DATA PRIVACY AND SECURITY 101 GUIDE

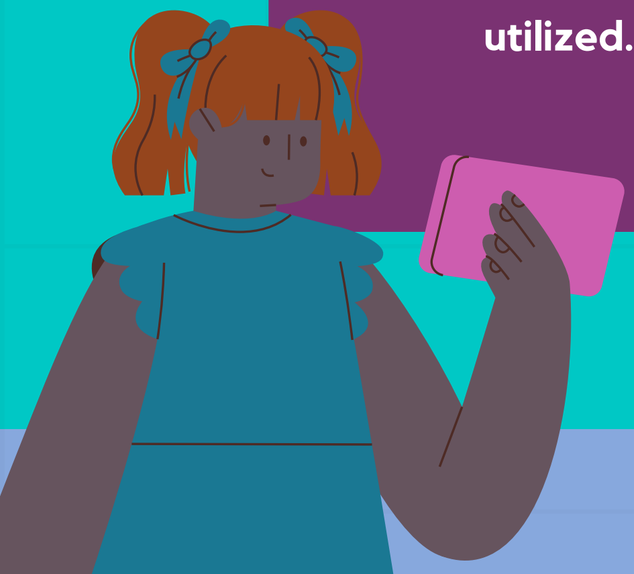
Compiled by DigiZens

LIST OF CONTENTS

- Definition of Data Privacy and Security
- Best Practices
- Benefits of Data Privacy for Digital Citizens
- Key Data Privacy Concepts
- Mobile Apps to Download

DEFINITION OF DATA PRIVACY

Data privacy refers to protecting sensitive information from unauthorized access, use, or disclosure while ensuring that individuals control how their data is collected, shared, and utilized. It encompasses the policies, procedures, and technologies implemented to safeguard personal data against breaches, misuse, or exploitation.



DEFINITION OF CYBERSECURITY

Key elements of data privacy include consent, transparency, confidentiality, integrity, and accountability in handling and managing data in compliance with applicable laws and regulations.

By prioritizing data privacy and protection, individuals and organizations can uphold ethical standards, mitigate privacy risks, and build a foundation of trust in digital interactions.

BEST PRACTICES

1 Understand Your Data

Understand what personal data is being collected, stored, and processed by the websites, apps, and services you use. Review privacy policies and terms of service to learn how your data is being handled.

2 Encrypt your Data

Encrypt sensitive data stored on your devices and in the cloud to protect it from unauthorized access. Use encryption tools and services to secure your communications and data transmission.

BEST PRACTICES

3 Keep Software Updated

Keep your operating system, software, and apps up-to-date with the latest security patches and updates. Enable automatic updates whenever possible to ensure you're protected against known vulnerabilities.

4 Secure Your Devices

Secure your devices with passcodes, biometric authentication, or other security features to prevent unauthorized access. Use device encryption to protect your data in case your device is lost or stolen.

BEST PRACTICES

5 Limit Data Sharing

Be cautious about sharing personal information online and only provide it when necessary. Minimize the amount of data you share on social media and other online platforms, and review privacy settings to control who can access your information.

6 Backup Your Data

Regularly backup your important files and data to an external hard drive, cloud storage, or other secure location. This will help protect your data in case of hardware failure, data loss, or ransomware attacks.

BEST PRACTICES

Privacy Settings

1. Review and adjust privacy settings on social media platforms and other online accounts to control who can see your information.

2. Be mindful of the information you share online and avoid oversharing personal details that could be used by cybercriminals.

BENEFITS OF DATA PRIVACY

The benefits of data privacy for digital citizens involve several positive aspects, including:

- Control Over Personal Information
- Protection Against Identity Theft
- Preservation of Reputation
- Prevention of Discrimination
- Trust in Digital Services
- Freedom of Expression

DATA PRIVACY MOBILE APPS TO DOWNLOAD

Privacy Badger: A browser extension that blocks trackers and advertisements, enhancing your online privacy while browsing.

Tor Browser: It anonymizes your web traffic by routing it through a network of servers, making it difficult to track your online activity.

ProtonMail: A secure email service that offers end-to-end encryption, ensuring your emails are protected from prying eyes.

CONCLUSION

Data privacy is essential for protecting individuals' personal information from unauthorized access or misuse. It involves measures to control how data is collected, shared, and used, ensuring confidentiality, integrity, and accessibility.

THANK YOU

Visit wwww.digizens.com
for more resources on Digital Citizenship