دليل الإرشادات الأمنية لاستخدام شبكات التواصل الاجتماعي

يوليو 2024

الإصدار والتوزيع:

جهة الإصدار	البريد الالكتروني	تاريخ الإصدار
المديرية العامة للسياسات والحوكمة وزارة النقل والاتصالات وتقنية المعلومات	Governance@mtcit.gov.om	2024

سجل الوثيقة:

النسخة	التاريخ	جهة الإصدار	الملاحظات
0.1	2016	هيئة تقنية المعلومات	
0.2	2024	وزارة النقل والاتصالات وتقنية المعلومات	

قائمة النشر:	
.1	جميع وحدات الجهاز الإداري للدولة
.2	الموقع الإلكتروني للوزارة

محتويات الدليل

التعاريف

الوزارة:
وزارة النقل والاتصالات وتقنية المعلومات

وحدات الجهاز الإداري للدولة:
يقصد بها الوزارات، والأجهزة العسكرية والأمنية، والمجالس، وغيرها من الوحدات التنفيذية التي تستمد سلطتها من الدولة، أيا كان اسمها، ويشمل ذلك الأشخاص الاعتبارية العامة القائمة على إدارة مرفق عام خدمي أو اقتصادي، كالهيئات العامة، والمؤسسات العامة. (المعرفة وفقا للمرسوم السلطاني رقم ٧٥ / ٢٠٢٠ في شأن الجهاز الإداري للدولة)

الهندسة الاجتماعية:
تعبير عن الوسائل غير التقنية أو منخفضة التقانة التي تستخدم لمهاجمة نظم المعلومات؛ كالكذب وانتحال الشخصية، والحيل، والابتزاز، والتهديدات.

المستفيد:
جميع فئات المجتمع ممن يقدم مشاركته العامة ويشمل المواطنين والمقيمين وزائري السلطنة وكذلك المنظمات غير الحكومية ومنظمات المجتمع المدني والجهات الحكومية والخاصة العاملة في السلطنة.

وسائل التواصل الاجتماعي:
هي مواقع تتيح للمستخدمين التواصل افتراضيا ومشاركة مختلف الاحداث مثل المناسبات اليومية، والقضايا السياسية والقضايا الاجتماعية. وتتم عملية نشر المحتوى بصيغ عدة مثل النصوص والصور وملفات الفيديو، ومن الأمثلة على وسائل التواصل الاجتماعي منصات: لينكد ان، فيسبوك، إكس، إنستجرام، وغيرها.

الحساب الرسمي:
الحساب الخاص بالوحدة على شبكات التواصل الاجتماعي الذي تم اعتماده، ويمثل الوجهة الإعلامية لتلك الوحدة، وينشر الأخبار والتصريحات الخاصة بها.

المقدمة

يشهد قطاع تقنية المعلومات والاتصالات في السلطنة تقدما ملحوظا. ليواكب التطورات التقنية المستمرة، حيث تم اتاحة العديد من الخدمات الحكومية عبر الإنترنت، كما وتزايد عدد الوحدات الحكومية التي تتواصل مع المستفيدين عبر وسائل التواصل الاجتماعي. وبالنظر إلى المخاطر المحيطة والحوادث الأمنية المتزايدة وتنامي التهديدات ضد مواقع وبرامج التواصل الاجتماعي، تسعى وزارة النقل والاتصالات وتقنية المعلومات بشكل دؤوب إلى الارتقاء بمستوى حماية الحسابات الرسمية المستخدمة في برامج التواصل الاجتماعي والمواقع والتطبيقات المرتبطة بها لحمايتها من الاختراق أو محاولات انتحال صفتها الرسمية لأهداف إساءة الاستخدام أو بث الإشاعات. حيث تعمل الوزارة على إنشاء وتحديث تعاميم التدابير والإرشادات الأمنية بما يتوافق مع المتطلبات والتحديات.

الغرض

تحديث التدابير والإرشادات الأمنية لحسابات التواصل الاجتماعي الرسمية لوحدات الجهاز الإداري للدولة والتطبيقات المتعلقة بها لتتوافق مع المتطلبات والتحديات الأمنية

نطاق التطبيق

جميع وحدات الجهاز الإداري للدولة.

الأهداف

يهدف هذا الدليل الى تعزيز أمن حسابات التواصل الاجتماعي لوحدات الجهاز الإداري للدولة وبما لا يتعارض مع السياسات الامنية الداخلية للوحدات أو تلك الصادرة من وزارة النقل والاتصالات وتقنية المعلومات.

حماية أمن حسابات مواقع التواصل الاجتماعي التابعة للوحدة

يوفر الدليل مجموعة من التدابير والإجراءات الأمنية لحماية الحسابات الحكومية في وسائل التواصل الاجتماعي (مرفق - 1)، وذلك للحد من التهديدات المحتملة والعمل على:

أولا: إدارة الحسابات

يتعين على الوحدة تحديد موظف معني بإدارة الحسابات الرسمية لها، ولا يتم ذلك إلا بعد إصدار قرار يفوضه بالقيام بهذه المهمة، على أن يحمل هذا القرار اسم الموظف والمسمى الوظيفي للموظف الذي سيتحمل مسؤولية إدارة هذا الحساب / الحسابات على أن تراعى الضوابط التالية عند اختيار الشخص المعني بإدارة حسابات الوحدة:

- إلمام الموظف بالمسائل التي سيتم التواصل بشأنها ومناقشتها مع الجمهور عبر الحسابات المختلفة.
- وعي الموظف بالأخطار المتعلقة بالهندسة الاجتماعية وطرق التحايل المحتملة وكيفية التصدي لها وتفادي الوقوع في أخطاء أمنية ذات صلة.
- امتلاك مهارات التواصل مع الجمهور وإتقان اللغة.
- الوعي التقني باستخدام مواقع التواصل الاجتماعي.
- استعداد الموظف للبقاء على اتصال مع الجمهور عبر قنوات التواصل الاجتماعي، والتعامل مع المواقف التي قد تتطلب الرد أو أي إجراء آخر في أي وقت من اليوم وعلى مدار الأسبوع (خارج الدوام الرسمي)
- إدراك الموظف بأنه يمثل الوحدة وبالتالي يمثل الحكومة في جميع ما يتم طرحه عبر حسابات الوحدة.
- التقيد بتوفير المعلومة الشافية والوافية للمستفيد.
- عدم استخدام حسابات الوحدة لأغراض شخصية لا تخدم أهداف الوحدة وتوجهاتها بأي شكل من الأشكال.
- عدم استخدام الحسابات الشخصية للتواصل مع الجمهور في كل ما يتعلق بشؤون الوحدة.

ثانيًا: إدارة المحتوى

- يتعين على الوحدة وضع آلية رسمية للنشر على وسائل التواصل الاجتماعي الخاصة بها على ان تكون متوافقة مع المتطلبات الامنية الصادرة في وثيقة إطار التصاميم الامنية للتطبيقات والخدمات الإلكترونية.
- يتعين أن يكون تواصل الوحدة مع المستفيد تواصلا موجها بعيدا عن العشوائية لضمان بث الرسالة بشكل صحيح وعلى وجه سريع ومباشر.
- يتعين على الموظف المعني بإدارة حسابات الوحدة تفضيل أو إعادة نشر التغريدات التي تضم أراء ومقترحات المستفيد لتحسين الخدمات المقدمة من الوحدة أو تطوير السياسات وبما لا يتعارض مع توجه الوحدة.

ثالثا: الخصوصية والسرية والأمان

يتعين على الموظف المعني بإدارة حسابات الوحدة التقيد بالآتي:

- اتخاذ جميع الاجراءات اللازمة لضمان حماية البيانات والمعلومات من اي اخطار محتملة كالاختراق او بث رسائل مغلوطة.
- التأكد من استخدام الموقع الرسمي أثناء محاولة تسجيل الدخول إلى حسابات الوحدة.
- التنسيق مع مكتب امن المعلومات والفريق التقني في الوحدة من أجل:
1- توفير الحماية اللازمة من مخاطر التصيد الاحتيالي، الهندسة الاجتماعية أو الهجمات على تطبيقات الويب.
- 2- أهمية توعية الموظفين بشأن الأخطار المتعلقة بالهندسة الاجتماعية وطرق التحايل المحتملة وكيفية التصدي لها وتفادي الوقوع في أخطاء أمنية ذات صلة.

إرشادات إدارة حسابات الوحدة في وسائل التواصل الاجتماعي

يجب اتخاذ الإجراءات والتدابير الأمنية الواردة في سياسة أمن المعلومات التي تتبعها الوحدة والتأكيد على تطبيق الاشتراطات التالية:

أولا: الأجهزة المستخدمة للوصول والتفاعل مع وسائل التواصل الاجتماعي

يتعين على الوحدة اتباع أفضل الوسائل والطرق لحماية الجهاز المستخدم لإدارة حسابات وسائل التواصل الاجتماعي التابعة لها عبر تطبيق ما يلي:

- يتعين استخدام جهاز مخصص لحسابات التواصل الاجتماعي المتعلقة بالوحدة، ويمنع استخدام الجهاز لأي أغراض أخرى.
- عدم استخدام الجهاز الشخصي الخاص بمشرف الحسابات لأغراض ادارة حسابات الوحدة

- تامين الحماية للجهاز عن طريق كلمة مرور قوية (لا نوصي باستخدام نمط أو رمز PIN وذلك لوجود وسائل وحيل كثيرة للوصول إليهما)
- تفعيل قفل الجهاز / الشاشة تلقائيا بعد ثوان معدودة من عدم الاستخدام.
- عدم تثبيت أي تطبيقات أخرى على الجهاز أو استخدام الانترنت أو البريد الإلكتروني لأغراض غير متعلقة بتعامل المؤسسة مع حسابات التواصل الاجتماعي، وذلك لتقليل احتمالية اختراق الجهاز أو إصابته بالبرمجيات الضارة.
- يتعين تحميل التطبيق الخاص بخدمة التواصل الاجتماعي من المتجر الرسمي للتطبيقات (مثل Apple Store أو Google Play) وعدم تحميل البرامج مجهولة المصدر من خارج المتاجر الرسمية.
- التأكد من تفعيل خاصية تعقب الجهاز والاقفال التلقائي في حالة الفقدان أو السرقة، لحماية الجهاز وتسهيل العثور عليه.
- الامتناع عن الدخول إلى الوظائف والتطبيقات غير الضرورية بالأجهزة أو تنزيل وتثبيت الألعاب وغيرها من التطبيقات المنتشرة في بعض برامج التواصل.
- عدم تحميل أي تطبيق طرف ثالث (مثل التطبيقات التي تحتوي على مزايا إضافية عن التطبيقات الرسمية)، أو التطبيقات غير الرسمية أو المشبوهة.
- عدم السماح لأي تطبيق آخر بالتزامن مع برامج التواصل الاجتماعي أو السماح لها باستخدام صلاحيات البرامج الرسمية.
- استخدام شبكة موثوق بها للاتصال بالإنترنت وتجنب الشبكات اللاسلكية العامة والمجانية.
- التأكد من تحديث نظام التشغيل والمتصفح وتطبيقات التواصل الاجتماعي بأحدث الإصدارات وبشكل مستمر ودوري لتجنب التهديدات الأمنية.
- التأكد من تحديث برامج مكافح الفيروسات والبرمجيات الضارة بشكل دوري.
- يمنع استخدام برامج VPN أو Proxy الخارجية للاتصال بالإنترنت.
- تجنب الدخول إلى الروابط المجهولة التي تظهر على صفحات الانترنت أو التي ترسل عبر البريد الالكتروني.
- الرقم المرتبط بالحساب يتبع للوحدة الحكومية وليس لمنتسبين معينين لتلك المهام، وذلك لسهولة استرداد الحسابات في حال فقدانها.

ثانيًا: خصائص كلمة المرور

تعتبر حماية البريد الالكتروني وكلمات المرور جزءا أساسيا لحماية حسابات الوحدة في مواقع التواصل الاجتماعي، ويتعين على الوحدة مراعاة التالي:

- استخدام كلمات مرور قوية ومختلفة لكل من البريد الالكتروني – المستخدم لفتح الحساب – وحسابات مواقع التواصل الاجتماعي، ويمنع إعادة استخدام كلمة المرور الواحدة على أي مواقع أو حسابات إلكترونية أخرى، وعلى الوحدة إعداد سياسة داخلية تحدد معايير خاصة بإنشاء واستخدام كلمة المرور، وكمثال لتلك المعايير الآتي:

1. إنشاء كلمة مرور لا تقل عن 12 حرف
2. استخدام مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز مثل (Da$2yN%gtu1^)
3. الالتزام بتغيير كلمة المرور بشكل دوري (كل شهر)
4. عدم تخزين او حفظ كلمات المرور على الأجهزة المستخدمة لإدارة الحسابات
5. إدخال بريد إلكتروني إضافي وأرقام الهاتف، ومعرفة بعض التفاصيل كتاريخ إنشاء الحساب، وتاريخ أخر تسجيل دخول، وأخر كلمة مرور مستخدمة، وإجابات الأسئلة الأمنية التي تم وضعها عند إنشاء الحساب، حيث سيتم لاحقا استخدام هذه التفاصيل لاسترجاع الحساب في حالة عدم تمكنك من تسجيل الدخول إليه.
6. عدم استخدام المعلومات الشخصية في كلمة المرور الخاصة بالحساب مثل أرقام الهواتف، وأعياد الميلاد، واسم المؤسسة، وأسماء الموظفين، .... الخ.

ثالثا: تفعيل خصائص التأمين الإضافية في بعض مواقع التواصل الاجتماعي

هناك مجموعة واسعة من برامج التواصل الاجتماعي التي توفر خصائص حماية إضافية للمستخدم، ويعتبر تفعيلها ذا أهمية قصوى من أجل زيادة مستوى الحماية المتعلقة بحسابات المؤسسة، وفيما يلي نستعرض تفعيل المصادقة الثنائية:
(Two Factor Authentication)

*يعتبر تفعيل هذه الخاصية أمًرا إلزاميا

- **فيس بوك:**

1- تفعيل تنبيهات تسجيل الدخول والمصادقة الثنائية (Login Alerts and Two- Factor Authentication):

https://ar-ar.facebook.com/help/909243165853369?helpref=about_content

2- تسجيل الخروج عن بعد (log out of Facebook):

https://ar-ar.facebook.com/help/211990645501187?helpref=faq_content

3- تجنب المحتوى غير المهم وعمليات الاحتيال (A void Spam and Scams):

https://ar-ar.facebook.com/help/1584206335211143/?helpref=hc_fnav

- **إكس:**

- تفعيل التحقق من تسجيل الدخول (login verification):
https://support.twitter.com/articles/20171414

- **انستجرام:**

- تفعيل المصادقة الثنائية (Two Factor Authentication):
https://help.instagram.com/566810106808145

- **يوتيوب:**

- تفعيل المصادقة الثنائية لحساب Gmail(Two Step Verification):
https://support.google.com/accounts/answer/185839?hl=en

- **سناب شات:**

- تفعيل المصادقة الثنائية (Two Factor Authentication):

https://support.snapchat.com/en-US/article/enable-login-verification

رابعًا: معايير التفاعل مع المستفيدين من حسابات الوحدة في وسائل التواصل الاجتماعي:

يتعين على الوحدة عدم الاستجابة لأي تهديد أو محاولة ابتزاز والتواصل مع الجهات المختصة مباشرة في حالة حدوث أي حادثة من هذا النوع، كما يمنع النشر أو التفاعل أو التعليق سواء تصريحا أو ضمنا بكل ما يحتوي على:

- الاستهانة بالمعتقدات الدينية أو الطائفية أو الإساءة إليها.
- التشهير أو القذف أو التمييز.
- النشر أو التعامل مع معلومات كاذبة وغير موثوقة.
- التعليق أو المشاركة في كل ما يدعم أو يحرض على القيام بأنشطة غير قانونية.
- التعليقات والمشاركات التي تخالف أي حقوق قانونية أو حقوق الملكية الفكرية.

خامسا: توثيق الحسابات الرسمية

تتيح خدمة توثيق الحسابات معرفة الحسابات الأصلية التي تمثل الجهات المعنية ذات الاعتبار ويتعين على الوحدة التقيد بالاشتراطات التالية عند توثيق الحساب الخاص بها:

- أن يعكس ملف الوحدة دور الوحدة ومجال عملها.
- أن تعبر صورة ملف الوحدة عن شعار الوحدة أو نشاطها.
- التأكد من توافق معرف الحساب مع اسم الوحدة أو القناة.
- توفير معلومات مفصلة عامة عن الوحدة تطابق الوصف على موقع الوحدة الإلكتروني وهذا ينطبق على جميع المعلومات العامة مثل أرقام الاتصال، عناوين البريد الإلكتروني، وساعات العمل الخ..
- عدم استخدام برامج زيادة المتابعين إطلاقا، لأنها تتعارض مع معايير التوثيق والشفافية.
- التحقق وتحديث ملف الوحدة للحساب جيدا قبل طلب التوثيق، لأن تغيير هذه المعلومات لاحقا قد يؤدي إلى إلغاء التوثيق.

- **طريقة توثيق الحسابات:**

1-لتوثيق حساب إكس اتبع الخطوات على الموقع الرسمي:

https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts

2- لتوثيق حساب فيس بوك اتبع الخطوات على الموقع الرسمي:

https://www.facebook.com/help/www/196050490547892?helpref=platform_switcher&ref=platform_switcher

3- لتوثيق حساب انستجرام اتبع الخطوات على الموقع الرسمي:

https://help.instagram.com/854227311295302

سادسا: في حالة اختراق أحد حسابات الوحدة

يتعين على الوحدة اتخاذ الاجراءات التالية في حال اختراق أحد حساباتها الرسمية على مواقع التواصل الاجتماعي:

1-القيام بإخطار الجهات المعنية بذلك على الفور.
2-استرجاع الحساب وتغيير كلمة السر مباشرة.
3-القيام باتخاذ الإجراءات التالية لوقف عملية الاختراق والحد منها:

- حذف أي منشور أرسل بدون علم.
- تنويه المتابعين بالاختراق ونفي ما قد تم نشره عبر الحساب إن وجد.
- حذف صلاحيات تطبيقات الطرف الثالث إن وجد.

سابعًا: الإجراءات المتبعة لاسترجاع الحسابات في بعض مواقع التواصل الاجتماعي

يتعين على الوحدة اتباع الخطوات التالية لاسترجاع حساباتها على وسائل التواصل الاجتماعي عن طريق الروابط المرفقة:

- **لاسترجاع حساب فيس بوك:**
https://ar-ar.facebook.com/help/117450615006715

- **لاسترجاع حساب إكس:**
https://help.twitter.com/ar/safety-and-security/twitter-account-hacked

- **لاسترجاع حساب انستجرام:**
https://help.instagram.com/149494825257596

- **في حالة اختراق أي حساب من حسابات جوجل أو الخدمات المرتبطة به حاول استرجاع الحساب عبر:**
https://support.google.com/accounts/answer/6294825?hl=ar

- **لاسترجاع حساب سناب شات:**
https://support.snapchat.com/en-US/a/reset-password

ثامنا: في حالة تعذر استرجاع الحساب

في حالة تعذر استرجاع الحساب بالطرق أعلاه، يتعين على الوحدة اتخاذ إجراء أخير وهو التواصل المباشر مع الموقع الرسمي والإبلاغ عن الامر.

- **فيس بوك:**

إذا تم استهداف أو اختراق مؤسستك عن طريق هجوم التصيد الإلكتروني، أرسل بلاغا إلى ممثل فيس بوك مع شرح القضية.
https://ar-ar.facebook.com/help/1216349518398524/?helpref=hc_fnav

- **إكس:**

إذا تم استهداف أو اختراق مؤسستك عن طريق هجوم التصيد الإلكتروني، تواصل على الفورمع إكس عن طريق الرابط التالي:
https://help.twitter.com/ar/forms/account-access

- **انستجرام:**

في حالة اختراق حساب إنستجرام فإن الخطوات أدناه توضح طرق استرجاعه.
https://help.instagram.com/149494825257596

- **يوتيوب:**

في حالة اختراق أي حساب من حسابات جوجل أ فإن الخطوات أدناه توضح طرق استرجاعه:
https://support.google.com/youtube/answer/76187?hl=ar&sjid=6782854619008142946-EU

- **سناب شات:**

في حالة اختراق الحساب، فإن الخطوات أدناه توضح طرق استرجاعه:
https://www.followchain.org/snapchat-account-compromised/#:~:text=How%20to%20fix%20Snapchat%20account%20compromised%201%201.,Send%20the%20form%20%26%20wait%20for%20Snapchat%E2%80%99s%20response

تاسعًا: الإصدارات ذات الصلة

- إطار التصاميم الأمنية للتطبيقات والخدمات الإلكترونية الحكومية (تعميم 2/ 2016).
- إطار التصاميم والإعدادات الأمنية للأجهزة الطرفية والأجهزة الذكية (تعميم 2017/3).

مرفق (1)

قائمة التدقيق

المهمة	الحالة	ملاحظات	التاريخ
مهام الإدارة في الوحدة:			
1- استخدام جهاز مخصص لحسابات التواصل الاجتماعي المتعلقة بالوحدة ويمنع استخدامه لأي أغراض أخرى			
2- وعي الموظف بالأخطار المتعلقة بالهندسة الاجتماعية وطرق التحايل المحتملة وكيفية التصدي لها وتفادي الوقوع في أخطاء أمنية ذات صلة			
3- تعهد الموظف بعدم استخدام الحسابات الرسمية لأغراض شخصية لا تخدم أهداف الوحدة وتوجهاتها بأي شكل			
4- تعهد الموظف بعدم استخدام الحسابات الشخصية للتواصل مع الجمهور في كل ما يتعلق بشؤون الوحدة			
5- توجد آلية رسمية للنشر على مواقع التواصل الاجتماعي مقرة من قبل الوحدة ومتوافقة مع التعاميم الصادرة في هذا الشأن			
مهام فريق تقنية المعلومات:			
1- فتح الحسابات باستخدام صندوق البريد الرسمي بالوحدة			
2- تفعيل قفل الجهاز/ الشاشة تلقائيا بعد ثوان معدودة من عدم الاستخدام			
3- عدم تثبيت أي تطبيقات أخرى على الجهاز أو استخدام الإنترنت أو البريد الالكتروني لأغراض غير متعلقة بتعامل الوحدة مع حسابات التواصل الاجتماعي			
4- تحميل التطبيق الخاص بخدمة التواصل الاجتماعي من المتجر الرسمي للتطبيقات (مثل Apple Store أو Google Play)			
5- التأكد من أن الجهاز لا يحتوي على أي برامج مجهولة المصدر أو أي برامج محملة من خارج المتاجر الرسمية			
6- تفعيل خاصية التعقب عبر الأقمار الصناعية والقفل الاحتياطي للجهاز في حالة فقدانه أو تعرضه للسرقة			
7- حظر الدخول إلى الوظائف والتطبيقات غير الضرورية بالأجهزة، أو تنزيل وتثبيت الألعاب وغيرها من التطبيقات المنتشرة في بعض برامج التواصل الاجتماعي			
8- حذف وعدم تحميل أي تطبيق طرف ثالث (مثل التطبيقات التي تحتوي على مزايا إضافية عن التطبيقات الرسمية)، أو التطبيقات غير الرسمية أو المشبوهة			
9- إلغاء وعدم السماح لأي تطبيق آخر بالتزامن مع برامج التواصل الاجتماعي أو السماح لها باستخدام صلاحيات البرامج الرسمية			
10-تعطيل خاصية تحديد المواقع في التطبيقات			

11-تفعيل تنبيهات تسجيل الدخول لجميع البرامج والتطبيقات			
12-تفعيل خصائص التأمين الإضافية، المصادقة الثنائية (Two Factor Authentication)			
13-التأكد من إدخال بريد إلكتروني إضافي وأرقام الهاتف لهدف استرجاع الحساب			
14-التأكد من أن إجابات الأسئلة الأمنية التي تم وضعها عند إنشاء الحساب معروفة			
15-توعية المستخدم بالمخاطر			
16-التأكد من وجود سجل يشمل بعض التفاصيل كتاريخ إنشاء الحساب			
17- إعداد سياسة داخلية لتحديد معايير إنشاء كلمة المرور واستخدامها			
مهام المستخدم:			
1- استخدام شبكة موثوق بها للاتصال، والامتناع عن استخدام الشبكات العامة والمجانية			
2- الالتزام بتحديث نظام التشغيل والمتصفح وتطبيقات التواصل الاجتماعي بأحدث الإصدارات وبشكل دوري			
3- تحديث برامج مكافح الفيروسات والبرمجيات الضارة بشكل دوري			
4- الامتناع عن استخدام برامج VPN أو البروكسي للاتصال بالإنترنت			
5- تجنب الدخول إلى الروابط المجهولة التي تظهر على صفحات الإنترنت أو ترسل عبر البريد الالكتروني			
6- عدم فتح ملفات أو فتح روابط من مصادر مجهولة أو مشبوهة			
7- كلمة مرور لا تقل عن 12 حرفا			
8- كلمة المرور تحوي مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز			
9- كلمة المرور لا تحوي حروفا متسلسلة ك "abcd1234"، أو متتاليات لوحة المفاتيح مثل "asdfghjkl"			
10-الالتزام بتغيير كلمة المرور بشكل دوري (كل شهر)			
11-الملف الشخصي يعكس دور الوحدة / الشخصية ومجال عملها			
12-تعبر صورة الملف الشخصي عن شعار الوحدة أو نشاطها			
13-تتوافر معلومات مفصلة عامة عن الوحدة تطابق الوصف على موقع الوحدة الإلكتروني، وهذا ينطبق على جميع المعلومات العامة مثل أرقام الاتصال، رسائل البريد الالكتروني، وساعات العمل			
14-الامتناع عن تغيير صورة الملف الشخصي، والمعلومات العامة، والموقع، وتفاصيل الاتصال، لان هذا الأمر قد يلغي توثيق الحساب دون ذكر أي سبب واضح! لذلك يجب التحقق وتحديث الملف الشخصي للحساب جيدا قبل طلب التوثيق، لأن تغيير هذه المعلومات لاحقا قد يؤدي إلى إلغاء التوثيق			
15-التأكد من سجل يشمل بعض التفاصيل: كتاريخ إنشاء الحساب، وتاريخ أخر تسجيل دخول، وأخر كلمة مرور مستخدمة			