# 7 ways hackers steal your identity on social networks

Social networking is a great way to connect with strangers, but it also makes it easier for others to collect your personal information.

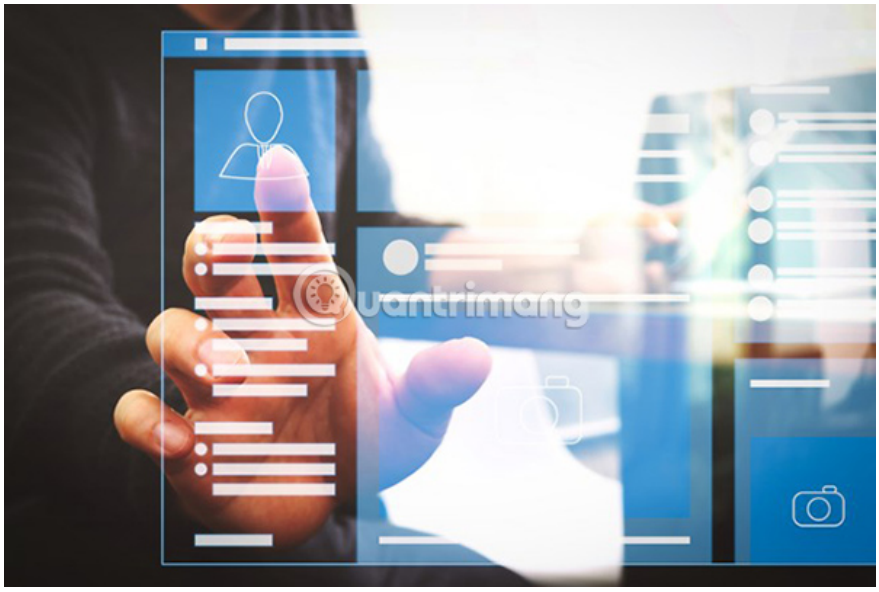
Social networking is a great way to connect with strangers, but it also makes it easier for others to collect your personal information. Fortunately, there are ways you can protect your online presence and prevent crooks from stealing your identity.

Here are some of the ways scammers use and how to counter their tricks.

## How do hackers steal your identity on social media?



## 1. Collect information from the profile



Sometimes, a hacker doesn't need to spend too much effort to steal someone's identity. Some people are quite generous about the amount of information they share on social media. Information they disclose includes their date of birth, address and phone number. If someone shares too much data, scammers can collect this information and use them to impersonate them.

1. Things you should not share on social networks

### How to prevent data collection from happening?

Although this sounds scary, it's also the most easily avoided. Take care of what you share online, even if you've set your privacy, only let your friends see them. Follow the golden rule: If you don't want to share something with a stranger, don't share it on social media accounts.

## 2. Stealing information through malicious applications and services

Some social networking sites allow you to install third party applications. Some websites offer specific services and require you to log in via a social networking site. Typically, these services are designed to provide features that social networks do not have. But these services can also create insecure spots.

If you're unlucky, you'll use an application or service that doesn't do its job properly; instead, it uses the permissions provided to collect information about you and send it back to the developer. malware.

### How to prevent identity theft through applications and services

Be careful about installing third-party applications or services. Be extra careful with apps that provide the ability to unlock a hidden feature, as these are likely trying to trick you into downloading malware.

When you use third-party services, make sure you read about the permissions that the application wants. If a simple tool asks for all possible permissions, be careful with it.

# 3. Install malware and trick users with phishing

Phishing attacks rely on tricking people into clicking on a link. This method works best when spread among a large group of adults. Unfortunately, social networking is a 'crowded' service that allows crooks to launch phishing attacks. By causing people to share the link (such as through the re-sharing of tweets), the phishing attack kept spreading.

These attacks are much worse when posted by a fake account. For example, the BBC reported on how a fake Elon Musk account spread a phishing attack to steal everyone's Bitcoin.

Phishing attacks are an effective tactic for identity theft. Malicious links can lead to malware, which is downloaded and activated to collect data. Some phishing links may be forged from a legitimate company or organization, and then ask for sensitive information from the user.

### How to avoid phishing?

If you see any suspicious links, never click on them. Phishing links often have an appeal that makes them hard to resist. They may disguise themselves as a news website that posts the death of a celebrity, or claim to have some bullshit rumors about one of your friends.

You can also take a phishing identification test (see link: *https://phishingquiz.withgoogle.com/).* When you learn how to identify a phishing attack, you're well equipped to protect yourself.

# 4. Attack users through their friends

Be very careful with people you know online, even if they are your real-life friends. Scammers realize that people don't click on phishing links as much as before, especially if the links are coming from accounts they've never heard before.

Some scammers take a sneaky approach and damage someone's social media accounts. Then, they send a friend's friend's account a phishing link, most likely the victim will click on it because it is from a friend. This link installs malware on a victim's computer, gathers information from them, and sends it to all his other friends.

### How to detect a 'fake' friend?

If you find that your friends are suddenly acting oddly, be sure not to click on anything they send you. For example, you might have a good friend who suddenly threatens by revealing the video and posting a link. This sign is a sure thing to determine if your friend's account is compromised, so be sure to contact them outside of your social networking site and let them know the situation.

Of course, you may receive a call informing you that a hacker has access to your account. If this happens, don't worry! You can get your account back. For example, you can contact Facebook to retrieve a hacked account.

# 5. Retrieve data from location tagging in images

If you have a picnic outside, it's fun to tag photos with your current location so people can see the museums, cafes and concerts you visit.

However, if you abuse this, you may end up giving away too much information, through location tracking. For example, if you upload a photo taken at home with location tracking, it may reveal information about where you live.

### How to take photos safely

You can still use location tagging when taking photos, but be careful about where and what you tag. If you're in a public place, there's no harm in letting people know where you are. When you're in a more private place, be sure to double check to make sure you don't upload photos that reveal your address.

If you have photos with location data in them, you can still upload them safely. For example, you can separate location data from photos.

## 6. Collect data through deleted information

The biggest problem with online information is that sometimes they cannot be deleted.

For example, if you had a Facebook account before but deleted it for a long time, there were sites like Wayback Machine that could remember your profile page. As a result, hackers can use these sites to find out information you once had online.

### How to resolve information that cannot be deleted?

If you've been a little generous with the information you've shared before, double-check sites like Wayback Machine to see if there's anything cached. If this is the case, it is best to contact the site to ask them to remove your page from the system.

Besides, make sure you delete all data on the websites you decide to leave, instead of just disabling the account. For example, there's a big difference between deactivating and deleting Facebook accounts for privacy.

## 7. Find out about you through friend requests


Sometimes a crook doesn't need to hide in the dark. They can add you as a normal friend and gather information that way. They may ask you questions about yourself and certain artificial interests, or make friends with you to try to violate privacy settings and learn more about you.

### How to avoid 'fake' friends?

In order for someone to be your friend on social media, you need to accept their request. As such, even if you are a friendly person, be cautious when receiving friend requests.

If the privacy settings disclose all your data to a friend, be careful of who you allow access to your profile. Making friends with a stranger can compromise your privacy.

## Keep your identity safe on social networks

Social networking is a great place to get to know people, but it is also a way for hackers to turn you into a 'prey'. By being wary of your data and learning about how hackers can access that data, you can avoid identity theft through social networks.

You finished reading the article "**7 ways hackers steal your identity on social networks**" 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.