**محاكاة عنوان البريد الإلكتروني وخادوم** بروتوكول **إرسال البريد البسيط (SMTP) المفتوح**

**ترحيل البريد المفتوح** (**open mail relay**) هو خادوم بروتوكول إرسال البريد البسيط (SMTP) تم إعداده بطريقة تسمح لأي شخص على الإنترنت بإرسال بريد إلكتروني من خلاله، ليس فقط البريد المرسل من أو إلى مستخدمين معروفين. وكان هذا الإعداد يمثل التكوين الافتراضي في العديد من خوادم البريد. وفي الواقع، كان هو الطريقة التي أنشئت بها شبكة الإنترنت في البداية، لكن مُرحِّلات البريد المفتوحة فقدت شعبيتها بسبب استغلالها من قبل مرسلي الرسائل غير المرغوب فيها والديدان الحاسوبية. وقد تم إغلاق العديد من المرحلات، أو تم وضعها على قوائم سوداء من خلال خوادم أخرى.

وفي منتصف التسعينيات، مع ظهور البريد الالكتروني غير المرغوب فيه، لجأ مرسلو الرسائل غير المرغوب فيها إلى إعادة توجيه بريدهم الإلكتروني من خلال خوادم البريد الإلكتروني التابعة لأطراف ثالثة بغية تجنب الكشف عنهم واستغلال الموارد الإضافية لخوادم الترحيل المفتوحة. وهكذا، كان مرسلو الرسائل غير المرغوب فيها يبعثون بريدًا إلكترونيًا واحدًا إلى الترحيل المفتوح ويضمنون فيه (بشكل فعال) قائمة كبيرة بنسخ مرفقة ("blind carbon copy "، نسخة كربونية مخفية)، ومن ثم يقوم المرحل المفتوح بترحيل هذا البريد غير المرغوب فيه إلى القائمة بأكملها. ولئن كان ذلك قد قلل إلى حد كبير من متطلبات عرض النطاق الترددي لمرسلي الرسائل غير المرغوب فيها عندما كانت اتصالات الإنترنت محدودة، فإنه أجبر كل رسالة غير مرغوب فيها على أن تكون نسخة طبق الأصل وبالتالي يسهل اكتشافها.

وبما أن مرحلات البريد المفتوحة لا تبذل أي جهد للتأكد من صحة هوية مرسل البريد الإلكتروني، فإن مرحلات البريد المفتوحة تكون عرضة لمحاكاة وانتحال عنوان البريد الإلكتروني.

وتتمثل **محاكاة البريد الإلكتروني** (**Email spoofing**) في إنشاء رسائل بريد إلكتروني بعنوان مرسل مزور.

ونظرًا لأن بروتوكولات البريد الإلكتروني الأساسية لا تملك أي آلية للتحقق من صحة الهوية، فمن الشائع أن تستخدم رسائل البريد الإلكتروني غير المرغوب فيها والتصيد الاحتيالي محاكاة من هذا القبيل بغية تضليل المتلقي بخصوص مصدر الرسالة.

عند إرسال بريد إلكتروني SMTP، يوفر الاتصال الأولي قسمين من معلومات العنوان:

* **بريد مرسل من**: - عادة يقدم للمتلقي على أنه مسار راجع: ترويسة ولكن لا تكون مرئية بشكل طبيعي للمستخدم النهائي، ولا يتم تلقائيا إجراء أي تدقيق يُبين أن النظام المرسل مرخص له بالإرسال نيابة عن ذلك العنوان.
* **مستلم من (RCPT TO)**: - يحدد عنوان البريد الإلكتروني الذي يتم تسليم البريد الإلكتروني إليه، ولا يكون مرئيًا عادة للمستخدم النهائي ولكن قد يكون موجودًا في العناوين الرأسية كجزء من ترويسة "مستلم:" ("Received:").

ويشار إلى هذه العناصر في بعض الأحيان على أنها عنوان "الظرف" ("envelope")، تشبيها بالظرف الورقي التقليدي. وإن لم يدل خادوم استلام البريد على وجود مشاكل في أي من هذه العناصر، يرسل النظام المرسل أمر "البيانات"، وعادة ما يرسل عدة عناصر مكونة للعنوانين، بما في ذلك:

* **من:** Joe Q Doe <joeqdoe@example.com> - العنوان المرئي للمستلم؛ ومرة أخرى، لا يتم تلقائيا إجراء أي تدقيق للتحقق من أن النظام المرسل مرخص له بالإرسال نيابة عن ذلك العنوان.
* **ردا على (Reply-to:):**  Jane Roe <Jane.Roe@example.mil> - وبالمثل، لم يتم التحقق منه.

وأحيانا:

* **المرسل**: Jin Jo jin.jo@example.jp>> - لم يتم التحقق منه أيضًا.

والنتيجة هي أن مستلم البريد الإلكتروني يرى وكأن البريد الإلكتروني مرسل من العنوان المشار إليه في عنوان "من:"؛ وقد يتمكن أحيانًا من إيجاد عنوان "بريد إلكتروني من" (MAIL FROM)؛ وإذا قام بالرد على البريد الإلكتروني، فسيتم توجيه الرد إما إلى العنوان المعروض في عنوان "من:" (From) أو "ردا على" (Reply-to): - ولكن لا يمكن عادة الاعتماد على أي من هذه العناوين، لذلك فإن الرسائل المرتدة التلقائية قد تولد نشرا/تبعثرا عكسيا (backscatter).

على الرغم من أن محاكاة البريد الإلكتروني تنجح في تزوير عناوين البريد الإلكتروني، إلا أنه من الممكن عمومًا تحديد عنوان بروتوكول الإنترنت الخاص بجهاز الكمبيوتر الذي يرسل البريد من سطور "مستقبل:" ("Received:") في ترويسة البريد الإلكتروني. في كثير من الحالات، من المحتمل أن يتعلق الأمر بطرف ثالث بريء ملوث ببرمجية خبيثة ترسل البريد الإلكتروني دون علم المالك.

*المصدر (باللغة الإنجليزية):* [*https://en.wikipedia.org/wiki/Open\_mail\_relay*](https://en.wikipedia.org/wiki/Open_mail_relay) *؛* [*https://en.wikipedia.org/wiki/Email\_spoofing*](https://en.wikipedia.org/wiki/Email_spoofing)*.*