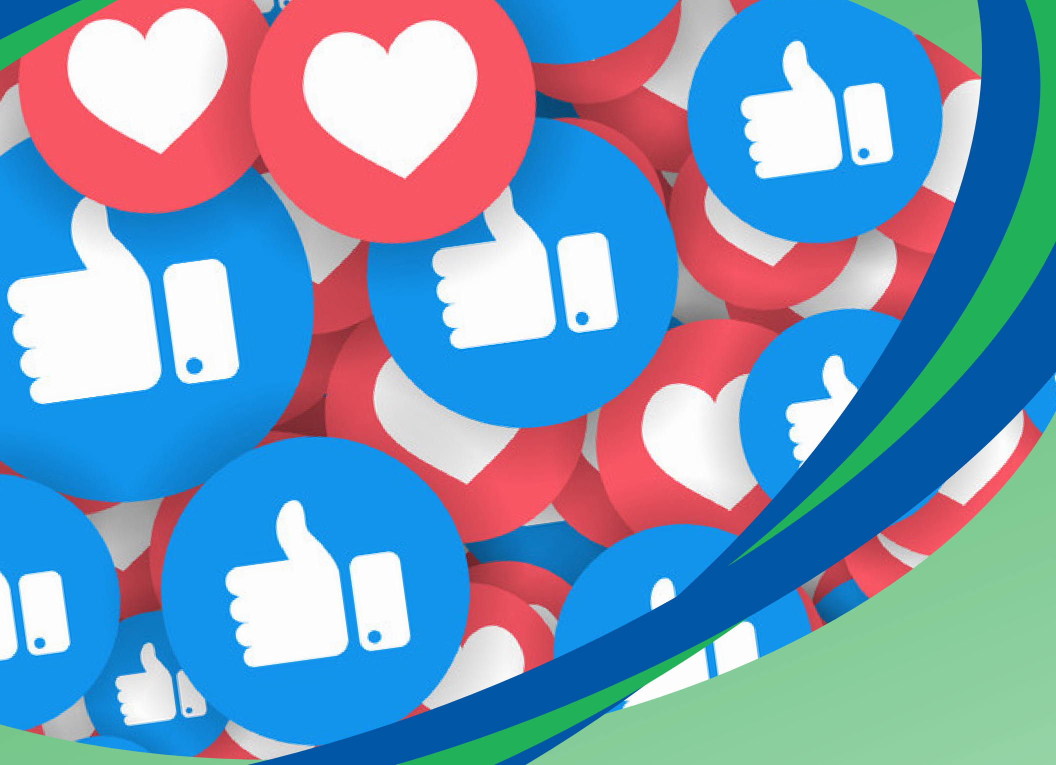

STAYING SAFE ON SOCIAL MEDIA

DIFFERENT SOCIAL MEDIA APPS AND HOW TO STAY SAFE

A TRAINING GUIDE

CSU COMPUTER SERVICES UNLIMITED

How to Stay Safe on Social Media

Social media has become a central part of our lives, and like any valuable tool (think email, smartphones, or cars), it requires management and mastery. Every day, new challenges arise to our safety and security.

Here are some ways to keep yourself protected and secure:

Treat your personal information like cash – Be cautious about who you share it with and think carefully before handing it out.

Check your settings – Even if a social media app isn't directly asking for your data, assume it may be collecting it by default. Adjust your mobile device settings (Camera, Microphone, Location, Contacts Sync) to OFF unless necessary, and reset to OFF after use.

Enable MFA (Multi-Factor Authentication) – Also known as two-factor authentication, this adds an extra layer of security, making it harder for hackers to access your accounts, even if they have your password.

Use long, strong, and unique passwords – Avoid reusing passwords and make sure they're hard to guess.

Share with care – The more you post, the easier it becomes for hackers to steal your identity or commit other crimes. Be mindful of who can see your posts; most platforms allow you to control who can view or interact with your content.

Think before you post – Remember that posts can linger forever and may come back to haunt you later.

Be selective with connection requests – Don't accept invitations from just anyone. Many social networks let you manage what information you share with different groups of friends.

Facebook

With nearly 3 billion users, Facebook is the most popular social media platform. But with its widespread use comes potential risks. It's easy to fall victim to scams when everything seems so friendly and inviting!

Visit facebook.com/help and adjust your settings under Privacy, Safety, and Security to activate important security measures you might not be aware of:

- **Security Features and Tips**: Enable alerts to notify you if someone tries to log into your account.
- **Your Privacy**: Customize who can view your Friends list, setting it to your desired level of privacy.
- **Control who can see what you share**: Use the audience selector to decide who can see each post. You can also adjust the audience after posting.

Stay vigilant and watch out for:

- Account-related scams
- "Free stuff" offers from third parties
- Charity and disaster relief scams
- Curiosity traps

Sources and additional information:

•**Privacy, Safety and Security**
https://www.facebook.com/help
•**7 Urgent Steps to Take When Your Facebook Account Gets Hacked**
(https://www.searchenginejournal.com/facebook-account-hacked/)
•**Facebook users can apply for their portion of a $725 million lawsuit settlement** (https://actsmartit.com/facebook-users-can-apply-for-their-portion-of-a-725-million-lawsuit-settlement/)

Reddit

Reddit is a popular platform for social news aggregation, content rating, and discussions. Registered users can submit links, text posts, images, and videos, which are then upvoted or downvoted by other members. As with any online platform, it's important to verify the accuracy of any information you come across.

How to Stay Safe on Reddit:

- Use a dedicated email address just for your Reddit account.
- Choose a username that doesn't reveal any personal information.
- Create a strong, unique password.
- Enable two-factor authentication for added security.
- Disable Google indexing for your account to keep your posts
- hidden from search results.
- Avoid sharing personal details that could identify you in real life, such as:
    - Your job or employer
    - Your home location
    - Personal information like your date of birth
    - Items you own
- Be cautious with links. Malicious users may use URL shorteners to lead you to dangerous sites, launch phishing attacks, place tracking cookies, or gather your personal information.

Sources and additional information:
https://www.expressvpn.com/blog/is-reddit-safe/
•Reddit was breached in February 2023. Although it appears that no user data or passwords were accessed, users should implement 2-factor authentication and change their passwords. Also, this is another example of why you should not use the same passwords on any accounts.
Source:
Reddit admits security breach (https://cybernews.com/news/reddit-admits-security-breach/)

LinkedIn

LinkedIn is often considered the “business” social media platform, but it’s not without its risks. Along with common scams like romance and crypto investment schemes, employment scams are also widespread. In these scams, recruiters may ask for sensitive personal information such as your Social Security number (SSN), bank account details, or even a credit report after you apply for a job.

Here’s what to watch for:

- Be wary of unsolicited job offers that seem too good to be true. If something catches your eye, double-check its legitimacy by visiting the company’s official website.
- When submitting your resume, only share publicly available information. Avoid including personal details like your phone number, address, or identification numbers.
- Be cautious of employers conducting interviews via text-only communication, particularly on encrypted messaging apps like WhatsApp or Telegram.
- Never purchase a credit report to share with an employer. Any job that requests this is likely a scam.

Sources and additional information:
•**Is LinkedIn Safe?** (https://techboomers.com/t/is-linkedin-safe)
•**LinkedIn deploys new secure identity verification for all members** (https://www.scmagazine.com/news/identity-and-access/linkedin-deploys-new-secure-identity-verification-for-all-members)

TikTok

While influencers may not be pleased, many governments—including our own—view TikTok as a significant threat to your privacy and security. The FBI and Federal Communications Commission have raised concerns that ByteDance could potentially share TikTok user data—such as browsing history, location, and biometric identifiers—with China's authoritarian government. As a result, authorities in North America, Europe, and the Asia-Pacific region have banned the TikTok app on government-issued devices and those used for official purposes due to cybersecurity concerns.

Here's some of the information TikTok collects:

- Profile details like your age, language, phone number, photo, and email address
- Data from third-party accounts (e.g., Facebook or Google) linked to your TikTok account
- Content you upload, such as photos and videos Information gathered from other "publicly available sources"
- Your search history on TikTok
- Device information, including your IP address, mobile carrier, time zone, and app/file names on your phone
- Keystroke patterns or rhythms
- Location data
- Messages sent and received from other users

TikTok (continued)

Once TikTok has access to your information, the company uses it for various purposes. This includes personalizing the content on your For You Page (FYP) and targeting you with ads. TikTok also shares your data with third parties.

Concerns grew in December when ByteDance revealed it had fired four employees who had accessed data on journalists from *Buzzfeed News* and *The Financial Times* while trying to identify the source of a leaked report about the company.

SCAMS? Yes, the Federal Trade Commission (FTC) labels TikTok a hotspot for scammers. The platform features many of the same scams found on other social media sites, including romance scams, investment scams, and phishing schemes. One common scam involves "follower" or "like" offers, where scammers promise to boost your followers or video likes for a small fee to make you appear as a TikTok star. The best response? Block them and report them as spam.

Finally, be cautious of TikTok trends. The platform is known for fueling dangerous challenges, such as the BORG drinking trend. If your child or teen uses TikTok, make sure you're aware of the latest trends and have conversations about them to ensure their safety.

Sources and additional information:

- **Why TikTok's security risks keep raising fears** (https://apnews.com/article/tik-tok-ceo-shou-zi-chew-security-risk-cc36f36801d84fc0652112fa461ef140)
- **Why TikTok is being banned on gov't phones in US and beyond** (https://apnews.com/article/why-is-tiktok-being-banned-7d2de01d3ac5ab2b8ec2239dc7f2b20d)
- **Is TikTok Safe?** Here's what you need to know (https://www.safewise.com/is-tiktok-safe/)

SnapChat

Snapchat is a private messaging app where content disappears quickly, making it seem like an unlikely target for hackers. But why would someone hack Snapchat? The main motives could include spying, blackmail, or stealing sensitive information such as phone numbers, passwords, and more.

How to Spot a Fake Snapchat Account:

- Check their Snap score. This shows how active they are on the platform. If they claim to be an influencer but have a Snap score in the low hundreds, it's likely a scam.
- Look at the Snap Map. Does their location match the one in their profile? Be cautious if there's a mismatch.
- Reverse image search. Use Google Image Search to check if their profile or story photos have been stolen from other sources. Scammers often use images from the internet for fake accounts.
- Check for a Bitmoji. Bitmojis are common on Snapchat. If an account doesn't have one, it could be a red flag.
- Consider their requests. If a random account adds you and asks for "help" or sends strange links, block them immediately. Similarly, if a friend sends you odd messages, contact them via another platform to confirm their safety.

Fake accounts often feature glamorous individuals showing off luxury items, sports cars, or large sums of money. Remember the golden rule of fraud prevention: "If it seems too good to be true, it probably is."

SnapChat (continued)

How to Prevent Snapchat Scams:

- Be cautious with links and QR codes, even if they come from friends or look-alike Snapchat emails. Use antivirus software for extra protection.
- Avoid adding strangers or accepting unknown friend requests. Verify suspicious activity by contacting friends directly through other channels if needed.
- Never share login details or respond to threatening messages. Snapchat will never ask for your password or passcode.
- Use a strong, unique password with at least 10 characters, including letters, numbers, and symbols. Consider a password manager.
- Enable Two-Factor Authentication (2FA) with an authenticator app like Google Authenticator, not SMS.
- Adjust privacy settings to limit who can send you Snaps, view Stories, or track your location, and consider using Ghost Mode.
- Keep your contact info updated to help recover your account if necessary.

These security tips ensure you and your teen can still have fun on Snapchat without putting their identity or your financial information at risk.

Sources and additional information:

•Anyone Can Hack Your Snapchat—Here's How to Stop Them
(https://www.makeuseof.com/how-to-hack-snapchat/)
•Snapchat Scams: Don't Fall for These 7 Insidious Scams
(https://www.aura.com/learn/snapchat-scams)

YouTube

While it's rare to get a virus directly from watching YouTube videos, there are still significant risks on the platform. Cybercriminals often trick users into clicking on links that install malicious software. These traps can be easier to fall for than you might think.

Here are some safety tips to follow:

- Avoid clicking links in video descriptions.
- Be cautious in the YouTube comments section.
- Video ads may lead to harmful sites.
- Enable YouTube's Restricted Mode for kids and consider using the YouTube Kids app.

AI-powered threats also pose risks. Some AI-generated YouTube tutorials promote malware like Raccoon, RedLine, and Vidar. These videos often disguise themselves as tutorials for downloading cracked software like Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD, and other paid programs, aiming to steal personal information.

Sources and additional information:

•**Can you get a YouTube virus?** (https://www.pandasecurity.com/en/mediacenter/mobile-news/youtube-virus-tips/)

•**Warning: AI-generated YouTube Video Tutorials Spreading Infostealer Malware** (https://thehackernews.com/2023/03/warning-ai-generated-youtube-video.html)

WhatsApp

WhatsApp lets users send texts, voice recordings, make calls, share documents, and more. While it's not primarily a "business" app, many people use it, so it's important to keep you and your data safe!

WhatsApp recently updated its policy to allow sharing information with other company-owned apps (Meta owns Facebook, Instagram, and YouTube). This could include data like your phone number, status updates, profile pictures, location, and messaging activity, depending on your settings. However, messages remain encrypted and, according to the privacy policy, should not be accessible to other apps.

Common WhatsApp scams include Family Emergency scams, Kidnapping scams, Account Takeover scams, Government Impersonation scams, Giveaway scams, Cryptocurrency scams, and Online Romance scams. These scams may urge immediate action, contain grammatical errors, come from unknown numbers, offer random giveaways, include suspicious links, or be sent from unusually long numbers.

Before taking any action, verify the request's legitimacy by contacting the person or organization directly. Never share personal or account information, and block any suspicious accounts.

Sources and additional information:

•**How To Avoid WhatsApp Scams** (https://money.com/how-to-avoid-whatsapp-scams/)
•**WhatsApp accessing microphone on Google Pixel 7, Galaxy S23 even when not in use**: reports (https://insiderpaper.com/whatsapp-using-microphone-on-google-pixel-7-galaxy-s23-even-when-not-in-use/

CSU COMPUTER
SERVICES UNLIMITED

14240-G Sullyfield Circle
Chantilly, VA 20151

Phone: 703-968-2600

Websites: csuinc.com,
vetitservices.com, csugov.com