Ministry of Federal Education and Professional Training

Cybersecurity Awareness

For further Information/Contact:
System Analyst, Ministry of Federal Education and Professional Training

CONTENTS

1 INTRODUCTION

1.1 Executive Summary

Cybersecurity is a critical aspect of protecting an organization's sensitive data and systems from cyber-attacks. Cyber-attacks can result in the theft or destruction of sensitive data, financial loss, and damage to an organization's reputation. Employee education and training on identifying and avoiding potential cyber threats, as well as reporting suspicious activity, is crucial for protecting an organization from cyber-attacks.

Honorable Prime Minister's Office has issued directives vide letter No.58-ITM/DS(IA-III)/2022 dated 29-09-2022 for establishment of focal point on Cybersecurity followed by capacity building of Human Resources.

In compliance of these directives, the Ministry of Federal Education and Professional Training has established a focal point in the Ministry under the supervision of Mr. Syed Junaid Akhlaq , Senior Joint Secretary(Admn) and Mr. Hameed Khan Niazi, Deputy Secretary (Admn). The Ministry has trained two Master Trainers, Mr. Talat Saeed, System Analyst and Mr. Shams-ur-Rehman, IT Specialist, through the National Information Technology Board (NITB) and National Cyber Security Academy (NCSA). Subsequently, these Master Trainers conducted a series of Cybersecurity Awareness Sessions for the personnel of Ministry and attached departments and organizations.

The Ministry has implemented "Train the Trainers" concept through these Cybersecurity Awareness Sessions. Training replication will continue in attached departments and organizations of the Ministry. In order to ascertain the skill development of Master

1 INTRODUCTION

Trainers, the Ministry utilized services of the Cisco Networking Academy[1] Program. Ministry also provided the opportunity to fifty-seven (57) master trainers in getting Cisco certificate on Cybersecurity Course.

1.2 Objectives

Cybersecurity helps to protect an organization's IT infrastructure and networks from unauthorized access, use, disclosure, disruption, modification, or destruction. By implementing robust cyber security measures, organizations can minimize the risk of a successful cyber-attack and protect their sensitive data and systems from unauthorized access or damage.

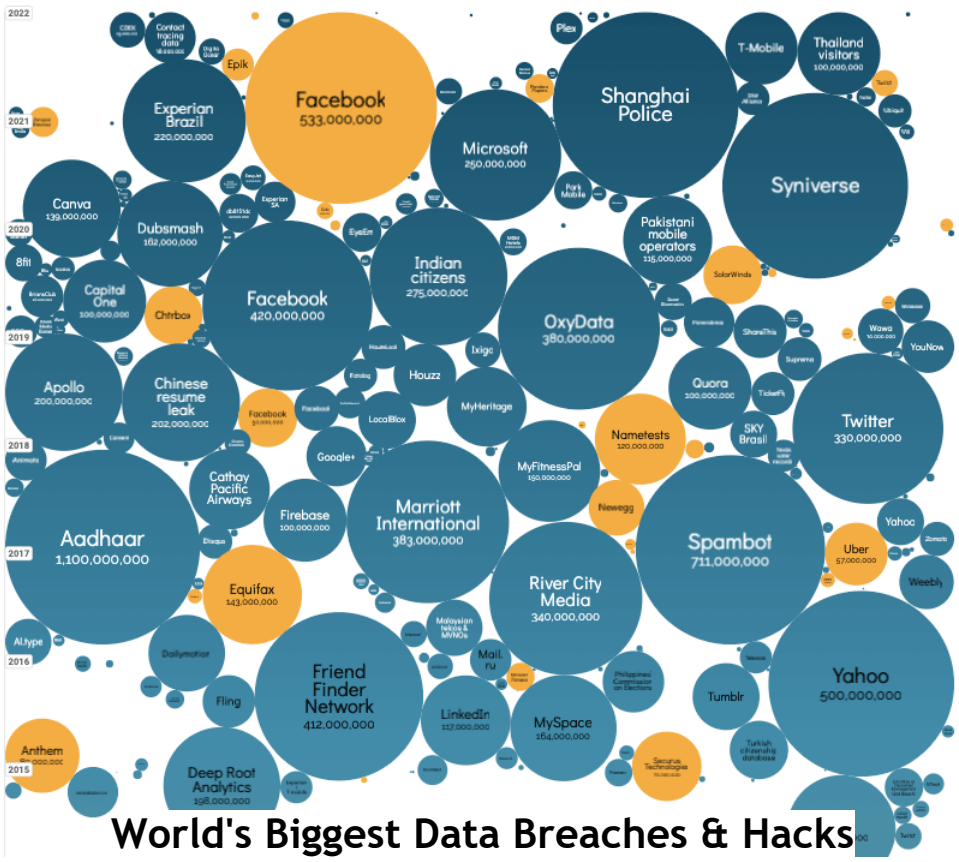
Employees are often the first line of defense against any cyber-attack. Inter alia, the employees need to be aware of various types of threats they may face, such as: phishing, malware, social engineering, and how to identify and avoid them. This can include best practices like avoid clicking on suspicious links, not opening attachments from unknown senders, and being cautious of fraudulent phone calls or messages.

Employees should also be trained on how to report a suspicious activity or potential cyber threat. This can include reporting an incident of receiving suspicious email or noticing a strange process running on their computer system. Timely reporting of suspicious activities can help organizations to quickly respond to potential threats and prevent them from causing harm.

[1] Cisco Networking Academy is a global IT and Cybersecurity education program that partners with learning institutions worldwide to empower people with career opportunities.

1 INTRODUCTION

The objectives of these awareness sessions were to, (a) educate individuals and attached departments/organizations focal persons about the potential threats and risks associated with the use of technology and the internet, and (b) to provide them with the knowledge and tools they need to protect themselves and their sensitive information from cyber-attacks. This also included information on topics such as safe browsing practices, identifying and avoiding phishing scams, protecting against malware, and maintaining the security of devices and networks. The goal was to increase the overall security of individuals and organizations and to reduce the risk of successful cyber-attacks. Instances of data breaches and hacks were also shared during the sessions.



As a follow up recommendation, it is important to provide refresher training and reminders to employees to keep them updated with the latest threats and best practices. For this purpose, Cybersecurity workgroup has been established through social media platforms for quick dissemination of information and reporting.

2 METHODOLOGY

"People impact security outcomes much more than any technology, policy, or process. People play an undeniable role in an organization's overall security and risk posture"
By: Garner, Leading Computer Trends Analyst

2.1 Cybersecurity Awareness

We live in a digital age where our personal and professional lives are intertwined on the internet. Almost everyone is active online, uses technology, and is on their mobile devices, making it easier than ever for hackers to target them. Through adequate security awareness training and cybercrime protection programs, organizations can protect themselves from emerging cybercrime threats.

According to IBM Cyber Security Intelligence Index, 95% of cybersecurity breaches are caused by a human error as firewalls cannot keep a staff member from succumbing to a phishing message. Organization could burn through millions on cutting edge security software but none of this will matter if employees are not appropriately prepared on the best way to spot and react to cyberattacks.

It is much simpler for cyber criminals to go through a short amount of time creating a phishing email than to spend months investigating zero-day vulnerabilities.

2 METHODOLOGY

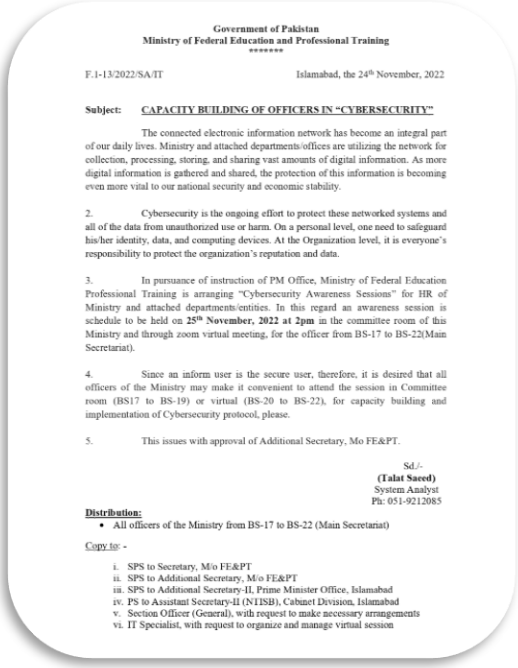
2.2 Capacity Building of HR in Ministry

A training program can help raise the awareness and knowledge towards being more susceptible to any threats – from phishing to physical security.

The capacity building the Ministry personnel was organized in two phases. In first phase training session was conducted in the committee room for officers from BS-17 and above. In second phase it was conducted for the staff in BS-15 and BS-16. Both sessions were also broadcasted through Zoom virtual meeting to encourage participation.

During these sessions, participants were informed that cybercrime can impact any organization and individual. Therefore, we want to create a cyber secure environment at the ministry for avoiding negative impacts.

The information and guidance provided during the sessions were intended to prepare them as first line of defense against possible cyber-attacks. Officers in the Ministry are now aware of the various types of threats including phishing, malware, and social engineering. They are sensitized to avoid clicking on suspicious links, not opening attachments from unknown senders, and being vigilant of fraudulent phone calls or messages.



Government of Pakistan
Ministry of Federal Education and Professional Training
****

F.1-13/2022/SA/IT Islamabad, the 24th November, 2022

Subject: **CAPACITY BUILDING OF OFFICERS IN "CYBERSECURITY"**

The connected electronic information network has become an integral part of our daily lives. Ministry and attached departments/offices are utilizing the network for collection, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

2. Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, one need to safeguard his/her identity, data, and computing devices. At the Organization level, it is everyone's responsibility to protect the organization's reputation and data.

3. In pursuance of instruction of PM Office, Ministry of Federal Education Professional Training is arranging "Cybersecurity Awareness Sessions" for HR of Ministry and attached departments/entities. In this regard an awareness session is schedule to be held on **25th November, 2022 at 2pm** in the committee room of this Ministry and through zoom virtual meeting, for the officer from BS-17 to BS-22(Main Secretariat).

4. Since an inform user is the secure user, therefore, it is desired that all officers of the Ministry may make it convenient to attend the session in Committee room (BS17 to BS-19) or virtual (BS-20 to BS-22), for capacity building and implementation of Cybersecurity protocol, please.

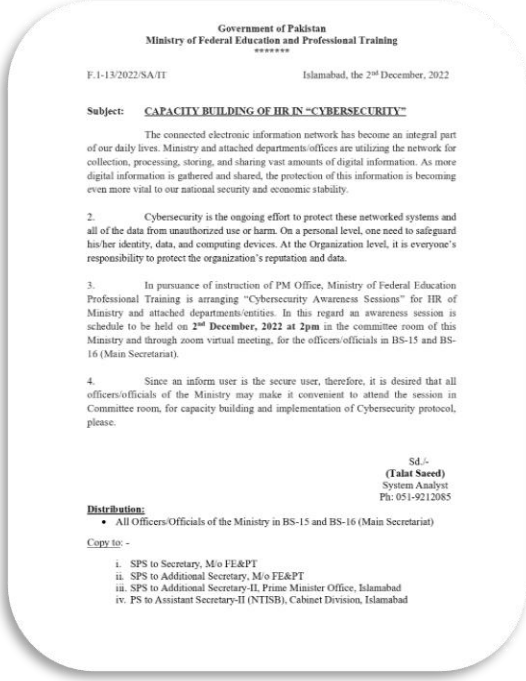
5. This issues with approval of Additional Secretary, Mo FE&PT.

Sd/-
(Talat Saeed)
System Analyst
Ph: 051-9212085

Distribution:
- All officers of the Ministry from BS-17 to BS-22 (Main Secretariat)

Copy to: -

i. SPS to Secretary, M/o FE&PT
ii. SPS to Additional Secretary, M/o FE&PT
iii. SPS to Additional Secretary-II, Prime Minister Office, Islamabad
iv. PS to Assistant Secretary-II (NTISB), Cabinet Division, Islamabad
v. Section Officer (General), with request to make necessary arrangements
vi. IT Specialist, with request to organize and manage virtual session



Government of Pakistan
Ministry of Federal Education and Professional Training
****

F.1-13/2022/SA/IT Islamabad, the 2nd December, 2022

Subject: **CAPACITY BUILDING OF HR IN "CYBERSECURITY"**

The connected electronic information network has become an integral part of our daily lives. Ministry and attached departments/offices are utilizing the network for collection, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

2. Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, one need to safeguard his/her identity, data, and computing devices. At the Organization level, it is everyone's responsibility to protect the organization's reputation and data.

3. In pursuance of instruction of PM Office, Ministry of Federal Education Professional Training is arranging "Cybersecurity Awareness Sessions" for HR of Ministry and attached departments/entities. In this regard an awareness session is schedule to be held on **2nd December, 2022 at 2pm** in the committee room of this Ministry and through zoom virtual meeting, for the officers/officials in BS-15 and BS-16 (Main Secretariat).

4. Since an inform user is the secure user, therefore, it is desired that all officers/officials of the Ministry may make it convenient to attend the session in Committee room, for capacity building and implementation of Cybersecurity protocol, please.

Sd/-
(Talat Saeed)
System Analyst
Ph: 051-9212085

Distribution:
- All Officers/Officials of the Ministry in BS-15 and BS-16 (Main Secretariat)

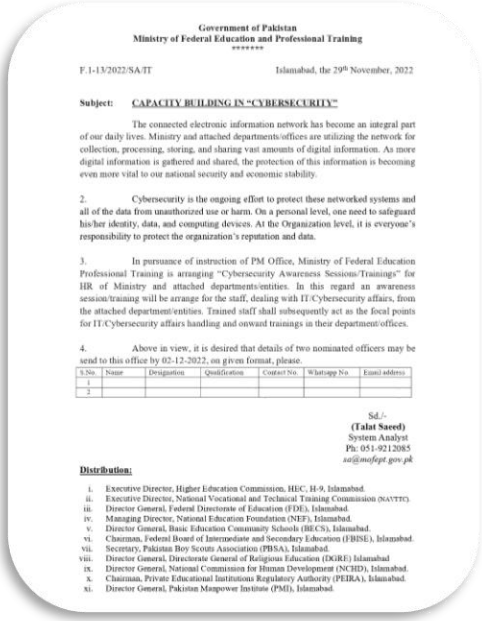
Copy to: -

i. SPS to Secretary, M/o FE&PT
ii. SPS to Additional Secretary, M/o FE&PT
iii. SPS to Additional Secretary-II, Prime Minister Office, Islamabad
iv. PS to Assistant Secretary-II (NTISB), Cabinet Division, Islamabad

2 METHODOLOGY

2.3 Capacity Building of Personnel in Attached Departments/ Organizations

The capacity building of personnel in the attached Departments and Organizations was executed through the nominations of Focal Persons. These Focal Persons will subsequently act as key contact points for handling Cybersecurity and subsequent trainings in their departments/offices.



Government of Pakistan
Ministry of Federal Education and Professional Training
****

F.1-13/2022/SA/TT Islamabad, the 29th November, 2022

Subject: CAPACITY BUILDING IN "CYBERSECURITY"

The connected electronic information network has become an integral part of our daily lives. Ministry and attached departments/offices are utilizing the network for collection, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

2. Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, one need to safeguard his/her identity, data, and computing devices. At the Organization level, it is everyone's responsibility to protect the organization's reputation and data.

3. In pursuance of instruction of PM Office, Ministry of Federal Education Professional Training is arranging "Cybersecurity Awareness Sessions/Trainings" for HR of Ministry and attached departments/entities. In this regard an awareness session/training will be arrange for the staff, dealing with IT/Cybersecurity affairs, from the attached department/entities. Trained staff shall subsequently act as the focal points for IT/Cybersecurity affairs handling and onward trainings in their department/offices.

4. Above in view, it is desired that details of two nominated officers may be send to this office by 02-12-2022, on given format, please.

S.No.	Name	Designation	Qualification	Contact No.	Whatsapp No.	Email address
1						
2						

Sd/-
(Talat Saeed)
System Analyst
Ph: 051-9212085
sa@mofept.gov.pk

Distribution:

i. Executive Director, Higher Education Commission, HEC, H-9, Islamabad.
ii. Executive Director, National Vocational and Technical Training Commission (NAVTTC).
iii. Director General, Federal Directorate of Education (FDE), Islamabad.
iv. Managing Director, National Education Foundation (NEF), Islamabad.
v. Director General, Basic Education Community Schools (BECS), Islamabad.
vi. Chairman, Federal Board of Intermediate and Secondary Education (FBISE), Islamabad.
vii. Secretary, Pakistan Boy Scouts Association (PBSA), Islamabad.
viii. Director General, Directorate General of Religious Education (DGRE) Islamabad
ix. Director General, National Commission for Human Development (NCHD), Islamabad.
x. Chairman, Private Educational Institutions Regulatory Authority (PEIRA), Islamabad.
xi. Director General, Pakistan Manpower Institute (PMI), Islamabad.

Training session was conducted at Federal Board of Intermediate and Secondary Education on 23rd December, 2022. A total of fifty participants attended in person and 10 participants joined via Zoom.

CYBERSECURITY AWARENESS SESSION

Location: Auditorium, FBISE, H-8/4
Date: 23-12-2022
Time: 9:00am
Facilitator: Talat Saeed, System Analyst

Agenda Items

09:00 – 09:30	Registration of Participation	
9:30 – 10:30	Cybersecurity: Threats and Preventions	**Talat Saeed** System Analyst
10:30 – 11:15	Cybersecurity and e-Governance	**Ahtesham Masood** Director, NITB
11:15 – 11:45	Effective utilization of e-Office portal	**Shams ur Rehman** IT Specialist
11:45 – 12:00	Refreshment	

Different topics related to Cybersecuirty were presented to the particpants. Primary focus included Cyber-threats and their preventions. Human factor was discussed in detail as it can potentially lead to big security problems. It was explained that how one click on a phishing link can expose a department's entire network to a malicious virus or a hacker.

The primary goal of Cybersecurity Awareness Training was to change the behavior of the ministry personnel. They are expected to be less susceptible to social engineering as a result of these sessions.

2 METHODOLOGY

Through social engineering a hacker can manipulate, influence, or deceive an employee to take action that isn't in the best interest of their organization. Common examples of social engineering attacks include phishing or spear-phishing by phone, email, postal service, or direct contact to trick people into doing something that will harm an organization's reputation. Employees need to be trained on reporting suspicious activity or potential cyber-threats, receiving suspicious emails, noticing strange process running on their computer. This can help organizations to quickly respond to potential threats and prevent them from causing harm.

"One of the most effective and commonly used methods of Cybersecurity awareness training being utilized by businesses today is interactive, Computer-Based Training (CBT). It uses modern technology such as laptops, tablets, smartphones, and Internet of Things (IoT) devices to engage your employees in learning about the invaluable role they play in protecting your business" (Oram Corporate Advisor). In order to utilize the potential of CBT, Ministry of Federal Education and Professional Training incorporated the blended learning model for Cybersecurity Trainings through Cisco Networking Academy Program.

All participants were then enrolled in 15 hours "Introduction to Cybersecurity" Instructor-led and online self-paced Course. The contents of course are as under:

- Introduction to Cybersecurity Introduction
- Chapter 1: The Need for Cybersecurity
- Chapter 2: Attacks, Concepts and Techniques

2 METHODOLOGY

- Chapter 3: Protecting Your Data and Privacy
- Chapter 4: Protecting the Organization
- Chapter 5: Will Your Future Be in Cybersecurity?
- Course Completion
- Final Exam
- Certificate of Completion

This training was assessed with frequent short quizzes and final examination for certification. This ensured that employees learn the valuable lessons and act as Organization's first line of cyber defense. Moreover, Ministry has the provision to monitoring the progress of learner through the Cisco Networking Academy dashboard.


Networking Academy

Certificate of Course Completion

Saad Irfan Khan

has successfully achieved student level credential for completing the Introduction to Cybersecurity course.

The student was able to proficiently:

- Explain the basics of being safe online, including what cybersecurity is and its potential impact.
- Explain the most common cyber threats, attacks, and vulnerabilities.
- Explain how to protect oneself while online.
- Explain how organizations can protect their operations against these attacks.
- Access a variety of information and resources to explore the different career options in cybersecurity.

Verified

Scan to Verify

January 12, 2023

Laura Quintana

Laura Quintana
Vice President and General Manager
Cisco Networking Academy

Participants enjoyed the training session, and acknowledged the efforts of Ministry for conducting an informative session. It's always encouraging to hear that participants enjoyed a training session and found it informative. The fact that they acknowledged the efforts of the Ministry is a testament to the hard work and dedication of those involved in organizing and delivering the training.

It's important to recognize and appreciate the value of such sessions, as they can have a significant impact on the knowledge and skills of the participants, as well as the overall effectiveness of the organization.

3 CONTENT SUMMARY

3.1 The Need for Cybersecurity

The connected electronic information network has become an integral part of our daily lives. Different types of organizations use this network to operate effectively. They utilize the network by collecting, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to national security and economic stability.

Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, one need to safeguard his/her identity, data, and computing devices. At the corporate level, it is everyone's responsibility to protect the organization's reputation and data. At the state level, national security, and the safety and well-being of the citizens are at stake.

The need for cybersecurity is becoming increasingly important as the world becomes more dependent on technology and the internet. There are several reasons why cybersecurity is necessary, including:

Protection of sensitive information: With the increasing use of technology and the internet, sensitive information such as personal data, financial information, and trade secrets is at risk of being stolen or misused.

3 CONTENT SUMMARY

Preventing cyber-attacks: Cybercriminals are constantly looking for ways to exploit vulnerabilities in computer systems and networks. Cybersecurity measures help to prevent cyber-attacks and protect against data breaches, unauthorized access, and other types of cybercrime.

Ensuring business continuity: Cybersecurity is critical for organizations to ensure that their operations can continue even in the event of a cyber-attack. This is particularly important for critical infrastructure, such as power grids and financial systems, which must remain operational to support the economy and the daily lives of people.

Maintaining public trust: Cybersecurity is also important for maintaining public trust in technology and the internet. When people feel secure using technology, they are more likely to adopt and rely on new technologies, which drives innovation and economic growth.

Complying with regulations: Many industries and sectors have regulations in place that require companies to implement adequate cybersecurity measures.

3.2 Who is doing hacking?

Hacking can be carried out by a variety of actors, including:

Cybercriminals: These individuals or groups engage in hacking for financial gain, such as stealing personal information to sell on the black market or to commit identity theft.

State-sponsored actors: Some nation-states engage in hacking as a tool of espionage or cyber warfare. These attacks can be used to steal sensitive information, disrupt critical infrastructure, or interfere with political processes.

Hacktivists: These individuals or groups hack websites and databases to draw attention to political or social issues. Their goal is often to bring attention to a cause or to protest against a particular entity.

Insider threats: Sometimes, the threat comes from within an organization, such as a current or former employee who has access to sensitive information and uses it for malicious purposes.

Script kiddies: These are novice hackers who use pre-written scripts or tools to carry out attacks. They may not have the technical expertise to carry out a complex attack, but they can still cause damage.

The motivations and objectives of hackers can vary widely, and the lines between these categories can sometimes be blurred.

3.3 Cyberwarfare

Cyberwarfare refers to the use of digital technologies, including computers, networks, and the internet, to conduct military operations or attacks against enemy targets. Cyberwarfare can take many forms, including:

Cyber Espionage: The theft of sensitive information or intellectual property for military or political advantage.

Cyber Attack: The use of cyber means to disrupt, disable, or destroy computer systems and networks, or to steal sensitive information.

Information Warfare: The use of information to influence public opinion, sow confusion, or interfere with decision-making.

Cyber Weaponization: The development of malware, viruses, and other malicious software that can be used for cyber-attacks.

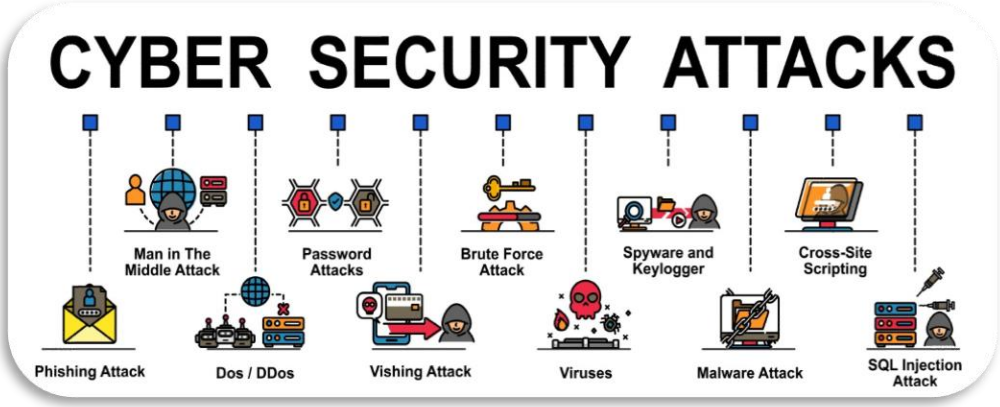
Cyberwarfare has become an increasingly significant concern for governments, military organizations, and businesses around the world, as the use of technology continues to expand and the internet becomes increasingly central to daily life and commerce. The potential impact of cyberwarfare is far-reaching, including economic disruption, physical damage to critical infrastructure, and loss of life.

3.4 Cybers-Attacks

There are different types of cybersecurity attacks, and new ones are being developed all the time. Some common types of cyber security attacks include:

Malware attacks: This type of attack involves the use of malicious software, such as viruses, Trojans, and ransomware, to harm computer systems and steal sensitive information.

Phishing attacks: Phishing attacks use fake emails, websites, or text messages to trick individuals into revealing sensitive information, such as passwords or credit card numbers.



3 CONTENT SUMMARY

Denial of Service (DoS) attacks: A DoS attack involves overwhelming a computer system or network with traffic to make it unavailable to users.

Man-in-the-Middle (MitM) attacks: In a MitM attack, an attacker intercepts communication between two parties and can alter or steal information being transmitted.

SQL injection attacks: SQL injection attacks target database systems by injecting malicious code into SQL statements.

Cross-Site Scripting (XSS) attacks: XSS attacks inject malicious code into webpages viewed by users, which can steal information or take control of the user's browser.

Advanced Persistent Threats (APTs): APTs are highly targeted and sustained cyber-attacks aimed at stealing sensitive information from government or corporate organizations.

Botnet attacks: Botnets are networks of compromised computers that can be controlled by attackers to carry out large-scale attacks, such as spamming or launching DoS attacks.

Malicious USB drives: It is a type of cyber threat that can be used to deliver malware and other malicious payloads to targeted computers. A malicious USB drive is typically a seemingly ordinary USB drive that has been modified to contain malware or other malicious code. When the USB drive is inserted into a computer, the malware can be executed, allowing the attacker to gain access to the computer and its data.

There are several ways in which a malicious USB drive can be used in an attack. For example, the drive can be left in a public place and then picked up by an unsuspecting victim, or it can be delivered as part of a phishing attack or a supply chain attack.

3.5 Latest Cybersecurity Challenges

The cybersecurity landscape is constantly evolving, and new challenges are emerging all the time. Some of the latest and most significant cybersecurity challenges include:

Cloud security: As more organizations move their data and applications to the cloud, they face new security challenges, such as protecting against unauthorized access, ensuring data privacy, and managing multiple cloud service providers.

Internet of Things (IoT) security: IoT devices, such as smart home devices and industrial control systems, are becoming increasingly common, but they also pose new security risks, as they can be easily hacked and used to carry out cyber-attacks.

Artificial Intelligence (AI) and machine learning-based attacks: Attackers are leveraging AI and machine learning to automate and scale their attacks, making it more difficult for organizations to detect and defend against them.

Cryptojacking: Cryptojacking is the unauthorized use of someone else's computer resources to mine cryptocurrency, which can slow down systems and consume significant amounts of energy.

5G security: The rollout of 5G networks presents new security challenges, as 5G technology is more complex and harder to secure than previous generations of cellular networks.

Remote work security: The COVID-19 pandemic has resulted in a massive increase in remote work, which has created new security risks, such as unsecured home networks and the use of personal devices for work purposes.

3.6 Cybersecurity Strategies

Overcoming cybersecurity challenges requires a combination of technical and non-technical measures. Here are some steps organizations can take to reduce their risk of a cyber-attack:

Implement strong passwords: Requiring employees to use strong, unique passwords and regularly changing them is an effective way to protect against password-based attacks.

Keep software up-to-date: Regularly updating software, including operating systems and applications, is essential to fixing known security vulnerabilities.

Use encryption: Encrypting sensitive data, both in transit and at rest, can prevent attackers from accessing it even if they gain unauthorized access to systems.

Implement a firewall: Firewalls can help prevent unauthorized access to a network by blocking incoming traffic from untrusted sources.

Train employees: Regular employee training on cyber security best practices and awareness of the latest threats can help reduce the risk of successful phishing attacks and other social engineering techniques.

3 CONTENT SUMMARY

Conduct regular security audits: Regular security audits can help identify and address vulnerabilities in systems and networks, allowing organizations to proactively address potential threats.

Use multi-factor authentication: Requiring multiple forms of authentication, such as a password and a security token, can provide an extra layer of protection against unauthorized access.

Backup data regularly: Regular data backups can help organizations quickly recover from a cyber-attack, reducing the potential damage from an attack and speeding up the recovery process.

Best practice for USB Drive: To reduce the risk of a malicious USB drive attack, it is important to follow basic cyber security best practices, such as never inserting a USB drive into your computer unless you are certain of its origin and contents. If you must use a USB drive, it is a good idea to scan it for malware before use, and to use encryption to protect sensitive data stored on the drive.

No single measure can guarantee complete protection against cyber threats, but by implementing a comprehensive security strategy that includes multiple layers of protection, organizations can significantly reduce their risk and be better prepared to respond to a cyber-attack.

3.7.1 Case Study: Pegasus

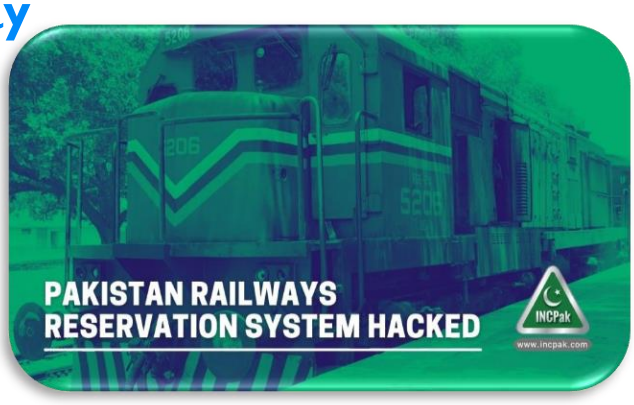
The Pegasus cyberattack is a well-known and highly sophisticated hacking operation that was discovered in 2016. The attack was carried out by a group believed to be associated with the Israeli intelligence agency, and it targeted high-value individuals and organizations in various countries, including politicians, journalists, human rights activists, and military officials.

Pegasus is a highly advanced and complex piece of malware that is capable of infecting a target's phone and giving attackers complete control over it. The malware can be delivered through a text message or a phone call, and once installed, it can steal sensitive information, such as text messages, emails, contacts, and other data stored on the phone.

The Pegasus cyberattack has been widely criticized for its potential impact on human rights and civil liberties, as it can be used to monitor and control the communications of political dissidents and other high-value targets.

3.7.2 Case Study: Pak Railway

Pakistan Railways reservation system was reportedly hacked on January 26, 2021 causing inconvenience for hackers around the country. The technical team at Pakistan Railways believes that the reservation



system was hacked by Indians, according to a report by 24 News HD.

According to the details provided by the local media outlet, the hackers have wiped out important data from the reservation system and the technical team at Pakistan Railways is clueless to the root cause of the problem.

3.7.3 Case Study: NBP

On the eve of Oct 29, the National Bank of Pakistan (NBP) encountered a phishing attack and people weren't able to use the services of the bank. Lately, the national bank has announced that customers' financial data has not been compromised and "has remained protected, confidential and secured." Along with that, the systems of the bank are also repaired.

3.7.4 Case Study: FBR

On 14th August 2021, the hackers attacked the FBR data center and caused to down all official websites operated by the tax machinery for more than 72 hours. The attack was identified immediately because of the scale of disruption that it caused.

FBR's technical wing stated that the hackers invaded the system by exploiting the weakest link, which was the Hyper-V software by Microsoft Inc. The second version

stated that the hackers disrupted the system by hacking the login ids and passwords of the data center administrators. Another report, which prepared by private and government cybersecurity experts, stated that the hackers used Spear-phishing emails as the medium for this breach.

3.7.5 Case Study: WhatsApp Voice Call

There have been reports of hackers exploiting a vulnerability in WhatsApp that allows them to compromise a user's device through a voice call. The vulnerability allows the attacker to inject malicious code into the user's device, even if the user doesn't answer the call. This can lead to the installation of spyware or other malicious software that can steal sensitive information or take control of the device.

It is important to keep WhatsApp, updated with the latest security patches and to be cautious about accepting calls or messages from unknown contacts.

3.7.6 Case Study: Free Wifi

In 2015, a group of researchers conducted an experiment to demonstrate how easy it is to hack into a Wi-Fi network that does not have proper security protocols in place. They set up a fake Wi-Fi network in a busy coffee shop and named it "Free Wi-Fi."

They did not password-protect the network, which made it easy for anyone to connect to it.

Within minutes of setting up the fake Wi-Fi network, several customers at the coffee shop connected to it, thinking it was a legitimate free Wi-Fi service. The researchers were able to intercept the internet traffic of these customers and view their online activities, including their login credentials for various websites.

They were also able to deploy malware onto the devices of the customers that connected to the fake Wi-Fi network, which allowed the researchers to control these devices remotely. The researchers could access the personal information of these customers, including their contacts, photos, and other sensitive data.

3.7.7 Case Study: QR Code

In 2019, a group of researchers discovered a vulnerability in the QR code scanning feature of some popular mobile apps that allowed hackers to redirect users to malicious websites. They created a fake QR code and placed it on a flyer that was distributed at a tech conference. The QR code led to a website that looked legitimate, but in reality, it was a phishing website designed to steal the login credentials of the users.

When users scanned the QR code using their smartphone, they were redirected to the phishing website, where they were prompted to enter their login credentials. The researchers were able to steal the login credentials of the users who fell for the phishing attack.

Users should be wary of scanning QR codes that are distributed in public places or on flyers, as they could be fake and lead to malicious websites.

4 CONCLUSION

4.1 Conclusion

Capacity building is essential for institutional growth. Training personal on cyber security protects an institution from threats like, E- deception. Ministry of Federal Education & Professional Training nurtures its human resources in an incentivized way. This will enable ministry's institutional capacity to face the challenges of 21st century. Cyber bullying exists in real and capacity building is the only way to cope it rightly.

Cyber threats are evolving and becoming more hazardous. It is essential that we remain vigilantly proactive for in protecting our digital assets. Promoting cybersecurity awareness creates a culture that ensures the safety and security of our digital infrastructure.

We have seen that the lack of cybersecurity awareness is a major cause of unauthorized access and cyber-attacks. The importance of strong passwords, regular software updates, and anti-virus protection cannot be overstated, and we must take responsibility for ensuring that our digital assets are secure.

In the future, we must continue to monitor the evolving threat landscape and adapt our cybersecurity strategies accordingly. It is essential that we stay informed about the latest cyber threats and adopt best practices to our digital assets. By prioritizing cybersecurity awareness and education, we can create a secure digital environment for us, our families, and our institutions.

It is important that organizations, educational institutions, and ministry work together to develop comprehensive cybersecurity strategies that prioritize cybersecurity awareness and education. By promoting cybersecurity awareness, we can create a culture of cybersecurity that ensures the safety and security of our digital infrastructure.

5 FEEDBACK

5.1 Participants Feedback

"The Ministry of Federal Education and Professional Training in collaboration with NTISB, on 23rd January 2022, conducted a session on Cybersecurity Awareness at FBISE auditorium. I had the privilege of attending the session. I found the course to be very practical. The main thing I learned was that, as a company, we need to share information and accountability across the board and have a little bit more insight into our processes and other operations. And we must set up such procedures, strategies, and staff training immediately. Simply said, I don't believe anyone is aware of or understands the significant degree of danger that cyberattacks bring. But apart from being extremely instructive, this course excelled at alarming or frightening me about the insecurity of my data being sent or received online. Overall, I loved the training and found it to be quite engaging. I'm hoping to be able to return with a more explicit understanding of my comprehension and how I can play my part in ensuring the safety of my organization and its employees' data".

Saad Irfan Khan
Lecturer CS, Department of Information Engineering Technology
National Skills University Islamabad.

"This interactive session illuminated us how to use information technology for our benefit in a safe environment. The mentors clearly stated the precautionary and security measures to avoid being threatened by hackers. They equipped us to save ourselves for being victim of cybercrimes in this Modern Electronic World. I would suggest that the ministry should conduct more sessions on this pattern to enlighten us how we can survive safely in the Era of Technology".

Javeria Aslam
Vice Principal,
Federal Directorate of Education, Islamabad

5 FEEDBACK

"The session on Cyber security was useful and informative. The online consequent Course is also full of learning.".

Nadia Mazhar
Vice Principal, Federal Directorate of Education

"The Cybersecurity Awareness Session taught us a lot and the activity was really beneficial. But during the workshop, the sound quality was poor which disturb the remote participants.".

Dr. Muhammad Abdul Qayum
Assistant Professor, Department of Computer Science
National Textile University Faisalabad.

"The Cybersecurity Awareness Session was an excellent one as it sensitised the participants about cybersecurity, its needs, and the ways how to secure our security while working in the world of technology and networking. I recommend such sessions for other employees of the department as well. We have also been registered in CISCO cybersecurity course and learnt how to secure our systems while working in an organisation. This will increase digital literacy and is helpful in achieving SDG# 4 and 17 (Quality Education, Partnership for Goals). I would love to take part in such a course in the nearby future as well".

NAUREEN SARWAR,
Vice Principal,
Federal Directorate of Education

6 PICTURES GALLERY

6.1 Journey Through Pictures