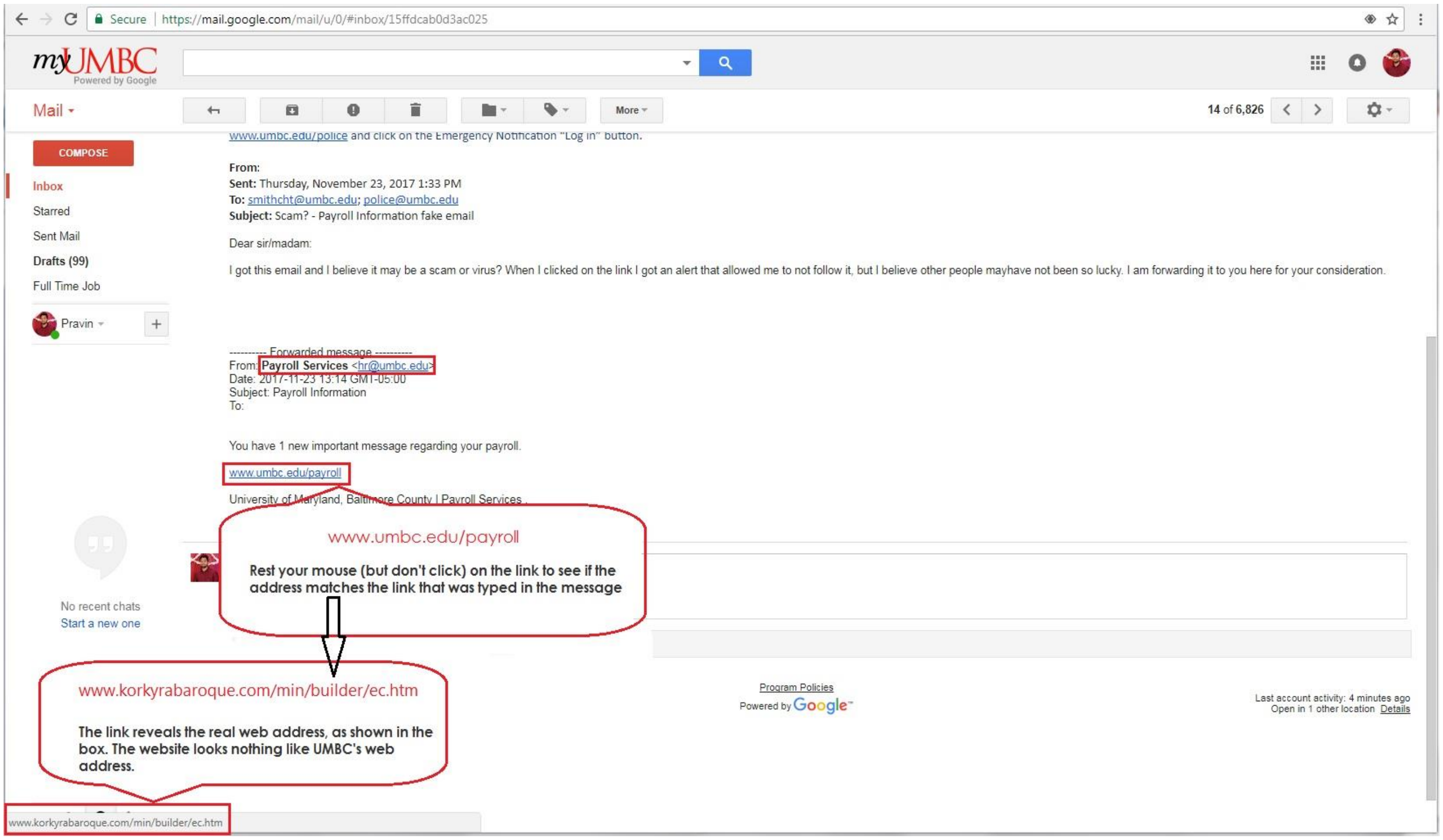
How to recognize phishing email messages and links:

Phishing email messages, websites, and phone calls are designed to steal money. Cybercriminals can do this by installing malicious software on your computer or stealing personal information off of your computer.

Cybercriminals also use social engineering to convince you to install malicious software or hand over your personal information under false pretenses. They might email you, call you on the phone, or convince you to download something off of a website.

What does a phishing email message look like?

- Spelling and bad grammar. Cybercriminals are not known for their grammar and spelling.
- Beware of links in email. If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box. The website doesn't look like UMBC's web address.


Secure | https://mail.google.com/mail/u/0/#inbox/15ffdcab0d3ac025
myUMBC
Powered by Google
Mail
More
14 of 6,826
COMPOSE
Inbox
Starred
Sent Mail
Drafts (99)
Full Time Job
Pravin
No recent chats
Start a new one
Program Policies
Powered by Google
Last account activity: 4 minutes ago
Open in 1 other location Details
www.korkyrabaroque.com/min/builder/ec.htm

www.umbc.edu/police and click on the Emergency Notification "Log in" button.

From:
Sent: Thursday, November 23, 2017 1:33 PM
To: smithcht@umbc.edu; police@umbc.edu
Subject: Scam? - Payroll Information fake email

Dear sir/madam:

I got this email and I believe it may be a scam or virus? When I clicked on the link I got an alert that allowed me to not follow it, but I believe other people mayhave not been so lucky. I am forwarding it to you here for your consideration.

---------- Forwarded message ----------
From: **Payroll Services** <hr@umbc.edu>
Date: 2017-11-23 13:14 GMT-05:00
Subject: Payroll Information
To:

You have 1 new important message regarding your payroll.

www.umbc.edu/payroll

University of Maryland, Baltimore County | Payroll Services .

www.umbc.edu/payroll

Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message

www.korkyrabaroque.com/min/builder/ec.htm

The link reveals the real web address, as shown in the box. The website looks nothing like UMBC's web address.

Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

- Threats. Have you ever received a threat that your account would be closed if you didn't respond to an email message? Cybercriminals often use threats that your security has been compromised.
- Spoofing popular websites or companies. Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.
- Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.

Please contact UMBC Police Department (police@umbc.edu) or Detective Smith (smithcht@umbc.edu) if you receive any suspicious emails.

Visit our website https://police.umbc.edu/ for more information.