How Online Identity Thieves Are Getting Smarter

A recent study concluded that 15.4 million Americans were victims of identity theft in 2016.

Your credit card may now have a security chip inside it, but you're as much at risk for identity theft as you ever were. Javelin Strategy & Research recently came out with its 2017 Identity Fraud Study and concluded that 6.15 percent of consumers, or 15.4 million Americans, were victims of identity theft in 2016. That's two million more people than the previous year.

But that doesn't mean the security chip in your credit card isn't protecting you from criminals. It is. The bad guys are simply finding new ways to cause havoc. In 2016, according to Javelin Strategy & Research, there was a *40 percent increase* of stealing credit card information without actually stealing the credit card.

"Identity thieves are bolder now than ever," says Anthony Howard, an information technology consultant in Atlanta.

Some of the audaciousness is due to the demand for stolen identities, Howard says. But there's another reason why identity theft is such a hot crime.

"Thieves have figured out that because identity theft happens so often, most [victims] don't bother to fill out a police report, which means rarely, if ever, do law authorities actually take action or even look for the perpetrators on a scam unless it's of some magnitude," Howard says.

You've known forever not to fall for those emails that promise your share of an inheritance if only you'll send over your banking information. You know that sharing too much personal information on social media is a no-no. And you've had it drilled into your head to not use

"password" as your online passwords. But here are some of the dicey areas of the internet you may not be aware of.

Online shopping wish lists. So you visit a favorite online store and make a shopping list of all the gifts that you want. That can be risky, says Matias Woloski, the CTO and co-founder of Auth0, a company based out of Buenos Aires, Argentina, that helps businesses secure and manage online user identities.

"Scammers use the information in these lists, which are often public, to learn more about their victims. This helps them craft more believable phishing emails," Woloski says.

Phishing is the practice of sending fake emails from credible looking sources. Woloski says you could get an email that looks like it's from your favorite online store, with the email telling you that a friend has purchased an item for you. Click here to verify your contact details.

You click, and you may have just verified some key information to a crook.

Websites having to do with online gaming. Even if you aren't a gamer, maybe you have kids who love online computer games. Gamers are vulnerable when it comes to online thieves, says Gunter Ollmann, who is based in Atlanta and is the chief security officer of Vectra Networks, a company headquartered in San Jose, California that helps consumers monitor hidden cyber attacks in their networks.

Much of our society wants to be satisfied *now*, and so maybe it isn't surprising that many players look for ways to "cheat" the game they're playing, so they can get to the next level more quickly. Ollmann says that many hackers will create "cheat sites," in which the gamer is instructed how to use the "cheat" to beat the game.

But, first, the gamer has to supply information like a cellphone number, or he or she might be required to download a "toolbar." Of course, the toolbar allows the hacker to get access to the gamer's computer.

"This works very well against teen mobile game players with little money," Ollmann says.

And money or not, he or she still has an identity that's worth plenty to the identity thief.

And this can happen even with anti-virus protection specifically designed to stave off these kinds of cons. Ollmann says sometimes teenagers ignore warning alerts.

"If they've spent 10 minutes answering questionnaires, see the progress bar at 95 percent and are told this last step is the final stage … they're socially engineered into installation," Ollmann says.

Spam emails asking if you want to unsubscribe. So you get some advertiser's unwanted email, and there's a link where you can unsubscribe. Grateful, you click on the link.

The problem, Ollmann says, is that sometimes, "the bad guys send spam from popular websites. … Once the details are entered, the victim gets a message that they are now unsubscribed – but the bad guys have harvested the ID information they were after."

How can you tell if the unsubscribe email is legitimate? It can be challenging to discern, Ollmann says. He suggests inspecting the URL. "Is the domain name consistent with the company it is presenting itself as? If not, then don't click on it," Ollmann says.

In other words, if in doubt, delete. Given how much spam your email box probably gets, that's probably the best approach, anyway.

Free stuff. This one is tricky because plenty of businesses send emails with coupons and offers. But look at them warily, says Robert Siciliano, a Boston-based identity theft consultant and the CEO of IDTheftSecurity.com.
"You might get an email offering a free screen saver or coupon, but when you open it, the software encrypts your drive and takes over your computer," Siciliano says.

Scary stuff. Siciliano says that you also might get a phone call from someone saying they are from Microsoft. The "representative" tells you they have scanned your computer and have found files that are malicious.
If you believe the person on the phone, you might believe them when they tell you they can remotely access your computer and fix the problem, after you install a program.
"When you install it, you give them access to everything, including personal and financial information, and they can do what they want with it," Siciliano says.

Protect yourself offline, too. By doing this, you'll protect yourself online.
"Some criminals are going back to physical theft to help fuel online identity theft," Woloski says. "They will break into homes and steal passports, birth certificates, bank statements – anything that can help them open new accounts in your name or gain access to existing accounts."
So just as you would be careful not to leave too much personal information on a social media website, don't leave your social security card lying somewhere within easy reach in your home.
"Keep really important documents in a safety deposit box, or a large safe that's hard to steal," Woloski says.

In other words, while being paranoid about keeping your identity safe online, don't forget to keep it safe everywhere else.

http://money.usnews.com/money/personal-finance/banking-credit/articles/2017-04-07/how-online-identity-thieves-are-getting-smarter