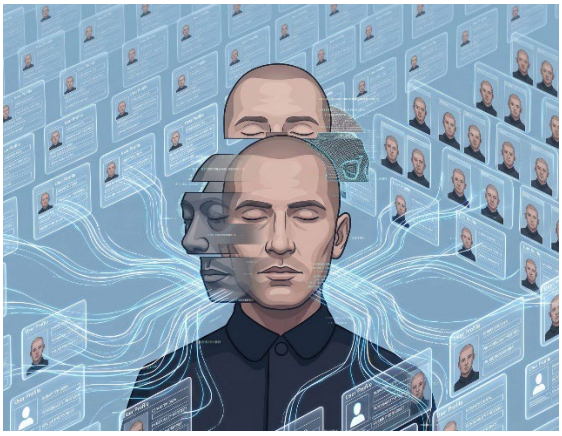
Protect Yourself from Social Media Account Takeovers



Your social media account contains valuable personal information, making it a target for cybercriminals. A social media account takeover can give a scammer access to your private messages, photos, contacts, and even your identity. Even if they don't gain access to your account, they may create a convincing fake profile that impersonates you – this is called profile cloning. Even then, the scammer can try to take advantage of your friends by impersonating you — for example, by trying to sell them fake designer sunglasses.

Fortunately, many social media account attacks can be prevented by following a few cybersecurity best practices.

What is a social media account takeover?

A social media account takeover happens when someone gains unauthorized access to your account and uses it as if they were you. Once inside, they might:

- Change your password and lock you out
- Send scam messages to your friends or followers
- Share malicious links or fake promotions
- Attempt to steal money or personal information from your contacts
- Use your account to spread malware or misinformation

Account takeovers often happen because attackers obtain your login credentials through phishing scams, password reuse, data breaches, or malware. You can control some of this by following some habits, like not reusing passwords or turning on multifactor authentication. In some cases, like if there was a data breach at the platform, you might not have much control besides taking steps like changing your password after finding out about the breach.

Not every social media scam is a hacked account: Profile cloning

Sometimes criminals don't need to hack your account at all. Instead, they create a fake social media profile using your publicly available information, such as your name, profile photo, and bio. This is often called profile cloning or account impersonation. The fake account may then send friend requests or direct messages to people you know. Because the profile looks legitimate, your friends or family may trust it without realizing its fake.

A cloned profile can't access your real account, but it can still damage your reputation and be used to scam others in your name. They might send messages to real friends about fake investment opportunities or try to start romance scams.

How do social media accounts get compromised?

Cybercriminals use a variety of tactics to gain access to accounts or impersonate users.

- **Phishing attacks :** A scammer sends an email, text, or direct message claiming there's a problem with your account. The phishing message might include a link to a fake login page designed to steal your username and password. If you get an email about this situation, contact the platform directly through the Contact Us page—social media platforms won't contact you through text, phone calls, or DMs. Don't click any any links in the message.
- **Password reuse:** If you use the same password across multiple websites, a data breach at one company could give criminals the credentials they need to access your social media accounts. Only use a password once.
- **Malware:** Malicious software installed on your device can capture passwords, cookies, or other sensitive information. Malware is often sent through phishing messages.
- **Public profile information:** For profile cloning scams, criminals simply collect information you've already shared publicly to build a convincing fake account.

How to protect your social media accounts

Fortunately, protecting your accounts doesn't require advanced technical skills.

- **Use long, unique passwords:** Every social media account should have its own unique password. A password manager can generate and securely store strong passwords, making it easier to avoid reusing credentials. Aim for passwords that are at least 16 characters long and a random string of characters.
- **Turn on multifactor authentication (MFA):** Multifactor authentication adds another layer of security beyond your password. Even if someone steals your login credentials, they'll still need your second authentication factor. Whenever possible, use an authenticator app instead of text message verification. Never share an MFA code with anyone!
- **Keep your devices and software updated:** Software updates often include security patches that fix vulnerabilities attackers actively exploit. We recommend enabling automatic updates for your phone, computer, web browser, apps, and software.
- **Watch out for phishing messages;** Be skeptical of any unexpected inbound messages claiming your account has been suspended, verified, or compromised. Instead of clicking links in emails or direct messages, open the social media platform yourself by typing the website or using the official app.
- **Review privacy settings:** Limiting what strangers can see makes it harder for criminals to build convincing fake profiles. Make some information items visible only to friends, like friends list, photos, workplace, and location. Some info you don't need to post onto social media at all, like your contact info and birthday. Think twice before sharing information that could answer security questions or help someone impersonate you. In general, think about what criminals could do with information you post publicly – for example, posting to a wide audience about your vacation while you are on vacation could let people know you aren't at home.
- **Be cautious with friend requests:** Receiving a friend request from someone you're already connected to can be a warning sign. Before accepting duplicate requests, contact the person through another method to confirm they created a new account.

How to spot a cloned social media profile

Fake accounts often look convincing, but there are usually warning signs. Look for profiles that:

- Have very few posts or recent activity
- Recently joined the platform
- Send unexpected friend requests
- Ask for money, gift cards, or personal information
- Share suspicious links
- Have copied your photos or another person's profile information

If something feels off, you don't need to friend them!

What to do if your account is hacked or cloned

If you think someone has taken over your account:

- Change your password immediately if you still have access.
- Enable MFA if it isn't already turned on.
- Review recent login activity and remove unfamiliar devices.
- Notify your friends that your account may have been compromised.
- Report the incident using the platform's account recovery tools.

If someone creates a fake account impersonating you:

- Search for the fake profile (or ask friends to look if you can't find it).
- Report it as impersonation through the social media platform.
- Ask friends and family to report the account as well.
- Warn your contacts not to accept friend requests or respond to messages from the fake profile.
- Review your privacy settings to reduce the amount of publicly visible information.

Stay a step ahead of social media scammers

Social media platforms make it easy to connect with others, but they also give criminals opportunities to exploit trust. A few minutes spent securing your accounts today can save you from major headaches recovering from an account takeover tomorrow.

FAQs about social media account takeovers

How do hackers take over social media accounts?

Most account takeovers happen through phishing scams, stolen passwords, password reuse after a data breach, malware, or social engineering attacks that trick users into revealing login credentials.

What's the difference between an account takeover and profile cloning?

An account takeover means a criminal gains access to your real account. Profile cloning happens when someone creates a fake account using your publicly available information to impersonate you without accessing your actual account.

How can I protect my social media accounts?

Use a unique password for every account, enable multi-factor authentication, keep your software updated, avoid phishing scams, and limit the personal information visible on your public profile.

What should I do if someone creates a fake social media profile pretending to be me?

Report the impersonation to the social media platform, ask your friends to report it as well, warn your contacts not to interact with the fake account, and review your privacy settings to limit the information available to scammers.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®
STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.