

نصائح السلامة:

حفاظا على أمنكم وسلامتكم عند استخدام الشبكة العالمية

تولي دائرة الشؤون التربوية والثقافية بوزارة الخارجية الأمريكية بالغ الأهمية لمسائل الأمن والسلامة المتعلقة باستخدامكم لشبكة الإنترنت، ولذلك نرجو أن تتكرموا بالنظر في نصائح السلامة التالي ذكرها عند استخدامكم للمواقع الشبكية الاجتماعية والبريد الإلكتروني والإنترنت:

1. لا تنشروا إطلاقا أي معلومات اتصال شخصية على شبكة الإنترنت، ولا تقوموا في أي وقت بإدراج عنوان البريد الإلكتروني أو رقم الهاتف في أي موقع إلكتروني عام مثل الصفحة التعريفية الخاصة بكم أو في أي مدونة أو منتدى أو تعليق على إحدى صوركم.
2. إذا كنتم تتمتعون بعضوية أحد المواقع الشبكية الاجتماعية، ننصحكم بإعادة انتباه مكثف لإعدادات الخصوصية المتعلقة بشخصكم، علما أن هذه الإعدادات تسمح لكم بتحديد مدى البيانات الشخصية التي يتم الكشف عنها وكذلك بتحديد الجهات التي تستطيع الاطلاع على هذه البيانات.
3. افحصوا بعناية أي شيء تريدون نشره على المواقع الشبكية الاجتماعية. وننصحكم بالامتناع عن نشر أي صورة أو فيديو أو نص على هذه المواقع إذا كان اطلاع أحد أفراد عائلتكم أو أحد منسوبي جهة عملكم على مثل هذه المواد سيؤدي إلى نوع من الإحراج لكم.
4. قبل إضافة أي ملحق لربط ملف التعريف الخاص بكم ("الودجة"—أحد التطبيقات للتشارك الإلكتروني مع الآخرين)، ننصحكم بالنظر فيما إذا كنتم فعلا تريدون تمكين الشخص الذي قام بإنشاء هذا الملحق من الوصول إلى الصفحة التعريفية وإلى البيانات الخاصة بأنشطتكم في الموقع الشبكي الاجتماعي. ولا تتسوا أن المواقع الشبكية الاجتماعية عادة لا تستطيع التحكم في هذه الملحقات، ولذلك ننصحكم بتوخي الحذر عند استخدام هذا النوع من الأدوات.
5. قوموا بإبلاغ إدارة الموقع الشبكي عن أية انتهاكات لشروط الاستخدام الخاصة بذلك الموقع. وعموما تتوفر في كافة المواقع الشبكية الرصينة، بما في ذلك المواقع الاجتماعية منها، وسيلة ما تمكنكم من القيام بالتبليغ عن الانتهاكات.
6. إن البريد الإلكتروني قابل لاستخدامه بغرض نشر البرامج الخبيثة أو للحصول على بياناتكم الشخصية بغية ارتكاب أعمال الاحتيال. ولحماية أنفسكم والحاسوبات التي تستخدمونها، نرجو أن تتكرموا بمراعاة المبادئ التوجيهية المبينة أدناه:

- يجب توخي بالغ الحذر عند التعامل مع الرسائل الإلكترونية والمكالمات الهاتفية التي تتلقونها دون سابق طلب من أفراد يرغبون في الحصول على بيانات شخصية. وإذا ادعى شخص غير معروف لكم أنه يتبع لهؤسسة مشروعة، ننصحكم بالسعي للتحقق من هوية ذلك الشخص بصفة مباشرة عند تلك المؤسسة.
- عندما تردون على أية رسائل إلكترونية أو مكالمات هاتفية لم تتطلق من مبادرتكم أنتم، يجب أن تتجنبوا في جميع الأوقات الكشف عن بيانات شخصية أو مالية (مثل أرقام بطاقات الائتمان والرقم السري الخاص ورقم التعريف).
- لا تقوموا بإرسال أية بيانات شخصية أو مالية عبر الانترنت قبل التحقق من الوضعية الأمنية للموقع الشبكي المعني. (تبدأ عناوين المواقع الشبكي الآمنة دائما بعبارة: "https://")
- افحصوا عناوين المواقع الشبكية الموجودة في أعلى الشاشة دائما بعناية. وقد تبدو المواقع الشبكية الخبيثة تماما مثل الموقع الأصلي المشروع، إلا أن العنوان قد يستخدم تركيبة أحرف مختلفة أو نطاقا بديلا (مثل: ".com" بدلا من: ".net").
- قوموا بتوفير الحماية اللازمة لحواسيبكم وسائر الحواسيب الأخرى التي تستخدمونها، وذلك عن طريق فحص جميع الوسائط المنقولة مثل محركات فلاش والأقراص المدمجة أو الرقمية قبل فتح أية ملفات موجودة في مثل هذه الوسائط، وذلك بغية التحقق من عدم وجود أية فيروسات داخل هذه الملفات وكذلك عن طريق فحص كافة الملحقات التي تتلقونها عبر البريد الإلكتروني قبل فتح أي من هذه الملحقات.
- لا تقبلوا أو تفتحوا أية ملفات تنفيذية واردة إليكم عبر البريد الإلكتروني (والمؤشر عليها في نهاية اسم الملف بالأحرف الثلاثة: ".exe")، علما أن مثل هذه الملفات التنفيذية قد تكون ذات خطورة بالغة.

