Email Safety: Don't Be a Phishing Victim

Like many organizations, JMLS can fall prey to phishing attempts. When people outside the JMLS network obtain JMLS passwords through successful phishing (meaning JMLS users have somehow shared their password), they can then access that JMLS account and send a massive amount of other phishing emails in an attempt to look legitimate. Then spam-blocking services outside of JMLS control see that JMLS user account and our institution as a source of malicious email and block all our email.

Email Safety Best Practices

Don't Click on Links in Email

The ITS department at JMLS will **never** send you email that asks you to click on a link to reset your password or for any other reason. Resetting your password should always and only be done via password.jmls.edu. You can always reach this page via the "Password change" link under Quick Links in eCommons.

What Is Phishing?

Phishing occurs when a person attempts to acquire personal or confidential information, such as usernames, passwords, and financial details, by posing as a known or trusted contact via email, instant messaging, or a website.

Forward Any Suspicious Email to the Help Desk

If you receive any email that requests your username and password, IMMEDIATELY be wary. Do not reply. Forward these messages to the Help Desk at helpdesk@jmls.edu and request that a Help Desk Analyst review the email. Also send any undeliverable notices to the Help Desk.

Check your Browser's Address Bar

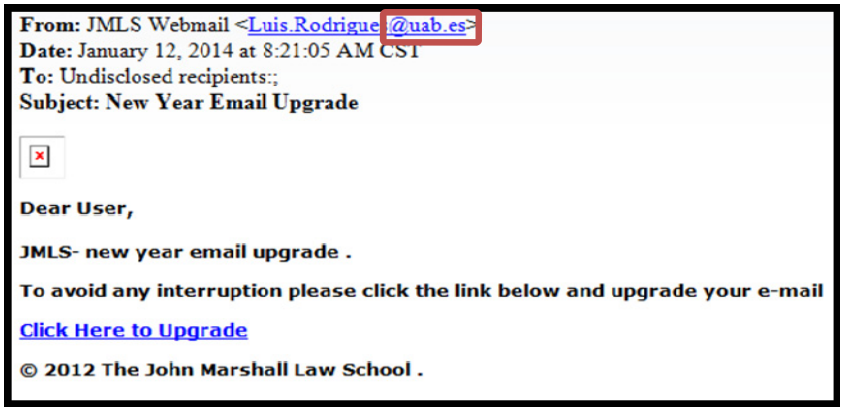
Check the address bar of your web browser to make sure it is a "jmls.edu" web address when accessing a school site.

Key Email Safety Tips

- Never supply your password via email or over the internet.
- ITS will never ask you to click on a link and then provide this information.
- Check the address bar at the top of your web browser.
- Contact the Help Desk with concerns and forward any suspicious email.
- Make sure all email addresses you send to are current and valid.

Phishing Email Examples

Here is an example of a phishing email. Note that this email claims to be from "JMLS Webmail," but the email address next to it does NOT come from a @jmls.edu account. Additionally, the message asks you to click on a link, which is something that ITS will no longer ask you to do.


From: JMLS Webmail <Luis.Rodrigue[illegible]@uab.es>
Date: January 12, 2014 at 8:21:05 AM CST
To: Undisclosed recipients:;
Subject: New Year Email Upgrade

Dear User,

JMLS- new year email upgrade .

To avoid any interruption please click the link below and upgrade your e-mail

Click Here to Upgrade

© 2012 The John Marshall Law School .

Here is another example. Note that this phishing attempt appears as if it comes from JMLS. This can be tricky, but note that it also asks you to click on a hyperlink to view a message. This is something that ITS will never ask you to do, so watch out for this type of scam.

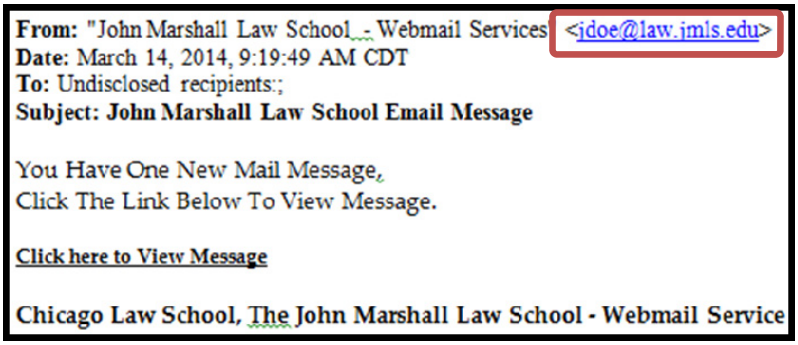

From: John Marshall Law School <online.service@jmls.edu>
Date: April 6, 2014 at 1:10:28 PM CDT
To: <rdonnell@jmls.edu>
Subject: 1 New Mail Message From JMLS ,

You Have One New Important Message,
Click The Link Below To View Message.

Click here to View Message

Chicago Law School, The John Marshall Law School

In this last example, this phishing attempt appears to come from a JMLS student address. This message was sent from a compromised student account (the email address was changed for privacy) that was used to send additional phishing messages.


From: "John Marshall Law School - Webmail Services" <jdoe@law.jmls.edu>
Date: March 14, 2014, 9:19:49 AM CDT
To: Undisclosed recipients:;
Subject: John Marshall Law School Email Message

You Have One New Mail Message,
Click The Link Below To View Message.

Click here to View Message

Chicago Law School, The John Marshall Law School - Webmail Service

Questions?

For additional help, please contact the **ITS Help Desk** via the Help Desk Portal at helpdesk.jmls.edu, by phone at 312.427.2737 x550, or by email at helpdesk@jmls.edu. You can also visit us in Room 733, 7th floor, State Street Building.