HOW TO PROTECT YOURSELF FROM SOCIAL MEDIA MANIPULATION

Verify account authenticity

Before interacting with an unfamiliar account, check its authenticity. Look for verified badges, review profile information, and check how long the account has been active. Be cautious of new accounts with few followers or posts.

Don't accept random friend requests

Be wary of friend or connection requests from people you don't know. Attackers often send requests to gather personal information or scam you. If you receive a request from someone you already know, verify it with them through another method before accepting.

Limit personal information

Avoid sharing too much personal information on your social media profiles, such as your phone number, address, or workplace. The less information you share publicly, the harder it is for attackers to use it against you.

Report fake accounts

If you come across a suspicious or fake account, report it to the social media platform. Reporting these accounts helps remove them and prevents others from falling victim.

Beware of unusual offers

Be cautious of messages or posts that offer deals, giveaways, or opportunities that seem too good to be true. Scammers often use fake profiles to lure victims into clicking malicious links or sending money.

Look for inconsistent activity

Fake profiles may have inconsistencies, such as posts in different languages, low-quality images, or a mix of unrelated content. If the profile's activity seems erratic or inconsistent, it may be a fake account.

QUICK TIPS

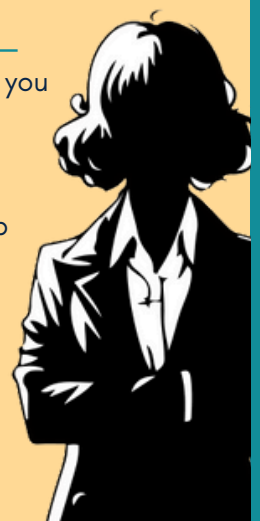
Verify before engaging—always check the legitimacy of an account before interacting with it, especially if it's unfamiliar.

Limit personal info—reduce the amount of personal information shared publicly to protect against targeted attacks.

Be cautious with friend requests—don't accept requests from people you don't know or double-check with friends if their request seems suspicious.

Report suspicious accounts—help prevent scams by reporting fake profiles to the social media platform.

Regularly review your privacy settings—regularly update your privacy settings to control who can access your information and posts.



Cyber Security Awareness Month 2024

Look Closer.
Think Smarter.

Protect Yourself from Social Media Manipulation

WHAT IS SOCIAL MEDIA MANIPULATION?

Social media manipulation occurs when cybercriminals use deceptive tactics to influence opinions, spread misinformation, or impersonate individuals to gain trust.

One of the most common forms of manipulation involves creating fake profiles—accounts designed to trick users into sharing personal information or engaging in harmful activities.

Common types of social media manipulation

Fake Profiles

Cybercriminals create fake social media accounts pretending to be someone else, such as a friend, family member, or influential figure. These accounts are used to build trust and convince victims to share personal information, money, or confidential details.

Astroturfing

This technique involves creating fake accounts to push certain opinions, ideas, or misinformation, making it seem like they come from a large group of people when in fact they are controlled by a small group or single individual.

Social Media Bots

Bots are automated accounts designed to mimic real users, often to spread misinformation, amplify certain posts, or engage in fake conversations. They can also be used to artificially inflate likes, shares, or comments to make content seem more legitimate.

Impersonation Scams

Criminals may impersonate celebrities, companies, or influencers using fake accounts to scam users, offering fake giveaways, investment opportunities, or requesting money for "charity" causes.

REMEMBER

Fake profiles are one of the most common ways cybercriminals manipulate social media users.
By staying cautious, verifying accounts, and limiting your personal information, you can protect yourself from falling victim to these deceptive tactics. Stay vigilant and help create a safer online community by reporting fake profiles when you encounter them.

RED FLAGS OF FAKE SOCIAL MEDIA PROFILES

- **Profiles with limited information or low activity.**
- **Accounts created recently with few posts or followers.**
- **Friend requests from people you don't know or duplicate requests from people you're already connected with.**
- **Unusual or generic messages, often asking for personal details or offering deals that seem too good to be true.**