المركز الوطني
للأمن السيبراني
National Cyber
Security Center

أمن الأجهزة المحمولة

المحـاور

- تعريف الأجهزة المحمولة
- استخدامات الأجهزة المحمولة
- فوائد استخدام الأجهزة المحمولة ضمن بيئة العمل
- سلبيات استخدام الأجهزة المحمولة ضمن بيئة العمل
- حماية الأجهزة المحمولة
- أهمية حماية الأجهزة المحمولة
  - أهمية حماية الأجهزة المحمولة بالنسبة للموظف
  - أهمية حماية الأجهزة المحمولة بالنسبة للمؤسسة
- سياسة استخدام الأجهزة الشخصية (BYOD)
- النص القانوني لسياسة استخدام الأجهزة المحمولة
- مخاطر استخدام الأجهزة المحمولة الشخصية في العمل
- تطبيق أمن الأجهزة المحمولة

تعريف الأجهزة المحمولة

يُمكن تعريف الأجهزة المحمولة على أنها أجهزة صغيرة الحجم وخفيفة الوزن وبشكل يُمكن مُستخدميها من حملها واستخدامها بسهولة حتى أثناء التنقل، وتشتمل الأجهزة المحمولة مجموعة واسعة من الأجهزة الإلكترونية مثل الهواتف الذكية والأجهزة اللوحية (التابلت) وأجهزة الكمبيوتر المحمولة (اللابتوب)، حتى أن بعض أنواع الأجهزة القابلة للارتداء كالساعات الذكية وغيرها يُعتبر من أشكال الأجهزة المحمولة.

استخدامات الأجهزة المحمولة في نطاق العمل

ينطوي استخدام الأجهزة المحمولة في بيئة العمل (سواء كانت الأجهزة شخصية وخاصة بالموظف أو تم تزويده بها من قبل مؤسسته) على العديد من الإيجابيات والفوائد، ولكنها أيضاً تتضمن بعض المحاذير والسلبيات التي قد تهدد الأمن الرقمي للمستخدم ولمؤسسته، وسنوضح تالياً الإيجابيات والسلبيات لاستخدام هذه الأجهزة:

فوائد استخدام الأجهزة المحمولة في بيئة العمل

لاستخدام الأجهزة المحمولة ضمن بيئة عمل المؤسسات والدوائر المختلفة العديد من الإيجابيات والفوائد، ومنها الآتي:

المرونة وسهولة التنقل:

حيث يتمكن الموظفون من القيام بأعمالهم في أماكن مختلفة ودون شرط التقيد بالتواجد في بيئة العمل المكتبية التقليدية.

تحسين الإنتاجية:

توفر الأجهزة المحمولة أدوات فعالة من شأنها زيادة كفاءة عمل الموظفين وزيادة انتاجيتهم، حيث يُمكن إنجاز المهام بشكل أسرع وأكثر كفاءة.

فوائد استخدام الأجهزة المحمولة في بيئة العمل

لاستخدام الأجهزة المحمولة ضمن بيئة عمل المؤسسات والدوائر المختلفة العديد من الإيجابيات والفوائد، ومنها الآتي:

التواصل الفعال:

لاستخدام الأجهزة المحمولة أثر كبير في تحسين قدرة الموظفين على التواصل، وذلك من خلال التفاعل عبر البريد الإلكتروني أو حتى الرسائل النصية، بالإضافة لعقد الاجتماعات عن بعد في خارج أوقات العمل ومن أي مكان.

الإدارة عن بعد:

يوفر استخدام الأجهزة المحمولة إمكانية الوصول إلى أنظمة وملفات المؤسسة عن بعد، مع الأخذ بعين الاعتبار أن هناك العديد من الأنظمة الحكومية التي لا يتمكن الوصول إليها إلا خلال تواجد الموظف في مكان عمله، وعادة ما تكون تلك الأنظمة حرجة وسرية ويتم تقييد الوصول إليها عن بعد لتحقيق الأمن السيبراني وتقليل خطر التعرض للهجمات الإلكترونية.

فوائد استخدام الأجهزة المحمولة في بيئة العمل

لاستخدام الأجهزة المحمولة ضمن بيئة عمل المؤسسات والدوائر المختلفة العديد من الإيجابيات والفوائد، ومنها الآتي:

التعرض للفقدان والسرقة:

يُعتبر خطر فقدان الأجهزة المحمولة أو سرقتها الخطر الرئيسية لاستخدامها، وذلك كونها قابلة للحمل والنقل، وهو ما قد يُهدد سلامة البيانات الموجودة على تلك الأجهزة ويعرضها لخطر الاختراق أو الاطلاع عبر المصرح به.

الهجمات السيبرانية:

الأجهزة المحمولة قد تكون أكثر عرضة لخطر الاختراق وحدوث الهجمات السيبرانية، وذلك أنها قد لا تكون خاضعة تماماً لسياسات الأمن السيبراني والاستخدام الآمن مثل تلك الأجهزة المكتبية التي يتم إدارتها من قبل موظفي تكنولوجيا المعلومات.

سلبيات استخدام الأجهزة المحمولة في بيئة العمل

شبكات الواي فاي غير الآمنة:

من الأخطار الرئيسية لاستخدام الأجهزة المحمولة هو الاتصال بشبكات واي فاي غير موثوقة، وهو ما يزيد من خطر تعرض المُستخدم وبيانات المؤسسة الموجودة على تلك الأجهزة للاختراق والتجسس.

الخلط ما بين الأعمال الشخصية ومهام العمل:

يُمكن أن يؤدي استخدام الأجهزة المحمولة إلى الخلط وعدم الفصل ما بين إنجاز المهام الرسمية الخاصة بالعمل وما بين إنجاز بعض الأمور الشخصية كاستخدام وسائل التواصل الاجتماعي وغيرها.

حماية الأجهزة المحمولة

يُمكن تعريف حماية الأجهزة المحمولة بأنها اتخاذ التدابير واستخدام التقنيات واتباع السياسات اللازمة لضمان أمان وحماية تلك الأجهزة (لابتوب، هواتف ذكية، وغيرها) من التهديدات الأمنية والهجمات السيبرانية وتحقيق عدم التعرض لأي من أنواع الجرائم الإلكترونية، ويهدف مفهوم حماية الأجهزة المحمولة إلى ضمان عدم تعرض بيانات المؤسسة ومعلوماتها أياً كانت درجة سريتها إلى الفقد او الاطلاع والوصول غير المصرح به.

أهمية حماية الأجهزة المحمولة

يُعتبر امر حماية الأجهزة المحمولة ذو أهمية كبيرة لكل من الموظف وللمؤسس على حد سواء، وكالآتي:

- بالنسبة للموظف

- بالنسبة للمؤسسة

أهمية حماية الأجهزة المحمولة بالنسبة للموظف

تجنُب المساءلة:

تؤدي حماية الأجهزة المحمولة بشكل صحيح إلى حماية الموظف قانونياً وضمان عدم تعرضه للمساءلة القانونية التي قد تطاله نتيجة تعرض بيانات المؤسسة للاختراق من خلاله أو من خلال جهازه المحمول، فكل موظف في دائرة أو مؤسسة رسمية مسؤول عن حماية حساباته الخاصة بالعمل حتى لو تم استخدامها من جهاز محمول شخصي أو غير شخصي.

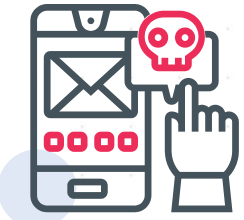
حماية البيانات الشخصية والرسمية:

تضمن حماية الأجهزة المحولة وأمنها تحقيق حماية للبيانات الشخصية الموجودة عبر الأجهزة وكذلك الأمر بالنسبة لتلك الرسمية.

أهمية حماية الأجهزة المحمولة بالنسبة للمؤسسة

حماية السمعة والثقة:

على المؤسسات القيام بكل ما يلزم لحماية الأجهزة المحمولة التي يتم استخدامها ضمن بيئة العمل وذلك للحفاظ على سمعتها أمام الجمهور وللحفاظ على استمرار ثقة عملاءها بأفضل شكل.



ضمان استمرارية تقديم الخدمة:

يُمكن أن تؤدي هجمة سيبرانية على جهاز محمول يتم استخدامه في العمل إلى توقف كامل او حتى جزئي للخدمات الإلكترونية التي تقدمها المؤسسات والدوائر المختلفة.

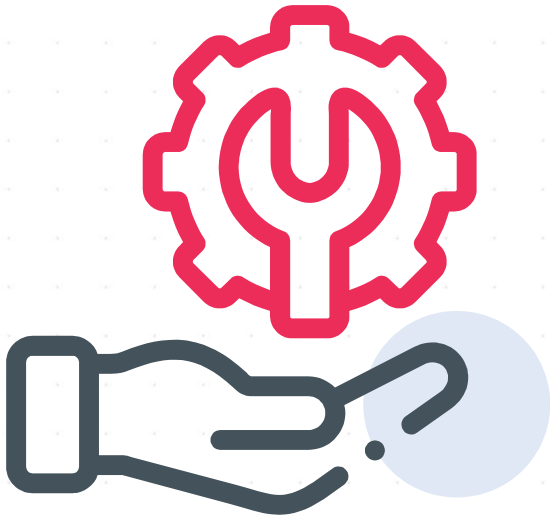
الحفاظ على خصوصية المواطنين:

ينعكس تحقيق الأمن السيبراني للأجهزة المحمولة التي يتم استخدامها في عمل الدوائر والمؤسسات على الحفاظ على سلامة البيانات والمعلومات الخاصة بالمواطنين، وهو ما يضمن عدم انتهاك خصوصيتهم.

النص القانوني لسياسة استخدام الأجهزة المحمولة

أوضحت وثيقة سياسة استخدام موارد تكنولوجيا المعلومات في وزارة الاقتصاد الرقمي والريادة آلية استخدام الأجهزة المحمولة الشخصية وفق النص الآتي:

يُسمح باستخدام الحواسيب المحمولة الشخصية (المملوكة شخصياً) إذا تحققت الشروط الآتية:



- إذا كان المستخدم ضمن نطاق الآمن الذي يخوله باستخدام الحاسوب المحمول وإذا كانت كل الحواسيب المحمولة الخاصة بالمؤسسة (قيد الاستخدام) ويتم التحقق من ذلك من قسم الدعم الفني.
- موافقة المسؤول المباشر وقسم الدعم الفني.
- أن يعلم المُستخدم بأن المعلومات الموجودة على جهازه الشخصي هي معلومات خاصة بالمؤسسة وخاضعة لهذه السياسة كما يحق للمؤسسة الاطلاع على محتويات هذه الحواسيب المحمولة الشخصية.

تطبيق أمن الأجهزة المحمولة

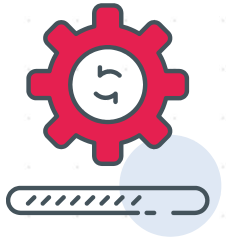
يُمكن تحقيق وتطبيق أمن الأجهزة المحمولة من خلال إتباع العديد من الإجراءات، ومنها الآتي:

تجنُب المساءلة:

يتوجب ضبط الجهاز بحيث يتم تفعيل ميزات القفل والإغلاق الموجودة خلاله، مثل كلمات المرور أو بصمة الأصبع، وذلك لضمان عدم تمكن الأشخاص غير المصرح لهم بالدخول لجهاز أو فتحه.

استخدام التشفير:

يُوصى باستخدام برامج التشفير لتأمين البيانات والمعلومات المحفوظة على الأجهزة المحمولة، وذلك لضمان عدم تسربها أو الاطلاع عليها حتى في حال فقدان الجهاز.



تحديث البرامج والتطبيقات:

يتوجب إجراء تحديث دوري ومنتظم للبرامج والتطبيقات ونظام التشغيل المثبت على الجهاز المحمول، حيث أن هذه التحديثات تعمل على سد الثغرات الأمنية الموجودة في تلك الأنظمة والبرامج.

تطبيق أمن الأجهزة المحمولة

استخدام شبكات واي فاي آمنة:

يتوجب تجنُب الاتصال بشبكات الواي فاي العامة أو غير الموثوقة من الأجهزة المحمولة وذلك لخطرها الداهم على التعرض لهجمات سيبرانية واقتحام الخصوصية أثناء الاتصال بتلك الشبكات.

إجراء نسخ احتياطي:

يتوجب إجراء نسخ احتياطي مُنتظم ودوري لكافة البيانات الحساسة الموجودة على الأجهزة المحمولة لضمان القدرة على استعادتها في حال تعرضها للتلف أو التخريب أو حتى الفقد.

الوعي بإجراءات الأمن السيبراني:

يتوجب أن يتلقى مستخدم الجهاز المحمول التثقيف والتوعية الكافية لإدراكه بأهم المخاطر السيبرانية وجرائم التصيد والاحتيال التي تتم عبر الإنترنت عموماً والبريد الإلكتروني بشكل خاص.

تطبيق أمن الأجهزة المحمولة

إتبـــاع تعليمـــات الأمـــن السـيبراني التـــي تفرضـــها المؤسسة:

يلزم مُستخدم الجهاز المحمول أن يتبـع كامـل التعليمـات والسياسـات التي يفرضها قسم الأمن السيبراني أو قســم تكنولوجيــا المعلومــات فــي مؤسسته.

استخدام كلمة مرور قوية :

يتوجب أن تكون كلمة المرور التي يتم تعيينهـا للأجهـزة المحمولـة محققـة لسياسات الأمان المُتبعة في مؤسستك، كـأن تكـون بطـول معـين وأن تكـون مركبـة بحيـث تتضـمن مجموعـة مـن الأحـرف الصـغيرة والكبيـرة والرمـوز والأرقــام، بالإضــافة إلــى ضــرورة تغييرها بشكل دوري ومستمر.

تفعيل نظام المصادقة الثنائي:

يُمكـن استشـارة قسـم الـدعم الفنـي فـي مؤسســتك لتفعيــل نظــام المصــادقة الثنــائي عبــر الأجهــزة والحســابات المختلفة، وذلك لإضافة طبقة ثانية من الحماية.

الخاتمة

في ختام حديثنا عن الأجهزة المحمولة وحمايتها فإنه يجدر التأكيد على أهمية التوعية بطرق الاستخدام الآمن لهذه التكنولوجيا، والتي على الرغم مما تحققه من فوائد كبيرة إلا أنها تُعتبر حرجة في ما يخص الأمن السيبراني، لذا يتوجب التأكد من تطبيق ما تم ذكره من إجراءات أمان لتجنُب أي تهديدات رقمية قد تنتج عن استخدام الأجهزة المحمولة سواء في العمل أو حتى في أنشطة الحياة الشخصية والخاصة.

نتمنى لكم السلامة في

العالم الرقمي.