Anti-Scam

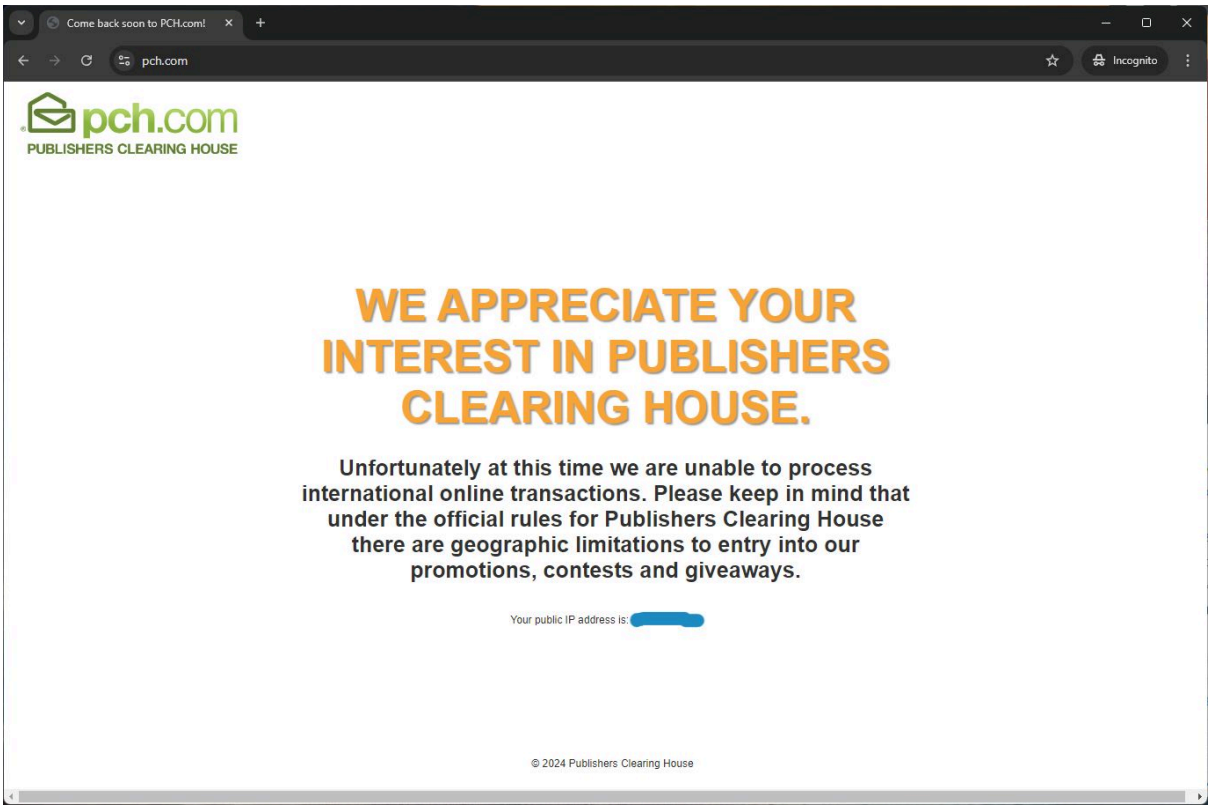
Publishers Clearing House and Sweepstakes Scams

I Won 9.8 Million Dollars from PCH?

I don't live in the US, but I do have a US-based phone number for business. The number gets a never-ending stream of spam SMS (text messages) from area codes far and wide warning me about cash due on packages I never ordered, inviting me to "spicy parties," and alerting me that members of my HOTLIST (whatever that is) are active now. Occasionally I'll get a call from a number I don't recognize and I just let it go to voice mail. Recently, I learned just how lucky I am when I got this message:

> *"Hello. My name is "David Green" and I'm calling from the Publishers Clearing House in regards to you being the second place lucky winner. Of 9.8 million dollars. Please give me a call back at 810-204-8927. Thank you."*

Wow! How could I be so lucky! I won the Publishers Clearing House sweepstakes without even entering! And without even living in the US! Wait a minute. Something's fishy here...



Breaching the geofence, I made my way to PCH's Fraud Protection page, which insists:

> *Publishers Clearing House (PCH) does NOT make or authorize outgoing calls to consumers to sell merchandise or magazines, or to solicit sweepstakes entries. Our major winners are notified by mail or in person (at our option) and we never phone ahead to disclose that someone has won a major prize. If you receive a phone call from someone claiming to be from Publishers Clearing House and are asked to send money, pay a fee or pre-pay taxes to enter, collect or claim a sweepstakes prize — STOP — you have not heard from the "real" Publishers Clearing House. The call you received was most likely from a fraudulent sweepstakes scam operation.*

Nuts. I guess my luck has run out.

My recent articles have focused on ways to secure network servers against cybervillains but this time, let's take a look at a more pervasive form of predatory behavior.

Do People Really Fall for This?

Yes, they do. This scam has been around in some form for many years. It's a numbers game. To make it work, the villains blast out phone calls and emails to thousands and thousands of potential victims at a time. Some potential victims are desperate. Some have entered the real PCH sweepstakes. Many are elderly. And if even a fraction of a percent respond, the juice is worth the squeeze for the evildoers.

The elderly are particularly vulnerable. A recent post (January 2024) in Reddit's "Scams" subreddit shared a common story:

> *Long story short, my dad fell for the publishers clearing house scam. Promised him all this money and he just had to pay the taxes. Etc. He called me today and confessed to it all. He took out a 100k refinance on his house. All his credit cards got stolen and maxed out. He depleted his savings.*
>
> *My dad is almost 70, lost his wife a few years ago and is lonely. He called me crying saying all he wanted to do was pay off my loans and my house and make life better for me. I feel horrible for him.*

It's not an isolated incident. Another post, this one from Reddit's "AgingParents" subreddit in July 2024, described a similar experience:

> *"One of our aging family members is a bright man and has fallen victim to the PCH scam. It started out with him getting a call from 'PCH' scammer letting him know he won the big prize. All he has to do is pay the taxes on it first then they'll release the funds. When he came to our house to tell us his great news we went into a panic.*

And the consequences can be dire, such as this story posted to Reddit in October, 2024:

> *My husband was told that he had won $8.5 million and was asked to send gift card numbers to the scammers for "taxes and fees" He cleaned out our savings account to the tune of $13k and overdrew his own checking account by another $4k. He also deposited 2 checks that they had sent him totalling $16,000 both of which bounced. One was a fraudulent check and one an identity theft. He now is facing legal repercussions because of cashing the two checks. Meanwhile he had*

> *converted the them into cash that he used to purchase money paks for the scammers so he's on the hook for that money now and overdrawn by $20k.*

According to the U.S. Federal Trade Commission's *Consumer Sentinel Network Data Book* for 2023, sweepstakes fraud was the third most-reported type of fraud in 2023 with over 150,000 reports and over $300 million lost by victims in the U.S.

How Does the Scam Work?

Like all confidence games, the "Publishers Clearing House Scam" (PCH *hates* it when the media calls it that) relies on deception to persuade victims to willingly give up their money. The villains convince their targets that if they just pay a (relatively) small amount today, they'll get a huge windfall later. And they can be very convincing!

Sometimes sweepstakes scammers will impersonate government officials from the U.S. Treasury Department, the Internal Revenue Service, or even the Federal Trade Commission. The scammers explain that a government officer will call soon to arrange payment of taxes and fees. The criminals then call back from a different fake number and impersonate the official, hoping that it makes the scam seem more legitimate. To many victims, it does. After all, now the sweepstakes company isn't asking for money; the U.S. government is! A recent episode of the American Association for Retired People's *The Perfect Scam* podcast featured just such a story -- A woman from the U.S. state of Michigan was persuaded to give up her entire life savings when a supposed FTC agent convinced her that the prize, taxes, and fees were all real.

Scammers often want their victims to use nontraditional, and often untraceable, payment methods to send money. In recent years, they may insist that victims buy gift cards that can be resold by the villains or to send cryptocurrency, which is usually untraceable and unrecoverable. In some cases, victims have been convinced to open new bank accounts and give the scammers control over the accounts. If a more traditional payment method is used, the villains will usually insist on cash and insist that it be sent through a money mule (who is often another unwitting victim in the scam).

There are two main forms of the scam: *advance payment* and *fake check*.

Advance Payment Scams

The hallmark of an *advance payment scam* is that victims are told that they have to pay some amount before they can claim their winnings. The justifications the

scammers use always sound logical. There are taxes to pre-pay. There are processing fees. There are bank transfer fees. There are legal fees. There are insurance fees. Maybe there are "slush money" fees to avoid more fees. Often, the initial amount is small and low-friction. Even a suspicious victim might be willing to pay a couple hundred dollars just in case the prize is legitimate. But then, the criminals ask for more, with each new amount larger than the last. And each time, they promise, "this is the last one." But it's never the last one.

A 2021 comment from Reddit's "Scams" subreddit sums it up:

> *"This happened to my 85yo father beginning in March 2021. The man called back a few days later to tell my dad he was a finalist. My dad fell for it, hook, line and sinker. Over several weeks my dad sent money 8 to 10 times. There was always a fee or a tax or something that my dad needed to pay for and then the prize patrol would show up with the big check. My dad paid thousands of dollars (US).*

Sometimes, when the scammers sense resistance from their victims, they move the goalposts in very creative ways. According to a recently-unsealed federal criminal complaint against a Costa Rican scammer who was arrested while traveling to the U.S., one victim was given incredible news: the prize will be substantially increased because the first place winner defaulted! Of course, this means that there are now more taxes and fees to pay. Sadly, the victim, identified only as "Victim-1" in the complaint, lost over $265,000 to the scammers.

Advance payment scams, of course, are not new. The villains have just moved on from Nigerian princes, dead uncles you've never heard of, overseas gold bars, and black money to more believable cons.

Fake Check Scams

Sometimes, the villains will offer to send a large cashier's check as the "first installment" from which the victims can begin paying the taxes and fees. The check is, of course, fake. This is how *fake check scams* work. In the U.S., checks can take days or even weeks to clear and can still bounce *even after the funds have been made available to a customer*. Scammers know exactly how to take advantage of this flaw in the U.S. banking system and use it to make their advance payment scams seem less risky and more genuine.

The victim unwittingly deposits the fraudulent check and once the funds seem to be available, they send money to the scammers. Not long afterwards, though, the bank discovers that the check was fake or stolen and they reverse the deposit, removing all of the deposited money from the victim's bank account. Now, the victim is out the

money they sent to the scammers *and*, if their account is overdrawn, they need to make good with the bank.

Even worse, banks take a dim view of customers who deposit fraudulent checks and they will often close all of the victim's accounts. Even if the bank sympathizes with the victim, they now realize that this is a high-risk customer who they do not want to continue doing business with.

The scammers, of course, always have a convincing excuse as to why the check was reversed and always come up with new ways to keep the victim's trust.

Recovery Scams

Eventually, victims stop sending money to the scammers, either because they realize that they have been victimized (often only after the intervention of loved ones) or, in the saddest cases, because they run out of money and loan options. But the scammers aren't done yet.

Increasingly, scammers have learned that they can go to the same well twice. This time, the villains impersonate "recovery specialists." They pretend to sympathize with the victim and insist that, through their expertise and connections in the banking industry, they (or someone they know) can recover some or all of the money that was lost. Of course, there is a fee for this service, and it must be paid in advance. Once the victim pays the recovery fee, the scammers vanish with the money.

The villains may contact the victim on social media with a convincing testimonial, something like this:

> *I lost $187,000. I tried to withdraw some of my money, but it was useless. After filing complaints with no response, I reached out to a recovery firm that has helped some victims in similar situations to get their money back. I will be willing to share my experience with another victim. Thanks to { reference to the scammer } on Instagram for recovering my lost funds. { link to the scammer's info }*

These *recovery scams* prey on people who have already been victimized and are looking desperately for a way to undo the damage. Often, recovery scammers are unrelated to the original scam, but learned about the opportunity through social media or internet posts. They are *never* legitimate. In the rare case where any money can be recovered, only law enforcement can facilitate the recovery, not random individuals on social media.

Protect Yourself and Others

Fraudulent activity like the Publishers Clearing House scam (sorry, PCH) continue to thrive because they work. And they continue to work because not enough people know about them. The only effective way to defend against these crimes is to become educated yourself (as you are now after reading this article) and to help educate others.

A 2018 bulletin from the U.S. Federal Trade Commission offers the following advice, specifically about sweepstakes scams:

> *If you think you've won a prize, here are a few things to know:*
>
> - *Never send money to collect a prize, sweepstakes check, or lottery winnings. If you have to pay, it's a scam.*
> - *Never deposit a check and send back money, even if the funds appear in your account. That's a sure sign of a scam.*
> - *If anyone calls asking you to pay for a prize, hang up and report it to the FTC at ReportFraud.ftc.gov.*

You can help your loved ones, particularly the elderly, by sharing information like this with them. Educate them about this and other scams and advise them to seek advice from others before ever sending money, especially to someone they don't know.
If you enjoy podcasts and want to stay up-to-date about the latest scams targeting the elderly, I recommend *The Perfect Scam*, a weekly podcast produced by the U.S.-based American Association for Retired People. The AARP also hosts The Fraud Watch Network, which has a scam victim support hotline available Monday-Friday 8:00 - 20:00 Eastern Time for people in the U.S. at 1-877-908-3360.

So, despite "David Green's" assurances, I have not, in fact, won $9.8 million. Not this time anyway.