CSU COMPUTER SERVICES UNLIMITED

Serving our community and Providing IT Service for over 30 years

Simplyifying Your Technology and Your Business.

14240-G Sullyfield Circle, Chantilly, VA 20151
Phone: 703-968-2600 | Fax: 703-968-5562
Website: www.csuinc.com

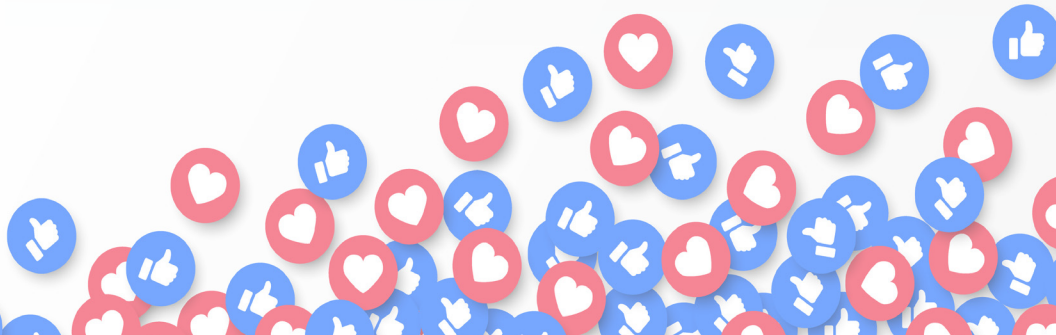
We Are Committed to Keeping You Connected.

CSU COMPUTER SERVICES UNLIMITED

Training Series

Presents...

Social Media: Is Your Business Being Smart and Staying Safe?



How to Stay Safe on Social Media

Our social media apps are part of our lives and like any convenient tool (think email, your smart phone and car) they need to be managed and mastered. Every day brings new challenges to your safety and security.

Here are some of the ways to keep yourself **protected and secure:**

1. ***Treat your personal info like cash*** *and think hard before you give it away*

2. ***Check your settings.*** *Even if the social media app isn't asking you for data, assume that it is collecting it with your implied acceptance. Mark your mobile device settings (Camera, Microphone, Location, Sync contacts) to OFF until they are needed for that function and then reset the default to OFF.*

3. ***Enable MFA (Multi-factor authentication also known as 2 factor authentication.*** It makes it hard for hackers to access your online accounts, even if they know your passwords.

4. ***Use long, strong and unique passwords.***

5. ***Share with Care!*** *The more information that you post, the easier it is for hackers to steal your identity and commit other crimes. Think who you allow to see your personal posts; most platforms allow you to limit who can see or engage with you.*

6. ***THINK BEFORE YOU POST!*** *Posts stay around forever and may come back to haunt you!*

7. ***Think twice before accepting a request or invitation to connect from just anyone.*** *Many social media networks have tools that allow you to manage the info you share with friends in different groups.*

Facebook

With almost 3 Billion users, Facebook is the **most used** social media app. Of course, it comes with dangers. It's easy to be scammed when everything looks so friendly and nice!

Go to Facebook.com/help and adjust your settings under Privacy, Safety and Security for some of the security measures you may not know about:

Under Security Features and Tips: get alerts when someone tries to login to your account.

Under Your Privacy: Adjust who can see your Friends section and set to your comfort level

Under Control who can see what you share on Facebook: use the audience selector to pick who you want to see the post. You can also change who it's shared with after posting.

Also watch for:

- **Account related scams**
- **Free stuff from third parties**
- **Disaster relief and other charity 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/)

LinkedIn

Considered the "Business" social media app, LinkedIn still has many traps. Along with the usual scam (romance, crypto investment, etc) **employment scams are rampant!** Once you apply, the recruiter asks you for personal data, such as your Social Security number (SSN), bank account information, or a credit report.

Here's what to look for:

•Be suspicious of unsolicited job pitches that seem too good to be true. If any offer piques your interest, verify that it's a legitimate opening by looking on the company's official website.

•When submitting a resume, only disclose publicly available information. Don't share details like your phone number, address, or identification numbers.

•Beware of employers who do text-only interviews, especially on encrypted chat apps like WhatsApp or Telegram.

•Never buy a credit report to share with an employer. Any job that requests this is 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

The "Influencers aren't happy but many governments, including our own think that TikTok is a huge threat to your privacy and security. The FBI and Federal Communications Commission officials have warned that ByteDance could share TikTok user data — such as browsing history, location, and biometric identifiers — with China's authoritarian government. Authorities in North America, Europe and Asia-Pacific have banned the TikTok app, mostly on government-issued phones or devices used for official business, citing cybersecurity concerns.

Among the information that they collect:

- Any information you add to your profile, like age, language, phone number, photo, and email address
- Any information it can gain from third-party accounts (like Facebook or Google) you link to your TikTok account
- Any content you upload, like photos and videos
- Information it can find about you from other "publicly available sources"
- Information about what you searched for on TikTok
- Information about your phone, including your IP address, your mobile carrier, time zone, and app and file names found on your phone
- Keystroke patterns or rhythms
- Location data
- Messages you send and receive from other users

TikTok (continued)

Once TikTok has your information, the company uses it. Some of the uses include tailoring what type of TikTok videos show up in your FYP (For You Page) and learning how to target you with ads. Tik Tok also shares your information with third parties. Concerns around TikTok were heightened in December when ByteDance said it fired four employees who accessed data on journalists from Buzzfeed News and The Financial Times while attempting to track down the source of a leaked report about the company.

SCAMS? Yes, The Federal Trade Commission (FTC) considers TikTok a goldmine for scammers. TikTok has many of the same scams that other social media apps have: **Romance Scams, Investment Sams and Phishing Scams** abound. Follower or like scams are where the messenger promises that, for a low fee, they'll boost your followers or video likes to make you look like a TikTok star. Just block them and report them for spam. Finally, **beware of TikTok trends**. TikTok is a breeding ground for dangerous trends like the BORG drinking trend. If you have a kiddo or teen on the app, be sure to stay on top of the latest trends and talk to your child about them.

Sources and additional information:

- **Why TikTok's security risks keep raising fears** (https://apnews.com/article/tik-tok-ceo-shou-zi-chew-security-risk-cc36f36801d84fc052112fa461ef140)
- **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 short-lived content is shared, so it may seem like an unsuspecting platform for hackers. You might be curious as to why someone would hack Snapchat. The main motives could be **illegally spying, blackmailing, or obtaining private information like your phone number, passwords, etc.**

How To Tell A Fake Snapchat Account From a Real One:

• Check their Snap score. This will show if they're actively using the platform. If they claim to be an influencer and have a Snap score of just a few hundred, it's likely a scam.

• Look at the Snap map. Does their real-life location match what they say in their profile?

• Search their profile/story photos in Google image search. Scammers will steal images from other sites and use them for their fake accounts. Upload a photo to Google image search to see where it came from.

• Check if they have a Bitmoji. A Bitmoji is the cartoon avatar by a person's name. Because it's so common for Snapchat users to have these, it can be a red flag if an account isn't using one.

• Think about what they're asking you. If a random account adds you and starts asking for "help" or sending you strange links, you should probably block them. This also goes for your friends. If someone you know starts sending you strange messages, contact them on a different platform and ask if everything's OK.

Fake accounts often feature attractive models and people flaunting cash, luxury goods, and sports cars. But never forget 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 suspicious of all links and QR codes in messages, even if they come from your friends (whose accounts may be hacked) or a lookalike Snapchat email. For added security, consider using antivirus software. This will automatically block malware and other malicious viruses for you.

• Never add strangers to your Friends List or accept unknown friend requests, even if they claim to be someone you might know.

• Text, email, or call your friends if you see sketchy behavior. Let them know their account may have been hacked.

• Never share your login credentials or trust threatening messages claiming to come from Snapchat. Snapchat will never leak your images or ask for your password or My Eyes Only passcode.

• Always create a strong password to prevent scammers from hacking into your account. Use a unique, hard-to-guess combination of at least 10 upper and lowercase letters, numbers, and symbols. Don't reuse this password for anything else. To help you keep track of these long passwords, consider a password manager.

•Set up Two-Factor Authentication (2FA) - but not SMS. 2FA makes your Snapchat more secure by sending a unique code to your device anytime you log in. However, hackers can bypass SMS authentication if they get access to your phone. Instead, use an authenticator app like Okta or Google.

•Adjust your privacy settings. Limit who can send you Snaps, view your Stories, see you in Quick Add, and find your location on Snap Map. Consider turning on Ghost Mode, so no one can see where you are.

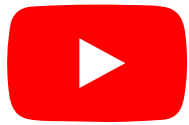
•Keep your email and phone number associated with your account updated. This will help verify that your account belongs to you if you ever lose access to it. These security tips ensure you and your teen can still have fun on Snapchat without putting their identity or your financial information at risk.

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 unlikely you'll ever get a YouTube virus from watching videos, real dangers exist on the site. Cyber criminals trick us into clicking links so they can install malicious software on our devices. Falling for such nefarious traps is easier than you think.

Here are some good rules to follow:

- Avoid clicking video description links
- Beware the YouTube comments section
- Video ads can lead you astray
- Enable YouTube Restricted Mode for Kids and Download the YouTube Kids App

AI also gets in on the act... Artificial Intelligence-generated YouTube Video Tutorials spread a variety of stealer malware such as
Raccoon, RedLine, and Vidar. The videos lure users by pretending to be tutorials on downloading cracked software versions such as Photoshop, Premiere Pro, Autodesk 3ds Max, AutoCAD, and other licensed products available only to paid users.

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 allows users to send texts and voice recordings, make video and voice calls, share documents and more.
Although we don't consider it a "business" app, we know that a lot of people use it, so we need to keep you and your data safe!
WhatsApp has made a change to their policy which allows them to share iformation with their other company-owned applications. (Meta owns Facebook, YouTube, and Instagram). This includes information like your cell phone number, status updates, profile pictures, locations and messaging activity depending on your settings. According to the privacy policy, messages remain encrypted and should not be accessed by other applications.

WhatsApp scams include **Family Emergency scams, Kidnapping scams, Account Takeover scams, Government Impersonator scams, Giveaway scams, Cryptocurrency scams, and Online Romance scams** to name some of the more prevalent. They will ask you to take immediate action, may include grammatical errors, come from unknown phone numbers, say you've won a random giveaway, include unfamiliar links, and may be sent from unusually long phone numbers.Before you do anything, verify the legitimacy of the request. Contact the person or company directly.
Don't share any account or private information.

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/

Reddit

Reddit is a social news aggregation, content rating, and discussion website. Registered users submit content to the site such as links, text posts, images, and videos, which are then voted up or down by other members.As with other platforms, you need to assess any information that you get for accuracy.

How to Stay Safe On Reddit:

How to keep yourself safe on Reddit

1. Sign in with an email that you use just for Reddit.
2. Create a username that does not contain clues to your identity.
3. Create a strong password.
4. Enable two-factor authentication.
5. Disable the ability for your account to be indexed by Google, thereby keeping your posts hidden from search results.
6. Avoid discussing anything that could identify you in real life. This includes:
   - oYour employment
   - oWhere you live
   - oPersonal details such as your date of birth
   - oThings you own
7. Be wary about the links you click, as malicious actors can use URL shorteners to direct you to dangerous sites, leave you vulnerable to phishing attacks, put cookies on your computer, and gather personal information about you.

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/)