10 ESSENTIAL CYBERSECURITY TIPS FOR BUSINESSES

Telecommunications providers around the world hold a wealth of cybersecurity data from their vast networks and customer bases. Members of the Global Telco Security Alliance offer 10 key insights businesses and other organizations need to know about the state of cybersecurity.

1. **Social Engineering is the Top Tactic**
   - Social engineering was the top method of compromise in 2019. 60% of incident investigators can attribute successful social engineering in the contact to lacks good of entry.

2. **100% of Web Apps are Vulnerable**
   - 100% of the web applications tested were exposed at least one vulnerability, with the median number of vulnerabilities ranging from 16 up from 11 in 2017.

3. **Sextortion Gains Ground**
   - Sextortion email campaigns, designed to spoof large companies and promote businesses, are on the rise, up 216% in 2022 compared to 2019.

4. **Cryptojacking Malware Skyrockets**
   - A steep increase year on year of 126% was observed in cryptojacking malware. Used to mine cryptocurrencies, it infects websites or infects cloud servers, encrypting sensitive data to access the mining process.

5. **Organizations Are Not Risk Driven**
   - 50% of organizations have programs that are not risk driven and are not aligned with risk management strategy. For most, the number of vulnerabilities is more than 50%.

6. **IT Security Involvement is Delayed**
   - Almost 25% of CISOs were not involved in cloud security, and CISOs are rarely involved in data breaches, which can delay the recovery process.

7. **Companies are More Vulnerable Than They Think**
   - Only 1 in 3 companies are communicating with their employees about the dangers of social engineering tactics, including spear phishing.

8. **App Detection and Remediation**
   - Malicious applications detected by less than 5 antivirus engines have a longer market shelf life, with a mean stay of over 48 days. Once a link is clicked, an attacker uses the app to detect 2% of them.

9. **Adobes is a Prime Malware Vector**
   - Among the 26 companies with the highest number of CVEs, Adobe, Microsoft, and Oracle were the top perpetrators in the quarter, with Adobe having the most vulnerabilities.

10. **Beware of Android Malware Apps**
    - Out of 2,000 applications submitted, 1,672 applications were malicious and remained on the market for over 30 days. For the most part, they were targeted by American and Russian attackers.