Quarter Security Awareness Newsletter

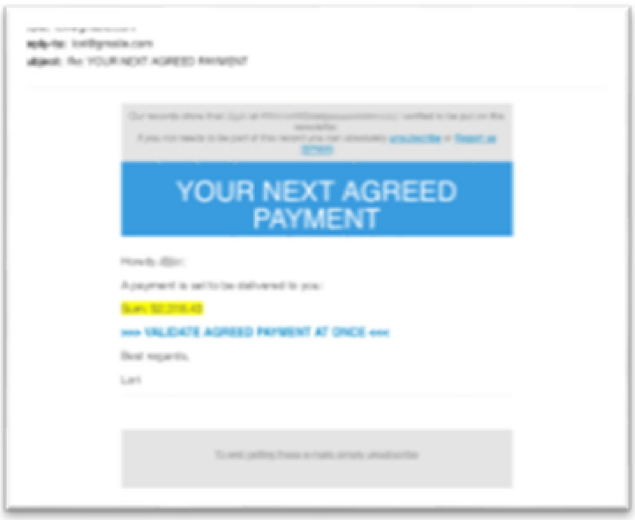
Why should you be on alert for suspicious emails?

Recently, universities and colleges have been subject to email phishing attacks where the hacker is seeking to change the individual's direct deposit information for their paycheck. The process used by the hacker is often as follows:

1. An individual receives a seemingly harmless email with a link to a website.
2. The link takes the individual to what appears to be a Microsoft Office 365 login page.
3. The individual logs in. ***(Allowing the hacker to collect these login credentials)***
4. The attacker uses those credentials to log onto the ***real*** Office 365 page.
5. Then the attacker sends emails from the individual's mailbox to payroll and changes the individuals direct deposit bank account.
6. The attacker gets paid at the next payroll cycle, and the individual does not.

Learn more at: https://www.ic3.gov/media/2018/180918.aspx

Important Email Statistics



- **91%** of all success data breaches in the history of technology have been traced back to a malicious spear phishing email message.
  - *Spear Phishing* – This is when the attacker generates a malicious email targeted directly at the receiver. Most often the attackers use information gathered about the individual through social media.

This number is equally disturbing as any technical countermeasures are immediately circumvented once the attacker knows the username and password of an individual within an organization.

- **54.9%** of all phishing emails are clicked within the first 60 minutes of delivery.

Malicious emails are specifically designed to illicit an emotional response from their recipients. They pull on emotions such as: **Fear, Greed, Urgency, Curiosity, Self-Interest, Helpfulness**.

The #1 Best Defense is You!

There are many ways to spot a malicious email, but probably the best is through emotion. If the email feels wrong, by eliciting one of the emotions listed above, then that is a sure sign that this may not be legitimate.

Second, before you click on any links, hover your mouse over the link for a moment. The smart tip displays the link location; if this does not match what was expected by the sender's email address, or the context of the message, this is a warning sign of an unsafe link. Beware of **http://tiny.url** or any links that seem to go on forever. These are just a few of the indicators that you may experience before being taken to a malicious site.

USE EXTREME CAUTION when a hyperlink takes you to a login page; attackers can do more now than ever before with this information. If you need to login to receive a document, voicemail, or invoice; be sure to perform a separate search for the company and contact them directly before submitting any login information onto sites you do not use regularly.

If you get SCAMMED!

1. Change your password **IMMEDIATELY!**
    a. The faster your response to this the less likely the attackers will leverage your information against you.
2. Contact IT Security: SecurityOffice@collegiseducation.com

    a. Be sure to include as much information as possible so this incident can be thoroughly investigated.

Reporting Emails

To assist in the investigation, please forward a copy of the malicious email directly to SecurityOffice@collegiseducation.com.
To forward a copy of an email message:

1. Select the suspicious email message in Outlook
2. Select **More** within the respond section of the ribbon, and then choose **Forward as Attachment.**
   *(You may also press **CTRL+ALT+F**)*
3. Address this message to SecurityOffice@collegiseducation.com and use the subject: **Malicious Message**