CDSE
Center for Development of Security Excellence

SOCIAL MEDIA SAFETY
SMART CARD

SOCIAL MEDIA
CONNECTS US GLOBALLY

Maximize social media security by:

- Using secure browsing (https)
- Reviewing your history to identify unauthorized access
- Using multi-factor authentication (MFA) to secure logins

✅ DO

- Secure your accounts with complex passwords/passphrases and a password manager.
- Keep anti-virus software up to date. Only download known or trusted apps.
- Report scammers, spammers, and fake accounts. Doing that helps keep the site safer for everyone.
- Review permissions to your account and data access in your security settings periodically.
- Encourage your family and friends to take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- "Opt Out" to prevent companies from collecting your personal information and data based on your activity on websites, devices, or apps for the purpose of advertising.
- Restrict privacy settings to who can view your profile, posts, and photos to friends only.

❌ DO NOT

- Do not connect with or message strangers. Generic photographs? Incomplete profile?Odd wording in message? Be on the lookout for fake profiles.
- Do not assume your posts, photos, direct messages, location, and activities are private. Privacy settings are not a complete solution.
- Do not reveal sensitive job information.
- Do not share personal information in online quizzes; this could be used to get into your account.
- Do not click links in unsolicited chats or direct messages.
- Do not enable location sharing on social media sites.
- Do not post Personally Identifiable Information (PII), such as birthdays, bank account numbers, credit card, or Social Security information.
- Do not post or share photos that let people know you're on vacation. Be vigilant.

WARNING SIGNS
OF A SCAM

- A sense of urgency
- Money, bitcoin, or gift cards
- Deliveries that can't be delivered
- Strange activity on your accounts
- Impersonated accounts of family, friends, businesses, or well-known people
- Invoices from companies you don't recognize
- Generic text messages from numbers you don't know
- Calendar invitations from strangers

WHEN IN DOUBT, REPORT IT!