For the Record...

DISSECTING THE MALICIOUS EMAIL

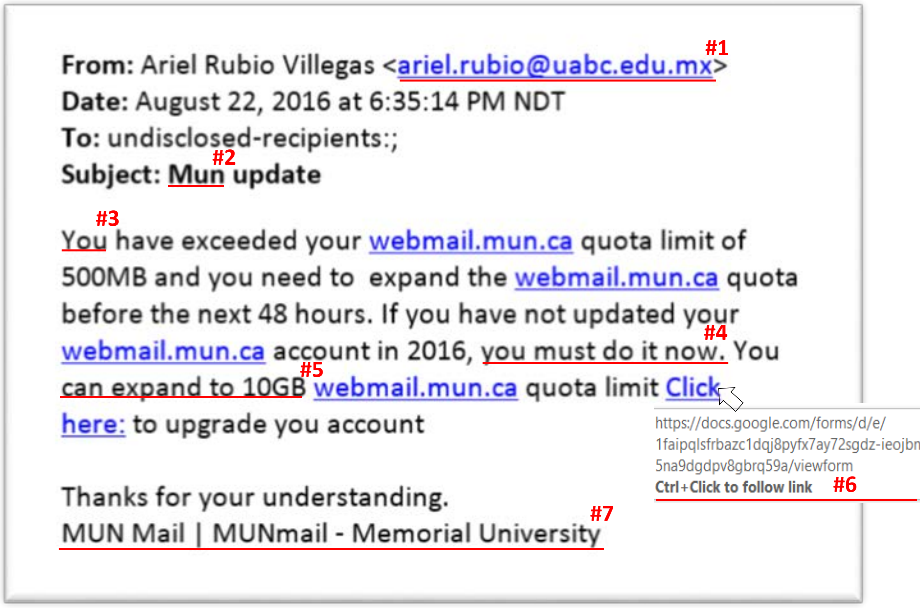
Overview

Cyber-attacks have become increasingly sophisticated and difficult to detect, and malicious email is one of the most common forms of attack. Better known as *spam*, Memorial University is receiving more and more of these emails every day. In the past year, the daily average number of emails received at the St. John's campus has tripled to about 2.7 million. While more than 90 percent of these incoming email are blocked each day, some still get through – and everyone must do their part to protect themselves and the University.

By clicking on a phony link in an email or opening an attachment, you may unknowingly put yourself and Memorial at risk. Malicious emails appear to come from legitimate sources. These malicious emails include fake invoices requesting payment, notices that your email quota has been exceeded, or warnings that your account has been accessed with a request to log in to verify your account. Cyber-attackers try to gain access to both your personal and University information by getting you to click on phony links. They also try to get you to open attachments filled with viruses that can infect and damage your computer, or ransomware that locks your files until you pay to get them back.

How to detect a malicious email

Here's an example of a recent phishing email received by some Memorial email users. There are seven signs that this is not a legitimate email:



From: Ariel Rubio Villegas <ariel.rubio@uabc.edu.mx>
Date: August 22, 2016 at 6:35:14 PM NDT
To: undisclosed-recipients:;
Subject: Mun update

You have exceeded your webmail.mun.ca quota limit of 500MB and you need to expand the webmail.mun.ca quota before the next 48 hours. If you have not updated your webmail.mun.ca account in 2016, you must do it now. You can expand to 10GB webmail.mun.ca quota limit Click here: to upgrade you account

https://docs.google.com/forms/d/e/1faipqlsfrbazc1dqj8pyfx7ay72sgdz-ieojbn5na9dgdpv8gbrq59a/viewform
Ctrl+Click to follow link

Thanks for your understanding.
MUN Mail | MUNmail - Memorial University

Signs of a malicious email

#1 – It purports to be from someone at MUN, but the email address is not a MUN email.

#2 – Mun is lower case in the subject line; it should be MUN.

#3 – The email is not directly addressed to you.

#4 – An urgent request for action.

#5 – It entices you to take action with the promise of a reward.

#6 – When you hover your cursor over the link, you can see it's not a MUN web address.

#7 – It does not provide contact information or a valid MUN unit/department.

For the Record...

What you can do to protect yourself

If something seems suspicious or does not feel right, it may be a cyber-attack.

Additional advice includes:

- Never click on web links or attachments in emails from unknown sources
- Never disclose your username and password. Look for signs to identify potentially malicious emails, including:
    - Requests for payment
    - Requests for your username and password
    - Hover your cursor over the web link to see if the website address is different than what appears in the body of the email
    - Slight variations, such as transposed letters, in the email address or website address
    - Spelling errors in the email
    - Unusual greetings
    - Requests for a quick response
- Use your Memorial email account for University business only and use a separate email account for personal matters, such as online shopping, banking, or sending and receiving jokes.
    - Keeping business and personal emails separate increases your chances of being able to identify what you should and shouldn't be receiving in each of your email accounts.
- Back up your files properly. If your backup drive is connected to your computer, it can also be affected by malware. If you need a managed backup service, contact your local IT support person or the ITS Service Desk at 864-4595 or help@mun.ca.
- If you receive a suspicious email, or if you believe you've downloaded a virus or ransomware file:
    - **Phone your ITS Service Desk immediately: 709-864-4595 (St. John's); (709) 639-2049 (Grenfell); 709-778-0628 (Marine Institute).**
    - Do not forward the message to others as a warning; this expands the number of email accounts that could potentially be affected.