



SECURE YOUR NETWORK

CYBER SECURITY

By Web Glaze Services

TABLE OF CONTENTS



1. Introduction
2. About us
3. Why us for Cyber Security
4. Objective for Cyber Security
5. Major Security Problem
6. Services We Offer
7. Process Flow for Cyber Security
8. Additional Services for Cyber Security
9. Contact us

INTRODUCTION

- The term Cyber security is used to refer to the security offered through online services to protect your online information.
- With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also.
- At Web Glaze Services, we take a proactive approach to cyber security, so you can focus on your business without worrying about cyber threats. Contact us today to learn more about our cyber security solutions and how we can help you to protect your business.





ABOUT US

Web Glaze Services is an IT based company and working in websites, digital marketing, print media and app services from last 8 years. Here you can get all of your IT requirements & Cyber Securities under one roof. Our main goal is to be provide best quality IT service with 24/7 Support. Our team is very sincere, hard working and experienced in this field.

Vision:

Our goal is to assist clients in increasing the effectiveness and efficiency of their product and service delivery.

Mission:

Our aim to become one of the most prosperous and favored IT solutions partner for diverse business requirements.



8+

Years in Business



467+

Projects Delivered



342+


Happy Clients



50+

Technical Experts





WHY US FOR CYBER SECURITY

Strength that will add to Web Glaze Services

We offer 24/7, 365 days a year service to assist our clients in most efficient way.

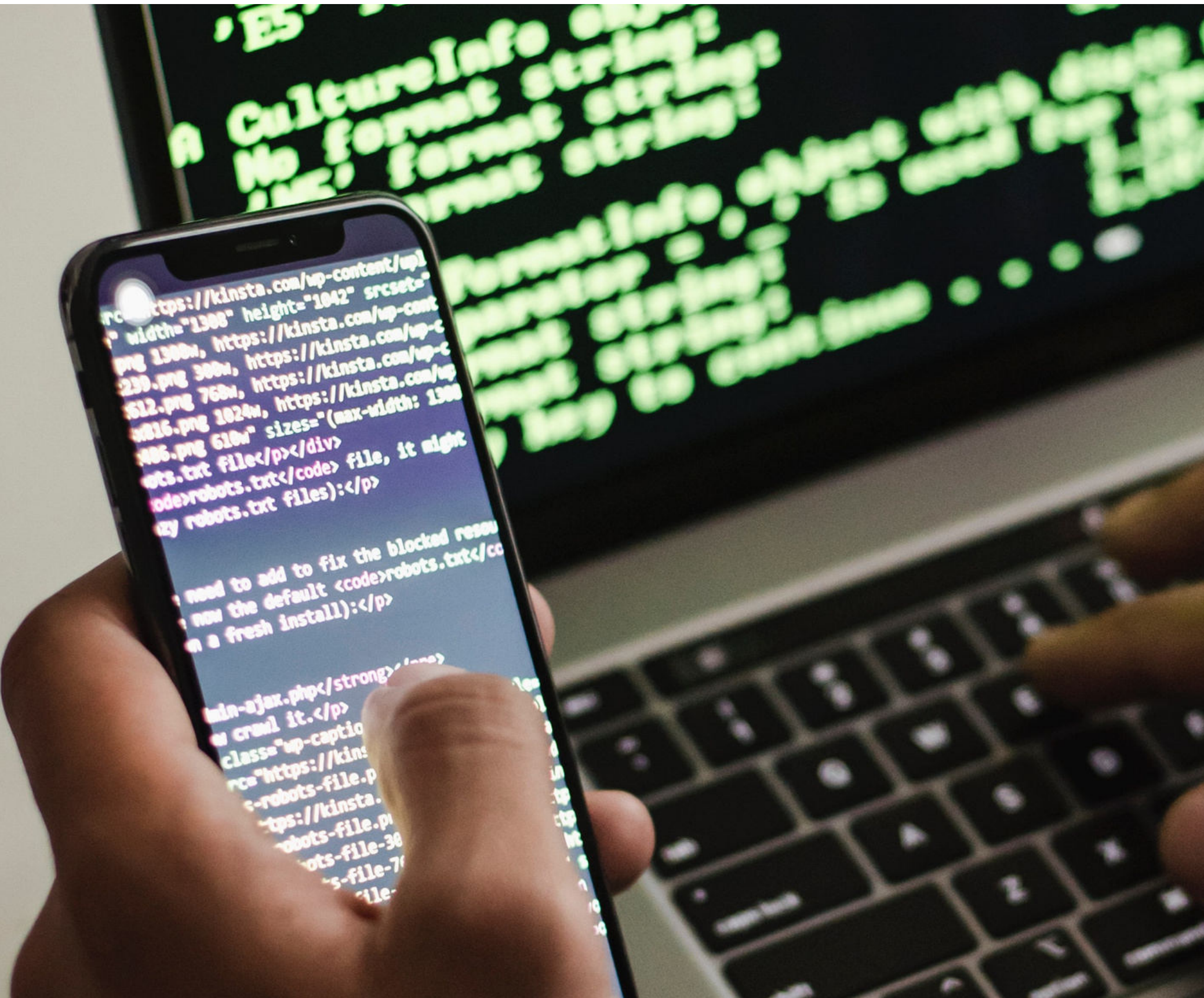
We have extensive experience of IT support services & development of custom tools to secure our clients.

Our team includes elite software engineers and cyber security experts to keep our culture fresh, innovative and energetic.

OBJECTIVE FOR CYBER SECURITY



- We will installed several customized software's in systems to provide uninterrupted data and network security.
- Our experts will develop best defense system for servers by identifying security defects & vulnerabilities.
- We will uncover system and & network flaws through complete penetration testing.
- We will do 24/7 networking security monitoring to detect attacks & secure servers and systems.
- We will train your employees regarding cyber threats & how to avoid them.



MAJORITY SECURITY PROBLEMS

- Virus
- Hacker
- Malware
- Trojan Horses
- Password Cracking

Viruses & Worms

A virus is a program that is loaded onto your computer without your knowledge and runs against your wishes.

Solutions

Install a security suite that protects the computer against threats such as viruses and worms.





Hackers

In common a **HACKER** is a person who breaks into computers usually by gaining access to administrative controls.

How To Prevent Hacking?

It is impossible to prevent computer hacking, however effective security controls including strong passwords and the use of firewalls can help you.

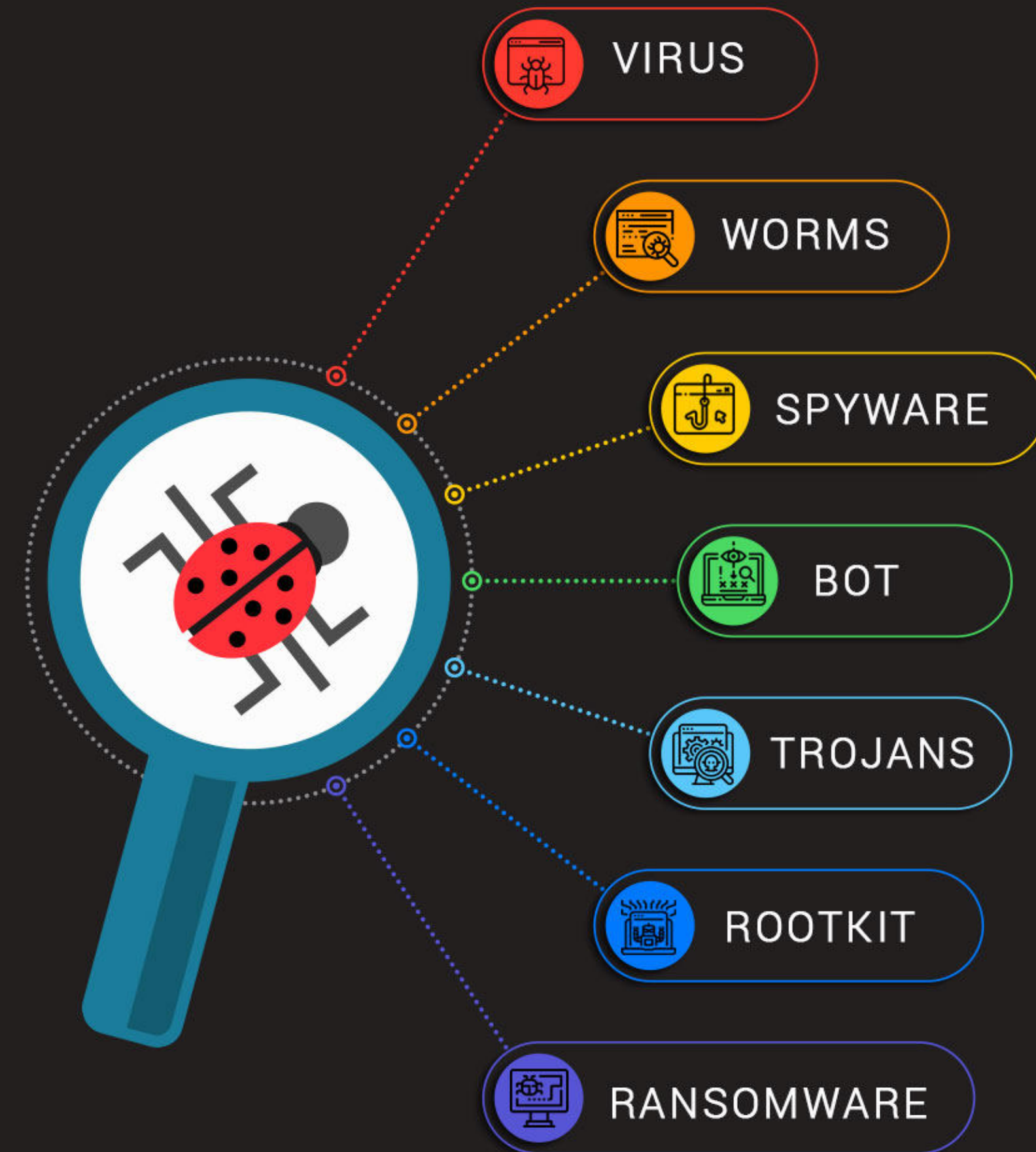
Malware

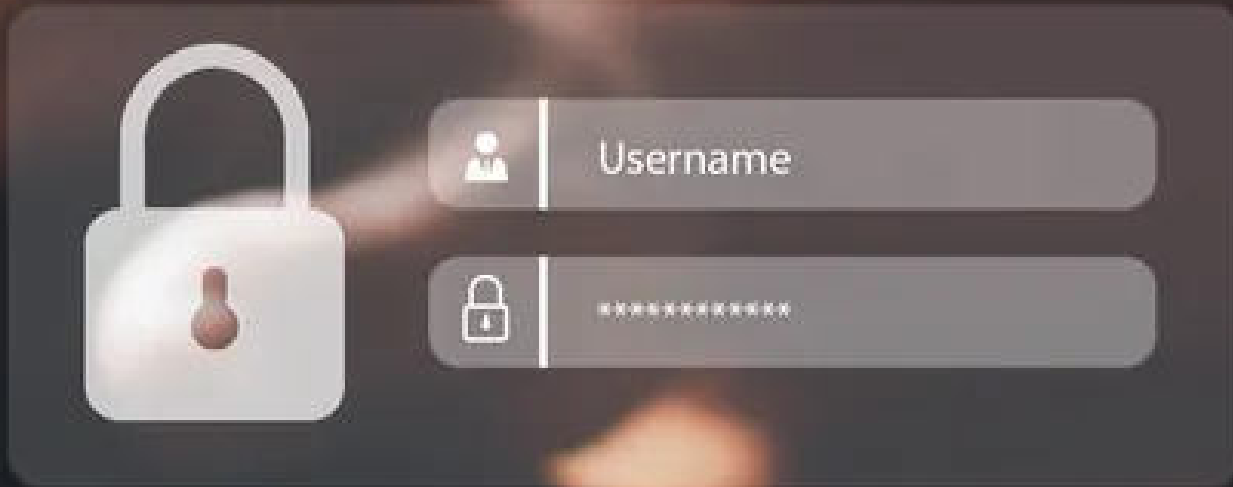
- The word "**MALWARE**" comes from the term "**MAL**icious Soft**WARE**".
- Malware is any software that infects and damage a computer system without the owners knowledge or permission.

To Stop Malware

- Download and Anti-Malware program that also helps prevent infections.
- Activate Network Threat Protection, firewall & antivirus.

TYPES OF MALWARE





Password Cracking

Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

Securing Password

- Use always strong password.
 - Never use same password for two different sites.
-



SERVICES WE OFFER

- **Application Security**
- **Web Application Security**
- **Android App security**
- **iOS App security**
- **Code Review**
- **Network Penetration Testing**

Application Security

Application security, also known as App Sec, refers to the practice of securing software applications from various threats and vulnerabilities throughout their development, deployment, and maintenance life cycle. It involves implementing security measures at each stage of the application development process to identify, prevent, and mitigate security risks that could potentially lead to unauthorized access, data breaches, or other malicious activities.

The primary goal of application security is to ensure the confidentiality, integrity, and availability of the application and its data.

APPLICATION SECURITY

Application Security Competency Framework

Design Security IN

- Secure Application Coding Practices
- Static Application Security Testing/Dynamic applications Security Testing
- Runtime Application Self-Protection
- Software Composition Analysis
- Patching

Penetration Testing

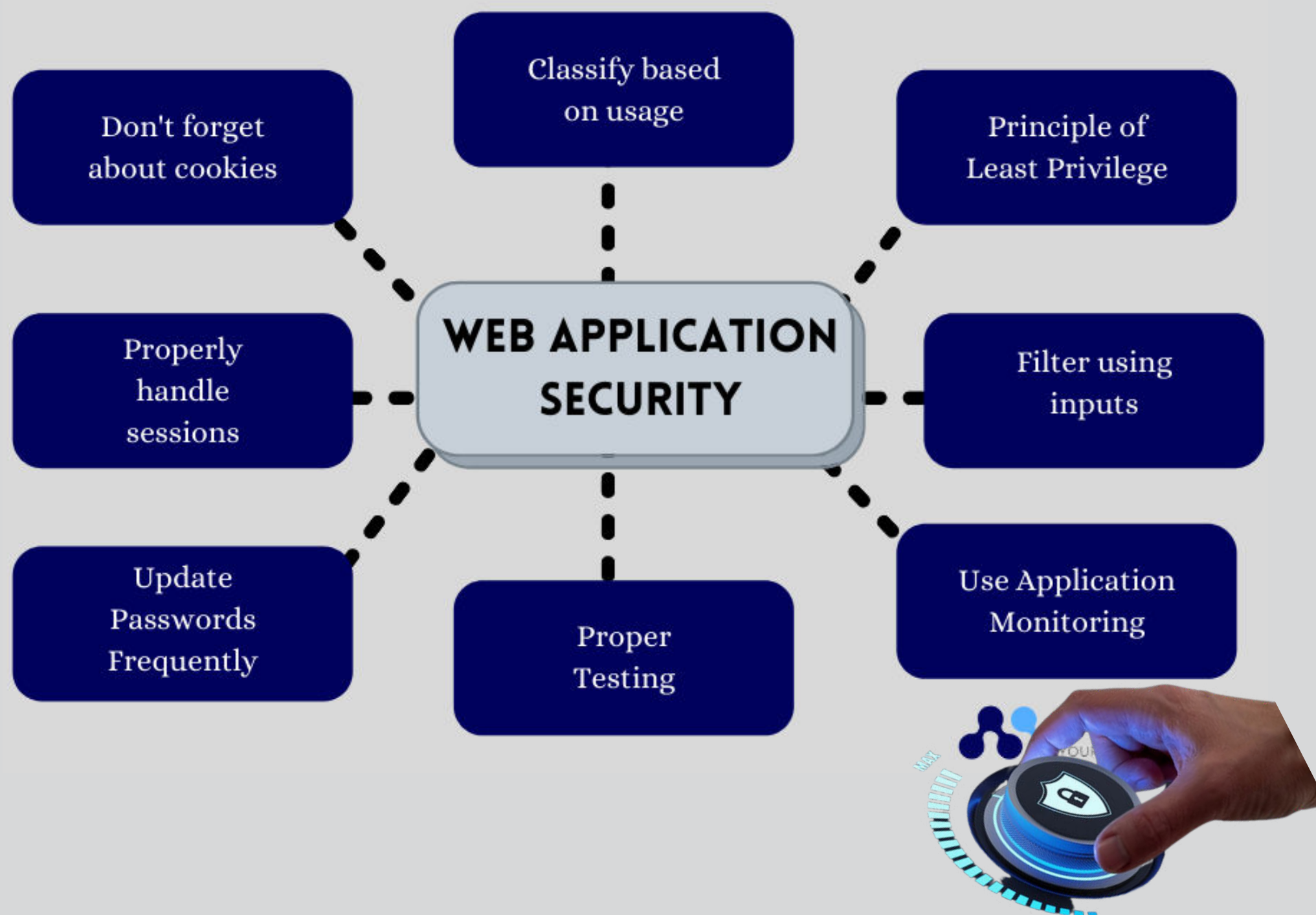
- Secure Application
- Secure Hosting Platform
- Tools
- Security Training
- Software Development Lifecycle
- Governance
- Management Commitment

Protect From Without

- AAP firewalls
- Host Hardening
- Network/distributed denial of service
- Detection
- Response

Web Application security

Web application security is a specialized subset of application security that focuses specifically on securing web applications. Web applications are software programs accessed through web browsers, and they are widely used for various purposes, such as e-commerce, social media, online banking, and more. Given their public-facing nature and exposure to the internet, web applications are prime targets for attackers, making web application security crucial to protect sensitive data and prevent unauthorized access.

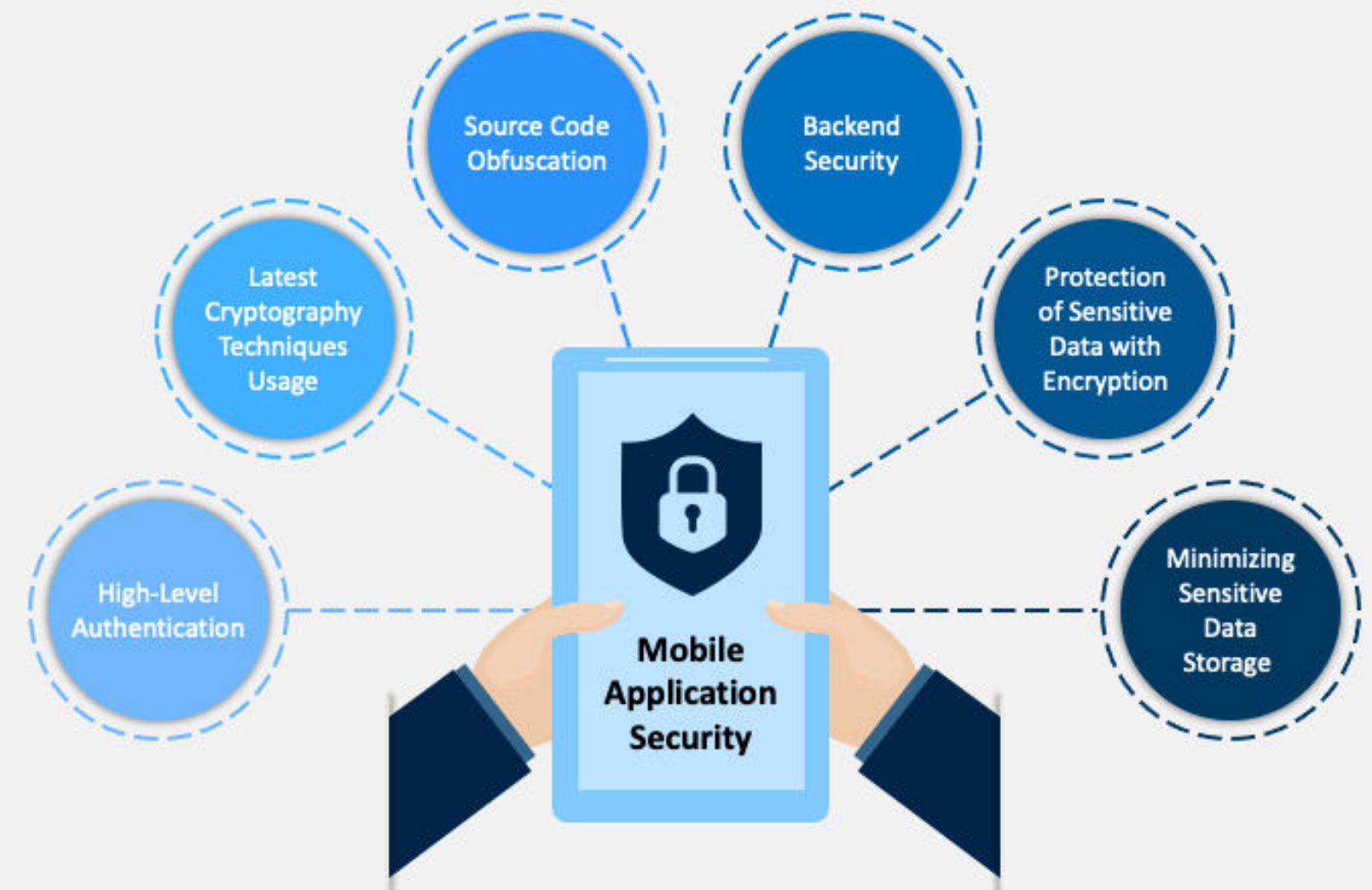


Android App Security

Android app security refers to the measures and practices taken to protect Android applications from potential threats and vulnerabilities. Android is a popular mobile operating system developed by Google, and its open nature makes it susceptible to various security risks. To ensure the confidentiality, integrity, and availability of Android applications and their data, we implement robust security measures throughout the app's development, deployment, and maintenance life cycle.

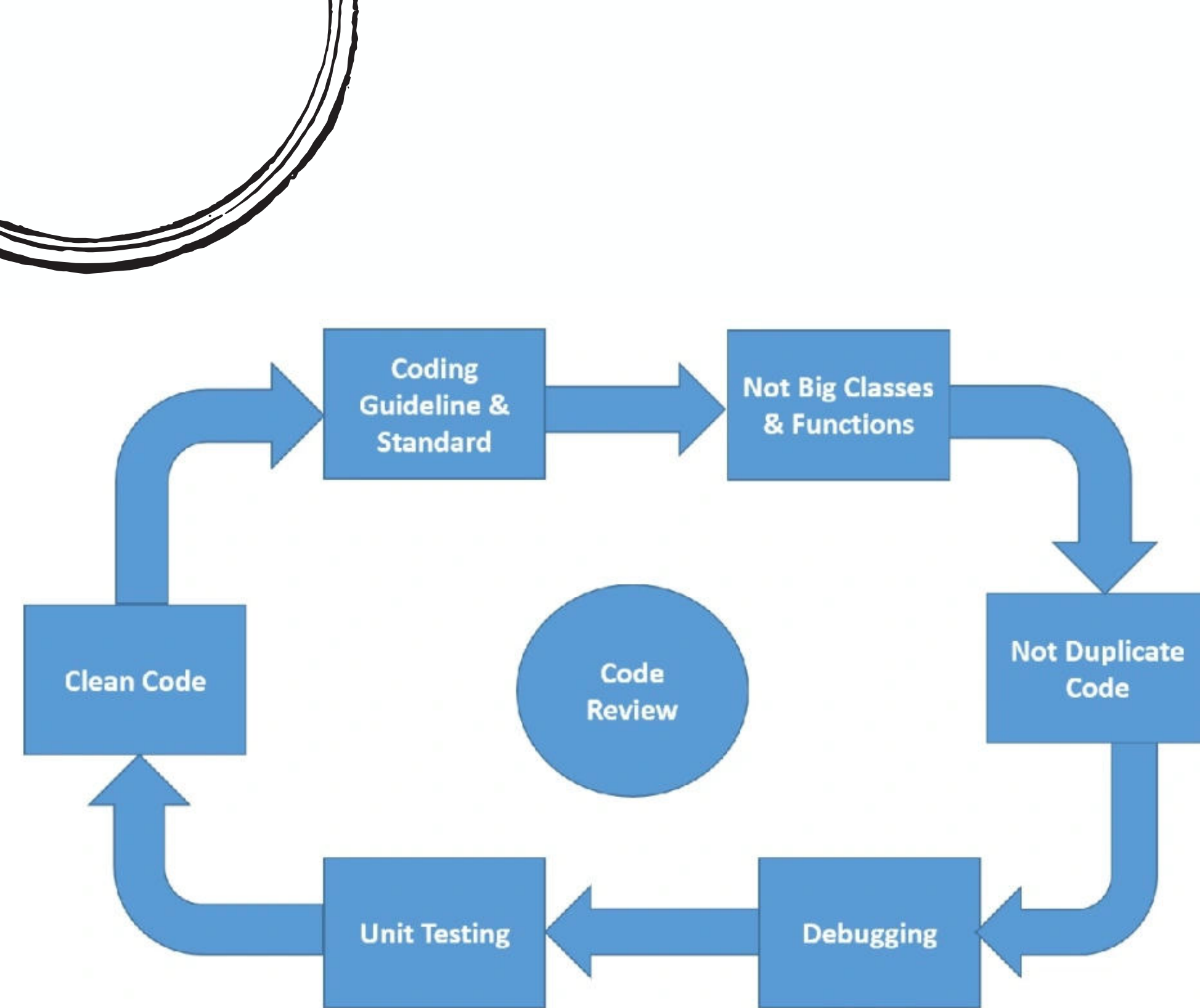
MOBILE APPLICATION SECURITY

Mobile App Security Best Practice Against Threats



Code Review

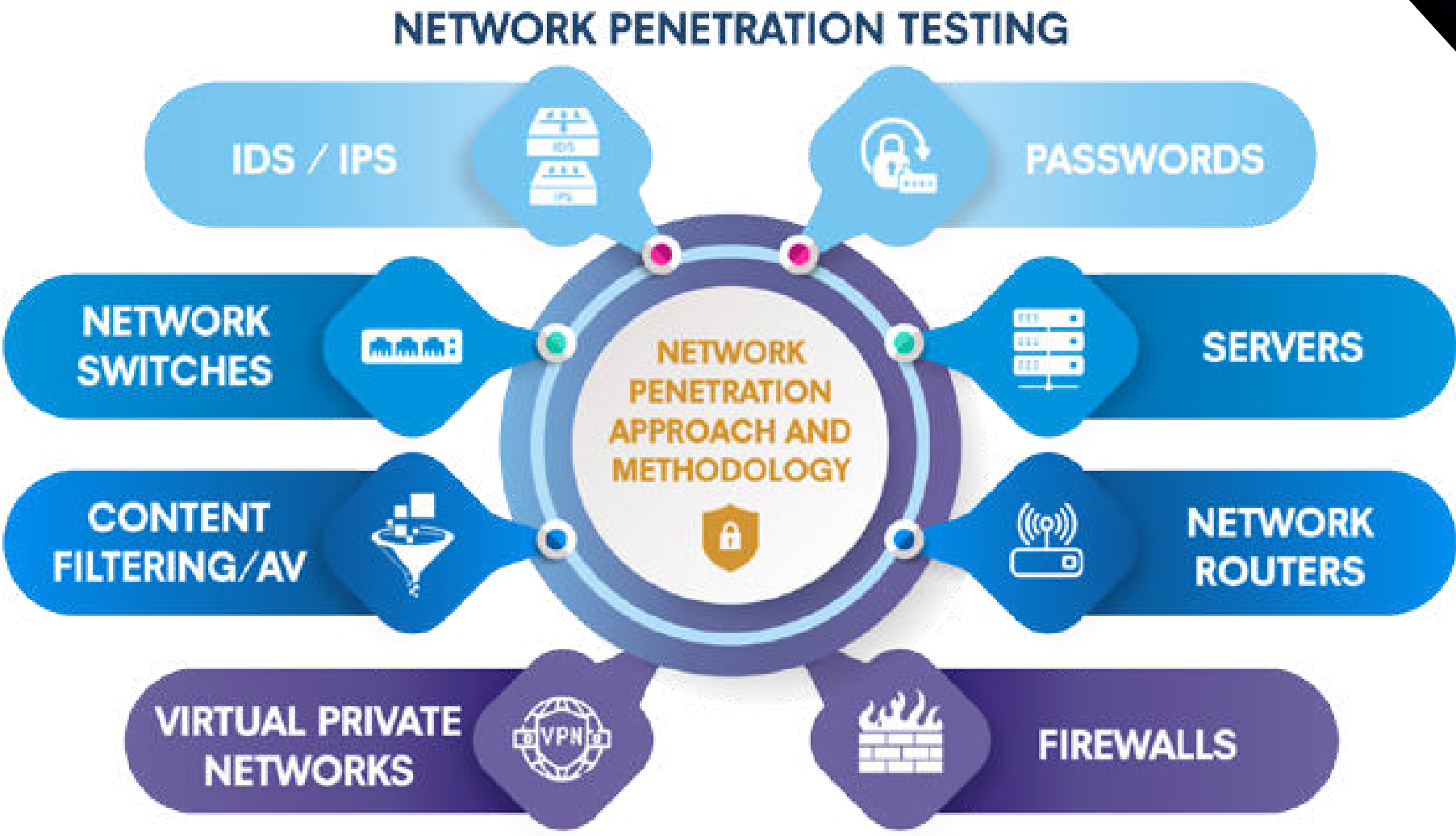
Code review is a systematic examination and evaluation of the source code written for a software application. It involves one or more developers or team members inspecting the code to identify and address issues related to code quality, best practices, security, and compliance with coding standards. Code reviews are an essential practice in the software development lifecycle, and they offer numerous benefits for both individual developers and the development team as a whole.

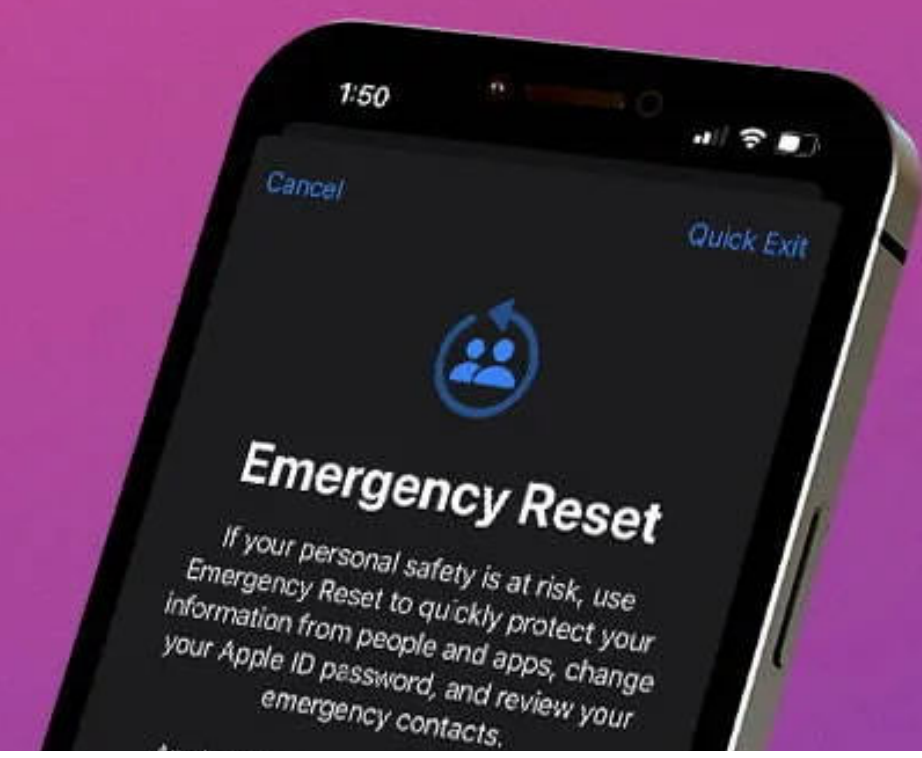


Basic Code Review Check List

Network Penetration Testing

Network Penetration Testing, also known as Ethical Hacking or White Hat Hacking, is a Cyber Security practice that involves simulating real-world cyber attacks on a computer network to identify vulnerabilities and weaknesses. The primary objective of network penetration testing is to evaluate the security of a network infrastructure and its components, including servers, routers, firewalls, and other devices, to help organizations proactively identify and address security risks before malicious hackers can exploit them.





iOS App Security

iOS app security refers to the practices and techniques used to secure applications developed for Apple's mobile operating system, iOS. Apple's iOS is known for its stringent security measures, We implement additional security measures to protect iOS apps from potential threats and vulnerabilities.

By adhering to iOS app security best practices, we build secure iOS apps that protect user data, maintain user trust, and adhere to Apple's security guidelines.

PROCESS FLOW FOR CYBER SECURITY

WEEK 1

Project Kickoff

- Understand Clients requirements.
- Mapping Clients Current IT system.
- Analyzing current network flaws.

WEEK 2

Planning

- Select the appropriate technology and flexible solutions against client's requirements.
- IT Experts allocation planning to execute check of each system in organisation.
- Encryption and authorization planning for server.

WEEK 3

Implementation

- Development of confidentiality and integrity of tools.
- Customized Firewall set up development.
- Virtual servers security set up.
- Property security setup with 24/7 technical support.

WEEK 4

Maintain & Train

- Maintain & manage security system for minimal disruption.
- Proper training of client's employees to avoid cyber threats.

ADDITIONAL SERVICES FOR CYBER SECURITY

Security & Networking

- Cyber Attacks protection
- Strategic recommendation for site
- Comprehensive visibility into network traffic

Software Development

- Custom software solution
- Product development
- Web and Mobile App



Cloud Services

- Cloud advisors, builder and provider
- Industry leading managed IT services

CONTACT US

WEB GLAZE SERVICES

Website

www.web-glaze.com

Email

info@web-glaze.com

Phone

+971 52 397 1654
+ 91 11 455 23706
+91 96501 78436

Address

Office 1213, Pearls Omaxe
Tower 2, Netaji Subhash Place,
Delhi - 110034

