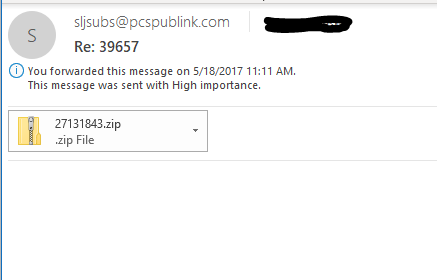
# Networking Lab 10 SMTP

## Spam Message 1

Examine the following email and answer the accompanying questions. Note: The email address in the From: header has been changed to “redacted” for privacy reasons.

### The email as displayed to the user



Question 1: Is there anything suspicious in this email?

### The email headers

Here is the header:

Received: from BN6PR02MB3218.namprd02.prod.outlook.com (10.161.152.28) by

DM5PR02MB3228.namprd02.prod.outlook.com (10.164.148.18) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256) id

15.1.1084.16 via Mailbox Transport; Thu, 18 May 2017 14:57:30 +0000

Received: from CY4PR02CA0018.namprd02.prod.outlook.com (10.169.188.28) by

BN6PR02MB3218.namprd02.prod.outlook.com (10.161.152.28) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256) id

15.1.1101.14; Thu, 18 May 2017 14:57:28 +0000

Received: from SN1NAM02FT035.eop-nam02.prod.protection.outlook.com

(2a01:111:f400:7e44::207) by CY4PR02CA0018.outlook.office365.com

(2603:10b6:903:18::28) with Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256) id 15.1.1101.14 via

Frontend Transport; Thu, 18 May 2017 14:57:28 +0000

Authentication-Results: spf=none (sender IP is 192.143.167.19)

smtp.mailfrom=airmobile.co.za; brcc.edu; dkim=none (message not signed)

header.d=none;brcc.edu; dmarc=temperror action=none

header.from=pcspublink.com;

Received-SPF: None (protection.outlook.com: airmobile.co.za does not designate

permitted sender hosts)

Received: from airmobile.co.za (192.143.167.19) by

SN1NAM02FT035.mail.protection.outlook.com (10.152.72.145) with Microsoft SMTP

Server id 15.1.1075.5 via Frontend Transport; Thu, 18 May 2017 14:57:25 +0000

Content-Disposition: attachment

Subject: Re: 39657

Importance: High

Content-Type: application/zip; name="27131843.zip"

To: <redacted@brcc.edu>

Message-ID: <149511940287.23064.11170174189267635002@airmobile.co.za>

From: <sljsubs@pcspublink.com>

Content-Transfer-Encoding: base64

Date: Thu, 18 May 2017 14:56:42 +0000

MIME-Version: 1.0

Return-Path: sljsubs@airmobile.co.za

X-MS-Exchange-Organization-Network-Message-Id: fb5294e5-47ea-43ca-db13-08d49dfe3380

X-EOPAttributedMessage: 0

X-EOPTenantAttributedMessage: 59b96094-b5c8-4ea9-9352-65eb3d51990f:0

X-MS-Exchange-Organization-MessageDirectionality: Incoming

X-Forefront-Antispam-Report: CIP:192.143.167.19;IPV:NLI;CTRY:;EFV:NLI;SFV:NSPM;SFS:(6009001)(5340300001)(2970300002)(428002)(199003)(189002)(44003)(229853002)(9686003)(8666007)(55930200001)(8676002)(53416004)(106466001)(71816002)(105586002)(305945005)(25786009)(110136004)(2171002)(6246003)(7696004)(86152003)(55016002)(356003)(6666003)(6506006)(6916009)(42882006)(7636002)(1096003)(54356999)(101416001)(118246002)(50986999)(40036005)(73894003)(36756003)(621065002)(100306002)(5002050100002)(2351001)(88526003)(2876002)(4270600005)(56080200008);DIR:INB;SFP:;SCL:1;SRVR:BN6PR02MB3218;H:airmobile.co.za;FPR:;SPF:None;MLV:ovr;A:1;MX:3;PTR:192-143-167-19.ip.airmobile.co.za;LANG:en;

Question 2: Compare the message headers Return-Path and From. If the user clicks “reply”, the message will be sent to the Return-Path address. Is there anything suspicious?

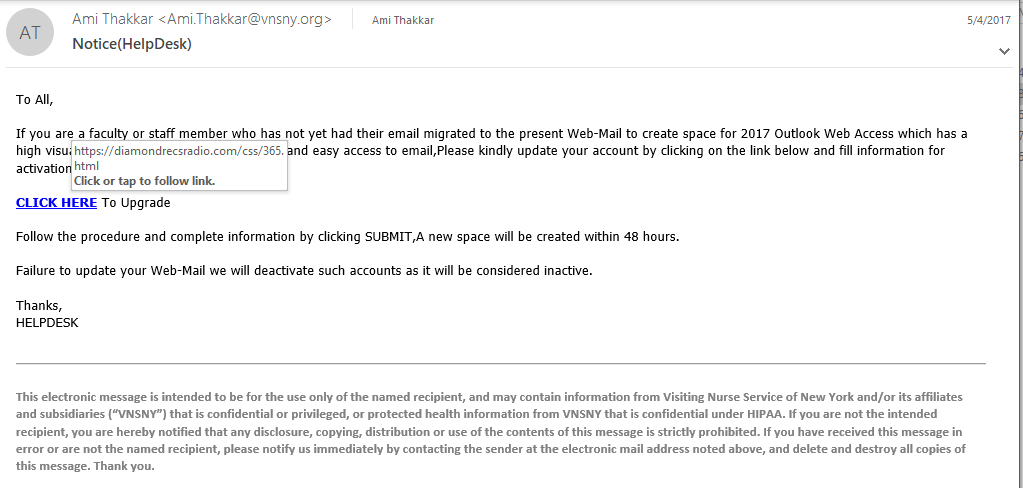
Question 3: What is the first server to receive the email, and where did the message originate? Give the domain name and IP address. Look up the IP address at [www.arin.net](http://www.arin.net). Where is that address?

Question 4: Are there email security mechanisms (SPF, DKIM, and DMARC) in the header that can vouch for the authenticity of the message?

Question 5: Phish or Legit?

## Spam Message 2

Examine the following email and answer the accompanying questions. This one is a bit confusing.



Question 1: Is there anything suspicious in this email? Note: The web site at the end of the link is no longer functioning, but when the user clicked the link they saw what appeared to be an Outlook Web Access login page.

### The email headers

Here is the header:

Received: from SN1PR0201MB1535.namprd02.prod.outlook.com (10.163.129.22) by

BLUPR0201MB1523.namprd02.prod.outlook.com (10.163.119.22) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256) id

15.1.1061.12 via Mailbox Transport; Thu, 4 May 2017 19:06:41 +0000

Received: from BY2PR02CA0096.namprd02.prod.outlook.com (10.163.44.150) by

SN1PR0201MB1535.namprd02.prod.outlook.com (10.163.129.22) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256) id

15.1.1047.13; Thu, 4 May 2017 19:06:39 +0000

Received: from CY1NAM02FT054.eop-nam02.prod.protection.outlook.com

(2a01:111:f400:7e45::208) by BY2PR02CA0096.outlook.office365.com

(2a01:111:e400:5261::22) with Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256) id 15.1.1075.11 via

Frontend Transport; Thu, 4 May 2017 19:06:39 +0000

Authentication-Results: spf=pass (sender IP is 65.51.234.5)

smtp.mailfrom=vnsny.org; brcc.edu; dkim=pass (signature was verified)

header.d=vnsny.onmicrosoft.com;brcc.edu; dmarc=bestguesspass action=none

header.from=vnsny.org;

Received-SPF: Pass (protection.outlook.com: domain of vnsny.org designates

65.51.234.5 as permitted sender) receiver=protection.outlook.com;

client-ip=65.51.234.5; helo=mail1.vnsny.org;

Received: from mail1.vnsny.org (65.51.234.5) by

CY1NAM02FT054.mail.protection.outlook.com (10.152.74.100) with Microsoft SMTP

Server (version=TLS1\_1, cipher=TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA) id 15.1.1047.9

via Frontend Transport; Thu, 4 May 2017 19:06:38 +0000

Received-SPF: None (mail1.vnsny.org: no sender authenticity

information available from domain of Ami.Thakkar@vnsny.org)

identity=mailfrom; client-ip=207.46.163.51;

receiver=mail1.vnsny.org;

envelope-from="Ami.Thakkar@vnsny.org";

x-sender="Ami.Thakkar@vnsny.org"; x-conformance=spf\_only

Received-SPF: Pass (mail1.vnsny.org: domain of

postmaster@NAM02-CY1-obe.outbound.protection.outlook.com

designates 207.46.163.51 as permitted sender) identity=helo;

client-ip=207.46.163.51; receiver=mail1.vnsny.org;

envelope-from="Ami.Thakkar@vnsny.org";

x-sender="postmaster@NAM02-CY1-obe.outbound.protection.outlook.com";

x-conformance=spf\_only; x-record-type="v=spf1"

X-IronPort-Anti-Spam-Filtered: true

X-IronPort-Anti-Spam-Result: A2GuIgA5ewtZezOjLs9cHAEBBAEBCgEBgm48AiZVEHoBARAHjmyQY5A3hwMcKCeFfQKFERMBAgEBAQEBAQEDEAEBCQ0KBygvg38sBwwhNwMDQAEBBQELJw8CAQwpGTIlAgQbiCQGgVYDFQMLlFaQZQKKTTcBAYI0AlqDCQEBBS8ngVKBdBiDIwEBAQEBBQEBAQEBAQEBGAMFhE6CEWiHMoETEQIBHSsSgg1ogjGJNIcrjQuHG4ZehyAZhSCKKoh5iQZ5AYE8NzRsC04ugToOg2oNggFaHAEBAQGGQg0XgQoBeBQBAQE

X-IPAS-Result: A2GuIgA5ewtZezOjLs9cHAEBBAEBCgEBgm48AiZVEHoBARAHjmyQY5A3hwMcKCeFfQKFERMBAgEBAQEBAQEDEAEBCQ0KBygvg38sBwwhNwMDQAEBBQELJw8CAQwpGTIlAgQbiCQGgVYDFQMLlFaQZQKKTTcBAYI0AlqDCQEBBS8ngVKBdBiDIwEBAQEBBQEBAQEBAQEBGAMFhE6CEWiHMoETEQIBHSsSgg1ogjGJNIcrjQuHG4ZehyAZhSCKKoh5iQZ5AYE8NzRsC04ugToOg2oNggFaHAEBAQGGQg0XgQoBeBQBAQE

X-IronPort-AV: E=Sophos;i="5.38,289,1491278400";

d="scan'208,217";a="158612525"

Received: from mail-cys01nam02lp0051.outbound.protection.outlook.com (HELO NAM02-CY1-obe.outbound.protection.outlook.com) ([207.46.163.51])

by mail1.vnsny.org with ESMTP/TLS/AES256-SHA256; 04 May 2017 15:05:51 -0400

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=vnsny.onmicrosoft.com;

s=selector1-vnsny-org;

h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;

bh=G22ybIVG/06n3aKbw6yENvGJpruYIz55dScR1gAEFNY=;

b=VnBSyasaGfaqF1/Rf41R1w3XtULSRdEfyt+t3Rgk0WaGvoVL9DqX1rTqdlCyuDGFfqETNdzaG76AvhMvuUD6mjN0BLnZSaWRG5mJE+mDCNZsUCY/K2KncV6nxCq2Dd39V5rAnlS4Pp9Syiaf2ob4tYZ8o08Cne019ANDm9Ka850=

Received: from MWHPR1301MB1885.namprd13.prod.outlook.com (10.174.168.148) by

MWHPR1301MB1885.namprd13.prod.outlook.com (10.174.168.148) with Microsoft

SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256) id 15.1.1084.7; Thu, 4 May

2017 19:05:40 +0000

Received: from MWHPR1301MB1885.namprd13.prod.outlook.com ([10.174.168.148]) by

MWHPR1301MB1885.namprd13.prod.outlook.com ([10.174.168.148]) with mapi id

15.01.1084.007; Thu, 4 May 2017 19:05:40 +0000

From: Ami Thakkar <Ami.Thakkar@vnsny.org>

To: Ami Thakkar <Ami.Thakkar@vnsny.org>

Subject: Notice(HelpDesk)

Thread-Topic: Notice(HelpDesk)

Thread-Index: AQHSxQaKKWMcWE8UYEG63dkKBmu+kqHkhVMQ

Date: Thu, 4 May 2017 19:05:40 +0000

Message-ID: <MWHPR1301MB18858CAAAB430870C54BD3EDF7EA0@MWHPR1301MB1885.namprd13.prod.outlook.com>

References: <MWHPR1301MB18852FC386B204D27D46CEFCF7EA0@MWHPR1301MB1885.namprd13.prod.outlook.com>

In-Reply-To: <MWHPR1301MB18852FC386B204D27D46CEFCF7EA0@MWHPR1301MB1885.namprd13.prod.outlook.com>

Accept-Language: en-US

Content-Language: en-US

X-MS-Has-Attach:

X-MS-TNEF-Correlator:

authentication-results: nhs-healthlink.com; dkim=none (message not signed)

header.d=none;nhs-healthlink.com; dmarc=none action=none

header.from=vnsny.org;

x-originating-ip: [25.174.164.4]

x-ms-publictraffictype: Email

Content-Type: multipart/alternative;

boundary="\_000\_MWHPR1301MB18858CAAAB430870C54BD3EDF7EA0MWHPR1301MB1885\_"

MIME-Version: 1.0

X-MS-Exchange-Transport-CrossTenantHeadersStamped: MWHPR1301MB1885

Return-Path: Ami.Thakkar@vnsny.org

X-MS-Exchange-Organization-Network-Message-Id: 5b7dac6c-1be4-4007-7f01-08d49320b15e

X-EOPAttributedMessage: 0

Question 2: Compare the message headers Return-Path and From. If the user clicks “reply”, the message will be sent to the Return-Path address. Is there anything suspicious?

Question 2a: What is the value of the To: message header? Suspicious?

Question 3: What is the first server to receive the email? Note that the IP addresses are all private IP addresses. The user probably had a mail client that connected directly to the company’s server. The client address is not obvious.

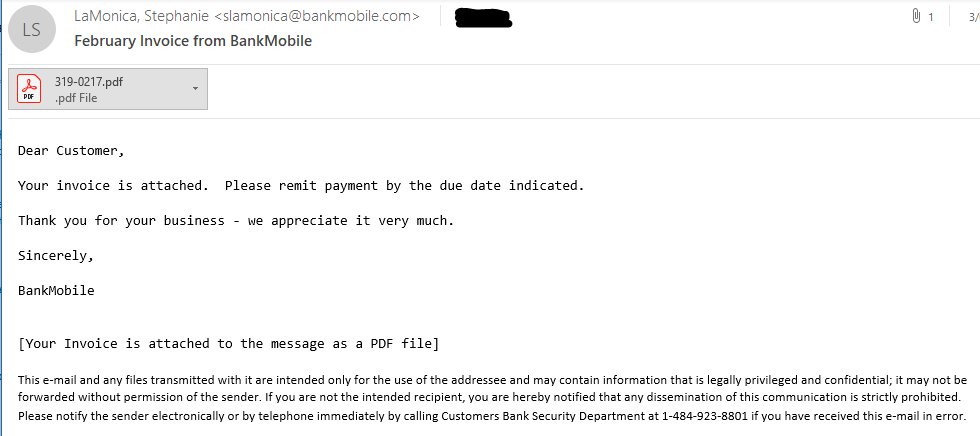
Question 4: Are there email security mechanisms (SPF, DKIM, and DMARC) in the header that can vouch for the authenticity of the message?

Question 5: Phish or Legit? (This one is difficult because the answer to question 1 appears to conflict with the answers to most of the other questions. Any guesses about what happened?)

## Message 3

Your head accountant forwards the following email to you, asking if it is legitimate. Note: The email address of the accountant has been changed to “redacted” for privacy reasons.

### The email as displayed to the user



Question 1: Is there anything suspicious in this email? When you open the attachment (carefully, in a Virtual Machine you can dispose of) it appears to be a normal bill. When you submit the attachment to VirusTotal.com, no virus is detected.

### The email headers

Here is the header:

Received: from CY1PR02MB1200.namprd02.prod.outlook.com (10.163.16.142) by

BN3PR02MB1192.namprd02.prod.outlook.com (10.162.168.18) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384) id

15.1.947.12 via Mailbox Transport; Mon, 6 Mar 2017 16:20:55 +0000

Received: from CY1PR0201CA0001.namprd02.prod.outlook.com (10.163.30.139) by

CY1PR02MB1200.namprd02.prod.outlook.com (10.163.16.142) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384) id

15.1.947.12; Mon, 6 Mar 2017 16:20:54 +0000

Received: from CY1NAM02FT045.eop-nam02.prod.protection.outlook.com

(2a01:111:f400:7e45::202) by CY1PR0201CA0001.outlook.office365.com

(2a01:111:e400:58b9::11) with Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384) id 15.1.947.12 via

Frontend Transport; Mon, 6 Mar 2017 16:20:54 +0000

Authentication-Results: spf=pass (sender IP is 216.205.24.197)

smtp.mailfrom=bankmobile.com; brcc.edu; dkim=none (message not signed)

header.d=none;brcc.edu; dmarc=permerror action=none

header.from=bankmobile.com;

Received-SPF: Pass (protection.outlook.com: domain of bankmobile.com

designates 216.205.24.197 as permitted sender)

receiver=protection.outlook.com; client-ip=216.205.24.197;

helo=us-smtp-delivery-197.mimecast.com;

Received: from us-smtp-delivery-197.mimecast.com (216.205.24.197) by

CY1NAM02FT045.mail.protection.outlook.com (10.152.75.111) with Microsoft SMTP

Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384) id

15.1.947.7 via Frontend Transport; Mon, 6 Mar 2017 16:20:53 +0000

Received: from PHOENICASOP2.NCB.INTERNAL (50.235.63.91 [50.235.63.91])

(Using TLS) by us-smtp-1.mimecast.com with ESMTP id

us-mta-57-1bwkyYpRPvyivPm-6ijJpg-1; Mon, 06 Mar 2017 11:20:49 -0500

Received: from PHOENIMBXOP5.NCB.INTERNAL ([fe80::25ed:2a6a:5001:6ebf]) by

PHOENICASOP2.NCB.INTERNAL ([::1]) with mapi id 14.03.0319.002; Mon, 6 Mar

2017 11:20:39 -0500

From: "LaMonica, Stephanie" <slamonica@bankmobile.com>

To: "redacted@brcc.edu" <redacted@brcc.edu>

Subject: February Invoice from BankMobile

Thread-Topic: February Invoice from BankMobile

Thread-Index: AdKWjRZ8z5jQxpIuShCFu8gkG816yA==

Date: Mon, 6 Mar 2017 16:20:39 +0000

Message-ID: <45F4D3605ADE3B41B362F22C158A7ABA2B243AC1@PHOENIMBXOP5.NCB.INTERNAL>

Accept-Language: en-US

Content-Language: en-US

X-MS-Has-Attach: yes

X-MS-TNEF-Correlator:

x-originating-ip: [192.168.90.46]

MIME-Version: 1.0

X-MC-Unique: 1bwkyYpRPvyivPm-6ijJpg-1

Content-Type: multipart/mixed;

boundary="\_004\_45F4D3605ADE3B41B362F22C158A7ABA2B243AC1PHOENIMBXOP5NCB\_"

Return-Path: slamonica@bankmobile.com

X-MS-Exchange-Organization-Network-Message-Id: 2a2e518f-a6ff-481b-0a55-08d464acc353

X-EOPAttributedMessage: 0

X-EOPTenantAttributedMessage: 59b96094-b5c8-4ea9-9352-65eb3d51990f:0

X-MS-Exchange-Organization-MessageDirectionality: Incoming

X-Forefront-Antispam-Report: CIP:216.205.24.197

Question 2: Compare the message headers Return-Path and From. If the user clicks “reply”, the message will be sent to the Return-Path address. Is there anything suspicious?

Question 3: What is the first server to receive the email, and where did the message originate? Give the domain name and IP address. Look up the IP address at [www.arin.net](http://www.arin.net). Where is that address?

Question 4: Are there email security mechanisms (SPF, DKIM, and DMARC) in the header that can vouch for the authenticity of the message?

Question 5: Phish or Legit?

Some links FYI

<https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol>

SMTP Transport Example

<https://en.wikipedia.org/wiki/MIME>

Multipart Messages

<https://www.howtogeek.com/108205/htg-explains-what-can-you-find-in-an-email-header/>

header troubleshooting