Bloomingdale Public Library

Getting Started: Social Media Safety

Common Social Media Scams and Tactics

Whether we notice it or not, there are always bad actors online looking for ways to get access to your accounts. There are a few main ways that they achieve this. See the signs and know when to walk away from an online interaction that feels wrong.

Baiting

Baiting attacks use a false promise to gain a victim's attention. They lure users into a trap that steals their personal information or infect their computer with malware. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application. Examples can be no-brainer ads that say things like "Click YES if you support freedom!" or show content that triggers negative emotional reactions from viewers. This has become more common over the years with AI and bot accounts infiltrating social media platforms and companies rolling back hate speech policies and reducing accountability. Bait can also be seemingly innocent things like personality quizzes, personality tests, and fake giveaways or contests.

Workers at "click farms" can operate dozens of devices with fake social media accounts to generate likes, follows, fake reviews, etc. -CHEQ

Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit or is malware itself. A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

Phishing

Phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims, prodding them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware. An example is an email sent to a user that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to a nearly identical but illegitimate website prompting the unsuspecting user to enter their current credentials and new password, which goes straight to the hacker. Phishing is not restricted to email services; it can happen through social media platform messaging and text messages. The FTC found that social media scams accounted for $3B in losses in the last two years, most often from undelivered goods found on social media ads and text message scams.

Common social media scam types

Romance/Impersonation	Fake Giveaways	Job Offers
Investment	Online Sales	Fake Charities

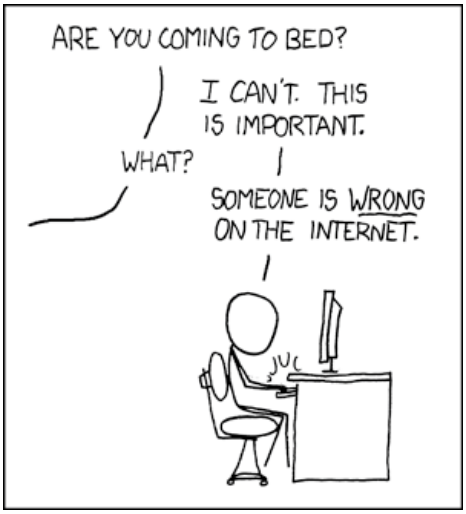
Bloomingdale Public Library

Getting Started: Social Media Safety

Simple rules for staying safe online

1. Never share your password. Sharing accounts increases risk.
2. Set up Multi-Factor Authentication to reduce vulnerability. Call, text, and app options may vary.
3. Think before you post. What information am I giving away? Who can see my post?
4. Remember, you **do not** have to reply to everything you see. Roughly 50% of all internet traffic comes from AI/bots that are trained to write emotionally triggering comments on social media. They are designed to provoke outrage and negative engagement. Clicks = advertiser money.
5. Nothing disappears on the internet. Everything posted online can be found again in a server backup or if someone takes a screenshot.
6. Review your privacy settings and check them for updates. Security settings are often updated.
7. Only accept friend requests from people you know personally. No celebrity randomly found your account. That wealthy prince isn't looking for a new benefactor.
8. Report things that look suspicious. If someone makes a strange public post, ask them about it outside of the platform. A hacked account in this scenario may say things like "Look at the deal I got on this name-brand product" and then share a weird link that clearly is not going to the official brand site.
9. Report harassment. If someone is threatening you or making remarks that are inappropriate to your relationship with them, take screenshots. Cyberbullying isn't just a problem for children.
10. Update your passwords frequently. Account data breaches happen all the time. Passwords to important things like bank accounts should not be used for social media accounts.
11. Backup important information and memories away from "the cloud" using a flash drive or blank CD. If a hacker deletes your account, sites cannot always guarantee account recovery.

Social Media Privacy Pages & General Internet Safety Tips



https://www.facebook.com/help/

https://about.instagram.com/safety

https://help.twitter.com/en/safety-and-security

https://parents.snapchat.com/safeguards-for-teens

https://support.tiktok.com/en/account-and-privacy

https://staysafeonline.org/resources/social-media/

https://staysafeonline.org/resources/online-safety-basics/

https://www.rainn.org/safe-media

https://www.imperva.com/learn/application-security/social-engineering-attack/

https://www.cisa.gov/news-events/news/staying-safe-social-networking-sites

https://www.socialmediasafety.org/

https://www.safesearchkids.com/a-teens-guide-to-social-media-safety/

https://www.samhsa.gov/kids-online-health-safety-task-force

Bloomingdale Public Library

Getting Started: Social Media Safety

*Depending on your device, you will either see the word **Settings** or a symbol like*  *or*  *for Settings. These settings options will let you reduce how much content social media apps share when you use their platforms.*

Multi-factor authentication (or 2 Factor Authentication) is an important security tool to prevent account hacking. Typically, this involves a phone number or Google Authenticator code that can only be accessed on your devices. Typically found under Settings > Security > Use Two-Factor Authentication.

Facebook Privacy Settings

Click on your profile picture > Settings & Privacy > **Privacy Checkup** this area will let you edit:

- Who can see what you share and how people can find you on Facebook.
- Your data and advertisement settings on Facebook.

Audience Selector option lets you control who sees your posts (Public, Friends, or Only Me)

Ad preferences can be found under Settings > Privacy > Ads. You cannot change the number of ads, only what type of content they feature.

Instagram Privacy Settings

Instagram accounts are Public by default. Anyone on Instagram can see your information if your account is Public. This can be changed in Settings > **Who Can See Your Content.** Private account benefits:

- Only followers you approve can follow your account.
- Only your followers can see your photos/videos on your profile or in your feed.
- Only your followers can see private accounts that you follow or follow you.

Activity Status lets people you follow and anyone you message see when you were last active or are currently online. This can be changed in Settings > **How Others Can Interact With You**. This section also allows you to select who can tag you in posts.

TikTok Privacy Settings

TikTok accounts are Public by default but parents can make their child's account private easily.

Go to your (adult) profile. Tap on the menu button in the top right-hand corner. Tap **Settings and Privacy** > **Family Pairing**. The app will walk you through how to link your accounts. Afterwards, tap your child's profile. Tap **Privacy and Safety**. Toggle ON **Private Account**. You can also change other Safety settings in this area like who can message your child.