



Avery Powell <averypowell16@gmail.com>

Fwd: Phishing e-mail

rthornt3@masonlive.gmu.edu <rthornt3@masonlive.gmu.edu>
To: Avery Powell <apowell9@masonlive.gmu.edu>

Fri, Nov 14, 2014 at 12:23 PM

Sent from my iPhone

Begin forwarded message:

From: "rthornt3@masonlive.gmu.edu" <rthornt3@masonlive.gmu.edu>
Date: November 11, 2014 at 8:17:11 AM EST
To: ITU Support Center <support@gmu.edu>
Subject: Re: Phishing e-mail

Thanks, just changed my password. I can also be reached at rythornton11@gmail.com or [724-316-8930](tel:724-316-8930).

Ryan A. Thornton
George Mason University
[724-316-8930](tel:724-316-8930)

From: ITU Support Center <support@gmu.edu>
Sent: Tuesday, November 11, 2014 8:14 AM
To: rthornt3@masonlive.gmu.edu
Subject: RE: Phishing e-mail

Please visit password.gmu.edu and update your password immediately.

Also, please provide us with an alternate email or phone # where we can reach you.

Regards,

Mukarram Shahzad

[703-993-8870](tel:703-993-8870)

ITU Support Center

George Mason University

From: rthornt3@masonlive.gmu.edu [<mailto:rthornt3@masonlive.gmu.edu>]

Sent: Monday, November 10, 2014 5:23 PM

To: ITU Support Center

Subject: Re: Phishing e-mail

Hi,

Regarding the email below... I clicked the link and tried to sign in. Is that bad?

Ryan A. Thornton

George Mason University

[724-316-8930](tel:724-316-8930)

From: MASON IT SECURITY OFFICE INCIDENT NOTIFICATION <INCIDENT-NOTIFICATION-L@metis3.gmu.edu> on behalf of IT Security Office <itsoinfo@gmu.edu>

Sent: Monday, November 10, 2014 5:00 PM

To: INCIDENT-NOTIFICATION-L@metis3.gmu.edu

Subject: Phishing e-mail

Good afternoon,

two new phishing e-mails are circulating in the Mason community. The e-mails were sent out Friday, Nov 7, and today, Monday, Nov 10. You are receiving this email because you may have received one or more of these malicious PHISHing emails.

Email #1 & Email #2:

From: George Mason University

From Email Address: alert AT [gmu.edu](mailto:alert@gmu.edu) OR corissa.james AT [music.gatech.edu](mailto:corissa.james@music.gatech.edu)

Subject: Message From George Mason University

The message body may have contained:

One(1) new update [Click here](#), to view message.

These messages also contained a link that redirects to a site purporting to be a Mason. ***It IS NOT a Mason site.*** It is an attempt to steal your password. The way to tell if a link to a site is legitimate is by placing your cursor over the link in the e-mail. The full URL should be clearly visible. If you are not sure whether the URL is correct, treat it as malicious. The ITU is working on the list of who received these PHISHing e-mails and is closing the accounts of those who responded to them.

If you received either of these phishing emails, **DO NOT** reply, **DO NOT** click any links, and **DO NOT** provide any personal information. Delete the bogus e-mail. We will never ask for this information via e-mail.

If you believe that you may have provided your username and password through this or any of the other phishing email sent recently, please contact the ITU support center at [703-993-8870](tel:703-993-8870) or support@gmu.edu

Be aware messages of this type are malicious phishing* attacks. Do not respond. If you have responded contact the ITU Support Center at [703-993-8870](tel:703-993-8870) or via e-mail at support@gmu.edu.

*Phishing is a term used by hackers who imitate legitimate companies and organizations in e-mails to entice users to share passwords, Social Security numbers, credit card or bank account numbers.

The Federal Trade Commission warns that victims of phishing can become victims of identity theft and offers tips on how to avoid it at www.ftc.gov/bcp/edu/microsites/idtheft/index.html.

How you can recognize a Phishing e-mail: www.ncsu.edu/cc/essentials/antivirus_security/phishing/recognize.html.

Best Regards

George Mason University

(c) 2014 George Mason University.