توعية أمنية Cybersecurity Awareness

أمن وسائل التواصل الاجتماعي Social Media Cybersecurity

مركز أمن المعلومات

دائرة الاستجابة للطوارئ المعلوماتية

11/15/2023

الهيئة الوطنية لخدمات تقانة المعلومات
National Authority for IT Services

أمن وسائل التواصل الاجتماعي

Social Media Cybersecurity

مقدمة:

مع تزايد شعبية منصات التواصل الاجتماعي وترابطها مع بعضها البعض أصبح استخدامها جزءاً أساسياً للتواصل اليومي لمعظم الجهات والشركات والأفراد في جميع أنحاء العالم سواء لجذب العملاء أو لتقديم الخدمات أو لنشر الإعلانات أو لمشاركة المعلومات والملفات والأفكار والآراء وتبادل الرسائل وغيرها من المحتوى المرئي والصوتي والمقروء.

لذلك أصبح من الأهمية بمكان أن يتم استخدامها بعناية ومسؤولية واتخاذ كافة الاجراءات اللازمة لحماية البيانات (خصوصية وسرية وسلامة المعلومات) الخاصة بحساباتكم على منصات وسائل التواصل الاجتماعي، مثل إعدادات الخصوصية، ومصادقة الحساب، والوعي بالتصيّد الاحتيالي، وتطبيقات وأذونات تطبيقات الطرف الثالث (مثل الالعاب)، والتصفح الآمن.

وعليه قمنا بإعداد هذا المقال موضحين فيه المخاطر والتهديدات الأمنية المرتبطة بأمن وسائل التواصل الاجتماعي، وفوائد اتخاذ الإجراءات الأمنية لحماية بياناتكم، بالإضافة إلى نصائح حول كيفية حماية المعلوماتك الشخصية والبقاء آمناً على مواقع التواصل الاجتماعي، نرجو الاهتمام والقراءة بعناية والعمل بالنصائح المضمنة.

المخاطر الشائعة والتهديدات المرتبطة بأمن وسائل التواصل الاجتماعي

يعد البقاء على اطلاع جيد بهذه المخاطر وتنفيذ الاحتياطات الأساسية بشكل فعال أمرًا ضروريًا لحماية نفسك ومعلوماتك عند استخدام منصات التواصل الاجتماعي.

- الوصول غير المصرح به: التسلل غير المصرح به لحسابات وسائل التواصل الاجتماعي الشخصية أو الخاصة بالشركة من قبل مجرمي الانترنت أو غيرهم من الجهات الفاعلة السيئة، مما قد يؤدي إلى اختراق الحسابات وتسريب البيانات أو الاستخدام غير المشروع.
- هجمات التصيد الاحتيالي: محاولة خادعة للحصول على معلومات حساسة، مثل كلمات المرور أو التفاصيل الشخصية، من خلال انتحال هوية كيانات حقيقية أو إنشاء ملفات تعريف مزيفة.

- البرامج الضارة والفيروسات: يمكن للروابط الضارة أو الملفات المصابة نشر البرامج الضارة والفيروسات عبر منصات التواصل الاجتماعي، مما يعرض أمان الأجهزة والشبكات للخطر.
- انتهاكات الخصوصية: يمكن أن تؤدي إعدادات الخصوصية غير الكافية/ غير المضبوطة أو المشاركة غير المقصودة للمعلومات الشخصية إلى تعريض الأفراد لانتهاكات الخصوصية أو سرقة الهوية أو التعقب عبر الإنترنت،
- الإضرار بالسمعة: يمكن أن يؤدي المحتوى غير المناسب أو مشاركة الصور الشخصية أو التعليقات السلبية أو المضايقات عبر الإنترنت إلى الإضرار بسمعة الفرد أو الشركة، مما يؤثر على الثقة والمصداقية والسمعة، وكمثال عن ذلك يمكن استخدام الصور الشخصية من خلال تقنيات التزييف العميق للإضرار بالسمعة وتلفيق فديوهات مزيفة.
- اختطاف الحساب: الاستيلاء غير المصرح به على حسابات وسائل التواصل الاجتماعي، غالبًا لأغراض ضارة، مما يؤدي إلى سرقة الهوية، أو نشر محتوى ضار، أو أنشطة احتيالية أو جرائم إلكترونية انطلاقاً من الحساب المخترق.
- استخراج البيانات وتتبعها: تقوم منصات وسائل التواصل الاجتماعي بجمع وتحليل بيانات المستخدم للإعلانات المستهدفة أو لأغراض أخرى، مما قد يعرض الخصوصية والمعلومات الشخصية للخطر.
- التنمر عبر الإنترنت: التحرش أو الترهيب أو السلوك المسيء الموجه للأفراد على منصات التواصل الاجتماعي، مما يسبب ضررًا نفسيًا وعاطفيًا.
- الحسابات المزيفة وعمليات الاحتيال والهندسة الاجتماعية: إنشاء ملفات تعريف مزيفة أو نماذج احتيالية على وسائل التواصل الاجتماعي، تهدف إلى خداع المستخدمين لتقديم معلومات شخصية أو تفاصيل مالية أو الانخراط في أنشطة احتيالية.

فوائد أمن وسائل التواصل الاجتماعي **للأفراد**

1. يحمي الخصوصية الشخصية: وذلك من خلال حمايته للمعلومات الحساسة ومنع الوصول غير المصرح به ، والحماية من سرقة الهوية والاحتيال وإساءة الاستخدام عبر الإنترنت، ومن خلال تقييد الوصول إلى الأفراد الموثوق بهم، وبذلك يضمن مستوى أعلى من الخصوصية.
2. يعزز السمعة عبر الإنترنت: فهو يسمح بتحكم أفضل في تواجد الشخص عبر الإنترنت، ويحمي من الإضرار بالسمعة بسبب المحتوى غير المناسب أو المضايقات. علاوة على ذلك، فإنه يخلق تجربة أكثر أمانًا ومتعة عبر الإنترنت من خلال تقليل التفاعلات مع المتنمرين عبر الإنترنت.

فوائد أمن وسائل التواصل الاجتماعي **للشركات**

1. يحمي بيانات الشركة الحساسة: حيث يلعب أمن وسائل التواصل الاجتماعي دورًا حيويًا في حماية الملكية الفكرية. فهو يمنع الوصول غير المصرح به ويعمل بمثابة درع ضد خروقات البيانات. ويعد هذا أمرًا بالغ الأهمية بشكل خاص للشركات التي تعتمد بشكل كبير على منصات التواصل الاجتماعي لتسويق البيانات القيمة ومشاركتها.
2. يخفف من مخاطر سمعة العلامة التجارية: تعد مراقبة التهديدات الأمنية ومعالجتها بشكل فعال أمرًا أساسيًا لحماية سمعة العلامة التجارية. فهو يساعد على تقليل مخاطر الوصول غير المصرح به إلى حسابات وسائل التواصل الاجتماعي، مما يضمن حماية الأصول القيمة. ومن خلال إعطاء الأولوية للأمن، تعزز الشركات مصداقيتها وتعزز الثقة بين العملاء وأصحاب المصلحة.
3. يساعد على البقاء متوافقًا مع اللوائح والمعايير: يعد تنفيذ ممارسات أمنية قوية أمرًا ضروريًا للامتثال للوائح حماية البيانات، والحفاظ على ثقة العملاء ودعم معايير الصناعة. ويمكن للشركات حماية نفسها من العواقب القانونية والمالية المحتملة، وضمان سلامة البيانات الحساسة والحفاظ على مكانة مرموقة في السوق من خلال إعطاء الأولوية للأمن السيبراني.

الهيئة الوطنية لخدمات تقانة المعلومات
National Authority for IT Services

نصائح حول كيفية حماية معلوماتك الشخصية والبقاء آمناً على مواقع التواصل الاجتماعي

من الممكن أن تكون أنت من شارك بيانات المرور الخاصة بك مع المحتالين، لذلك كن دائما على وعي

1. اقبل دعوات الصداقة من الأشخاص الذين تعرفهم فقط.
2. قم بتحديث برامج التواصل الاجتماعي.
3. لا تستخدم شبكة انترنت مفتوحة للعموم.
4. استخدم كلمة مرور قوية (8 محارف (رموز وارقام وأحرف كبيرة وأحرف صغيرة).
5. غير كلمات مرورك بشكل منتظم.
6. لا تستخدم كلمات مرور وأسئلة أمان تتضمن معلومات معروفة عنك.
7. لا تستخدم نفس كلمة المرور لجميع حساباتك على منصات التواصل الاجتماعي أو حساب بريدك الإلكتروني.
8. استخدم خاصية المصادقة الثنائية العوامل لرفع مستوى الحماية.
9. استخدم جهازك فقط لتصفح حساباتك.
10. ابق إعدادات الخصوصية الخاصة بك على أعلى مستوى ممكن.
11. كن حكيما وفكر جيدا قبل نشر أي شيء على الانترنت واعتبر أي معلومة تنشرها تبقى دائمة على الانترنت.
12. لا تتسرع في النقر على أي رابط يغريك بمال أو عمل أو يرهبك باختراق حسابك واستعادته من خلال النقر على الرابط أو أي من الأساليب المماثلة، حتى لو كانت تأتي من صديق أو قريب (قد لا يعلم أن الرابط خطير، أو ربما تم اختراقه) فقط قم بحذف الرابط. لن يتم إرسال أي شيء مهم لك بهذه الطريقة مال أو فرصة عمل أو أي من المغريات! من المرجح أن تحتوي الروابط التي لم تطلبها على فيروسات من شأنها أن تضر جهازك أو تسمح للأشخاص بالدخول إلى جهازك لسرقة معلوماتك وأموالك وهويتك.
13. لا تدخل في مسابقات مشبوهة على الانترنت باستخدام بريدك الالكتروني وكلمات مرورك.
14. لا تحتفظ بتفاصيل حسابك على وسائل التواصل الاجتماعي في أماكن يمكن للآخرين الوصول إليها.
15. إذا تلقيت رسالة عبر الإنترنت تقول إنها من الحكومة أو من شركة، فلا ترد بمعلوماتك الشخصية.
16. لا تثق برسائل البريد الالكتروني أو الرسائل النصية التي تطلب إعادة تعيين كلمة المرور إذا لم تطلبها انت بنفسك ! ولا ترسل أكواد التحقق أو التي تردك عبر الرسائل النصية أو البريد الإلكتروني لأي أحد.
17. احذر ولا تصدق كل شيء واحصل على معلوماتك من الصفحات الرسمية والموثوقة.
18. لا ترسل الأموال ولا كلمة المرور الخاصة بك إلى أي شخص تلتقي به من مواقع الانترنت.

19. قم على الفور بحظر أي شخص ينشر شيئ مهدد على أي من حساباتك .لا ترد .لا تكتب أشياء فظة أو عدائية قد تجعلك أكثر من هدف. قم بالإبلاغ عن التهديدات الشخصية للشرطة وموقع التواصل الاجتماعي الذي تم نشره عليه.

20. في حال تعرض حسابك للاختراق:

حاول استرداد حسابك باستخدام أسئلة الأمان وآليات الاسترداد المتاحة، وتأكد من جمع الأدلة عن الحادث، واطلب المساعدة من أفراد أسرتك وجهات إنفاذ القانون.

21. وضع سياسة تنظيمية لوسائل التواصل الاجتماعي:

- تقديم تعليمات واضحة حول كيفية إنشاء وإدارة حسابات وسائل التواصل الاجتماعي الرسمية.
- من لديه حق الوصول إلى حسابات وسائل التواصل الاجتماعي؟
- من الذي يتم السماح له بالنشر ومن يحتاج إلى الموافقة على منشوراته؟
- ما المعلومات التي يجب عدم مشاركتها على وسائل التواصل الاجتماعي؟
- إذا نشرت صورًا أو معلومات الموقع أو أية معلومات تعريفية أخرى عن موظفيك أو شركائك أو الحاضرين في الحدث، فهل طلبت إذنهم وهل وضعوا المخاطر في الاعتبار؟

22. ضبط إعدادات الخصوصية والأمان بشكل صحيح:

- هل ترغب في مشاركة منشوراتك مع العامة أو مع مجموعة معينة من الأشخاص؟
- هل يجب أن يتمكن أي شخص من التعليق أو الرد أو التفاعل مع رسائلك أو منشوراتك؟
- هل يجب أن يتمكن الأشخاص من العثور عليك وعلى منظمتك باستخدام عنوان البريد الإلكتروني أو رقم الهاتف (الشخصي أو المتعلق بالعمل)؟
- هل ترغب في مشاركة موقعك تلقائيًا عندما تقوم بالنشر؟
- حظر حسابات تسيء لك.
- هل ترغب في حظر كلمات معينة أو علامات كلمات رئيسية؟

تذكّر: لا تحتاج أبداً إلى إعطاء بيانات شخصية مهمة، مثل أرقام الهوية أو أرقام البنوك أو كلمات المرور أو عنوانك على مواقع التواصل الاجتماعي أو عملك ومكانه. وأنّ لكل موقع من مواقع التواصل الاجتماعي إعدادات خصوصية وسلامة مختلفة.

23. الشعار أو العلامة التجارية: ضع إرشادات لضمان ظهور هوية مؤسستك أو علامتك التجارية في منشوراتك على وسائل التواصل الاجتماعي.

24. إرشادات المحتوى: حدّد ما هو مقبول وما يجب تجنبه عندما يتعلق الأمر بالمحتوى الذي تشاركه.
25. الاعتبارات القانونية والأخلاقية: تناول موضوعات مهمة مثل حقوق الطبع والنشر ومتطلبات الخصوصية والإفصاح.
26. المصادقة الثنائية: تعد إضافة المصادقة الثنائية أمرًا بالغ الأهمية للأمان عبر الإنترنت لأنها تخفف من المخاطر المرتبطة بكلمات المرور المخترقة. إذا تم اختراق كلمة المرور أو تخمينها أو حتى تصيدها، فإنها لم تعد تمنح المتسللين إمكانية الوصول. وبدون توفر العامل الثاني، تصبح كلمة المرور وحدها عديمة الفائدة.
27. تقييد الوصول إلى أفراد محددين: يتضمن تأمين حساباتك على وسائل التواصل الاجتماعي تقييد الوصول إليها. على الرغم من أن التهديدات الخارجية تشكل مصدر قلق، إلا أن خروقات البيانات يمكن أن تنشأ أيضًا من داخل مؤسستك. لا يحتاج كل فرد في فريقك إلى معرفة كلمات مرور الحساب، حتى لو كانوا يتعاملون مع مهام الوسائط الاجتماعية. يمكنك تعيين أدوار مختلفة لأشخاص مختلفين مع ضمان اختلاف الأذونات بناءً على كل دور. يساعد القيام بذلك في تقييد الوصول إلى البيانات أو الميزات الحساسة، كما يسمح بمساءلة أفضل. ومن الضروري أيضًا تنفيذ نظام يمكّنك من إلغاء الوصول إلى الحساب عندما يغادر الموظفون أدوارهم أو يغيرونها.
28. أتمته سير عمل الموافقة: لا يتعين عليك منح حق الوصول للنشر لكل شخص يدير حساباتك الاجتماعية. يمكنك تبسيط سير العمل الخاص بك عن طريق الاستفادة من عمليات الموافقة. سيكون لدى المعتمدين فقط المرونة اللازمة لتعديل المحتوى أثناء مرحلة الموافقة، وإجراء تعديلات سريعة دون الحاجة إلى رفض الرسالة وإعادة تركيبها. وهذا لا يؤدي إلى تحسين الكفاءة وتوفير الوقت فحسب، بل يعمل أيضًا كاستراتيجية دفاعية للحد من عدد الأشخاص الذين يحتاجون إلى القدرة على النشر.
29. منح شخص متخصص زمام الأمور: ليكون الوصي اليقظ لوجودك الاجتماعي أمرًا بالغ الأهمية لإدارة المخاطر. ويتولى هذا الشخص مسؤوليات مختلفة مثل:
    - تطوير وتنفيذ السياسة الأمنية.
    - مراقبة تواجد العلامة التجارية على وسائل التواصل الاجتماعي.
    - إدارة الوصول والأذونات.
    - مواءمة استراتيجيات وسائل التواصل الاجتماعي مع الأهداف الأمنية.
    - التعاون مع قسم تكنولوجيا المعلومات.
    - تدريب أعضاء الفريق على الممارسات الأمنية.

30. الاستجابة السريعة للحوادث الأمنية: عادة، يتم شغل هذا الدور بواسطة شخص متخصص، من المهم الحفاظ على تعاون قوي مع قسم تكنولوجيا المعلومات لمعالجة المخاطر المحتملة بشكل فعال. ويجب أن يعتمد أعضاء الفريق على هذا الشخص للحصول على إرشادات في حالة حدوث أي أخطاء على وسائل التواصل الاجتماعي قد تعرض الشركة للخطر، مما يتيح استجابات سريعة ومناسبة.
31. تنفيذ نظام الإنذار المبكر: ضمان المراقبة الشاملة لجميع القنوات الاجتماعية الخاصة بك، بما في ذلك القنوات المستخدمة بشكل متكرر والخاملة. كما ذكرنا سابقًا، يوصى بتعيين شخص مسؤول للتحقق من صحة جميع منشورات الحساب، بدءًا من إسنادها إلى تقويم المحتوى الخاص بك. تحقق من أي منشورات غير متوقعة، حتى تلك التي تبدو مشروعة وتنحرف عن خطة المحتوى الخاصة بك. ويمكن أن يشير إلى خطأ بشري أو خرق أمني محتمل.

استخدم استراتيجية مراقبة وسائل التواصل الاجتماعي الخاصة بك لتحديد ومعالجة الحسابات الوهمية والمخادعة، والإشارات غير المناسبة للعلامة التجارية من قبل الموظفين أو الآخرين المرتبطين بشركتك، والمحادثات السلبية المحيطة بعلامتك التجارية.

32. ابقَ على اطلاع: يعد التحقق بانتظام من مشكلات أمان الوسائط الاجتماعية الجديدة أمرًا بالغ الأهمية لمعالجة التهديدات ونقاط الضعف الناشئة بشكل فعال. يتطور المشهد الرقمي باستمرار، ويتيح البقاء منتبهًا التعرف الفوري على المخاطر المحتملة والتخفيف من حدتها.
33. إجراء عمليات التدقيق الأمني:

- قم بمراجعة إعدادات خصوصية الشبكة الاجتماعية كل ثلاثة أشهر للتكيف مع أي تحديثات قد تؤثر على خصوصية حسابك والتحكم في استخدام البيانات.
- تقييم وتحديث امتيازات الوصول والنشر لمنصة وحسابات إدارة الوسائط الاجتماعية الخاصة بك، وإلغاء الوصول للموظفين السابقين وتعديل الأدوار حسب الحاجة.
- ابق على اطلاع حول التهديدات الأمنية الأخيرة لوسائل التواصل الاجتماعي من خلال الحفاظ على علاقة جيدة مع فريق تكنولوجيا المعلومات لديك ومراقبة منافذ الأخبار الرئيسية.
- قم بإجراء مراجعة ربع سنوية لسياسة وسائل التواصل الاجتماعي الخاصة بك للتأكد من أنها تتطور مع تغير شعبية الشبكة والممارسات الأمنية والتهديدات الناشئة، وبالتالي تعزيز أمان حساباتك الاجتماعية.

دمتم بأمان