع الأجهزة التي تستخدمها. هذا البرنامج هو خط دفاعك الرئيسي ضد الفيروسات وأنواع أخرى من البرامج الضارة.
تأكدي من تحديث برنامج مكافحة الفيروسات لديك دائمًا حتى يتمكن من التعامل مع أي تهديدات أمنية جديدة تسمح لك برامج مكافحة الفيروسات بفحص جهازك بالكامل بحثًا عن البرامج الضارة اجعلي من المعتاد إجراء عمليات فحص منتظمة لأجهزتك لاكتشاف البرامج الضارة مبكرًا ومنعها من الانتشار، إذا كنت بحاجة إلى تنزيل شيء ما، فتأكدي من استخدام برنامج مكافحة فيروسات لفحص التنزيل بحثًا عن البرامج الضارة قبل فتحه .

يأتي Windows مزودًا ببرنامج مكافحة فيروسات مجاني وموثوق به Microsoft Defender مدمج، يمكنك الحصول عليه لحماية جهازك بشكل أفضل من خلال ضبط بعض الإعدادات.

حافظي على تحديث برامجك وأجهزتك

تصيب البرامج الضارة أجهزتك من خلال البحث عن الثغرات الأمنية في البرامج واستغلالها. يبحث المتسللون والمجرمون باستمرار عن نقاط الضعف هذه، تقوم الشركات التي تنشئ برامج بإصلاح الثغرات الأمنية من خلال تصحيحات الأمان التي تم إصدارها في التحديثات لذلك ، من المهم تثبيت التحديثات بمجرد توفرها .
أيًا كان الجهاز الذي تستخدمينه ، تأكد من أنك تستخدمين أحدث إصدار من نظام التشغيل. من الجيد ضبط نظام التشغيل وبرامج مكافحة الفيروسات على التحديث تلقائيًا، قومي بتحديث بقية البرامج الموجودة على أجهزتك بشكل متكرر وبشكل منتظم.
إذا لم تكن هناك تحديثات لنظام التشغيل على هاتفك المحمول تم تقديمها خلال الأشهر الستة الماضية، فمن المحتمل جدًا أن يكون هذا الطراز قديمًا لم تعد الشركة المصنعة تدعمه، في هذه الحالة، ضعي في اعتبارك استبدال الهاتف بطراز جديد يحصل على تحديثات أمنية مهمة.

استخدمي حساب غير رئيسي

يمكن أن تكون البرامج الضارة مدمرة بشكل خاص لجهازك والبيانات الموجودة عليه عندما تقوم بتسجيل الدخول إلى حساب رئيسي، من الجيد إنشاء حساب مستخدم بامتيازات محدودة على جهاز الكمبيوتر الخاص بك واستخدامه في المهام اليومية العادية، عندما تقوم بتسجيل الدخول إلى حساب بامتيازات مقيدة، يكون من الصعب جدًا على البرامج الضارة العثور على طريقة للوصول إلى جهازك وإجراء تغييرات على مستوى النظام.

تعرفي على ما تقوم بتثبيته على جهازك

يتم تجميع الكثير من البرامج الضارة مع برامج مشبوهة أو مضمنة في إصدارات مقرصنة من البرامج الشرعية، من أضمن الطرق لإصابة جهاز الكمبيوتر الخاص بك ببرامج ضارة تثبيت برامج مقرصنة (غير مرخصة) عليه، إذا كنت تحتاجين حقًا إلى برنامج معين ولكنك لا تستطيعين تحمل تكاليفه ، فضعي في اعتبارك أن هناك بدائل مجانية لجميع منتجات البرامج الرئيسية تقريبًا. قد توفر هذه البدائل وظائف محدودة ولكنها ستنجز المهمة دون جعل البرامج الضارة ميزة ثابتة لتجربتك عبر الإنترنت. عندما تسنح لك الفرصة، قومي بتنزيل التطبيقات فقط من خلال متاجر التطبيقات الرسمية، عند تثبيت شيء ما لأول مرة ولم تكوني على دراية بالتطبيق تأكدي من قراءة المراجعات لمعرفة ما إذا كان المستخدمون الآخرون قد وجدوا البرنامج جديرًا بالثقة. اجعلي من المعتاد إعادة زيارة جميع التطبيقات المثبتة على أجهزتك بشكل منتظم واحذفي التطبيقات التي لم تعودي تستخدمينها أو تثقين بها.

احذري من المرفقات

إنها إحدى قواعد السلامة الرقمية الأساسية التي لا يجب عليك مطلقًا تنزيل أو فتح المرفقات التي تصلك في رسائل البريد الإلكتروني أو رسائل الوسائط الاجتماعية أو نصوص الهاتف المحمول من أشخاص لا تعرفينهم أو لا تثقين بهم تمامًا. المخادعون والمجرمون مغرمون بشكل خاص بملفات Word و Excel و PowerPoint و PDF المصابة بالبرامج الضارة، إذا كانت رسالة بريد إلكتروني أو أي نوع آخر من الرسائل تبدو غريبة أو مريبة بالنسبة لك ، فإن أفضل طريقة للتعامل معها هي حذفها على الفور.

من الجدير بالذكر أيضًا أنه حتى الأشخاص الذين تعرفينهم وتثقين بهم يمكن أن تتعرض حسابات

بريدهم الإلكتروني للاختراق. لذلك إذا تلقيت بريدًا إلكترونيًا غير متوقع يحتوي على مرفق منهم، فمن الجيد أن تتحققي من الشخص الذي تعتقدين أنه أرسل لك البريد الإلكتروني قبل فتحه.

تحققي من الروابط قبل الضغط عليها

يجب ألا تنقري أبدًا على الروابط المرسلة من قبل أشخاص أو مؤسسات لا تعرفينها. يجب أيضًا أن تجعلي من المعتاد التعامل مع كل رابط تتلقينه باعتباره خطرًا محتملاً. عندما تتلقين تنبيهًا من زميل أو مصرفك أو خدمة الوسائط الاجتماعية التي تستخدمينها ، لا تنقري على الرابط في البريد الإلكتروني، مرري مؤشر الماوس فوق الرابط لمشاهدة عنوان موقع الويب بالكامل، يمكن أن يساعدك هذا في تحديد ما إذا كنت تريدين النقر فوق هذا الارتباط أم لا.

تحتوي الكثير من الروابط على برامج خبيثة، من شأنها أن تشكل خطرا على اجهزتنا وخصوصيتنا ومعلوماتنا، لذلك يجب التأكد من سلامة هذه الروابط قبل النقر والدخول اليها، يستخدم موقع virustotal.

خطوات التأكد من سلامة الروابط باستخدام موقع:

1. اذهبي الى موقع https://www.virustotal.com/
2. قومي بنسخ الرابط الذي تودين فحصه، لا تقومي بالنقر أو الدخول للرابط
3. اختاري الروابط URL
4. قومي بلصق الرابط في المكان المخصص له وقومي بالضغط على اشارة البحث

ويمكن أيضا فحصه باستخدام ماسح ضوئي للرابط مثل (https://safeweb.norton.com/) الذي يتيح لك إدخال عنوان لرابط مريب والتحقق منه للسلامة.

لا تثقي في الرسائل او الصفحات التي تظهر فجأة

لقد مررنا جميعًا بهذه التجربة: أنت تتصفحين الإنترنت وفجأة تظهر نافذة منبثقة تخبرك أن جهاز الكمبيوتر الخاص بك قد أصيب بالفيروس وتوصي بتنزيل بعض البرامج لحماية جهازك، لا تصدقي هذه الرسائل.

كوني حذرة مع الهارد ديسك و الفلاش ميموري

غالبًا ما تنتقل البرامج الضارة عبر أجهزة مختلفة عبر وسائط قابلة للإزالة مثل بطاقات ذاكرة ومحركات الأقراص الثابتة الخارجية وبطاقات الذاكرة المحمولة وما إلى ذلك، لا تقومي أبدًا بإدخال مثل هذا الجهاز في جهاز الكمبيوتر الخاص بك إذا كنت لا تعرفين من أين أتى. عندما يتعين عليك استخدام جهاز وسائط قابل للإزالة ومعرفة مصدره ، فمن المستحسن استخدام برنامج مكافحة فيروسات لفحص الجهاز قبل فتحه.

في النهاية

يرجو فريق سلامات ان يكون هذا الدليل افادكن وحاز على اعجابكن
بامكانكن التواصل معنا من خلال موقع سلامات الإلكتروني لإعطاء ملاحظاتكم
أو الاستفسار الالكتروني
support@salamatmena.org
نتمنى لكم سلامة رقمية دائمة وعافية متكاملة
وتذكروا دائما أن سلامتكم النفسية في إنترنت آمن

سلامات
Salamat

دليل مواجهة العنف الرقمي
لطالبات الجامعات في الأردن

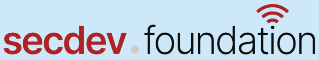
كل الشكر لكل من ساهم في اعداد وتجميع محتوى هذا الدليل

- امل ابو اسحاق
- فداء العملة
- لينا المومني
- رانيا الصرايرة
- أحمد حجاب

نفذ هذا الدليل بواسطة منظمة سيكدف – برنامج السلامة الرقمية "سلامات" بالشراكة مع مركز المعلومات والبحوث التابع لمؤسسة الملك الحسين.

قائمة المراجع التقنية:

موقع برنامج سلامات
موقع سلامتك ويكي


secdev . foundation


KING HUSSEIN FOUNDATION
مركز المعلومات والبحوث
INFORMATION AND RESEARCH CENTER