Toxic tagging is rampant on social media: Here's how to stay safe!

Have you been tagged by someone on Facebook, X or another social networking service? It's possible it's a scam, especially if it includes a link.

Don't click that link!

These accounts can involve complete strangers or people you know. This is called malicious tagging, a practice increasingly used by scammers.

How does the malicious tagging trick work?

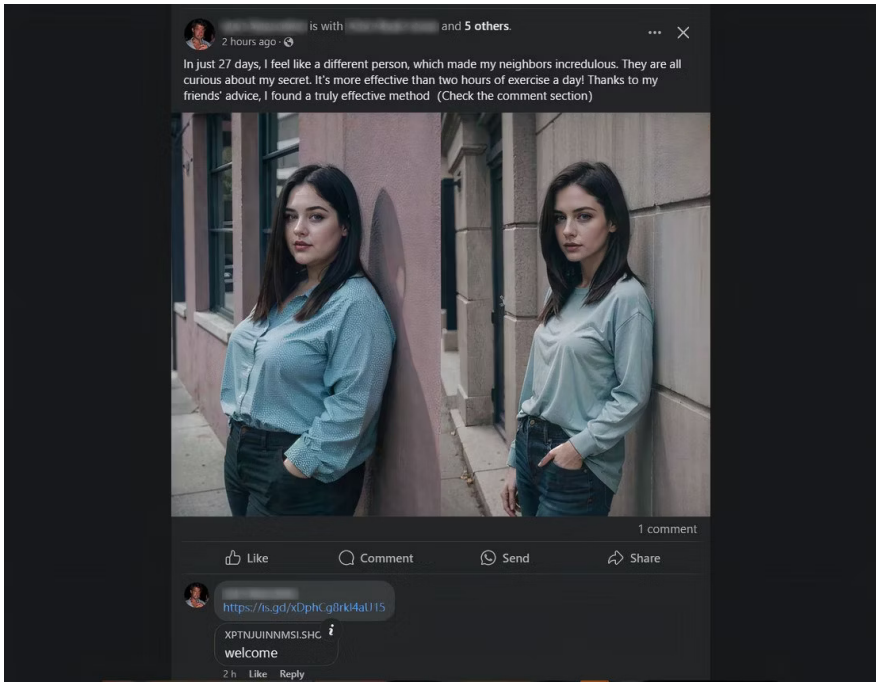
Hackers create fake accounts or take over real profiles on social networks and find other accounts to try to take over. They then tag those accounts in a message and include a link. The message can be just a link or more often they lure the victim by writing something to urge them to click.

When victims click on this link, they unknowingly download malware or are redirected to a malicious website. This can lead to further infections or theft of personal data through phishing.

If cybercriminals have enough details, they can also take over victims' social media accounts and spread the scam even further.

How to detect malicious tagging on social networks

You'll see this scam on many social media sites, but most commonly on X (formerly Twitter) and Facebook. Facebook made this scam more widespread by allowing accounts to tag people in a specific group. On Facebook, these messages are often added as comments below another post.



What does malicious tagging look like? Perhaps you have encountered examples. Usually, they include a link with brief content. This could be a promise of a gift, a mention of a big news story, or something as casual as "I think you'll like this."

URLs are often long and meaningless, meaning they do not lead to a recognized website. They can also come with fake images, often created using AI.

What to do if you get tagged in a suspicious link?

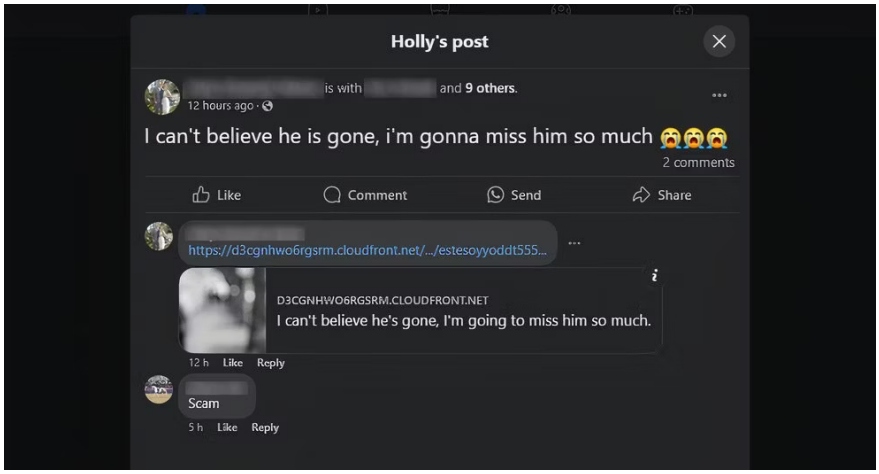
Do not click on any links.

They are malicious and can download malware to your device or steal your personal information.

So, what are the next steps to take?

The first is to just ignore it. Most people do the same. There is nothing wrong with choosing this option, but others may still fall for the scam.

If commenters have tagged people in a Facebook group, you can warn others about the danger. It's a community-minded thing to do, and I'm sure others will appreciate it. This will help ensure people don't get scammed.



Likewise, you can flag fake or hijacked accounts to fight cybercriminals. Social media apps have many different ways to do this. For example, on X, you have to go to the Help Center. On Facebook, you need to send a report via the **Find support or report profile** button on the offending account.

Note : You should limit who can contact you on Facebook and other social networking sites to reduce the risk of being scammed or of your private data falling into the wrong hands.

What to do if you have clicked on a malicious link?

First, don't provide any personal information. You should never give any private data to strangers - or any website you don't trust 100%. Even personally identifiable information (PII) like your name and date of birth is valuable to cybercriminals.

If you've given away private data, re-evaluate what you've given away to hackers. If that data includes account details, you'll need to quickly change your password in another tab or on another device.

Financial information is rarely stolen through this type of scam, but if it is, you should contact your bank or financial institution immediately.

Regardless of your device, you should scan your system with antivirus software. iPhones and iPads don't need security software, so just close any page the malicious link leads to and you'll be fine. Android or jailbroken devices are a different matter and should be scanned.

If you click on a malicious link on your PC or laptop, you definitely need to scan it with antivirus software. Check recent downloads as well. Scammers can easily install malware by tagging you on social media. Fraudulent applications may also have been added to your system.

Yes, malicious tagging is a headache, but as long as you stay vigilant, you can beat the scammers.

You finished reading the article "**Toxic tagging is rampant on social media: Here's how to stay safe!**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.