Examples of phishing emails that appear to come from MIT

See also

- What is a phishing email?

Things to look for to identify phishing messages

There have been several variations of emails that appear to be coming from a legitimate MIT email address, but which, in fact, are not. Many of these emails appear to come from either the MIT network group or the MIT email account team. Never reply to these kinds of emails.

Things to look for to verify if the email is a phishing email:

- Spelling errors and bad grammar
- Odd formatting (e.g., incorrect use of capital letters or punctuation)
- No real person's name included in either the greeting or signature of the email
- A return or reply-to email address that is not from mit.edu. You can view "full headers" to see what is listed as the actual return address.
- If a password is being requested, you know the email is not legitimate. No legitimate business will ever request your password. Look at what else is being requested as well (e.g., requesting your sex and country or territory should be a tip off that this would never come from MIT)
- A fake phone number, email or person listed as the contact information
- No mention of a phone number to call or person to contact
- Deleting an account due to lack of response or reaching a "quota": MIT doesn't do things like this to our community.

Examples

Below are just a few of the many examples of these emails (spelling errors and typos have been kept intact). They are all based on the same premise:

According to these emails, you need to confirm your account by supplying a username and password, otherwise your email account or some other MIT subscription will be deactivated. MIT would never take such action, threaten deactivation, or ask an MIT email account holder to confirm their account through email.

These messages are not coming from MIT
Although these messages may appear to be coming from MIT, they are in fact from an address that has either been hacked or simulated. MIT will never ask you to confirm or supply your passwords. These messages are an attempt to steal your username and password for illegitimate purposes. **DO NOT REPLY TO THESE MESSAGES OR CLICK ON THE LINKS OR ATTACHMENTS WITHIN THEM! Just delete them.**

Example 1: This email appears to be from MIT Libraries.

What gives this away: This one is difficult to spot as bogus, but the name, address and phone number are not legitimate. If an email has a signature with contact information, it is a good idea to try to contact the person before responding.

```
Subject line: ILLiad Access

Dear User,

Your access to the ILLiad is expiring soon and it won’t be accessible for you. You must reactivate your account in order to continue to have access to this service. For this purpose, click the web address below or copy and paste it into your web browser. After logging in, your access is reactivated and you will be redirected to your ILLiad profile.

https://idp.mit.edu/idp/Authn/MIT_A5L9LVR8LBB23A7EG5GTuQGm88v0LGTuQB00JA4fuyI2X61J3JELU8L9NGJDFM3LF-13.
```
If you are not able to login, please contact Joe Follett at jfollett@mit.edu for immediate assistance.

Sincerely,

Joe Follett
Access Services Manager
MIT Libraries
617.258.5937
jfollett@mit.edu

Example 2: This email appears to be coming from “helpdesk@mit.edu.”

What gives this away: MIT will never threaten to terminate your account for reaching your quota. Any email from IS&T about webmail will be signed by a real person from IS&T with their name and contact information.

Subject line: Webmail alert
Dear User,
Your WebMail has exceeded the allocated monthly quota.
To avoid account termination, kindly click on our website below to restore your account.
www.mit.edu
Thank you.
Massachusetts Institute of Technology

Example 3: This one is using a similar message as Example 2 above.

What gives this away: Any email about MIT mailbox quotas will come from Microsoft Exchange Server (not a person). The “from” email address was of a person who is not from the IT Help Desk. Be informed: What happens when a mailbox goes over quota?

Subject line: Web-mail Urgent Update
Dear Web-mail User,
Your mailbox is almost full.
Current size 20GB of 23GB.
Your mailbox is almost full CLICK HERE (link) and Re-login again with your email information for the update to be effected.
IT Help Desk.
Massachusetts Institute Of Technology
This has become necessary to serve you better.
Copyright ©2014

Example 4: This email appeared to be coming from “info@mit.edu.”

What gives this away: The use of exclamation marks and bad grammar, an unclear message about the issue, as well as no name or contact information.

Subject line: Urgent News!
Hello,
Your two incoming mails is on pending status due to our recent database upgrade. Please log-on to the new MIT WebMail Upgrade Access using the link provided below to login for online account upgrade and await Help desk. We apologize for any inconvenience and appreciate your understanding. (A link to Google docs was inserted here.)
Sign,
Example 5: This email appeared to be coming from "webmaster@mit.edu."  
What gives this away: Use of bad grammar, the request for a password (IS&T never asks for this) and no name or contact information.

Subject line: System Upgrade

Good day.

This is to inform you that we will be undergoing system upgrade and maintenance of our systems between 5pm-7pm today. As a result you will be required to provide us with your password and other necessary information in order for us to upgrade your webmail. Once again we are sorry for any inconveniences this might cause you.

Regards,
MIT team.

Example 6: This email appeared to be coming from "accountupgrade@MIT.EDU." There have been various iterations of this same message.  
What gives this away: IS&T never asks for personal information through email, the lack of an official signature and use of exclamation marks.

Subject line: Verify Your Mit Account Now

Dear Mit Account Owner,

This message is from Mit messaging center to all Mit email account owners. We are currently upgrading our data base and e-mail account center. We are deleting all Mit email account to create more space for new accounts.

To prevent your account from closing you will have to update it below so that we will know that it’s a present used account.

****************************************************
CONFIRM YOUR EMAIL IDENTITY BELOW
Email Username : ............ .......
EMAIL Password : ...............
Date of Birth : ...............
Country or Territory : ..........
****************************************************

Warning!!! Account owner that refuses to update his or her account within Seven days of receiving this warning will lose his or her account permanently.

Thank you for using Mit!
Warning Code: VX2G99AAJ

Thanks,
Mit Team
mit.edu BETA

Example 7: This email has come from various addresses.  
What gives this away: One version didn’t even spoof an MIT address, using "gcimanagement@gci.net" and appeared to come from GCI Webmail Management. Another ‘from’ address was "mitaccountmanagement@MIT.EDU." The threatening language, exclamation marks and lack of signature also give this one away.

Subject line: Confirm Your Mit Webmail Account

Dear Mit Webmail Subscriber,

To complete your Mit Webmail account, you must reply to this email immediately and enter your password here (*********)

Failure to do this will immediately render your email address deactivated from our database.

You can also confirm your email address by logging into your Mit Webmail account at //webmail.mit.edu/

Thank you for using Mit Webmail!

THE Mit Webmail TEAM
Example 8: This email took advantage of the growing awareness of these kinds of email scams. 
What gives this away: IS&T has no PO Box, never asks for personal information through email, the odd phone number, use of a yahoo.com return email address, a fictional name within the signature.

Subject line: International World Scam Alert

WEBMAIL MIT EDUCATION:
P O Box 02139-4307 77 massachusetts avenue cambridge, ma (Customer Services)

INTERNATIONAL WORLD SCAM ALERT

This is to inform you that mails are been sent to email address all over the world and they are all scams. So be more carefull on how you get along with them. So please you have to co-operate with us on how we fight them please send the following informations so we put up a scam alert on your emil address.... Alert Code:iwsamitc175

1.Name in full:
2.Home Address:
3.Age:
4.Grade level:
5.username:
6.E-mail password:
7.Phone Number:
8.Nationality:
9.Sex:

please contact as soon;

Email:mitcustomer_service@yahoo.com
Phone Number:+191 73336663
Remember to quote your alert code number in all correspondence.

Sincerely,
Mr. Gate Woods
WEBMAIL MIT.EDU

Example 9: This email took advantage of a published MIT event.
What gives this away: Use of a gmail.com return email address, no name in the signature, vagueness around the job and who the interview is with, and requiring the recipient to download software as a first step.

Subject line: Employment Opportunity ( MIT Fall Career Fair )

From: Maureen Scott scottmaureen050@gmail.com
Sent: Wednesday, November 12, 2014 8:41 AM

Dear Applicant

Your resume on ( MIT Fall Career Fair ) has been reviewed and forwarded to the Head of Operation and you have been considered and scheduled for an online interview to discuss more about the job position that you are to occupy. You are required to set up a yahoo messenger account or download a Yahoo IM (http://messenger.yahoo.com/download/) on your desktop if you don't have one. After this process you are to add Mrs Rita Townley on her Yahoo IM, email is (ritatownley40@yahoo.com) to your yahoo buddy list ASAP for the job briefing and comprehensive details. She is online waiting to talk to you.

Venue: On line Via Yahoo Messenger
Training is Available
Human Resources

Your swift and timely response matters a lot in this beneficial position.

Best Regards.