BhutanNOG(June 2017)

ALISHA GURUNG
BHUTAN TELCOM LIMITED

Senders and Receivers

Recipient: alisha@gmail.com

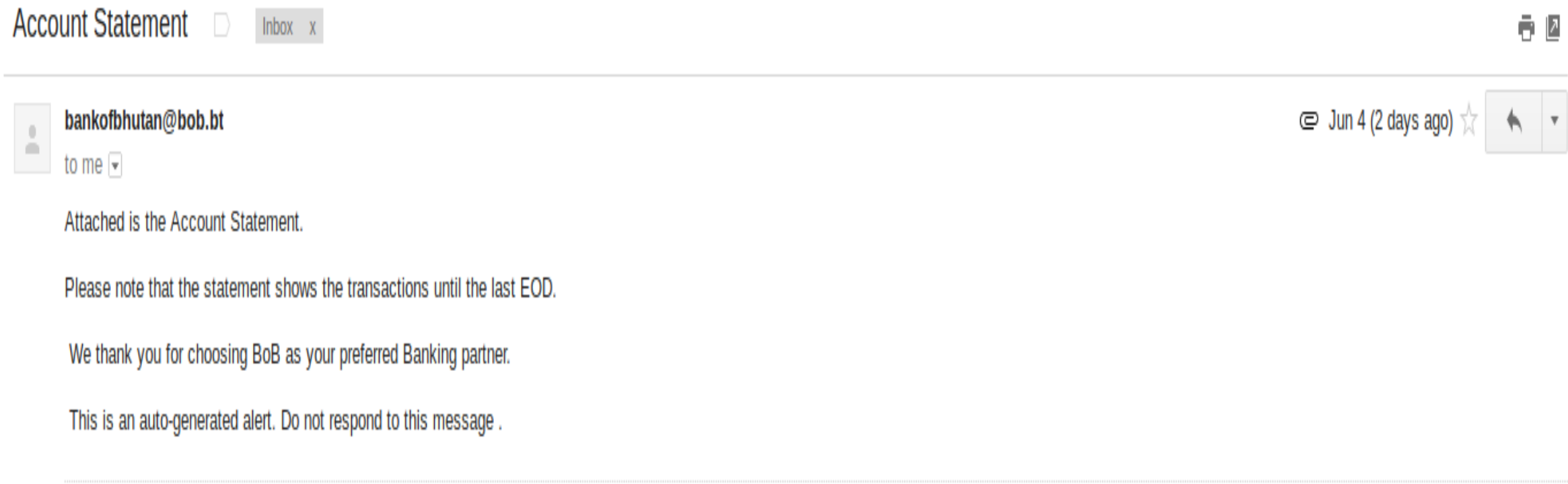
Forged sender: ceo@gov.bt

Actual Sender: bankofbhutan@bob.bt

FAKE EMAIL


Urgent
Inbox x
CEO, Bhutan Telecom Limited <ceo@gov.bt>
to me
6:54 AM (3 hours ago)
Dear Alisha,
Your have been transferred to some other region. Please come to my office to talk more about it.
Best Regards,
CEO, Bhutan Telecom Lim...
ceo@gov.bt
Show details

Genuine Mail



Account Statement

Inbox x

bankofbhutan@bob.bt

to me

Jun 4 (2 days ago)

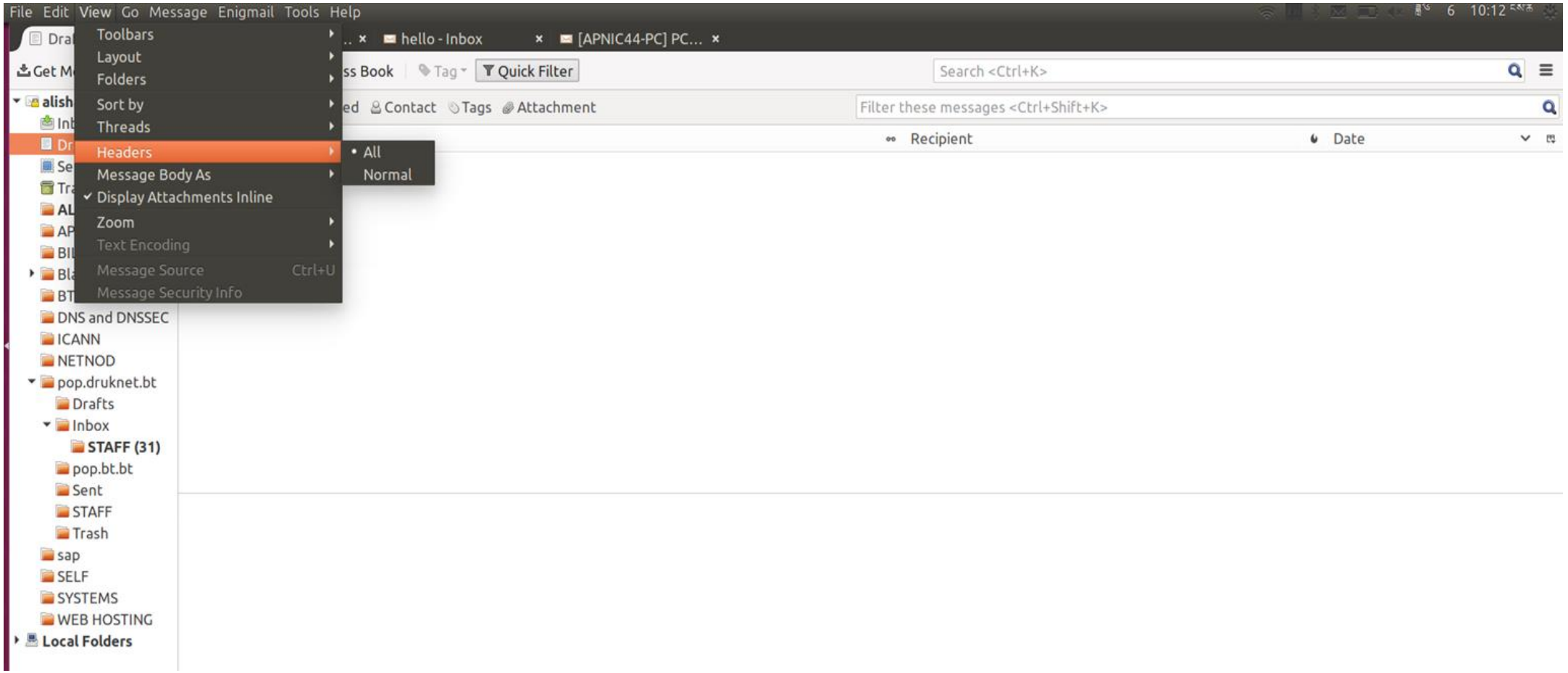
Attached is the Account Statement.

Please note that the statement shows the transactions until the last EOD.

We thank you for choosing BoB as your preferred Banking partner.

This is an auto-generated alert. Do not respond to this message .

EMAIL CLIENTS



```
Delivered-To: alisha@gmail.com
Received: by 10.80.220.72 with SMTP id y8csp284376edk;
        Mon, 5 Jun 2017 17:54:35 -0700 (PDT)
X-Received: by 10.223.133.181 with SMTP id 50mr7143438wrt.27.1496710475061;
        Mon, 05 Jun 2017 17:54:35 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1496710475; cv=none;
        d=google.com; s=arc-20160816;
        b=ZgrkE577PMLA2DwNtMVceY9CrG/zZtKn/bR/A+GoMRnJp1QeDZH8OJb5wLYCBLiqn8
         SSOumOI6YdHTqNUVAQzt4+JTYaq5JoWTC/jME9o07MMS40nKD+6hPbj0L7FHDZ5bocNL
         +G6ANB8SL09EZVRn9CqHQKx8bBfx92J63qtsXhlcXqYY4te7n0HWFesVWlwQvXKW4xMP
         ZnaZODGBwpqOOjep7DZPUoZX0tCwZ6G7qC28++xPtNKyIicfTcuDmmXKxYi0JQfl7zXY
         928Y5vl7lLbyoU7FT1cM3Puf3Ty8iqQxYId0lf6fFycIPpCy8Po4GEtgK6DBLJrcxIIl
         85+w==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:message-id:reply-to:errors-to:importance:from:subject:to
         :arc-authentication-results;
        bh=v5aaCHJstUW8eqlhl1dRD5yBc9lomqCK8X0i0wjfbZ8=;
        b=MCmQTHglIsVaLWrhwRoeYnthulk2QR2gKObJ20mefGnYkZyFlg0UZWYCa0qPmPt8u7
         LlAw7DqzH4gKZgRG7263dxcTcwbE0qxfUrngPAjE7PxFIMCQUy40wgcHMl6rV2o7a41P
         cE8A6O6fnzRkCEV3H8J6Ic6+pEsJE74bkpt73jFva1HS4dQaS6sfEnZ3nyk8LBtLMNrI
         JHIrWGQxuuesJbKthD8CrygrRW1X0MuEgpDbo1z7CD4UqzZEFFvQmQCZzvehMhtkG7zO
         YEWPxx7aKV6dquyrLRlYSthZrMolwBw0ZVr55NQWuFKmPjSHFKO/9k1YbFBROCQhRLQZ
         Ke2w==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 46.167.245.71 is neither permitted nor denied by best guess record for domain of ceo@gov.bt) smtp.mailfrom=ceo@gov.bt
Return-Path: <ceo@gov.bt>
Received: from emkei.cz (emkei.cz. [46.167.245.71])
        by mx.google.com with ESMTPS id g97si31278804wrd.178.2017.06.05.17.54.34
        for <alishateddy@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 05 Jun 2017 17:54:34 -0700 (PDT)
Received-SPF: neutral (google.com: 46.167.245.71 is neither permitted nor denied by best guess record for domain of ceo@gov.bt) client-ip=46.167.245.71;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 46.167.245.71 is neither permitted nor denied by best guess record for domain of ceo@gov.bt) smtp.mailfrom=ceo@gov.bt
Received: by emkei.cz (Postfix, from userid 33) id EB800D6C19; Tue,
  6 Jun 2017 02:54:33 +0200 (CEST)
To: alisha@gmail.com
Subject: Urgent
From: "CEO, Bhutan Telecom Limited" <ceo@gov.bt>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: ceo@gov.bt
Reply-To: ceo@gov.bt
Content-Type: text/plain; charset=utf-8
Message-Id: <20170606005433.EB800D6C19@emkei.cz>
Date: Tue,
  6 Jun 2017 02:54:33 +0200 (CEST)
```

```
Delivered-To: alisha@gmail.com
Received: by 10.80.182.252 with SMTP id f57csp911425ede;
        Sun, 4 Jun 2017 02:27:48 -0700 (PDT)
X-Received: by 10.84.254.2 with SMTP id b2mr9065485plm.185.1496568468281;
        Sun, 04 Jun 2017 02:27:48 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1496568468; cv=none;
        d=google.com; s=arc-20160816;
        b=0oLUtHEbgwznojb1kdrHClPDBm1IqI3f4TrrFkXWrSTyGMantVFtTDqZIcg12XHUbM
         WG4Q41htkmgCYn4QAVmFfExPs57b5Asb6S3v/nJRntQyoI8X4yGFgDFGnF1OENVYMZ32
         tuAgAQCRFw7TqJCZ0Tb+iep9bUC8Mji+k/uydw3RiCxlk2MtCyOTFGUVc6Qh+tjf6H6N
         RfnHTdpjnP1HjYSISZKVQbwXaaLXe7NxixlmuPoXqyk2/9L9sl7ZO/5wN3KD5WGqqmkE
         wn1TMDgRIoaThwofb06EJImeg3UdH0J719TC3oWgroaDqCOEjX9/QzWdPuhjMsfgoZoF
         ai2Q==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=mime-version:subject:message-id:to:from:dkim-signature:date
         :arc-authentication-results;
        bh=UlumKZTfqbaCVOLJaYp25L5a4VpgXUhc5NWQbN4+N1Q=;
        b=dde+wpXkZfzaJGn1yTtwhf68Y0CkK9VkyrX3nMzxkH2uWcIq/ZLrrGT3vEEqUOBsa/
         VPW3HeuHkyZElxkCqBjZlf1XwjVxFTwAyWkMWFxfim7JQeeiWfbdEZ8Tf8nBWfWLlE8T
         CUdRpFv4W4SLpgo9+gHU8Pgi9V78y7IPW3wv6AeshNDVjOOriF62mHHccCReP5ok7aFS
         7EYNFSCu9RyS9Og4KuSAW4ZrS+0PfFxAkUNRqDICXKzNt+HwsUxVufXG2dq6OHHYNvqj
         l1WIm/azXtdmkKLQ3pDEpd38d2zasMefsBM7zA666Cds/rCJAAfRP2+S5UrGDBsJVr9T
         zDHw==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=neutral (invalid public key) header.i=@bob.bt;
       spf=pass (google.com: domain of bankofbhutan@bob.bt designates 202.144.136.150 as permitted sender) smtp.mailfrom=bankofbhutan@bob.bt;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=bob.bt
Return-Path: <bankofbhutan@bob.bt>
Received: from mail.bob.bt (mail.bob.bt. [202.144.136.150])
        by mx.google.com with ESMTPS id n11si4303340plg.49.2017.06.04.02.27.46
        for <alishateddy@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Sun, 04 Jun 2017 02:27:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of bankofbhutan@bob.bt designates 202.144.136.150 as permitted sender) client-ip=202.144.136.150;
Authentication-Results: mx.google.com;
       dkim=neutral (invalid public key) header.i=@bob.bt;
       spf=pass (google.com: domain of bankofbhutan@bob.bt designates 202.144.136.150 as permitted sender) smtp.mailfrom=bankofbhutan@bob.bt;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=bob.bt
Date: Sun, 04 Jun 2017 02:27:48 -0700 (PDT)
X-SmarterMail-Authenticated-As: bankofbhutan@bob.bt
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=bob.bt; s=b0b2014;
        h=content-type:mime-version:subject:message-id:from;
        bh=UlumKZTfqbaCVOLJaYp25L5a4VpgXUhc5NWQbN4+N1Q=;
        b=pEiBDDK3CCWC3Mx6uQKiXkfhyN4UeIeo8Aex+k/7o4eNsGpZmlG6iDzdaUWM5/KxS
          QT9sOGkwQXd9wHB8jsq4DpZ9deuBQZZTcPJmAEifyW5kWiCmAVYN8X6BdCD3wdkPD
          f/dTFf+9LIhwaCyw6EexvFTGs4vhhYHFuaDnOoMAw=
Received: from MOBILEBANKINGPP (Unknown [192.168.15.20]) by mail.bob.bt with SMTP (version=Tls cipher=Aes128 bits=128);
```