



الرسائل غير المرغوب فيها

لكل سيناريو، حدّدوا ما إذا كانت الرسالة بريداً غير مرغوب فيه، وما إذا كان ينبغي عليكم مشاركة أي معلومات مع المرسل. يُرجى كتابة إجاباتكم على كل سؤال في المكان المخصّص لذلك.

السيناريو الأول: وصلتكم رسالة إلكترونية من محام يُخبركم أن قريباً لكم من بعيد قد تبرّع لكم بمبلغ من المال. يقول نص الرسالة، "لاستلام المبلغ المالي، فضلاً أرسلوا لي رقم الحساب البنكي ورقم التوجيه البنكي الخاصين بكم، حتى نتمكن من إتمام الإيداع."

هذه على الأرجح رسالة إلكترونية غير مرغوب فيها. حتى لو استخدم المرسل الاسم الصحيح لقریبكم، إلا أنهم ربما ليسوا من يدعون. يمكن أن يكون المرسل قد حصل على المعلومات المتعلقة بصلة القرابة من خلال وسائل أخرى. مشاركة معلومات حساباتكم البنكية بنطوي دائماً على مخاطرة، ويجب توخّي الحرص عند القيام بذلك. لا ترسلوا معلوماتكم أبداً إلى شخص ما إلا إذا اتصلتكم بهم أولاً، وحتى بعد ذلك يجب توخّي الحذر للغاية. مثلاً، قد لا تكون فكرة جيدة أن ترسلوا معلوماتكم عبر رسالة إلكترونية، لأنها غير مشفرة. لهذا السبب تمتلك العديد من المستشفيات ومكاتب المحاماة والبنوك مواقع إلكترونية خاصة للتواصل معكم.

السيناريو الثاني: أرسل لكم صديقكم/صديقكم رسالة نصية، يبلغونكم فيها أنهم يحاولون البحث عن صورة عرضتموها عليهم من قبل، ولكن ليس لديهم الإذن بالاطلاع عليها. ولكنكم غير قادرين على الدخول إلى جهاز الكمبيوتر الخاص بكم في الوقت الحالي لإرسال الصورة لهم. يجيبكم الصديق أو الصديقة، "يمكنني تسجيل الدخول إلى حسابكم بسرعة شديدة لتنزيل الصورة - ما هي كلمة مرور حسابكم؟"

في حين أن هذه ليست رسالة غير مرغوب فيها، إلا أنه يجب ألا تشاركوا كلمات المرور الخاصة بكم مع أشخاص آخرين. بمجرد حصولهم على كلمات مروركم، يمكنهم قفل حسابكم أو الوصول إلى حسابات أخرى على الإنترنت باستخدام نفس كلمة المرور. بالإضافة إلى ذلك، إذا رأى طرف ثالث أو مخترق أو متفحرج رسالتكم، فيمكن لعدد أكبر من الأشخاص الدخول إلى حساباتكم بدون علمكم.

السيناريو الثالث: وصلتكم رسالة إلكترونية من مدرستكم، تزعم أنه قد تم اختراق العديد من حسابات الطلاب. ويقول نص الرسالة، "لقد اكتشفنا مؤخراً أن العديد من حسابات الطلاب قد تعرّضت للاختراق. نعتذر عن ذلك، ونؤكد لكم أننا نعمل على حل المشكلة. لإعادة تعيين حسابكم، يُرجى الرد على هذه الرسالة الإلكترونية باستخدام اسم المستخدم وكلمة المرور."

من الشائع عدم مطالبة المستخدمين بمثل هذه المعلومات. حتى إذا بدا لكم المرسل مشرعاً، يجب أن تفترضوا أن أي رسالة إلكترونية تطلب كلمة مروركم هي رسالة غير مرغوب فيها.

السيناريو الرابع: وصلتكم رسالة إلكترونية من البنك حيث تملكون حساباً مشرعاً. يقول نص الرسالة أن بيانات البنك قد تعرّضت للاختراق، وأنه يجب عليكم تسجيل الدخول لتغيير كلمة مرور حسابكم في أقرب وقت ممكن، وتغيير كلمات المرور على أي حسابات تحمل كلمة المرور ذاتها.

الإجراء الصحيح هو فتح نافذة متصفح جديدة، ومن ثم الدخول إلى الموقع كما تفعلون عادةً. عادةً ما تقوم الشركة أو البنك بذكر معلومات من هذا النوع (أي أنه قد تم اختراق الحسابات) على البوابة الخاصة بخدمة العملاء. يجب أن تكون التعليمات الموجودة على البوابة قابلة لاتباعها بأمان. كما هو الحال في السيناريو الثالث، لن تطلب أي جهة مشروعة بيانات اعتماد الحساب منكم عبر رسالة إلكترونية.

المصدر: يستضيف Meta هذا المحتوى ويتضمن حالياً موارد التعلم المستمدة من مشروع *Youth and Media* في مركز

Berkman Klein Center for Internet & Society في جامعة هارفارد، بموجب ترخيص *Creative Commons Attribution*

ShareAlike 4.0 International. يمكنكم الاستفادة من هذا المحتوى، بما في ذلك نسخ الأعمال المشتقة وإعدادها، سواء كانت تجارية أو غير تجارية، طالما

أنكم تتسبون مشروع *Youth and Media* كمصدر أصلي وتتبعون الشروط الأخرى للترخيص، وتشاركون أي أعمال أخرى بموجب نفس الشروط.