PNGO
شبكة المنظمات الأهلية الفلسطينية

دليل الأمان الرقمي للمنظمات الأهلية

2020

دليل الأمان الرقمي للمنظمات الأهلية

إصدار: شبكة المنظمات الأهلية

إعداد: شركة توبس للاستشارات والخدمات

مشروع تعزيز الديمقراطية وبناء قدرات المنظمات الاهلية الفلسطينية

بالشراكة مع المساعدات الشعبية النرويجية

2020

مقدمة

يعتبر التباعد المكاني من أهم الاحتياطات الواجب اتخاذها للحد من تفشـــــــــي فيروس كورونا في أوساط العمل، وربما أصبح العمل عن بعد بديلا في بعض الأوقات، ولذلك من الأهمية بمكان الإشارة إلى بعض الأمور التي تستوجب العناية في هذه الأوقات والتي أصبح فيها الاعتماد على البيانات والانترنت والحياة الرقمية كبيرا ومتطلبا أساسيا لاستمرار العمل.

وبالنظر إلى الحياة الرقمية والشبكات العالمية فإن التعرض لمخاطر فقدان البيانات أو سرقتها أو انتحال الشخصية والتجسس وتخطي الخصوصية أمر وارد وبالذات على العاملين في المجتمع المدني ومجالات حقوق الانســـان، فقد تفرض الجهات الحكومية حظرا الحركة والتنقل أو تفرض المراقبة والمتابعة الفردية بدعوى مراقبة العدوى ومنع انتشارها، وقد تستغل بعض الشركات هذه الأزمة لتزيد من نشاطها التسويقي عن طريق الحصول على بيانات المواطنين والعديد من المخاطر التي تؤدي بالنهاية إلى خسارة للأفراد والمؤسسات.
لذلك في إطار جهود شبكة المنظمات الأهلية الفلســـــــطينية الرامية لتنمية قدرات المنظمات الأهلية وفقا لأسس ومبادئ الديمقراطية والشـــفافية والإدارة الرشيدة وتعزيز المشاركة المجتمعية، تصدر الشبكة هذا الدليل الإرشادي والإجرائي حول الحماية الرقمية والأمن الرقمي في المنظمات الأهلية الفلســـطينية، حيث تم الأخذ بعين الاعتبار السياق الفلســـطيني، والمفاهيم الخاصة بالحماية الرقمية، بالإضافة إلى الإطار الإجرائي للعمل في المنظمات الأهلية.

لقد تم إصدار هذا الدليل ضمن مشـــروع «تعزيز الديمقراطية وبناء قدرات المنظمات الأهلية»، والذي تنفذه الشـــبكة بالشـــراكة مع المساعدات الشعبية النرويجية. إن تطوير هذا الدليل هو حصيلة لجهد أشرفت عليه الشبكة أخذا بعين الاعتبار تجربة منظمات المجتمع المدني واحتياجاتها، واحتياج وملاحظات الموظفين أنفسهم بالإضافة إلى الاستعانة بخبرات وتجارب ذوي الاختصاص في هذا المجال، ليشكل أداة تساهم في نظم الحماية الرقمية لدى المنظمات الأهلية الفلسطينية والذي تلقائيا ينعكس إيجابا على أداء هذه المنظمات الأهلية.

وتنتهز الشبكة هذه الفرصة للتقدم بجزيل الشكر للمساعدات الشعبية النرويجية على دعمها وشراكتها والتي من خلالها تم إصدار هذا الدليل. كما تتقدم بالشكر والتقدير إلى الاستشاري م. محمد أبو كميل وأ. ساجي عبيد على تعاونهما وجهدهما في إعداد الدليل. كما تتقدم الشبكة بالشكر لكافة المؤسسات والخبراء على مشاركتهم الفعالة في الجلسات وورش العمل المختلفة وملاحظاتهم القيمة التي ساهمت بشكل كبير في تطوير هذا الدليل وإصداره

شبكة المنظمات الأهلية الفلسطينية

2020

حول هذا الدليل:

في العصر الحالي أصبحت التكنولوجيا متشابكة جدًا مع حياتنا، من الصعب تخيل الحياة بدونها، الحياة كلها بجميع جوانبها بما في ذلك العمل.
البرامج والتطبيقات المرتبطة بها ومكالمات الفيديو والسُحب (مساحة تخزينية على الانترنت) ورسائل البريد الإلكتروني والخوادم والحسابات المختلفة احتلت جزءاً كبيرا من عملنا، خصـــوصًا في تلك الظروف التي أجبرتنا على العمل عن بعد، أمرٌ محمود، قد يتحول لغير ذلك إن لم نتعامل معه بحذر!

لماذا هذا الدليل:

المنظمات الأهلية مستهدفة!
كل نوع من البرامج أو المشـاريع التي تنفذها منظماتنا قد تكون مسـتهدفة من قبل أحدهم. كما أن هناك برامج قد تكون أكثر حسـاسية ومدعاة للابتزاز أو الاحتيال أو عرضة للتهديدات. حملات المناصرة وبرامج حقوق الإنسـان مسـتهدفة أيضـا من قبل مجموعات قد تسـعى إلى الإضرار بالمنظمة أو العاملين بها، كذلك المعلومات عن المستفيدين والموظفين مطمع للكثيرين. مشاريع التنمية هي أيضا عرضة للفساد حتى داخليا!

أيها الزملاء، إذا كانت التكنولوجيا عامل تمكين قوي، فمن الأهمية بمكان التفكير في الجانب الآخر، إن لم نهتم جيدًا فيمكن لهذه القوة أن تضـــع أنفسنا ومنظماتنا في خطر.
لذا، في دليلنا هذا نقدم مجموعة من النصـــــائح الأساسية للمنظمات الأهلية لحمايتها وحماية بياناتها وموظفيها من المتطفلين والقراصنة الرقميين.

الفهرس

الباب الأول

الإطار النظري

أولاً: أمن البيانات:

نقصد به حماية البيانات الخاصة بنا وبمؤسساتنا من أي قوة مدمرة أو من أي فعل غير مرغوب به من قبل مستخدمين غير مخولين.

الأمان الرقمي

يشير مصطلح "الأمان الرقمي" إلى: كل تلك الطرق المختلفة والمتعددة التي تكون غايتها هي حماية حسابات الإنترنت المتعلقة في الحاسب الآلي وحماية الملفات من التسلل أو التدخل والتطفل من قبل مستخدمين خارجيين (غير مصرحين). وقد يطلق عليه "الأمن السيبراني" نسبة لكلمة Cyber التي تعني العالم الرقمي بعمومه.

الفيروس

في العالم الرقمي الفايروس هو نوع من البرامج الضارة يهدف إلى إتلاف المعلومات الموجودة على جهاز الحاسوب أو محوها أو تعديلها قبل نشرها للآخرين.

حصان طروادة

أحد المصطلحات المنتشرة في عالم الأمان الرقمي، وهو نوع من البرامج الضارة يتخفى غالبًا في صورة برنامج شرعي، ويمكن أن يستخدم المجرمون الإلكترونيون والمتطفلون أحصنة طروادة في محاولتهم للوصول إلى أنظمة المستخدمين، وتسمح أحصنة طروادة بمجرد تنشيطها للمجرمين الإلكترونيين بالتجسس عليك وسرقة بياناتك الحساسة والتسلل إلى نظامك.

فايروس برنامج الفدية

هو نوع من الفيروسات التي تصيب الأجهزة, يمنع المستخدم من الوصول إلى نظام التشغيل، ويشفر جميع البيانات المخزنة, بهدف ابتزاز أصحاب البيانات وطلب فدية مالية مقابل اعادتها.

التشفير

في العالم الرقمي، التشـــفير هو تحويل البيانات من شكل قابل للقراءة إلى شكل مُرمَّز لا يمكن قراءته أو معالجته إلا بعد فك تشـــفيره، وهو وحدة البناء الأساسية في أمن البيانات وهو أبسط الطرق وأهمها لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من قبل دخيل.

المعلومات في كافة المجالات، لذلك هناك ضغط واضح من كافة شرائح المجتمع على المؤسسـات والهيئات لتحسـين خدماتها واتاحتها على كافة القنوات الرقمية.

أهمية التشفير

حول أهمية التشـفير يقول مارتن كليبمان –مهندس في منصـة التواصل الاجتماعي المهنية لينكد إن–: "رغم أنّ التشـفير خلال البث منتشـر الاستخدام، إلّا أنّ به مشاكل أمنيّة جديّة. مثلاً، قد يتم تهكير مزوّد الانترنت من قبل خصم له، أو من قبل أحد العاملين في الشّركة، ممّا يتسبّب في تسرّب معلومات حسّاسة. قد يتسبّب خلل لدى مقدّم خدمة الانترنت في إفساد البيانات. لهذه الأسباب، يشجّع خبراء الأمن الرّقمي استخدام التّشفير من طرف لطرف للتّخفيف من أثار التعرض لهذه الهجمات."

الحقوق الرقمية

يصف المصطلح الحقوق التي تسمح للفرد بالوصول إلى العالم الرقمي واستخدامه وإنشائه ونشره أو الوصول إلى أجهزة الحاسوب وغيرها من الأجهزة الإلكترونية أو شبكات الاتصـــال واستخدامها. ويتعلق هذا المصـــطلح بشـــكل خاص بحماية وإعمال الحقوق الموجودة، مثل الحق في الســـرية أو حرية التعبير في سياق التقنيات الرقمية الجديدة، وخصـــوصًا شبكة الإنترنت، ويتم اعتبار الوصول إلى شبكة الإنترنت حقًا تكفله قوانين الدول المتعددة.

ثانياً: المؤسسات والتحول الرقمي:

التحول الرقمي

يُعـرف التحول الـرقمي بأنه عملية انتقال القطاعات الحكومية أو غير الحكومية إلى نموذج عمل يعتمد علـى التقنيات الـرقمية في انجاز مهامها وتوفير قنوات جديدة لها.

مزايا التحول الرقمي

التحول الرقمي له فوائد عديدة ومتنوعة تشـــمل القطاع غير الحكومي والمنظمات الأهلية، منها أنه يوفر التكلفة والجهد بشـــكل كبير ويُحســـن الكفاءة التشـغيلية وينظمها، ويعمل على تحسين الجودة وتبسيط الإجراءات للحصول على الخدمات المقدمة للمستفيدين، كما يخلق فرص لتقديم خدمات مبتكرة وإبداعية بعيداً عن الطرق التقليدية في تقديم الخدمات ويساعد التحول الرقمي المؤسسات غير الحكومية على التوسع والانتشار في نطاق أوسع والوصول إلى شريحة أكبر من المستفيدين والجمهور.

التحول الرقمي ضرورة في تحسين كفاءة المؤسسات

أصبح التحول الرقمي من الضروريات بالنسبة لكافة المؤسسات والهيئات التي تسعى إلى التطوير وتحسين خدماتها وتسهيل وصولها للمستفيدين، والتحول الرقمي لا يعني فقط تطبيق التكنولوجيا داخل المؤسسة بل هو برنامج شامل كامل يمس المؤسسة ويمس طريقة وأسلوب عملها داخلياً بشكل رئيسي-وخارجياً وأيضا من خلال تقديم الخدمات للجمهور المستهدف لجعل الخدمات تتم بشكل أسهل وأسرع. كما أن التحول الرقمي يسهم في ربط القطاعات والمنظمات ببعضها بحيث يمكن انجاز الأعمال المشتركة بمرونة وانسجام عال، وقد أصبحت الضرورة ملحة أكثر مما مضى-لتحول المؤسسة رقمياً، ويعود ذلك وبشكل أساسي إلى التطور المتسارع في استخدام وسائل وأدوات تكنولوجيا المعلومات في كافة المجالات، لذلك هناك ضغط واضح من كافة شرائح المجتمع على المؤسسات والهيئات لتحسين خدماتها واتاحتها على كافة القنوات الرقمية.

تطبيق التحول الرقمي

يتم تطبيق التحول الرقمي عبر مزيج يشمل التقنيات والبيانات والموارد البشرية والعمليات، حسب التفصيل التالي:

التقنيات:

حيث يتم بناء التحول الرقمي باستخدام منظومة من الأجهزة، وأنظمة التشغيل، ووسائط التخزين، والبرمجيات التي تعمل ضمن بيئات تقنية ومراكز معلومات تسمح باستخدام جميع الأصول بكفاءة تشغيلية غير منقطعة ومستقرة، كما يستلزم ضمان مستوى خدمة مناسب لأفراد المؤسسة وعملائها وموردیها عبر فرق مهنية مسؤولة عن إدارة المنظومة التقنية والبنية التحتية للشبكة سواء أكانت هذه المنظومة محلية أو سحابية.

البيانات

يفترض أن تقوم المؤسسات بجهود إدارة وتحليل البيانات بشكل منتظم وفعال وذلك لتوفير معلومات وإجراءات نوعية موثوقة وكاملة مع توفير وتطوير أدوات مناسبة للتحليل الإحصائي والبحث عن البيانات والتنبؤ بالمستقبل، كما يجب متابعة البيانات بشكل مستمر لضمان استمرار تدفقها والاستفادة منها بشكل يتماشى مع أهداف المؤسسة وتوقعاتها.

الموارد البشرية

تُشكل الموارد البشرية جانبًا حيوياً يصعب على المؤسسات تطبيق التحول الرقمي بدونه، إذ يتوجب توفير كوادر مؤهلة قادرة على استخدام البيانات وتحليلها لاتخاذ قرارات فعالة، كما يتطلب تخطيط الرؤى وتنفيذها كفاءات بشرية وخبرات علمية وعملية مع إيمان بالتغيير والتطوير.

العمليات

وهي عبارة عن مجموعة من النشاطات أو المهام المرتبة والمترابطة التي تنتج خدمة معينة أو منتجا معين للمستفيدين. يجب على المؤسسات إرساء بناء تقني فعال يسمح بتطوير العمليات على الصعيدين الداخلي والخارجي وذلك لضمان التطبيق الأمثل للتحول الرقمي، ويتضمن ذلك الموائمة الداخلية والخارجية في إنجازات العمليات مع وجود رقابة في إنجاز العمليات والذي يعتبر أحد المفاتيح الرئيسية في المدخلات والمخرجات للمنظمة.

ثالثاً: التقنيات الرقمية التي تستخدمها المنظمات الأهلية:

التقنية الرقمية:

هي التقنية (الوسائل والأساليب) التي تعتمد على أجهزة ومعدات التي تعمل بالنظام الثنائي (٠-١) لتمثيل البيانات، مثل الحاسوب والأجهزة الذكية الأخرى التي تعتمد على برمجيات خاصة.

التقنيات الرقمية التي تستخدمها المنظمات لتيسير أعمالها ومشاريعها

- تقنيات التواصل بين الموظفين ومشاركة البيانات.
- تقنيات تساعد في تطوير وتنفيذ ومراقبة البرامج والمشاريع.
- تقنيات للربط بين القائمين على البرنامج، المجتمع، والمتبرعين.
- تقنيات للتأكد من سلامة وأمن الموظفين وأصول المنظمة وكذلك مصداقية المعلومات.

رابعاً: تقييم المخاطر الرقمية:

فهم المخاطر الرقمية التي قد تتعرض لها المنظمة والعاملين فيها وبرامجها مهمة معقدة وصعبة، خصوصًا وأنها تتطور باستمرار. بالعادة تُسند هذه الوظيفة إلى قسم تكنولوجيا المعلومات في المنظمة، أو لعضو مدرب من الموظفين. مع ذلك، فإن العديد من الحوادث الرقمية ليست بسبب عيوب فنية أو تقنية لدى المؤسسة أو أجهزتها وأدواتها، لكن بسبب "سوء السلوك الرقمي" من الموظفين والعاملين.

لذلك يتطلب الأمن الرقمي تطوير إجراءات تشغيل معيارية وسياسات فعالة لتوجيه الموظفين والعاملين أثناء استخدامهم للتكنولوجيا.

الهندسة الاجتماعية

استخدام الخداع والحيل للتلاعب بالأفراد من أجل الكشف عن معلوماتهم الرسمية أو الشخصية والتي يمكن استخدامها لأغراض احتيالية.

خامساً: التهديدات الرقمية:

في الوقت الحاضر، هناك مجموعة متنوعة من التهديدات الرقمية، والتي يمكن أن تؤثر على المنظمة وكذلك العاملين لديها منها:

١-تهديدات قد تتعرض لها المنظمة:

- قرصنة الملفات
- الإضرار بالسمعة والتشهير
- مراقبة الاتصالات أو التجسس
- الاحتيال / السرقة المالية
- التضليل / الأخبار الكاذبة
- سرقة البيانات الخاصة بالموظفين أو المستفيدين

٢-تهديدات قد يتعرض لها الموظفون:

- الابتزاز
- تتبع الحركة
- الاحتيال / السرقة المالية
- سرقة البيانات الشخصية

تأتي التهديدات عبر الإنترنت عادةً على أحد الشكلين:

- **الهجمات المباشرة:** الهجمات التي تستهدف فرد أو منظمة من أجل غرض محدد.

ومن الأمثلة على ذلك "هجوم القوة العمياء" **Brute Force Attack** وهو يشير إلى عمليات الهجوم بطريقة التخمين التي يتم الاعتماد عليها لمحاولة استحصال معلومات معينة كاسم المستخدم وكلمة السر أو الرقم التعريفي الشخصي **PIN** عن طريقة تخمين مجموعه من الاحتمالات المتوقعة أو إيجاد صفحات أو روابط مواقع الويب مخفية وكذلك إيجاد المفتاح لفك شفرات الرسائل والبيانات، وذلك من خلال تطبيقات وبرامج خاصة تقوم بعمليات التخمين وفقًا لآلية خاصة.

- **الهجمات غير المباشرة:** الهجمات واسعة النطاق التي غالباً ما تتخذ شكل عمليات الاحتيال أو محاولات التصيد الاحتيالي، والتي قد لا تستهدف بشكل مباشر منظمة بعينها أو موظف بعينه. من الأمثلة عليها: التصيد الاحتيالي (**Phishing** رسائل البريد الإلكتروني الاحتيالية المقنعة على أنها من كيان جدير بالثقة، والذي يطلب من المتلقي القيام بإجراءات معينة مثل النقر فوق الروابط أو فتح المرفقات)

الباب الثاني

الإطار الاجرائي

أولاً: السياسات والمبادئ:

سياسة الأمان الرقمي أمر لا بد منه لجميع المنظمات، بغض النظر عن الحجم، فهي تُخبر الموظفين بالمبادئ والأساليب والمسؤوليات التي يجب أن يراعوها أثناء تعاملهم مع العالم الرقمي الخاص بالمنظمة وعملها، وتضمن أن يتصرف الموظفون بطريقة مناسبة.

كذلك ستكون السياسة الأمنية للمنظمة حجر الأساس لإدارة المخاطر الأمنية التي قد تواجهها، والأدوار والمسؤوليات التي يتحملها الموظفون في إدارة هذه المخاطر.

> "لايزال الشعور الزائف بالأمان سائدًا وهو أحد الأسباب الرئيسية وراء نجاح مجرمي الإنترنت في هجماتهم. إنهم يعلمون أن معظم المؤسسات ربما أنفقت الأموال على أساسيات الأمان الرقمي، لذا فهم ببساطة يستهدفون الحلقة الأضعف وهي "العاملين"."

تطوير سياسة أمنية:

تتمحور معظم سياسات الأمان حول أربعة أقسام رئيسية:

١. بيان حول أهمية أمن بيانات المنظمة وسلامة العاملين بها، ونطاق السياسة ومن تنطبق عليه.

٢. قسم "المبادئ" الذي يشرح المبادئ الرئيسية التي تشكل نهج المنظمة لأمن الموظفين وسلامتهم وأمن برامج وبيانات المنظمة.

٣. قسم "المسؤوليات" الذي يحدد هيكل إدارة المخاطر الأمنية في المنظمة والأدوار والإجراءات المخصصة لمواقع محددة.

٤. قسم "الحد الأدنى من متطلبات الأمان" يحدد متطلبات الأمان التنظيمي المحددة التي يجب أن تكون موجودة.

ثانيًا: تدقيق الأمان الرقمي للمنظمات:

تتمثل الخطوة الأولى نحو بيئة رقمية آمنة في منظمتنا، في اكتشاف الثغرات الموجودة وإيجاد أفضل الحلول للتعامل معها، وهنا يأتي دور "تدقيق الأمان الرقمي" والذي يستند على معايير وإرشادات وإجراءات ذلك الأمان، فضلاً عن تنفيذ هذه الضوابط.

دعونا نراقب منظمتنا، ونملأ قائمة الفحص **Check List** التالية:

الأمـن الفيزيائي (المادي)	لدى المؤسسة سياسات لتقييد الوصول المادي إلى الخوادم أو أنظمة المعلومات الإلكترونية؟	☒
	لدى المؤسسة ضوابط مثل أقفال الأبواب وأنظمة التحكم في الوصول ومراقبة الفيديو؟	☒
	يتم التحكم في الوصول إلى المكتب إما عن طريق الأمن أو مكتب الاستقبال، وسجل الدخول، وشارات الدخول؟	☒
	أجهزة الحاسوب والأنظمة الأخرى مؤمنة فعليًا (يصعب وصول الدخلاء إليها واستخدامها)؟	☒
أمن البنية التحتية لتكنولوجيا المعلومات	تم شراء جميع أنظمة التشغيل المستخدمة على أجهزة كمبيوتر المؤسسة (Windows مثلًا) رسميًا؟	☒
	تحتوي جميع الأجهزة على برنامج مضاد للفيروسات تم شراؤه رسميًا؟	☒
إدارة أمن البرامج	تمتلك المؤسسة سحابة تخزين خاصة تتجدد سنويا؟	☒
	يوجد تحديث دوري ورسمي لكافة البرامج المستخدمة بإشراف متخصص؟	☒
	تمتلك المؤسسة نظام إدارة معلومات ممتاز خاص بها؟	☒
الأمن السيبراني	• هل تستخدم مدير كلمات المرور؟	☒
	• هل تستخدم فقط البرامج والتطبيقات وملحقات المستعرض الشرعية من مصادر موثوقة؟	☒
	• هل يتم قفل الأجهزة تلقائيًا عند تركها دون رقابة؟	☒
	• هل استخدام USB ومحركات الأقراص الصلبة الخارجية من مصادر غير مألوفة مقيد؟	☒
	لدى المؤسسة ضوابط مثل أقفال الأبواب وأنظمة التحكم في الوصول ومراقبة الفيديو؟	☒
	• هل لديك نسخ احتياطية مجدولة يوميًا لجميع الملفات والبيانات الهامة؟	☒
	• هل لديك خطة التعافي من الكوارث واستمرارية الأعمال؟	☒

الأمن السيبراني	• هل لديك سياسة استخدام مقبولة تغطي استخدام أجهزة الكمبيوتر والأجهزة المحمولة وموارد تكنولوجيا المعلومات الأخرى بالإضافة إلى أدوات الوسائط الاجتماعية؟	☒
	• هل تراجع الأذونات بانتظام للوصول إلى المجلدات والأنظمة والتطبيقات المشتركة وإزالة الأشخاص الذين لم يعودوا بحاجة إلى الوصول؟	☒
	• هل لديك إجراء قياسي لعزل الآلات المصابة وتنظيفها؟	☒
	• هل تجري بانتظام عمليات تدقيق في عمليات التصيد واختبارات الاختراق؟	☒
	• هل تحتفظ بالأسئلة الشائعة حول سياسات تكنولوجيا المعلومات والأمن الخاصة بالشركة؟	☒
	• هل لديك نسخ احتياطية مجدولة يوميًا لجميع الملفات والبيانات الهامة؟	☒
	• هل يمكنك مسح الأجهزة المحمولة عن بُعد في حالة فقدها أو سرقتها؟	☒

بعد مراجعتنا للـ **Check List** السابق، دعونا ننتبه أننا بحاجة لتصويب أي خلل أو نقص لدى مؤسستنا في اجراءات الأمان المذكورة على النحو التالي:

-الأمن الفيزيائي (المادي): يجب على المؤسسة حماية أجهزتها الرقمية من أي وصول غريب لها بشكل مادي.

-أمن البنية التحتية للمؤسسة: يجب على المؤسسة تأمين بنيتها الرقمية التحتية، جميع البرامج وأنظمة التشغيل (مثل نظام ويندوز) المستخدمة يجب أن تكون مدفوعة تم شراءها بطريقة رسمية. استخدام النسخ المسروقة والمعدلة من البرامج بشكل غيررسمي، قد يشكل خطرًا أمنيا على المؤسسة, فمثل تلك البرامج قد تكون ملغومة من قراصنة العالم الرقمي.

-الأمن السيبراني: ينبغي أن يكون لدى المؤسسة من هو متفرغ لمتابعة اجراءات الأمان الخاصة بالعالم الرقمي لها، ويتابع بشكل دوري البرامج والمعدات والاجهزة الرقمية المستخدمة في المؤسسة.

مدير كلمات المرور:
هو تطبيق برمجي يساعد في حفظ كلمات السر الخاصة بك والمستخدمة في أماكن مختلفة، وعادةً ما يقوم التطبيق بتخزينها في قاعدة بيانات مشفرة.

ثالثاً: اجراءات وممارسات للحماية الشخصية والمؤسساتية:

أصدقائي العاملين في المنظمات والمؤسســـات، أخصُ من يباشر استخدام أدوات ووسائل العالم الرقمي منكم، يقع على عاتقكم مســـؤوليات كبيرة, انتبه لا تكن أنت الثغرة التي تُؤتى مؤسستك منها.

أذكرلكم هنا مجموعة من الممارسات والإجراءات، أرجو الانتباه لها لحماية أنفسكم ومؤسساتكم وبياناتها.

رابعاً: الربط الآمن بين المكاتب والمستفيدين والشركاء:

لضـــمان عمل آمن لمؤسســـاتنا ولبياناتنا وبيانات المســـتفيدين، خصـــوصًا في حالات العمل عن بعد، لابد أن نراعي مجموعة من الإجراءات والممارسات:

١- استخدام شبكة الاتصال الخاصة الافتراضية: Virtual Private Network (VPN)

شبكة الاتصـــال الخاصة الافتراضية **(VPN)** عبارة عن شبكة اتصـــال خاصة يتم إنشـــاؤها ضمن البنية التحتية لشـــبكة عامة، مثل شبكة الإنترنت العالمية، ويمكن للمؤسسات استخدام شبكة **VPN** في إنشاء اتصال آمن بالمكاتب البعيدة والمستخدمين البعيدين من خلال الوصول إلى الإنترنت عبرجهة خارجية بتكلفة معقولة.

وتوفِّرشبكة الاتصـــال الخاصة الافتراضية أعلى مســـتوى ممكن للأمن من خلال تقنيات المصـــادقة ومســـارات شبكة **VPN** المرتكزة على أمن بروتوكول الإنترنت **(IPsec)** المشـــفَّرأو على طبقة مآخذ التوصيل الآمنة **(SSL)** وتعمل كل هذه التقنيات على حماية البيانات المنقولة عبر شبكات **VPN** من الوصول غيرالمرخَّص به.

ويمكن للمؤسســـات الاستفادة من بنية الإنترنت التحتية سهلة التوفيرلشـــبكات **VPN** في إضافة مواقع أو مســـتخدمين جدد على نحوٍ سريع. وإلى جانب ذلك، يمكنها أيضًا زيادة الوصول إلى شبكات **VPN** دون الحاجة إلى استثمار كبيرفي توسيع البنية التحتية.

٢- الاجتماعات الرقمية (الافتراضية) الآمنة:

سرية الاجتماعات بين العاملين ببعضـــهم وكذلك بين العاملين والمســـتفيدين من جهة أخرى، تعتبرمن أهم أولويات المؤسســـات والمنظمات، الأمرالذي أصبح أكثرتهديدًا مع انتقاله للعالم الرقمي خصوصًا في تلك الحالات والظروف التي تستدعي ذلك.

دعونا نتحدث أكثرعن الاجتماعات الرقمية، وكيف نُعِد اجتماعًا رقميا آمنًا.

في البداية يجب أن نهتم جيدًا في اختيار أداة جيدة لذلك تكن أكثرأمانًا، يجب أن نبحث عن الأدوات التي تعتمد أنظمة تشـــفيروأنظمة أمان أكثر تعقيدًا.

منصة Jitsi

منصة بسيطة وامنة للاجتماعات الافتراضية ينصح بها الكثيرون:

منصة Jitsi هي منصة اجتماعات فيديو مشفرومجاني. تقوم بتشفيراتصالك قبل أن يغادرجهازك. منصة Jitsi تحمي مستخدميها من أخطارالمراقبة والتدخل في المكالمات وإساءة استخدام المعلومات الخاصة بالمشاركين.

> كجهة مختصة بحماية العاملين في مجال حقوق الانسان، نصحت منظمة frontline defenders الجميع باستخدام منصة Jitsi في عملهم واجتماعاتهم، ذكرت ذلك في دليلها الخاص الموجه لفئتها المستهدفة.

مزايا منصة Jitsi

- الاتصال والبيانات مشفرة
- المجهولية "لا يوجد حاجة إنشاء حساب أو إدخال أية معلومات شخصية إجراء محادث"
- يمكن إجراء المحادثة أو الاجتماع عبرمتصفح الإنترنت بدون الحاجة لتنصيب التطبيق على الجهاز يمكن تنصيب تطبيق "جيتسي" على أجهزة الكمبيوترأو هواتف أندرويد و IOS"
- عند إنشاء غرفة محادثة، يكفي ارسال رابط المحادثة لأي شخص، للانضمام إلى المحادثة.

خطوات العمل على Jitsi

- عبرمتصفح الإنترنت، ندخل إلى موقع المنصة https://meet.jit.si
- نقوم بانشاء اسم لـ"غرفة المحادثة" التي نريد إنشاءها.
- نضغط على خيار "GO"
- نضغط على "Allow"
- أنت الآن في غرفة المحادثة
- خيارات وأدوات غرفة المحادثة
- خيار "Set your display name" لاختياراسمك كماتريدين\ترين عرضه في غرفة المحادثة.
- خيار "Start / Stop screen sharing" لمشاركة وإيقاف مشاركة الشاشة مع الآخرين.
- خيار "Raise / Lower your hand" عادة، يتم استخدامه لطلب الإذن للتحدث.
- خيار "Open / Close chat" إجراء محادثة نصية بين جميع المتصلات والمتصلين وعند إغلاق\مغادرة جميع المشاركات والمشاركين المحادثة، يتم بشكل تلقائي حذف المحادثة.

خيار "Mute / Unmute" للتحكم بإقفال وتفعيل الميكروفون.

- خيار "Leave" إنهاء المحادثة.
- خيار "Start / Stop camera" للتحكم بتشغيل وإيقاف تشغيل الكاميرا.
- خيار "View and invite members" لإظهار الأشخاص الموجودين داخل غرفة المحادثة.
- خيار : "" "Share link" للحصول على رابط غرفة المحادثة وانشاء كلمة سر لغرفة المحادثة.

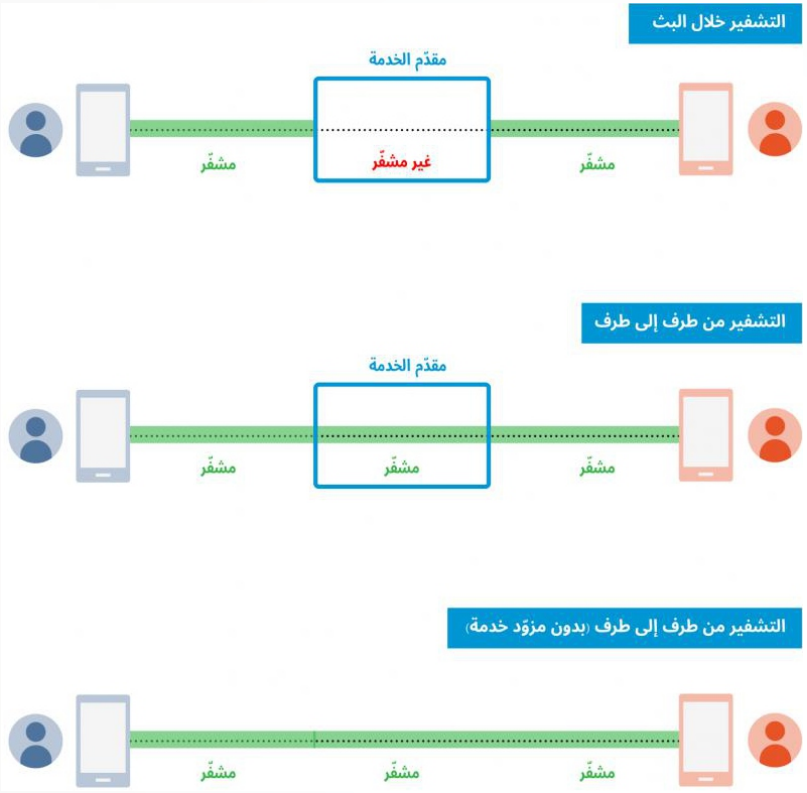
٣- المراسلات الرقمية الآمنة، وخصوصية المستفيدين

في كثير من برامج منظماتنا ومشاريعها نكون بحاجة لإجراء مراسلات مع المستفيدين أو العملاء، وبالعادة قد تتناول المراسلات بيانات حساسة قد تشكل انتهاكاً لخصوصياتهم لو تسربت.

هنا نتكلم عن أفضل تطبيقات المراسلة المشفّرة وعن آلية عملها وحمايتها للبيانات بطريقة التشفير.

٣,١- التشفير من طرف لطرف

التشفير من طرف إلى طرف يعني تعمية الاتصالات والمراسلات لجعلها غير متاحة لأطراف ثالثة. عندما يتواصل جهازين أو أكثر عن طريق تطبيق بهذا المستوى من التشفير، يتم نقل المعلومات باستخدام شيفرة سريّة وليس عبر نصّ بسيط وغير مؤمّن. حيث لا يمكن لأي شخص سوى "الطّرفين" المعنيين قراءة الرّسائل، سواء كان مزوّد خدمة الانترنت أو مطوّر التطبيق أو أي كان. تتم حماية البيانات ضد التلاعب والمراقبة والقراصنة الرقميين في مراحل بثّها وتخزينها. ويتم حفظ مفتاح التشفير محلياً لرفع مستوى الحماية.



٣,٢ - تطبيقات المراسلة الأكثر أمناً:

تطبيق Telegram

بكلماتهم: "تيليجرام برنامج مراسلة يهتم بالسرعة والخصوصية." يعتبر تيليجرام من تطبيقات المراسلة الأكثر أماناً.
يمكّن تيليجرام للمستخدمين الحريصين جدّاً على أمنهم الرّقمي تفعيل المحادثات السرية التي تكون بين طرفين فقط عبر إعدادات التّطبيق.
كما أنّ الخدمة أطلقت إمكانيّة حذف الرّسائل أو الملفّات والصور من جهازي الطّرفين. كما أنّ هناك خاصيّة التدمير الذاتي للرسائل والصور والفيديوهات بعد مدّة من الزّمن وذلك بعد رؤيتها أو فتحها من قبل الطّرف المتلقّي، حيث تختفي في الجهازين.
ويذكر بأنّ جميع المحادثات السّريّة محدّدة بأجهزة طرفي المحادثة ولا يتم تخزينها على نظام تيليجرام السّحابي، بمعنى أنّ أمن ما يخزّن عليها يرتبط بأمن أجهزة طرفي الاتصال.

تطبيق Wire

هناك تطبيق دردشة مشفّر آخر يستحق التّجربة وهو واير. التشفير من طرف لطرف فيه هو المفترض ولا يتطلّب أيّة إعدادات، بما في ذلك المحادثات والملفّات والصّور والملفّات النصيّة وغيرها.
واير منصّة مفتوحة المصدر وتشاركيّة تحوي الكثير من الميّزات الرّائعة: مثل التشفير التّام للاتصال عبر الفيديو، والتشارك الآمن للملفّات، ومزامنة تواجد الملفات على الأجهزة المختلفة. هناك نسخة مجّانيّة لاستخدام واير الخاص، وأخرى مدفوعة للمنظّمات. الأهم في واير أنّه لا يحتاج إلى رقم خلوي، بل يمكن تثبيته عبر أي بريد إلكتروني.
يعمل واير على مختلف النّظم: ويندوز، آندرويد، iOS، ماك OS، لينوكس وكذلك على المتصفّحات المختلفة
(Chrome، Firefox، Edge، Opera)

تطبيق WhatsApp

نفذّت واتساب التشفير من طرف إلى طرف عام ٢٠١٦، لمحاولة لها في تأمين اتصالات المستخدمين. ويذكر أنّ فيسبوك اشترت واتساب، الذي يستخدمه أكثر من مليار شخص. (سجّلت أكثر من ثغرة أمنيّة في التّطبيق، آخرها عبر شركة التّجسّس الإسرائيليّة "إن أس أو" التي اكتشفت أنّه عبر مكالمة واحدة -سواء تلقّاها الطرف المعني أم لا، يصبح الجهاز معرّضاً للتجسّس بما في ذلك تشغيل الميكروفون والكاميرا في أي وقت. ومنذ ذلك الوقت حلّت واتساب المشكلة مطالبةً مستخدميها بتحديث التّطبيق)

تطبيق Viber

تضمّنت النّسخة السادسة من تطبيق ڤايبر التشفير من طرف إلى آخر، بما في ذلك الملفّات والمحادثات الصّوتيّة. كما أنّ الشركة نشرت شرحاً مفصّلا باللغة الإنجليزية لكيفيّة عمل نظام التّشفير لديها، يتضمّن كيفيّة إضافة المفتاح الخاص إلى أكثر من جهاز لضمان التشفير من طرف لآخر عليها جميعاً.

تطبيق Line

بعد زلزال توهوكو المدمّر الذي حصـــــل في ٢٠١١ ، بنى مجموعة من المهندسين اليابانيين هذا التطبيق كَحل للتواصل، حيث دمّرت الفاجعة بنية الاتّصالات التّحتيّة في بلادهم، فكان الانترنت هو الطريقة الوحيدة للتواصل. بعد سنوات، أضاف **Line** التّشـفيرمن طرف إلى آخر عبرخاصيّة تُسمّى "تغليف الحروف" وهي متوفّرة لجميع مستخدمي التطبيق لكن يجب تفعيلها للاستفادة منها.

تطبيق KakaoTalk

تطبيق المحادثات الخاصّة مقرّه كوريا وهو يقوم بالتشـــفيرالتّام لجميع المحادثات منذ ٢٠١٤ . ولكن كما الحال في تيليجرام، يجب تفعيل خاصيّة "**Secret Chat**" من أجل ضمان تشفيرمحادثاتهم من طرف لطرف.

تطبيق Dust

هو تطبيق تواصل خاص آخريستخدم التّشفيرمن طرف إلى طرف كخاصيّة رئيسيّة للأمن والخصوصيّة.
تحاول دست أن تكون منصّة دردشة اجتماعيّة بمستوى عالي في الأمن والخصوصيّة.

تطبيق Threema

لا يقتصـرهذا التطبيق على التشـفيرمن طرف لآخرعلى الرسائل النصـيّة فحسـب، ولكنّه يتضـمّن المحادثات الجماعية والمكالمات الصّوتيّة وكذلك الملفّات. لا يمكن لأحد سـوى المتلقّي المعني قراءة رسـائلكم. التطبيق ليس مجّاني لكنه ليس باهظ الثمن. ويفتخرمطورو التطبيق بأنهم يحذفون الرّسائل من خوادمهم فورتلقّيها.
هناك خاصيّة للدردشة الخاصّة على **Threema** تساعد المستخدمين في حماية كل حديث عبررمزسرّي خاص به. وذلك لضمان سريّة الأحاديث.

تطبيق Wickr – Secure Messenger

تمّ تطويرهذا التطبيق من قبل مجموعة من خبراء الأمن الرّقمي ومناصري الخصوصيّة في عام ٢٠١٢ ، وهو أيضـاً مشـفّرمن طرف لآخر. التطبيق مفتوح المصدرولا يتطلّب التّسجيل، لا يتطلب إضافة رقم هاتف ولا عنوان بريد إلكتروني. وهو لا يجمع بيانات ولا يمكنه بالتالي الوصول إليها.

تطبيق Silence

هذا التطبيق مفتوح المصـــدرومجّاني. كان معروف سابقاً بـــ **SMSecure** ، وهو بســـيط وسهل الاستخدام كما يســـتخدم رسائل ال **SMS** المشفّرة دون الحاجة إلى انترنت، وهو يشفّر الرّسائل النّصيّة خلال البث وعلى الهواتف الخاصة.

تطبيق Pryvate Now

هذا التطبيق مجّاني ومتوفّر على الهواتف التي تعمل على أنظمة آندرويد أو iOS. في عام ٢٠١٥، ربح هذا التطبيق جائزة "Best Business Best Mobile App" وهو يضمن أنّ اتصالاتكم مؤمّنة ومشفّرة بشكل كامل. لا يتضمّن عمل هذا التطبيق خوادم أو وسطاء للاتصال. كما أنّ فيه ميّزة "التدمير الذّاتي" التي تمكّنكم من حذف رسائلكم في جهاز المُتلقّي في أي وقت.

خامساً: أمان أجهزة الحاسوب

تعتبر أجهزة الحاسوب التي تستخدم في عمل المنظمة، أكثر الأجهزة والمعدات التي قد تشكل خطرًا على بياناتنا وسلامتنا إن لم يتم التعامل معها بشكل صحيح. فيما يلي مجموعة من النصائح للحفاظ على أمان أجهزة الحاسوب تحدثت عنها شركة مايكروسوفت:

١- ابق على اطلاع بالتحديثات: تأكد من تلقي التحديثات التلقائية لنظام التشغيل (Windows مثلًا)، الأمر الذي سيساعد على إبقاء الأجهزة في حماية جهاز الكمبيوتر وشركتك.

٢- ثبِّت بحذر: تجنب تثبيت أي برنامج من خارج مكان عمل غير موافق عليه أو غير مُدار من قبل شركتك. بإمكان البرامج غير المصرح بها إنشاء ثغرات أمنية خطيرة.

٣- استخدم مزايا المصادقة القوية: احرص على استخدام مزايا مصادقة قوية تحمي جهازك من استخدام الغرباء له.

> استخدم Windows Hello للمصادقة: يمكنك تسجيل الدخول إلى Windows 10 بشكل أكثر أماناً باستخدام ميزة التعرف على الوجه أو بصمة الإصبع أو رقم PIN الخاص بـ Windows Hello.

٤- حافظ على قوة كلمات المرور: إذا كان عليك استخدام كلمة مرور، فاستخدم كلمة مرور قوية. تتكون كلمة المرور القوية من ١٣ حرفاً على الأقل أو أكثر وتحتوي على مجموعة من الأحرف الكبيرة والأحرف الصغيرة والأرقام والرموز. قم بتغيير كلمات المرور بشكل منتظم ولا تعيد استخدام كلمات المرور القديمة أو كلمات المرور التي تستخدمها حالياً في أماكن أخرى

٥- انقر بعناية: انتبه إلى الروابط المشبوهة. فبإمكانها أن تظهر في رسائل البريد الإلكتروني أو التغريدات أو المنشورات أو الإعلانات عبر الإنترنت أو الرسائل أو المرفقات، وفي بعض الأحيان تتخفى كمصادر معروفة وموثوقة.

٦- احذر من شبكة Wi-Fi العامة: إذا اتصلت بإحدى شبكات Wi Fi غير الآمنة باستخدام جهاز الشركة، فأنت تعرض نفسك ومنظمتك إلى الخطر.

٧- خزن بياناتك بأمان: إذا كانت شـــــركتك توفر مورداً لتخزين عملك مثل OneDrive for Business أو SharePoint، فيجب استخدام ذلك كلما أمكن بدلاً من تخزين العمل على جهاز الكمبيوتر المحلي فقط. من خلال حفظ ملفاتك في موارد الشـــركة، يمكنك أن تكون واثقاً من أنها تم نسخها احتياطياً بشكل آمن وأنها متوفرة دائماً، حتى في حالة تعرض جهازك المحلي للتلف أو السرقة.

٨- اســـتعرض الويب بأمان: تجنب زيارة المواقع التي من المحتمل أن تقدم محتوى غير مشروع. تقوم العديد من هذه المواقع بتثبيت البرامج الضارة بسرعة أو تعرض التنزيلات التي تحتوي على البرامج الضارة.

٩- راقب الرسائل الخادعة: يبحث بعض المخادعين في وسائل التواصل الاجتماعي عن معلومات وظيفية ويرسلون رسائل بريد إلكتروني يبدو أنها حول معاملات متعلقة بالعمل. كن حذراً عند الاســـتجابة أو الرد على الاتصـــالات غير المرغوب فيها سواء عبر البريد الإلكتروني أو الهاتف أو الرسائل النصية.

> إذا كنت تســـتخدم جهاز الحاسوب ولاحظت شيئاً غير معتاد، فقم بإعلام قسم تكنولوجيا المعلومات بمنظمتك بذلك. يساعد هذا في التأكد من بقاء شبكة المنظمة آمنة.
> إذا كنت ضحية خداع أو تم الاستحواذ على ملفاتك عن طريق برامج الفدية الضارة، فتجنب التعامل مع المخادعين مباشرة.

١٠- احم أجهزتك فعليًا: يمكن ســـرقة محركات الأقراص القابلة للإزالة والأجهزة المحمولة، بما في ذلك أجهزة الحاســـوب المحمولة والهواتف الخلوية بسهولة مع جميع البيانات الموجودة عليها. حافظ على أمان هذه الأجهزة وقم بتخزينها بشكل صحيح.

العمل من المنزل والأمان الرقمي!

كثير من الظروف قد تضـطرنا للعمل عن بعد من منازلنا، لعل أبرزها جائحة كورونا وما ألزمتنا به من عزل اجتماعي، الأمر الذي يحتم علينا الانتباه لبعض إجراءات الأمان الرقمي التي تتعلق بالعمل بهذه الصورة خصوصًا لدى الذين لم يعتادوا عليه.

إجراءات العمل عن بعد أكثر أمانًا:

- لا تسمح لأفراد العائلة باستخدام أجهزة العمل الخاصة بك. إذا كان عليك الابتعاد عن جهازك للذهاب إلى المطبخ أو الحمام، فاقفل جهازك لمنع الآخرين من رؤية ما تعمل عليه. اضغط على مفتاح شعار Windows + L على جهاز يعمل بنظام Windows، أو اضغط على Control + Command + Q على جهاز Mac لقفل الشاشة بسرعة. عند عودتك، سيتعين عليك إجراء تسجيل دخول سريع، ويجب أن يكون كل شيء في المكان الذي تركته فيه.

• استخدم فقط شبكة Wi-Fi المشـــفرة للأعمال. تعد شبكة Wi Fi المشـــفرة باستخدام WPA-2 أكثر أمانًا من شبكة Wi-Fi المفتوحة للجميع للوصول إليها. إذا كنت تعمل من المنزل، فتأكد من تأمين شبكة Wi-Fi المنزلية.

• إذا كنت بحاجة إلى الوصول إلى الموارد، مثل الخوادم لدى شركتك، فاستخدم (VPN الشبكة الافتراضية الخاصة) للاتصال بشبكة مكتبك. تنشئ VPN نفقًا مشفرًا لتدفق حركة مرور الشبكة الخاصة بك من خلاله وتجعل من الصعب على الآخرين اعتراض حركة المرور الخاصة بك. إذا لم تكن متأكدًا مما إذا كانت شركتك تقدم VPN أو كيفية الاتصال بها، فتحقق من مسؤول دعم تكنولوجيا المعلومات لديك.

• ابق على اتصال بمؤسستك أثناء العمل عن بُعد. قد يكون لدى قسم تكنولوجيا المعلومات لديك طلبات خاصة أو إتاحة أدوات جديدة لك. إذا كنت تشك في تعرض جهازك أو بياناتك للاختراق بأي شكل من الأشكال، فقم بإخطار موظفي تكنولوجيا المعلومات على الفور حتى يتمكنوا من التحقيق في الموقف واتخاذ خطوات لمنع حدوث ضرر غير ضروري.

• الآن، أكثر من أي وقت مضى، قاوم إغراء استخدام أدوات غير معتمدة أو تخزين البيانات خارج موارد الشركة. إذا كنت بحاجة إلى شيء لا تملكه لإنجاز عملك، فاطلب من قسم تكنولوجيا المعلومات لديك أو اتبع التسلسل الاداري. من الممكن تمامًا أن تكتشف أنظمة لا تعمل بشكل جيد عندما لا تكون في المكتب. الآن هو الوقت المثالي لإعلام قسم تكنولوجيا المعلومات حتى تتمكن من حل هذه المشكلات معًا.

> **نصيحة:** حتى إذا كنت لا تتصل بموارد الشركة، فإن استخدام VPN لنشاطك على الإنترنت يمكن أن يكون أكثر أمانًا.

• إذا تلقيت مكالمة هاتفية غير متوقعة من شخص لا تعرفه يدعي أنه من فريق الدعم الفني لشركتك، احصل على اسمه، ثم أغلق المكالمة واتصل بالدعم الفني لمنظمتك مباشرة.

• إذا تلقيت مكالمة هاتفية غير متوقعة من شـــخص يدعي أنه من دعم Microsoft أو Google مثلًا، فيجب عليك إنهاء المكالمة على الفور. لا يتصـــل فريق دعم الشـــركات بالعملاء مباشرةً إلا إذا اتصلت بهم لطلب الدعم.

• تعد حماية الملفات والمجلدات بكلمة مرور واحدة من أفضل الطرق لمنع الآخرين من الوصول إلى المعلومات الشخصية أو الحساسة، ويحتوي نظام التشغيل ويندوز ١٠ على أدوات تشفير مدمجة تتيح لك حماية الملفات والمجلدات وتأمينها بكلمة مرور.

تشفير الملفات على حاسوبك

يساعد تشفير الملفات على حماية بيانات مؤسستك عن طريق تشفيرها. يمكن أن يقوم شخص واحد فقط الذي يستخدم مفتاح التشفير الصحيح (مثل كلمه مرور) بفك تشفيرها.

خاصية التشفير المضمنة في ويندوز ١٠:

• اختر الملف أو المجلد الذي تريد حمايته بكلمة مرور، وانقر بزر الماوس الأيمن على الملف أو المجلد.

• من القائمة اختر (خصائص) Properties.

- في علامة تبويب (عام) General، اضغط على خيار (متقدم) Advanced.
- حدد خيار (تشفير المحتويات لتأمين البيانات) Encrypt contents to secure data.
- اضغط على زر (موافق) OK.
- انقر على (تطبيق) Apply لبدء عملية التشفير.
- ستظهر لك نافذة منبثقة تسأل عما إذا كنت تريد تشفير هذا المجلد فقط، أو المجلدات الفرعية والملفات، حدد الخيار الذي يناسبك ثم اضغط على (موافق).
- في النافذة التالية، سترى ثلاث خيارات لنسخ مفتاح التشفير احتياطيًا حتى تتمكن من استخدامه للوصول إلى ملفاتك أو مجلداتك في حالة فقد الوصول إليه، اختر (نسخ احتياطي الآن) Back up now.
- بمجرد عمل نسخة احتياطية من المفتاح سيصبح الملف أو المجلد مؤمنًا باستخدام مفتاح تشفير مرتبط بحساب مستخدم ويندوز ١٠ الخاص بك، وبهذه الطريقة، لن يرى أي شخص آخر يحاول الوصول إلى الملف أو المجلد إلا نصًا مختلطًا بدلاً من المحتويات الفعلية للملف أو المجلد، حتى إذا سجل الدخول بحساب مستخدم مختلف.

سادساً: حماية أجهزة الهاتف الذكية:

اعتمادنا الكبير على أجهزة الهاتف الذكية في جميع أمور حياتنا بما فيها العمل، جعل من الصعب فصل العمل عنها. فليس هناك من ينكر قدرتها على تحسين وتيسير إجراءات العمل.

الأمر الذي جعل التهديدات الأمنية تتزايد، خصوصًا كلما ازداد عدد المتعاملين مع الهواتف وتطبيقاتها في عمل المنظمة سواء الموظفين أو العملاء.

> بمجرد دخول المتسللين للهاتف، فإن الاحتمالات تكون كبيرة ومخيفة قد تصل لأن يملك أحدهم السيطرة الكاملة على الهاتف الذكي ويتمكن من الوصول لكل بيانات العمل التي قد تحزن عليه أو يتم تداولها عبره.

كيف نحمي أجهزة الهاتف الذكية المستخدمة في العمل؟

١- استخدام كلمة مرور قوية لشاشة الهاتف

- إنشاء كلمة مرور قوية ففي حال فشلت محاولة المتطفل إدخال كلمة المرور لعدد معين من المرات، يتم قفل الهاتف وتعطيله، وفي بعض الحالات يتم حذف كل البيانات عنه.
- قم بإنشاء أطول رمز وصول ممكن لهاتفك الذكي أو استخدم مستشعر البصمة.

٢-مراقبة الصلاحيات والأذونات التي حصت عليها التطبيقات من هاتفك

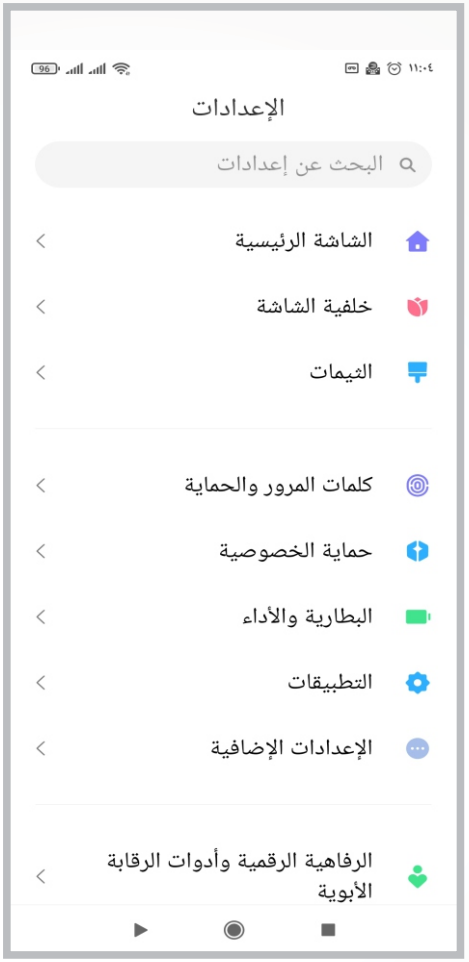
من أكثر الثغرات التي قد تمكن المتطفلين من الوصـــــــــــول لهاتفك وبياناتك واختراق أمنك وبيانات العمل التي تحفظها وتداولها عبره، هي التطبيقات، التي قد تعطيه صلاحيات للوصول لك ولبياناتك كتشغيل الكاميرا والميكروفون أو الدخول لملفاتك.

لذلك فلك النصائح التالية:

- لا تقم بتنزيل أي تطبيق قبل أن تبحث عما يجعلك تثق به (اسم الجهة المالكة للتطبيق - تقييمات وتعليقات المستخدمين - سؤال المختصين)
- اقرأ الشـــــروط بعناية قبل قبول وتنزيل التطبيق، مع رفض التطبيقات، التي تطلب حقوقا وأذونات غير ضرورية مثل الوصول إلى رسائلك أو موقعك بدون داع.
- افحص الصـــــلاحيات أو الأذونات التي يحصل عليها التطبيق من هاتفك.

كيف أعرف الصـــــلاحيات التي يحصـــــــل عليها التطبيق من هاتفي؟

- في هاتفك تـــــوجه الى الإعدادات أو الضبط
- ثم توجه إلى التطبيقات
- الآن توجه إلى مديـــــــــــر/إدارة التطبيقات
- اضـــغط على اســـم التطبيق الذي تنوي فحص الصلاحيات التي يحصل عليها
- هنا ستجد جميع الصـــــلاحيات أو الأذونات التي يحصل عليها التطبيق
- افصـــــــل أو اترك أي اذن قد تجده مناسبًا، يحق للتطبيق الحصـــول عليه دون قلق.



٣-توخّ الحذر من تطبيقات المتاجر غير المصرح بها

تجنب استخدام المتاجر البديلة، لأنها يمكن أن تحتوي على برامج ضارة. ومن الأفضل تنزيل التطبيقات فقط من App Store و Google Play.

٤-احذر من نقاط Wi-Fi الساخنة الموجودة في الأماكن العامة.

تجنب تماما استعمال الشبكات اللاسلكية العامة غير المشفرة (WLAN)، لأنه من الناحية النظرية يمكن للقراصنة اختراق الهواتف الذكية والحواسيب اللوحية والاطلاع على البيانات الخاصة بالمستخدم. لذلك ينصح خبراء التقنية بضرورة استعمال الشبكات اللاسلكية المشفرة، رغم أنه يمكن التجسس عليها أيضا من الناحية النظرية.

أما إذا لم يكن هناك بديل أمام المستخدم عن استعمال الشبكات اللاسلكية العامة المنتشرة في المقاهي والمطاعم، فعندئذ عليه استعمال خدمة الشبكة الافتراضية الخاصة "VPN" التي تحمي تدفق البيانات عن طريق تقنيات التشفير.

٥-احذر من الرسائل النصية

إن الرسائل النصية هدف سهل للبرامج الضارة التي تستهدف الأجهزة المحمولة، لذا ننصح المستخدمين بعدم إرسال البيانات الحساسة مثل تفاصيل البطاقات الائتمانية أو المعلومات الخاصة المهمة في نصوص.

سابعاً: شبكة الانترنت والتصفح الآمن

في عملنا نعتمد بشكل كبير على شبكة الانترنت والتصفح داخلها، ومهما كانت إجراءات الأمان التي قامت بها الجهة المختصة بمنظمتنا لتأمين أجهزتها من المخاطر التي قد تأتي لها من الشبكات الخارجية، إلا أنه وكما تكلمنا سابقًا، قد تكون ممارسات وسلوكيات الموظف أو العامل بالمنظمة هي الثغرة.

هنا سنتكلم في مجموعة من النصائح لتصفح آمن عبر الإنترنت.

١-استخدم متصفحًا آمنًا

المتصفح هو بوابتك الأولى لمواقع الانترنت، اختيارك أو استخدامك للمتصفح الخاطئ قد يكون السبب في تعرض أمنك للخطر.

استخدم متصفحات آمنة لشركات معروفة كـ Google Chrome وغيرها.

> **متصفح TOR**
>
> يعتبر متصفح TOR الأكثر أمانًا بفضل خصائص الأمان المدمجة به، هو إصدار محدّث ومطوّر أمنيًا من متصفح موزيلا فيرفُكس.
>
> قد يكون من سلبياته هو أن بطيء مقارنةً بغيره من المتصفحات وذلك بسبب اجراءات الأمان التي يجريها.

٢-افحص الصلاحيات والأذونات التي تحصل عليها مواقع الويب من جهازك

الكثير من المواقع بحاجة لصلاحيات وأذونات يحصل عليها منك لكي يستطيع اتمام مهمته وتقديم خدمته لك بأكمل وجه، فقد يحتاج موقع Facebook مثلا أذونات منك ليتمكن من فتح كاميرا جهازك كي تستطيع بث فيديو مباشر لك.

المشكلة في المواقع غير الموثوقة والتي قد تطلب منك أذونات وصلاحيات لا تستحقها وليست بحاجة لها.

كيف أفحص وأضبط الصلاحيات التي يحصل كل موقع أقوم بزيارته ؟

- بعد زيارتك لموقع الويب المقصود، اضغط على أيقونة القفل في الأعلى بجوار رابط الموقع.
- اضغط على اعدادات المواقع الالكترونية.
- هنا ستظهر جميع الأذونات التي يحصل عليها الموقع، تستطيع ضبطها من خلال اختيار أحد الخيارات (سماح - منع - السؤال أولًا).

٣-استخدم نافذة التصفح الخفي

انتبه، المتصفحات عادةً تقوم بتسجيل بيانات عنك، كمواقع الويب التي قمتَ بزيارتها وبياناتك التي قمت بإدخالها وغيرذلك.
وقد تكون أحيانًا غيرمعني بأن تقوم تلك المتصفحات بعمليات التسجيل هذه، خصوصًا حينما تستخدم جهازًا آخرًا غير جهازك الشخصي.
ففي هذه الحالة أنت بحاجة لاستخدام ما يسمى بـ التصفح الخفي

كيف أقوم بتفعيل نافذة التصفح الخفي؟

- التصفح الخفي على متصفح كروم

في الجزء العلوي الأيسر من المتصفح، اضغط على القائمة ثم توجه لخيار التصفح الخفي.

- التصفح الخفي في موزيلا فايرفوكس

ندخل إلى متصفح الفايرفوكس ونضغط على الجزء العلوي الأيسر ونختار أيقونة التصفح الخفي.

- إذا كنت تستخدم أوبرا قم بتشغيله واضغط على **Ctrl+Shift+N**.
- إذا كنت تستخدم إنترنت اكسبلورر قم بتشغيله واضغط على **Ctrl+Shift+P**.
- إذا كنت تستخدم غوغل كروم قم بتشغيله واضغط على **Ctrl+Shift+N**.
- إذا كنت تستخدم الفايرفوكس قم بتشغيله واضغط على **Ctrl+Shift+P3**.

٤-استخدم محرك بحث آمنًا

هناك العديد من محركات البحث الآمنة التي تسعى لحفظ أمنك وخصوصيتك، بحيث تكون عمليات البحث فيها مشفرة، وقد طورت العديد من المحركات خصائصًا إضافية لضمان تصفح الإنترنت بشكل آمن.

ولعل من أبرز هذه المحركات:

Search Encrypt

Start Page

DuckDuckGo

Gibiru

Swiss Cows

٥-استخدم مواقع الويب المحمية

تأكد دائماً من وجود علامة **https** في بداية عنوان موقع الويب الذي تزوره.

العلامة التي تعني أن الموقع يحمل الصفة الرسمية ويتمتع بالأمان، ويحمي بيانات مستخدميه.

الشبكة الافتراضية الخاصة VPN

الشبكة الافتراضية الخاصة أو Virtual Private Network واختصاراً VPN هي وسيلة حماية شائعة الاستخدام أثناء تصفح الإنترنت، تتضمن مجموعةً من التقنيات التي تهدف إلى إضافة طبقة حماية إضافية إلى الشبكات العامة والخاصة.

يعُد الـ VPN أحد الحلول الآمنة التي يسمح للمستخدمين سواء كانوا أفراداً أو أعضاءً في المنظمات بإرسال واستقبال البيانات، مع المحافظة على سرية الشبكة الخاصة، وهذا يعني أنك تستطيع إنشاء شيء أشبه بنفقٍ سرّيٍّ ضمن شبكة مؤسستك للتمتع بالوصول إلى الأنظمة الداخلية الخاصة، كما يمكنك أيضاً من الوصول إلى شبكة الانترنت وتصفحها بشكلٍ آمنٍ تماماً.

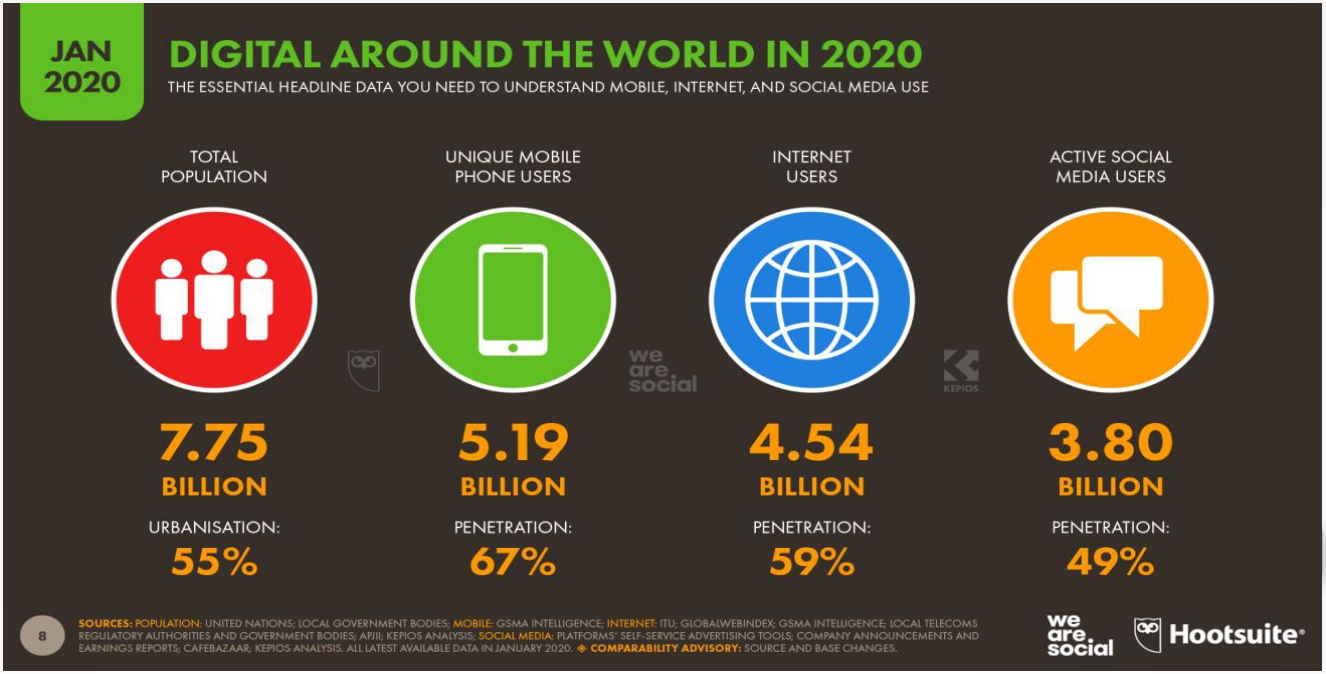
جميع البيانات التي تمر عبر اتصال VPN تكون آمنةً -نظرياً- ولا يمكن لأي أحدٍ اعتراضها، مما يجعلها أسرع وسيلةٍ شائعةٍ لتصفح الويب بسريّة.

التعامل مع الـ VPN وتجهيز المؤسسة للتعامل بها يعد من تخصصات مختص الشبكات فيها. لكن بإمكانك الاطلاع على آلية تفعيلها والمزيد من التفاصيل من المقالة المفصلة التي نشرتها شركة سيسكو أحد أكبر الشركات المختصة في عالم الشبكات في العالم. من هنا

ثامناً: منصات التواصل الاجتماعي

قد نحتاج في اتمام وتسيير عملنا استخدام منصات التواصل الاجتماعي، سواء بالتعامل مع الاطراف الأخرى كالمستفيدين من المنظمة مثلا، أو لزيادة وصول المنظمة للعالم الخارجي، مما يضطرنا إلى تداول بعض البيانات عبرها فيما يخص العمل والمنظمة، الأمر الذي يحتم علينا أيضًا كأي وسيلة رقمية أن نراعي مجموعة اجراءات امان رقمي.

> أكثر من ٤,٥ مليار مستخدم للإنترنت بالعالم (٥٩٪ من البشر)، منهم أكثر من ٣,٨ مليار شخص (٤٩٪ من البشر) يستخدمون وسائل التواصل الاجتماعي. ذلك بحسب تقرير صادر في يناير الماضي لمؤسسة WE ARE SOCIAL المعنية بقياس استخدام وسائل التواصل الاجتماعي بالتعاون مع مؤسسة Hootsuite



كيف نحمي حساباتنا في منصات التواصل الاجتماعي؟

المتابع للإجراءات الامان في نصات التواصل الاجتماعي المختلفة يجدها متشابهة بشكل كبير، فإتقان تأمين منصة واحدة يجعل من السهل التعامل مع بقية المنصات.

حماية حساباتنا على منصة الفيسبوك (مثال)

كيف أحمي حسابي في منصة الفيسبوك؟

١- قم بتفعيل خاصية تسجيل الدخول بخطوتين (المصادقة الثنائية)

خاصية المصادقة الثنائية تزيد عملية تسجيل الدخول لحسابك تعقيدًا، الأمر الذي يجعله أأمن وأصعب على القراصنة والخصوم.

من خلال هذه الخاصية ستزداد خطوات تسجيل الدخول لحسابك إلى خطوتين بدلًا من خطوة واحدة.

الخطوة الأولى هي اضافة اسم المستخدم وكلمة المرور، أما الخطوة الثانية ستكون تأكيد الدخول من خلال الهاتف إما برسالة SMS تحتوي على كود تفعيل متغير، أو من خلال التطبيق.

> حقائق:
> • فيسبوك هو منصة التواصل الاجتماعي الأكثر استخداماً في فلسطين.
> • يستخدم الخصوم فيسبوك باستمرار لمهاجمة الناشطين وأصحاب الآراء المخالفة وكذلك الضعفاء.

كيف أفعِّل خاصية المصادقة الثنائية؟

- في حسابك توجه الى الاعدادات بالضغط على السهم في الزاوية العلوية اليسرى
- ثم اختر الأمان وتسجيل الدخول
- الآن توجه لصندوق المصادقة الثنائية، ثم قم بتفعيل خيار استخدام المصادقة الثنائية.

٢- راقب عمليات تسجيل الدخول لحسابك

الفيسبوك يُمكِّنك من مراقبة عمليات تسجيل الدخول لحسابك، يُمكِّنُك من معرفة متى تم الدخول لحسابك ومن أي جهاز ومن أي موقع جغرافي (من خلال عنوان الـIP)

وذلك من خلال صندوق المكان الذي سجلت دخولك منه داخل صفحة الأمان وتسجيل الدخول.

٣- راقب الصلاحيات التي حصلت عليها التطبيقات والمواقع من حسابك:

الكثيرمن التطبيقات أو مواقع الويب التي نتعامل معها تطلب منا ربطها بحســـاباتنا على منصـــات التواصل الاجتماعي، سواءً لتقوم بمهمتها المتعلقة بتلك المنصات أو لتسهيل عملية تسجيل الدخول فيها.

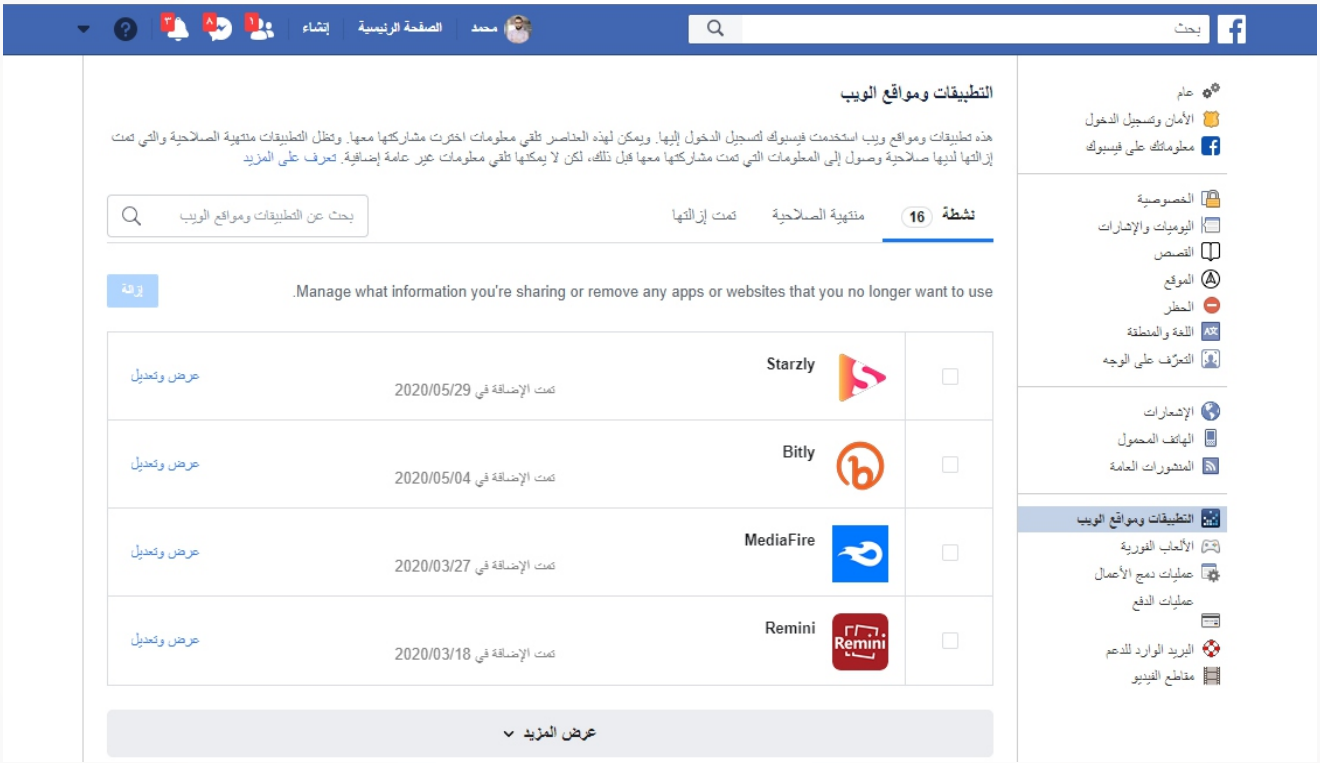
العملية قد تكون خطيرةً لو قمنا بها مع التطبيق أو موقع الويب الخطأ، في البداية يجب أن تكون واثقاً بتلك التطبيقات أو المواقع التي تـــــربطها بحسابك، ثانيا يجب عليك أن تنتبه قبل اتمام عملية الربط إلى الصلاحيات أو الأذونات التي ستحصل عليها تلك التطبيقات من حسابك.

منصة الفيسبوك تمكنك من مراجعة الصلاحيات والأذونات التي قُمتَ بمنحها للتطبيقات ومواقع الويب المرتبطة بحسابك أو ما يتم تسميتها بـ third party أو الطرف الثالث.

في صفحة اعدادات الفيسبوك توجه إلى تبويب التطبيقات ومواقع الويب

هنا ستظهرلك جميع التطبيقات ومواقع الويب التي قمت بربطها بحسابك والتي تستخدم فيسبوك للدخول إليها.

عند النقرعلى كل تطبيق منها سيظهرلك ما هي الصـــلاحيات والأذونات التي قمتَ بمنحها للتطبيق، كما يمكنك هنا إزالة هذا التطبيق وسحب الصلاحيات منه.



برامج وأدوات لإدارة وتسيير عمل المنظمة رقميًا بشكل آمن

تتنوع وتتعدد البرامج والأدوات التي يمكن استخدامها في إدارة وتنفيذ وتسيير أعمالنا رقميًا، خصوصًا في الوقت الحالي الذي اضطر فيه العالم إلى رقمنة عمله.

الكثير من الشركات تحرص على توفير حزمة كاملة من الأدوات تعمل بشكل متكامل لذلك.

دعونا نسلط الضوء على حزمة متكاملة من الادوات تقدمها شركة جوجل لتسيير الأعمال رقميًا بشكل آمن جدًا.

Google Workspace أو ما كانت تسمى سابقًا G-Suite (جناح جوجل)

هي بمثابة مجموعة من المنتجات المُخصصة للأعمال والشركات تقدمها جوجل، وهي تجمع بين تطبيقات الشركة (جوجل) مثل **Gmail** و **Drive** و **Docs** و **Sheets** وغيرها الكثير.

وتُقدّم جوجل هذه الخدمات باشتراك شهري لمساعدة الشركات على تنظيم أعمالها والتعاون بين أفرادها، في سبيل تحقيق النجاح.

ما الفرق بينها وبين تطبيقات جوجل المجانية؟

يظهر الفرق تمامًا عند حديثنا عن مميزات هذه الحزمة:

مميزات Google Workspace

تتضمن بعض هذه المميزات، مشاركة التقاويم بين العاملين بالمنظمة، والتخزين السحابي غير المحدود بشكل اختياري، وأدوات تحكم إدارة متقدمة، مثل إضافة وحذف المستخدمين من العاملين بالمنظمة، والتحقق الثنائي، وتسجيل الدخول الأحادي، وأدوات دمج البيانات البسيطة لنقل جميع بيانات المنظمة أو المؤسسة **Google**.

بالإضافة إلى كل ذلك، تأتي خدمة **G Suite** مع إمكانية إدارة الأجهزة المحمولة، مما يتيح لك تنشيط / إلغاء تنشيط الأجهزة المحمولة، والتحكم في التطبيقات التي يتم تفعيلها على الأجهزة المستخدمة في العمل الخاص بالمنظمة، والحذف الكامل عن بُعد في حالة خرج الموظف عن إطار الشركة.

وإلى جانب كل هذه المميزات، تسمح لنا هذه الحزمة أيضاً بإضافة عنوان بريد إلكتروني مخصص لاسم الدومين الخاص بالمنظمة (العنوان لن يكون **Gmail** @ بل باسم المؤسسة أو المنظمة).

مزايا أمان رقمي تتيحها Google Workspace

- **لوحة بيانات أمان موحدة:**

تمتلك إحدى إصدارات **Google Workspace** لوحة بيانات أمان موحدة، يمكننا من خلالها الحصول على إحصاءات حول مشاركة الملفات الخارجية ورؤية الرسائل غير المرغوب فيها والبرامج الضارة التي تستهدف المستخدمين داخل المؤسسة أو المنظمة والمقاييس التي

تعرض فعالية الأمان في لوحة بيانات واحدة شاملة.

- **اتخاذ إجراء بشأن التهديدات:**

يمكنك تحديد مشاكل الخصوصية والأمان في نطاقك وفرزها واتخاذ إجراء بشأنها. ويمكنك تنفيذ إجراءات مُجمَّعة على مستوى المؤسسة لحذف الرسائل الإلكترونية الضارة. كما يمكنك التحقُّق من مشاركة الملفات لاكتشاف عمليات استخراج البيانات المُحتملة ومنعها.

- **خفض مستوى الخطورة عن طريق اعتماد اقتراحات السلامة الأمنية:**

يمكنك البقاء على استعداد لمواجهة التهديدات من خلال دليل البدء السريع، والذي يوفر إعدادات الأمان المقترحة ويقدم نصائح مخصصة حول أفضل ممارسات الأمان المتعلقة بالمحتوى والاتصال والتنقل وأمان المستخدم.

- **الحصول على إحصاءات من مركز الأمان:**
- عرض الملف: يمكنك التعرُّف على الملفات التي تمت مشاركتها خارج نطاقك من قبل العاملين.
- المصادقة: يمكنك معرفة عدد الرسائل التي لا تستوفي المعايير.
- التشفير: يمكنك التأكُّد من أن الرسائل التي تم إرسالها عن طريق نطاقك مُشفَّرة.
- تسليم البريد الإلكتروني: يمكنك الاطِّلاع على النسبة المئوية للرسائل الواردة التي تم قبولها وما إذا سمحت الإضافة إلى القائمة البيضاء بتسليم رسائل مُريبة أم لا.
- تصنيف الرسائل غير المرغوب فيها والبرامج الضارة: يمكنك تحليل الرسائل التي تم اعتبارها رسائل غير مرغوب فيها أو تصيُّدًا احتياليًا أو مُريبة أو تحتوي على برامج ضارة.
- تقييم المستخدم: يمكنك تقييم القوائم البيضاء عن طريق مراجعة ما إذا وضع المستخدمون علامة على الرسائل التي تم تسليمها كرسائل غير مرغوب فيها أو تصيُّدٍ احتيالي.

مراجع ودعم

- مواقع إلكترونية مفيدة ومراجع الدليل

- صفحة الدعم لدى منصة الفيسبوك

- صفحة الدعم لدى مايكروسوفت

- موقع شركة كاسبرسكاي

الحماية الرقمية أثناء استخدام المنزل كمكان للعمل

- موقع Heimdal_security

- صفحة مركز الأمان لخدمة Google Workspace

- موسوعة ويكيبيديا

شبكة المنظمات الأهلية الفلسطينية

Palestinian NGO's Network - PNGO

082847518

pngoportal@gmail.com

PNGO Portal