The complicit is the robber, not the hacker?

Bank card hacking is a persistent societal issue that needs immediate consideration at the government and the institutional level. The increasing frequency of these incidents highlights the vulnerabilities in our financial institutional mechanism and the need for stronger cybersecurity measures and legislation on the complicity aspect by the government.

Recent data breaches have exposed the sensitive information of millions of people, making it easier for hackers to commit fraud. According to a survey, the UAE, Bahrain, and Kuwait have become safe havens for individuals involved in these crimes. In some cases, hackers have managed to infiltrate financial institutions for extended periods, stealing large amounts of money. This not only causes economic losses but also erodes trust in the security of our banking systems.

Research shows that legislation has targeted the perpetrators, not the local facilitators behind this criminal societal issue worldwide. Therefore, it is necessary and timely request to the heads of government and departments consider this if they want to run a smooth system and establish peace in the countries suffering from this contagious societal sickness.

To address this issue, we need to:

1. **Enhance Cybersecurity Measures**: Financial institutions must invest in advanced security protocols and regularly update their systems to protect against new threats. Now the time has come to revisit existing protocols and strengthen with adherence to ethical values.

2. **Conduct Thorough Investigations in conjunction with moral values**: Each incident should be meticulously reviewed to understand how the breach occurred, identify the hidden hands involved, and determine the necessary steps to prevent future attacks. New protocols based on moral values should be established for the person investigating the issues. Morally corrupt individuals should not be appointed to the investigation, as it is a matter of institutional reputation, integrity, and credibility.

3. **Promote Awareness about adherence to legal and ethical values**: Educating the public about the importance of cybersecurity and how to protect their personal information can help reduce the risk of hacking.

4. **Reinforce Regulations with moral values**: Governments and regulatory bodies should enforce stricter cybersecurity standards and hold institutions accountable for non-compliance with decent values and legal protocol breaches.

5. **Institutional Responsibility:** Institutions must guarantee the security and integrity of their systems by implementing robust cybersecurity procedures, conducting thorough investigations, promoting awareness of legal and ethical values, and enforcing strict regulations to maintain reputation, credibility, and the trust of the public**.**

The above recommendations are a minimum prerequisite to track the system and maintain institutional reputation and credibility. Inherently, nobody likes to cheat or be cheated, it’s the complicit individuals who are jeopardizing the reputation and credibility of their institutions for personal gains or vendetta.

Hence, it is to be noted that Societal growth comes through peace and prosperity and is a positive indicator of progress for the institutions and the state. Therefore, the legislature and heads of the institutions are responsible for the interests and reputation of their institutions.

Author:

Engr. Arshad Naeem Chaudhry

Date:1/1.2025