الامتدادات الأمنية لنظام اسم النطاق

ساعد في حماية معلومات DNS التي ترسلها عبر الإنترنت

تسمح الامتدادات الأمنية لنظام اسم النطاق (DNSSEC) للمسجّلين **بالتوقيع الرقمي** للمعلومات التي يدخلونها الى نظام اسم النطاق (DNS). وهذا يحمي العملاء من خلال التأكد من أن بيانات DNS التي تعرضت للتلف سواء عن طريق الخطأ أو بسبب برامجيات ضارة، لا تصل إليهم.

الجدول الزمني

عندما تم تصميم نظام اسم النطاق، لم يحظى الأمن بالتركيز اللازم. يمكن للمهاجمين **اختراق رسائل DNS الخاصة بك** وكذلك **إعادة توجيه رسائلك إلى موقع آخر** على الإنترنت بدلاً من الموقع الذي طلبته.

أوجد مجتمع DNS الفني الحل النهائي لهذه المشكلة - DNSSEC. تقوّي DNSSEC المصادقة في نظام DNS باستخدام التواقيع الرقمية القائمة على **تشفير المفتاح العام.**

DNSSEC قيد التشغيل

يجب تمكين جانبين من DNSSEC لكي تعمل.

يجب على المسجلين، المسؤولين عن نشر معلومات DNS التأكد من أن بيانات **DNS الخاصة بهم موقعة من قبل DNSSEC.**

يتعين على مشغلي الشبكات **تمكين التحقق من DNSSEC على محلليهم** الذين يتعاملون مع عمليات بحث DNS للمستخدمين.

منافع نشر امتدادات DNSSEC

تحفز الابتكار.
تتحقق DNSSEC من بيانات DNS وتحميها، مما يمكن الثقة بالبيانات في التطبيقات خارج نظام DNS.

تقلل من التعرض للهجمات.

تساعد في حماية الإنترنت، المستخدمين النهائيين، الشركات، المنظمات والحكومات.

شجّع مشغلي شبكتك على تمكين امتدادات DNSSEC

للمزيد من المعلومات يرجى زيارة الموقع:

http://go.icann.org/OCTOpublications
http://go.icann.org/DNSSEC

ICANN

تصميم قسم الاتصالات في ICANN – مايو 2020