INFORMATION TECHNOLOGY SECURITY

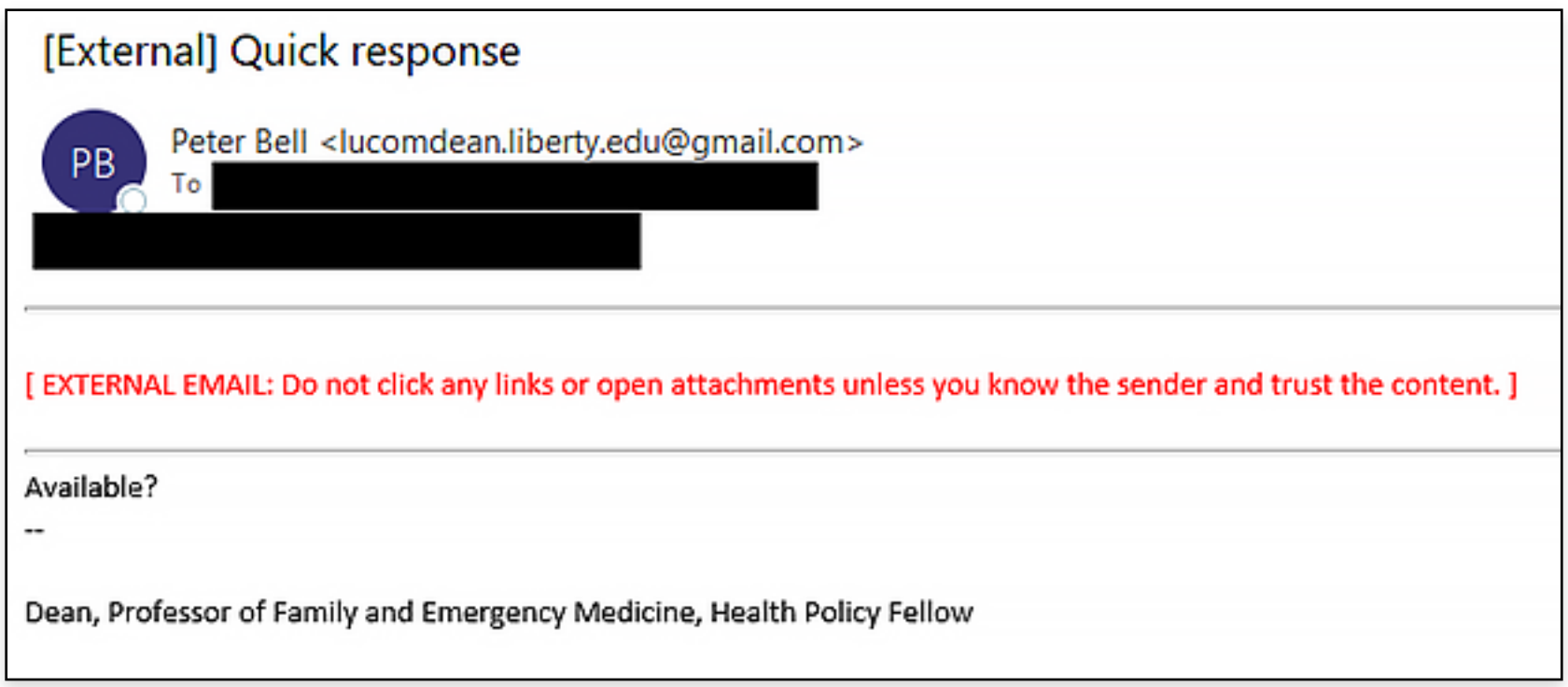
January 10, 2020

Introduction

Liberty University IT Security has recently been notified of several targeted scam email campaigns directed at faculty and staff. These emails typically fit an easy-to-identify pattern; here are some examples from a recent scam attempt to help you identify similar messages so you can protect Liberty University and your colleagues from these malicious scams.

How do I recognize one of these scams?

These emails usually come from non-Liberty email addresses but are designed to appear as if they were sent from an official LU email account. Let's take a look at an example:


[External] Quick response

PB

Peter Bell <lucomdean.liberty.edu@gmail.com>

To [redacted]

[redacted]

[EXTERNAL EMAIL: Do not click any links or open attachments unless you know the sender and trust the content.]

Available?

--

Dean, Professor of Family and Emergency Medicine, Health Policy Fellow

In the screenshot above, we can see that the email address contains the name of a faculty member and pretends to come from Liberty's domain (liberty.edu). However, when we pay attention to the end of the email address, we see that the source of this message was a Gmail account

How do I recognize one of these scams? (continued)

Also note that the subject line of the email has the word [External] added to it, as well as a banner at the top of the email message indicating that it did not come from a Liberty University account. Often, the initial message is intended to elicit an immediate response so that you will reply without carefully reading the email. If you get a suspicious message like this, please report it using Office365 or Outlook's built in reporting features. (See the link later in this article.)

What follows is an example of further communication with the scammer. If they receive a reply, the scammer will usually follow up by saying that they are in a meeting, cannot access their phone, and need you to help them by getting something from the store:

Subject: Re: [External] Quick response

I'm so tied up right now I would have preferred to call you but can't call you at the moment because am in a meeting and phone aren't allowed during the meeting ,i need you to help me out on something very important right from any store around.Let me know if you can do this.

If replied to again, the scammer will usually ask for the purchase of some sort of gift card (often from iTunes, eBay, or Google Play Store), with the offer of reimbursement later, and usually instructions on how to send the gift cards.

I need you to help me get ebay gift card from the store,i will reimburse you back when i get to the office.
I need to send it to someone and i need to get it sent Asap.

When you get them,remove each card from the pack scratch off the silver panel at the back of each card to show the claim code then take a picture of the cards and send it to me here ok.
And don't forget to keep the hard copies for me .

It has even been sometimes seen that the scammer would claim to offer reward or favor with administration in return for this "favor".

Remember to think critically.

Would your Dean or another member of the Liberty University administration contact you from an external email address? Would they ask you to purchase gift cards for a service like iTunes or eBay that your department doesn't use? Is there a sense of urgency that seems excessive or unclear? What is so urgent that the items cannot be hand delivered? Are there grammar, spelling, or punctuation mistakes that seem unusual? Does the email

Remember to think critically. (continued)

seem to use manipulative language offering favor with your department, or saying it's a gift for family?

Due to the changing nature of technology and the ingenuity of cyber criminals, it is difficult to detect and block all scam and phishing emails with automated methods. We rely on the Liberty University community to help IT Security by recognizing and reporting emails like this one.

What should I do if I receive a scam, or phishing email?

Use the built-in features of Outlook and Office365 webmail to report these types of messages. Please see the HelpDesk DIY article "How can I stay safe against phishing and email scams?" for further details (KB0011021)

What should I do if I receive a suspicious email, but I am not sure that it is phishing or a scam?

Try calling or emailing the person at their official Liberty email address and ask if it was them. Ask your colleagues if they have seen a similar email, or the address before. Call HelpDesk Remote Support or visit a Campus Support office and look at the email with a Support Specialist to determine if it is legitimate.