Notice to Suppliers

Email Security

Originator: Neil Cassidy
Job Title: Chief Information Security Officer
Business Unit: All

NTS Number: 594
Issue: 1
Date: 18 December 2023

For the attention of the Managing Director

Scope/Applicability:

All Rolls-Royce suppliers and partners.

Dear Supplier,

Introduction:

At Rolls-Royce we are constantly looking to improve our cyber security. Rolls-Royce has updated its technical and business policies to ensure the sender or recipient of Rolls-Royce email can be verified, and email communications are protected in transit from unauthorised access and disclosure.

By aligning its policies with UK National Cyber Security Centre (UK NCSC) email security standards [Ref 1], Rolls-Royce has enhanced its protections against cyber criminals sending emails purporting to be Rolls-Royce and made it harder for emails to be intercepted and read in transit.

The purpose of this Notice is to inform you of the changes to Rolls-Royce email and communication security policies and provide the opportunity for you to review your services and bring them in line with best security practice [Ref 1].

The changes will come into effect on 28th February 2024. You must act now; review your email security settings and ensure you can continue to securely communicate with Rolls-Royce by email.

Action Required:

1. Share this NTS with your email/IT administrators. Ask them to review and confirm your email services align with best security practice [Ref 1]. If your email services:
    a. comply, no further action is required.
    b. do not comply, they should follow steps 2 – 3 of this guidance to implement encryption and anti-spoofing measures.
2. Configure your email services using UK NCSC guidance or US Cybersecurity & Infrastructure Security Agency (US CISA) guidance [Ref 1]:
    a. Read UK NCSC guidance. See https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/recommended-implementation-plan
    b. Set up encryption for email in transit between your email services and Rolls-Royce. See https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/protect-email-in-transit
    c. Put policies in place to check inbound and outbound email to prevent spoofing using Domain-based Message Authentication, Reporting and Conformance (DMARC). See https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/configure-anti-spoofing-controls
    d. Verify and/or configure your DNS records

3. Check your email services are secure:
    a. Check email certificates are valid and renewed
    b. Check email is authenticating correctly
    c. Check your email server is active and responsive
    d. Check your email services are encrypting email
    e. Communicate the changes to your organization who are running email filtering services, cloud-based applications that send email (e.g., MailChimp), line of business applications that send emails (e.g., HR or finance/payroll systems).

   UK organisations can verify their email services are secure using the UK NCSC Email Security Check Service [Ref 2]
4. Failure to follow these steps means that after 28th February 2024 you will not be able to send to or receive email communications with Rolls-Royce.

NTS Category:	**Authorised by:**
General Information	Rob Cowan
	Chief Information Officer

Ref 1: https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing or https://www.cisa.gov/resources-tools/resources/enhanced-email-and-web-security

Ref 2: https://emailsecuritycheck.service.ncsc.gov.uk/ or https://github.com/ukncsc/mail-check