



**رئاسة الجمهورية اللبنانية  
المديرية العامة**

نَعْمَيْمِ رَقْمٌ ع

الى مستخدمي شبكة الانترنت في المديرية العامة لرئاسة الجمهورية بشأن اختراق شبكة الانترنت

١. تتعرض الأجهزة والإدارات الرسمية لخروقات مختلفة منها سرقة المعلومات او تشفير المعلومات او ضرب الموقع الإلكتروني او سرقة حسابات التواصل الاجتماعي ...
  ٢. ان معظم الاختراقات (فوق ٧٠٪) هو سببه المستخدم بحد ذاته، أي طريقة عمله ومدى وعيه باستخدام الكمبيوتر خاصة لناحية البريد الإلكتروني وكيفية معالجته.
  ٣. ان المثال ادنى يعطينا صورة واضحة على احدى الطرق في كيفية الغش لاستدراج المستخدم للنقر وتحميل برامج خبيثة او سرقة معلوماته.... يمكن معاينته والاطلاع على الفروقات.
  ٤. لقد تعرضت مؤخراً عدة جهات رسمية للخرق إضافة الى بعض المصارف والمؤسسات الخاصة.
  ٥. ان الطريقة المثلثة لتلافي الخرق هي عبر اتباع الخطوات التالية:
    - ا. لا تقر على أي رابط وارد في أي بريد الكتروني، حتى لو تضمن تحذير او تنبيه مهما كان. الحل هو باستعمال Chrome او Edge وفتح حسابك مباشرة منه (Facebook, email.....).
    - ب. لا تفتح أي ملف او تحمل أي ملف وارد بالبريد الإلكتروني.
    - ج. تأكد من الرابط الموجود واقرأ المصدر، واذا كان بريد مستعجل وضروري اتصل وتتأكد من المصدر عبر وسيلة ثانية.
    - د. راجع الأخطاء الاملائية في العنوان وفي المضمون فهي دلالة على انه بريد ملغوم.
    - هـ. استعمل طريقة حماية إضافية (2 Factor authentication) كرقم الخلوي او Google/Microsoft Authenticator.
    - و. دائماً اطرح على نفسك السؤال التالي: هل يرددني بريد مماثل من هذا الشخص/الجهة او هذه المرة الأولى؟
    - زـ. انتبه من استعمال الـ Wi Fi في المقاهي او المطارات، فيمكن خرق جهازك عبر هكذا شبكات.



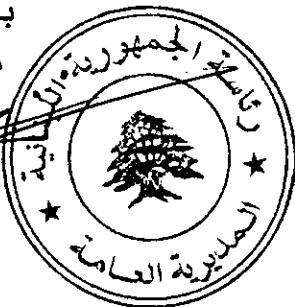
**رئاسة الجمهورية اللبنانية  
المديرية العامة**

- ح. انتبه من تشريح هاتفك مباشرة بکابل USB من المطار او المقاهي كونه وسيلة  
مباشرة للخرق.
- ٦- في جميع الحالات، مراجعة مكتب المعلوماتية.

بعدا في ٤/٨/٢٠١٤

مدير عام رئاسة الجمهورية

أنطوان شقير





رئاسة الجمهورية اللبنانية  
المديرية العامة

مثال لإحدى الطرق في كيفية الغش لاستدراج المستخدم للنقر وتحميل برامج خبيثة أو سرقة معلومات

## SPAM EMAIL

## SPOT THE DIFFERENCE

there are 6 differences between the fake and real emails. See if you can find them.

### FAKE

**From:** support@microsoft.co.uk  
**Sent:** 16/01/2023 11:44  
**To:** Bob Smith <Bob.Smith@company.com>  
**Subject:** Urgent Action Needed!

 Outlook

Microsoft Account

**Verify your account**

We detected some unusual activity about a recent sign in for your Microsoft account. You might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

<http://account.live.com/ResetPassword.aspx>

Thanks,  
The Microsoft Team

### REAL

**From:** support@microsoft.co.uk  
**Sent:** 16/01/2023 11:44  
**To:** Bob Smith <Bob.Smith@company.com>  
**Subject:** Unusual Sign In Activity

 Outlook

Microsoft Account

**Verify your account**

We detected some unusual activity about a recent sign in for your Microsoft account **bo\*\*\*\*\*@company.com**. You might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

[REVIEW RECENT ACTIVITY](#)

Thanks,  
The Microsoft Team