NCA-06.050224: NCERT Advisory – Social Media Account Security

1. Introduction

Based on the recent responses and investigations into different incidents, NCERT has identified several critical loopholes in the management of social media accounts within organizations. These loopholes stem from negligence in security protocols, lack of access control awareness, unauthorized access and transfer of credentials, insecure storage of passwords, and unsanctioned downloads. The severity of these issues is high, with the potential for significant compromise of organizational accounts and sensitive information.

2. Impact

The exploitation of this mismanagement could result in unauthorized access to organizational social media accounts, misuse of administrative privileges, unauthorized actions on social media platforms, and exposure of sensitive information to potential breaches. Such compromises could lead to reputational damage, loss of trust, and legal implications for affected organizations.

3. Affected systems and devices

These loopholes affect organizational social media accounts across platforms such as Facebook, X, and LinkedIn. Any organization utilizing these platforms for official communication and engagement is at risk.

4. Recommendations

NCERT recommends the following measures to mitigate the risks associated with these vulnerabilities:

- Implement strict access control protocols, including formal approval processes for granting administrative privileges.

- Restrict admin access to a few designated officers only, not more than two.

- Utilize platform-specific role-based access control mechanisms to assign tailored access levels to team members.

- Enforce two-factor authentication (2FA) for all administrators to enhance account security.

- Regularly review and update access permissions to align with organizational roles and responsibilities.

- Educate team members on secure login practices, password management, and awareness of social engineering threats.

- Monitor account activity logs for signs of unauthorized access or suspicious behavior.

- Stay informed about platform regulations, guidelines, and security updates to ensure compliance.

5. Guidelines for Reporting the Breach

In case of a security breach, organizations should adhere to the following reporting guidelines:

- Officially report to the designated officer in-charge within the organization.

- Report the incident to the NCERT incident response team:

  a. **Incident Reporting Form**: https://pkcert.gov.pk/report-incident/
  b. **Email**: cert@pkcert.gov.pk

- Report the breach to relevant social media platforms for prompt action and support:
  a. **Reporting Breach to Facebook:**
  [https://www.facebook.com/hacked]
  b. **Reporting Breach to LinkedIn:**
  [https://www.linkedin.com/help/linkedin/answer/a1340402]
  c. **Reporting Breach to X:** [https://help.twitter.com/en/safety-andsecurity/x-account-compromised]

6. References

- **Facebook Page Roles**: [https://www.facebook.com/help/289207354498410]

- **X Multi-User Access**: [https://business.x.com/en/help/troubleshooting/multi-userlogin-faq.html]

- **LinkedIn Page Roles**:
  [https://www.linkedin.com/help/linkedin/answer/a541981]

- **Facebook Security Settings**:
  [https://www.facebook.com/privacy/dialog/keepyour-account-secure/]

- **X Security Features**: [https://help.twitter.com/en/safety-and-security/accountsecurity-tips]

- **LinkedIn Security Tips**:
  [https://www.linkedin.com/help/linkedin/answer/a1375084]

NCERT urges organizations to prioritize the implementation of these recommendations to safeguard their social media accounts against potential threats and loopholes in user management.