**How To Identify Scams On Social Media**

Posted on [November 15, 2024](https://blogs.k-state.edu/it-news/2024/11/15/how-to-identify-scams-on-social-media/) by [Cathy Rodriguez](https://blogs.k-state.edu/it-news/author/cathyr/)

Communications Strategist - Div Communications and Mrktg

Shared by Deb Andres, K-State Research & Extension

Family & Consumer Sciences Agent

Flint Hills District



Social media is a powerful tool for connecting with friends, sharing experiences, and discovering new content. But it’s also a hotspot for scams. Cybercriminals use clever tactics to trick users into giving up personal information, money, or even access to their accounts. Follow these tips to learn how to spot these scams on social media.

**Watch for Red Flags in Messages**

Scammers often send messages that look like they’re from someone you know or a trusted company. These messages might ask for personal information, like your password or Social Security number, or try to get you to click on a suspicious link. Be cautious if:

* The message seems urgent or too good to be true.
* The person asks for money, especially through gift cards or wire transfers.
* The language or tone doesn’t sound like the person you know.

**Be Wary of Unverified Accounts**

Before you trust a profile or page, check for verification. Official accounts often have a verification badge—a blue checkmark on platforms like Twitter or Facebook. Scammers sometimes create fake accounts that look almost identical to real ones. Look for these signs of a fake account:

* The username or handle is slightly off (e.g., extra letters or numbers).
* The account has few followers or posts.
* The content is repetitive or copied from other sources.

**Question Unsolicited Offers**

If you receive an unexpected offer for a prize, job, or investment opportunity, proceed with caution. Scammers often lure victims with promises of easy money or amazing deals. Before you engage, ask yourself:

* Did I enter a contest? (If not, it’s likely a scam.)
* Why would a legitimate company offer this out of the blue?
* Can I find reviews or information about this offer from trustworthy sources?

**Source:** [**https://blogs.k-state.edu/it-news/2024/11/15/how-to-identify-scams-on-social-media/**](https://blogs.k-state.edu/it-news/2024/11/15/how-to-identify-scams-on-social-media/)

*Making connections for youth, families, and communities – Deb Andres*

**How To Identify Scams On Social Media**

Posted on [November 15, 2024](https://blogs.k-state.edu/it-news/2024/11/15/how-to-identify-scams-on-social-media/) by [Cathy Rodriguez](https://blogs.k-state.edu/it-news/author/cathyr/)

Communications Strategist - Div Communications and Mrktg

Shared by Deb Andres, K-State Research & Extension

Family & Consumer Sciences Agent

Flint Hills District

**Part 2**

Last week, I shared the first in a 2-part article written by Cathy Rodriguez with the Kansas State University IT department. The article shared that there has been $2.7 billion dollars lost since 2021 through social media scams.

During this holiday season of elevated advertising and purchasing, it’s more important than ever to protect your money by being aware of the many ways you can get scammed. In this second part article, Cathy provides some additional safeguards to use as you engage in various social media platforms.

**Avoid Clicking on Suspicious Links**

Links in posts, messages, or ads can lead to harmful websites designed to steal your information. These sites might look like real ones but will ask you to log in or enter sensitive information. Protect yourself by:

* Hovering over links to see where they actually lead before clicking.
* Avoiding links that shorten or obscure the real destination.
* Only logging in to websites by typing the URL directly into your browser.

**Don’t Share Too Much Personal Information**

Scammers can use your publicly shared information to target you more effectively. Be careful about what you post on your profile and in your posts. Limit the personal details you share, such as:

* Your phone number, address, or email.
* Information about your family, like your mother’s maiden name.
* Details about your daily routines or travel plans.
* Be leery of quizzes and personality tests. These tests seem like harmless fun. However, these tests have become a jackpot for scammers due to their popularity.  When you open a quiz or personality test on social media, the platform will ask you for access to your profile information. When you encounter a quiz or social media test that asks for unnecessary personal details or permissions, do not proceed.

**Report Suspicious Activity**

If you come across a potential scam, report it to the platform immediately. Social media companies rely on user reports to identify and remove scams. Reporting helps protect others from falling victim as well.

Protect Yourself on Social Media

People are losing over [$2.7 billion](https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers) in total losses due to social media scams. That figure alone should be enough to convince you to be cautious online. When on social media, always think before you click and adopt a skeptical attitude towards unsolicited messages or offers. When in doubt, always err on the side of caution.

Stay safe, and think before you click! *Making connections for youth, families, and communities – Deb Andres*

**Source:** [**https://blogs.k-state.edu/it-news/2024/11/15/how-to-identify-scams-on-social-media/**](https://blogs.k-state.edu/it-news/2024/11/15/how-to-identify-scams-on-social-media/)