التاريخ: 26 ديسمبر 2019
الموضوع: نشرة اتصالات الأمنية – اعتماد DMARC
الهدف: حماية عملاء اتصالات من رسائل البريد الإلكتروني الاحتيالية
فئة العملاء: عملاء اتصالات

ملخص

الاحتيال عبر البريد الإلكتروني: هو ممارسة احتيالية يقوم فيها المرسل بانتحال مصدر بريد إلكتروني معروف في المحاولة للحصول على معلومات شخصية من مستلم البريد الإلكتروني.

استجابة اتصالات

من أجل حماية عملاء اتصالات من الاحتيال عبر البريد الإلكتروني وحماية خصوصية العملاء، طبقت اتصالات بنجاح ضوابط أمنية جديدة لإطار سياسة المرسل Sender Policy Framework (SPF) وتوثيق الرسائل المستندة إلى مصدر بريد إلكتروني ومطابقتها Domain-based Message Authentication, Reporting & Conformance (DMARC)

ستضمن أدوات التحكم الجديدة أن جميع رسائل البريد الإلكتروني المرسلة إلى عملائنا من اتصالات يتم إرسالها بالفعل من مرسلي اتصالات المعتمدين.

على مدار العام، راقبنا اتجاهات البريد الإلكتروني الخاصة بنا واستكملنا سياسة DMARC ، ونحن فخورون بأن نعلن أن اتصالات أصبحت الآن من بين **6.1** ٪ من المؤسسات التي نشرت DMARC على مستوى العالم.

فوائد العملاء

ستوفر المبادرة الأمنية الجديدة من اتصالات الفوائد التالية لعملاء اتصالات:

1) حماية خصوصية العملاء وبياناتهم.
2) تقليل شكاوى العملاء بشأن تلقي العروض الترويجية المزيفة والفواتير الخاطئة والفواتير المتأخرة، إلخ...
3) تقليل عبء أنظمة البريد الإلكتروني الخاصة بالعملاء عن طريق حظر عدد كبير من الرسائل غير المرغوب فيها ورسائل البريد الإلكتروني المخادعة.

المطلوب من العملاء

لا يوجد أي إجراء مطلوب من قبل عملاء اتصالات الأفراد، ومع ذلك، يجب على عملاء اتصالات المصنفين ضمن الشركات والمؤسسات والهيئات التحقق من إعدادات نظام بريدهم الإلكتروني SPF وDMARC من اتصالات.

إذا لاحظت أي رسائل إلكترونية مشبوهة يُزعم أنها مرسلة من اتصالات (@etisalat.ae) ، فيرجى الإبلاغ عنها إلى spamreport@etisalat.aeحتى نتمكن من تحليلها واتخاذ الإجراءات اللازمة.

للاستفسار

لأية أسئلة أو توضيحات، يرجى الاتصال بنا على itsecurity@etisalat.ae