Grande Prairie Regional Association of Volunteer Organizations

101, 10101 100 Avenue
Grande Prairie, AB T8V 0V4
www.volunteergrandeprairie.com
E: info@volunteergrandeprairie.com
P: 780-538-2727 | F: 780-539-5986

We are Proud Partners of:

KEEPING YOUR ORGANIZATION'S FACEBOOK PAGE SAFE

Recently, we've seen a worrying trend happening within some of our non-profit/charitable organizations. Groups or individuals within these organizations, unhappy with their current leadership, have been taking over their Facebook pages. This usually happens due to trust issues and differing viewpoints. When these factions get hold of the password and change it, the rightful leaders lose control of their main communication tool. Recovering these pages is very difficult, and Facebook® support often can't help.

To prevent this from happening and to keep your organization's Facebook page secure, we are sharing some important steps. These steps focus on preventing issues before they start. By following them, your organization can protect its online presence and maintain a safe and effective way to communicate with your members.

Preventing Unauthorized Access and Hijacking of Organizational Facebook Pages

1. Establish Clear Access Policies:

a. **Define Roles and Responsibilities:**

- ✓ Clearly identify who is authorized to access and manage the Facebook page.
- ✓ Limit access to a small, trusted group of individuals, preferably board members or senior staff.

b. **Create a Social Media Policy:**

- ✓ Develop a comprehensive social media policy outlining acceptable use, responsibilities, and consequences for policy breaches.
- ✓ Ensure all members, staff and volunteers understand and sign the policy.

2. Strengthen Password Management:

a. **Use Strong, Unique Passwords:**

- ✓ Create strong, unique passwords for all social media accounts. Avoid easily guessable passwords.

b. **Change Passwords Regularly:**

- ✓ Implement a schedule for changing passwords (e.g., every three months).
- ✓ Change the password immediately if an authorized user leaves the organization or role.

c. **Utilize Password Managers:**

- ✓ Use a reliable password manager to store and share passwords securely among authorized users.

3. Enable Two-Factor Authentication (2FA):

a. **Set Up 2FA:**

- ✓ Enable two-factor authentication on the Facebook account. This adds an extra layer of security by requiring a second form of verification (e.g., a code sent to a mobile phone) in addition to the password.

4. Monitor Access and Activity:

a. **Regularly Review Access Logs:**

- ✓ Periodically review the Facebook account's access logs to monitor who is accessing the page and from where.
- ✓ Look for any suspicious activity or unauthorized access attempts.

b. **Assign a Monitoring Role:**

- ✓ Designate a trusted individual or committee to oversee and monitor the Facebook page's activity.

5. Develop a Crisis Management Plan:

a. **Create a Recovery Plan:**

- ✓ Develop a clear plan for regaining control of the Facebook page in case of unauthorized access.
- ✓ Include steps such as contacting Facebook support, gathering evidence, and communicating with members.

b. **Document All Procedures:**

- ✓ Maintain detailed documentation of all policies, procedures, and actions taken to secure the Facebook account.

6. Foster Trust and Communication:

a. **Promote Open Dialogue:**

- ✓ Encourage open and transparent communication among board members, staff, and volunteers to build trust.

b. **Regular Team Meetings:**

- ✓ Hold regular meetings to discuss social media policies, address concerns, and reinforce the importance of security.

7. Educate and Train Members:

a. **Provide Training:**

- ✓ Offer training sessions on social media security, password management, and the importance of 2FA.

b. **Raise Awareness:**

- ✓ Keep members informed about potential risks and best practices for maintaining account security.

8. Implement Access Controls:

a. **Limit Administrative Privileges:**

- ✓ Restrict administrative privileges to a few trusted individuals. Others should have limited access based on their role.

b. **Regularly Review Permissions:**

- ✓ Regularly review and update access permissions to ensure they align with current roles and responsibilities.

We are here to assist you in implementing these preventive measures. If you have any questions or need further support, please do not hesitate to contact us. Your organization's security is our priority, and we are committed to helping you maintain a safe and effective online presence.

Sincerely,

Carol-Anne Pasemko

Executive Director