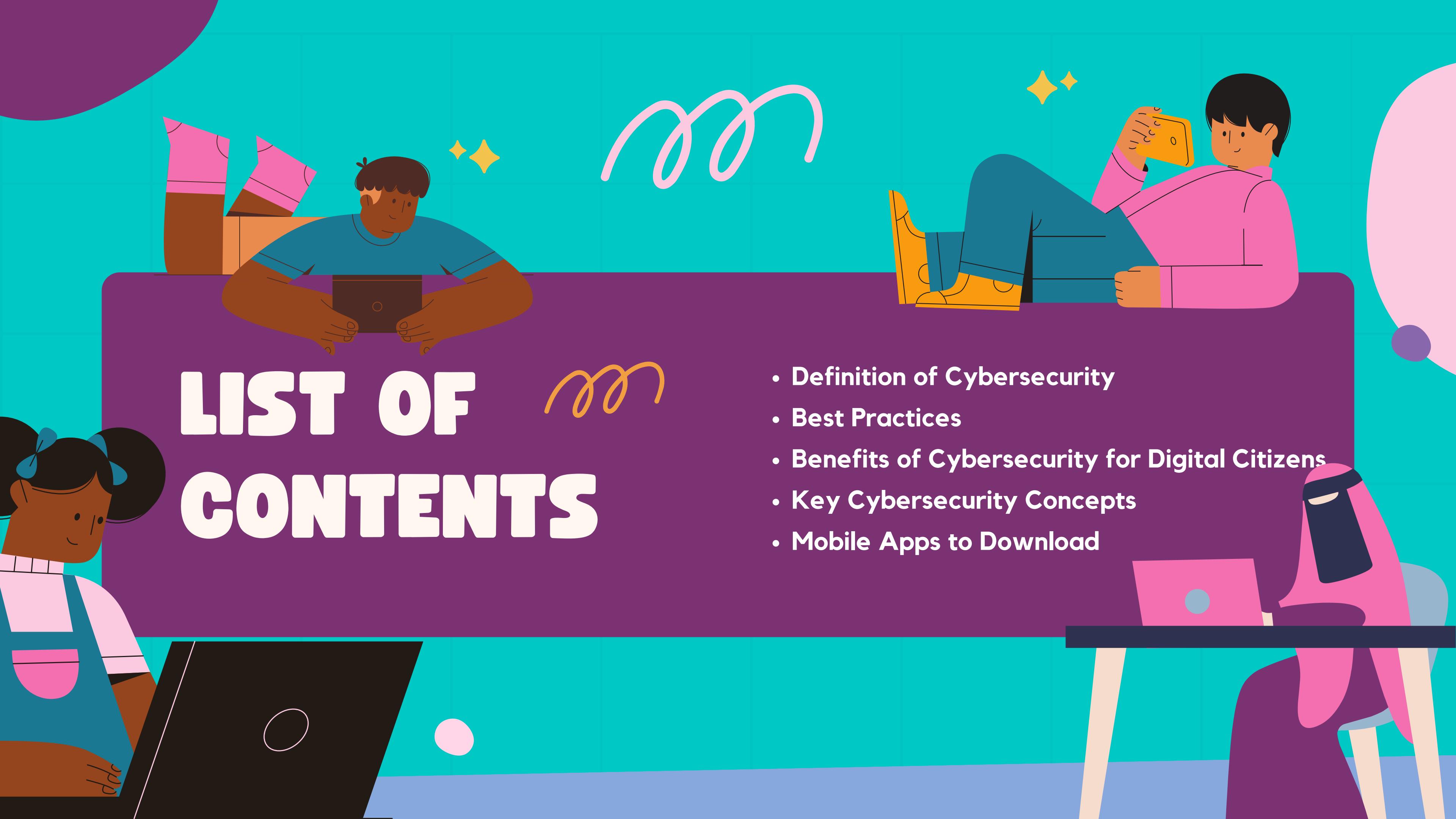




CYBERSECURITY 101

GUIDE

Compiled by DigiZens

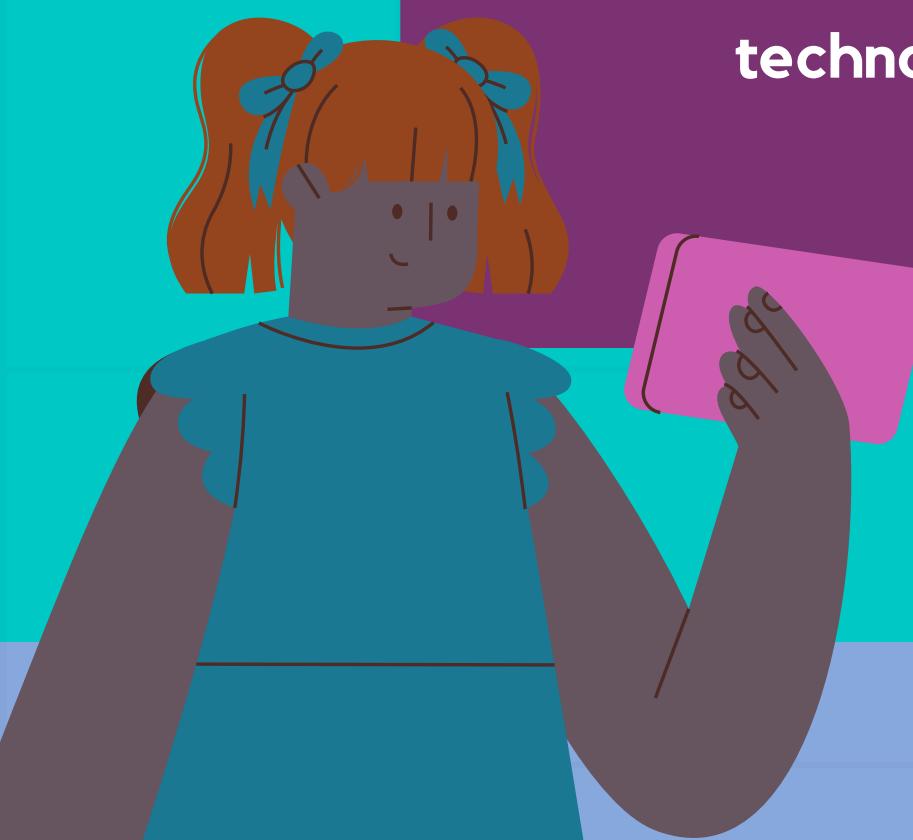


LIST OF CONTENTS

- Definition of Cybersecurity
- Best Practices
- Benefits of Cybersecurity for Digital Citizens
- Key Cybersecurity Concepts
- Mobile Apps to Download

DEFINITION OF CYBERSECURITY

Cybersecurity protects digital systems, networks, and data from cyber threats, including hackers, malware, and unauthorized access. It encompasses a range of practices, technologies, and processes designed to prevent, detect, and respond to security breaches and vulnerabilities.



DEFINITION OF CYBERSECURITY

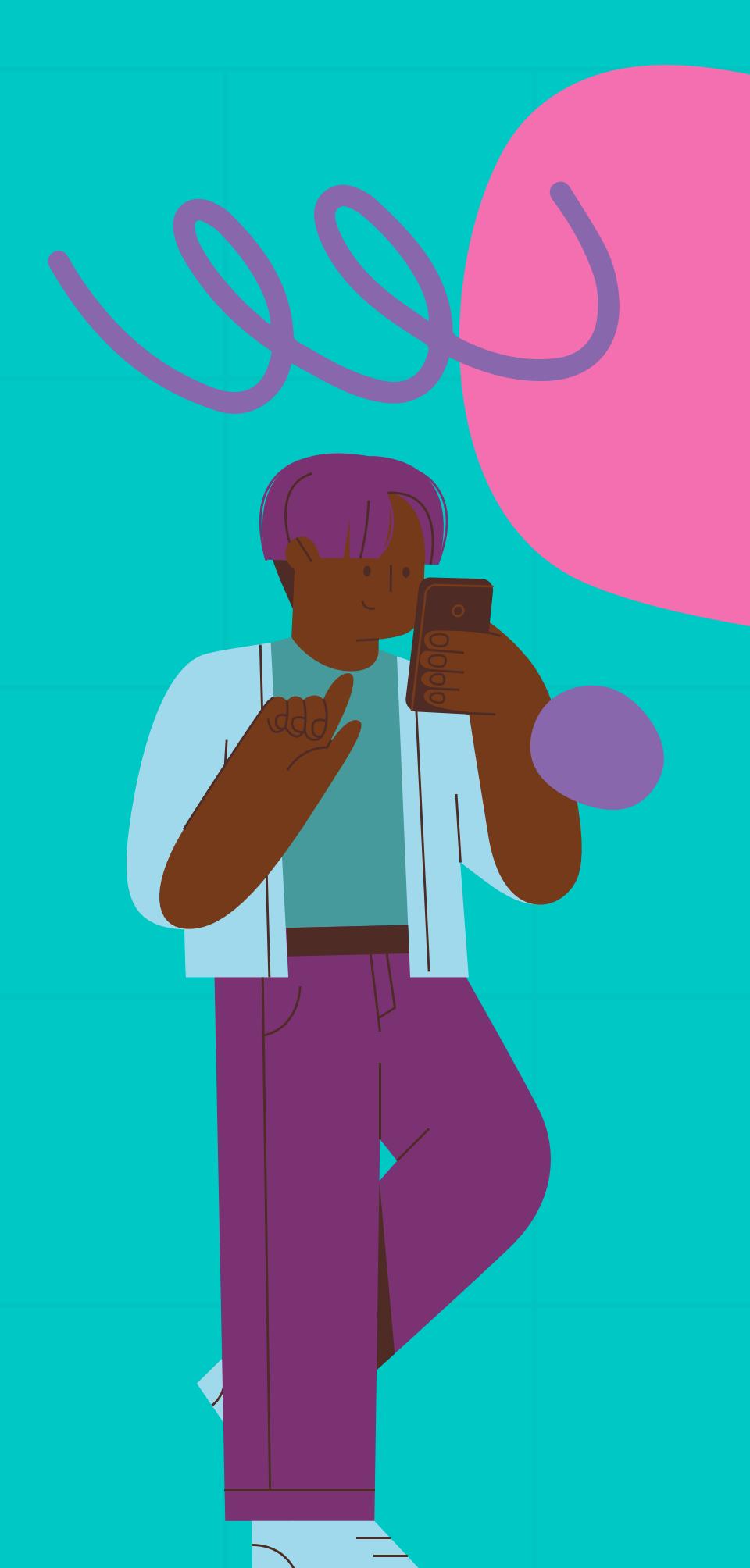
Key aspects of cybersecurity include implementing robust security measures, such as firewalls and encryption, educating users about cybersecurity best practices, conducting regular security assessments and audits, and staying updated on emerging threats and vulnerabilities.

By prioritizing cybersecurity, individuals and organizations can mitigate risks, safeguard sensitive information, and maintain the integrity and availability of digital assets.





BEST PRACTICES



Password Security

1

Use strong, unique passwords for each of your accounts.
Avoid using easily guessable information such as birthdays or pet names.

2

Aim for passwords that are at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special symbols.

3

Consider using a password manager to securely store and generate complex passwords for your accounts.

BEST PRACTICES



2FA

2 Two-Factor Authentication (2FA)

Enable 2FA whenever possible to add an extra layer of security to your accounts. This typically involves receiving a code on your phone or using a biometric method in addition to entering your password.



3

Software Updates

Keep your operating system, software, and apps up-to-date to patch security vulnerabilities. Enable automatic updates whenever possible to ensure you are protected against the latest threats.





BEST PRACTICES

Phishing Awareness



1

Be cautious of suspicious emails, messages, or links, especially those asking for personal or financial information.

2



Verify the sender's email address and be wary of urgent requests or offers that seem too good to be true.

3

Avoid clicking on links or downloading attachments from unknown or untrusted sources.



BEST PRACTICES

Secure Wi-Fi Networks

1

Use strong encryption (such as WPA2) and a unique password for your home Wi-Fi network to prevent unauthorized access.

2

Avoid using public Wi-Fi networks for sensitive activities like online banking or shopping, as they may not be secure.



BEST PRACTICES



Safe Browsing Practices

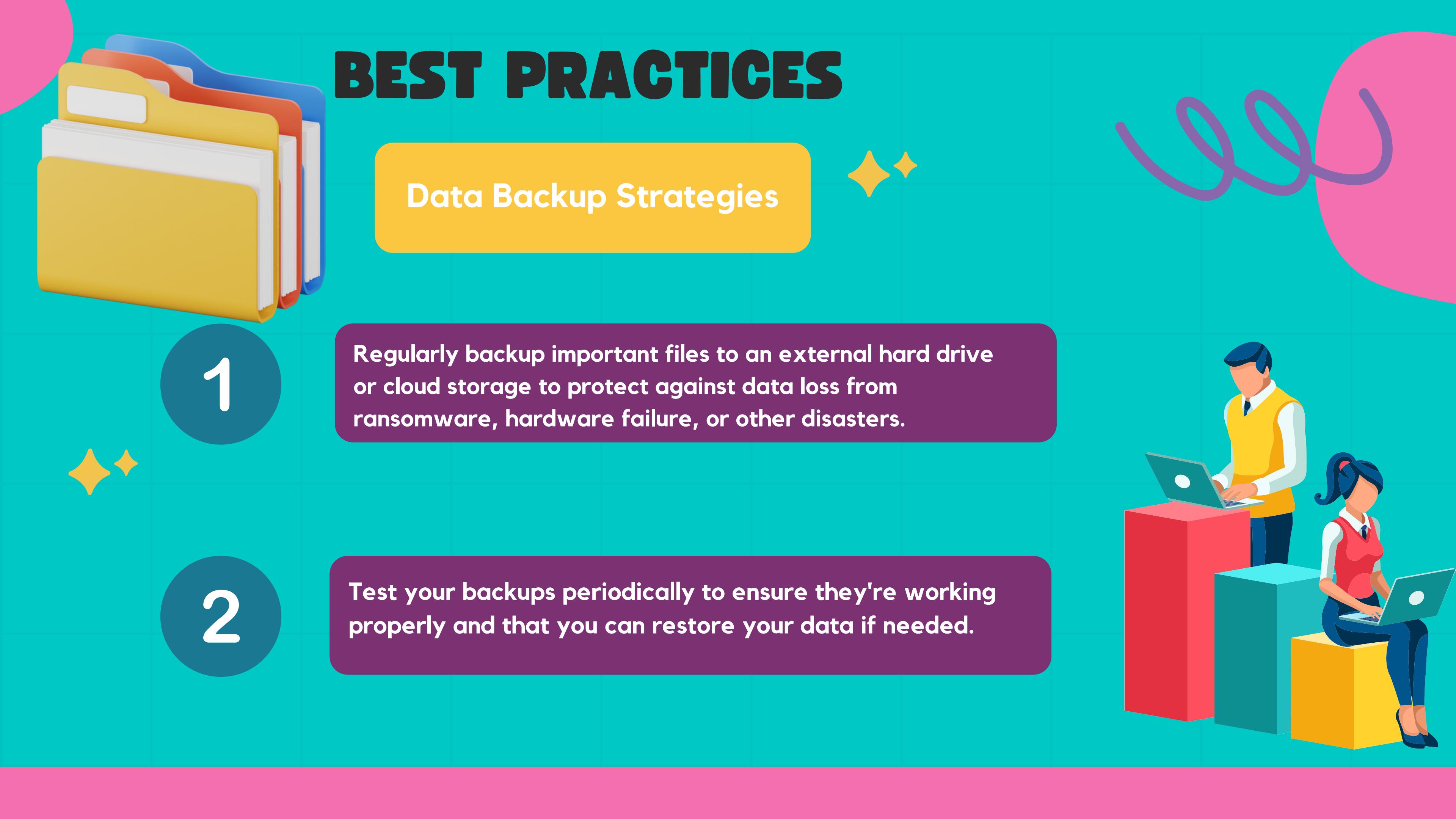
1

Look for HTTPS in the URL when visiting websites, especially when entering sensitive information like passwords or credit card details.

2

Be cautious of pop-up ads, unsolicited downloads, and websites that prompt you to install software or plugins.





BEST PRACTICES

Data Backup Strategies

1

Regularly backup important files to an external hard drive or cloud storage to protect against data loss from ransomware, hardware failure, or other disasters.

2

Test your backups periodically to ensure they're working properly and that you can restore your data if needed.



BEST PRACTICES



Privacy Settings



1

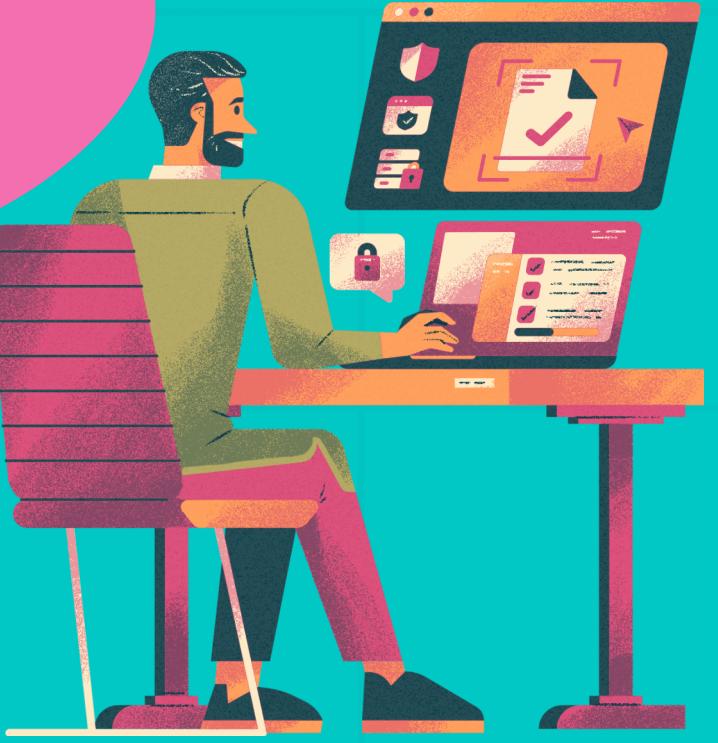
Review and adjust privacy settings on social media platforms and other online accounts to control who can see your information.



2

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





BEST PRACTICES

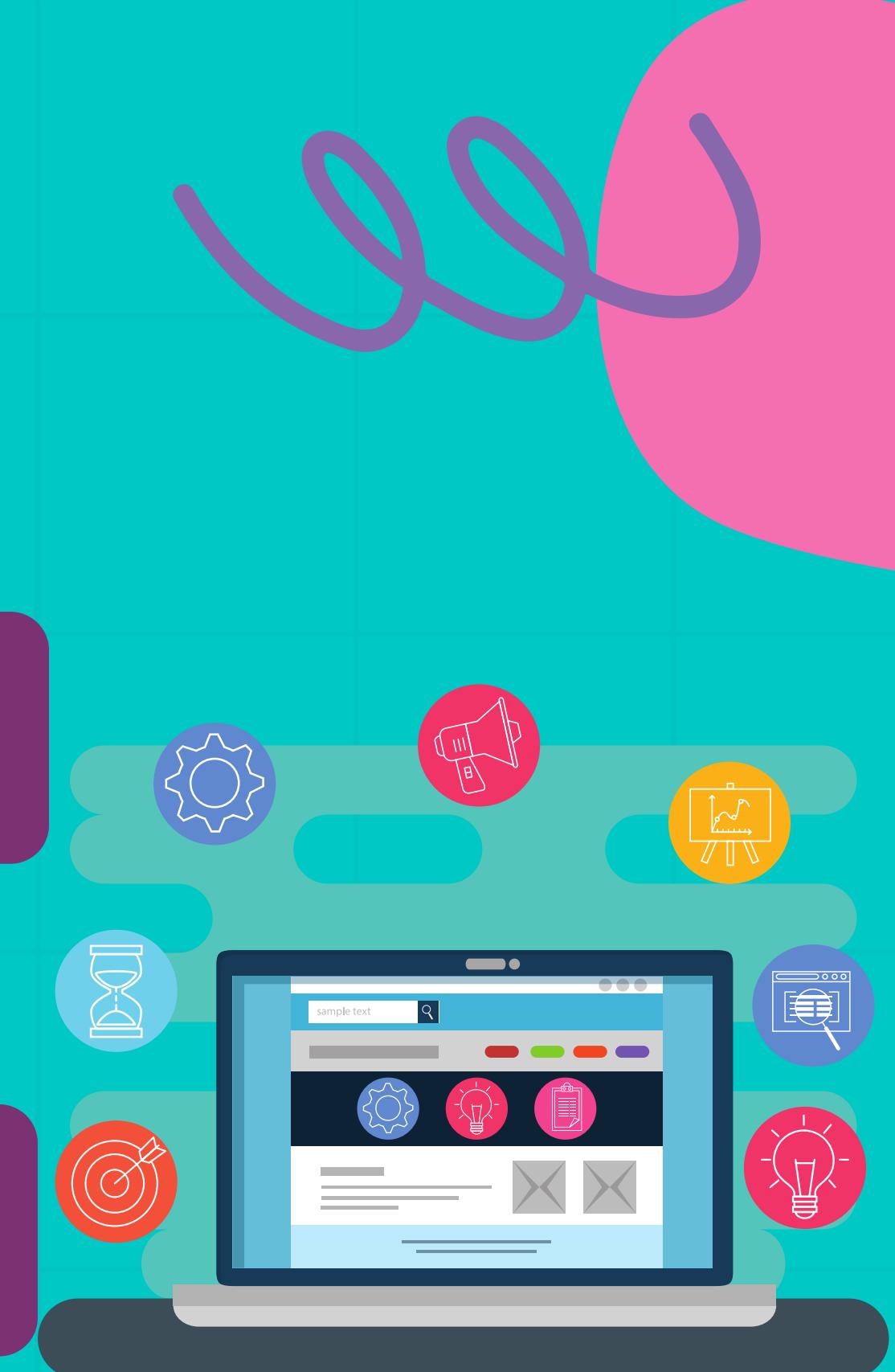
Stay Informed

1

Stay informed about common cybersecurity threats and best practices for protecting yourself online by following reputable cybersecurity blogs, news sources, and organizations.

2

Consider attending cybersecurity awareness training sessions or webinars to deepen your knowledge and skills.



BEST PRACTICES

Trust Your Instincts

1

If something seems too good to be true or feels suspicious, it's better to err on the side of caution and investigate further before taking action.

2

Trust your instincts and don't hesitate to ask for help or guidance if you're unsure about the legitimacy of an email, website, or request.



BENEFITS OF CYBERSECURITY

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

Safeguarding financial assets

Ensuring privacy and autonomy

Protection of personal information

Prevention of identity theft

Safe browsing experience

Defense against online fraud



KEY CYBERSECURITY CONCEPTS

Confidentiality

Integrity

Awareness

1. **Confidentiality:** Ensuring that sensitive information is only accessible to authorized individuals and remains private from unauthorized access or disclosure.
2. **Integrity:** Maintaining the accuracy and reliability of data and systems by preventing unauthorized alteration, modification, or destruction.
3. **Availability:** Ensuring that information and resources are accessible and usable when needed while protecting against disruptions or denial of service attacks.

CYBERSECURITY MOBILE APPS TO DOWNLOAD



LastPass

NordVPN

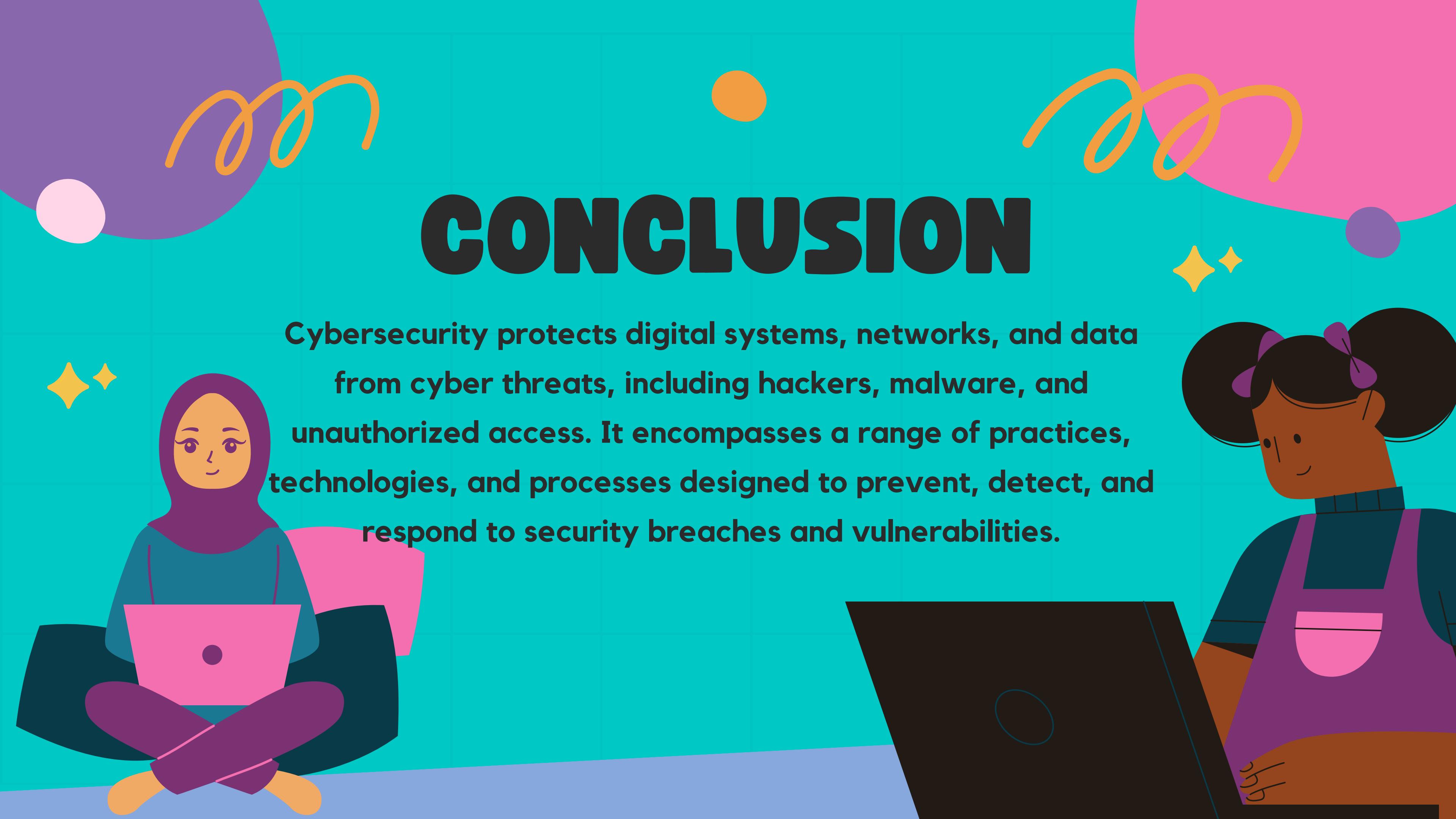
Google
Authenticator

DuckDuckGo

Avast

CONCLUSION

Cybersecurity protects digital systems, networks, and data from cyber threats, including hackers, malware, and unauthorized access. It encompasses a range of practices, technologies, and processes designed to prevent, detect, and respond to security breaches and vulnerabilities.



THANK YOU

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

DIGIZENS

