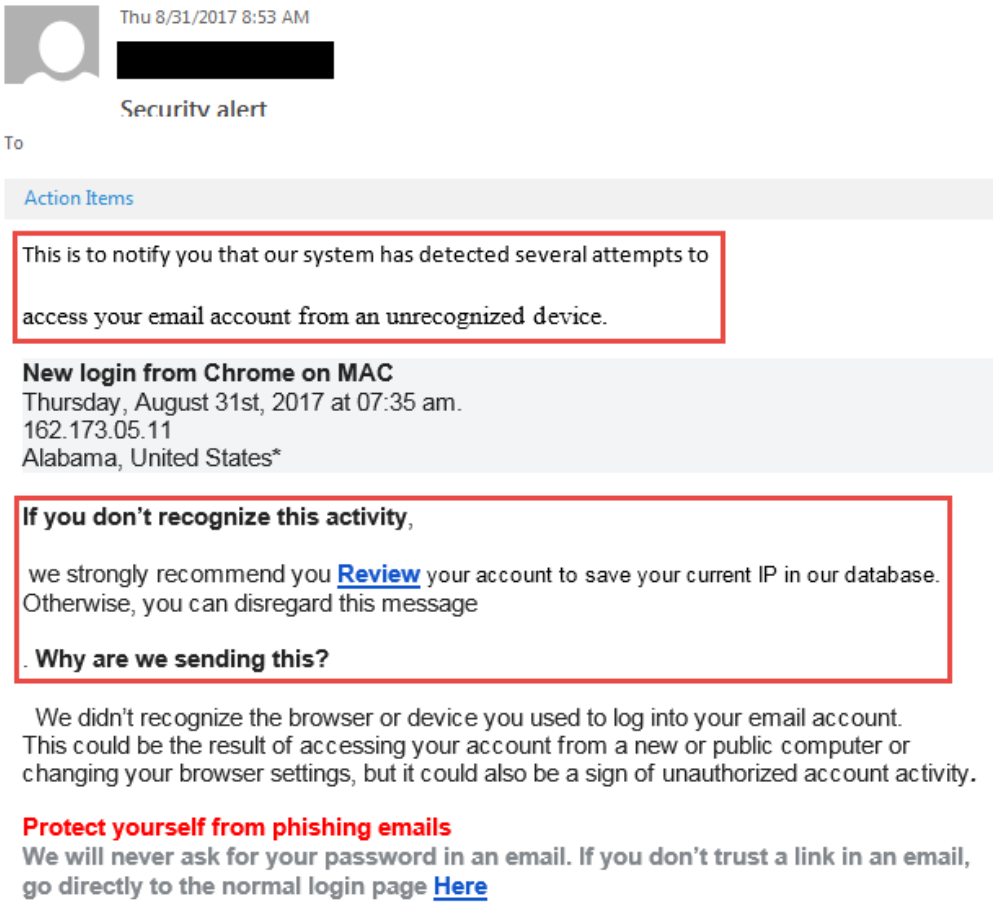
Phishing Emails: Tips from a Staff Senator

These are by no means official instructions. They are tips that staff senators have gathered from ITS during the various phishing attempts and gathered from other staff members.

Contents

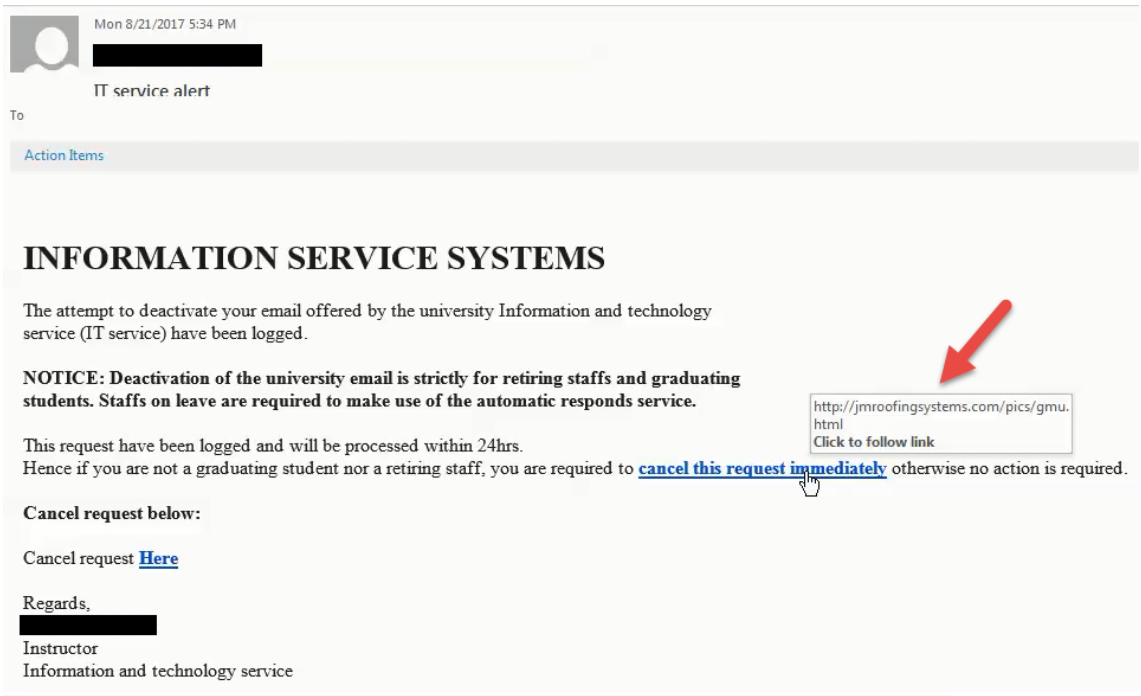
What to look out for

- Poor grammar
- Poorly formatted email (see below)
- Suspicious or unusual requests
    - Emails asking for personal information, passwords, etc.
- A link without the s in https://
    - The s means it's a secure site
- Example: lines of text are broken in strange places and punctuation on the wrong lines, etc.



Things to check if you suspect phishing

- Double click on the sender's name: look at the email. *Sometimes* the email will not match the name, or the email will not be a Mason email.
    - Do NOT assume that emails are okay if they are from a gmu.edu address. Phishing attempts can use a gmu.edu address or use a compromised Mason account.
- Hover over the link they sent (but DO NOT click on it) to see if the URL is suspicious.
    - Although when you click on the link, the website may look like a Mason website, hovering over the link should show the true URL (see examples below).



Mon 8/21/2017 5:34 PM

[redacted]

IT service alert

To

Action Items

INFORMATION SERVICE SYSTEMS

The attempt to deactivate your email offered by the university Information and technology service (IT service) have been logged.

NOTICE: Deactivation of the university email is strictly for retiring staffs and graduating students. Staffs on leave are required to make use of the automatic responds service.

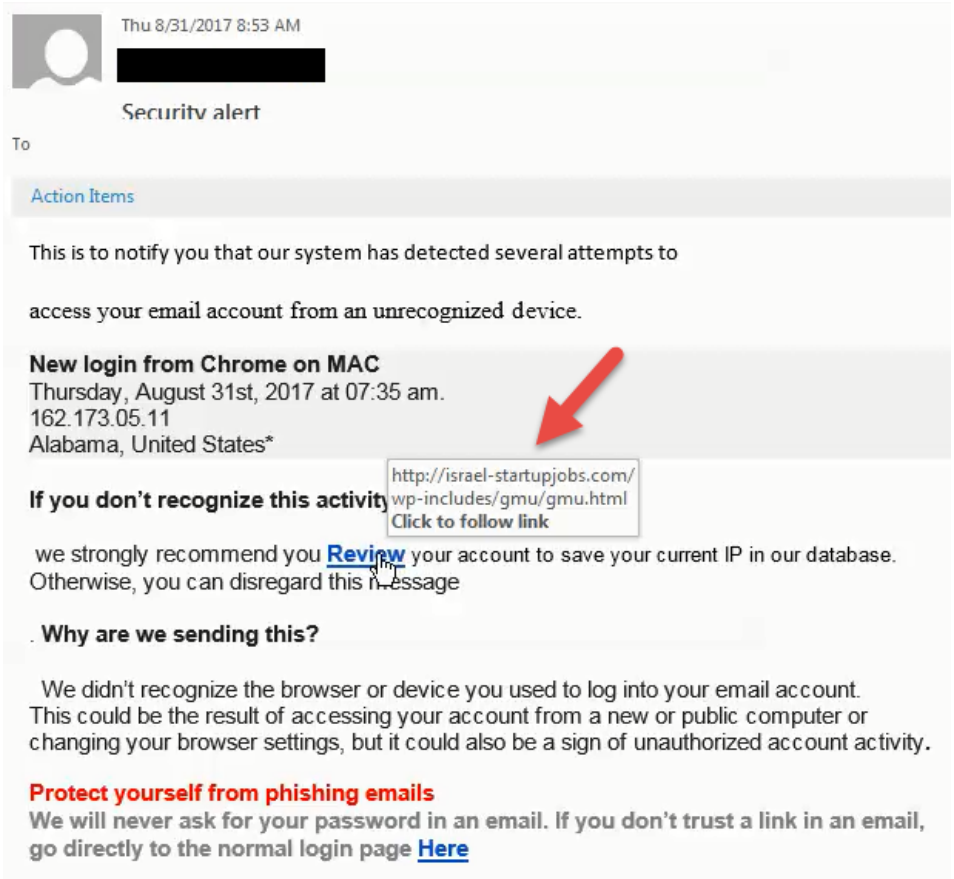
This request have been logged and will be processed within 24hrs.
Hence if you are not a graduating student nor a retiring staff, you are required to **cancel this request immediately** otherwise no action is required.

http://jmroofingsystems.com/pics/gmu.html
Click to follow link

Cancel request below:

Cancel request **Here**

Regards,
[redacted]
Instructor
Information and technology service



Thu 8/31/2017 8:53 AM

[redacted]

Security alert

To

Action Items

This is to notify you that our system has detected several attempts to

access your email account from an unrecognized device.

New login from Chrome on MAC
Thursday, August 31st, 2017 at 07:35 am.
162.173.05.11
Alabama, United States*

http://israel-startupjobs.com/wp-includes/gmu/gmu.html
Click to follow link

If you don't recognize this activity

we strongly recommend you **Review** your account to save your current IP in our database.
Otherwise, you can disregard this message

. **Why are we sending this?**

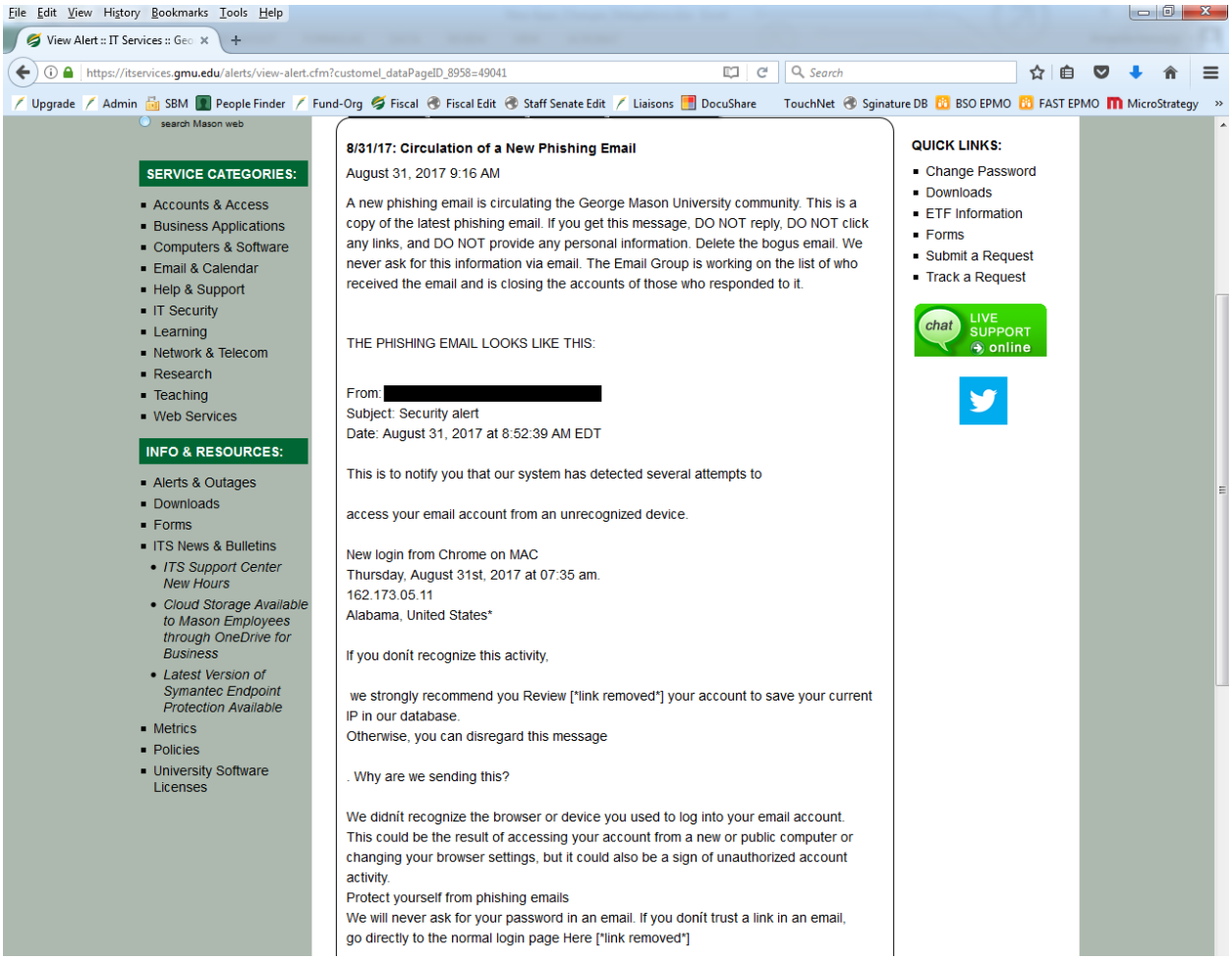
We didn't recognize the browser or device you used to log into your email account.
This could be the result of accessing your account from a new or public computer or changing your browser settings, but it could also be a sign of unauthorized account activity.

Protect yourself from phishing emails
We will never ask for your password in an email. If you don't trust a link in an email, go directly to the normal login page Here

- Check the ITS Alerts page to see if this specific email has been reported: https://itservices.gmu.edu/alerts/index.cfm.
    - Click on Security Alerts.
    - Look for alerts for the date the email arrived and click to Read More.

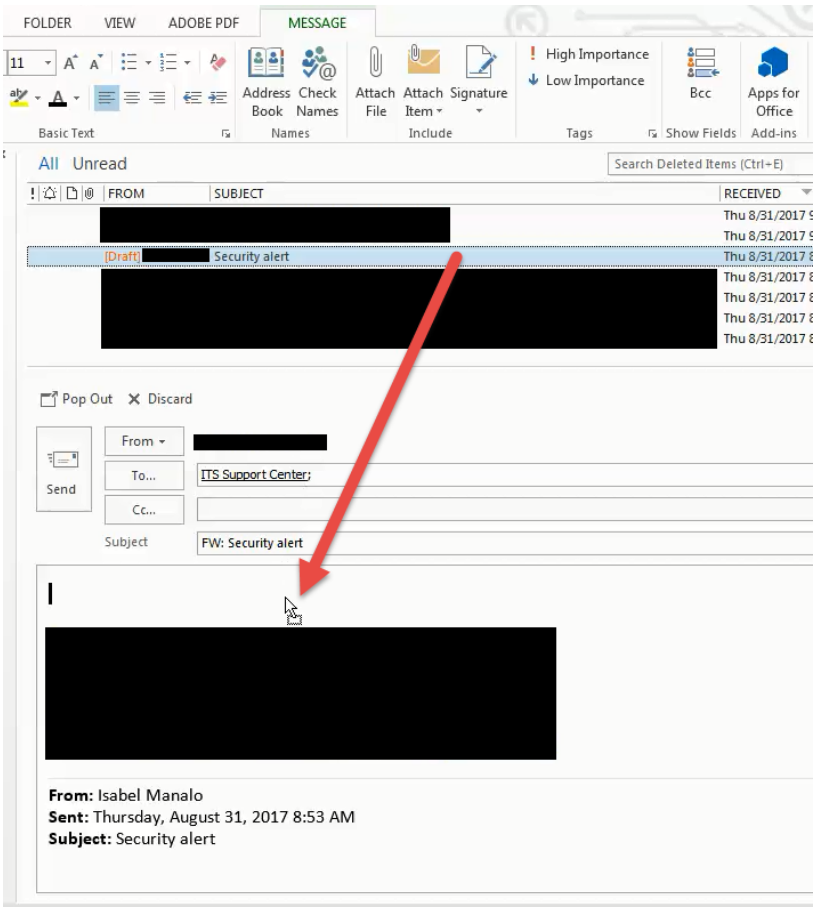
- This will show the specific email, so you can check if it's the one you got.
- Note: there may be multiple alerts for a single day, so be sure to check all alerts for the day you received the email.

o Example: ITS alert for the email from 8/31/2017 with subject "Security Alert" (above):

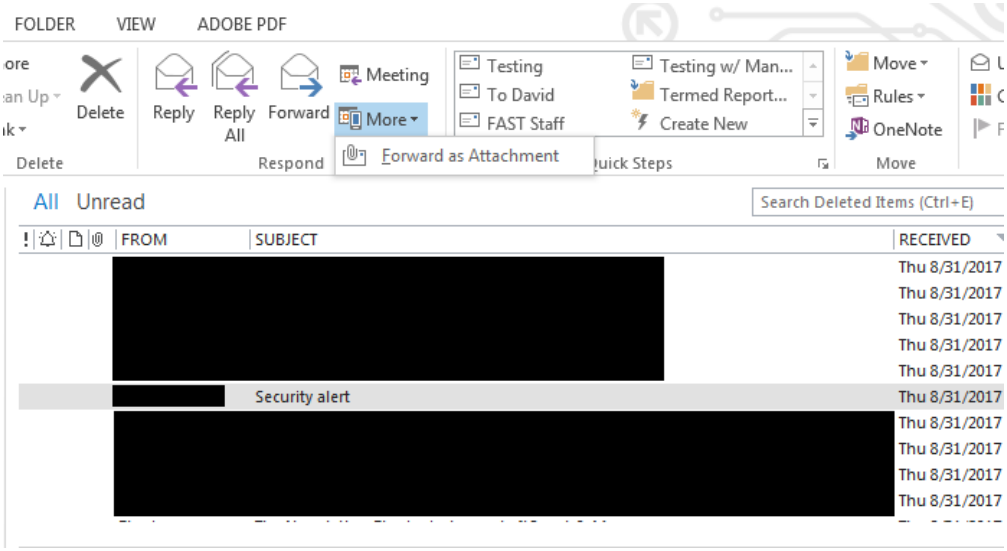


Forwarding phishing emails to the ITS Support Center

- If you forward the email to the ITS Support Center (support@gmu.edu), you should *attach* the email too.
  - Attaching the email gives the security office more information like where the email originated from, etc.
  - Attaching an email:
    - Click on the email you are forwarding and drag it down to the body/message of the email you are forwarding.



OR



If you clicked the link and entered credentials

- Change your password as soon as you realize it at https://password.gmu.edu.

- Contact the ITS Support Center at 703-993-8870 or support@gmu.edu to report that you were a responder to a phishing email.
    - Don't be embarrassed to report if you've responded! It could be your personal information that was compromised, as well as, university information.

Other Resources

- Watch the *Avoiding Phishing Scams* video on https://www.lynda.com/.
- Review some general information on phishing emails on the IT Security Office's website: http://itsecurity.gmu.edu/Resources/Phishing.cfm.
- Recent phishing attempts at Mason: http://itservices.gmu.edu/alerts/.

October: National Cyber Security Awareness Month

- See the schedule of events here: http://itsecurity.gmu.edu/Resources/cybersecurity.cfm.
- The IT Security Office is offering a giveaway for National Cyber Security Awareness month:
    - Go to https://www.lynda.com/, search for the *Avoiding Phishing Scams* video, and watch it.
    - Once you've watched, click on your profile in the top right corner and choose certificates from the drop down. Save your certificate as a PDF and email it to itsinfo@gmu.edu.
    - You will be entered in a drawing for a $10-$25 gift card.