SECURZE

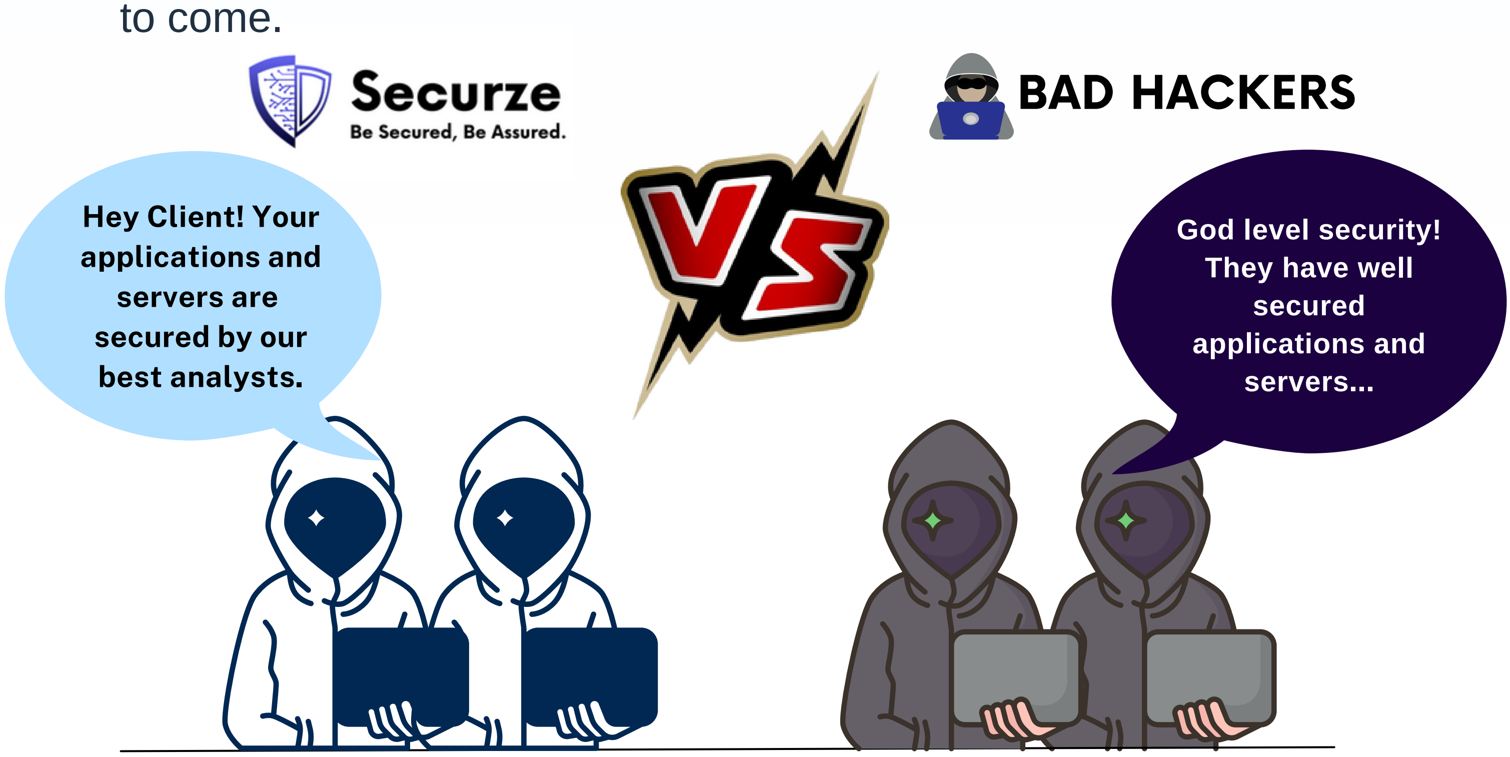
SECURING WHAT MATTERS MOST

NAVIGATING CYBER SECURITY CHALLENGES: MOVING FORWARD TO 2024...

www.securze.com	securze
info@securze.com	securze_com
+91 84510 73938	Securze

2023, we at Securze experienced an exceptional year marked by significant achievements in the realm of cybersecurity. Our unwavering commitment to fortifying digital defenses led us to successfully thwart multiple cyber attacks, solidifying our position as a trusted guardian in the cybersecurity landscape. Through our carefully crafted cybersecurity checklists, we not only shielded countless individuals and businesses from threats but garnered global acclaim for our impactful contributions. The recognition and gratitude received from people worldwide serve as a testament to the effectiveness of our strategies.

At Securze, our dedicated team's relentless efforts in identifying cyber attacks and criminals underscore our mission to bolster the security of businesses and nations alike. As we celebrate the triumphs of 2023, we eagerly look forward to advancing our steadfast commitment to securing the digital frontier in the years to come.


Securze
Be Secured, Be Assured.
VS
BAD HACKERS
Hey Client! Your applications and servers are secured by our best analysts.
God level security! They have well secured applications and servers...

11 CYBERSECURITY CHECKLISTS

Securze's 2023 cybersecurity initiative shines through the release of 11 targeted checklists, empowering individuals and businesses to navigate the complexities of digital threats. From phishing defense to regulatory compliance, our comprehensive guides reflect our commitment to fostering a resilient and secure digital landscape.

- Professional Cyber Security Checklist for Your Business
- Professional Cyber Security Checklist for Your Website
- IRDA Information and Cyber Security Guidelines and Penalties 2023-2024
- SEBI Cyber Security Guidelines for Portfolio Managers 2023-2024
- Cybersecurity: The Dos and Don’ts for Every Employee
- Advisory for SEBI Regulated Entities REs Regarding Cyber Security 2023
- **8 Steps Guide To Identify Phishing Emails**
- Professional-Guide-On-What-To-Do-If-Youve-Been-Hit-By-Ransomware
- Must-Have-Cyber-Security-Tools-For-Every-Business
- Top 10 Common Cyber Security Mistakes Employees Make and How to Avoid Them
- Advance Network Security Checklist

MOST POPULAR ★★★ MOST POPULAR ★★★ MOST POPULAR

SAFEGUARDING INDIAN ENTERPRISES, UNMASKING CYBER THREATS, AND TRANSFORMING VULNERABILITIES INTO STRENGTHS

In 2023, Securze embarked on a remarkable journey of impact, contributing significantly to the cybersecurity resilience of numerous Indian companies across diverse sectors. Our expertise played a pivotal role in assisting multiple stock broker companies, banks, healthcare firms, gaming companies, fintech innovators, and insurance companies in identifying and addressing potential security vulnerabilities within their systems. Through diligent assessments and responsible disclosure practices, we responsibly reported security issues, working collaboratively with these organizations to implement effective solutions.

Our proactive stance extended beyond vulnerability identification, as we uncovered and reported data breaches affecting various companies. Swiftly notifying the affected parties, we not only ensured that they were promptly informed of potential risks but also delved into the identification of threat actors behind these incidents. This comprehensive approach allowed us to guide these companies through the intricate process of remediation, bolstering their cybersecurity postures and reinforcing their commitment to data protection.

In these collaborative efforts, Securze exemplified its dedication to creating a more secure digital landscape for Indian businesses. As we reflect on the positive impact achieved in 2023, we are motivated to continue our mission of safeguarding organizations and contributing to a resilient and secure future for the cybersecurity ecosystem.

ENTERING 2024...WHAT SHOULD YOU DO?

BUSINESS OWNERS & C-EXECUTIVES >>>

- Develop and enforce a **cybersecurity policy** in your organization.
- Conduct **risk assessments** and **security audits** at least once a year.
- Allocate budget and resources for cybersecurity measures.
- Foster a cybersecurity-aware culture within the organization by conducting **cyber security trainings** through experts. Implement a thorough cybersecurity training program for new hires.
- Establish an **incident response plan** and practice it regularly.
- Test the business continuity plan through **simulated cyber-attacks**. This could be exercised by conducting either VAPT or Red Teaming against the organization.
- Adopt **NIST or other cyber security frameworks** to enforce cyber secured culture in the organization. Establish a robust security governance framework.
- Ensure secure offboarding processes for departing employees. Revoke access promptly for employees who no longer require it.
- Encourage employees to report security incidents or concerns promptly.
- Develop a communication plan for addressing stakeholders during a security incident. Designate spokespersons for media and public communication.
- Provide clear and timely updates to employees, customers, and partners.

EMPLOYEES >>>

- Attend regular **cybersecurity training** sessions.
- Use **strong, unique passwords** and enable multi-factor authentication (MFA).
- Be cautious with email attachments and links; **verify sender authenticity**.
- Report any suspicious activity or potential security incidents.
- Regularly update software and systems to patch vulnerabilities.
- Use **Virtual Private Network** (VPN) for secure remote access. Only use the VPN provided by your company and not any third-party free VPN. If company has not provided a VPN service, ask them to implement for safe transfer of data.
- Ensure home **Wi-Fi is password-protected** and uses WPA3 encryption. Keep your **Wi-Fi password strong**. Do not share it with others.
- **Secure physical workspaces** to prevent unauthorized access. Lock your drawers.
- Encrypt sensitive data during transmission and storage using a key/password.
- Regularly update and patch home network devices such as your Wi-Fi router.
- Lock screens & devices when not in use, especially in shared or public spaces.
- Avoid storing sensitive information on personal devices unless necessary.
- **Report lost or stolen devices** immediately to the IT department.
- Take care of your juniors and teach them the importance of cyber security.
- Employees play a crucial role in the overall cybersecurity posture of the organization.

Securze

Be Secured, Be Assured.

For business inquiries, **contact us.**

- I find security issues in applications before a hacker finds them and damages the business, thus helping businesses identify and fix security issues at a very early stage.

Harsh Parekh
Founder, Securze

🌐 www.securze.com	securze
✉ info@securze.com	securze_com
☎ +91 84510 73938	in Securze