In today's hyper-connected world, cybercrime is becoming increasingly complex and deceptive. We kindly urge all users—especially those engaging in remote work or cloud-based activity—to exercise extra caution when interacting with unfamiliar emails, websites, or file attachments. A single misplaced click on a fraudulent link can compromise entire systems and personal identities. Even messages that appear to come from trusted contacts may be part of a social engineering attack.

Please ensure your software is up to date, enable two-factor authentication on all platforms where it's available, and avoid using the same password across multiple services. If you suspect that your account has been breached or you receive suspicious communications, do not ignore it. Report it to our cybersecurity response team immediately. Our goal is to empower you—not to scare you—and together, we can create a safer digital environment.