**Phishing awareness and Training for university community**

Be cautious and avoid fraud..!

* **the significance of this awareness/ training:**

Despite advances in technology and security measures put in place to guard against breaches and protect our data, people continue to pose a security risk. Phishing is one of the cybercrimes with the highest success rate. Email, Bad links, text mistakes, etc... could be used to spread the infection. X university has a high ranking in researching and other domains globally, which makes it a target for these types of attacks. You will be able to identify and avoid this type of attack after completing this training.

* **Content:**

1. Outline of awareness and training program includes:

* Target population (faculty members) and potential risks associated with phishing attacks.
* All possible deliverables.

1. Focusing on one of the deliverables and develop and direct it to the faculty members.
2. What are the potential challenges for this awareness and training?
3. References.
4. **Outline of the awareness and training program:**

* Since people are the weakest link in security, **faculty members at X university (the target population)** should exercise caution while opening emails, using X university’s network, or clicking links that seem out of the ordinary. Phishing has become the most popular attacks against human. **The risks associated** with this type of attacks can result in:
* Unauthorised access to confidential data: by clicking over malicious links, the attacker could steal the identity and impersonalize the victim to get access to sensitive data in the system.
* Financial loses: once the attacker gain access to the system, he could install malware to move inside the network or encrypt the data and ask for ransom.
* Identity theft: Phishing attacks most often attempt to obtain personal data, including passwords, social insurance number and email address...etc. these data can be used to identify specific individuals to get access to their accounts.
* Damage the university reputation: the harm after successful phishing attack may lose faith in a university’s ability to protect the personal data.

X university provided policies and guidelines in its website (link is below) to be safe in the community.

* **Deliverables:**

1. Workshops and events: to enhance awareness of phishing attacks, a workshop with academics and IT professionals should be organised. Material and real evidence of actual instances will leave their mark on how unsafe it is.

This deliverable's objective is to provide hands-on training and practical experience in how to avoid phishing. And to guide them on what to do if they become victims of phishing.

1. Advertising for greater awareness: Campaigns can be carried out in a variety of ways, such as sending faculty members direct emails or distributing flyers and posters in strategic locations across the buildings. The content must describe phishing, its dangers, and the recommended techniques to prevent it.

This deliverable's objective is to promote awareness visually about phishing in a way that is both simple to access and understand. And to raise awareness about phishing.

1. Online contests: Modules concerning phishing attacks and their threat will be provided to faculty members during training. At the end, in order to gauge their comprehension of phishing, participants will be asked to respond to questions.

This deliverable's objective is to warn about, and get ready for, phishing attacks among the faculty members. and after the session, evaluate their understanding.

1. **Developing one of the deliverables:**

Online contest with training modules:

1. **Overview of Phishing:**

What is phishing: it’s a method used by online fraudsters to try to steal personal data including usernames, passwords, and credit card numbers.

1. **Phishing Attack Types:**
2. Email Phishing: most popular one. Fake domain often contains character substitution, like “r” and “n” to make “rn” instead of “m”. Sometimes the scammer will use a copy of legitimate email and replace the link inside the email with new one to direct the victim and steal the data (called clone phishing).
3. Spear Phishing: It makes use of trusted sources for communication. Individuals are frequently the target. It is known as whaling when the goal is particularly exceptional (whale refer to high value individuals).
4. Vishing and Smishing: Scammers may use fraudulent text messages to lead their victims to malicious websites or speak with victims on the phone while posing as legitimate institution or organisation.
5. HTTPS Phishing: Since HTTPS is a more secure form of HTTP, a scammer may utilise it to give the impression that they are a legitimate business.
6. Pop-up Phishing: The browser displays a message informing the user that the requested website wishes to display notifications when they attempt to access it. Malware would be installed by the pop-up when you click "Allow."
7. **Attacks that are successful lead to...**

• Identity Theft. • Loss of Sensitive Information.

• Financial Losses. • Unauthorized access to the system.

• steal Usernames and Passwords.

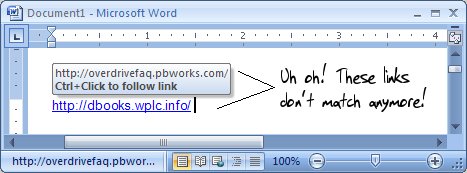
• Malware and Ransomware Installation.

• Backdoors (access to systems) to Launch Future Attacks against the university.

• Reputational Damage to the university.

**Guidelines for Recognizing a Phish:**

1. Inconsistent links: by hovering the cursor over the link (without clicking on it), the complete link must appear in left corner or somewhere in the page. The two links must match, if not, then it’s probably fraudulent.



source: scls.typepad.com.

1. Incorrect grammar and spelling:

* Double check the grammar and the spelling in the email. It might have letter substitution or if you know the sender is a native speaker, then he might will not have errors.
* Pay attention on the domain name. Every domain name is unique.

1. Strange Correspondence: X university will never ask you in email for personal information (SIN number, payment card number, passwords .. etc).
2. Urgent or Threatening Language: Attackers may use urgency to force victims into clicking on harmful links or giving up critical information. You must be sure before submitting such information.

**Online contest.**

1. Phishing is a method used by scammers to steal your identity. \*True \* false
2. What are the right types of phishing:

\*Email, text massage, phone and malicious link. \* Email, id card, driving licence \*Phone, car keys, wallet.

3- successful phishing attacks lead to: \*Steal password, username \* unauthorised access \* Reputational Damage. \* All above.

4- by hovering over the link on a website, another link must appear, if they match mostly, It’s trusted link. \*true \*false.

1. **The potential challenges are:**
2. The time for X university (to implementing such a program) and the faculty member (time consuming and prioritise other responsibilities).
3. The cost essentially if the program will cost a lot for example having an outreach event.
4. Faculty members might be resistance to change.
5. Unsupportive management.

**outlined deliverables are the most appropriate and relevant to overcome these challenges because they come with many advantages depends on the deliverable itself:**

* 1. Workshops and events: The faculty members can put in some work hours to broaden their IT-related understanding of phishing and to encourage participant networking and collaboration so they can exchange ideas and best practises.
  2. campaigns for greater awareness: more time may be saved, and the program will benefit more participants. These campaigns can make a lasting impression.
  3. Online contests: more affordable for X university and comfortable for the participants (at their own time). It is also a powerful technique to interact with a large audience.

**References:**

1. <https://www.bluevoyant.com/knowledge-center/8-phishing-types-and-how-to-prevent-them>
2. <https://cehs.usu.edu/scce/files/phishing-awareness.pdf>
3. <https://scls.typepad.com/techbits/2011/06/finding-and-replacing-hyperlinks-in-word-with-alt-f9.html>