# طرق تعزيز أمن البريد الإلكتروني

تقنيـة البريد الإلكتروني تعتمد على برتوكـول SMTP لنقل الرسـائل بين الخـوادم حـول العالـم، البروتوكول يعتبـر لامركـزي (decentralized) ممـا يجعل عملية التحقق من هوية المرسـل صعبـة. لذلـك تسـتخدم تقنيـات أخـرى للحـد مـن عمليـات اسـتغلال ذلك البروتوكول لإرسـال الرسـائل الغيـر مرغـوب بهـا مثـل: الرسـائل الاقتحاميـة (SPAM) والرسـائل الانتحاليـة (Spoofing) والرسائل التصيدية (Phishing).

نظـراً لانتشـار تلـك الهجمات وما تشـكله من خطـورة على المنشـآت، يوصـي المركز الوطنـي لأمن المعلومـات بهيئة الاتصـالات وتقنيـة المعلومـات بتطبيـق التقنيـات التالية لتعزيز أمن البريد الإلكتروني في المنشأة:

## ضبـط الإعدادات التاليـة لنظام أسماء النطاقات (DNS) بعد حصر جميع الخـوادم التـي تـقـوم بإرسـال رسـائل باسـم المنشـأة

**SPF**

تفعيل Sender Policy Framework (SPF) والذي يعمل على تمكين المنشـأة من تسـجيل عناويـن الخوادم المرخـص لها بإرسـال البريـد الإلكتروني، كمـا يعمل على التحقـق مـن عناويـن IP لرسـائل البريـد الإلكتروني الـواردة من خـلال مقارنتها مع محتوى SPF في نظام أسماء النطاقات للمصدر.

**DKIM**

تفعيـل DomainKeys Identified Mail (DKIM) والـذي يعمـل على توثيق رسـائل البريد الإلكتروني المرسـلة والتحقق من أن البريد الإلكتروني كان بالفعل مرخصًا من قبـل صاحب النطاق وسـليما مـن التعديـلات، عن طريق إعطـاء البريـد الإلكتروني توقيعًا رقميًا (DKIM) تتم إضافته إلى الرسالة ويتم تأمينه باستخدام التشفير.

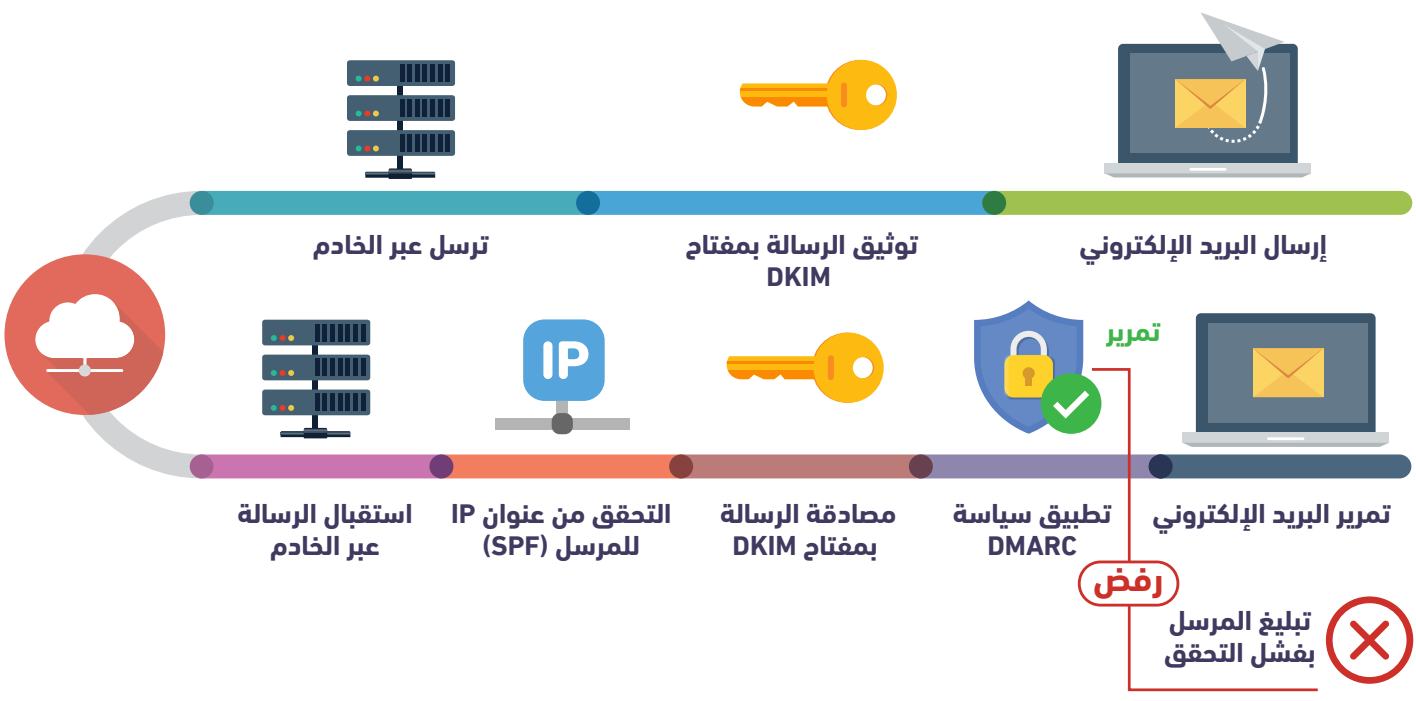
**DMARC**

تفعيـل (Domain-based Message Authentication, Reporting & Conformance DMARC) والتي تعمل على مصادقة البريد الإلكتروني باستخدام تقنيتيّ SPF وDKIM المذكـورة، وفقـاً للسياسـات المطبقـة وبالتالـي تعمل علـى تمرير/رفض الرسائل عبر خوادم البريد.

**!** ينصـح بتطبيـق التقنيات بشـكل تدريجـي والتأكد من صحتها باسـتخدام بعض أدوات ومواقع الفحص، واختبار فاعليتها بإرسـال رسائل تجريبية من خارج الشبكة

## تفعيل إعدادات خادم البريد الخارجي ليقوم بالتحقق من هوية الرسائل الواردة

- فحـص سـجلات SPF للعنـوان المرسل منه ومطابقته مع الخادم الذي قام بالإرسال
- المصادقة الإلكترونية DKIM لتأكيد مصدر الرسالة
- تنفيذ سياسات DMARC المعتمدة من صاحب النطاق للمُرسل
- مطابقـة عنوان خادم المرسـل مع قوائم الحجب للرسائل الاقتحامية (DNSBL او RBL)
- تحديد السياسات المناسبة للتعامل مع الرسالة حسب مخرجات تقنيات الفحص السابقة
- فحص محتوى الرسـالة للبحث عن كلمات تُسـتخدم عـادة فـي الرسـائل التصيديـة والاقتحامية
- اسـتخدام أنظمـة الحمايـة الخاصـة بالبريد الإلكتروني لكشف الفيروسات والهجمات التصيدية والاقتحامية




يمكن تفعيل تلك التقنيات للمنشـأة التي تسـتخدم خوادمها الخاصة للمراسـلات البريدية، لكـن في حال اسـتخدام خدمات البريد الإلكتروني من طرف ثالـث فيجب التحقق معهم من إمكانية تطبيقها، مثلاً: قوقل G Suite ومايكروسوفت Office365 تدعم تلك التقنيات.

**!** تطبيق هذه التوصيات لا يعني الحماية المطلقة من الرسائل التصيديـة والغيـر مرغوب فيها ، لكن تسـاعد علـى الحد من نسبة كبيرة منها، وتبقى توعية المستخدمين هي الأهم.