DICCI

CYBER CRIME ALERT

URGENT ALERT FOR DICCI MEMBERS

With deep sorrow, we mourn the tragic demise of Shri Laxman Sadhu Shinde, a respected businessman from Pune and our brother, who was kidnapped and murdered after being lured to Patna, Bihar under the guise of a fake business deal. Our heartfelt condolences go out to his family in this difficult time.

BEWARE OF CYBER FRAUD & BUSINESS SCAMS

Investigations have revealed that a criminal gang meticulously studied his business profile, contacted him through emails and phone calls, and tricked him into traveling for a fraudulent deal.

TO ENSURE YOUR SAFETY, PLEASE STAY VIGILANT

- Verify all business invitations—Crosscheck details before traveling for deals.
- Be cautious of unsolicited offers—Fraudsters exploit online information.
- Avoid large financial transactions upfront—Especially with unknown contacts.
- Share your travel details with family or trusted associates.
- Report suspicious activity to authorities immediately.

DICCI urges all members to exercise extreme caution while engaging in business discussions, particularly those initiated online. Let us honor Shri Laxman Shinde's memory by staying alert and protecting one another.

STAY SAFE. STAY AWARE.

DICCI

सतर्क

SATARK Guidelines to Avoid Cyber Frauds & Fake Business Traps for All all the Business Community

S – Scrutinize All Business Inquiries

Thoroughly verify emails, company profiles, GST/CIN, and caller IDs. Be alert to fake websites, spoofed domains, and exaggerated offers.

A – Avoid Traveling Alone

For first-time business meetings in unfamiliar cities: Take a colleague or a known contact. Prefer meeting in public or verified business spaces. Always share your itinerary with someone you trust.

T – Think Before You Click

Be cautious of links and attachments in unsolicited emails. Use antivirus software and enable spam filters. Watch out for phishing attempts and impersonation.

A – Authenticate All Deals and Documents

Validate every MoU, purchase order, or contract. Do not share confidential documents without a legal review. Be careful of urgent payment demands or fake tenders.

R – Restrict Sharing Financial Details

Never disclose OTPs, account details, or passwords over email/phone. Use secure, verified payment channels. Set up transaction alerts and daily limits.

K – Keep Your Team Trained

Regularly educate staff about cyber threats and fraud trends. Encourage a culture of verification. Teach your team to take necessary actions against frauds