Saved With A Click

Spam & Phishing

Presented by:

Ottawa Public Library

National Capital FreeNet

National Capital FreeNet | Libertel de la Capitale Nationale

Agenda

- Email Background
- Spam
- Phishing
- Have I Been Hacked?
- Website Spoofing

Email Background

- Exchanging electronic messages first appeared in the 1960s with the advent of “time-sharing” systems
- By the mid-1970s electronic messages evolved into the form we use today

Email Background (Con’t)

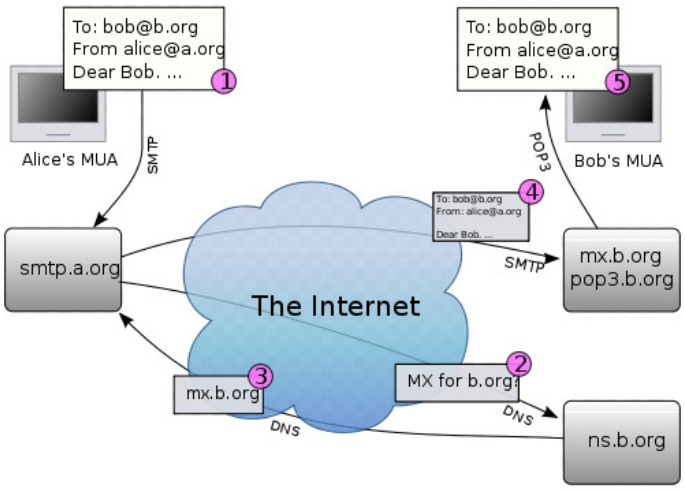
- Early versions often required users to be using the same time shared computer
- Today’s email systems do not require the sender and recipient to be on the same network or on-line at the same time

Email Background (Con't)

- Today's email systems are based on a store and forward model
- Email servers accept, forward, store and deliver messages
- Format and handling of messages is defined by the IETF (http://www.ietf.org/) in a series of RFC documents

Email Background (Con't)

- Sending and receiving email involves a suite of protocols: SMTP, POP3 and IMAP



Email Background (Con't)

- When first conceived no thought was given to the need for message privacy or integrity so messages are always sent in clear, readable text

Spam

- Spam is usually defined as unsolicited commercial email, typically in the form of marketing
- Mail server bounce or message transfer failure messages are not spam

SPAM (Con't)

- Origin of the term is unknown
- SPAM, like physical admail, is more of an annoyance than anything else because it wastes bandwidth and the time it takes to deal with it
- Governments try to regulate and control SPAM but with little effect

SPAM (Con't)

- Although fines can be significant spammers persist because it is inexpensive to do and the chance of getting caught is minimal
- Best to simply delete SPAM that makes it into you inbox
- Don't reply or try to unsubscribe, only confirms your email address is valid

SPAM (Con't)

- Most email providers offer some form of message filtering to reduce the amount that makes it through to the inbox
- Other forms of spamming are starting to appear: smishing and vishing

SPAM (Con't)

- When registering at websites it can be prudent to provide a disposable email address
- That way if the amount of messages from the website becomes excessive you can simply delete the email address

PHISHING

- A subclass of spam often employing social engineering to obtain credentials (via fake websites) or to install malware
- Phishing attempts can come in several forms: email, social media, phone call or text message

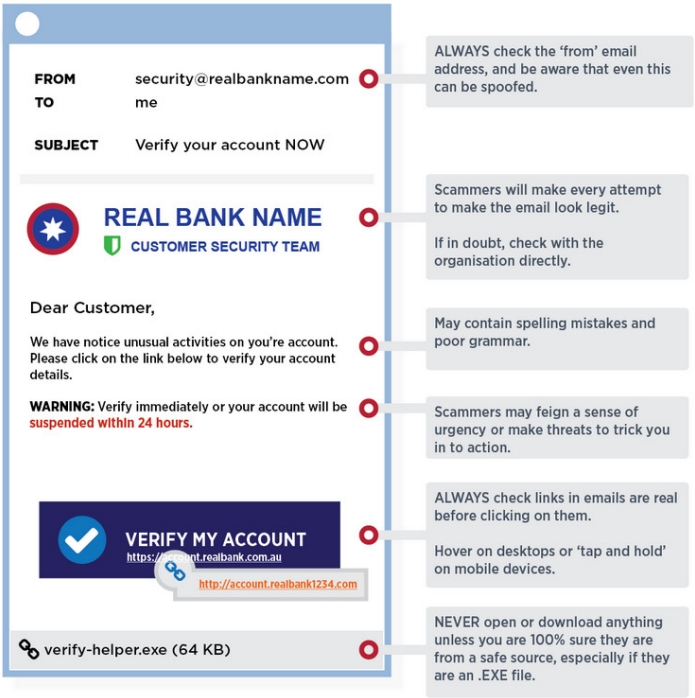
PHISHING (Con't)

- Messages designed to look legitimate often mimicking legitimate organizations
- Warning signs include:
  - Not addressing you by name
  - Spelling and grammar mistakes
  - Conveying a sense of urgency

PHISHING (Con't)

- Common scenarios include:
  - Asking you to:
    - verify your personal or login information
    - confirm an on-line purchase
    - verify credit card details
  - Offering prizes for completing a survey
  - Convey a sense of urgency

PHISHING (Con't)



PHISHING (Con't)

- Protect yourself by:
  - Not clicking links or opening attachments
  - Search names or exact wording to check for scam reports
  - Never providing personal or financial information
  - Use your own bookmark to visit sites

PHISHING (Con't)

- Other common forms include:
  - Spear phishing - targets business with personalized email designed to look from a trusted source
  - Pharming - redirects you to a fake version of a legitimate website via a poisoned DNS entry

PHISHING (Con't)

- Check your email phishing knowledge

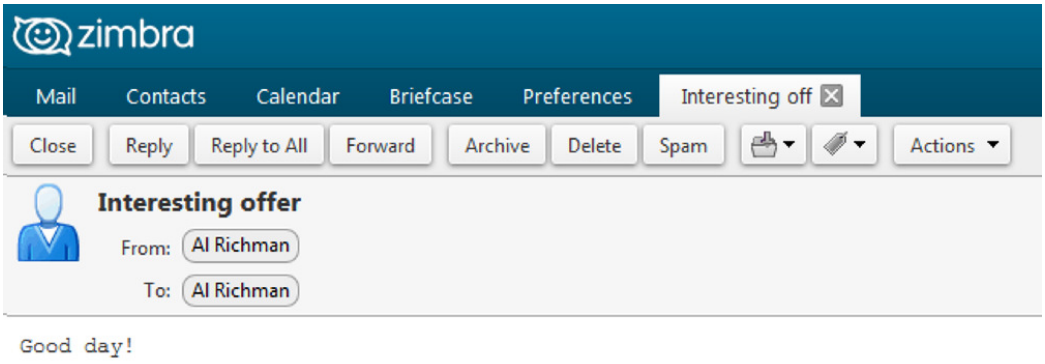
  https://www.sonicwall.com/en-us/phishing-iq-test-landing

Have I Been Hacked?

- Email spoofing which involves falsifying email sender information is rampant
- Email software usually hides the message envelop or header but it is key to understanding where the message really came from

Have I Been Hacked? (Con't)

- Here is what we usually see



Have I Been Hacked? (Con't)

- Here is what the header really is

```
Return-Path: XXXXX@ncf.ca
Received: from localhost (LHLO mail.ncf.ca) (127.0.0.1) by pallando.ncf.ca
 with LMTP; Wed, 21 Jan 2015 06:25:09 -0500 (EST)
Received: from mail.ncf.ca (localhost [127.0.0.1])
        by mail.ncf.ca (Postfix) with ESMTP id 26C239FA0E
        for <XXXXX@ncf.ca>; Wed, 21 Jan 2015 06:25:09 -0500 (EST)
Received: from mx2.ncf.ca (radagast.ncf.ca [134.117.136.59])
        by mail.ncf.ca (Postfix) with ESMTP id 11D299F7BE
        for <XXXXX@ncf.ca>; Wed, 21 Jan 2015 06:25:09 -0500 (EST)
Received: from mx2.ncf.ca (localhost [127.0.0.1])
        by mx2.ncf.ca (Postfix) with ESMTP id A4B5D8335B
        for <XXXXX@ncf.ca>; Wed, 21 Jan 2015 06:25:16 -0500 (EST)
Received: from [115.79.52.167] (unknown [115.79.52.167])
        by mx2.ncf.ca (Postfix) with ESMTP id E98288332B
        for <XXXXX@ncf.ca>; Wed, 21 Jan 2015 06:25:15 -0500 (EST)
Message-ID: <430572C99E34BE256314AFF8B6866BAF@4V67LC3V48>
From: <XXXXX@ncf.ca>
To: <XXXXX@ncf.ca>
Subject: Interesting offer
Date: 21 Jan 2015 23:59:06 +0600
MIME-Version: 1.0
Content-Type: text/plain;
        charset="cp-850"
Content-Transfer-Encoding: 8bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5931
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.5931
X-AV-Checked: ClamAV using ClamSMTP
X-NCF-Filtered: By ProxSMTP on pallando Wed Jan 21 06:25:09 2015 -0500 (EST)
```

Have I Been Hacked? (Con't)

- Email header analysis is easy using https://mxtoolbox.com/EmailHeaders.aspx

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	unknown 115.79.52.167	mx2.ncf.ca	ESMTP	1/21/2015 11:25:15 AM	
2	1 Second	mx2.ncf.ca 127.0.0.1	mx2.ncf.ca	ESMTP	1/21/2015 11:25:16 AM	
3	*	mx2.ncf.ca 134.117.136.59	mail.ncf.ca	ESMTP	1/21/2015 11:25:09 AM	
4	0 seconds	mail.ncf.ca 127.0.0.1	mail.ncf.ca	ESMTP	1/21/2015 11:25:09 AM	
5	0 seconds	localhost 127.0.0.1	pallando.ncf.ca	LMTP	1/21/2015 11:25:09 AM	

Have I Been Hacked? (Con't)

- If your email address has been spoofed it doesn't mean you have been hacked and there is nothing you can do about it
- Usual signs that your email address has been spoofed are server bounce messages or others asking why you sent them a message

Have I Been Hacked? (Con't)

- Signs that you may have been hacked:
  - You can't login to retrieve email
  - Messages appear in your *Sent Folder* that you didn't send
  - Messages you are expecting never arrive

Have I Been Hacked? (Con't)

- Steps to take if you were hacked:
  - Change your account password
  - Recover your account if locked out
  - Change account recovery options
  - Check all auto response settings and other automated message rules
  - Check related accounts tied to your email

Have I Been Hacked? (Con't)

- Steps to take if you were hacked:
  - Change passwords for all other accounts that used the same password
  - Advise your contacts to be alert for possible spam sent by the hacked account
  - Regularly back up your email account and associated contacts

Website Spoofing

- Fake website designed to mimic a legitimate site
- Usually part of an email phishing scam
- Attempts to trick you into providing personal and/or financial information

Website Spoofing (Con't)

- Telltale signs of a fake website:
  - Site URL is incorrect
  - Asks for personal or financial information
  - Low resolution graphics
  - Poor spelling and grammar
  - Not a secure website (http**s**://)

Website Spoofing (Con't)

- Be careful when typing URL address to avoid landing on a fake site
- If unsure about a domain:
  - Check it with a WHOIS query (e.g. https://who.is/)
  - Enter it in a search engine
  - Verify the contact information

Website Spoofing (Con't)

- If you end up at a fake site:
  - LEAVE IT IMMEDIATELY
  - Report it to:
    - The legitimate site owner
    - Google https://safebrowsing.google.com/safebrowsing/report_badware/

Website Spoofing (Con't)

- Check your website spoofing knowledge

https://www.opendns.com/phishing-quiz/


QUESTIONS