PRIVACY
TECHNOLOGY-BASED SOLUTIONS FOR PRIVACY PROTECTION

GROUP 9

BAGONGON, BOMBEO, CALIPES, NOJA, ROMEO

OBJECTIVES

01 UNDERSTAND

To understand what is technology-based solutions for privacy protection

02 TO KNOW

To know the different technology-based solutions for privacy protection

03 EXPLAIN

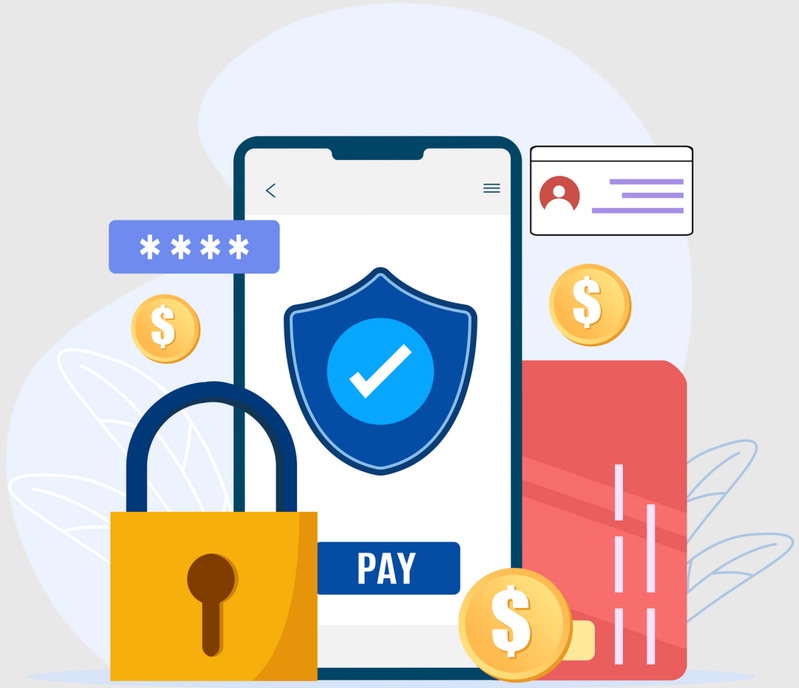
To explain the importance

Privacy is a fundamental human right, and as our lives become increasingly digitized, protecting personal information has become a growing concern. **Technology-based solutions** play a crucial role in safeguarding privacy in the digital age.

Technology-based solutions for privacy protection

The use of various technological tools and strategies to safeguard individuals' personal information and maintain their privacy in an increasingly digital and data-driven world.

Technology-based solutions for privacy protection



Here are some key technology-based solutions for privacy protection:

1. ENCRYPTION

Encryption is the process of converting data into a code to prevent unauthorized access. It's a fundamental tool for privacy protection.

EXAMPLE

Secure Online Banking

SOME KEY **ENCRYPTION TECHNOLOGIES** INCLUDE:

End-to-End Encryption:

This ensures that only the sender and the intended recipient can read a message or access data. **Messaging apps** like WhatsApp and Signal use end-to-end encryption.

SOME KEY **ENCRYPTION TECHNOLOGIES** INCLUDE:

Transport Layer Security:

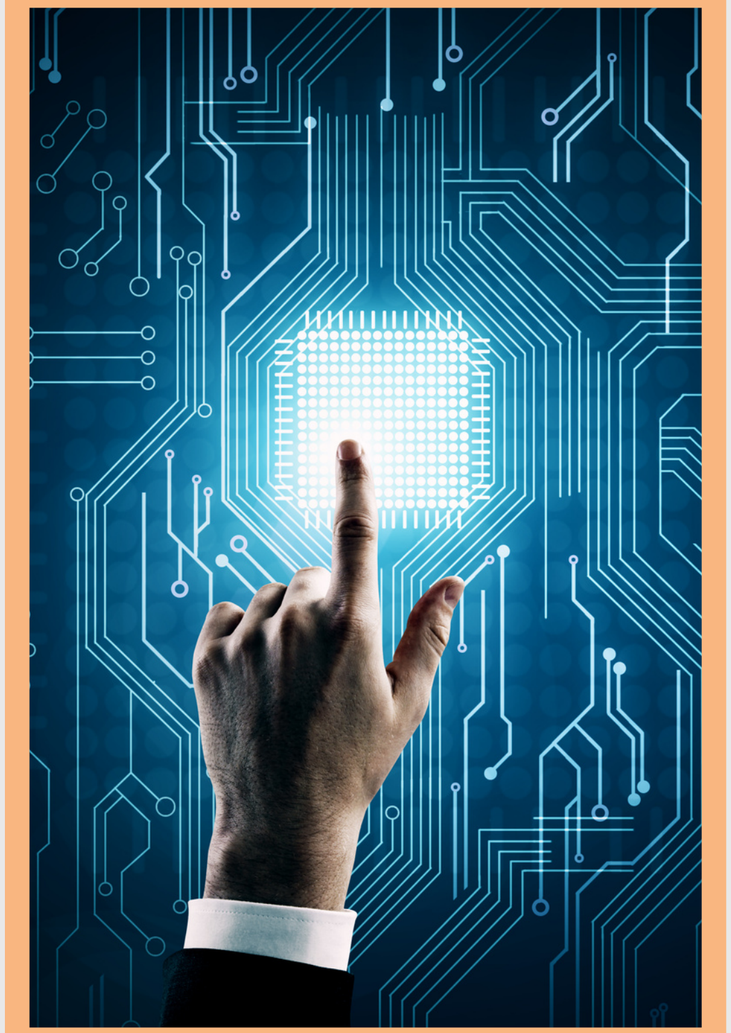
TLS secures internet connections, such as browsing and email, by encrypting data **transmitted between the user and the server.** It's recognizable by the "https://" in website URLs.

2. VIRTUAL PRIVATE NETWORKS (VPNS):

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data.

EXAMPLE OF HOW VPNS USED:

VPNs used to ensure confidentiality and security while working online from a **coffee shop** by protecting critical company information from risks linked to public Wi-Fi.



3. PRIVACY-FOCUSED BROWSERS

Several web browsers prioritize user privacy by blocking trackers and cookies. Examples include Mozilla Firefox, Brave, and Tor. These browsers offer enhanced privacy features like fingerprint protection and ad-blocking.

4. TWO-FACTOR AUTHENTICATION (2FA)

2FA adds an extra layer of security by requiring users to provide two forms of verification before gaining access to their accounts. This could be something they know (password) and something they have (e.g., a mobile app code).

5. Biometric Authentication

Biometric technologies, such as fingerprint and facial recognition, provide a secure and convenient way to access devices and accounts. They are challenging to fake or steal compared to traditional passwords.

6. PRIVACY-ENHANCING TOOLS

Tools like password managers, email encryption services like ProtonMail, and privacy-focused search engines like DuckDuckGo, help individuals protect their online presence. .

7.PRIVACY-PRESERVING CRYPTOCURRENCIES

Cryptocurrencies like Monero and Zcash offer enhanced privacy features, making it difficult to trace transactions and balances, unlike Bitcoin, which is more transparent

8. Data Minimization

Data minimization is the practice of collecting and storing only the necessary information required for a specific purpose, rather than gathering extensive user data. By implementing data minimization, companies can protect privacy and reduce the risk of data breaches.

Data Minimization Principles

Adequate

all collected data is sufficient to meet your stated objectives

Relevant

collected data is rationally linked to the objectives

Limited

no unnecessary data is collected or stored

Timely

data is periodically reviewed and removed when unnecessary

9.Blockchain Technology

Blockchain technology is a decentralized and immutable ledger that enhances data security and privacy. It consists of a chain of blocks, where each block contains a list of transactions. Once a block is added to the chain, it cannot be altered, ensuring the integrity of the data.

BENEFITS OF
Blockchain Technology

1. **Decentralization**: Blockchain operates on a decentralized network of computers, eliminating the need for a central authority (like a bank).
2. **Immutability:** Once data is recorded in a blockchain, it cannot be easily altered or deleted.
3. **Security:** Blockchain uses advanced cryptographic techniques to secure transactions. Each block is linked to the previous one, creating a secure chain.
4. **Accessibility:** Blockchain technology is accessible to anyone with an internet connection, fostering financial inclusion in regions with limited access to traditional banking services.
5. **Innovation:** Blockchain has the potential to revolutionize various industries, including finance, supply chain, healthcare, and more.

10. Privacy by Design:

This approach involves building privacy protections into the design of products and services from the beginning. It ensures that privacy is considered at every stage of development.

Conclusion

In an era where personal information is constantly at risk, technology-based solutions are indispensable for safeguarding privacy. These solutions range from encryption and VPNs to privacy-focused browsers and biometric authentication. Additionally, the principles of data minimization and privacy by design are vital in building a privacy-centric digital world

Importance Technology-based solutions for privacy protection

Technology-based solutions for privacy protection like a digital shield that helps keep your personal information safe when you use the internet or digital services. These tools and practices are important because they stop bad actors, like hackers and companies that want to collect your data, from getting access to your private information

THANK YOU