

► SOCIAL MEDIA BEST PRACTICES 1

► USEFUL INFO 1

► LOYOLA AWARE 2

► IN THE NEWS 2

University Information Security Office Newsletter



“You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable.”

- Daryl White, DOI CIO

Phishing Emails

Yuyang Zhao

Phishing emails are one of the easiest forms of cyber attack for criminals to carry out. Phishing emails typically claim to be from a legitimate, trusted company and either ask you to provide sensitive information or ask you to click on a hyperlink and redirect you to a malicious site. Another form of phishing email could be asking you to open or download files that are designed to infect your device.

Phishing email attacks are frequently used by attackers. To protect your information, here are a few things you need to know.

How can you tell it's a Phishing Email?

1. Be suspicious about any links included in the email. Use other methods to access trusted sites (e.g. browser bookmarks or searching the web).
2. Official organizations are serious about their emails. Legitimate messages usually do not have spelling mistakes or poor grammar. The expression in the email should also be formal.
3. Pay extra attention to the sender's email addresses. Is it from the usual sender?
4. Do not open an attachment if you are not expecting one.
5. Malicious attachments are a common phishing tactic. If you are not sure about whether an email, attachment, or link is


safe, please forward the email to DataSecurity@luc.edu.
Please refer to the numbered items in the screenshot below for examples of applying these principles to a real-world phishing attack:

1. The email is not addressed to the recipient. They do not know the recipient's name. User ID (LUC) is not an identifier.
2. Pay attention to the grammar, word choice, and punctuation. This does not read like an official email.
3. If you look closely, you will find this URL is unusual. It contains "LUC" but it is from weebly.com (not our official website luc.edu). Some links may even disguise themselves, so always hover your cursor over the link for a moment to reveal the true destination.
4. The email does not mention which department or office it is from. E-mail Team is a vague expression.

References


What is a Phishing Email and How Do I Spot the Scam?
<https://www.webroot.com/us/en/resources/tips-articles/what-is-phishing>

Dear user ID (LUC)  1

This is to notify you for the final time that we have stopped processing incoming emails on your account since you have refused to UPDATE your account, and we might be forced to delete your account if this noticed is ignored again. Please take a second to secure yours below....  2

Kindly follow the link (<https://lucdu.weebly.com/>)  3

Your security is our primary concern.

Regards,
 E-mail Team  4

University Information Security Office

Email: DataSecurity@luc.edu
 Telephone: (773) 508-7373
 Location: GC Room 230
 Hours: M-F 8AM-5PM

Useful Information



Loyola Information Security Social Media

@LUCUISO
<https://www.facebook.com/lucuiso/>
<http://blogs.luc.edu/uiso/>

Current information regarding security risks at Loyola

Password Security

Yuyang Zhao

Why do we need secure passwords?

Passwords are the first line of defense that we have to protect our information. If a hacker is able to guess your password, they can wreak all kinds of havoc. This could include almost anything, such as accessing your University resources, bank accounts, or even using your information to set up new credit card or loan accounts.

How do I create a strong password?

Your password should never include the following:

1. Any simple or potentially guessable combinations such as sequential characters or numbers, personal information, dates, etc.
2. Words contained in any dictionary.
3. Anything based on your username, even with slight variations.

What makes your password strong:

1. Use at least 8 characters (longer than this is preferable).
2. Use a mixture of characters classes (Upper and lower case letters, numbers, special characters, and even spaces).
3. Use a completely unique password for every site of service that you use.

Other good practices:

1. Do not share your password with others under any circumstances.
2. Do not write your password down, or store it in an unencrypted computer file.
3. Update your password if you fear (or are notified) that it may have been exposed. Changing passwords on a regular basis is always a best practice.
4. Never provide credentials when requested through email.
5. Use a password manager program to store your passwords.
6. Instead of using a link provided in an email, go to the site directly from your browser.
7. Try to use multi-factor authentication if available.

References

Keeping Safe: the Importance of Good Passwords, Don Cranford, <https://www.katalystsolutions.com/newsletter/issue-1/39-keeping-safe-the-importance-of-good-passwords.html>

What is a secure password and why is it important to have one? <https://www.namecheap.com/support/knowledgebase/article.aspx/9517/45/what-is-a-secure-password-and-why-is-it-important-to-have-one>



Loyola Aware

Cai Wang

Loyola's Information Security Awareness Program – Loyola Aware – is now hosted on a new platform. New and updated training modules are available for all faculty and staff.

Loyola Aware is Loyola's information security awareness program designed for all faculty and staff. The purpose of the program is to increase security awareness by providing short video snippets that bring to light specific topics in information security. By increasing awareness, the program allows everyone to recognize IT security concerns and respond accordingly.

The Loyola Aware training modules can be accessed online using your UVID and password. Each module contains a brief video followed by three to five assessment questions. The idea is to reinforce the video content by asking questions to let the participant self-assess their understanding about each topic. The modules contain a variety of topics including social engineering, email, messaging, web browsing, and many others.

To Access Loyola Aware:

1. Navigate to <https://access.sans.org/go/loyolauniversitychicago> and log in using your UVID and password.
2. All current LUC employees should already be enrolled in Loyola Aware. If you have any trouble logging into the site, please email DataSecurity@luc.edu.
3. There should be two sections on the home page: "Required Training" and "Recommended Training". Training modules are assigned based on your role at Loyola. Required Training modules are mandatory to complete, and normally have a due date. Recommended Training modules are not mandatory, but are strongly recommended.
4. All modules require a minimum score of 60% to pass. There is no limit on the number of times you may take an assessment, and you can click on the Gradebook to check your scores and get immediate feedback.
5. After completing all training that was assigned to you, you will be issued a downloadable certificate.