Social Media

Many of us communicate with family, friends, or even co-workers via social media. These platforms allow us to stay more connected than ever.

Regardless of how well-protected your social media account is, a good rule of thumb is to assume EVERYTHING you post on the Internet is available to EVERYONE.

Key Tips

While numerous technologies exist to protect kids on the Internet, these are only short-term safeguards. The most influential and long-term protection for kids on the Internet is their education.

1. Periodically review your privacy and security settings for each social media account. Social media sites often, by default, allow anyone around the world to see your content.

2. Watch out for phishing attempts, including messages from your friends/connections. At some point, one or more of your digital connections may be hacked by a fraudster. Be cautious if asked for personal or financial information over these channels. A friend getting hacked could result in a previously private message you sent being accessed.

3. Only accept connection requests from those you know or trust. Fraudsters regularly break into social media accounts and try to build more digital connections, leading to future scams. Be cautious of connection requests from accounts with very few connections or unknown requests that immediately ask for information or help.

4. Be mindful of what you post. Posting pictures of your family, including ages, family members, and other personal information, is a fraudster's paradise. This information can be later used to commit fraud against you.

STAR is committed to your financial security and privacy. For more tips and information, please visit STAR's security page. STAR also has a dedicated Fraud team ready to assist with any fraud-related matters.