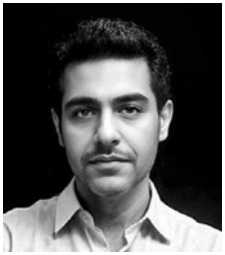

SAAIM KHAN, *Founder and Managing Director, Jumpstart Security*
www.jumpstart.security

Saaim, with over two decades in IT and cybersecurity, has a rich background in technology consulting and software development, leading to his roles as the Founder and Principal Consultant at Cyber Matters and Jumpstart Security. Known for blending business acumen with technical expertise, Saaim offers comprehensive, strategic solutions to clients worldwide. His certifications include CISM and ISO 27001, along with degrees in Software Engineering and Project Management. Saaim is committed to advancing cybersecurity knowledge and collaboration.

TIP 1 - CULTIVATE A SECURITY MINDSET

Educate your team to prioritise security in every aspect of the business. Foster an environment where everyone feels responsible for maintaining cybersecurity, understanding that their actions can protect or jeopardise the company's well-being.

TIP 2 - RECOGNISE AND REPORT PHISHING ATTEMPTS

Train employees to identify phishing emails or fraudulent communications. They should know how to verify requests for sensitive information and report suspected phishing attempts to prevent financial loss or data breaches.

TIP 3 - VET THIRD-PARTY VENDORS CAREFULLY

Ensure that any third-party services or products you use comply with high-security standards. Regularly assess their security measures and data handling practices to safeguard your business from indirect vulnerabilities.

TIP 4 - SECURE YOUR BUSINESS PREMISES PHYSICALLY

Physical security measures are crucial. Secure your office equipment, servers, and any physical documents containing sensitive information to prevent unauthorised access or theft.

TIP 5 - IMPLEMENT FINANCIAL SAFEGUARDS

Use secure, verified processes for financial transactions and keep thorough records. Educate your staff about the risks of business email compromise scams and verify any unusual payment requests directly.

TIP 6 - DEVELOP A COMPREHENSIVE CRISIS MANAGEMENT PLAN

Prepare for various types of emergencies, including cybersecurity incidents. Your plan should include communication strategies, steps to mitigate damage, and recovery procedures, ensuring business continuity.

TIP 7 - REGULARLY REVIEW AND UPDATE SECURITY POLICIES

Cyber threats evolve rapidly; so should your defences. Regularly review and update your security policies and practices to address new challenges and ensure ongoing protection.

TIP 8 - FOSTER STRONG CUSTOMER TRUST

Communicate your commitment to security to your customers. Be transparent about your data practices and respond promptly and effectively to any concerns or incidents, thereby building trust and loyalty.

TIP 9 - STAY INFORMED ABOUT EMERGING SCAMS

Stay abreast of the latest scams targeting businesses. Subscribe to cybersecurity newsletters, attend relevant webinars, and participate in industry forums to remain informed and prepared.

TIP 10 - LEVERAGE CYBER INSURANCE

Consider investing in cyber insurance to mitigate financial risks associated with data breaches, cyberattacks, and other security incidents. It can provide a safety net and support recovery efforts in the aftermath of an incident.