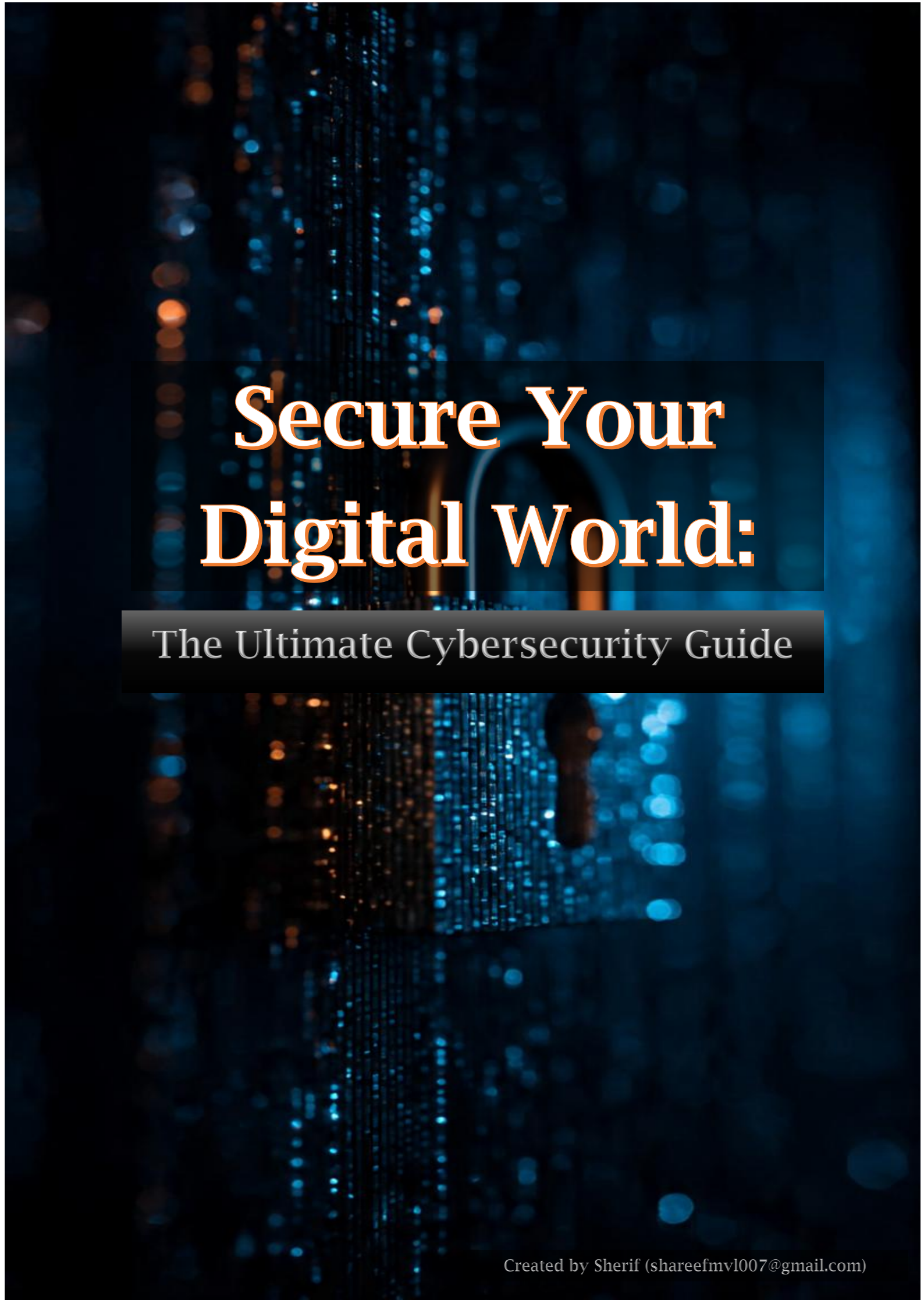

Secure Your Digital World:

The Ultimate Cybersecurity Guide

Created by Sherif (shareefmvl007@gmail.com)

■■ Cybersecurity & Online Safety Guide

A complete beginner-to-advanced guide with Indian context, tips, and quick facts.

■ Network & Wi-Fi Protection

• Change default router admin password after setup
• Use WPA3 or WPA2 encryption, avoid WEP or open networks
• Hide SSID and limit Wi-Fi access to trusted devices
• Update router firmware regularly from manufacturer's website
• Disable remote admin access unless required
• Use guest networks for visitors to isolate main devices
• Monitor connected devices via router dashboard or Fing app
• Avoid public Wi-Fi for banking; use VPN if necessary
• Use firewall on home router and disable WPS
• For advanced setups, consider DNS filtering like NextDNS or Quad9

■ **Pro Tip:** Use a Raspberry Pi or OpenWRT router for better visibility and control over your network

■■ **Caution:** Never use open Wi-Fi without VPN

■ **Did You Know?** Public Wi-Fi hacking can occur in under 30 seconds using packet sniffers

■ **Did You Know?** Most free hotspots are unsecured

Network & Wi-Fi Protection Checklist

Do	Don't
Use WPA3/WPA2 encryption	Use WEP or open Wi-Fi
Hide SSID	Broadcast SSID publicly
Use guest networks	Allow untrusted devices on main network

■ Password & Authentication

• Use strong passwords: at least 12+ characters mixing letters, numbers, symbols
• Avoid reusing passwords across websites
• Use password managers like Bitwarden, KeePass, or 1Password
• Enable Two-Factor Authentication (2FA) everywhere possible
• Prefer hardware keys (YubiKey, Titan Key) for critical accounts
• Regularly update passwords for banking and email accounts

Created by Sherif (shareefmvl007@gmail.com)

• Never share OTPs or passwords, even with ‘official’ callers
• Use biometric locks (fingerprint/face) for device access
• Use unique master password for password manager
• Backup security codes for 2FA in secure location

■ **Pro Tip:** Store master password securely offline

■■ **Caution:** Avoid saving passwords directly in browsers

■ **Did You Know?** Reusing passwords is the most common cause of account breaches
■ **Did You Know?** 2FA can prevent 90% of automated attacks

Password & Authentication Checklist

Do	Don't
Use 12+ character passwords	Use short or predictable passwords
Enable 2FA	Rely only on passwords
Use hardware keys for critical accounts	Share OTPs with anyone

■ Application & Software Safety

• Download apps only from trusted stores (Google Play, Apple App Store, vendor-specific stores)
• Check app permissions; deny unnecessary access like location or contacts
• Avoid cracked or modded apps — often include malware
• Install Indian government trusted security apps like M-Kavach2
• Regularly update software, OS, and browsers
• Enable Play Protect or equivalent security scanner
• Uninstall unused or suspicious apps immediately
• Avoid APK downloads from unknown websites
• Use VirusTotal or sandbox to test suspicious apps before installation
• Disable installation from unknown sources in settings

■ **Pro Tip:** Ensure apps are legitimate and what they are scanning

■■ **Caution:** Do not allow installation from unknown sources

■ **Did You Know?** Malicious apps often masquerade as games or utilities
■ **Did You Know?** Over 70% of mobile malware is delivered via third-party app stores

■ Browser & Website Security

• Use privacy-focused browsers like Firefox, Brave, or DuckDuckGo
• Enable HTTPS-only mode and check for padlock icon before logging in
• Avoid clicking random popups or download links
• Use ad-blockers and anti-tracking extensions
• Clear cookies and browsing data periodically
• Do not save credit card info in browsers
• Verify shortened URLs using preview tools
• Check website certificates for TLS 1.2/1.3 or QUIC

■ **Pro Tip:** Check padlock symbol and certificate authenticity

■■ **Caution:** Expired or self-signed certificates are vulnerable

■ **Did You Know?** Man-in-the-middle attacks can steal data even on familiar networks
■ **Did You Know?** Expired certificates increase risk of phishing

■ Email & Third-Party Permissions

• Avoid opening suspicious attachments
• Do not click unknown links
• Verify sender email addresses before acting
• Limit third-party app access to email (e.g., Cred, Gmail)
• Revoke old permissions periodically
• Use email filters and alerts
• Avoid giving email read/write access unnecessarily

■ **Pro Tip:** Use OAuth only for verified apps

■■ **Caution:** Never give apps full email read/write access unnecessarily

■ **Did You Know?** Phishing emails often mimic official sources
■ **Did You Know?** Compromised accounts can propagate spam automatically

■ Backup & Device Hygiene

• Backup personal photos and data regularly to trusted cloud platform
• Clear local data after backup to avoid theft
• Enable disk encryption
• Use remote-wipe for lost devices

• Regularly update OS and apps
• Maintain multiple backup copies in separate locations

■ **Pro Tip:** Always encrypt backups for sensitive data

■■ **Caution:** Avoid keeping unnecessary local copies of confidential files

■ **Did You Know?** Ransomware can encrypt local files within minutes
■ **Did You Know?** Device theft is a common cause of data loss

■ Banking & Digital Payment Security

• Avoid using credit cards unless necessary
• Set online and offline transaction limits for cards
• Reduce NFC debit/credit card limits
• Register email with bank for alerts, not only mobile number
• Do not share bank account credentials or OTP
• Monitor transactions regularly
• Use RBI-approved apps and UPI apps
• Do not respond to WhatsApp or SMS money scams
• Avoid using 3rd-party loan apps without reading terms

■ **Pro Tip:** Use email alerts and banking notifications

■■ **Caution:** Beware of fake SMS, WhatsApp payment messages

■ **Did You Know?** UPI frauds often exploit social engineering quickly
■ **Did You Know?** Banks never ask for PIN/OTP via phone/email

Banking & Digital Payment Security Checklist

Do	Don't
Use RBI-approved UPI apps	Use unverified 3rd-party apps
Set transaction limits	Allow unlimited transactions
Monitor bank alerts	Share OTPs or PINs

■■ Remote Access & Admin Hardening

• Use SSH keys instead of passwords for remote login
• Disable root login

• Change default ports (e.g., SSH from 22 to random)
• Whitelist IPs or use VPN for remote access
• Patch servers regularly
• Monitor open ports
• Use fail2ban or similar intrusion prevention

■ **Pro Tip:** Use key-based login for all remote devices

■■ **Caution:** Never use default credentials

■ **Did You Know?** Attackers scan common ports first

■ **Did You Know?** Exposed SSH without keys is high risk

■ Social Engineering & Scam Awareness

• Verify friend requests/messages via call before action
• Do not send money online without confirmation
• Avoid get-rich-quick schemes
• Ignore ‘digital arrest’ threats online
• Report scams immediately to cyber police
• Educate family and friends about phishing

■ **Pro Tip:** Use official channels to verify requests

■ **Did You Know?** Attackers often impersonate trusted contacts

■ **Did You Know?** Phishing campaigns are increasing rapidly

■ Corporate & Workplace Safety

• Do not use personal accounts on corporate devices
• Be aware of TLS interception by proxies
• Use company-approved software only
• Store credentials securely
• Logout from shared systems
• Use VPN for remote work

■ **Pro Tip:** Segregate personal and work data

■ **Did You Know?** Corporate networks may log all activity

■ **Did You Know?** Forward proxies can decrypt HTTPS locally

■ Detection, Monitoring & Recovery

• Use antivirus and antimalware software
• Enable firewall monitoring
• Use IDS/IPS if possible
• Check logs regularly
• Apply patches promptly
• Test recovery plans periodically

■ **Pro Tip:** Keep system monitoring alerts enabled

■■ **Caution:** Do not ignore security alerts

■ **Did You Know?** Early detection reduces ransomware impact
■ **Did You Know?** Regular monitoring can prevent major breaches

■ Physical Device & Data Disposal

• Overwrite storage before selling or recycling devices
• Remove SIM/microSD cards
• Enable device locks
• Use remote-wipe
• Keep backup before disposal
• Record high-quality videos to fill storage before deleting

■ **Pro Tip:** Use secure erase tools

■ **Did You Know?** Deleted files can be recovered easily without full overwrite
■ **Did You Know?** Physical theft is a real threat

■ Advanced Tools & Government Resources

• Use VPN from trusted providers
• Segment home network (IoT/Guest)
• Check email breaches on HaveIBeenPwned
• Use M-Kavach2, NetGuard, Cyber Swachhta Kendra
• Report cybercrime at cybercrime.gov.in or call 1930
• Follow CERT-In advisories

■ **Pro Tip:** Use hardware security keys for sensitive accounts

■ **Did You Know?** CERT-In provides real-time advisories

■ **Did You Know?** National tools help prevent malware infections

Advanced Tools & Government Resources Checklist

Tool	Purpose
M-Kavach2	Mobile security for Indian users
Cyber Swachhta Kendra	Malware detection and removal
HaveIBeenPwned	Check email breach status

■ Quick Safety Checklist

- Use strong, unique passwords with 2FA enabled
- Update all software and apps regularly
- Use RBI-approved apps for UPI and banking
- Enable disk encryption and backups
- Avoid public Wi-Fi without VPN
- Check email for breaches on HaveIBeenPwned
- Report cybercrimes at cybercrime.gov.in or 1930
- Use M-Kavach2 for mobile security
- Verify URLs and sender emails before clicking
- Educate family on phishing and scams
- Monitor bank transactions and set alerts
- Use privacy-focused browsers like Brave
- Securely erase devices before disposal
- Segment home network for IoT devices

■ **Pro Tip:** Review this checklist monthly

■ **Did You Know?** Following this checklist reduces 95% of common cyber risks

Quick Safety Checklist

My Device Record	Status
Router Firmware Updated	■ Yes ■ No
2FA Enabled on Accounts	■ Yes ■ No
Backups Encrypted	■ Yes ■ No
M-Kavach2 Installed	■ Yes ■ No