الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للامن السيبراني
National Cyber Security Agency

Digital Safety Guide

Digital Safety Guide

Intellectual Property Rights

To Contact The National Cyber Security Academy

www.ncsa.gov.qa/
academy@ncsa.gov.qa
00974 404 663 79
00974 404 663 62

Table of Contents

Introduction

In the light of seeking to build a cybersecurity-safe community and improving cybersecurity and digital safety indicators at the level of the state, institutes and society; the National Cyber Security Agency has launched the National Initiative for Digital Safety that targets the various society segments. It presents cyber awareness content contributing to promoting cybersecurity culture in the society to become a public culture and a lifestyle entrenching digital safety indicators in the society.

The swift technological advance, the vertical and horizontal spread of the internet, cyberspace development, and the emerging complicated cyber threats, particularly after AI revolution and generative AI, directly contributed to escalating the cyber threats faced by all society categories with no exception. This reality necessitates a growing attention to be paid to the spread of cyber awareness and culture and equipping people with cyber-awareness content that gives them the capacity to handle internet and modern technology safely and efficiently.

On the other hand, spreading cyber awareness and culture depends on different awareness tools including the guides considered to be effective. Accordingly, this guide was born to be a treasure trove of the different cyber risks that can be encountered by individuals in their daily interaction with the internet and its various applications. Moreover, it offers advice and general instructions on how to deal with cyber risks with a special focus on risks threatening personal data and the dangers of social engineering and phishing. It also tackles how to secure online accounts and emails, and other relevant concepts.

Concept of the Guide

The concept of the guide is anchored in the significance of the National Initiative for Digital Safety seeking to promote the indicators of cybersecurity and digital safety in the society. The concept also revolves around presenting awareness content with the purpose of enabling all the segments of the society to accurately identify the cyber risks that can be found in their daily interaction with the internet and technological tools.

The concept is extended to include providing the different society categories with a guide and reference to know how to deal with cyber risks and threats. In this way, the guide is not limited to a certain segment of the society, but it is rather directed to all the segments of the society. That is why it includes a comprehensive, not personalized, awareness content to suit all the awareness needs of all the society and entrench the added knowledge value expected from the guide.

The concept of the guide aims to stimulate the critical and analytical thinking of individuals by drafting analytical questions to the readers at the end of every chapter of the guide. Thus, the guide goes beyond indoctrination to become a relatively interactive book which elevates its expected effect and helps in fixing the content in the minds of targeted segments.

Purpose of the Guide

The guide aims to achieve a set of objectives centred around enhancing cyber awareness and culture among various segments of society. The key objectives of the guide are as follows:

1. Clarifying the concepts of cybersecurity and digital safety and explaining the points of agreement and difference between them.

2. Providing society with cyber awareness content related to the most important, common, and well-known cyber threats and risks.

3. Promoting a culture of digital safety in society, transforming it into a common culture and lifestyle.

4. Empowering individuals to accurately identify cyber risks, raising awareness about their dangers, and how to deal with them.

5

Providing a special reference on digital safety that is accessible to all, enabling continuous reference to learn about cyber risks.

6

Explaining the common mistakes users make when dealing with the internet and raising awareness about the risks of these practices.

7

Contributing to achieving the goals of the National Initiative for Digital Safety by helping to enhance cybersecurity and digital safety indicators in the country.

Chapter 1
The Concept of Cybersecurity and Digital Safety

- Introduction
- Cybersecurity Concept
- Cybersecurity Objectives
- Cybersecurity Pillars
- Cybersecurity Domains
- Digital Safety Concept and Dimensions
- Digital Safety Objectives
- The Intersection and Differences between Cybersecurity and Digital Safety
- Activities

Introduction

The widespread of technology and internet has led to the relative popularity of cybersecurity and digital safety concepts. It is now widely used by specialists and non-specialists. However, for the society segments of non-specialists in IT and cybersecurity, these concepts may sound similar which is not accurate. Despite the intersection between both concepts, each of them tackles a specific dimension and is different in terms of scope, goals and axes.

The complete analysis and realisation of cybersecurity and digital safety concepts represent the main entrance to enhancing cybersecurity awareness and digital safety culture in the society. From the practical perspective, it is not possible to promote digital safety in the society when all its members are unaware of this concept accurately and lack the knowledge of its axes, goals, scope, and effect. Based on this, this chapter defines cybersecurity, digital safety and relevant concepts.

Cybersecurity Concept

Cybersecurity is defined as

> "the protection of systems, networks, and critical infrastructure, including information systems and operational technology systems, their components such as hardware and software, the services they provide, and the data they contain, from any unauthorised access, disruption, modification, inspection, use, or exploitation".

It is also defined as:

> "a set of technical, administrative, and organisational measures used to prevent the theft of electronic information of individuals and organisations, and to aid in the recovery of any stolen information[1].

1. Yusuf, A. (2015). Cybercrimes in the Arab Gulf States: International and local countermeasures. Cairo, Egypt: Dar Al-Kutub Al-Arabiya. pp. 68-74.

These definitions clearly show that cybersecurity involves the measures and actions taken by governments, institutions, and specialised cybersecurity bodies to protect critical infrastructure and safeguard systems and networks from cyberattacks. Thus, it is a set of practical measures implemented by cybersecurity and information technology specialists.

The term 'cybersecurity' is composed of two words: 'security', which is the opposite of fear and signifies reassurance, tranquillity, and a sense of safety when dealing with something; and 'cyber', which refers to the digital space, the internet, and all the tangible and intangible elements associated with them, such as devices, networks, software, and more. The word 'cyber' is derived from 'cybernetics', a term associated with the science of automatic control and the ability to control machines[2].

The term "cybernetics" has Greek origins, deriving from the ancient Greek word meaning "governor." It was first introduced in the 1940s to refer to the science of control and communication between living beings and machines. Within this context, the term "cybernetics" may be defined as:

> "The processes of managing all that is digital and connected to the internet"

2. Kamal, M. (2022). Cyber Terrorism: When the Terrorist Uses the Keyboard Instead of the Bomb. Cairo, Egypt: Dar Kelim. p. 11..

Cybersecurity Objectives

Cybersecurity strives to accomplish a comprehensive set of objectives focused on maintaining the stability of cyberspace, encompassing both tangible and intangible elements. The following provides a detailed breakdown of the most critical of these objectives:

1

Protecting Sensitive Information and Data

The primary goal is to safeguard sensitive data, such as financial and health information and trade secrets, from theft or tampering.

2

Addressing Cyberattacks

Through measures and procedures that enable the anticipation and handling of attacks before they target institutions and critical infrastructure.

3

Supporting Swift Recovery from Cyberattacks

Cyberattacks can lead to significant economic losses and disrupt operations and technology. To mitigate these impacts, cybersecurity aims to rapidly address damages and restore systems to normal function.

4

Ensuring Business Continuity

By safeguarding electronic systems from disruptions and outages, cybersecurity promotes uninterrupted business operations.

5

Adhering to Standards and Laws

Many countries and companies are obligated to comply with cybersecurity laws and regulations designed to protect sensitive data and information.

6

Protecting Critical Infrastructure

Cybersecurity is essential for safeguarding critical infrastructure, including communication systems, energy grids, water supplies, and other technology-dependent systems.

7

Fostering Digital Trust

By securing information systems, cybersecurity enhances trust in digital transactions and electronic commerce.

Cybersecurity Pillars

Cybersecurity encompasses several interconnected components that work together to achieve its objectives. The most important of these components are as follows:

1 Cybersecurity Strategy Organisation

Cybersecurity focuses on developing both preventive and remedial cybersecurity strategies. Preventive strategies involve measures taken to protect institutions and critical infrastructure before a cyberattack occurs. Remedial strategies, on the other hand, deal with attacks after they have happened, working to minimise their negative impacts and support recovery efforts.

2 Technical Axis

This relates to the technologies and tools used to protect systems and networks, such as antivirus software and firewalls.

3 Legal Axis

This axis focuses on developing and implementing laws and policies that govern the behaviour of individuals and companies regarding cybersecurity.

4 Organisational Axis

The organisational axis is concerned with managing cybersecurity within institutions and ensuring that everyone follows the best security practices and standards.

5 Capacity Building

This aims to enhance skills and knowledge in the field of cybersecurity through training and education.

6 International Cooperation

This involves cooperation between countries and international organisations to confront cross-border cyber threats.

Cybersecurity Domains

Cybersecurity operates across multiple sectors and domains to achieve its goals. These areas may evolve and expand as the cyberspace grows and develops. The following outlines the most significant of these domains:

Network Security

In this sector, cybersecurity focuses on protecting networks from cyberattacks and digital intrusions and aims to maintain their operational efficiency.

Application Security

Application security strives to create a safe digital environment for applications. It involves incorporating digital security standards into the application design process to make them resistant to hacking. This area also focuses on developing applications that can defend against cyberattacks and detect and remove malicious software.

Information Security and Data Safety and Privacy

This axis of cybersecurity focuses on implementing the necessary measures and safeguards to ensure the security of information and data. Its primary goal is to protect sensitive information from theft, hacking, and other malicious attacks.

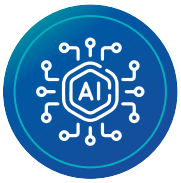
End-user Security

This axis is a critical and primary focus in cybersecurity. It is concerned with providing digital security for individuals, protecting them from potential threats such as personal data breaches, ransomware attacks, and other digital risks[3].

Cloud Security

It is a set of procedures and techniques designed to protect data, applications, and infrastructure in cloud environments. Cloud security also forms an essential part of cybersecurity, as it focuses on countering threats targeting cloud computing resources, such as data theft, unauthorised access, or cyberattacks. This is to ensure the integrity of information and maintain the confidentiality and continuity of operations.

3, What is end user security? CISCO, https://www.cisco.com/site/us/en/learn/topics/security/what-is-user-security.html#jump-anchor-3



Artificial Intelligence (AI)

With its rapid advancements, AI has become a cornerstone of cybersecurity and a critical domain within it. It can be used and utilized in several important areas, the most important of which are the following:

- **Using Artificial Intelligence to Counter Cyberattacks:** Through AI technologies, it is possible to confront cyberattacks. This is due to its high ability to process large amounts of data in record time, enabling it to identify potential digital vulnerabilities and address them before they are discovered by attackers. Additionally, its techniques can be used to support recovery indicators after cyberattacks.

- **Countering AI-Powered Cyber Threats:** Cyber attackers have leveraged AI to develop more sophisticated and successful cyberattacks. By rapidly identifying digital vulnerabilities and employing deepfakes and highly convincing phishing messages, AI has enhanced the threat landscape. In response, cybersecurity professionals are developing strategies, policies, and procedures to effectively address these advanced cyber threats.

Digital Safety Concept and Dimensions

Digital safety refers to the collective practices adopted by companies and individuals to protect against cyber threats. It primarily focuses on education and awareness, aiming to equip individuals and the general public with the knowledge to recognise cyber risks, understand how to deal with them and establish preventive measures.
Digital safety is based on a set of dimensions, as follows:

1

Privacy

The protection of personal information and sensitive data when they are used or shared via the internet.

2

Safety

It is the focus of digital safety by avoiding cyber threats such as malware and hacking.

3

Awareness and education

They are the backbone and the cornerstone of digital safety to strengthen the capacity to identify and avoid cyber threats including phishing and online fraud.

4

Responsible behaviour

To safely and responsibly interact with others via the internet either on social media or on other digital environments.

Digital Safety Objectives

Digital safety aims to achieve several goals and focuses mainly on protecting people from cyber risks through awareness and education. The goals are broken down as follows:

1 Privacy Protection

With the goal of ensuring that individuals can control how their personal data is used and shared and guaranteeing that it is not exploited by unauthorised parties.

2 Awareness of Safe Internet Use Rules:

Through raising awareness among individuals about how to protect themselves from cyber threats, such as phishing, identity theft, and others.

3 Limiting Cybercrime

Digital safety aims to reduce cybercrime through education and safe cyber practices. It also aims to decrease the chances of individuals being exposed to cyberattacks such as electronic fraud and data theft.

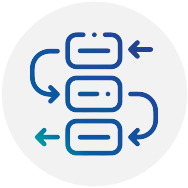
4 Promoting Ethical Cyber Behaviour

By encouraging users to adopt safe and responsible behaviours when interacting online, including refraining from publishing or sharing harmful or unsafe content.

5 Protecting the Most Vulnerable Groups to Cyber Threats

Many social segments are described as most vulnerable to cyberattacks, meaning that their experience with the internet and their awareness of its risks are low, making them prime targets for criminals, such as children and adolescents who may be more susceptible to online dangers. Digital safety programs contribute to educating parents and teachers on how to protect these individuals.

With the increasing reliance on the internet and technology in everyday life, digital security has become more important than ever. It aims to protect individuals from threats that could impact their personal, financial, and social lives, fostering trust in technology and helping to create a safe and sustainable digital environment.



Intersection and Differences between Cybersecurity and Digital Safety

While the concepts of cybersecurity and digital safety intersect at certain points and axes, they differ in others. They diverge in overall concept, objectives, scope, and other dimensions. The following table illustrates the differences between the two concepts according to various axes.

Axis to be compared	Cybersecurity	Digital safety
General concepts	The concept focuses on protecting systems, networks, and critical sensitive data from cyberattacks and threats. It also aims to secure information and vital infrastructure from breaches and threats.	The concept emphasises educating and raising awareness among individuals about how to protect themselves from cyber threats while using technology and the internet. It also focuses on safe behaviours and awareness of the personal risks that users may face.
Scope	Cybersecurity focuses on issues related to network security, data protection, developing cybersecurity strategies, and collaborating with government agencies and companies in the field of cybersecurity.	It primarily focuses on raising awareness and educating individuals, including privacy protection, fraud prevention, and safe internet usage.

Axis to be compared	Cybersecurity	Digital safety
Objectives	• Protecting sensitive data. • Ensuring business continuity by protecting systems and critical infrastructure. • Putting preventive and remedial cyber strategies. • Developing plans to counter cyberattacks. • Compliance with laws and regulatory standards.	• Protecting privacy to ensure control over the use of personal data and prevent its exploitation. • Raising awareness about safe internet usage guidelines to safeguard individuals from cyber threats such as phishing and identity theft. • Reducing cybercrime through education and secure cyber practices. • Promoting ethical cyber behaviour by encouraging responsible internet usage. • Protecting the most vulnerable groups from cyber threats, such as children and adolescents, through awareness and support.

Axis to be compared	Cybersecurity	Digital safety
Target audience	It primarily focuses on institutions, governments, and companies that need to secure their information and systems.	It targets the public, including those who are not experts in cybersecurity and information technology, to educate them on how to protect themselves and their personal information.
Used techniques and tools	Cybersecurity employs advanced technologies such as encryption, artificial intelligence, firewalls, intrusion detection systems (IDS), and analysis of emerging systems and threats to monitor and protect systems.	Training and awareness methods, such as workshops and training courses, are used to enable individuals to recognise cyber threats and take steps to protect themselves.
Handling threats	It addresses complex and advanced threats that require immediate response and sophisticated technology.	Digital security addresses the most common threats, which target individuals, such as phishing, through education and awareness.

In conclusion, cybersecurity and digital safety are crucial concepts for nations, institutions, communities, and individuals. Cyber threats have become ubiquitous, making cybersecurity culture a national and social priority.

It must be emphasised that government agencies and institutions responsible for cybersecurity and digital safety cannot achieve cybersecurity and digital safety in society alone without the active cooperation of various segments of society. Digital safety is a collective responsibility that requires the cooperation and concerted efforts of various parties.

Activities

Activity 1

Research the activities, events, programs, and initiatives of the National Cyber Security Agency in the State of Qatar. Identify its most important activities, determining whether they fall under the scope of cybersecurity or digital safety.

Activity 2

Research the most common cyber threats faced by institutions and individuals, explaining the difference in the nature of the attacks targeting each.

Activity 3

Individuals face multiple cyber risks. Research these risks and identify the negative impact of each.

Chapter 2
Cyber Risks Concept and Types

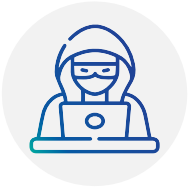
- **Introduction**
- **Cybercrimes**
- **Cyber Risks Concept**
- **Cyber Risks Types**
  * Ransomware
  * Spyware
  * Phishing
  * Social Engineerin
- **Cyber Threats to Networks**
- **Activitie**

Introduction

With the rapid spread of the internet and the expansion of cloud computing, big data, and artificial intelligence, the importance of digital security is increasing. The technological revolution has made society and individuals more vulnerable to cyber threats that can lead to multiple losses, including financial losses, reputational damage, data loss, and even disruption of critical infrastructure.

The concept of cyber risks has become an increasingly significant concern for both individuals and organisations. Cyberattacks have grown more sophisticated and diverse, encompassing ransomware, espionage, phishing, social engineering, data breaches, and other cyber threats.

Generally, it is impossible to enhance digital safety awareness within a community without a comprehensive understanding of cyber risks and their negative consequences. Based on this premise, this chapter will define cyber risks and threats, outline their various types, and explain how to prevent them.



Cybercrimes

> Qatar's legislation has focused on cybercrimes, imposing penalties on perpetrators to deter them. These laws bolster the country's digital safety indicators. The Cybercrimes Law, enacted in 2014, defines cybercrime as "any act that involves unlawful use of information technology means, information system, or the information network, in breach of the provisions of this law[4]."

4. Cybercrime Prevention Law of Qatar, No. 14 of the Year 2014, Al Meezan, available at the following link: https://almeezan.qa/LawView.aspx?opt&LawID=6366&language=ar

Generally, cybercrimes are distinguished by certain features from conventional crimes as follows:

1. Cybercrimes rely on using technological devices such as computers and smartphones to carry out hacks and extort victims.

2. These crimes are highly covert, as their traces can be easily hidden, or they may not be reported due to fear or socio-cultural reasons.

3. Cybercrimes are characterised by extreme speed; they can be executed within seconds.

4. Cybercrimes can be carried out remotely, meaning they have no geographical boundaries, especially in the context of digital globalisation.

5. The legal pursuit of cybercrimes faces numerous challenges, especially when the criminal is in a different country than the victim.

6. These crimes are considered «soft» as they are carried out using technical tools without the need for physical force.

Cyber Risks Concept

Cybersecurity risks refer to the threats and challenges that target information systems and technical networks, ranging from data theft and destruction to the disruption of vital services. These risks encompass both internal and external factors, such as malicious attacks carried out by hackers or human errors that lead to data leakage.

Cybersecurity risks are not limited to harmful activities such as viruses or direct attacks on systems only. They also include weaknesses in technological infrastructure, misuse of security systems, and unconscious human behaviour that may facilitate the breaching of systems.

Cyber Risks Types

Cyber risks encompass various types, all of which pose threats and cause harm to users. Below is an outline of the most significant types of these risks.

1

Ransomware

Ransomware is a form of electronic extortion. It is malware used by malicious actors to extort money from others[5].

Ransomware is one of the most dangerous forms of cyberattacks in the modern era. This type of malicious software encrypts system files or data, and the attacker then demands a ransom to restore access to those files. Ransomware is often distributed through phishing emails or by exploiting security vulnerabilities in inadequately protected systems.

Ransomware has become an increasingly global threat, targeting large organisations such as hospitals and multinational corporations, and causing significant financial losses.

5 . Guidelines on Ransomware Software, National Cyber Security Agency, available at the following link: https://ncsa.gov.qa/sites/default/files/2024-10/NCSA_CSGA_Guidelines_Ransomware_Attacks_AR_V1.0.pdf?csrt=5855983971683337

Ransomware Types

- **Crypto Ransomware:** It encrypts users' important files and hinders access to them until the ransom is paid. It is the most popular type.
- **Locker Ransomware:** It doesn't encrypt files; however, it shuts the whole system and prevents users' access to it. It usually asks for paying a ransom to return the control over the device[6].
- **Scareware:** A type of malicious software that pretends as legitimate security programmes. It frightens users by displaying messages warning of fabricated security issues and demands a ransom to resolve the alleged problem.

Principles of Prevention of Malicious Software

In spite of the dangers of malware, prevention can be easily achieved by following a set of precautions, including:

- **Data backup:** It is the most important protection measure that enables the user to retrieve the data if they are encrypted.
- **Updating operation systems and anti-virus software:** Updates reduce the security loopholes and help protect the devices from cyberattacks.
- **Using firewalls:** Firewalls contribute to preventing attacks from malware that target the devices.
- **Understanding the operation mechanism of malware:** Full awareness of the operation mechanism of the different types of malwares is major for protecting the society.

6. Guidelines on Ransomware Software, National Cyber Security Agency, available at the following link: https://ncsa.gov.qa/sites/default/files/2024-10/NCSA_CSGA_Guidelines_Ransomware_Attacks_AR_V1.0.pdf?csrt=5855983971683337

2

Spyware

Spyware are malware sneaking into the system to collect personal information and data like bank account information, passwords, and users' personal history. Usually, spyware are installed via malicious links or fake applications.

Spyware are often used in fraud actions to steal identity and spy on the activities of individuals and companies posing themselves as the largest cyberattacks.

Types of Spyware

- **Keyloggers:** This software records every click on the keyboard to record sensitive information like passwords or credit cards information.
- **Adware:** It displays unwanted ads on the users' devices to collect personal information by interacting with these ads.
- **Trojans:** They open a loophole in the system that allows the hackers to remotely sneak into the device.

3

Phishing

Phishing is a form of cyberattacks that depend on social engineering to deceive users into disclosing sensitive information such as passwords or credit cards data, etc. This is usually done by fake emails that seem as if they come from trusted sources[7].

Types of Phishing

Phishing is one of the most popular and most dangerous cyberattacks for their smooth implementation and ability to easily manipulate individuals, including:

- **Email Phishing:** Emails containing malicious links or attachments are sent to deceive users into disclosing their personal data.
- **Spear Phishing:** In this type of phishing, the phishing message is sent to certain individual or institution with the purpose of obtaining specific sensitive information.

7. Given the seriousness of phishing, a separate chapter will be dedicated to it within the context of this guide.

4

Social Engineering

Social engineering is a term used to describe a technique employed by cyber attackers. Through this technique, attackers persuade victims to divulge personal information or to interact with them in a way that benefits the attacker. This might involve encouraging victims to click on malicious links, which can lead to the installation of harmful software. Attackers often exploit the lack of cybersecurity knowledge among internet users. It relies on manipulating human behaviour to deceive users into providing information or taking actions that facilitate cyberattacks. Attackers analyse the victim›s behaviour to gather information that can aid in compromising a system.

Social Engineering Techniques

- **Social engineering is a deceptive technique that is difficult to detect due to its heavy reliance on exploiting human behaviours rather than technical vulnerabilities. It encompasses a variety of techniques. Outlined below are the most significant and well-known examples:**
- **Baiting:** A social engineering technique that lures users into traps to steal their personal data and inflict harm on their systems using malicious software. This technique exploits victims› curiosity and greed.
- **Pretexting:** A social engineering technique employed by attackers, it involves a carefully crafted set of lies and rumours designed to deceive the victim into believing they must provide critical and sensitive data to avert an imminent threat, thus paving the way for a fraudulent scheme.

In general, social engineering is a preferred method for cybercriminals as it enables them to gain access to networks, devices, and accounts without the need to undertake complex technical tasks such as breaching firewalls or bypassing antivirus software and other protective technologies.

Prevention of Social Engineering Attacks

To prevent attacks that rely on social engineering, it is essential to adhere to the following tips and procedures:

- **Awareness and Education**

  Raising awareness about digital security and safe browsing practices is a cornerstone of preventing social engineering attacks. It is also crucial that all segments of society understand the concept of social engineering and how it is exploited in phishing scams and other attacks that rely on psychological manipulation. Additionally, there is a need to educate people on how to identify suspicious attempts and remain vigilant in the face of unusual situations, such as messages requesting personal information or passwords.

- **Identity Verification**

  Identity verification is a crucial and effective method to prevent the risks of social engineering attacks. By employing two-factor authentication, we can verify the identity of individuals attempting to access systems or sensitive data. Additionally, it is essential to verify the sources of emails or phone calls, particularly if they contain suspicious requests.

- **Protecting Personal Information**

  It is imperative to minimise the sharing of personal information online or through social media platforms. Attackers may exploit this information to make their attacks more convincing. It is also advisable to avoid disclosing sensitive data in public spaces or via unencrypted channels.

- **The Use of Antivirus Software**

  It is imperative to install and regularly update antivirus software to detect malware that is transferred to user devices through social engineering techniques. Additionally, it is essential to activate firewalls and security systems that prevent unauthorised access to networks.

- **Strict Security Policies**

  To safeguard against the risks of social engineering within organisations, it is imperative to establish clear security policies governing access requests to sensitive information. The principle of least privilege should be strictly enforced, granting employees only the minimum permissions necessary to perform their duties.

- **Caution with Emails**

  Email is one of the most frequently utilised channels in social engineering attacks. It is therefore crucial to remain vigilant when handling unexpected emails or those containing unfamiliar attachments, especially if sent by unknown individuals. Avoid clicking on suspicious links, even if they appear to be from trusted sources, and always verify their authenticity first.

- **Reporting Incidents**

  When individuals or employees encounter a social engineering threat or incident, it is imperative to report the matter immediately so that appropriate measures can be taken. At an individual level, specialised authorities should be informed, while within organisations, established protocols should be followed.

Cyber Threats to Networks

Cybercrimes targeting electronic networks pose a significant threat to both individuals and corporations. The primary objective of these crimes is to steal data or to damage the network in an unauthorised manner. These crimes often rely on the use of malicious software that spreads automatically, causing various types of damage such as theft of personal or financial information, online extortion, or disruption of electronic services.

Primary Objectives of Network Attacks

The unlawful objectives of network attacks include the following:

- The theft of critical data, including personal, financial, and corporate information.
- Financial fraud through the unlawful acquisition of bank accounts and credit cards.
- Cyber espionage targeting governments, institutions, or individuals.
- Extortion and ransomware attacks, involving threats to victims or the encryption of their data in exchange for payment.
- System breaches aimed at disrupting operations or facilitating illicit activities.
- Violations of intellectual property rights, such as software piracy and digital content infringement.
- Disruption of online services provided by institutions and corporations.
- The dissemination of misleading information to manipulate public opinion or deceive individuals.
- The hijacking of smart devices for executing cyberattacks.
- Targeting critical infrastructure, such as power grids and transport networks, to cause disruption.

Types of Network Attacks

Under the umbrella of network attacks, there are several types. The most significant of these are:

1

Denial-of-Service (DoS) attacks

These attacks aim to disrupt electronic services reliant on networks by overwhelming the system with an immense volume of requests, rendering it incapable of responding.

2

Wireless Network Attacks

These are targeted attacks on wireless communication systems, which aim to exploit security vulnerabilities in these systems and breach them.

3

Evil Twin Attacks

These attacks target Wi-Fi networks; the attacker creates a fraudulent page that mimics the original page of the server users are connecting to. They then infiltrate the network and steal sensitive information such as passwords and personal data.

4

Bluetooth Attacks (Bluejacking)

Bluejacking is the act of sending/transmitting unsolicited messages only. Bluesnarfing to access data, bluebugging to access and spy.

Network Attack Protection Methods

To prevent network attacks, the following measures can be taken:

- Installing antivirus software and using firewalls to protect systems.
- Updating operating systems periodically to address security vulnerabilities.
- Raising user awareness about attack methods, such as phishing messages and fake websites.
- Enabling two-factor authentication to enhance the security of account access.

These preventive measures are essential to mitigate the impact of cyberattacks and ensuring the safety of sensitive information and data.

In conclusion, cyber threats are evolving rapidly and continuously, meaning that current effective prevention methods may not be as effective soon, especially as attackers are constantly developing new threat tools. Therefore, there must be a continuous effort to raise awareness of these risks and promote cybersecurity and digital safety concepts. Practically speaking, it is impossible to achieve high indicators of cybersecurity and digital safety without the cooperation of various segments of society, and this cooperation relies primarily on cybersecurity awareness and education.

Activities

Activity 1

Collect data on the number of cybercrimes committed worldwide in 2023 and compare it to the data for 2022. What do you conclude?

Activity 2

Social engineering attacks benefit from the rapid developments in the field of artificial intelligence. Research how cyber attackers exploit artificial intelligence.

Activity 3

The law is concerned with providing protection from cybercrimes, as well as with data privacy. Give examples of this.

Chapter 3
Phishing Attacks

- Introduction
- Mechanism of Phishing Attacks
- Objectives and Impacts of Phishing Attacks
- Types of Phishing
- Indicators of Exposure to Phishing Attacks
- Activities

Introduction

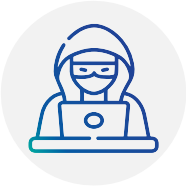
Phishing has become a prevalent cyber threat, as this type of attack requires minimal technical expertise and is relatively inexpensive for attackers compared to other cyberattacks. Additionally, it allows for targeting many victims simultaneously.

In phishing attacks, the internet is exploited to deceive victims into revealing their personal data, such as passwords and credit card numbers. This is achieved through various methods and tools, including the creation of a fraudulent website to lure the victim. The link to this fraudulent site is sent via email or social media messages. These messages contain malicious links, and if a user clicks on these links, their sensitive personal and financial data is hacked through malicious software installed via these links.

Phishing attacks primarily rely on psychological manipulation to coerce victims into acting impulsively. By impersonating a familiar individual or reputable entity, they create a false sense of urgency or desire, exploiting emotions such as fear, anxiety, curiosity, greed, and ambition to achieve their goals. In such instances, users may be inclined to make hasty decisions, often prompted by a message urging them to 'take immediate action.' This deceptive tactic aims to pressure users into acting quickly without sufficient awareness.

International statistics indicate a continuous rise in the number of phishing attacks and the magnitude of resulting losses. This is because deceiving individuals into clicking on malicious links within fraudulent emails is significantly easier compared to other types of cyberattacks. A report by Cisco on cybersecurity threats revealed that phishing is responsible for 90% of data breaches worldwide. Furthermore, a 2022 IBM study linked phishing to 550 cyberattacks, resulting in estimated losses of $4.9 million[8].

8. Global data breach costs reach all-time high of $4.9M, IBM says, on site: https://www.cybersecuritydive.com/news/ibm-data-breach-cost-credentials-phishing/722689/



The Mechanism of Phishing Attacks

Phishing attacks primarily rely on the attacker impersonating someone else via email, social media, or SMS to obtain sensitive information about the victim. To achieve this, the attacker uses open sources to gather personal information about the victim. For instance, the phishing message might include personal details that only close acquaintances would know. The presence of such information in the message leads the user to believe that it is from someone they know, thus prompting them to comply with the attacker›s requests.

This information is gathered by the attacker from a variety of sources, including the personal and professional information that users share on social media platforms. Therefore, the risk of falling victim to phishing can be reduced by minimising the amount of personal data shared on social media platforms.

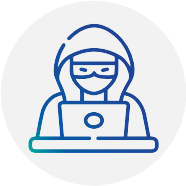
In this type of attack, the victim receives an email that appears to be from a trusted source, such as a friend or a government agency. Once the user clicks on the attached files, which are usually hyperlinks directing them to a malicious website, the attack commences. Malicious software is installed on their device, or they are redirected to fraudulent websites, initiating the process of stealing sensitive information, including passwords and credit card numbers.

Objectives and Impacts of Phishing Attacks

Phishing attacks are designed to achieve several objectives for attackers. The most prominent of these are:

- **Theft of sensitive data, such as bank account information and passwords, to use in fraudulent operations.**
- **Exploiting stolen data in other attacks, such as ransomware attacks or advanced cybersecurity breaches.**
- **Installation of malicious software on the targeted users' devices, allowing attackers to spy on or take control of the system.**
- **Breaching the systems of targeted organisations, using stolen login data, as an initial step to carry out sabotage attacks or steal information.**
- **Deceiving the victim into accessing fake websites that mimic the original ones, to steal login credentials or other sensitive information.**

Regarding the consequences of phishing attacks, at the organisational level, such attacks can disrupt internal systems, leading to significant financial losses and damaging the organisation›s reputation due to the compromise of customer data. This places organisations at odds with regulatory frameworks designed to protect data within countries. At the individual level, attacks can result in identity theft or the misuse of personal information for other crimes, leading to long-term damage such as reputational harm or financial loss.



Types of Phishing

Phishing attacks can take various forms. Below is an explanation of some of the most common types:

Spear Phishing

This type of phishing is targeted at a specific individual within an organisation, with the aim of stealing their login credentials. The attacker gathers personal information about the target beforehand, such as their name, position, and contact details. This type of attack can be used for identity theft, financial fraud, manipulation of the organisation›s financial data, espionage, or the theft of confidential data for resale to competitors. In general, individuals with access to important data, such as CEOs, are targeted.

It is important to note that spear phishing is a type of phishing attack, but differs from it in several ways. Most notably, spear phishing targets a specific individual, whereas phishing attacks are broad-based, aiming to steal sensitive data from users in general without personalisation[9].

9. What is spear phishing? Proofpoint, available at: https://www.proofpoint.com/de/threat-reference/spear-phishing.

Vishing

This type of phishing relies on phone calls or voice messages, aiming to defraud targets and steal their personal and financial data. This method heavily depends on social engineering, a modern technique that exploits basic human instincts such as trust or fear. Attackers manipulate these emotions to influence victims into making decisions that benefit the attacker, such as revealing sensitive information or transferring money[10].

Often, the attacker will pose as someone known to the victim or as an official from an organisation with which the victim generally interacts, to deceive them into providing sensitive information to facilitate the remainder of the fraudulent scheme. Vishing can be carried out by exploiting the victim›s personal desire for financial gain, such as enticing them with incredibly cheap deals or advertising a fictitious competition with a large monetary reward.

Email Phishing

This is one of the most common types of phishing attacks. In this type of attack, the perpetrator relies on email to send a phishing message, crafting it to appear as if it is from a trusted source. The aim is to infiltrate the device to steal sensitive and financial data or to steal the user›s identity.

Generally, there are several signs or indicators that distinguish phishing emails:

- **Unusual writing style:**
  For example, if a user receives a message from someone they know, they may notice a difference in the writing style. This is a primary indication that the message could be a phishing attempt.

10. What is voice phishing? Kaspersky, available at the following link:
https://me.kaspersky.com/resource-center/definitions/vishing

- **Grammatical and spelling errors**

  Grammatical and spelling errors are characteristic of fraudulent messages, especially those claiming to be from official organisations. These organisations are usually meticulous about proofreading their messages before sending them to users.

- **Discrepancies in Email Addresses and Links**

  A discrepancy between the email address and the links is a strong indicator of a fraudulent message. Users should always verify the email address received from the organization against the authentic one found on its official website.

- **Creating a Sense of Urgency and Fear**

  Phishing emails often manipulate recipients by inducing fear or anxiety about their financial transactions or personal information. They may demand sensitive data, so it's essential to remain vigilant, exercise caution, and avoid rushing to provide any personal information online.

- **Suspicious Attachments**

  If an email contains attachments, the file extension can be a red flag. Uncommon file types like .scr, .exe, or .zip may indicate a malicious attempt. Before opening any attachment, it's crucial to scan it with antivirus software[11].

- **Requests to Download Software or Click Links**

  Legitimate companies rarely ask users to download specific software or click on unfamiliar links. If an email requests such actions, it›s likely a phishing attempt. Users should avoid complying with these requests.

11. 10 Most Common Signs of a Phishing Email. On site: https://www.titanhq.com/blog/10-tell-tale-signs-that-spam-email-is-a-phishing-scam/.

HTTPS Phishing Attacks

In this type of phishing attack, the assault is executed via HTTPS; a malicious email is sent to the target user, containing a link to a counterfeit website. The aim is to deceive the victim into submitting their personal information. HTTPS phishing sites are the preferred choice for attackers as they can convince victims that they are dealing with a trustworthy source. This kind of phishing attack is often described as low-risk and high-reward.

It›s worth noting that a staggering 91% of cyberattacks originate from phishing emails sent to users. These emails lure victims to malicious websites through links disguised as legitimate sources, such as well-known companies or individuals. A prime example of this type of fraudulent attack is the 2014 Sony Pictures hack, where attackers gained access to the company›s systems by sending spoofed emails. Employees fell victim to these fraudulent links, enabling the attackers to steal passwords and critical data[12].

Pharming

Pharming, a term blending ‹phishing› and ‹farming›, is a particularly common type of cyberattack targeting financial institutions and banks. In this type of attack, a fraudulent website is created, and unsuspecting users are redirected to it to steal sensitive information. These counterfeit websites are designed to collect personal details such as passwords, bank account numbers, and other confidential data, or to install malicious software onto victims› computers.

12. HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust. On site: https://www.keyfactor.com/blog/https-phishing-attacks-how-hackers-use-ssl-certificates-to-feign-trust/.

Pop-up Phishing

Pop-up phishing messages are those that appear to users while they are browsing the internet, resulting from attackers exploiting websites infected with malicious software. These messages appear in the form of warnings about threats to the device, which alarms the user and suggests that their device is at risk. Often, these messages ask users to download «antivirus» software to fix the problem, but in reality, these programs are malicious and aim to hack users› devices and steal their data or defraud them.

Clone Phishing

It is a type of phishing attacks where the attacker duplicates an authentic email previously sent from a trusted source to the victim. The original email is ‹cloned› and then resent to the victim with slight modifications, such as replacing original links with malicious ones or inserting malicious attachments.

The danger lies in the fact that the cloned email appears familiar and trustworthy to the victim, as it is a copy of one they have already received[13]. This significantly increases the likelihood of the victim clicking on links or opening attachments without caution. This technique is often used to exploit the trust between the sender and the victim to achieve goals such as stealing personal information or installing malware on the victim's device.

13. Clone phishing: What it is and how to prevent it. NORTON. On site: https://us.norton.com/blog/online-scams/clone-phishing

The aim of this type of phishing attack is to steal sensitive information such as account details or passwords, as well as to install malicious software that allows the attacker to hack into systems or infiltrate the victim's data. This attack is carried out in several steps:

- **Duplicating the original email:** An exact copy of an email previously sent from a trusted source is made.
- **Modifying links or attachments:** The attacker alters the links or attachments to direct the user to malicious websites or malware.
- **Resending the email:** The email is sent to the victim, who may trust the email as it appears familiar.

Indicators of Exposure to Phishing Attacks

There are several indicators that users may be experiencing a phishing attack. The most important of these are as follows:

1

Receiving Unexpected Login Attempt Notifications

Users may receive email notifications indicating that someone has tried to log into their accounts. If the user did not initiate these login attempts, it could suggest that an unauthorised person is trying to gain access to their accounts.

2

Unusual Device Slowdown and Overheating

If a computer or mobile device becomes noticeably slower and overheats without apparent reason, it may be due to malicious software running in the background and consuming the device›s resources.

3

Annoying Pop-up Windows

The sudden appearance of pop-up windows claiming that your device is infected with viruses is a sign of malware, or the presence of adware attempting to trick users into downloading malicious software. These pop-ups may also be part of a phishing scam.

4

Automatic Opening and Closing of Browsers and Applications

If browser windows or applications are opening and closing on their own without user interaction, this could indicate that the device has been compromised and that there is malicious software controlling the system.

5

Sending Unusual Messages to Friends

If friends or colleagues report receiving unusual or suspicious messages from you, it may indicate that your email account or social media platforms have been compromised and are being used to send unauthorised messages.

6

Receiving Unsolicited Emails

An increase in the number of spam or junk emails in your inbox could indicate that your email information has been compromised. This means you may have been a victim of phishing or a malware attack, such as spyware.

To prevent phishing attacks, it is essential to follow these guidelines:

- Use antivirus software and keep it updated regularly.
- Enable two-factor authentication to add an extra layer of security and to better protect the data.
- Avoid clicking on suspicious links or downloading untrusted files from the internet.
- Change your passwords periodically and use strong, complex passwords.

In conclusion, phishing attacks are the most common type of cyberattack, and the number of victims is rapidly increasing. The resulting financial and social losses are also on the rise. The best solution to address and prevent these attacks is to follow safe internet browsing practices. Prevention of these risks is more effective than intervention after an attack, a fundamental principle of cybersecurity and digital safety. A proactive approach to cybersecurity risks is far more effective than a reactive one.

Activities

Activity 1

List in a table the main types of phishing attacks, outlining the mechanism of each type and the methods of prevention.

Activity 2

Recent trends in phishing attacks increasingly rely on artificial intelligence, research how to prevent phishing attacks that rely on artificial intelligence.

Activity 3

Search on the internet for international models of phishing cases, and identify the mistakes that users made until they fell victim to fraud.

Chapter 4
Cyber Risks in the Workplace

- Introduction
- Cyber Risks in the Workplace: Their Nature and Types
- Impact of Cyber Risks on the Workplace
- Remote Work and Cyber Risks
- Strategies for Mitigating Cyber Risks in Remote Work Environments
- Challenges in Cybersecurity Risk Management in the Light of Emerging Technologies
- Activities

Introduction

With the growing reliance on technology and digital communication in this era, public and private companies' dependence on cloud services and network data transfer and the spread of remote working, work environments encounter continuous cyber threats that involve economic entities represented in companies and their staff. This threatens the stability of the work environment including management and employees, in addition to the stability of the state economy.

This reality necessitates an increasing focus on cybersecurity within workplaces, promoting a culture of digital safety and transforming it into a prevailing organisational culture among employees at all administrative levels. Cybersecurity for companies is not solely the responsibility of cybersecurity and information technology specialists, but extends to non-specialist employees, especially since many cyberattacks targeting companies may originate from a breach by an employee, allowing the breach to spread to the entire company.

Cyberattacks have become increasingly sophisticated and organised over time, leading to a surge in demand for advanced protective solutions and measures. Moreover, cyber risks not only threaten business continuity but also result in significant financial losses, reputational damage, and legal challenges.

Cyber Risks in the Workplace: Their Nature and Types

Cybersecurity risks in the workplace refer to threats targeting digital systems and sensitive data within companies and institutions.

These risks include attempts to breach systems, data theft, and the dissemination of malicious software, all of which may result in operational disruption or significant financial losses.

With technological advancements, such threats have become increasingly advanced, particularly with the widespread use of the internet, email, and cloud storage. Therefore, organisations must implement robust security measures, such as regularly updating systems, using strong passwords, and raising awareness about phishing attacks, to safeguard their data against cyber threats.

Cyber risks in workplace environments are varied and encompass multiple levels of threats targeting devices, networks, and data. These threats can be categorised into the following groups:

1 Insider Threats

Insider attacks occur when a current or former employee exploits their privileges to access company data or disrupt its operations. Such incidents may arise due to a lack of awareness of cybersecurity protocols or a deliberate attempt to gain unlawful benefits. The severity of these attacks lies in the attackers' familiarity with the internal system, enabling them to effectively exploit vulnerabilities[14].

14.Defining Insider Threats, CISA, on site: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

2 Advanced Persistent Threats (APTs)

These are long-term, organised attacks aimed at stealing sensitive data or espionage on systems, carried out by groups with highly advanced technical skills. These attacks primarily target banks, governments, and companies associated with critical infrastructures[15].

3 Cloud Security Breaches

With businesses increasingly relying on cloud computing, safeguarding stored data has become a significant challenge, particularly if it is not adequately secured, as this may lead to data theft. Moreover, attacks on cloud service providers can result in the exposure of sensitive information belonging to multiple clients simultaneously[16].

4 Dumpster Diving

This refers to traditional cyber threats where attackers seek sensitive company or individual information by searching through waste or rubbish. This includes paper documents that have been disposed of insecurely, such as:

- **Passwords written on paper.**
- **Drafts of agreements or contracts.**
- **Banking or financial data.**
- **Sensitive information about employees or customers.**
- **Notes containing system login details**

15. What are advanced persistent threats? IBM, on site: https://www.ibm.com/think/topics/advanced-persistent-threats
16. Cloud Security Issues and Challenges, Kaspersky, available at the following link: https://me.kaspersky.com/resource-center/preemptive-safety/cloud-security-issues-challenges

Attackers exploit the fact that many companies or individuals dispose of documents or electronic devices (such as hard drives or old phones) without taking adequate precautions, such as complete destruction. Attackers collect this information and exploit it in more sophisticated attacks, such as social engineering or identity theft[17].

How to Protect Against Cybersecurity Risks in the Workplace

With the increasing reliance on technology for task execution, cybersecurity has become essential for safeguarding critical information in workplace environments. To mitigate risks, there are general guidelines that can help enhance security, including:

- **Employee Awareness**
  Conduct regular training sessions to educate employees on data protection practices, such as avoiding suspicious links and messages.
- **Continuous Monitoring**
  Utilise tools to detect any unusual activity within the company's systems.
- **Access Restriction**
  Grant employees limited access rights based on their roles and prevent unnecessary access to sensitive data.
- **Software and Hardware Updates** Ensure the installation of the latest security updates to prevent the exploitation of vulnerabilities.
- **Secure Data Disposal** Shred sensitive documents and erase data from old devices before disposal.

17. Ramonas , Lukas. What is a dumpster diving attack? Nordvpn, may 2023, on site: https://nordvpn.com/blog/dumpster-diving-attack/

Protecting the Workplace from Various Risks

Protection Against Insider Threats

- Ensure that employees are not granted unnecessary access privileges.
- Monitor any unusual behaviour that may indicate attempts at data breaches or unauthorised access.

Protection Against Advanced Persistent Threats (APT)

- Utilise advanced security software to detect any network intrusion attempts.
- Segment the network into smaller sections to prevent attackers from easily accessing all systems.

Protection Against Cloud Breaches

- Select reputable service providers that implement high security standards.
- Enable two-factor authentication for login to safeguard accounts from theft.

Protection Against Dumpster Diving

- Shred sensitive documents before disposal.
- Permanently delete all data from electronic devices before selling or discarding them.

By implementing these measures, organisations can protect their data and reduce the risk of cyberattacks, ensuring a secure and reliable workplace environment.

Impact of Cyber Risks on the Workplace

Cyber threats can have a severe impact on organisations in numerous ways. Below is an explanation of the most significant ones.

1 Financial Losses

Financial losses are among the most severe consequences of cyberattacks. These costs can arise from several factors, such as:

- **Repairing Damage:** Following an attack, companies must repair their systems and recover damaged data.
- **Paying Ransom:** In the case of ransomware attacks, companies may be forced to pay substantial sums to recover their data.
- **Loss of Revenue:** If attacks disrupt operations for an extended period, revenues may be significantly impacted.

2 Impact on Reputation

When a company experiences a cyberattack that result in customers› data breach, its reputation can be irreparably damaged. The loss of customer and partner trust can lead to customer attrition and lost future business opportunities. For example, Sony Pictures Entertainment suffered a major cyberattack in November 2014 attributed to a group known as the «Guardians of Peace». The attack resulted in the leak of large amounts of sensitive data, including emails and personal information of employees[18].

3 Legal and Regulatory Implications

Many countries impose strict regulations on the protection of personal data, such as the General Data Protection Regulation (GDPR) in the European Union. This is because any data breach can result in legal penalties and financial fines[19].

18. Cieply, Michael and Brooks Barnes, Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm,The New York Times, december 2014 , on site: https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html

19. What-is-gdpr? , Gdpr, on site: https://gdpr.eu/what-is-gdpr/

Remote Work and Cyber Risks

With many companies adopting remote work policies, cybersecurity risks associated with this work model have become more prevalent. Some of the most significant challenges facing organisations include:

1 Insecure Data Access

Employees working remotely depend on personal internet networks, which are generally less secure than corporate networks safeguarded by firewalls and intrusion detection systems. The use of unsecured Wi-Fi networks further increases the risk of company data being compromised.

Furthermore, the use of personal devices for work poses a significant risk to data security and system integrity. Personal devices are often less secure than company-provided devices, lacking adequate security software and may not receive regular updates, making them vulnerable to cyberattacks that could lead to the leakage of sensitive data or the compromise of work systems.

Furthermore, transferring sensitive files to personal devices

increases the risk of data breaches, particularly if they are stored or shared through insecure means. For this reason, employees should adhere to storing files on internal company servers and using only authorised systems. Additionally, using public or home internet networks for work exposes data to the risk of espionage or interception. Therefore, it is advisable to rely on the internal company network, which offers high levels of security. Companies can also enable Virtual Private Network (VPN) services to ensure secure remote access for employees, allowing them to access files and systems securely without compromising data confidentiality.

2 Unsecured Personal Devices

While working remotely, employees may rely on personal devices that lack an adequate level of security, such as the absence of recent updates or antivirus software, making them vulnerable to attacks and malware. Additionally, the use of these devices by family members may increase the likelihood of exposure to cybersecurity risks.

3 Identity and Access Management (IAM)

One of the biggest challenges companies face when working remotely is ensuring that access to data is secure. Identity and Access Management (IAM) is crucial to guarantee that individuals accessing systems have only the necessary permissions[20]. The use of weak passwords or the failure to enable two-factor authentication (2FA) exposes systems to the risk of being hacked.

20. What IAM is and what it does, Microsoft, on site: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam

4 Cloud Application Usage

With the increasing reliance on cloud applications for remote work, securing them has become an urgent necessity to avoid cyber risks. Therefore, companies must adopt robust security measures, such as encryption, multi-factor authentication, and monitoring of suspicious activities.

Since any security vulnerability may lead to data breaches or unauthorised access, thereby threatening business operations. Therefore, it is recommended to collaborate with service providers to implement international security standards and ensure data protection and business continuity[21].

5 Increased Exposure to Social Engineering Attacks

Given the physical separation of employees in remote work environments from their colleagues and supervisors, they may face difficulties in verifying the authenticity of emails or phone calls they receive.

This geographical distance increases the likelihood of falling victim to sophisticated fraudulent techniques, such as phishing as it becomes challenging for them to ascertain whether a message or call is genuine or fabricated. In the absence of direct interaction, it becomes easier for attackers to manipulate employees, enticing them to click on malicious links or disclose sensitive information, thereby heightening their exposure to social engineering attacks.

21. Coachable Moments: Insider Risks, Cloud Storage and Remote Work Security, proofpoint, on site: https://www.proofpoint.com/us/blog/information-protection/coachable-moments-insider-risks-cloud-storage-and-remote-work-security

Strategies for Mitigating Cyber Risks in Remote Work Environments

To reduce cyber risks in a remote work environment, companies must adopt multifaceted strategies, including the following:

1

Training and Awareness

Companies must organise regular training programs to educate employees about cyber threats and best practices to avoid them. They should also raise awareness about digital safety in the workplace, how to report incidents, and other cybersecurity and digital safety fundamentals.

2

Protecting Sensitive and Critical Data

Managing access rights through granting employees limited permissions and utilising multi-factor authentication (MFA) is essential. To safeguard sensitive data within the workplace, it must be classified according to its sensitivity level and encrypted during both transmission and storage. Additionally, it is imperative to ensure the secure deletion of unnecessary data through specialised software or the physical destruction of storage media.

Encrypted backups, continuous monitoring through intrusion detection and prevention systems (IDS/IPS), and cybersecurity training for employees are effective tools for data protection.

In cloud environments, it is essential to choose secure cloud service providers who rely on encryption and strict access management policies.

Compliance with regulations such as the General Data Protection Regulation (GDPR) is fundamental, and it is advisable to conduct regular security audits to ensure the effectiveness of security policies.

3

Use of Virtual Private Networks (VPNs)

Companies should ensure that all remote workers use secure VPNs. These networks encrypt the connection between the device and the company›s internal network, making it difficult for attackers to intercept data[22].

To control access to sensitive data and systems, an Identity and Access Management (IAM) system can be employed, which relies on role-based permissions to ensure that employees can only access the information they require to perform their duties. Additionally, two-factor authentication (2FA) can be enabled to enhance security and prevent unauthorised access.

22. What is a VPN? Microsoft, on site: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-a-vpn

4

Data Encryption

Data encryption is one of the best methods for protecting data, whether it is stored on employee devices or being transmitted across a network. Therefore, all sensitive data should be encrypted; this means that even if attackers can access it, they will not be able to read it. Implementing advanced encryption at the operating system and application levels is a critical step in ensuring information security.

5

Implementing Mobile Device Management (MDM) Solutions

During remote work, employees often use mobile devices to access company systems. To secure these devices, Mobile Device Management (MDM) solutions can be used. These solutions allow companies to control devices, enforce restrictions, and track them in case of loss or theft[23].

6

Continuous Security Monitoring and Analysis

Companies must continuously monitor all systems and infrastructure to identify any suspicious activity or potential breaches. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can be used to monitor and analyse network traffic to detect any unusual behaviour.

23.What is mobile device management (MDM)? , IBM, on site: https://www.ibm.com/topics/mobile-device-management.

7

Strict Policies for the Usage of Cloud Applications

Companies using cloud computing must set strict policies for the usage of cloud applications where the used apps are secured and support safety criteria such as data encryption, IAM, and authentication.

8

Regular Updates and System Maintenance

It is necessary to regularly update all the systems and applications to guarantee having the recent security correction. This is because cyberattacks usually exploit the bugs found in the old versions. Thus, regular updates of devices and software are an important action to achieve protection from these threats.

9

Meeting Management and Security

Meeting management and security are vital in enhancing cybersecurity in remote work. With the growing reliance on virtual tools like Zoom and Microsoft Teams, it is necessary to pursue strict security practices to make sure that meetings are conducted in a safe environment. Meetings should

also be protected with strong passwords and by enabling security features like waiting rooms, which allow organisers to control who is permitted to join. Additionally, it is crucial to use end-to-end encryption for conversations to ensure that data exchanged during meetings, whether files or chats, remains encrypted and inaccessible to hackers or unauthorised third parties. To maintain meeting security, there are several practical guidelines, including:

- **Use Strong passwords:** To ensure meeting privacy and restrict access to only invited participants.
- **Enable two-factor authentication (2FA):** To verify the identity of participants and ensure access is granted only to authorised individuals.
- **Lock the meeting after it starts:** To prevent any attempts to join the meeting once it has begun.

In addition, utilising a Virtual Desktop Infrastructure (VDI) is an effective solution for providing a secure and isolated work environment. This system allows employees to access company resources through a virtual desktop that is fully managed by the company, thereby limiting the exposure of sensitive data to any malicious software that may be present on employees› personal devices. The following is an explanation of the benefits of an isolated desktop:

- **Malware Protection:** Ensures that installed software is protected and centrally managed without user intervention.
- **Separation of Work Environment from Personal Devices:** Reduces the risk of data leakage or unauthorised use outside the framework of security policies.
- **Centralised Update Management:**Guarantees that the latest security patches are applied to all users without delay.

10

Identity and Access Management (IAM)

Identity and Access Management (IAM) is a fundamental pillar of cybersecurity, especially in light of the significant shift towards remote work. IAM is concerned with managing and identifying the individuals who are authorised to access an organisation's resources and systems, ensuring that these individuals have only the necessary permissions to perform their tasks. IAM systems help control user identities, define their permissions, and enhance the company's ability to monitor activities and prevent breaches. IAM encompasses fundamental principles including:

- **Principle of Least Privilege**

  One of the best practices in Identity and Access Management (IAM) is to apply the principle of least privilege. This means that each user should only have the necessary permissions to perform their job duties. By minimising unnecessary privileges, the risk of unauthorised access or misuse is significantly reduced. For example, an accounting employee does not require access to marketing or software development databases.

  Multi-Factor Authentication (MFA)

  Multi-factor authentication (MFA) is a cornerstone of enhanced security within identity and access management (IAM). MFA relies on using more than one method to verify a user's identity, such as something the user knows (a password) and something the user possesses (a mobile phone to receive a verification code). MFA is one of the best ways to prevent phishing attacks and brute-force password attacks. Even if a password is compromised, the additional verification step thwarts any unauthorised access attempts.

- **Continuous Monitoring and Auditing**

  A primary responsibility of identity and access management is to monitor and record all activities related to system access. Access logs must be continuously monitored and analysed to detect any suspicious activities or unauthorised access attempts. For instance, users attempting to access resources they are not authorised to use or those trying to access systems outside of normal working hours can be identified.

  Continuous auditing enables organisations to review access systems and verify employee adherence to established policies. Periodic tests can be conducted to review permissions and ensure that employees do not have more privileges than necessary.

- **Automated Identity Management**

  Given the increasing complexity of systems and the growing number of remote workers, automated identity management has become crucial. Automated systems can streamline the processes of granting and revoking permissions efficiently and quickly, ensuring that the right resources are provided to the right individuals without delay. For instance, when a new employee is hired, an automated system can rapidly create a new account and grant the employee the appropriate permissions based on their role. Similarly, upon the termination of an employee's contract or their transition to a new position, the system can automatically revoke or modify their permissions, thereby mitigating the risk of former users retaining unnecessary privileges.

- **Role-Based Access Control (RBAC)**

  Role-Based Access Control (RBAC) is an effective IAM method that grants permissions based on a user's job role rather than assigning individual permissions. In other words, permissions are assigned to a specific set of roles that employees hold, and anyone who holds that role automatically receives the same permissions.

  RBAC also enables organisations to reduce the complexities of access management and ensure a fair and organised distribution of privileges. For instance, all employees in the finance department receive specific permissions, while the IT department has different privileges.

- **Cloud Identity and Access Management (Cloud IAM)**

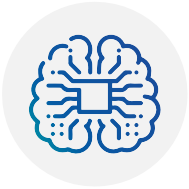
  As reliance on cloud computing grows, cloud identity and access management have become a fundamental part of security strategy. It facilitates control over access to cloud resources and manages permissions across multiple cloud platforms.

  Cloud IAM solutions offer features such as:

  * **Unified Access Management:** Companies can use a single platform to manage permissions across multiple cloud services.
  * **Integration with Authentication Services:** Such as Google Cloud Identity or Azure Active Directory to provide unified authentication and centralised user management.
  * **Reporting and Analytics:** For monitoring and managing access logs to cloud resources.

- **Mitigating Identity Theft Attacks**

Identity and Access Management (IAM) plays a crucial role in safeguarding organisations from identity theft attacks. Identity theft is a common hacking technique where attackers attempt to exploit an employee's credentials to gain unauthorised access to sensitive systems. By implementing IAM, stringent policies can be enforced, such as monitoring for unusual user behaviour and ensuring all access adheres to security policies.



Challenges in Cybersecurity Risk Management in the Light of Emerging Technologies

As technology rapidly evolves and reliance on artificial intelligence and the Internet of Things (IoT) in work environments increases, cyber threats are becoming increasingly sophisticated. The future is likely to see a rise in complex attacks that leverage artificial intelligence and the use of robotics. This places new demands on organisations, requiring them to find innovative ways to enhance cybersecurity.

1 Cybersecurity and the Internet of Things (IoT)

Internet-connected devices have become an integral part of many companies, adding a new layer of complexity to risk management. Each connected device represents a potential entry point that can be exploited by attackers. Cybersecurity managers must therefore ensure that all these devices are adequately secured and continuously monitored..

2 Artificial Intelligence and Advanced Attacks

While artificial intelligence (AI) technologies offer immense opportunities to enhance cybersecurity, they also provide powerful tools for hackers. AI can be used to automate attacks and rapidly analyse data to discover security vulnerabilities. To keep pace with these developments, organisations need to develop defensive technologies that rely on AI and machine learning to proactively detect threats.

3 Data Management in Hybrid Work Environments

As organisations continue to navigate the hybrid work model, effectively and securely managing data becomes paramount. Companies must implement strategies that enable employees to seamlessly transition between on-site and remote work without compromising security. One effective solution is adopting virtual desktop infrastructure (VDI), which allows employees to access their personalised work environments from anywhere, mitigating risks associated with local data storage on personal devices.

As technology advances and cyber threats become more sophisticated, it is imperative for companies to implement comprehensive preventive measures to safeguard both traditional and remote work environments. Remote work poses additional challenges, necessitating the development of multi-faceted security strategies that encompass data, device, and communication protection.

Companies that neglect cyber risks find themselves vulnerable to significant financial losses, loss of customer trust, and legal consequences. Therefore, cybersecurity cannot be treated as an option but is an essential component of the continuity and success of any organisation in the digital age.

Cybersecurity is not a one-time task; it is an ongoing process that requires continuous monitoring and improvement to address ever-evolving threats.

In conclusion to this chapter, it is essential to emphasise that cyber risks in the workplace are not static but rather dynamic and evolving in line with cyber developments. Therefore, it is imperative to continuously enhance employees› awareness of cybersecurity concepts and digital safety. Overall organisational management, and specifically cybersecurity and information technology management, cannot alone ensure the stability of the work environment.

Therefore, cooperation among all employees, both specialists and non-specialists, at all administrative levels is essential. A single technical or knowledge gap can have a significant impact on the entire organisation, thus highlighting the importance of cybersecurity and digital safety indicators in both traditional and remote work environments.

Activities

Activity 1

Search for examples of cyberattacks that have targeted various organisations and explain the underlying causes of these breaches.

Activity 2

Create a table highlighting the differences between the cyber threats faced by remote work systems and traditional work systems.

Activity 3

The responsibility for enhancing digital security within organisations lies with all employees, regardless of their administrative level. Compose a research paper discussing the integration of roles between cybersecurity and IT specialists and non-specialist staff within organisations.

Chapter 5:
The General Data Protection Regulation (GDPR)

- Introduction
- General Data Protection Regulation (GDPR)
- Core Principles of the GDPR
- GDPR Penalties
- Consent Requirements Under the GDPR
- The Role of the GDPR in Enhancing Digital Security
- Activities

Introduction

Data protection laws play a crucial role in safeguarding individual privacy and fostering trust in institutions. By guaranteeing individuals› rights to control their personal information, these laws contribute to a secure operating environment. Moreover, they define the responsibilities and obligations of institutions, facilitating compliance.

These laws also enhance digital security by providing measures to protect data from breaches. Moreover, they contribute to economic development and innovation by offering a clear and reliable legal framework. Therefore, most countries are keen to develop their own data protection laws, in addition to the existence of international regulations and protocols that focus on data security.

Given the significance of these regulations, this chapter will be dedicated to studying and analysing them, and to identifying their role in protecting data at both the individual and institutional levels.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is one of the most significant pieces of legislation on personal data protection worldwide. Adopted by the European Union in April 2016, it came into effect on 25 May 2018. The GDPR aims to strengthen the protection of individuals› personal data within the European Union and to provide a unified legal framework for privacy protection.

GDPR Goals

GDPR aims to achieve the following goals:

1 Personal Data Protection

- **Primary Objective:** The GDPR aims to protect the personal information of individuals, such as their name, address, phone number, email address, and financial information.
- **Emphasis on Privacy:** The law aims to ensure that personal data remains confidential and is not used in ways that infringe on individuals› rights.

2 Promoting Transparency

- **Data Disclosure:** Companies are required to inform individuals about how their data is collected, the purposes for which it is used, and the parties with whom it may be shared.
- **Clear Information:** The information provided must be easy to understand, enabling individuals to make informed decisions about their data.

3 Empowering Individuals

- **Individuals' Rights:** The GDPR grants individuals a range of rights, including the right to know how their data is being used and the right to have it retrieved, empowering them to have control over their personal data.
- **Active participation:** Empowers individuals to make decisions about how their information is used, increasing their sense of security and trust.

4 Unification of Laws in the European Union

- **A Unified Legal Framework:** The GDPR aims to unify data protection legislation across all EU member states, making it easier for companies to comply with various laws.
- **Reduction of Complexity:** It helps to reduce the administrative and organisational complexity that companies may face when operating in multiple countries.

5 Enhancing Security

- **Security Requirements:** The GDPR emphasises the need for robust security measures to protect personal data from unauthorised access, breaches, and cyberattacks.
- **Regular Assessment:** Companies must conduct regular assessments of data risks and adhere to best practices in information protection.

6 Data Minimisation

- **Collecting Only Necessary Data:** The GDPR emphasises the importance of collecting only the data that is strictly necessary to fulfil the stated purposes. This reduces the amount of data stored and the associated risks.
- **Reducing Storage:** Limits the retention of data for extended periods, thereby minimising individuals› exposure to the risk of data breaches.

7 Providing Additional Individual Rights

- **Right of Access:** Individuals have the right to know whether their data is being processed and to be informed about the nature of that data.
- **Right to Rectification:** Individuals can request the correction of any inaccurate information.
- **Right to Erasure:** They can request the deletion of their personal data in certain circumstances.
- **Right to Data Portability:** Individuals are entitled to transfer their data to an alternative service provider if they desire to do so.
- **Right to Object:** They can object to the processing of their personal data for specific purposes, such as direct marketing.

8 Developing a Compliance Culture

- **Enhancing Adherence to Laws:** The GDPR aims to foster a culture of compliance within organisations by providing a clear framework.
- **Training and Awareness:** Companies are required to provide training to their employees on the importance of data protection and individual rights, which contributes to enhancing the level of awareness among employees.

9 Increasing Trust between Individuals and Companies

- **Building Trust:** By protecting personal data and promoting transparency, the GDPR contributes to building trust between individuals and companies.
- **Enhancing Relationships:** This trust strengthens the relationships between consumers and companies, leading to a better user experience.

10 Adapting to the Evolving Digital Environment

- **Responding to Technological Advancements:** The GDPR aims to keep pace with the rapid developments in information technology and data protection, ensuring the protection of individuals in an increasingly complex digital world.
- **Flexibility:** Enables departments to adapt to changes in how personal data is processed.

Core Principles of the GDPR

GDPR includes a set of main principles that all institutions have to adhere to:

1 Legitimacy and transparency

- **Lawful Processing:** Personal data must be processed lawfully and fairly.
- **Disclosure:** Organisations must provide clear information to individuals about how their data is processed, including the purposes and means used.

2 Limiting Data Collection

- **Specific Data Collection:** Personal data must be collected for specified, legitimate purposes and may not be further processed in a manner incompatible with those purposes. **Purpose Specification:** The purposes for which personal data is collected must be clearly stated to individuals.

3 Data Minimisation

- **Appropriate Processing:** Personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Data Minimisation:** The collection of personal data should be limited to what is necessary for fulfilling the specified purpose.

4 Accuracy

- **Data Updates:** Data must be accurate and up to date. Organisations should take the necessary steps to correct any inaccurate information without delay.
- **Responsibility for Accuracy:** Organisations are responsible for maintaining data accuracy.

4 Data Retention

- **Retention Period:** Personal data should not be retained for longer than is necessary for the purpose for which it was collected. The longer the retention period, the greater the risk to which the data is exposed.
- **Limiting the Period:** Organisations must set a certain period for holding data based on the purpose of data processing. In other words, organisations must determine in advance how long they will retain data.

5 Security

- **Data Security:** Appropriate technical and organisational measures must be implemented to ensure the protection of personal data from unauthorised processing or loss.
- **Breach Notification:** Organisations must report any suspected data breaches on time, in accordance with applicable laws.

6 Responsibility

- **Compliance:** Organisations must be able to demonstrate their adherence to GDPR principles, which requires having internal procedures and thorough documentation.
- **Risk Assessment:** Organisations must conduct regular assessments of data risks and take necessary steps to mitigate these risks.

GDPR Penalties

The GDPR imposes strict penalties on organisations that violate its rules. These penalties are designed to enhance compliance and encourage respect for individuals› rights.

Types of Penalties

The penalties imposed under the GDPR fall into two main categories:

1

Financial Penalties

- May reach up to 20 million euros or 4% of the annual global turnover, whichever is greater[24].
- Penalties are imposed based on the severity of the violation, its impact on individuals, and the extent of the organization's cooperation with authorities.

2

Corrective Actions

Authorities may impose corrective actions, such as:

- Halting data processing: If there is any risk to the data.
- Requiring organizations to correct or delete data.
- Taking other measures to enhance compliance.

24. What are the GDPR Fines? on site: https://gdpr.eu/fines/.

Criteria for Determining Penalties

Authorities consider several factors when determining penalties, including:

1

Nature of the violation

The severity of the violation and its impact on individual rights.

2

Past compliance

Whether the organisation has committed previous violations.

3

Cooperation with authorities

The extent to which the organisation has cooperated with authorities during the investigation.

4

Remedial measures

Whether the organisation has taken steps to prevent future violations.

Reporting Breaches

Organisations must report any data breaches within 72 hours of becoming aware of an incident if there is a risk to individuals› rights. If the breach is serious, the affected individuals must also be notified.

Examples of Penalties

- Data protection regulators under the General Data Protection Regulation (GDPR) have imposed hundreds of fines on companies, including Google and Facebook, totalling over 114 million euros in the first 20 months of 2020[25].
- On 17 January 2020, the Italian supervisory authority announced that it had imposed two separate fines of €8.5 million and €3 million on Eni Gas e Luce (EGL), an Italian electricity and gas supply company. These fines were imposed in response to two separate violations of the General Data Protection Regulation (GDPR)[26].

25. How the GDPR could change in 2020, on site: https://gdpr.eu/gdpr-in-2020/

26. Italy fines Eni Gas e Luce €11.5 million for multiple GDPR violations, on site: https://gdpr.eu/italy-fines-energy-company-for-multiple-gdpr-violations/

Consent Requirements Under the General Data Protection Regulation (GDPR)

The GDPR imposes several fundamental requirements on consent to ensure that it is valid and enforceable. Key elements include:

1 Clarity

- **Clear Information:** The information provided to individuals about the treatment should be clear and easy to understand, helping them make informed decisions.
- **Understandable Language:** Simple and direct language should be used, avoiding complex legal terminology.

2 Freedom of Choice

- **No Coercion:** : Individuals must have the complete freedom to accept or reject consent to the use of their data without any pressure or influence.
- **No Conditionality:** The provision of a service or product cannot be made conditional on individuals consenting to the processing of their data, unless such processing is necessary to provide that service.

3 Specific Consent

- **Specific Purposes:** Consent must be given for specific, defined purposes, rather than in a general or unspecified manner. **Distinction Between Purposes:** Consent should be sought separately for each purpose of processing.

4 Right to Withdraw

- **Right to Withdraw Consent:** Individuals should have the right to withdraw their consent at any time, and the process of withdrawing consent should be as simple as giving it.
- **Informing Individuals:** Individuals must be informed of their right to withdraw consent.

5 Record of Consent

- **Confirmation of Consent:** Organisations must maintain records confirming that individuals have provided their consent, documenting the method by which consent was given.
- **Date and Time:** The records should include the date and time when consent was provided.

6 Transparency

- **Informing Individuals:** Individuals must be clearly informed about how their data is used, including their rights.
- **Updating Information:** Information related to consent must be updated if processing methods change.

The Role of the General Data Protection Regulation (GDPR) in Enhancing Digital Security

The General Data Protection Regulation (GDPR) plays a significant role in enhancing cybersecurity and digital safety. Here are some key aspects of this role:

1 Defining Security Standards

- **Security Requirements:** The GDPR mandates that organisations implement appropriate technical and organisational measures to protect personal data. This includes safeguarding data from unauthorised access, leakage, and breaches.
- **Risk Assessment:** Organisations must conduct regular assessments of data risks and update security measures accordingly.

2 Reporting Breaches

- **Mandatory Reporting:** The GDPR mandates that organisations report any data breaches within 72 hours of becoming aware of them. This promotes timely responses and mitigates potential harm.
- **Greater Transparency:** By reporting violations, GDPR contributes to enhancing transparency and trust between individuals and organisations.

3 Promoting a Culture of Compliance

- **Awareness and Training:** The GDPR encourages organizations to provide training and awareness programs for employees regarding the importance of data protection and best practices in cybersecurity.
- **Administrative Responsibility:** This enhances a culture of accountability within organizations, leading to proactive measures for data protection.

4 Developing Security Strategies

- **Comprehensive Strategies:** The GDPR encourages the development of comprehensive cybersecurity strategies that encompass all aspects of personal data processing.
- **Threat Response:** Organisations must be prepared to address cybersecurity threats, in order to enhance overall security levels.

5 Enhancing Individual Rights

- **Empowering Individuals:** The GDPR grants individuals greater control over their data, encouraging them to take steps to protect their personal information.
- **Providing Transparency:** By informing individuals about how their data is used, the GDPR enhances individuals› sense of security and trust.

6 Compliance with Global Standards

- **Alignment with Other Laws:** GDPR contributes to aligning security standards with international laws and regulations, helping organisations comply with global cybersecurity requirements.

Activities

Activity 1

Research cases where major organisations have violated the General Data Protection Regulation (GDPR). Analyse the reasons for the violation and the fines imposed and explain how the penalties affected the organisation's reputation and business operations.

Activity 2

Design a diagram illustrating the lifecycle of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR). This should cover the entire process including data collection, processing, storage, and eventual deletion, while highlighting the roles of individuals and organisations at each stage.

Activity 3

Write a report explaining how data protection laws and regulations contribute to enhancing digital trust between organisations and individuals. Include examples that demonstrate the impact of these laws on the digital business environment.

Chapter 6
Data Protection Laws and Individual Rights in the State of Qatar

- Introduction
- Law No. 13 of 2016 on the Protection of Personal Data in Qatar
- Individuals› Rights Under Qatari Law
- The Role of the Law in Enhancing Digital Security in Qatar
- Cybercrime Prevention Law Promulgated by Law No. 14 of 2014
- The Role of Cybercrime Prevention Law in Enhancing Digital Security
- Activities

Introduction

Data protection laws in the State of Qatar play a fundamental role in enhancing digital security, safeguarding individuals› privacy, and ensuring a secure digital environment that aligns with international standards. By establishing legal frameworks that regulate the collection, processing, and storage of personal data, these laws contribute to reducing cybersecurity risks, fostering trust in digital services, and supporting sustainable digital transformation.

Moreover, Qatar's Personal Data Protection Law and the Cybercrime Prevention Law strengthen organisations' ability to combat cyber threats while ensuring individuals› rights to control their data. As such, these regulations serve as a cornerstone for enhancing digital safety and fostering a secure business environment that encourages innovation and investment. Recognising the significance of these legislative measures, this chapter focuses on analysing Qatar's data protection laws and their role in reinforcing cybersecurity, while also examining their impact on individuals and organisations.

Law No. 13 of 2016 on the Protection of Personal Data in Qatar

This law provides a vital legal framework aimed at protecting personal data and ensuring privacy. Its provisions apply to personal data when it is processed electronically, or when it is obtained, collected, or extracted in any other manner with a view to its electronic processing, or when it is processed by a combination of electronic and conventional means [27].

The law defines 'personal data' as:

> Any information relating to a natural person who can be identified, directly or indirectly, through this information or by combining this information with others. This includes all data that can be used to identify an individual, whether collected or processed electronically or conventionally, such as names, identification numbers, health data, and addresses.

27. Law No. (13) of 2016, Personal Data Privacy Protection, issued by the National Cybersecurity Agency. Available at: https://assurance.ncsa.gov.qa/ar/privacy/law

The State of Qatar seeks to align its legislation with international standards, particularly in the areas of data protection, cybersecurity, and individual rights. Accordingly, it enacted Law No. 13 of 2016 on Personal Data Protection, in compliance with the General Data Protection Regulation (GDPR), alongside the Cybercrime Prevention Law. These measures aim to strengthen the protection of individuals' privacy and secure the digital environment, thereby enhancing Qatar's position as a leading advocate for digital rights and cybersecurity in the region.

The importance of Law No. 13 of 2016 on the Protection of Personal Data in the state is evident through the following points and axes:

1 Protection of Individuals' Privacy

- **Guaranteeing rights:** The law safeguards individuals' rights to control their personal information, thereby enhancing privacy.

- **Protection of sensitive data:** It protects sensitive data like health and financial information from the unauthorised usage.

2 Increasing Confidence

- **Building confidence among individuals and institutions:** A legal framework that protects data enhances individuals'sense of security when interacting with institutions.

- **Stimulating digital engagement:** This facilitates digital interaction and helps develop new services.

3 Data Processing Regulation

- **Clear Legal Framework:** The regulation provides a necessary framework for how data can be collected and used, making it easier for organisations to understand their obligations.

- **Defining Responsibilities:** It defines the responsibilities required of organisations and individuals when handling data.

4 Compliance with International Standards

- **Alignment with Global Legislation:** This enhances the alignment of local laws with international standards such as the General Data Protection Regulation (GDPR).

- **Fostering International Cooperation:** It facilitates cooperation with other countries in the field of data protection.

Individual Rights Under Qatari Law

Every individual has the right to the protection of their personal data. The processing of such data is only permitted within a framework of transparency, respect for human dignity, and accepted practices. Furthermore, personal data cannot be processed without the individuals' consent[28], **Among the individuals' rights are:**

- **Withdrawing their previous consent for the processing of their personal data.**
- **Objecting to the processing of their personal data if it is unnecessary for the purposes for which it was collected.**
- **Requesting the deletion or erasure of their personal data once the purpose for which the data was collected has been fulfilled.**
- **Requesting the correction of their personal data, attaching evidence to support their request.**

Generally speaking, and in accordance with Qatari law, before processing personal data, individuals must be notified of a range of information. This includes details about the entity processing the data, the legitimate purposes for processing personal data, a comprehensive and accurate description of the processing activities, and the extent to which personal data is disclosed for legitimate purposes.

28. Law No. (13) of 2016 concerning the Protection of Personal Data Privacy, Individuals' Rights, Ministry of Justice, available at: https://almeezan.qa/LawView.aspx?opt&LawID=7121&language=ar#Section_17483.

Responsibilities of Personal Data Controllers

- Review of data privacy procedures.
- Identification of processing equipment responsible for protecting personal data.
- Training and awareness-raising among information processors.
- Establishment of secure internal systems to receive and examine complains.
- Effective management of personal data and use of appropriate techniques.
- Comprehensive compliance audits.
- Verification of compliance with the instructions by the data processor.

The Role of Law in Enhancing Digital Security in Qatar

This law creates a secure and sustainable digital environment that supports innovation and growth within the country. It aims to protect individuals› personal information, thereby enhancing user confidence when interacting with digital services. Furthermore, it mandates that institutions implement security measures to safeguard data, ensuring that information is not subject to breaches or unauthorised use.

The law also enhances transparency by granting individuals the right to access information about how their data is used, thereby empowering them to control their personal information and contributing to a higher level of awareness about the importance of data protection. This, in turn, fosters a culture of digital security within society.

Cybercrime Prevention Law Promulgated by Law No. 14 of 2014

The law aims to regulate illegal online activities and impose strict penalties on those who commit such crimes. The law addresses a range of illegal behaviours, including online fraud and online defamation. Its objective is to protect consumers and victims of cybercrime, and to enhance cybersecurity within the country.

Types of Cybercrimes under the Cybercrime Prevention Law

Cybercrime Prevention law seeks to combat a wide range of cybercrimes, including cyberbullying, online defamation, spamming, hateful comments, unauthorized publication of personal information, digital identity theft, cyber hacking, e-commerce fraud, and manipulation of individuals› personal data.

Cybercrime refers to any illegal activity carried out using digital technologies, targeting individuals, institutions, or even government systems. These crimes include digital theft, forgery, and privacy violations. For example, when someone steals a digital identity to use it in financial transactions or to obtain confidential information, this is considered a cybercrime.

On the other hand, cybersecurity is a science and a set of practices aimed at protecting systems, networks, and data from digital threats and cyberattacks. Cybersecurity focuses on prevention before crimes occur by securing digital infrastructure and developing policies and strategies for protection.

To strengthen deterrence against cybercrimes, the law has imposed strict penalties on individuals who commit such offenses. For instance,
a person who commits fraud on bank accounts or electronic payments is subject to a prison sentence ranging from six months to five years and a fine ranging from 10,000 to 50,000 Qatari Riyals[29].

Significance of Qatar's Cybercrime Law

The law holds significant importance in several aspects, the most notable of which are as follows

1. **Protection of the society:** The law provides a legal mechanism to combat the cybercrimes threatening individuals and institutions.

2. **Enhancing cybersecurity:** The law defines the types of crimes and penalties which enhances the country's cybersecurity.

29. Cybercrime Prevention Law of Qatar, Law No. 14 of 2014, Al Meezan, available at: https://almeezan.qa/LawView.aspx?opt&LawID=6366&language=ar.

3 **Protection of personal data:** The law includes provisions that safeguard personal data and sensitive information from breaches.

4 **Increasing awareness level:** The law contributes to spreading awareness of the dangers of cybercrimes and the protection methods.

5 **Promoting trust in the digital environment:** The law sets a framework that promotes the trust of individuals and companies in using digital services.

6 **International cooperation:** The law encourages cooperation with other countries to combat cybercrimes.

7 **Deterring crimes:** By enacting strict sanctions, people are deterred from committing cybercrimes.

The Role of Cybercrime Prevention Law in Enhancing Digital Security

This law contributes to enhancing digital security in the country through several important aspects and aims to combat crimes occurring in cyberspace, thereby helping to protect individuals and society.

The law also defines various types of cybercrimes, such as hacking, fraud, and defamation, which helps raise awareness within society about potential risks by establishing deterrent penalties for offenders. It reinforces the principle of deterrence, thereby reducing the likelihood of cybercrimes being committed.

Furthermore, the law contributes to strengthening cooperation between local and international authorities in combating cybercrime, enabling the exchange of information and expertise to address crime more effectively. It also includes mechanisms for monitoring and investigating crimes, thereby enhancing the authorities› ability to confront risks.

In conclusion to this chapter, the cyber risks faced by data at both personal and institutional levels are increasing, highlighting the importance of the laws and regulations governing it. These regulations set the necessary standards to ensure data security and integrity, as data is the cornerstone of cyberspace, and its exposure to risks threatens social and economic stability.

In general, while laws play a crucial role in enhancing data security, they cannot achieve this objective without effective collaboration from companies, institutions, and individuals. Laws and regulations serve as organisers and guides for individual and institutional efforts, rather than a replacement for them.

Activities

Activity 1

Create a table highlighting the points of agreement and disagreement between Qatar's Law No. 13 of 2016 on the Protection of Personal Data and the General Data Protection Regulation (GDPR).

Activity 2

Qatar›s Cybercrime Prevention Law is considered one of the most important laws in enhancing cybersecurity. Explain how this law contributes to reducing cybercrime.

Activity 3

The personal data of children is a significant issue that laws and regulations seek to protect. Explore the role of these laws and regulations in protecting children›s data, supporting your answer with relevant examples.

Chapter 7
Risks of Artificial Intelligence: Challenges in the Age of Advanced Technology

- Introduction
- Artificial Intelligence and Enhancing Cybersecurity and Digital Safety Indicators
- Risks of Artificial Intelligence
- AI-Powered Phishing
- Risks of Generative AI
- Real-world Cases of Fraud and Forgery Using AI
- Activities

Introduction

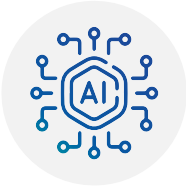
Artificial Intelligence (AI) is an advanced branch of modern technology aimed at enabling machines to perform tasks that typically require human intelligence, such as learning, reasoning, and decision-making.
The concept of AI first emerged in the mid-20th century, specifically in 1956, when the term was first used at a scientific conference in the United States. Since then, AI has undergone tremendous development, transforming from a mere theory into a technology used in many fields, such as healthcare, transportation, commerce, finance, banking, and industry.
Despite its numerous benefits, AI also carries significant risks. With its rapid advancement, challenges related to security, privacy, and economic risks have emerged. Moreover, artificial intelligence has become a tool exploited in advanced fraud and forgery operations, thereby heightening the necessity to warn of its risks and establish regulations to govern its use. This is particularly significant as it is now employed in the development of cyberattack tools, enabling the identification of digital vulnerabilities at a faster pace. Additionally, it is utilised in enhancing social engineering tools, such as deepfake technologies and other methods employed in cyberattacks.

This perspective should not be interpreted as implying that artificial intelligence has only drawbacks. On the contrary, organisations concerned with cybersecurity and digital safety are increasingly relying on artificial intelligence to develop cyber tools and strategies. This is achieved through its capability to process vast amounts of data simultaneously and utilise the results of such analyses to enhance cyber manoeuvres, simulate attacks, and identify and address digital vulnerabilities before they are exploited by attackers.

It can thus be argued that artificial intelligence in the realm of cybersecurity is a double-edged sword. While it can be employed to strengthen cybersecurity indicators and digital safety at the level of nations, institutions, and communities, it can equally be used to advance tools for cyberattacks and threats. Ultimately, its impact depends on the purpose of its application and the entity utilising it.

Artificial intelligence is considered a revolutionary technology used in numerous fields to facilitate human life and enhance efficiency. However, its accelerated use raises questions about its positive and negative impacts, particularly in the field of cybersecurity. Below is a table illustrating these roles:

1	2
Positive role	**Negative role**
Enabling machines to perform tasks that require human intelligence such as learning and reasoning.	Challenges related to security and privacy with the advancement of artificial intelligence.
Its use in multiple fields such as healthcare, transportation, commerce, and the financial sector.	Its exploitation in advanced fraud and forgery operations such as deepfake technology.
Supporting cybersecurity through the processing of massive volumes of data.	Developing tools for cyberattacks and rapidly detecting cyber vulnerabilities.
Enhancing cyber manoeuvres, and simulating attacks to identify vulnerabilities and address them.	Its use in social engineering tools to launch cyberattacks.
Enhancing digital security and safety at the level of nations and institutions.	Reliance on the intent of the entity using it, which makes its use a double-edged sword.



Artificial Intelligence and Enhancing Cybersecurity and Digital Safety Indicators

Artificial intelligence offers significant added value to efforts to enhance cybersecurity and digital safety at the institutional and community levels. It aids in the early detection of cyberattacks more effectively than traditional tools. AI techniques are also characterised by their ability to process large amounts of data quickly and with high accuracy, reducing the risk of human error in analysis. These techniques are used through various tools, including machine learning models and predictive analytics. The following is an explanation of how cybersecurity and digital safety policy efforts benefit from AI technologies:

Using Machine Learning to Detect Threats: Machine learning techniques enable the analysis of large amounts of data quickly to detect indicators of compromise. This helps accelerate investigations and uncover unclear threat patterns. For example, tools like Cisco Secure Endpoint & Cisco Umbrella use machine learning to detect suspicious behaviours.

Predictive Analytics: AI-based algorithms enable the analysis of data from multiple sources, such as the dark web and open sources, to detect and predict potential threats before they occur, helping to mitigate the impact of potential cyberattacks.

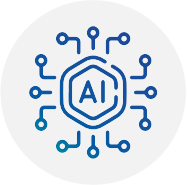
Web Application Penetration Testing: AI can simulate potential attacks on systems to determine the strength of defensive measures against attacks. This also helps in discovering vulnerabilities in the system and fixing them before attackers can exploit them.

Analysing Network Traffic: AI is capable of analysing network traffic accurately and quickly, enabling the early detection of attacks and the detection of advanced malware that may not be detected by traditional tools.

Training and Qualifying Cybersecurity and Digital Safety Specialists: AI techniques contribute to training cybersecurity professionals by identifying weaknesses in their knowledge and providing tailored training tools to address these gaps. Additionally, they simulate realistic intrusion scenarios to train them to handle real-world situations.

Managing Cyber Drills: Cyber drills are an effective way to discover weaknesses in defence systems and test the readiness of teams to respond to attacks. AI can organize these drills in a way that simulates real-world attacks, making them more realistic and effective.

Detecting Phishing Attempts: Through AI techniques, it is possible to detect phishing attempts, such as deepfake videos.



Risks of Artificial Intelligence

The use of artificial intelligence by cybercriminals has contributed to an increase in the risks and costs of cyberattacks, both financially and socially. The following highlights the most significant of these risks:

1

Loss of Privacy

As the use of artificial intelligence in big data analysis increases, privacy emerges as one of the biggest risks. Modern AI systems rely on vast amounts of data to learn and develop, requiring the collection of user data and personal information. This leads to the invasion of individuals' privacy and the exploitation of their data in unexpected ways. For instance, users' personal data may be stolen or sold without their knowledge, resulting in a violation of their privacy.

2

AI-Powered Fraud

Artificial intelligence has become an effective tool for modern fraudsters. It's used to generate fake messages or create counterfeit online accounts, making it easier for criminals to execute fraudulent schemes. For instance, deepfake[30] technology is emɹployed to create counterfeit audio-visual content featuring real people saying or doing things they never actually did.

3

Cybercrime Automation

With the advancement of artificial intelligence, it has become possible to automate cyberattacks. Machine learning techniques can learn system vulnerabilities and attack them faster and more efficiently than humans can. A prime example is the use of AI in developing ransomware that can identify the most valuable files in a system and encrypt them to extort victims. In 2021, there was a significant increase in ransomware attacks worldwide, demonstrating the significant impact of AI in facilitating cybercrime.

30. What is deepfake technology? TECHTARGET, on site: https://www.techtarget.com/whatis/definition/deepfake

4

Empowering Cybercrime

AI technologies contribute to making cybercrimes more complex and dangerous by reducing the need for human intervention in various stages, such as developing malware or managing fraudulent operations. Additionally, AI enables criminals to analyse large amounts of data quickly and efficiently, allowing them to identify vulnerabilities and high-value targets. These technologies can also study current defence strategies to identify weaknesses, making it easier to bypass them and execute precise attacks.

5

Evolution of Phishing and Social Engineering Attacks

Phishing and social engineering attacks, especially, have benefited greatly from artificial intelligence. Modern technologies can create fake websites or realistic images to deceive victims, in addition to AI-powered phishing bots. For instance, the voice of the CEO of a British energy company was cloned using AI, prompting an employee to transfer $243,000 to the attacker's account[31]. These techniques make it easier for attackers to convince victims, and attacks relying on voice and image impersonation have increased significantly.

31. Jesse Damiani. A Voice Deepfake Was Used To Scam A CEO Out Of $243,000, FORBES, on site: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/

6

Exploitation of Bots in Cyberattacks

Attackers can exploit bots to perform a range of fraudulent tasks, such as submitting fraudulent loan applications or manipulating prices in financial markets. AI-powered bots make these processes faster and more accurate, increasing the risk of cyberattacks and online fraud.

7

Emerging Cyber Threats from Artificial Intelligence Applications

With the advancement of artificial intelligence (AI) applications, new threats have emerged that can be exploited for malicious purposes, including:

- **Self-learning attacks:** AI algorithms are capable of analysing system defences and autonomously developing their attacks.
- **Manipulation of information:** AI can be utilised to spread false news and influence public opinion by generating deceptive content that is difficult to verify[32].
- **Concealment of malicious software:** AI techniques are employed to enhance the sophistication of viruses and malware, enabling them to evade detection by traditional security systems[33].

.

32. Increasing Threat of DeepFake Identities, HOMELAND SECURITY, on site: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

33. Risks and Mitigation Strategies for Adversarial Artificial Intelligence Threats, HOMELAND SECURITY on site: https://www.dhs.gov/sites/default/files/2023-12/23_1222_st_risks_mitigation_strategies.pdf

- **Automated hacking attacks:** AI can facilitate advanced cyber intrusions by analysing vast datasets to identify and exploit security vulnerabilities.

To counter these risks, it is essential to develop advanced security systems that leverage AI technology, enhance cybersecurity awareness among technology users, and update cybersecurity strategies to keep pace with the latest advancements in AI.

AI-Powered Phishing

With the advent of artificial intelligence, the risks associated with phishing attacks have significantly increased, making individuals more susceptible to falling victim to these cybercrimes. Here›s how phishing scams leverage AI:

- **Advanced Social Engineering:** Attackers rely on social engineering techniques to craft highly personalised phishing emails tailored to each individual victim. Big data provides attackers with access to detailed information about each target, making it difficult for recipients to identify the malicious intent of these messages.
- **Creating Realistic or Semi-Realistic Phishing Content:** Using AI algorithms, it is possible to generate realistic content that mimics the style and format of legitimate legal correspondence, whether emails or websites. This makes it difficult for security systems to distinguish between fraudulent and legitimate activities.
- **Scalability of Attacks:** The automation provided by AI enables attackers to carry out large-scale phishing campaigns, including designing, distributing messages to thousands of individuals, and interacting with their responses; thereby increasing the likelihood of deceiving a larger number of victims.

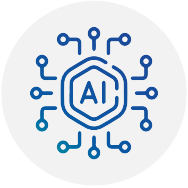
- **Evading Security Programs:** AI algorithms learn from the responses of security systems, enabling them to bypass phishing and malware detection software. Attack methods are constantly modified to evade detection by traditional security filters.

- **Targeted Attacks:** By leveraging the advanced data collection and analytical capabilities of artificial intelligence, attackers can create highly customised phishing attacks aimed at specific individuals or groups, exploiting their interests and vulnerabilities. This significantly enhances the effectiveness and success rate of such attacks.

- **Automated Vulnerability Identification:** Instead of manually searching for vulnerabilities in systems, AI can automate the process of scanning networks to identify weaknesses and potential entry points that can be exploited in phishing attacks.

- **Easy Password Guessing:** Using machine learning algorithms, models can be developed to guess passwords more accurately. These models analyse patterns and increase the likelihood of successfully accessing victims› accounts.

- **Using Deepfakes:** Through deepfake videos and audio recordings created by AI, attackers can impersonate important figures, making it easier to steal identities or manipulate public opinion.



Risks of Generative AI

Generative AI is a type of artificial intelligence capable of creating new content or generating innovative outputs based on patterns learned from previous data. It utilises machine learning models such as deep neural networks (Deep Learning) to generate text, images, music, programming code, and even complex designs.

Generally, generative AI possesses a set of characteristics and features. Here›s an overview of the most significant ones:

1 **Content Generation:** It can create original content such as articles, images, music, or videos. For example, «ChatGPT» generates text in response to text inputs.

2 **Pattern Learning:** Generative AI works by learning from large amounts of data and discovering underlying patterns, then using those patterns to create new and innovative outputs.

3 **Practical Applications:** It is used in various fields such as digital art, creative writing, product design creation, code generation, and in developing automated conversations with robots.

> Generative Artificial Intelligence (Generative AI) is a powerful and innovative tool; however, it simultaneously contributes to the escalation of cyber threats in various ways. It is being exploited by attackers to enhance their methods and increase the efficacy of their attacks

Below are some of the principal impacts of generative AI on cyber threats:

1 ## Increased Accuracy of Phishing Attacks

Generative AI can be used to create high-quality fraudulent emails containing accurate and realistic language, tailored to each individual victim. This makes it difficult for users to distinguish between genuine and fake messages. AI can also generate more convincing fake websites to facilitate phishing attacks.

2

Development of Audio and Visual Deepfake Techniques

Deepfake technology, which relies on generative AI, is used to create realistic fake videos and audio clips. This allows attackers to impersonate influential or well-known individuals to deceive victims and induce them to take specific actions, such as transferring money or revealing sensitive information.

3

Generating Malware

Generative AI can design new malware capable of evading traditional antivirus software. Using deep learning, AI can develop new forms of viruses or attacks that are more sophisticated and better able to bypass protection systems.

4

Testing Advanced Attacks

Generative AI can simulate cyberattacks and test new strategies to improve their effectiveness. It can also develop sophisticated models that enable attackers to analyse security responses and continuously modify attack methods to evade detection.

5

Password Guessing

Using generative AI and machine learning techniques, password-guessing techniques can be improved, making attacks on accounts more accurate and effective. These models can analyse patterns of common passwords and predict new passwords based on available data.

6

Targeting Victims More Accurately

Generative AI can analyse big data to identify individuals and organisations that are most vulnerable to cyberattacks. This precise targeting increases the chances of successful attacks and reduces the likelihood of detection.

Real-world Cases of Fraud and Forgery Using AI

1 Deepfake Extortion (2020)

In 2020, deepfake technology was used to extort an American politician. Criminals created deepfake videos depicting the politician in compromising and immoral situations, threatening to release these videos if a large sum of money was not paid. Although the videos were fake, their impact was strong enough to make the victim seriously consider the threat. This incident is a prime example of how AI can be used for extortion and damaging the reputation of individuals.

2 AI-Powered Attacks on Banks

Global banks have experienced a surge in sophisticated cyberattacks that leverage artificial intelligence in innovative and dangerous ways. These attacks have evolved beyond traditional methods or manual network intrusions; AI is now integrated to meticulously analyse banking systems and pinpoint security vulnerabilities. Attack techniques have advanced to the point where AI can autonomously explore systems, leveraging machine learning algorithms to identify anomalies and exploit system weaknesses.

AI has not only been used for system analysis but has also facilitated simultaneous attacks on multiple banks. This coordinated approach, which overwhelms cybersecurity teams, has led to a surge in successful attacks. For instance, a series of banks in Asia and Europe were simultaneously targeted, resulting in a theft of nearly $100 million before the breaches were detected and malicious activities halted[34].

One of the most alarming aspects of these attacks is the ability of attackers to conceal their malicious activities using AI. Post-breach, AI techniques are employed to modify financial data subtly, making the attack difficult to detect. By manipulating transactions and bank transfers to appear legitimate, attackers can siphon off funds without raising suspicions. Even when anomalies are detected, security systems struggle to trace the attack›s origin or pinpoint the exact breach point.

34. Cyber Attacks on Banking Industry Organizations in 2021, RSI Security, on site: https://blog.rsisecurity.com/cyber-attacks-on-banking-industry-organizations-in-2021/

In conclusion, artificial intelligence is witnessing rapid advancements, with current evidence suggesting that reliance on AI and generative AI will increase across most fields soon. This progress will likely be accompanied by cybercriminals exploiting these developments, underscoring the dual nature of AI as both a positive and negative force, depending on how it is utilised. To enhance protection against its associated risks, particularly in relation to cybercrimes and phishing attacks, it is imperative to raise awareness of these dangers at both institutional and individual levels.

Activities

Activity 1

Search the internet for cases of phishing or cybercrimes that were carried out using artificial intelligence techniques. Infer the mistakes made by users that led them to fall victim to these crimes.

Activity 2

Compare the benefits and risks of artificial intelligence in a table.

Activity 3

Both cybersecurity and digital safety, on the one hand, and cyber threats, on the other, have benefited from artificial intelligence technologies. This dynamic resembles a race to harness these advancements between organisations focused on cybersecurity and digital safety and malicious cyber entities. Investigate how each of these parties utilises artificial intelligence to achieve their respective objectives.

References

1. Youssef, Amir. (2015). Cybercrime in the Gulf Cooperation Council Countries and International and Local Efforts to Combat It: Internet and Computer Crimes in the GCC Countries. Egypt: Dar Al-Kutub Al-Arabiya.
2. Kamal, Mohamed. Cyberterrorism: When the Terrorist Uses a Keyboard Instead of a Bomb. Dar Kleem for Printing, Publishing, and Distribution (Cairo, Egypt), 1st edition, 2022.
3. What is End User Security?, CISCO, available at: https://www.cisco.com/site/us/en/learn/topics/security/what-is-user-security.html#jump-anchor-3
4. Cybercrime Prevention Law of Qatar, Law No. 14 of 2014, Al Meezan, available at: https://almeezan.qa/LawView.aspx?opt&LawID=6366&language=ar
5. Guidelines on Ransomware Software, National Cyber Security Agency, available at: https://ncsa.gov.qa/sites/default/files/202410-/NCSA_CSGA_Guidelines_Ransomware_Attacks_AR_V1.0.pdf?csrt=5855983971683337.
6. Guidelines on Ransomware Software, National Cyber Security Agency, available at: https://ncsa.gov.qa/sites/default/files/202410-/NCSA_CSGA_Guidelines_Ransomware_Attacks_AR_V1.0.pdf?csrt=5855983971683337.

7. Given the seriousness of phishing, a separate chapter will be dedicated to it within the context of this guide.
8. Global Data Breach Costs Reach an All-Time High of $4.9M, IBM Says, available at: https://www.cybersecuritydive.com/news/ibm-data-breach-cost-credentials-phishing/722689.
9. What is Spear Phishing?, Proofpoint, available at: https://www.proofpoint.com/de/threat-reference/spear-phishing.
10. What is Voice Phishing (Vishing)?, Kaspersky, available at: https://me.kaspersky.com/resource-center/definitions/vishing.
11. 10 Most Common Signs of a Phishing Email, available at: https://www.titanhq.com/blog/10-tell-tale-signs-that-spam-email-is-a-phishing-scam/.
12. HTTPS Phishing Attacks: How Hackers Use SSL Certificates to Feign Trust, available at: https://www.keyfactor.com/blog/https-phishing-attacks-how-hackers-use-ssl-certificates-to-feign-trust/
13. Clone Phishing: What It Is and How to Prevent It, Norton, available at: https://us.norton.com/blog/online-scams/clone-phishing
14. Defining Insider Threats, CISA, available at: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
15. What Are Advanced Persistent Threats?, IBM, available at: https://www.ibm.com/think/topics/advanced-persistent-threats
16. Cloud Security Issues and Challenges, Kaspersky, available at: https://me.kaspersky.com/resource-center/preemptive-safety/cloud-security-issues-challenges

17. Ramonas, Lukas. What is a Dumpster Diving Attack?, NordVPN, May 2023, available at: https://nordvpn.com/blog/dumpster-diving-attack/
18. Cieply, Michael and Brooks Barnes. Sony Cyberattack: First a Nuisance, Swiftly Grew Into a Firestorm, The New York Times, December 2014, available at: https://www.nytimes.com/201431/12//business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html
19. What is GDPR?, GDPR, available at: https://gdpr.eu/what-is-gdpr/
20. What IAM is and what it does, Microsoft, available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam
21. Coachable Moments: Insider Risks, Cloud Storage, and Remote Work Security, Proofpoint, available at: https://www.proofpoint.com/us/blog/information-protection/coachable-moments-insider-risks-cloud-storage-and-remote-work-security
22. What is a VPN?, Microsoft, available at: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-a-vpn
23. What is Mobile Device Management (MDM)?, IBM, available at: https://www.ibm.com/topics/mobile-device-management
24. What are the GDPR Fines? on site: https://gdpr.eu/fines/
25. How the GDPR Could Change in 2020, available at: https://gdpr.eu/gdpr-in-2020/
26. Italy Fines Eni Gas e Luce €11.5 Million for Multiple GDPR Violations, available at: https://gdpr.eu/italy-fines-energy-company-for-multiple-gdpr-violations/

27. Law No. (13) of 2016 on the Protection of Personal Data Privacy, National Cyber Security Agency, available at: https://assurance.ncsa.gov.qa/ar/privacy/law.
28. Law No. (13) of 2016 on the Protection of Personal Data Privacy and Individuals› Rights, Ministry of Justice, available at: https://almeezan.qa/LawView.aspx?opt&LawID=7121&language=ar#Section_17483
29. Cybercrime Prevention Law of Qatar, Law No. 14 of 2014, Al Meezan, available at: https://almeezan.qa/LawView.aspx?opt&LawID=6366&language=ar
30. What is Deepfake Technology? TECHTARGET, available at: https://www.techtarget.com/whatis/definition/deepfake
31. Jesse Damiani. A Voice Deepfake Was Used to Scam a CEO Out of $243,000, FORBES, available at: https://www.forbes.com/sites/jessedamiani/201903/09//a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/
32. Increasing Threat of Deepfake Identities, Homeland Security, available at: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf
33. Risks and Mitigation Strategies for Adversarial Artificial Intelligence Threats, Homeland Security, available at: https://www.dhs.gov/sites/default/files/20231222_23/12-_st_risks_mitigation_strategies.pdf.
34. Cyber Attacks on Banking Industry Organisations in 2021, RSI Security, available at: https://blog.rsisecurity.com/cyber-attacks-on-banking-industry-organizations-in-2021

This Guide

Amid the rapid evolution of cyberspace and the accompanying escalation of cyber threats and risks, digital safety is no longer a mere intellectual luxury or a secondary concern. Instead, it has become a paramount priority for nations, institutions, communities, and individuals alike, now recognised as a matter of utmost importance. In alignment with this perspective, the concept of the Digital Safety Guide emerged as one of the key awareness tools within the framework of the National Initiative for Digital Safety.

This guide serves as a comprehensive reference and an essential knowledge resource for various segments of society. It encompasses up-to-date insights into cybersecurity and digital safety, providing detailed information on key cybersecurity concepts, identifying emerging cyber threats, and offering guidance on how to effectively address them, which will positively enhance societal security and strengthen cyber resilience.