Social Media Security Settings Checklist

Account Security

- Use a unique, strong password for each platform (Facebook, LinkedIn, Instagram, X, etc.).
- Enable Multi-Factor Authentication (MFA) on all accounts.
- Update recovery email and phone number to something current and secure.
- Review and remove any old or unused accounts.

Privacy Settings

- Limit who can see your posts and personal details (set profiles to "Friends" or "Connections" instead of "Public").
- Adjust settings so only you can see your friends list or connections.
- Turn off location sharing for posts and check-ins.
- Review who can tag you or post on your timeline.

App & Device Access

- Check which devices are logged into your accounts—log out of anything unfamiliar.
- Review and remove third-party apps with unnecessary access.
- Disable "Remember Me" on shared or public devices.

Notifications & Monitoring

- Turn on login alerts for new devices or suspicious activity.
- Review your recent login history for unusual activity.
- Set up alerts for mentions of your name or brand (protects against impersonation).

Red Flags to Watch For

- Messages from "friends" asking for money or unusual links.
- Profiles pretending to be you or your business.
- Ads or posts that look too good to be true—verify before clicking.

Pro Tip: Social media is public by design—treat every post like it could be shared outside your control.

1218 Amber Drive • 345-2900 • 1-800-465-3933 • sales@teleco.ca • Teleco.ca

TELECO
Integrating Technologies