Date: 26 December 2019

Topic Type: Etisalat Security Bulletin - DMARC Adoption

Subject: Protecting Etisalat Customers from Fraudulent Emails

Customers' Category: Etisalat Corporate Customers

Brief

Email Spoofing or Email Scam is a fraudulent practice where a malicious sender is impersonating a known source in an attempt of getting personal information from the email recipient.

Etisalat Response

In order to protect Etisalat customers from fraudulent emails and protect their privacy, Etisalat have successfully implemented new security controls of Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting and Conformance (**DMARC**). The new controls will ensure that all the emails sent to our customers are genuinely sent from authorized Etisalat senders.

Throughout the year, we have monitored our email trends and concluded the **DMARC** policy, and we are proud to announce that Etisalat is now amongst the **6.1%** of the organizations who have deployed **DMARC** globally.

Customer Experience

The new security initiative from Etisalat will bring the following benefits to our customers:

1. Protect customers' privacy and data
2. Reduce customers' complaints regarding receiving fake promotions, wrong bills and late payments, etc...
3. Offloading customers' email systems by blocking large volume of spam and spoofed emails

Customers' Actions

There is no required action from Etisalat individual consumers. However, Etisalat corporate customers must configure their email platform to honor the Etisalat's SPF and **DMARC** settings. If you observe suspicious emails claimed to be sent from Etisalat (@etisalat.ae), please report them to spamreport@etisalat.ae so that we can analyze them and take action where appropriate.

Questions

For any questions or clarifications, please contact us at itsecurity@etisalat.ae