ISSUE: 11 YEAR: 2016

University Information Security Office Newsletter

"Your mailbox has exceeded the storage limit which is 10GB as set by the administrator, you are running at 13.6 GB, please re-authenticate your mailbox click or copy the link below:" - Common Phishing Email

From the ISO's Desk

This month we highlight phishing. According to SC Media, The Anti-Phishing Working Group (APWG) observed more phishing attacks in the first quarter of 2016 than in any other three-month span since it began tracking data in 2004. In keeping with those findings, the APWG reported that the number of phishing websites it detected jumped a startling 250 percent between October 2015 and March 2016. The 2016 Verizon Data Breach Investigations Report found that 89% of data breaches had a financial or espionage motive, with the median time for the first user of a phishing campaign to open the malicious email clocking in at 1 minute, 40 seconds. Data for more than 7,500 students at the City College of San Francisco was compromised as the result of an employee falling victim to a phishing email that was disguised as a request for student information. Falling for a phish can happen to anyone. Being able to identify a phish goes a long way in protecting yourself and those whose information that we are entrusted.

Jim Pardonek
Information Security Officer

Our November awareness topic is Email and Messaging.

Please visit: http://www.luc.edu/uiso/awareness/loyola_aware.shtml for further information.

If you have any questions in regrading to Loyola Aware, please contact the data security team by email (datasecurity@luc.edu) or call x87373 (703-508-7373)

Phishing

Jim Pardonek

What is Phishing?

Phishing is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.

There were over 22 million reported phishing attacks worldwide in the first quarter of 2016 alone. This is 4 times higher than the same period in 2015.

What are the Thieves looking for?

Don't think that it's just your banking details that are important. Some emails attempt to gain control over your account login. The issue is that most people use the same login information on various other accounts. This means that if they compromise your email account, they can potentially reset all your other passwords. So in addition to keeping strong and varying passwords, you have to always be on the lookout for bogus emails masquerading as the real thing. While most phishing attempts are amateurish, some are quite convincing. This makes it very important for the recipient to understand how to recognize phishing at the surface level as well as how they work under the hood.

Examine What's in Plain Sight

Most phishing attempts, attempt to make you aware of an activity on an account which is intended to alarm you into reacting. The message could appear to come from your work IT Helpdesk, FDIC, the IRS, the bank, or even someone familiar to you in your address book. So the call to action in the phish is to verify or restore your account by submitting just about every piece of personal information you can think of.

What to look for?

While there certainly are exceptions, pretty much every phishing and scam email is loaded with red flags directly in the message themselves. Even if the text is convincing, you can usually find many mistakes littered throughout the message body which indicate the message is not legit. Look for links in an email and use the "hover-over" technique. Browsers will display the actual link location that a visual links destination. If the links don't match the sender, run away. When it comes to staying safe online, it never hurts to have a good bit of cynicism. Be cynical of any email that appears out of the blue or stresses that actions need to be taken "or else"!

In summary there are some things to look for to identify a phish. Look for an unprofessional email title. See if the sender address does not match the title. In most phish the images look a bit amateurish: They don't match the background or look formatted to fit the style of the email. Often a generic greeting is used: A company you've done business with or contacted before you will likely use your name instead of a vague greeting. Reply by email is requested: Because scammers are not the legitimate companies, they are likely to request an email response. Secure information is requested: Legitimate companies would never request such sensitive information via email. Typos and poor grammar are a big hint that the email is fraudulent.

Ransomware

Chris Campbell

While many of us are familiar with the term "malware", ransomware has become one of the most feared malware categories. It has also gained quite a lot of media exposure recently, and for good reason. Ransomware is a type of malware that is designed for a single purpose: obtaining a ransom payment for something it holds hostage on a machine (typically files).

Most ransomware variants share several common themes. The first of these is the ability to encrypt important user files locally, as well on any connected drives. In most cases, there is no way to reverse the encryption without obtaining a unique key that was sent to the attacker. Once the encryption process is complete, a message will be displayed with instructions. The instructions typically include a warning that your files are unrecoverable without the attacker's help, as well as methods to submit some form of anonymous payment in return for access to your data. Some types of ransomware will take an even more devious approach, such as starting to delete files every so often. Others will not even bother to restore the files whether the ransom is paid or not.

Email is a common method for distributing ransomware, but it can also be included in malicious web sites (or even malicious advertisements on an otherwise trustworthy page). Emails will typically make use of an attachment to infect your machine. Word documents are common, but any file type has the potential to be malicious. Alternatively, an email may include a link that covertly redirects you to a malicious page when clicked.

Fortunately, it is relatively easy to safeguard against ransomware. The simplest method is to ensure that you have up-to-date backups of your system. These need to be stored on media that is not usually connected to your system, such as a portable USB drive. Connect the drive each time you need to take a backup, then disconnect and store it in a safe place. Usual security practices will help as well, such as ensuring you have an active antivirus that provides a real-time protection feature. Please visit the following link for more information about antivirus products: http://www.luc.edu/uiso/resources/antivirus.shtml. Finally, make sure you are wary of unexpected email. It may even come from the account of someone you trust, so following up over the phone before opening a suspicious message is often best.

Be mindful of whether the information you are sharing is really necessary, such as locations, political views, weekend plans, etc.

Whaling

Jonah Murray

If you are aware of basic information security terms or if you have been following along with National Cyber Security Awareness Month, you probably know what phishing is (In case you don't know what it is, phishing is an attempt to acquire personal information from a victim by forging some kind of trusted electronic communication).

Phishing is unfortunately fairly common although it is also well-known, which makes it less effective. A less-known form of phishing is whaling. Whaling is a phishing attack aimed directly at C-Level executives and other high-profile targets within businesses and large organizations. Whaling attacks involve fake documents that are tailored for upper-level management. These can include forged company-wide emails, FBI subpoena emails, and emails containing the target's name, organization, or job title in order to lure them in. The attacks are usually meant to obtain a wire transfer of a hefty amount of money or valuable sensitive documents.

Whaling can also take the form of a forged email from a C-Level executive corresponding with a high level employee. For example, a high level finance employee may receive an email claiming to be from an executive, with a similar email address and similar phrasing to the real executive. The email may ask for account numbers, strategies, algorithms, or anything else of value from a high-level employee. Whaling is a critical issue because it is very easy to treat these emails as legitimate and the costs of giving sensitive information to a whaler is immense.

Another thing that makes whaling so dangerous is that they are often social engineering attempts. This means that instead of providing a link to a malicious website, they act as a legitimate person with a legitimate need. The emails are written by a person and the request for information is personal and straightforward. Since they do not contain links or attachments, these whaling attacks become even harder to detect. Luckily, vendors are building tools that specifically target whaling emails. These tools look for key words and phrases in emails that indicate whaling attempts and indicate to the user the risk level of each email.

Regardless of what software is developed to fight security threats, information security awareness training is key to all levels of an organization. Whether you are an entry level employee or a C-level executive, be aware of cyber security threats and ensure that your colleagues and managers are aware of them as well.

University Information Security Office
For more information or to report a security incident:
Email: DataSecurity@luc.edu
Web: www.luc.edu/uiso
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM

References:
The Latest in Phishing: June 2016, Wombat Security Blog
APWG report: Phishing surges by 250 percent in Q1 2016, SC Magazine