CMPG 215

Risk Analysis

Antonet Zwane 41509056

Introduction

In the last couple of years, the rate of phishing has increased more than any information security crime. As more people are getting into the technological world, phishing is also getting advanced and mirrors or exposes the user while the cybercriminal is observing every move of the user. Phishing is when cybercriminals deceive people or users to reveal sensitive information. “Phishing” refers to lures of fishing for sensitive information. The threat that the institution can be exposed to is Phishing. Phishing is when cybercriminals deceive people or users of a system into revealing sensitive information about an organization, in this case an institution or university. Phishing most of the time starts with emails and these emails can be targeted at the employees at the North West University. This is called the “spear phishing” because it is targeted only to the employees and most of the time the employees fall for it because the emails really seem genuine and are not suspicious. The following risk analysis for the North West University will assess the potential impact of the phishing attack if it occurs, the likelihood, the vulnerability of the university and the possible solutions or measures that the university can take to protect itself from possible attacks in the future or when a phishing attack happens, as the university mostly use emails to communicate amongst users or members of it.

Likelihood Of Phishing Attack

As North West University is a big and public institution it is more prone to cyber threats and attacks to its network or cybercriminals will try their best to gain access to the data of the university because of the resources that the university has and the money that the university may have. The university also has a variety of users including students, alumni, faculty, and staff, that use the university email to communicate each day and are usually the weakest that can be targeted or used to gain access to the university system. University users receive a huge number of emails daily and may not pay that much attention to the attack when it occurs than when they are using their personal email. To protect themselves the North West University may have very complex IT infrastructures that serve as security or protection which sometimes focuses on protection only and may be very difficult for it to detect actual phishing attacks when they occur.

The IT infrastructure usually serves as a disaster recovery plan or strategy rather than dealing with the incident immediately when it happens to prevent the attack from spreading and causing more damage to the network of the institution. The university is constantly involved in many international events especially research so, the involvement of the university in research

and events that strategically benefit the university economically attracts cybercriminals to steal the intellectual property of the university. Lastly unlike other institutions like security

institutions or businesses where the focus is security and protection only the university focuses on many things at once, data like student accounts, employee accounts, medical and health information, data regarding accommodation for students, sponsors and funders data as well as research conducted by the university and many more, so it is very likely to get an attack because the university does not focus on one factor.

Potential impact of phishing attack

If cybercriminals or attackers can gain access to the North West University network or system, the potential impact will be so significant. Cybercriminals will unauthorized gain access to sensitive information like research data or thesis, student information and records, financial records and information, intellectual property and other sensitive information that the university has and that can cause them a lot if exposed. The reputation of the university firstly will be at stake. No one will want to associate themselves with North West University because of the attack and a lot can be lost. Financially the university will be under great and huge losses with sometimes huge amounts that cannot be recovered in a year or two years. Theft of identity for all the users of the university system or network, including upper management, employees, students, alumnus and all the university system users, which is usually the cybercriminal impersonating someone from the university.

The attack can also leave the university under legal problems or legal liabilities as the university must account for the disaster or incident sometimes if the cybercriminals gained access to the university network through an employee's email it can be considered as negligence or ignorance and sometimes may put the employee under serious criminal charges even though they were not aware of the attack. The university will be liable for almost every legal charge regarding the attack. Phishing attacks can also cause highly disruptive ransom or malware attacks for the university and compromise university security. The phishing attack could also disruption learning and teaching processes because students and lectures will not be able to access educational materials that are used to conduct classes as now the university must focus on fixing the problem and making their users aware of the attack

Vulnerabilities

A lot of factors or vulnerabilities can lead to the university being prone to phishing or being at risk of phishing and cyber-attacks. As mentioned before the university has a lot of users or people that use the university email address, which can make it easier for the cybercriminal to

pose as someone from the university, especially when there is a lot of work, the user is most likely to click on a random email if they see that the email is from the university whilst it's a cybercriminal impersonating the university. When the user is working under pressure and is receiving many emails from the university, they will make decisions without thinking twice. Another factor is lack of awareness, many university users are not educated or have limited education about cyber-attacks, phishing in this case and the risks of phishing, also how to identify them, more especially students because they don't have the basis in information and communications technology more especially in terms of security. The university has access to sensitive information and that alone makes it very prone to phishing attacks and a target to cybercriminals, so that they can gain unauthorized access and most importantly for financial gain. Weak passwords can also be a weakness that the institution has for their emails, or their work professional tasks can be targeted. Outdated systems that the university still uses and don't give themselves a chance to update can also be a vulnerability and a disadvantage for them, which can attract cybercriminals. Lastly the IT infrastructure, most of the time universities in general tend to have complex infrastructure or infrastructure that is difficult to understand and that alone makes it difficult to detect phishing attacks and makes it difficult to prevent phishing attacks from affecting the network of the university.

Possible solutions or measures against phishing attacks

Raising awareness and educating university users, students and employees about phishing attacks, their impact on the university and how they can also affect them as an individual. The university should provide training for everyone in their institution on how to detect phishing because as mentioned the users of the university network or system are the first target by cybercriminals because they can be easily manipulated and deceived. Training could involve seminars both online and face to face to accommodate everyone, mock phishing emails can be used to also show the users how a phishing email is and how to quickly avoid it when they see or come across it and to also allow them to test themselves and assess their knowledge about phishing attacks that they learned about in the conducted seminars. Teaching the users how to set a strong password that cannot be easily traced or found by cybercriminals, passwords can include characters, capital letters and numbers. The university must implement security controls, like authentication (multi-factor authentication) to prevent unauthorized access to the university's data by cybercriminals, authentication like allowing the users to use their fingerprints or face recognition when they are accessing the university's emails or resources and to verify their identity.

Email filtering software like N-Able Mail Assure (SolarWinds), Spam Bully, Spam Titan and other email filtering software can be used to detect, prevent and block from affecting the system of the university and to block phishing attacks from reaching the user's email or inboxes. The

university must ensure that its system and security are always updated with the latest software and security updates and not outdated as this can cause problems for them and can attract cybercriminals if the system and security used are outdated. IR or incident response plans must be developed to respond quickly and effectively to the occurrence of phishing attacks and even to other security attacks that may occur. The university should also be not afraid to report the phishing attack if it occurs so that drastic measures can be taken by authorities and not try to take measures into their own hands. The North West University can also share with other universities that were once attacked by phishing or other attacks they faced in the past to honestly share ways and plans of how to face phishing attacks in the future if they occur and that can also help to use that university or institution as reference to the North West University users to actually see the impact the phishing attack has on an institution so that can raise awareness and also educate them, that could also help other universities and cause unity amongst them.

Conclusion

Phishing attacks remain one of the huge and growing cyber-attacks, especially for huge institutions like North West University. The university is a huge institution that deals with many departments, like finances, health, education, accommodation and many other departments and usually has a very huge database that makes it to be a good target for cybercriminals, also they have a huge user base as they have different users like students, lectures and all, their IT infrastructure is complex most of the time and they hold or have access to very sensitive information regarding their users, most of the time. Most of the time cybercriminals exploit humans or users as they are the weakest link of the university and can be easily manipulated and deceived.

The North West University must always have an incident response plan or IR developed to help them respond quicker when a phishing attack has occurred and take measures like educating their users and raising awareness about phishing attacks as their users are mostly the institution's vulnerability and often not educated about cyber-attacks and their impacts to the university. An updated system and security will save or prevent the university from the danger and impacts of phishing attacks. The university must also be aware of its vulnerabilities and further research how to improve itself to protect mostly their access to sensitive information and to make itself less attractive to cybercriminals which are realistically difficult because the university always serves as an attraction to cybercriminals but to make themselves less attractive to such. Sharing of ideas and past attacks by other universities or institutions can serve as physical evidence to users that usually don't believe if they are told, to educate them and raise awareness. I honestly will encourage the education and awareness of users about the phishing attack.

Reference List

Frontiers

Frontiers | Phishing Attacks: A Recent Comprehensive Study and a New Anatomy (frontiersin.org)

Taylor&Francis Online

Full article: Securing higher education against cyberthreats: from an institutional risk to a national policy challenge (tandfonline.com)

Google Scholar

O'Leary, D.E., 2019. What phishing e-mails reveal: An exploratory analysis of phishing attempts using text analysis. *Journal of Information Systems*, *33*(3), pp.285-307.