

SOCIAL MEDIA:

What Hackers Can Learn About you in Less than 30 Minutes



Have you ever stopped to think how much information about yourself can be found on your social media profiles? [Take a quick test:](#)

Find a random person on social media.

Take 30 minutes to read through their posts and included information in their profile. Odds are, you now know a lot about this person whom you've never met. Could someone find the same information about you if they searched your profile?

From where you currently live and work to where you went on vacation last year and what you ate for dinner last night, we share a large

amount of information about ourselves on social media. As the digital age progresses, there are now over 2 billion active social media accounts with countless photos and status updates on nearly everything we do. With this rise of shared information, we also see a rise in identity theft.

One-in-four Americans experienced an information security breach within the past year.¹

The amount of knowledge available online about an individual person likely surpasses what your closest friends and family even know about you. **In particular, the rise of social media has allowed hackers to easily gain personal information about individuals...without even hacking a profile.**

The Evolution of Social Media and the Internet

In 1997, the first recognizable social media site, Six Degrees, was created. From there, the first blogging site became popular in 1999. We then see sites including MySpace, LinkedIn, and YouTube start becoming popular in the 2000's. Today, Google has over 900 million users worldwide. Facebook has nearly 1.5 million active users per month. Most of us have had some type of connection to these companies. Imagine how much information they know about you!

Protecting your Data While Always Connected

A recent IBM study estimates over one billion records were leaked in 2014, up 25% from the previous year.² That's one billion leaked emails, credit card numbers, passwords, and other personal information hackers can use for identify theft. Taking this a step further, **hackers can combine this information with what they find on social media profiles to gather additional data about you such as your address, employer, habits, and more.** While users can't prevent a data breach from happening within a company, they can take extra precautions online to help secure their data and what's available.

Social media provides a way to stay connected to friends and family across the world. However, **keep in mind how much information you put out there and who you share it with.** Most hackers can find basic information about you by scanning your accounts, including:

- | | | | |
|---|--------------------------------|---|---|
| ! | Full name (and nicknames) | ! | Email address |
| ! | Address or current town | ! | Past places lived and worked |
| ! | Age | ! | Who you know |
| ! | Current employer and job title | ! | Your hobbies and interests |
| ! | Phone number | ! | Where you are and when
(by analyzing status updates) |

Hackers can cleverly use this information to their advantage. If a hacker has your credit card number and they know you commonly shop at certain stores, they can charge your credit card with purchases from there knowing you may not catch it. This information is only a start. If a hacker happens to gain access to your social security number, they can use this information to apply for credit cards or even a mortgage using your name.



No one is safe from an attack. Determined hackers will find a way to steal your data if they really want to. However, you don't need to make it easy for them. **Here are some ways to protect your personal information and keep your online presence secure when using social media:**

- ✓ **Learn how websites use your information.** Many social media websites sell your data to third party companies. The less information they have, the less likely you'll become a victim of identify theft in the event of a data breach.
- ✓ **Use privacy settings.** You can use privacy settings within your profiles to choose who can search for you profile and who can see what information. Only accept requests from people you know and trust.
- ✓ **Choose what data to share.** Is it necessary to post your address and phone number on your profile? Do you need to tell everyone about everything you do? Most won't think anything about sharing pet photos, but one in six people will use a pet name in a password. Looking at your status updates and interests will help hackers guess your passwords and security questions.
- ✓ **Be mindful of others.** Posting information about your friends and family puts them at risk as well. Be mindful of the information you put out there, especially about children, and respect their requests to not be included within your post.
- ✓ **Don't link your accounts.** Yes, linking your accounts makes things very convenient. However, if a hacker breaks into one account they can break into all accounts to steal sensitive data.
- ✓ **Search yourself online.** If someone has hacked into any of your accounts or is using your information online, your name or other private information will most likely come up within a search engine on sites and places you don't expect. You can also use this opportunity to see how your social media profiles are seen in search results and what others outside your network can see.

Social media users can continue to have fun and share online by following just a few simple steps to secure their profiles and understand what available information is out there. Remember, everyone is at risk for an attack and, even though you may follow through to protect your accounts, it's still possible for hackers to wreak havoc with your online reputation, credit history, bank accounts, and more.

1. <http://www.aicpa.org/Press/PressReleases/2015/Pages/AICPASurveyOneinfourAmericansVictimizedby-InformationSecurityBreaches.aspx>
2. <http://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03073usen/WGL03073USEN.PDF>