

Protect Your Social Media Accounts

Bad actors are constantly looking for new ways to find personal information, and your personal social media accounts are no exception to that.

Your social media accounts are more than just a collection of your favorite photos, fun ideas, and personal relationships. It is a collection of personal information that can be easily obtained by bad actors and used for targeted attacks.

What information could my personal social media accounts hold?

- Contact information
- Data of birth
- Time and personal location
- Financial information
- SSN
- Personal information and hobbies
- Email addresses
- Home address
- List of closest contacts of friends and family

Protect your sensitive information on your social media accounts.

Be cautious about what you post online by asking these questions first:

- Could this assist a cybercriminal in answering a security question or guessing my password?
- Could a bad actor use this information to commit identity fraud?
- Could someone use information from my profile or specific posts to determine if I am home or on the road?
- Could any of this information hurt my reputation? How might my digital footprint be impacted by this content?

Stay vigilant and be skeptical before you click:

- Not all posts and direct messages from friends are real. Use your cybersecurity intuition to determine if you can trust the messenger or not. You can always double check with a friend on if they sent you something via communications like calling, text, or talking to them in person.
- Be cautious of giving over social media account access to other applications and software's that may ask for it. Ensure that the third-party service is legitimate before handing over access to your social media accounts as social media viruses can arise by sharing account access.
- Only accept friend requests from people you know. Many fake accounts are made replicating friends/families profile photos and will attempt to friend everyone which could lead to potential financial fraud. If you see a new account friend request from someone you know, double check that it is them before interacting with them or accepting the request.

Keep your social media account secure:

- It is recommended that you keep your social media account profile private. Vet the amount of people who you befriend and restrict access from robots and unwanted users.
- Enable Multi-Factor Authentication for your accounts and turn on additional security settings in your account settings.

-
- Control the application preferences on your mobile devices. Social media apps are typically free and try to make money by selling user data. Turn off settings like access to camera, microphone, and location tracking when you are not using the app.

Social Media Security Checklist:

- ☐ Avoid oversharing on your posts, profile, and photos.
- ☐ Enable Multi-Factor Authentication for your account.
- ☐ Use different strong passwords for each social media account.
- ☐ Reject unknown friend requests.
- ☐ Avoid using unsecure public networks while accessing your accounts/using internet.
- ☐ Examine your available security settings and privacy controls.

This material is for general information only and is not intended to provide specific advice or recommendations for any individual. This material was prepared by LPL Financial, LLC

Tracking #656290 (Exp. 11/27)