



KEMENTERIAN PENDIDIKAN TINGGI
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI

POLITEKNIK
MALAYSIA
SULTAN MIZAN ZAINAL ABIDIN



Digital Etiquette

2nd Edition

Ab Aziz Ikhwan bin Ab Wahab
Siti Farahiah binti Mohamed
Wan Eliani binti Wan Hassan

Digital Etiquette

2nd Edition

Ab Aziz Ikhwan bin Ab Wahab
Siti Farahiah binti Mohamed
Wan Eliani binti Wan Hassan

Hak cipta terpelihara. Tiada bahagian ini boleh diterbitkan semula atau ditukar dalam apa jua bentuk dengan apa cara jua sama ada elektronik, mekanikal, fotokopi, rakaman dan sebagainya sebelum mendapat kebenaran bertulis daripada Pengarah Politeknik Sultan Mizan Zainal Abidin.

Diterbitkan oleh:
Politeknik Sultan Mizan Zainal Abidin
Km 08, Jalan Paka,
23000 Kuala Dungun, Terengganu

09-840 0800

DISCLAIMER AND COPYRIGHT

The eBook titled "Digital Etiquette: 2nd Edition" is published online in November 2025.

This eBook is the original work of Ab Aziz Ikhwan bin Ab Wahab, Siti Farahiah binti Mohamed and Wan Eliani binti Wan Hassan.

Copyright is protected. Any opinions and experiences expressed here are solely those of the author. Reproduction of any part of this writing in any form or by any means, whether electronic, photocopying, mechanical, recording, or otherwise, without the author's permission, is prohibited. The author also does not guarantee that the content is suitable for readers, but all content is based on the author's own experiences and expertise.



Preface

Alhamdulillah, praise to Allah SWT, with His grace and mercy, the First Edition of e-book Digital Etiquette : 2nd Edition has finally completed. We hope that this e-book will be helpful as a guideline in their learning process. This e-book is developed as a guide and reference for lecturers also. Special thanks also to those who were directly or indirectly involved in the completion of this e-book. Any positive feedback mostly welcomed and appreciated.



Abstract

In today's interconnected world, understanding digital etiquette is essential for maintaining respectful and secure online interactions. This interactive guide explores the principles of digital conduct, covering critical areas such as e-access, e-literacy, e-safety, and e-rules. It delves into personal data protection, cyber security issues, and the impact of cyber crimes like hacking, fake news, and identity theft. Through engaging content and practical tips, readers will gain the knowledge and skills needed to navigate the digital landscape responsibly and safely. This guide is a valuable resource for anyone looking to enhance their digital etiquette and security awareness.

Discover our Interactive eBook

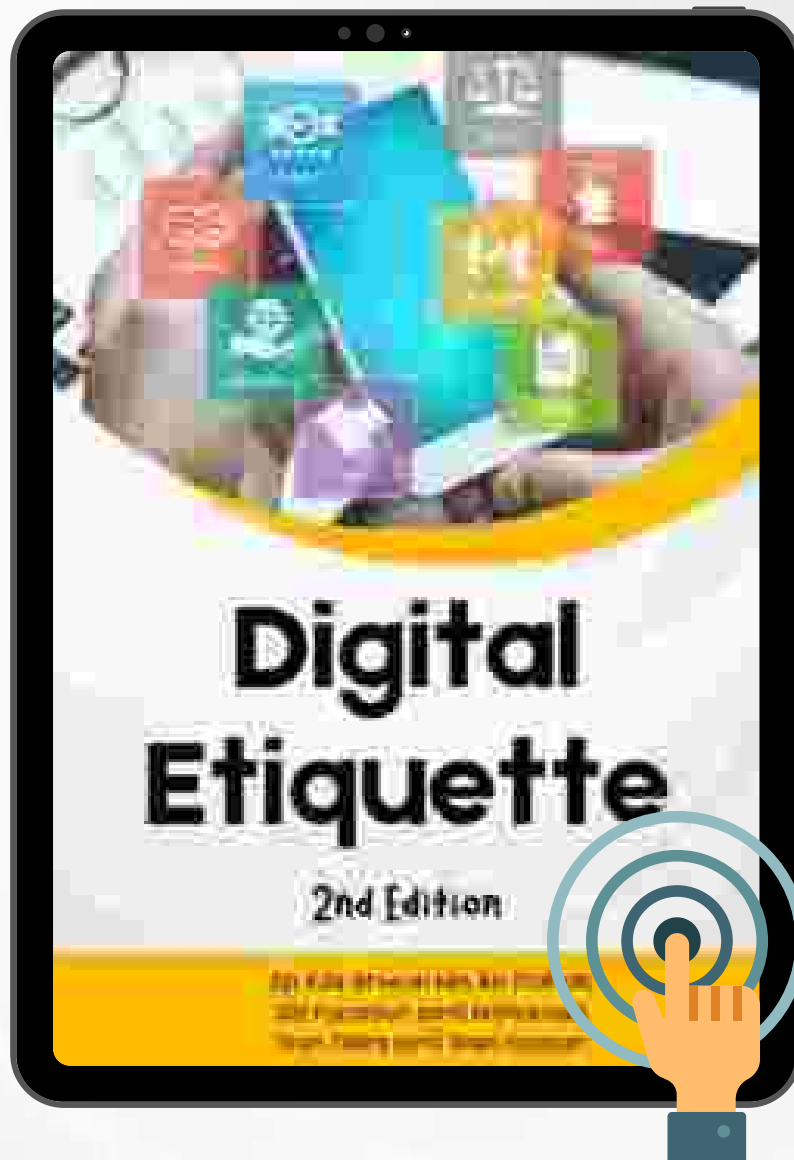
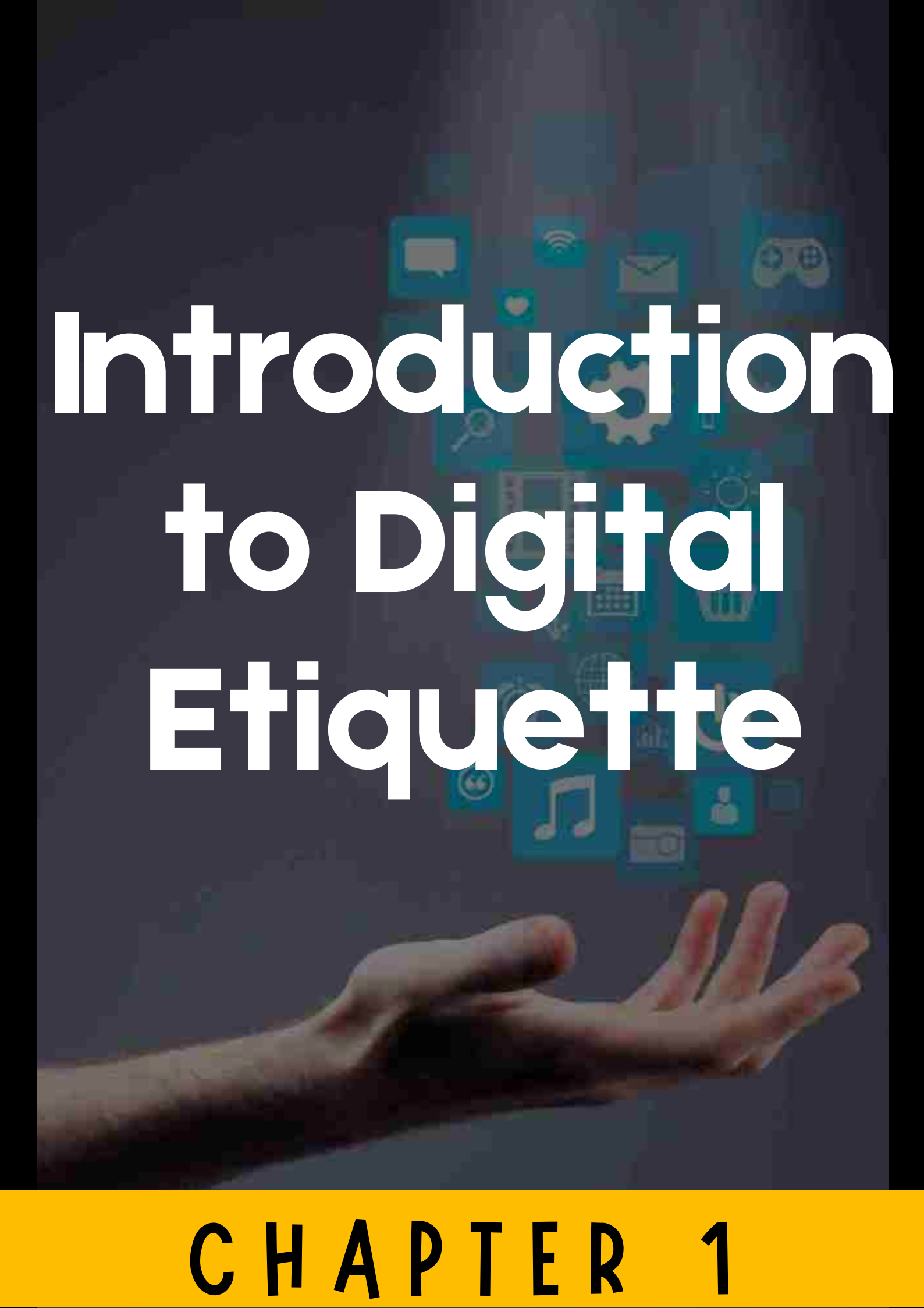


TABLE OF CONTENTS

Chapter 1 : Introduction to Digital Etiquette	1
1.1 Describe the Concept of Digital Etiquette	2
1.2 Digital Etiquette Issues in Key Areas	4
Chapter 2 : Personal Data Protection	26
2.1 Describe Purpose and Legal Act of Personal Data Protection	27
2.2 Identify the Importance of Personal Data Protection	34
2.3 Identify the Intrusion of Personal Data	38
Chapter 3 : Cyber Security Issues	44
3.1 Describe the concept and legal act of cyber security	45
3.2 Identify the effect of cyber crimes on a particular sector	49
3.3 Identify issues in hacking, fake news and identifying theft	54
Conclusion	60



Introduction to Digital Etiquette

CHAPTER 1

1.1 Describe the Concept of Digital Etiquette



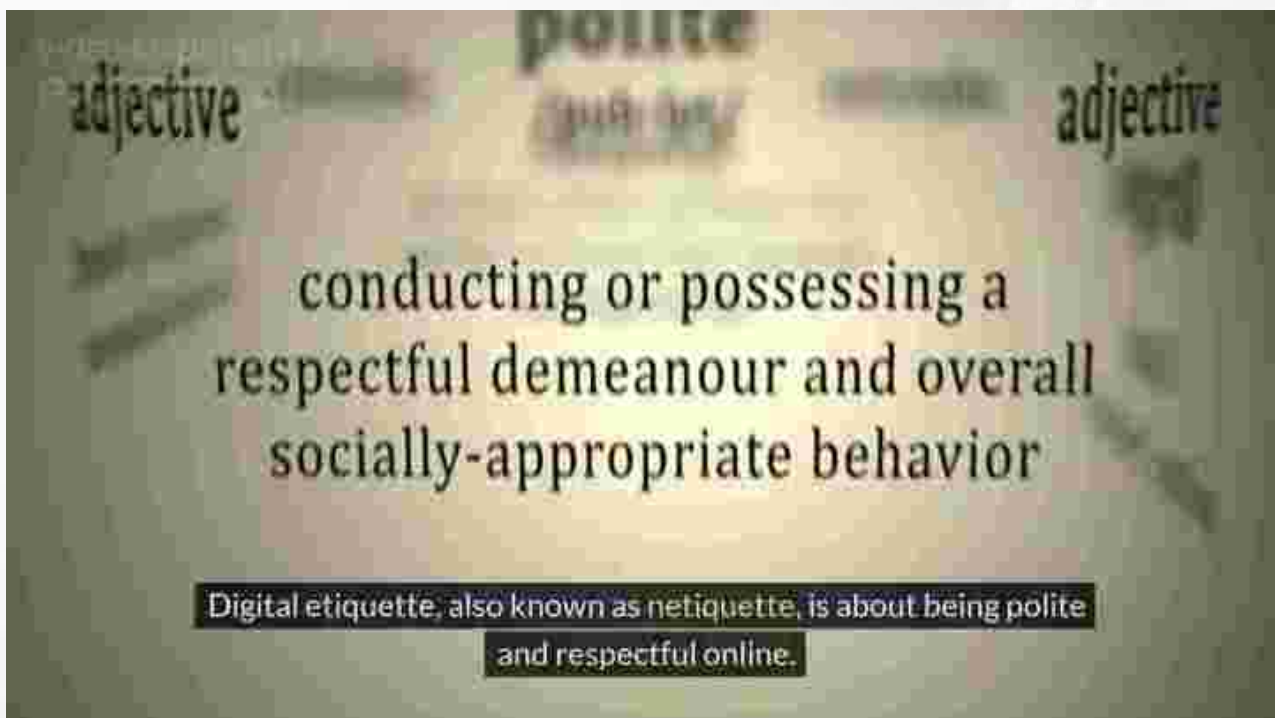
Digital etiquette, also known as "netiquette," is the code of conduct for interacting online. It encompasses the norms and guidelines that dictate how individuals should behave in digital environments to ensure respectful, efficient, and effective communication. Just as social etiquette helps maintain harmony and respect in face-to-face interactions, digital etiquette does the same in virtual spaces.

Understanding Digital Etiquette

Digital etiquette involves a broad spectrum of behaviors, from basic manners like saying "please" and "thank you" in emails to more complex actions like respecting privacy and avoiding plagiarism. The primary goal of digital etiquette is to foster positive interactions and prevent misunderstandings and conflicts. With the proliferation of digital communication channels such as emails, social media, instant messaging, and forums, adhering to digital etiquette has become increasingly important.

Importance of Digital Etiquette

Adhering to digital etiquette ensures smooth and positive interactions. It helps build a respectful and productive online community, whether in personal, educational, or professional settings. Good digital etiquette fosters trust, collaboration, and effective communication, making digital interactions more enjoyable and meaningful.



What is Digital Etiquette

In conclusion, digital etiquette is essential for maintaining civility and efficiency in our increasingly digital world. By understanding and practicing the principles of netiquette, individuals can contribute to a respectful and harmonious online environment, ultimately enhancing their own digital experiences and those of others.

1.2 Digital Etiquette Issues:

1.2.1 e-Access

e-Access, short for electronic access, refers to the ability of individuals to utilize digital technologies and access online resources and services. It encompasses the availability, accessibility, and usability of digital tools and platforms for all individuals, regardless of their socio-economic status, geographic location, or physical abilities. Ensuring equitable e-Access is fundamental to achieving digital inclusion and bridging the digital divide.



Understanding e-Access

e-Access involves multiple dimensions including:

- **Availability:** The availability of digital infrastructure, such as high-speed internet, reliable electricity, and digital devices, is a primary component of e-Access. In many parts of the world, especially in rural or underdeveloped regions, lack of infrastructure remains a significant barrier to digital access.

- **Affordability:** Even when digital infrastructure is available, the cost of internet services and digital devices can be prohibitive for many individuals. Ensuring that digital access is affordable is crucial to achieving universal e-Access. This involves not only reducing costs but also providing subsidies or financial assistance to those in need.
- **Digital Literacy:** Having access to digital tools and the internet is not enough; individuals must also possess the skills and knowledge to use them effectively. Digital literacy encompasses the ability to navigate the internet, use software applications, understand digital security, and critically evaluate online information.
- **Accessibility:** Accessibility refers to the design of digital tools and platforms that can be used by everyone, including people with disabilities. This includes features like screen readers for the visually impaired, voice recognition software, and keyboard accessibility for those with motor impairments. Websites and applications should adhere to accessibility standards such as the Web Content Accessibility Guidelines (WCAG).





Challenges to e-Access

Several challenges hinder the realization of equitable e-Access:

1. **Digital Divide:** The disparity between those who have access to digital technologies and those who do not is known as the digital divide. This divide is often along socio-economic, geographic, and demographic lines. Bridging this gap requires targeted efforts and investments in infrastructure and education.

2. Educational Opportunities:

e-Access allows individuals to access educational resources, participate in online learning, and improve their skills, leading to better job prospects and personal development.

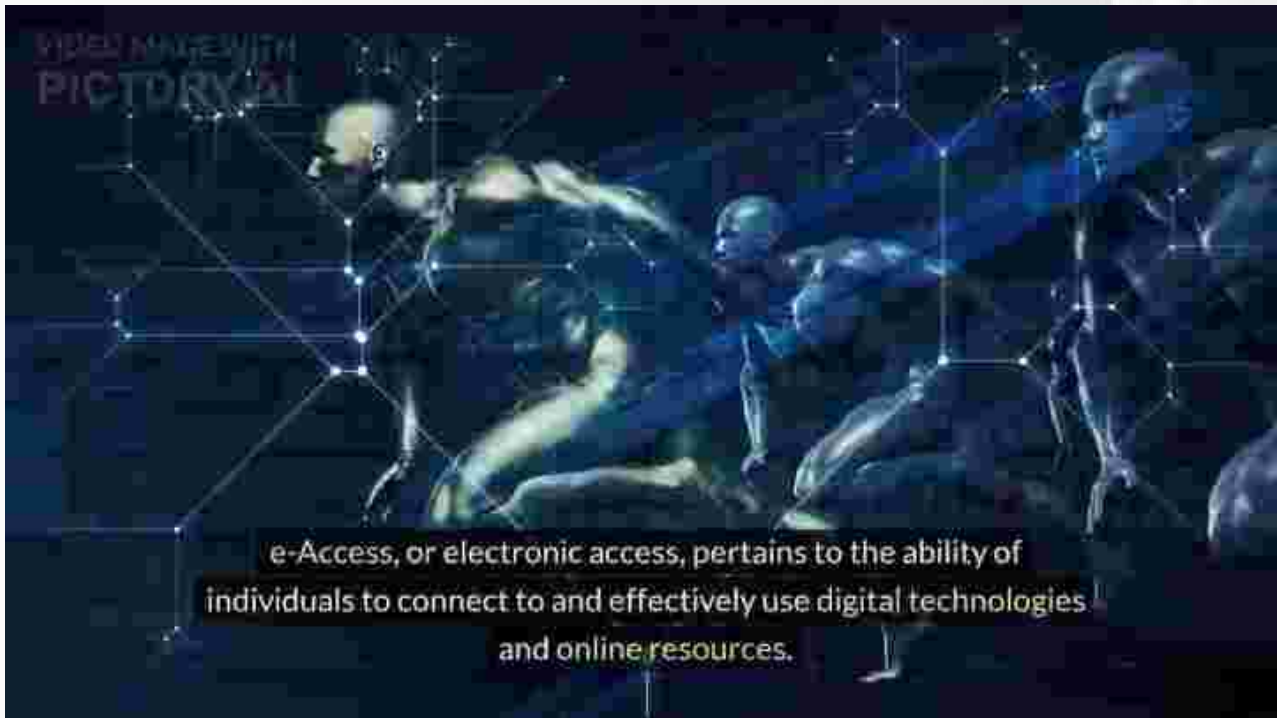
3. **Social Inclusion:** Digital access helps individuals stay connected with family and friends, participate in social and civic activities, and access essential services such as healthcare and government assistance.

Importance of e-Access

Ensuring e-Access is crucial for several reasons:

1. **Economic Growth:** Access to digital tools and the internet can drive economic growth by enabling new business opportunities, enhancing productivity, and creating jobs.
2. **Educational Opportunities:** e-Access allows individuals to access educational resources, participate in online learning, and improve their skills, leading to better job prospects and personal development.
3. **Social Inclusion:** Digital access helps individuals stay connected with family and friends, participate in social and civic activities, and access essential services such as healthcare and government assistance.
4. **Empowerment:** e-Access empowers individuals by providing them with information and tools to make informed decisions, advocate for their rights, and participate in the digital economy.





What is e-Access

In conclusion, e-Access is a multifaceted concept that is essential for achieving digital inclusion and equity. By addressing the challenges and promoting universal access to digital technologies, we can ensure that everyone has the opportunity to participate fully in the digital age.

1.2.2 e-Literacy

e-Literacy, or electronic literacy, refers to the set of skills and knowledge necessary to effectively and responsibly use digital technologies. In the context of digital etiquette, e-Literacy is essential as it equips individuals with the capabilities to navigate the digital world safely, efficiently, and respectfully.



Understanding e-Literacy

e-Literacy encompasses a broad range of competencies, including:

- **Basic Computer Skills:** The ability to operate computers and digital devices, including using operating systems, navigating file systems, and utilizing basic software applications such as word processors and web browsers.
- **Internet Navigation:** Understanding how to effectively search for information online, use search engines, and discern credible sources from unreliable ones.

- **Digital Communication:** Proficiency in using digital communication tools such as email, social media, and instant messaging. This includes understanding the etiquette of online communication, such as being concise, respectful, and aware of tone and context.
- **Digital Content Creation:** Skills related to creating and sharing digital content, including writing blog posts, creating videos, and using graphic design software. This also involves understanding copyright laws and respecting intellectual property.
- **Cybersecurity Awareness:** Knowledge of basic cybersecurity principles to protect personal information and digital devices from threats like viruses, phishing, and hacking. This includes understanding how to use strong passwords, recognize phishing attempts, and use security software.
- **Privacy Management:** Understanding how to manage and protect one's privacy online. This includes knowing how to use privacy settings on social media, understanding data protection laws, and being aware of the implications of sharing personal information online.





Challenges to e-Literacy

Several challenges hinder the realization of equitable e-Literacy:

1. **Access to Education:** Not everyone has access to the educational resources needed to develop e-Literacy skills. Addressing this requires investment in educational programs and resources, especially in underserved communities.

2. **Rapid Technological Changes:** The fast pace of technological advancements can make it challenging for individuals to keep their skills up-to-date. Continuous learning and adaptation are necessary to maintain e-Literacy.
3. **Lack of Awareness:** Some individuals may not recognize the importance of e-Literacy or may not be aware of the resources available to improve their skills.

Importance of e-Literacy in Digital Etiquette

1. **Enhanced Communication:** e-Literacy improves the quality of digital communication by enabling individuals to express themselves clearly and effectively.
2. **Informed Decision-Making:** With the ability to evaluate online information critically, individuals can make informed decisions based on credible sources. .
3. **Cybersecurity:** e-Literate individuals are better equipped to protect themselves from online threats. Knowledge of cybersecurity practices helps prevent identity theft, data breaches, and other cybercrimes, contributing to a safer digital environment for everyone..
4. **Digital Citizenship:** e-Literacy fosters responsible digital citizenship. It encourages individuals to use digital technologies ethically, respect others' rights and privacy, and contribute positively to the online community. .





What is e-Literacy

In conclusion, e-Literacy is a critical component of digital etiquette, enabling individuals to navigate the digital world safely, effectively, and responsibly. By promoting e-Literacy, we can foster more respectful, informed, and secure online interactions, contributing to a healthier digital ecosystem.

1.2.3 e-Safety

e-Safety, or electronic safety, refers to the practice of using digital technologies in a manner that ensures the safety, security, and well-being of individuals while online. In the context of digital etiquette, e-Safety involves adopting behaviors and practices that protect oneself and others from various online threats, including cyberbullying, phishing, and data breaches.

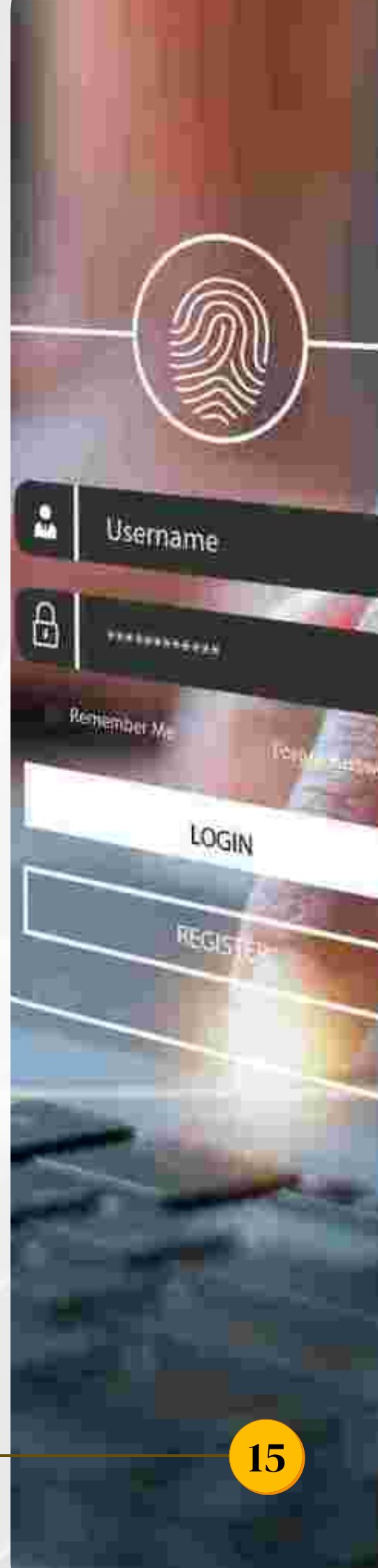


Understanding e-Safety

e-Safety encompasses several critical areas:

- **Personal Information Protection:** Safeguarding personal data such as names, addresses, phone numbers, and financial information is essential. Users should be aware of privacy settings on social media, understand the importance of strong passwords, and recognize the risks of sharing too much information online.

- **Cyberbullying Prevention:** Cyberbullying involves the use of digital platforms to harass, threaten, or demean others. Promoting respectful communication, reporting abusive behavior, and supporting victims are crucial steps in preventing and addressing cyberbullying.
- **Safe Online Communication:** Practicing safe communication involves being cautious about whom you interact with online. It includes not engaging with strangers, being wary of unsolicited messages, and knowing how to block and report suspicious or harmful contacts.
- **Recognizing Scams and Phishing Attempts:** Phishing is a common technique used by cybercriminals to deceive individuals into providing sensitive information. Recognizing phishing emails and messages, not clicking on suspicious links, and verifying the authenticity of requests for personal information are vital e-Safety practices.
- **Secure Online Transactions:** When conducting financial transactions online, it is crucial to use secure websites (indicated by HTTPS in the URL) and reputable payment systems. Users should also regularly monitor their bank statements for unauthorized transactions.





Challenges to e-Safety

1. **Lack of Awareness:** Many individuals are not fully aware of the risks associated with online activities and the necessary steps to protect themselves.

2. **Rapid Technological Changes:** The fast-paced evolution of digital technologies can outstrip the ability of users to stay informed about new threats and protective measures.

3. **Accessibility of Security Tools:**

Not all users have access to advanced security tools or know how to use them effectively. Ensuring that security features are user-friendly and widely available is important..

4. **Cybercrime Sophistication:**

Cybercriminals are constantly developing new methods to bypass security measures. Staying ahead of these threats requires ongoing vigilance and updates to security protocols.

Best Practices for e-Safety

1. **Use Strong, Unique Passwords:** Create complex passwords for different accounts and change them regularly. Consider using a password manager.
2. **Enable Two-Factor Authentication:** Add an extra layer of security to accounts by enabling two-factor authentication (2FA).
3. **Be Skeptical of Unsolicited Communications:** Avoid clicking on links or downloading attachments from unknown or suspicious sources.
4. **Educate Yourself and Others:** Stay informed about the latest e-Safety threats and best practices. Share this knowledge with friends and family.
5. **Report and Block Abusive Behavior:** Use the tools provided by digital platforms to report and block cyberbullying, harassment, and other abusive behaviors.





In conclusion, e-Safety is a vital aspect of digital etiquette that involves protecting oneself and others from online risks. By practicing and promoting e-Safety, individuals can contribute to a safer, more secure, and respectful digital environment.

1.2.4 e-Rules

e-Rules, or electronic rules, refer to the guidelines, regulations, and policies that govern behavior in digital spaces. These rules are essential for maintaining order, security, and respect online. Understanding and adhering to e-Rules is a fundamental aspect of digital etiquette, ensuring that individuals interact responsibly and legally in the digital world.



Understanding e-Rules

e-Rules encompass a variety of regulations and guidelines, including:

- **Terms of Service (ToS):** These are the rules and guidelines that users must agree to follow to use a digital service or platform. Terms of service outline acceptable behavior, prohibited activities, and the consequences of violations. Users should read and understand these terms to avoid unintentional breaches.

- **Privacy Policies:** Privacy policies explain how a digital service collects, uses, and protects user data. Understanding privacy policies helps users make informed decisions about sharing personal information and ensures that their data is handled appropriately.
- **Community Guidelines:** Many online communities, such as forums and social media platforms, have specific guidelines that dictate acceptable behavior. These guidelines often include rules against harassment, hate speech, and the sharing of inappropriate content.
- **Copyright and Intellectual Property Laws:** e-Rules also include laws that protect the rights of content creators. Users must respect copyright and intellectual property rights by not plagiarizing or sharing copyrighted material without permission.
- **Anti-Cyberbullying Policies:** Many digital platforms have policies in place to prevent and address cyberbullying. These policies outline what constitutes bullying behavior and the steps users can take to report and combat it.





Challenges in Adhering to e-Rules

1. **Lack of Awareness:** Many users do not fully understand the e-Rules of the platforms they use. This can lead to unintentional violations.
2. **Complexity of Regulations:** e-Rules, especially legal regulations like GDPR, can be complex and difficult to understand.
3. **Rapid Changes in Technology:** The fast-paced evolution of digital technologies means that e-Rules are constantly being updated. Staying informed about these changes can be challenging for users.
4. **Enforcement Issues:** While e-Rules exist, enforcement can be inconsistent. Digital platforms must ensure that rules are enforced fairly and transparently to maintain user trust.

Best Practices for Adhering to e-Rules

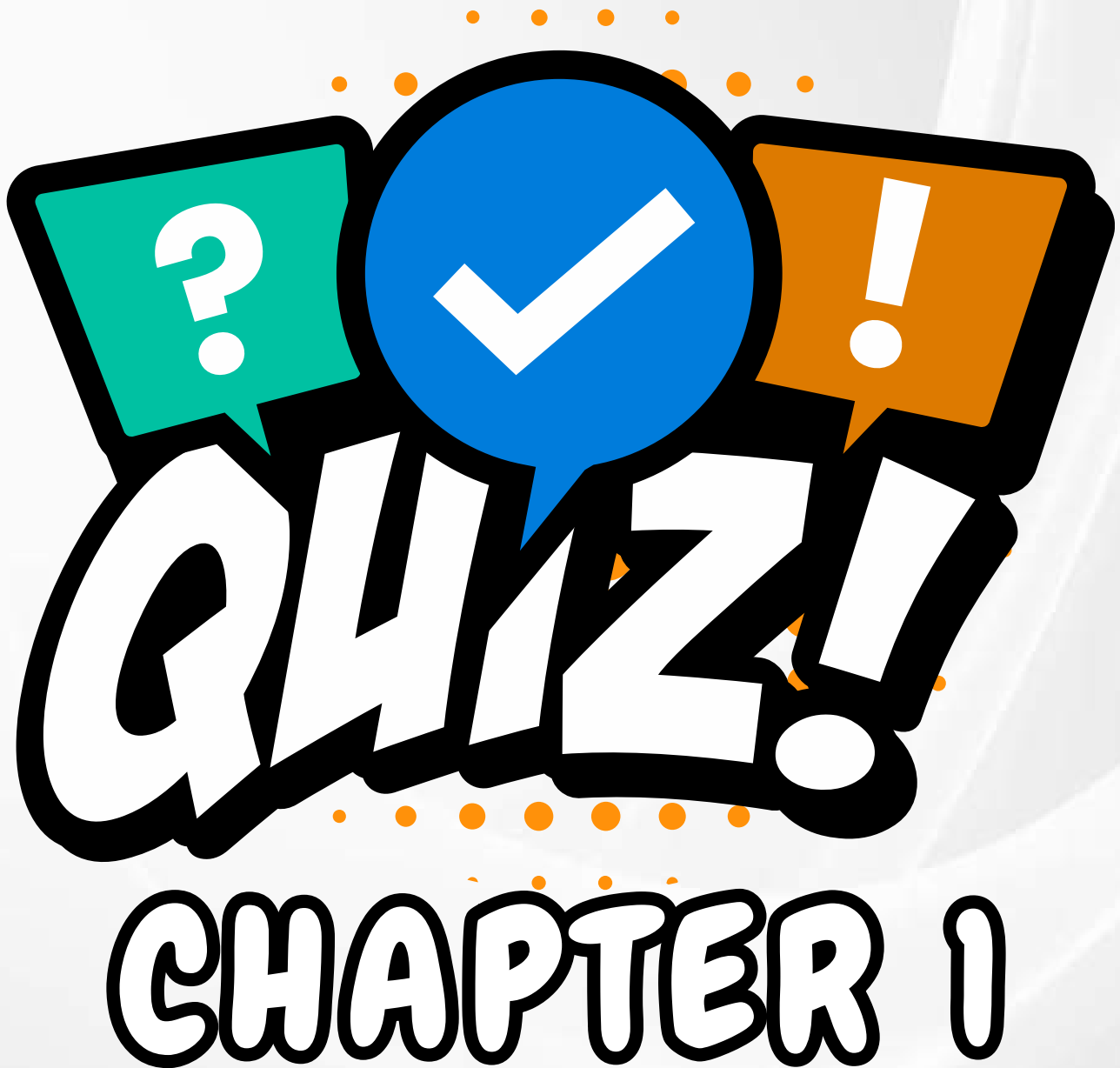
1. **Read and Understand Terms of Service:** Before using a digital platform, take the time to read and understand its terms of service and privacy policy. This helps avoid unintentional breaches of rules.
2. **Respect Community Guidelines:** Follow the community guidelines of online platforms to contribute to a positive environment. Report any violations you encounter.
3. **Protect Intellectual Property:** Always credit original creators and avoid sharing copyrighted material without permission. Use content under proper licenses.
4. **Be Aware of Privacy Practices:** Understand how your data is being used and take steps to protect your privacy, such as adjusting privacy settings and being cautious about the information you share.
5. **Report Abusive Behavior:** If you encounter cyberbullying or other abusive behaviors, use the reporting tools provided by the platform. Support others who may be victims of such behavior.

A close-up photograph of a hand holding a small, rectangular, light-colored sign. The sign has the words "FOLLOW THE RULES!" printed in bold, black, sans-serif capital letters. The background is slightly blurred, showing more of the hand and the sign's edges.

**FOLLOW
THE RULES!**



In conclusion, e-Rules are essential for maintaining a respectful, safe, and orderly digital environment. By understanding and adhering to these rules, users can protect themselves and others, fostering a positive and responsible digital community.

A graphic featuring three speech bubbles at the top: a teal one with a white question mark, a blue one with a white checkmark, and an orange one with a white exclamation mark. Below these, the word "QUIZ!" is written in a large, bold, white, stylized font with a thick black outline. Underneath "QUIZ!", the words "CHAPTER 1" are written in a similar bold, white, stylized font with a thick black outline. Small orange dots are scattered around the speech bubbles and the word "QUIZ!".

QUIZ!

CHAPTER 1

Quiz #1: Digital Etiquette

Sign in to keep track of your progress. [Sign in](#)

Digital etiquette includes being respectful and considerate of others' communication.

1 point

☒ True

☐ False

Posting negative comments or engaging in cyberbullying is acceptable in digital spaces.

1 point

☐ True

☒ False

Ignoring messages or emails without responding is a polite behavior in digital etiquette.

1 point

☐ True

☒ False

Sharing false information or spreading rumors online aligns with the concept of digital etiquette.

1 point

☐ True

☒ False

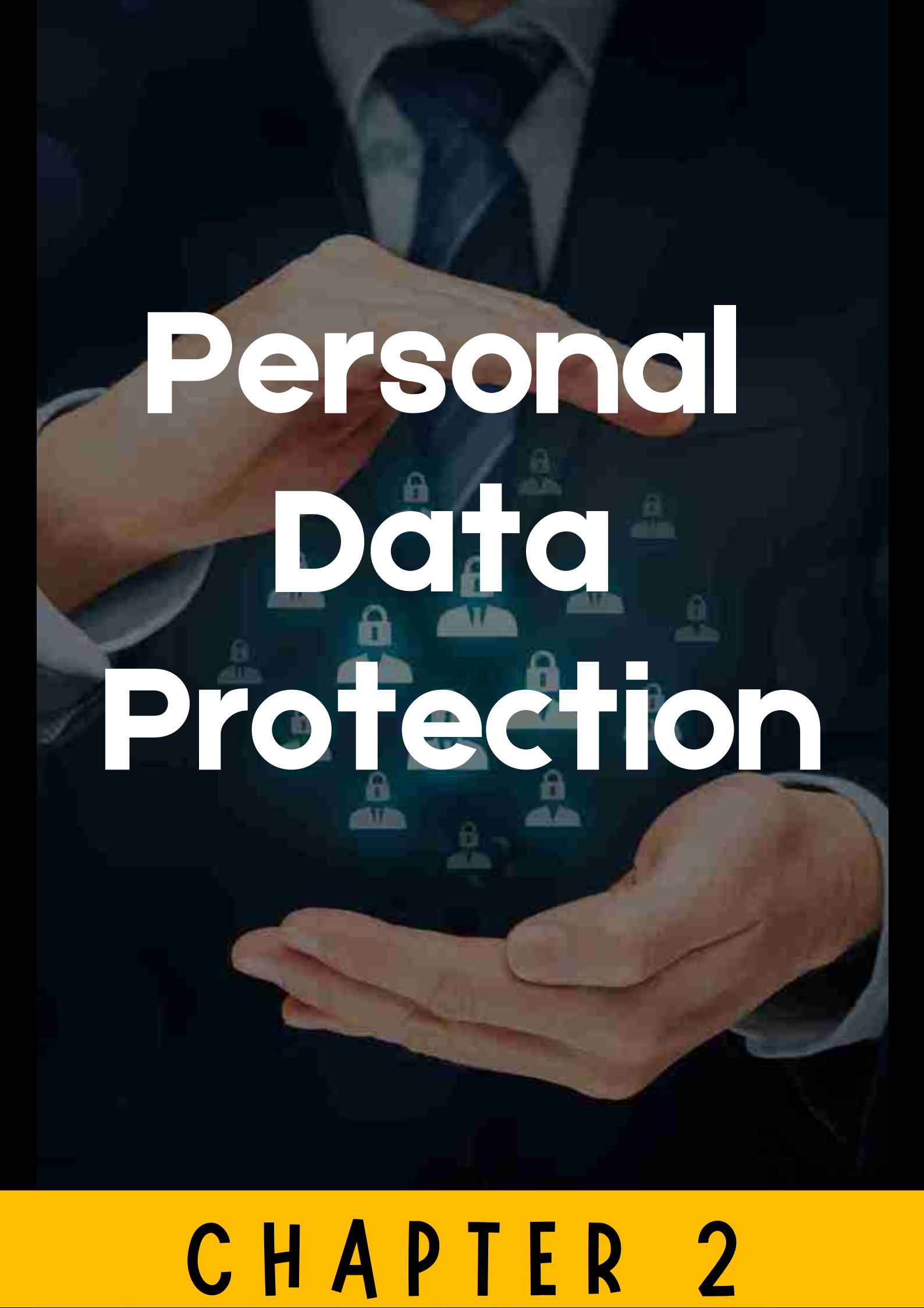
Submit

[Clear form](#)

Completed

You have correctly answered 0/5.

1

A person in a dark suit and blue tie is holding a transparent shield with both hands. The shield is covered with numerous small, light blue icons, each depicting a person's silhouette with a padlock on their chest, representing data protection. The background is dark and out of focus.

Personal Data Protection

CHAPTER 2

2.1 Describe Purpose and Legal Act of Personal Data Protection



Purpose of Personal Data Protection

Personal data protection is essential in today's digital age, where vast amounts of personal information are collected, stored, and processed by various organizations. The primary purposes of personal data protection include:

- **Safeguarding Privacy:** The foremost purpose of personal data protection is to safeguard individuals' privacy. Personal data often includes sensitive information such as names, addresses, financial details, and health records, which, if mishandled, can lead to privacy breaches and identity theft.

- **Empowering Individuals:** Data protection laws and practices empower individuals by giving them control over their personal information. This includes the right to know what data is being collected, the right to access their data, the right to correct inaccuracies, and the right to request deletion of their data.
- **Building Trust:** Organizations that prioritize data protection build trust with their customers and users. When people know that their personal data is handled responsibly and securely, they are more likely to engage with and trust the organization.
- **Preventing Misuse:** Data protection helps prevent the misuse of personal information for fraudulent activities, discriminatory practices, and other malicious purposes. It ensures that personal data is used ethically and only for legitimate purposes.
- **Ensuring Compliance:** Personal data protection laws require organizations to comply with specific regulations and standards, ensuring that they adopt best practices in data handling and security.



Legal Act Data Protection

Various legal acts and regulations around the world have been established to protect personal data. Some of the most significant ones include:

1. General Data Protection Regulation (GDPR):

The GDPR, implemented by the European Union in May 2018, is one of the most comprehensive data protection regulations globally. It applies to all organizations that process the personal data of EU residents, regardless of where the organization is based. Key provisions include:

- **Consent:** Organizations must obtain explicit consent from individuals before collecting their data.
- **Data Subject Rights:** Individuals have the right to access, correct, and delete their data.
- **Data Breach Notification:** Organizations must notify authorities and affected individuals of data breaches within 72 hours.



Legal Act Data Protection

2. California Consumer Privacy Act (CCPA):

Enacted in January 2020, the CCPA is a state-level regulation in the United States that grants California residents specific rights regarding their personal information. Key aspects include:

- **Right to Know:** Consumers have the right to know what personal data is being collected and how it is used.
- **Right to Delete:** Consumers can request the deletion of their personal information.
- **Right to Opt-Out:** Consumers can opt-out of the sale of their personal data.
- **Non-Discrimination:** Consumers exercising their CCPA rights cannot be discriminated against.

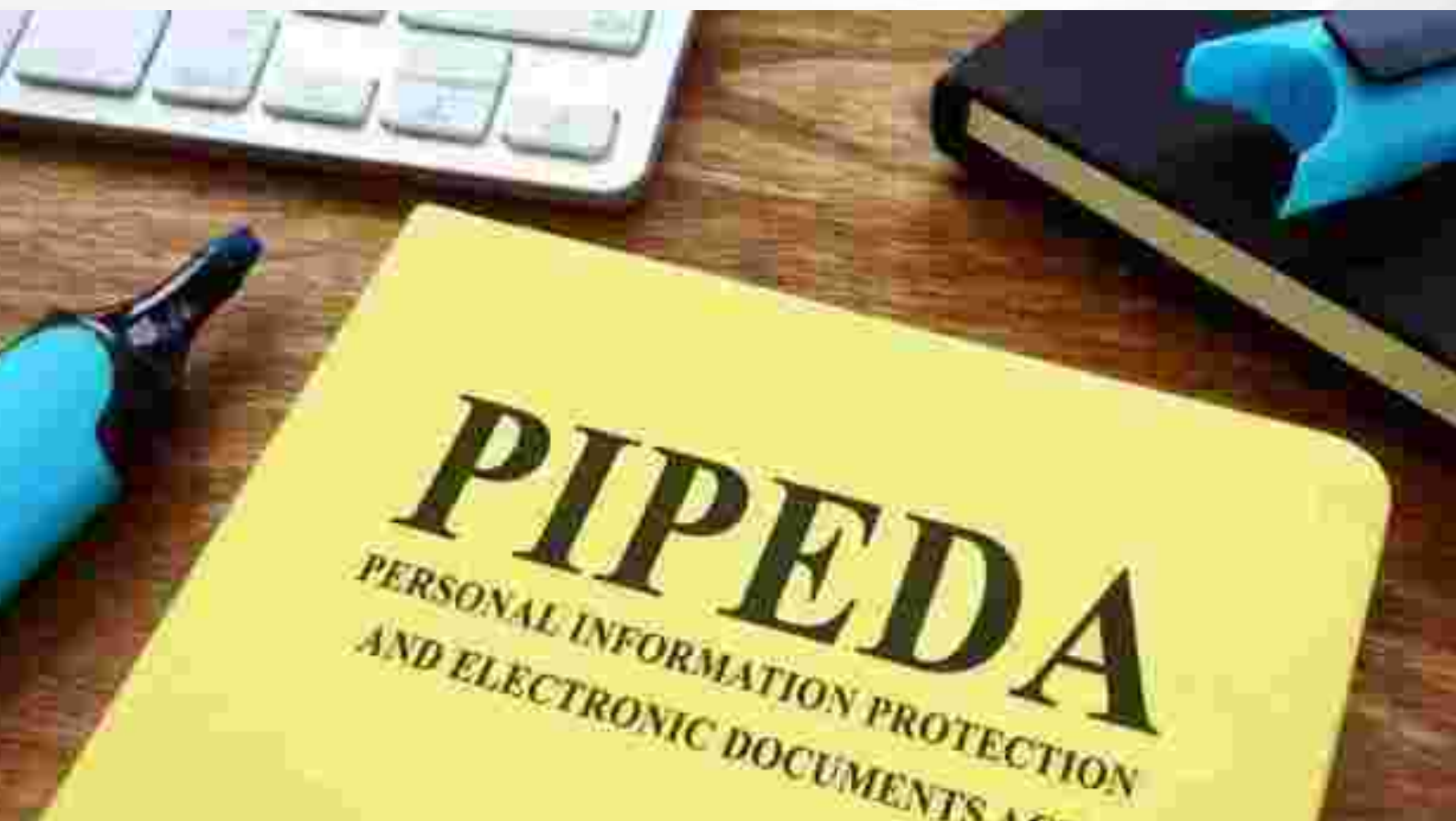


Legal Act Data Protection

3. Personal Information Protection and Electronic Documents Act (PIPEDA):

PIPEDA is Canada's federal privacy law for private-sector organizations, which sets the ground rules for how businesses must handle personal information. Key principles include:

- **Accountability:** Organizations must be accountable for the personal information they collect.
- **Identifying Purposes:** Organizations must identify the purposes for which personal data is collected.
- **Consent:** Individuals must consent to the collection, use, and disclosure of their personal information.
- **Safeguards:** Organizations must protect personal data with appropriate security measures.



Importance of Legal Acts in Personal Data Protection

Legal acts like GDPR, CCPA, and PIPEDA play a crucial role in personal data protection by:

- **Standardizing Practices:** They establish standardized practices for data protection that organizations must follow, ensuring consistency and reliability in how personal data is handled.
- **Enforcing Accountability:** These laws hold organizations accountable for protecting personal data, with significant penalties for non-compliance, thus incentivizing robust data protection measures.
- **Enhancing Transparency:** They promote transparency in how personal data is collected, used, and shared, allowing individuals to make informed decisions about their data.
- **Protecting Rights:** They protect the rights of individuals, giving them more control over their personal information and how it is used.





In conclusion, personal data protection serves to safeguard privacy, empower individuals, build trust, prevent misuse, and ensure compliance with legal standards. Legal acts like GDPR, CCPA, and PIPEDA are instrumental in enforcing these protections and establishing a secure digital environment.

2.2 Identify the Importance of Personal Data Protection

In the digital age, personal data protection has become increasingly important due to the vast amounts of information being collected, processed, and shared online. The significance of safeguarding personal data extends across multiple dimensions, impacting individuals, businesses, and society at large.



Here are the key reasons why personal data protection is crucial:

1. Preservation of Privacy

Privacy Rights: Protecting personal data is fundamental to preserving an individual's right to privacy. Privacy is a basic human right recognized in various legal frameworks.

Control Over Personal Information: Data protection laws empower individuals by giving them control over their personal information. This includes the right to access their data and decide how their data is used.

2. Protection Against Identity Theft and Fraud

Identity Theft: One of the most direct and harmful consequences of inadequate data protection is identity theft. When personal information such as social security numbers, credit card details, or login credentials are stolen, they can be used to commit fraud, causing financial and emotional distress to victims.

Fraud Prevention: Effective data protection measures help prevent fraud by ensuring that personal information is securely stored and handled.

3. Building Trust in Digital Services

Consumer Trust: Trust is a cornerstone of the digital economy. When businesses demonstrate a commitment to protecting personal data, they build trust with their customers. This trust is essential for fostering long-term relationships and encouraging the use of digital services.

Reputation Management: Data breaches and privacy scandals can severely damage an organization's reputation. By prioritizing data protection, businesses can safeguard their reputations and maintain the confidence of their stakeholders.



4. Compliance with Legal and Regulatory Requirements

Legal Obligations: Numerous laws and regulations, such as the General Data Protection Regulation (GDPR), mandate strict standards for data protection. Compliance with these laws is not only a legal obligation but also a critical component of ethical business practices.

Avoiding Penalties: Non-compliance with data protection laws can result in hefty fines and legal penalties. For instance, under the GDPR, organizations can be fined up to 4% of their annual global turnover for severe violations.

5. Enhancing Cybersecurity

Cybersecurity Measures: Personal data protection is closely linked to cybersecurity. Protecting personal data involves implementing strong cybersecurity measures to prevent unauthorized access, data breaches, and other cyber threats.

Resilience Against Attacks: A robust approach to data protection helps organizations become more resilient against cyber attacks. By securing personal data, they can reduce the risk of cyber incidents and ensure quicker recovery if breaches occur.

6. Ethical Responsibility and Corporate Social Responsibility

Ethical Responsibility: Beyond legal requirements, organizations have an ethical responsibility to protect the personal data of their customers, employees, and partners.

Corporate Social Responsibility: Protecting personal data is an integral part of corporate social responsibility.



In conclusion, the importance of personal data protection cannot be overstated. It is essential for preserving privacy, preventing identity theft and fraud, building trust in digital services, ensuring compliance with legal requirements, enhancing cybersecurity, and fulfilling ethical and corporate social responsibilities. As digital technologies continue to evolve, the need for robust data protection measures will only grow, making it imperative for individuals and organizations to prioritize the security and integrity of personal information.

2.3 Identify the Intrusion of Personal Data

The intrusion of personal data refers to unauthorized access, use, disclosure, or loss of personal information. Such intrusions can lead to serious consequences, including financial loss, identity theft, and reputational damage.



Here are the primary forms of personal data intrusion:

1. Data Breaches:

- **Hacking:** Exploiting software, network, or system vulnerabilities to access personal data.
- **Malware:** Malicious software, including viruses and ransomware, can infiltrate systems to steal or corrupt personal data.
- **Phishing:** Fraudulent emails, deceive individuals into revealing personal information, such as passwords or credit card numbers.

2. Insider Threats:

- **Malicious Insiders:** Employees or contractors misuse their access to personal data for personal gain, such as selling data on the black market.
- **Negligent Insiders:** Careless employees may unintentionally expose data by mishandling storage or sending sensitive information to the wrong recipient.

3. Physical Theft:

- **Stolen Devices:** Personal data is compromised if laptops, smartphones, or USB drives are stolen, especially if not encrypted.
- **Document Theft:** Physical documents with personal information can be stolen from offices, mailboxes, or improperly disposed of.

4. Data Exposure:

- **Misconfigured Databases:** Cloud services and databases may be incorrectly configured to allow public access, leading to data leaks.
- **Unsecured Networks:** Using unsecured Wi-Fi networks can expose data to interception by cybercriminals.



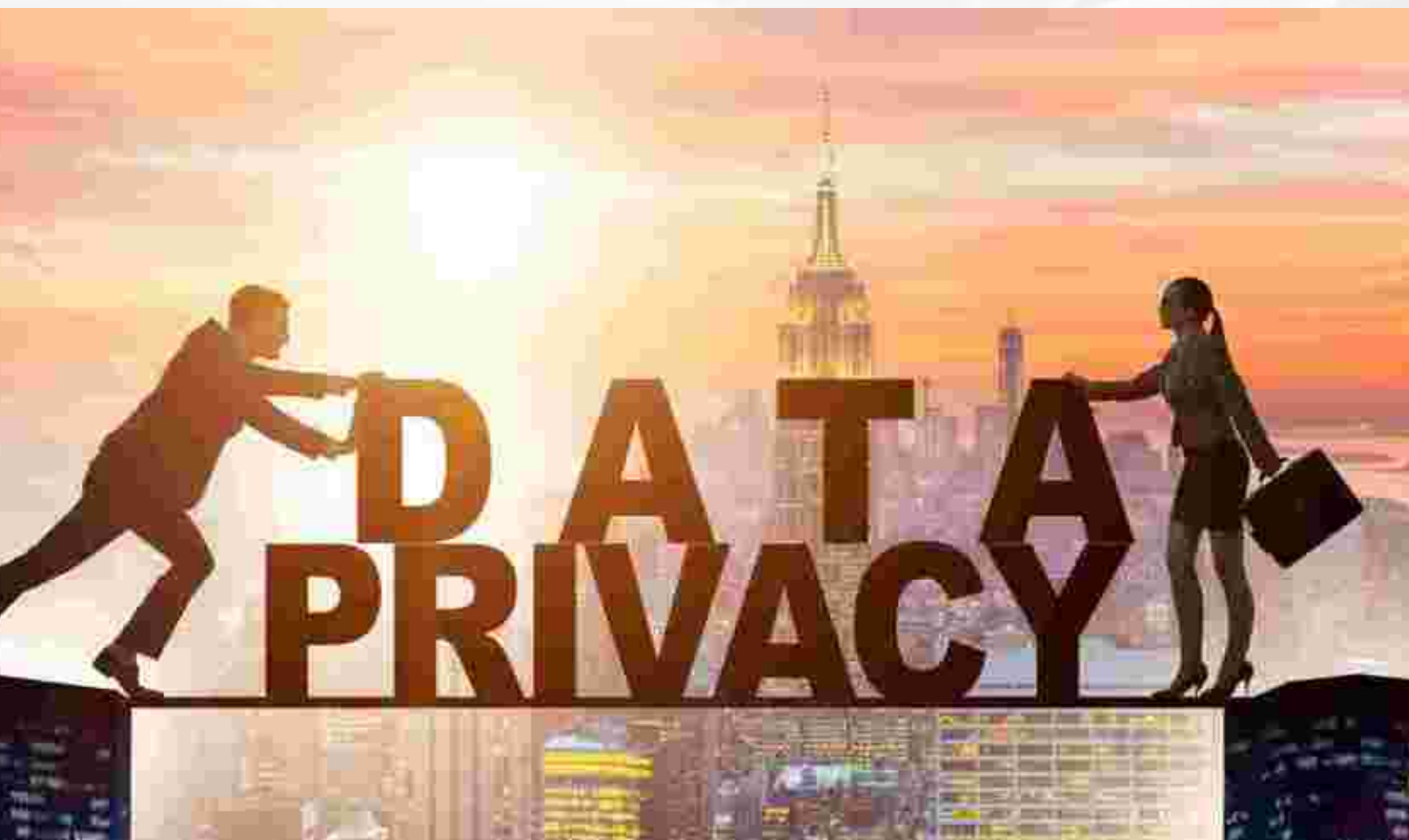
Consequences and Prevention

1. Consequences:

- Financial loss and identity theft
- Reputational damage for organizations
- Legal penalties for non-compliance with data protection laws
- Emotional distress for affected individuals

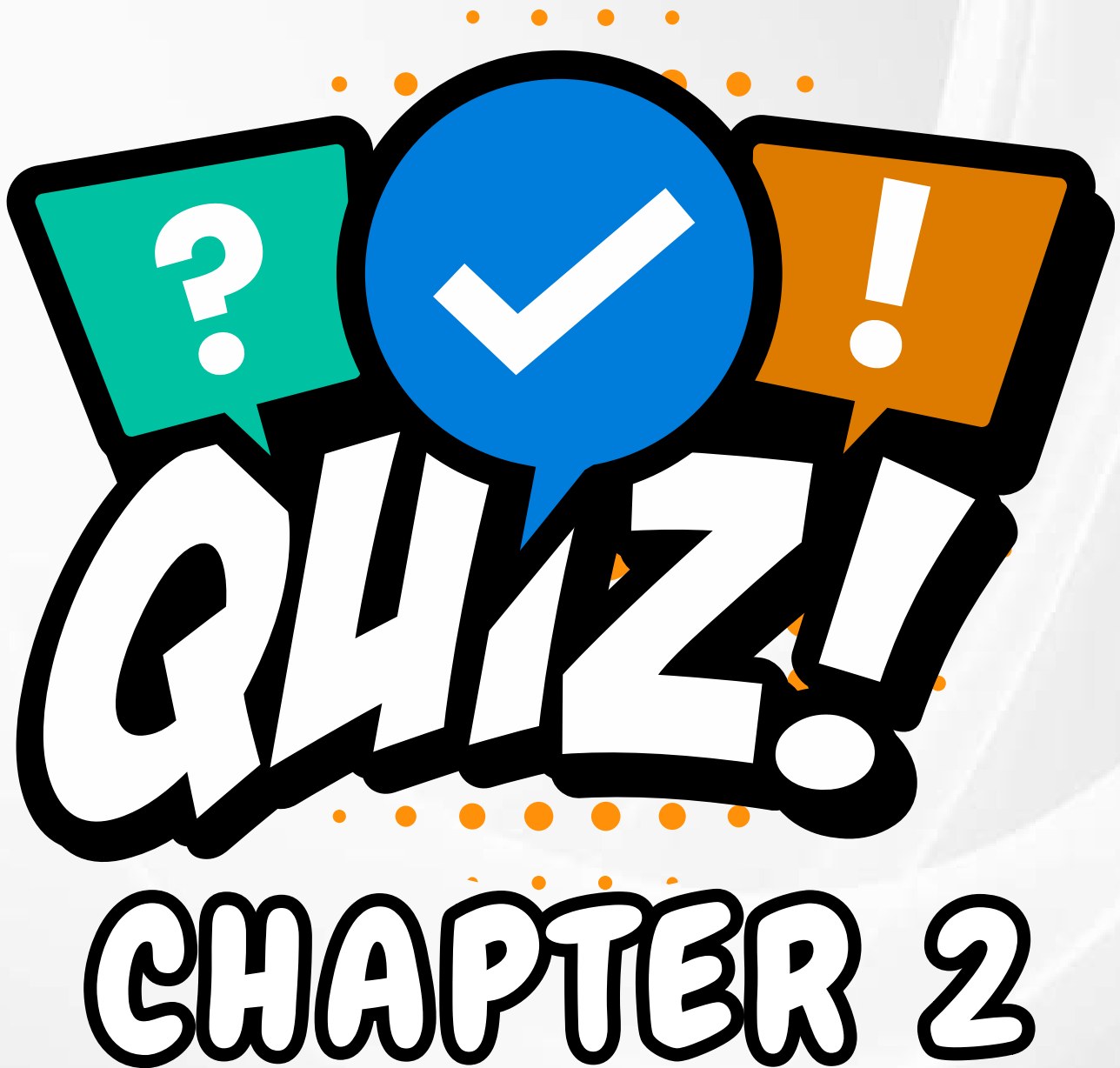
3. Prevention:

- Implement robust security practices like strong passwords and multi-factor authentication.
- Educate employees on data protection and phishing risks.
- Ensure physical security for sensitive data.
- Develop clear incident response plans to quickly address breaches.





In summary, personal data intrusion poses significant risks, and understanding its forms is crucial for implementing effective protection measures. By staying vigilant and proactive, individuals and organizations can safeguard personal information against unauthorized access and misuse.

A graphic featuring three speech bubbles at the top: a teal one with a white question mark, a blue one with a white checkmark, and an orange one with a white exclamation mark. Below these, the word "QUIZ!" is written in a large, bold, white, stylized font with a thick black outline. Underneath "QUIZ!", the words "CHAPTER 2" are written in a similar bold, white, stylized font with a thick black outline. Orange dots are scattered around the speech bubbles and the word "QUIZ!".

QUIZ!

CHAPTER 2

Quiz #2: Personal Data Protection

[Sign Up](#) | [Log in](#) or [Join our community](#) | [Feedback](#)

Personal data protection laws only apply to big corporations.

Answer

- ☐ True
- ☐ False

Anonymized data is considered personal data under data protection laws.

Answer

- ☐ True
- ☐ False

Individuals have the right to request access to their personal data held by organizations.

Answer

- ☐ True
- ☐ False

Data protection regulations do not apply to information shared on social media.

Answer

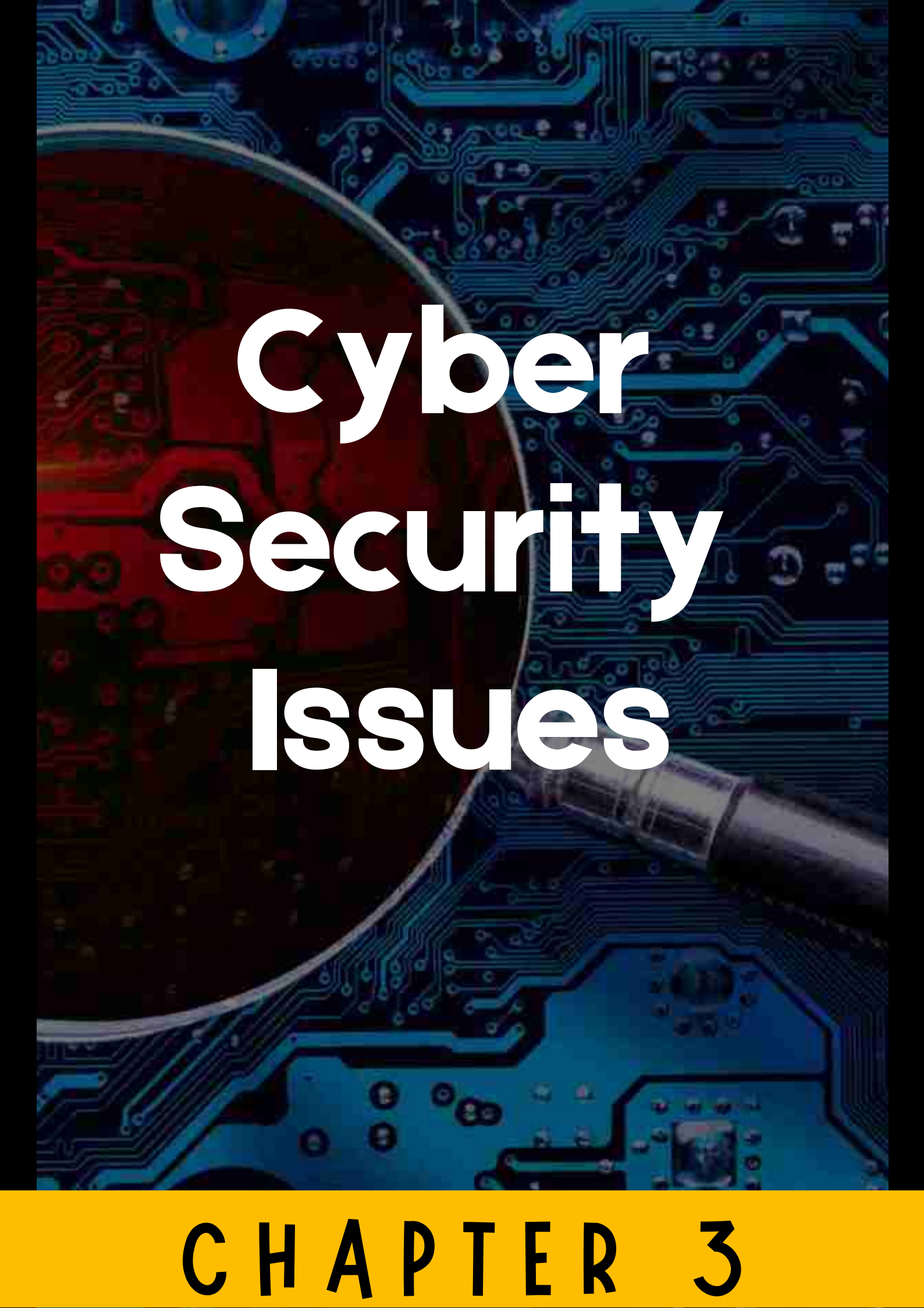
- ☐ True
- ☐ False

Submit

Clear form

Google Forms

This form can receive up to 1000 responses

The background of the slide is a close-up, high-contrast image of a computer circuit board. The board is primarily blue with intricate white and silver circuit traces. A large, semi-transparent red circle is overlaid on the left side of the image. A silver pen tip is visible in the lower right quadrant, pointing towards the center of the red circle. The text 'Cyber Security Issues' is centered over the image in a large, white, sans-serif font.

Cyber Security Issues

CHAPTER 3

3.1 Describe the Concept and Legal Act of Cyber Security

Cyber security involves protecting systems, networks, and programs from digital attacks aimed at accessing, changing, or destroying sensitive information, extorting money, or disrupting operations.

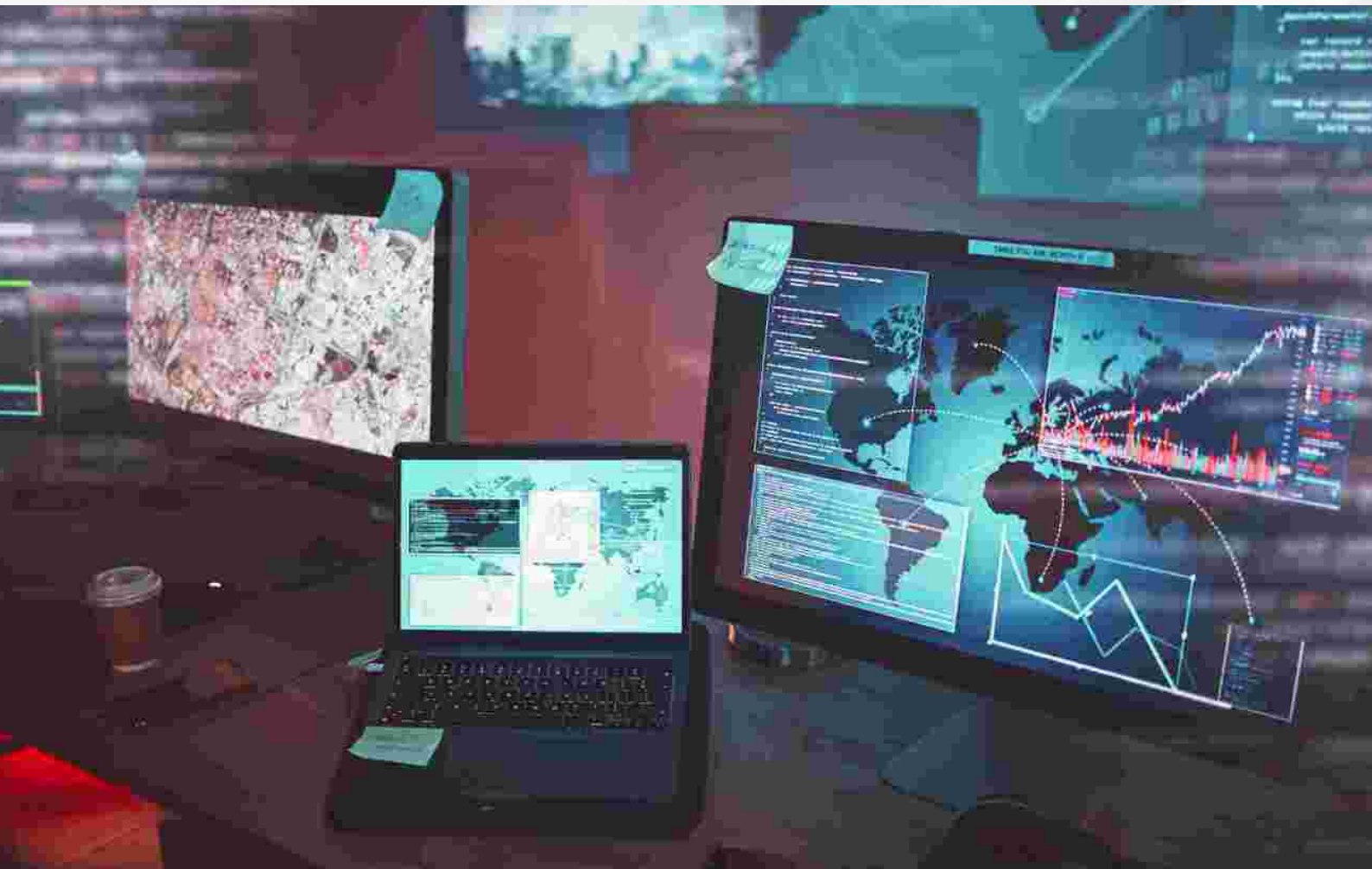


Key aspects include:

- **Confidentiality:** Ensuring information is accessible only to authorized individuals.
- **Integrity:** Maintaining the accuracy and completeness of data.
- **Availability:** Ensuring that information and systems are accessible when needed.

Cyber security encompasses several components:

- **Network Security:** Safeguarding the network infrastructure from unauthorized access and misuse.
- **Application Security:** Protecting software from threats.
- **Information Security:** Ensuring data integrity and privacy.
- **Operational Security:** Managing how data is handled and protected.
- **End-user Education:** Teaching best practices to users, like not clicking on unknown links.



Legal Acts of Cyber Security

General Data Protection Regulation:

- Requires organizations to implement data protection measures and report breaches within 72 hours.
- Enhances accountability and promotes robust data protection.

Network and Information Security (NIS) Directive:

- Applies to essential services and digital service providers.
- Mandates appropriate security measures and incident reporting.

Personal Information Protection and Electronic Documents Act:

- Governs the handling of personal information by private sector organizations.
- Requires security safeguards against unauthorized access and disclosure.

Health Insurance Portability and Accountability Act:

- Protects patient data in healthcare.
- Requires secure practices to ensure confidentiality and integrity of health information.

Importance of Cyber Security Legal Acts

- **Standardization:** Legal acts provide a framework that standardizes cyber security practices across industries and regions.
- **Accountability:** These laws hold organizations accountable for the security of the data they manage.
- **Consumer Confidence:** Strict data protection regulations help build and maintain consumer trust.
- **Global Coordination:** Cyber security threats often transcend national borders, making international cooperation essential.
- **Risk Mitigation:** By enforcing robust security practices, legal acts help organizations mitigate risks associated with cyber attacks.
- **Innovation and Economic Stability:** Ensuring a secure cyber environment promotes innovation and economic stability.
- **Protection of Sensitive Information:** Legal acts ensure that sensitive information, such as personal, financial, and health data, is adequately protected.





Cyber security is a critical aspect of modern digital infrastructure, aimed at protecting systems, networks, and data from cyber threats. Legal acts like GDPR, CISA, the NIS Directive, HIPAA, and PIPEDA play a vital role in establishing standards, ensuring compliance, and enhancing overall security posture. By understanding and adhering to these regulations, organizations can better protect themselves and their stakeholders from the ever-evolving landscape of cyber threats. These legal frameworks not only provide a foundation for secure digital practices but also promote a culture of accountability and trust in the digital ecosystem.

3.2 Identify the Effect of Cyber Crimes on a Particular Sector

Cyber crimes impact a wide array of sectors, each facing unique challenges and repercussions. The effects of cyber crimes extend beyond immediate financial losses, influencing operational stability, reputational integrity, regulatory compliance, and even national security.



1. Financial Loss

- **Direct Theft and Fraud:** Cyber criminals often steal money directly from businesses and individuals through methods like phishing, hacking, and unauthorized transactions.
- **Ransomware Payments:** Many organizations pay ransoms to regain access to their data, adding to their financial burdens. Even when they choose not to pay, the cost of data recovery and system restoration can be substantial.

2. Operational Disruptions

- **Downtime and Productivity Loss:** Cyber attacks can cripple business operations by shutting down critical systems. This downtime translates to lost productivity and revenue, especially in sectors like manufacturing, where continuous operation is crucial.
- **Supply Chain Disruption:** Attacks targeting supply chains can have a ripple effect, delaying production and delivery schedules, causing a loss of business, and damaging relationships with suppliers and customers.

3. Reputational Damage

- **Erosion of Trust:** Customers and partners may lose trust in a business that fails to protect their data. This loss of confidence can lead to a decline in customer base and difficulties in establishing new business relationships.
- **Negative Publicity:** High-profile breaches often attract media attention, damaging the public perception of the affected organization. This can have long-term effects on brand reputation and market position.

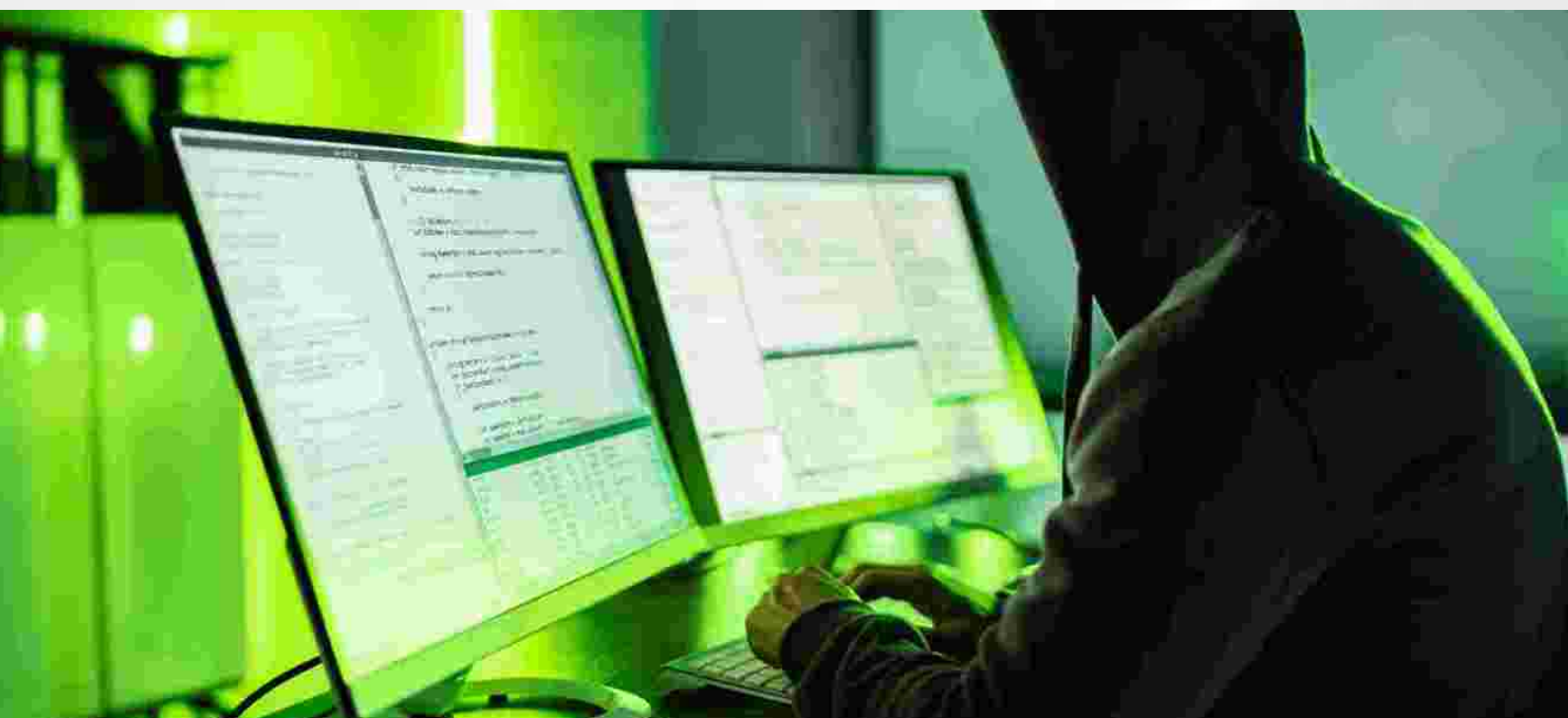


4. Compliance and Legal Risks

- **Regulatory Fines:** Non-compliance with data protection laws like GDPR, HIPAA, and PCI DSS can result in substantial fines.
- **Litigation:** Victims of data breaches may sue organizations for failing to protect their personal information.

5. National Security Threats

- **Critical Infrastructure Attacks:** Cyber attacks on critical infrastructure, such as power grids, water supplies, and transportation systems, can threaten national security and public safety. These sectors are increasingly targeted due to their essential role in society.
- **Espionage:** State-sponsored cyber attacks aimed at stealing sensitive government or corporate information pose a significant threat to national security and economic stability.





Cyber crimes have far-reaching effects across financial, operational, reputational, and legal domains. The increasing sophistication of cyber threats necessitates robust security measures, proactive risk management, and adherence to regulatory standards to mitigate these risks and protect organizational and national interests.

3.3 Identify Issues in Hacking, Fake News, and Identity Theft

Cyber crimes such as hacking, fake news dissemination, and identity theft pose significant challenges across various sectors, affecting individuals, businesses, and society at large.

3.3.1 Hacking

- **Data Breaches:** Hackers often infiltrate systems to steal sensitive information, including personal data, financial details, and intellectual property. High-profile breaches can lead to significant financial losses, legal penalties, and reputational damage.
- **System Disruption:** Hacking can disrupt critical services and operations, from corporate networks to public infrastructure. This disruption can cause operational downtime, loss of productivity, and severe economic impact.
- **Cyber Espionage:** Hackers, particularly those sponsored by states, may engage in cyber espionage to gather confidential information from government agencies or corporations, threatening national security and competitive business advantages.

3.3.2 Fake News

- **Misinformation:** The spread of fake news can mislead the public, creating confusion and panic. It can distort public perception and influence behaviors based on false information.
- **Political Manipulation:** Fake news can be used to manipulate political outcomes, sway public opinion, and interfere in elections. This undermines democratic processes and erodes trust in political institutions.
- **Reputational Harm:** Businesses and individuals targeted by fake news may suffer reputational damage. False reports can lead to a loss of customer trust and a decline in market value.



3.3.3 Identity Theft

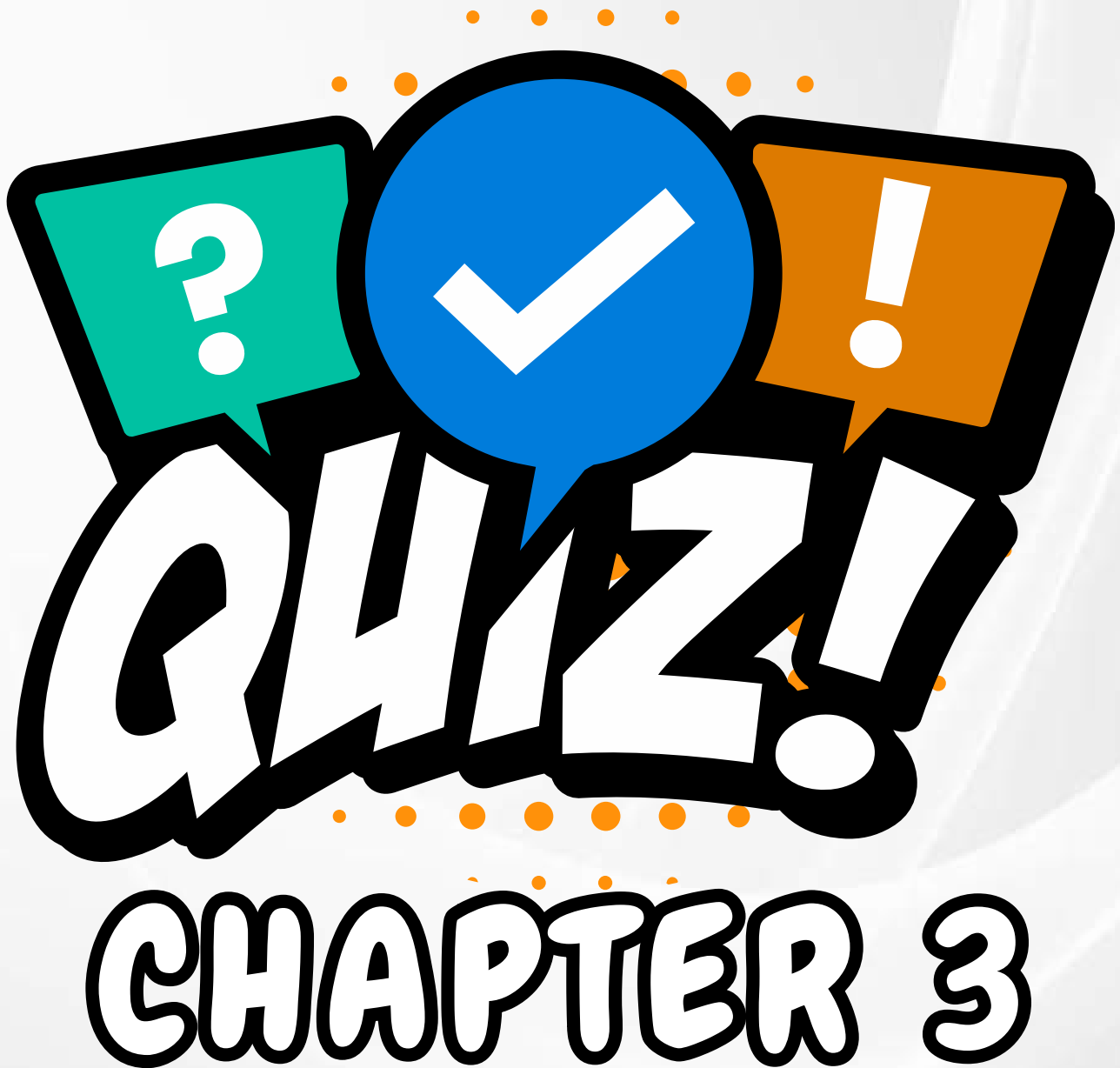
- **Financial Fraud:** Identity theft can result in unauthorized transactions, drained bank accounts, and fraudulent credit card charges. Victims often face long and complex processes to recover their financial stability.
- **Personal Impact:** Victims of identity theft may experience emotional distress and a prolonged sense of vulnerability. The process of restoring one's identity can be time-consuming and stressful.
- **Business Risk:** Companies that handle sensitive customer information must implement robust security measures to prevent identity theft. A failure to protect this data can lead to legal liabilities and a loss of consumer trust.



IDENTITY
THEFT



Hacking, fake news, and identity theft present significant issues in the digital age. They threaten financial stability, operational efficiency, personal security, and societal trust. Addressing these challenges requires comprehensive cyber security strategies, public awareness, and strict regulatory measures to safeguard against these pervasive threats. Implementing robust security protocols, educating the public on recognizing misinformation, and enhancing legal frameworks to combat identity theft are crucial steps in mitigating the impact of these cyber crimes.

A graphic featuring three speech bubbles at the top: a teal one with a white question mark, a blue one with a white checkmark, and an orange one with a white exclamation mark. Below these, the word "QUIZ!" is written in a large, bold, white, stylized font with a thick black outline. Underneath "QUIZ!", the words "CHAPTER 3" are written in a similar bold, white, stylized font with a thick black outline. Orange dots are scattered around the speech bubbles and the word "QUIZ!".

QUIZ!

CHAPTER 3

Quiz #3: Cyber Security Issues

Signed in as [Gediminas](#) | [Log out](#) | [My profile](#) | [My progress](#)

Using public Wi-Fi networks is completely safe and does not pose any cybersecurity risks.

Answer

☐ True

☒ False

Creating strong and unique passwords for different accounts is not important for cybersecurity.

Answer

☐ True

☒ False

Phishing is a cyber attack method where attackers trick individuals into providing sensitive information.

Answer

☐ True

☒ False

Multi-factor authentication is not an effective way to enhance cybersecurity.

Answer

☐ True

☒ False

CONCLUSION

As we traverse the ever-evolving digital landscape, understanding and practicing digital etiquette becomes increasingly crucial. This book has provided a comprehensive exploration of the principles that underpin respectful and responsible online behavior. We've delved into critical areas such as e-access, ensuring everyone has equal opportunities to participate online; e-literacy, equipping individuals with the skills to navigate and create digital content responsibly; e-safety, protecting ourselves and others from digital threats; and e-rules, adhering to the norms and regulations governing online interactions.

Moreover, the significance of personal data protection and the impact of cyber security issues such as hacking, fake news, and identity theft have been underscored. By adhering to these principles, we can protect our personal information, safeguard against cyber threats, and foster a respectful digital community.

Practicing digital etiquette not only enhances our online interactions but also builds a foundation of trust and respect within the digital community. As we move forward, it is imperative to continue educating ourselves and others about the importance of digital etiquette. By doing so, we contribute to a safer, more inclusive, and more respectful online environment, ensuring that our digital world is a place where everyone can interact positively and securely.

References

- 1 - What is Netiquette?
<https://www.webroot.com/us/en/resources/tips-articles/netiquette-and-online-ethics-what-are-they>
- 2 - What is Netiquette? 20 Internet Etiquette Rules
<https://www.kaspersky.com/resource-center/preemptive-safety/what-is-netiquette>
- 3 - Evaluating News: Digital Etiquette
<https://libguides.trschools.k12.wi.us/evaluatingnews/netiquette>

Discover our interactive eBook



eISBN 978-967-0047-88-1



9 789670 047881