They knew everything about me–How modern identity thieves profile victims

pcworld,com, March 2025, Incogni article

The key to avoiding identity theft is understanding how it works. Learn what makes you a target–in order to not become one.

Identity theft is one of those boogeymen of the internet age. It's the stuff of hacker movies from the '90s: one day your keycard, bankcard and phone just stop working, then it turns out someone has taken over your life and is living large on your dime. Far-fetched, sure, but not completely divorced from reality.

How do you end up in an identity thief's sights? Most don't just select victims at random. Stealing someone's identity and actually getting away with selling or using it takes a lot of planning, work, and time-consuming operational-security measures. With this kind of risk and time investment in play, it makes sense that identity thieves would want to choose potential victims carefully.

Like law enforcement looking for a suspect, they use various profiling techniques to do this. But first:

What exactly is identity theft?

Identity theft is basically what it sounds like: someone stealing your personally identifiable information (PII) in order to use parts of your identity for their own ends. It doesn't have to mean that you've been replaced by an imposter in your daily life, in fact it rarely if ever does.

Somebody who uses your credit card details without permission, gains access to your email and uses it to message people or sign up for things, or logs into your crypto-exchange account is committing identity fraud, among other crimes. You probably wouldn't know anything was up until the consequences of the identity thief's actions caught up with *you*.

Avoid becoming a target of identity thieves by understanding how they choose potential victims.

Anatomy of identity theft

There are many—too many—different types of identity theft cases out there. They all hit three common notes, though. To commit identity theft, the perpetrator has to:

- Choose a potential victim
- Gather information about their target
- Adopt their target's identity, or parts thereof
- Exploit their target's identity, usually for financial gain.

The details will vary, and many schemes will include additional steps, sometimes becoming incredibly intricate and complex in the process, but this is the basic outline. The first stages are the profiling stages, and it's there that you can best avoid being caught in identity thieves' nets.

Profiling: Target selection

The first stage of any identity theft and the first of three profiling stages. There are many ways you can end up on an identity thieve's radar. They fall into three categories: representing a big score, appearing like an easy target, and—worst of all—a combination of the two.

What marks you as a lucrative target

Anything that suggests you have a lot of money or, more specifically, liquid assets and cash on hand can paint a target on your back. One of the worst things you can do is to advertise the fact that you have a lot of money tied up in a cryptocurrency like Bitcoin. Few things attract identity thieves more than finding out that all that stands between them and a small (or large) fortune is a single seed phrase.

You need not be wealthy to attract the wrong kind of attention. Just sold a home or vehicle? Data brokers are on it, and identity thieves know to look for recent sales like these, knowing that the seller probably has a lump sum sitting around.

Anything that suggests you've got money, assets or simply a good credit score is enough to attract identity thieves and other scammers. Don't leave the boxes from your new, ultra high-end home-theater system out on the curb, don't brag about your crypto prowess online, and don't let data brokers spread the news of your recent retirement or inheritance far and wide.

What marks you as an easy target

The other major way you can end up being profiled by identity thieves is to appear like you're an easy target. Because even if you only have a couple of hundred dollars on hand, if it looks like it'll be quick, easy and safe to take that money from you, someone will come up to the plate and take a swing.

There are two ways you can pop up as an easy mark on scammers' radars: by having a ton of personal information available online and by having fallen for scams in the past. If you've engaged with scammers in text messages or over the phone—whether they managed to swindle you or not, but especially if they did—then you're effectively if not literally on a list.

This isn't to say you're at fault or gullible or anything like that, but engaging with scammers will generally lead to more scam attempts, including attempts to steal your identity. The one thing you can do here is be more vigilant going forward, hanging up on scam calls and ignoring scam messages (easier said than done).

Profiling: OSINT

The next thing most identity thieves will do is look around online (and sometimes offline) for any personal information they can find just sitting there, out in the open. This is called "open-source intelligence" or OSINT for short.

They need this information for the next stages in their schemes. Just by using a regular web browser, they can find many of your online accounts, your photos, possibly your place of work, information about your educational and work history, and much more besides. They can use this information to get into your accounts, find people close to you, and generally "get to know you."

Something that's made this stage faster and easier than ever before, especially in the US, is the rise of data brokers, including so-called people search sites (also known as people finder sites). Using these services, an identity thief can get a detailed, ready-made profile on you with just a few clicks, and for as little as a dollar.

To protect yourself against this profiling stage, be careful about what information you post online, including on social media. Consider using a personal information removal service like Incogni to disrupt data brokers' attempts to aggregate and disseminate your personal information through their networks.

Incogni: Remove your profiling data with ease

If you're worried about who has access to your personal information, data removal services like Incogni do the tedious work of contacting data brokers on your behalf and removing your personal info from their databases—saving you countless hours of research, emails, and paperwork.

Incogni limits your personal exposure on the web, monitors places where your personal information is held, and ensures that data brokers regularly keep that information off of their platforms. The benefits of using a data removal service include receiving fewer spam and marketing robocalls, lowering the risks of identity theft, and cleaning up your exposure after a data breach.

Profiling: Data gathering

Once an identity thief has a handle on all the personal information they can find in publicly available sources (including data brokers that operate out in the open), they can start to drill down into other sources to fill in any blanks.

This can take many forms, from downloading or buying hacked account credentials (usernames, emails and passwords) to conducting phishing campaigns against you and those close to you. The identity thief, at this stage, is looking for the missing details they need to SIM-swap your phone or gain access to your online accounts, especially your email accounts.

Hackers and identity thieves will generally zero-in on your email accounts and SIM card because they can use them to reset passwords to other accounts, like crypto-exchange and financial accounts, for example.

There's not much you can do about the member-only forums (including darknet forums) that identity thieves use to get your credentials, but you can limit how useful those credentials are to them. Make sure each of your accounts is secured by a strong, *unique* password—one that you don't use anywhere else.

Account takeover

The profiling stages are over once the identity thief or thieves have all they need to start taking over your accounts. They're not interested in taking over all your accounts, they probably only need one or two of them and the email accounts that they can use to reset the passwords.

The most common method, and the one a bad actor will probably try first, is called "credential stuffing." This involves using those hacked passwords from the data-gathering stage and trying them on your other accounts. If you re-use passwords between accounts, they're in.

Think two-factor authentication SMSs will stop that from happening? They won't if the identity thief knows enough about you to call your mobile carrier pretending to be you and request that they transfer your number to the thief's SIM card (this is what "SIM-swapping" is).

At this point, your identity has been stolen. Now comes the worst part—exploitation.

Exploitation

This is the goal of identity theft: exploiting your personal information to commit further crimes. These crimes could be emptying out your crypto wallets, draining your bank accounts, or something a little more subtle.

Identity thieves can use your information to take out loans or claim government benefits in your name, to redirect and steal your tax returns or even to seek otherwise legitimate employment (using your SSN, for example). They often also use stolen identities when committing unrelated crimes, leaving you on the hook with law enforcement.

All you can do at this late stage is react and do damage control. The FTC has an identity theft portal that can guide you through the process of creating a recovery plan. Prevention isn't only better than cure, it's also cheaper, easier and less stressful.

Use a personal information removal service to stop identity thieves at the earliest possible stages of their schemes: before they can even notice you, let alone digging deeper and building a file on you.