

INFORMATION SECURITY AND ETHICS

ASSIGNMENT 1

SYEDA MAHAM JAFRI - 22796

OVERVIEW OF ORGANIZATION:

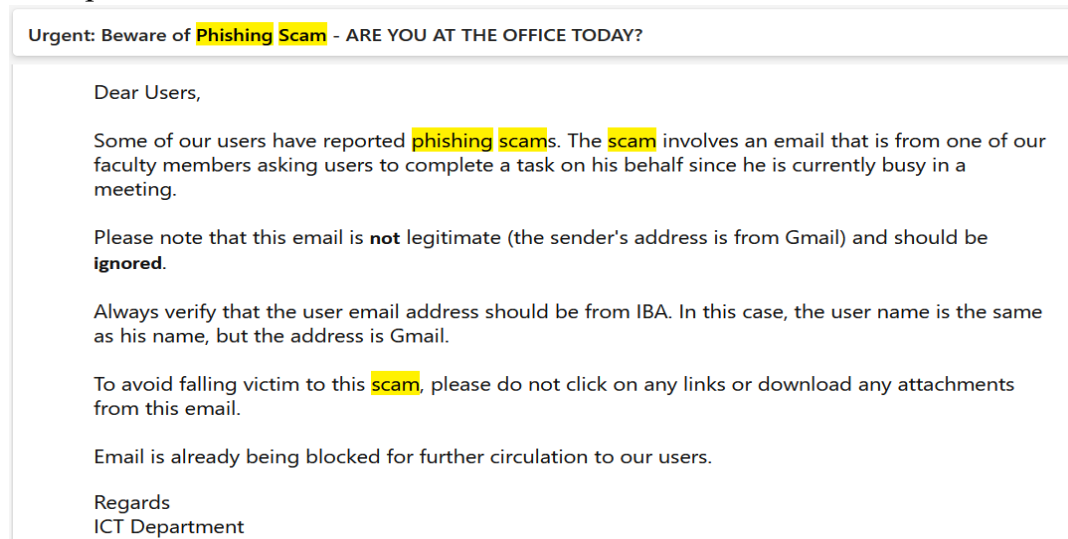
In 1955 the Institute of Public and Business Administration (IPBA) was established, making it one of the oldest business schools outside North America(1) . IBA is amongst the most reputed and renowned academic institutions of Pakistan. At undergraduate level, IBA offers degrees in Business Administration, Accounting and Finance, Computer Science, Economics, Economics and Mathematics, Mathematics, Social Sciences and Liberal Arts. The graduate programs offered by the IBA include degrees in Business Administration, MBA Executive, Computer Science, Economics, Islamic Banking and Finance, Journalism, Management, Data Sciences, Finance and Mathematics. The doctoral programs offered at the Institute include degrees in Computer Science, Economics and Mathematics. (2)

THREATS AND VULNERABILITIES:

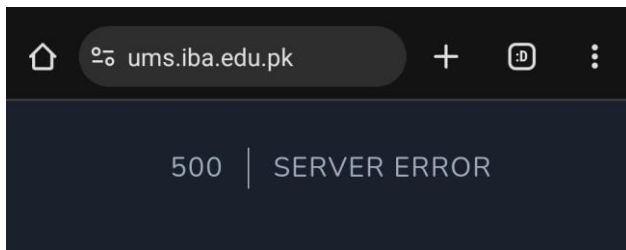
- **CYBER ATTACKS:**

A cyberattack is any process of stealing, exposing, altering, disabling, or destroying data, applications or other assets through unauthorized access to a network, computer system or digital device.

Recently IBA students, staff and faculty member became be a victim of this Phishing scam through an email from one of the faculty members in which he was requesting the individuals who had received the email to complete some task on his behalf since he was occupied with something. This was one of the tricks to get an unauthorized access to systems containing personal data, student records, financial information etc. Although the students and faculty staff were informed about this and the spread of this email further was stopped, however if this attempt had succeeded this would have resulted in data breach.



Another cyber attack that IBA has definitely experience recently is the denial-of-service attack. This was when the recently launched ums could not handle the excessive requests and became unavailable to the students at the time of enrolment.



Security Controls:

- IBA should conduct regular training and awareness programs for both student and faculty especially for those who do not have a CS background to train them on how to identify a phishing scam.
- Secondly IBA must strictly implement the policy of communication of any kind to be through official channel and through emails provided by IBA to faculty and students.

Impact on IBA's CIA:

1. Confidentiality:
This would lead to unauthorized disclosure of details such as login credentials or personal data.
2. Integrity:
The attackers through the unauthorized access can manipulate data which imposes a serious risk on a university's credibility.
3. Availability:
The denial-of-service attack would make it impossible to access something when required, hence nullifying the concept of availability.

• INSIDER THREATS:

Insider threats are the kind of security risks that originates from within an organization and is posed by those who have access to an organizations physical or digital assets. The potential insider threats include the current or former employees who could make use of privileged access to steal personal or financial data for personal or financial gain. These insider threats are extremely hard to detect since in the case of threat or attacks being made from an outside source there are some boundaries that need to be crossed before they can reach the information however in the case of insider threat the attacker already has access to data and their exploit might not even be apparent until the data is entirely gone.

A university like IBA is one of the centres of cutting-edge research, innovation and development. With most of the faculty being PHD's or research students, IBA stores a variety of research papers in its database which have been published under it or have been obtained through collaborations with various other companies. In the era of intense academic and professional competition, having access to meaningful and accurate resource papers is a real challenge, and anyone who has access to them is a possible target for insider threats as to sharing them without consent or permission for financial gains even before they got published.

Security Controls:

In order to mitigate the risk of insider threats the first step IBA needs to implement is to effectively identify them. There are two ways of detecting insider threats, one by observing the behavioural indicators that is monitoring an insider's actions such as constant breaking of IBA'S

policy, asking for access to sensitive information that is not needed for their role etc and second by keeping an eye of digital behaviours which are noticeable on someone's computer or device. These include unusual login attempts, excessive data downloads, viewing content that doesn't pertain to their roles etc.

Once IBA has efficiently identified these insider threats it can then move on to handling this risk and trying to prevent it by implementing few of the suggested techniques.

- Firstly, IBA should set a comprehensive security policy that included procedures for detecting, blocking and investigating this misuse.
- Secondly it should focus on implementing Privileged Access Management making it easier for the IT teams to track and control who has access to what, it ensures that only authenticated and authorized users can access specific resources.
- Insider Threat Programs should be carried out to ensure that the community members understand the role of insider threat and should be encouraged to report perceived threats.



Single Sign-On

Sign in

username@OX.AC.UK

[Can't access your account?](#)

Next

They should make use of something like this that ensures that your email should confirm to a certain format in order to be able to access what you want.

Your username should be entered in the form
'abcd1234@OX.AC.UK'

[Reset your Single Sign-On password](#)

[Activate a new account](#) using an activation code

[University of Oxford Computer Usage Rules](#)

Exam Staff Login

Error: You don't have rights to access this portal.

Username

Enter Username

Password

Enter Password

Login

Impact on IBA's CIA:

1. Confidentiality:

Malicious insiders may intentionally access or disclose confidential data to unauthorized individuals. For eg: A staff member with access to student records illicitly shares confidential information with external parties.

2. Integrity:

This may lead to the alteration of academic records, research findings, or other critical data.

3. Availability:

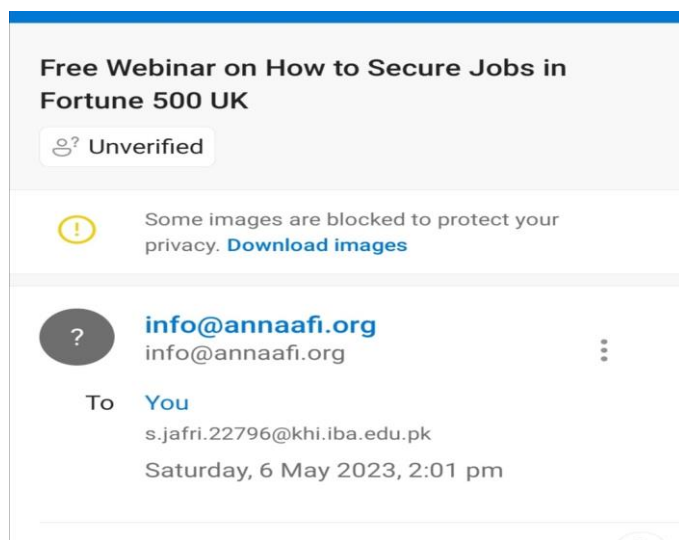
May cause disruptions to the availability of critical systems or services. Malicious insiders can intentionally disrupt operations, leading to service outages or other forms of unavailability.

- **SOCIAL ENGINEERING ATTACKS:**

Social engineering attacks are when a hacker uses the manipulation techniques such as exploiting human error to get what it wants from the victim that is infiltrating their systems. These social engineering attacks include certain patterns such as urging the user to perform a certain task. The educational institutions are the most targeted ones in this case since they have a huge amount of valuable information stored which offers an extensive attack surface.

Since IBA comes under the educational institutions, it stores a wide range of information including details, academic record, grades, schedules and financial information related to their students, faculty and employees along with the details of its sponsors and organizations associated with it etc. The vast attack surface exposes IBA to the threat of these social engineering attacks.

One of the ways that IBA can become the victim of this is through pretexting. Emails of verifying whether or not the user has requested an email of password reset of various platforms such as the Oracle, LMS or the newly introduced UMS which hasn't been yet tested thoroughly. Another way IBA can experience this through emails is of scholarships being offered. These emails may contain the links which may direct the users to an unwanted website that asks the user to fill a form. In both these cases the attacker is creating a fabricated scenario by impersonating a trusted entity. If the victim in this case which may be the student or faculty complies then the attackers would successfully commit identity theft and can now use this data further to carry out malicious activities



Security Controls:

- Increase the spam filtering via email gateways and successfully flag these attempts as spam in your inbox.
- Implementing multi factor authentication. Now in order to gain access this would require another factor apart from username and password which increases the chances of preventing these social engineering tactics.

- Try obtaining SSL certification from authorities since this will help it to achieve encryption which in turns makes their information much more secure.

Impact on IBA's CIA:

1. Confidentiality:
There is risk of exposure of personal information or sensitive data which includes private communications, personal data, or even access credentials to sensitive systems. This results in data breaching as well.
2. Integrity:
Once gained access the attacker can easily manipulate the data according to their purpose of attacking and decisions made based on this inaccurate data can be flawed, leading to potentially harmful consequences for the organization.
3. Availability:
Social engineering attacks may indirectly impact availability by tricking individuals into performing actions that disrupt systems or services. Additionally, successful attacks can lead to security incidents that affect the availability of critical resources.

• NETWORK VULNERABILITIES:


Network vulnerabilities refer to weaknesses in a computer network's design, implementation, or operation that can be exploited by malicious actors to compromise the confidentiality, integrity, or availability of the network and its data. Identifying and addressing these vulnerabilities is crucial for maintaining a secure and resilient network infrastructure.

The network vulnerability that IBA faces is assigning of weak passwords to the student by the ICT department. Moreover, something that has further added to this vulnerability is the fact that the password that used to be only for the access of your university wifi is now also your password for ums (which holds your personal, academic and financial details) and lms (that holds your assignments). Due to this generality and assigning of weak passwords any other student can guess your password quite easily by make changes to a few digits. Not only that but students who figure out your password to one of the platforms can easily use this password to plagiarize your assignments and take away your credit.

Reminder Urgent: Protect Your Account - Do Not Share Passwords

US

UMS Support <umsupport@iba.edu.pk>
To: Students-All <Students-All@iba.edu.pk>


Fri 1/12/2024 10:23 AM

Dear Students,

I hope this email finds you well. We recently received complaints about unauthorized access to student accounts leading to course drops. We take the security of your accounts very seriously, and we want to remind you to never share your password with anyone.

Sharing passwords can compromise the confidentiality of your account and potentially lead to unauthorized actions, such as course drops or other security breaches. To ensure the safety of your account and personal information, please follow these important guidelines:

Change Your Password:

As a precautionary measure, we strongly recommend changing your password immediately. Use a strong, unique password that includes a combination of letters, numbers, and symbols.

Security Controls:

- IBA should establish and implement a policy of keeping strong passwords by allowing to keep passwords that require a minimum length, a mix of uppercase and lowercase letters, numbers, and special characters.
- They should set password expiration periods to prompt users to change their passwords regularly.
- They can also use multi factor authentication to add an additional layer of security.

Impact on:

1. Confidentiality:

Unauthorized access results in compromise the confidentiality of data. This includes student records, research findings, financial data, and personal information.

2. Integrity:

This can result alteration, corruption, or manipulation of data for eg: de-enrollments, changes in financial ledgers etc

3. Availability:

This can lead to service disruptions, making critical systems and resources unavailable to students, faculty, and staff, for eg: if access from only one system is allowed and some one else has already accessed from your credentials then you wont be able to access the site you want.

• PHYSICAL SECURITY THREATS:

Physical security threats refer to potential risks and dangers that can harm or damage an organization's tangible assets, including people, facilities, and equipment. These threats often involve direct physical actions or events that compromise the security and safety of a physical space.

Recently IBA has faced quite some physical security threats in terms of theft cases. This definitely became the cause of concern for many students since they were used to of leaving their laptops or mobiles on charge in case of low battery in library or prayer areas while they attended their classes. A huge number of incidents were reported, and actions were taken to identify who was behind these thefts however hardly anyone was caught. The stolen valuables may have a lot of personal, academic and financial details of the people they belonged to.

Thefts on Campus!

! This message was sent with High importance.

Thefts on Campus!



Office of Student Affairs

To: Students-All <Students-All@iba.edu.pk>

Cc: Office of Student Affairs <osa@iba.edu.pk>; +3 others



Mon 9/4/2023 5:34 PM

👍 4 ❤️ 5 😂 13 😮 5 😬 9

Dear Students,

We have received reports of multiple **thefts** of phones, wallets, and bags in the last 2 weeks. As per the IBA Code of Conduct and policy in the Student Handbook <https://www.iba.edu.pk/News/student-handbook2023-24.pdf> :

- Students are advised to display their IBA ID card and take care of their personal belongings at all times.
- The safety and security of personal belongings of students, including vehicles, is their own responsibility. IBA will not be responsible for any loss because of carelessness/irresponsible behaviour.

However, we are investigating the cases and checking CCTV footage - if we find the perpetrator(s) strict disciplinary action will be taken which may include expulsion from IBA. Both campuses are spaces where students, staff, and faculty should feel that they and their belongings are safe and secure. **Theft of personal belongings and valuables is unacceptable at IBA. We expect you all to behave responsibly.**

Security Controls:

- IBA should carry out risk assessment strategies and consider factors such as location, campus layout, access points, and the nature of assets to be protected.
- They should also invest in better quality surveillance systems and come up with a separate operational team that is capable of investigating these matters thoroughly and increasing the likelihood of retrieving the lost assets.

Impact on IBA's CIA:

1. Confidentiality:
Theft of physical or data storage devices may result in the loss of confidential information.
2. Integrity:
The integrity of personal or professional belongings is compromised when they are stolen or tampered with, leading to potential loss or unauthorized access to data.
3. Availability:
The unavailability of personal belongings due to theft can disrupt normal activities, causing inconvenience to students and affecting their ability to participate in academic and social engagements.

References:

1. (History and Timeline: IBA Official Website, n.d.)
2. (Institute of Business Administration, Karachi: Wikipedia, n.d.)^{3]}