المركز الوطني
للأمن السيبراني
National Cyber
Security Center

حماية البريد الإلكتروني

المحـــــاور

- البريد الإلكتروني في الأمن السيبراني
- تعريف حماية البريد الإلكتروني
- أهمية حماية البريد الإلكتروني
- إجراءات حماية البريد الإلكتروني
- ضوابط استخدام البريد الإلكتروني

البريد الإلكتروني في الأمن السيبراني

- على الرغم من أهمية البريد الإلكتروني واستخداماته المتعددة على الصعيد الشخصي والمؤسسي، إلا أن البريد الإلكتروني يُعتبر بمثابة باب مفتوح على مصراعيه أمام الهجمات السيبرانية والجرائم الإلكترونية المختلفة.
- تُشير العديد من الدراسات المتخصصة أن ما يقارب 90 بالمئة من الهجمات السيبرانية التي يتم شنها على الأشخاص والمؤسسات تحدث من خلال رسائل البريد الإلكتروني المخادعة التي تستخدم وسائل مختلفة منها الهندسة الاجتماعية في سبيل خداع المُستخدِم والوصول إلى بياناته ومعلوماته.
- وهذا الأمر يعكس أهمية تأمين وحماية البريد الإلكتروني ومعرفة أبرز الإجراءات التي يتوجب اتباعها لتحقيق ذلك.

تعريف حماية البريد الإلكتروني

- يُشير مفهوم حماية البريد الإلكتروني إلى تلك الممارسات والإجراءات التي من شأنها حماية حسابات البريد الإلكتروني والاتصالات التي تتم خلالها الوصول غير المصرح به والتجسس والإطلاع غير الشرعي.

- يُمثل البريد الإلكتروني نقطة سهلة للدخول إلى الحسابات والأجهزة الأخرى وخاصة أنه يعتمد على الخطأ البشري الناتج عن سلوك المُستخدِمين، فكل ما يتطلبه الأمر لحصول هجمة إلكترونية على مؤسسة بأكملها هو قيام أحد المُستخدمين بنقرة خاطئة على رابط مُخادع موجود في بريد إلكتروني مُضلل.

أهمية حماية البريد الإلكتروني

لحماية البريد الإلكتروني فوائد متعددة على المؤسسة بأكملها، ومنها الآتي:

- تأمين البريد الإلكتروني يحمي العملاء و يحافظ على سمعة المؤسسة.
- تأمين البريد الإلكتروني يؤدي إلى حفظ البيانات الحساسة والوثائق الرسمية و يمنع الوصول غير المصرح لها.
- حماية البريد الإلكتروني تعزز الإنتاجية بتجنب التوقفات والاضطرابات المحتملة للعمل.
- يوفر حماية البريد الإلكتروني واتباع السياسات الضرورية حماية قانونية للموظفين من التسريبات الناتجة عن الهجمات السيبرانية.

إجراءات حماية البريد الإلكتروني

يوجد العديد من الإجراءات التي يُمكن من خلالها حماية البريد الإلكتروني الخاص، ومنها الآتي:

تعزيز كلمات المرور:

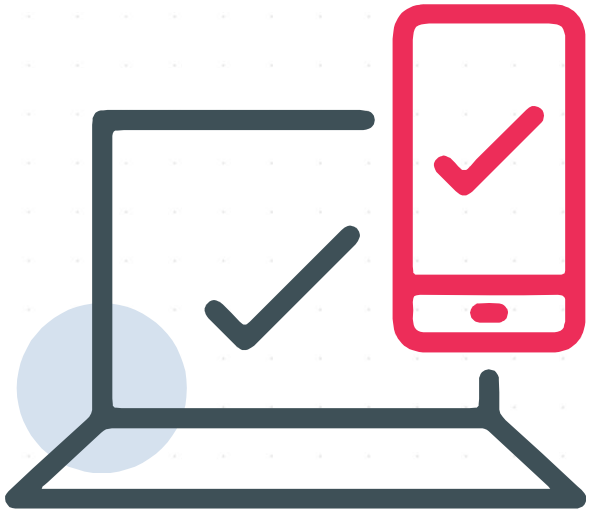
- تُعتبر كلمة المرور القوية خط الدفاع الأول في حماية البريد الإلكتروني.
- يجب تعيين كلمة مرور قوية وعشوائية ومُعقدة بحيث تتضمن مزيجاً من الأحرف الصغيرة والكبيرة والأرقام والرموز فيصعب تخمينها من قبل مُجرمي الإنترنت.

إجراءات حماية البريد الإلكتروني

استخدام شبكات موثوقة للاتصال:

- يجب أن يتم استخدام البريد الإلكتروني من خلال الاتصال بشبكات موثوقة فقط.
- في حالة الاتصال بالإنترنت واستخدام البريد الإلكتروني أثناء الاتصال بشبكات غير موثوقة فإنه يُمكن لأي شخص عبر هذه الشبكات الحصول على بيانات الدخول لحساب البريد الإلكتروني؛ وهو ما يجعله عرضة للاختراق والتجسس.

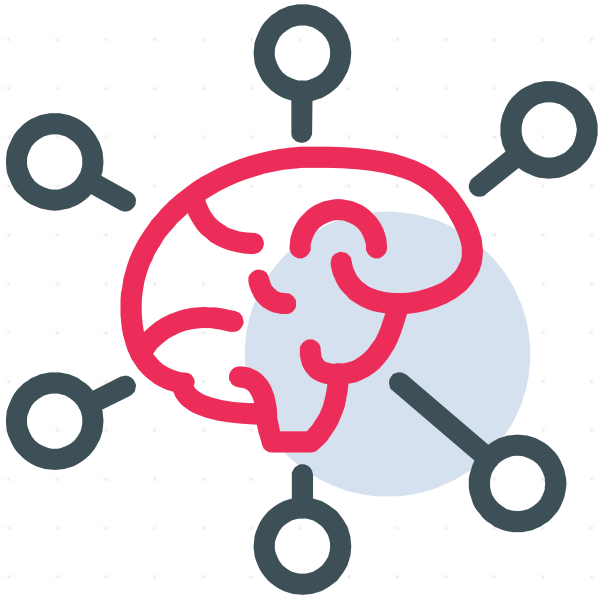
إجراءات حماية البريد الإلكتروني



تفعيل نظام المصادقة الثنائية:

- يُعتبر تفعيل نظام التحقق الثنائي (Two-Factor Authentication) والذي يُشار له بالاختصار (FA2) أحد أهم الإجراءات في سبيل تحقيق الحماية للبريد الإلكتروني.
- يجعل هذا الخيار إمكانية اختراق البريد الإلكتروني أمراً صعباً حتى في حالة معرفة أو توقع كلمة المرور من قبل مجرمي الإنترنت.

إجراءات حماية البريد الإلكتروني



فكّر قبل أن تنقر:

- من أهم السياسات الفاعلية في سبيل تحقيق الأمان والحماية للبريد الإلكتروني هو الشك في كل ما يرد من رسائل يتم خلالها مطالبة المُستخدِم بإجراء معين كالنقر فوق رابط أو تحميل مرفق أو غيره.
- يجب التفكير جيداً قبل النقر على أي مرفق أو رابط في رسائل البريد الإلكتروني والتحقق من الجهة المرسلة.

إجراءات حماية البريد الإلكتروني

عدم الكشف عن البيانات الخاصة:

- لن تقوم أي جهة رسمية حكومية كانت أو خاصة بمطالبة المُستخدِم بالكشف عن أي من بياناته الشخصية أو كلمات المرور لأي من حساباته.
- يجب عدم الإفصاح عن مثل تلك البيانات أياً كانت الجهة التي تطلب القيام بذلك.

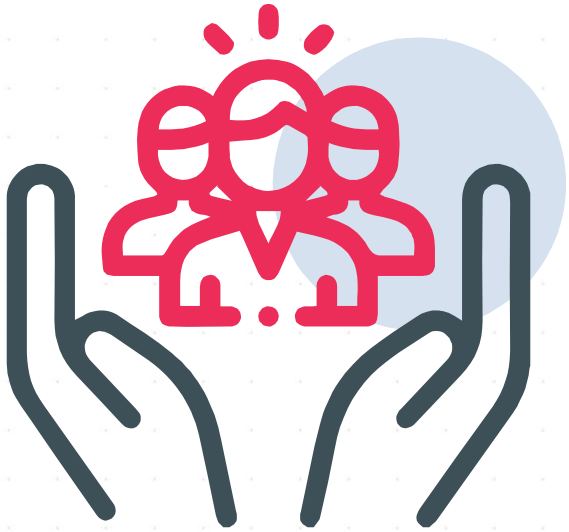
إجراءات حماية البريد الإلكتروني

مراجعة إعدادات الخصوصية والأمان:

- تأتي حسابات البريد الإلكتروني الرسمية الخاصة بالمؤسسات بإعدادات أمان مثبتة ومُعدة من قبل مختصي تكنولوجيا المعلومات في المؤسسة أو الدائرة.

- في حال استخدام بريد إلكتروني شخصي فإنه يتوجب على المُستخدِم مراجعة إعدادات الأمان الافتراضية لحساب البريد الإلكتروني مثل تفعيل خاصية تصفية البريد العشوائي وغيرها من الإعدادات التي تزيد من حماية حساب المُستخدِم.

إجراءات حماية البريد الإلكتروني



توعية الموظفين وتثقيفهم:

- يُعتبر العامل البشري هو المُسبب الأول لنجاح معظم الهجمات السيبرانية التي يتم شنها على الأفراد والمؤسسات.
- لا بد من توعية الموظفين بأهم إجراءات وسياسات حماية البريد الإلكتروني، ومراجعة هذه السياسات والإجراءات بشكل دوري للتأكد من فهمها وتطبيقها بالشكل الصحيح.

ضوابط استخدام البريد الإلكتروني الحكومي

يوضح الآتي تعليمات استخدام البريد الإلكتروني في نظام استخدام موارد تكنولوجيا المعلومات الخاص بالمؤسسات الحكومية في المملكة الأردنية الهاشمية، والذي يتماشى مع تحقيق الاستخدام الآمن للبريد الإلكتروني الرسمي:

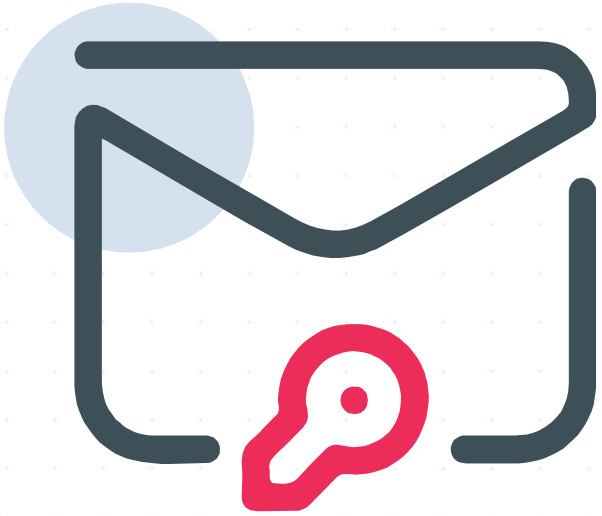
1. عدم إرسال رسائل تحمل طابعاً تشهيرياً بأي شخص أو طابع افترائي أو علامات تدعو إلى العدوان أو إشارات إلى العنصرية، أو إشارات تدل على الفحش أو الإباحية، لأن ذلك يعرض المرسل إلى المساءلة القانونية.

2. عدم إرسال رسائل تحتوي على فيروسات إلى جهات أخرى، لأن ذلك سيعرض المستخدم إلى المساءلة القانونية.

3. . يمنع إرسال الرسائل الإلكترونية بشكل عشوائي ومن غير مبرر لذلك.

ضوابط استخدام البريد الإلكتروني الحكومي

4. يمنع تزييف أو محاولة تزييف الرسائل الالكترونية.
5. يمنع المستخدم من إخفاء أو محاولة إخفاء هويته الحقيقية عند إرسال الرسائل الالكترونية.
6. يمنع استخدام البريد الإلكتروني الخاص بالآخرين دون أخذ موافقتهم بشكل مسبق.
7. يجب على المستخدم عدم فتح الملفات أو الروابط المرسلة من عناوين مشبوهة أو الملفات من الأنواع غير المألوفة.
8. في حال الاشتباه بالرسالة الإلكترونية المُستقبلة فإن على المستخدم التحقق من مرسل الرسالة ، أو تبليغ مسؤول أمن المعلومات وفريق الدعم الفني عنها.



ضوابط استخدام البريد الإلكتروني الحكومي

9. يجب على المستخدم أرشفة بريده الإلكتروني على مجلد خاص بذلك وبحيث تكون جميع الرسائل الإلكترونية محفوظة على مكان واحد عبر الجهاز.

10. يقوم فريق الدعم الفني بتفعيل خاصية التوقيع الإلكتروني على أجهزة جميع مستخدمي البريد الإلكتروني، بحيث أن الرسائل الإلكترونية تكون موقعة من المرسِل ومحمية تماماً من التغيير أثناء النقل وبالتالي لا يمكن للمستخدم إنكار محتواها فيما بعد.

11. يتم إرسال المرفقات الرسمية للجهات الرسمية بالتوافق مع قائمة تصنيف المعلومات المُتبعة في المؤسسة، وبشكل يتماشى مع درجة سرية هذه الوثائق.

الخاتمة

في عصر التواصل الرقمي يُعتبر حماية البريد الإلكتروني أمراً بالغ الأهمية وذلك لأهمية هذه التقنية في تبادل المعلومات والتواصل سواء بالنسبة للأفراد أو حتى للمؤسسات، ويتم ذلك باتباع التدابير الأمنية الرقمية السليمة والالتزام بسياسات الأمن السيبراني والتركيز بشكل كبير على توعية المُستخدِم بالتهديدات والمخاطر السيبرانية التي يُمكن شنها من خلال البريد الإلكتروني كالتصيدُ الاحتيالي بواسطة أساليب الهندسة الاجتماعية المختلفة.

نتمنى لكم السلامة في

العالم

الرقمي.