

How AI Is Fueling A New Wave Of Air Conditioner Scams

By [Steve Weisman](#),
Contributor.

Steve Weisman writes about white-collar crime.

Jul 05, 2026, 12:40pm EDT

The summer of 2026 is already shaping up to be one of the hottest on record with a major heat wave affecting much of the country and the National Weather Service's Climate Prediction Center [warning](#) of an elevated risk of extreme heat throughout much of the country for the rest of July. In Europe things are even worse with more than 1,300 deaths being attributed to the extreme heat before we have even gotten into the hottest days of July and August.

In the face of this extreme threat, people are turning to air conditioners for their homes to fight the heat. Scam artists, the only criminals we refer to as artists are only too willing to meet this increased demand for air conditioners with offers of non-existent air conditioners at discount prices, which is not surprising because scammers are always taking advantage of whatever has the interest of the public and turning that interest into a scam. And unfortunately, AI has made their job easier.

Scammers use AI to construct phony websites which often appear to be those of legitimate retailers as well as ads on social media to lure people into buying a much-needed air conditioner that never is delivered.

Phony Websites

Scammers create phony retail websites that either appear to be that of legitimate retailers such as Walmart or are just websites that come up high in a search engine search when you are looking to buy a particular item. Unfortunately, this problem has gotten worse with scammers now able to use AI to create phony retail websites that look entirely legitimate. Also, merely because a website comes up high in a search engine search does not mean that it is legitimate. Scammers either pay for an ad that brings a high position in a search or are sufficiently savvy to create a site that the search engine's algorithms will pick for a high position in a search.

In the past, scammers would lure you into providing your credit card or debit card (which you should never use for purchases because the law does not protect you as much from fraudulent use) and then use your card to make purchases or if you provided your debit card, they would then access your bank account. Now, however, the scammers are getting greedy. Often when you attempt to use your credit card on their phony website you will be told that your card has been declined and so you need to use a second card. Once you do, you have now turned over two credit cards to the scammer to use for fraudulent purchases in your name.

How do you determine if you are on a legitimate website?

Look at the URL. If you are making a payment, you want the URL to be preceded by https rather than merely http. The "s" means that your communication is being encrypted and while even some phony websites may go the extra step and use encryption, most do not and so this is an easy way to spot a scam.

Sometimes carefully checking the domain name for a counterfeit website will provide an indication that it is a scam. If the domain name has nothing to do with the real name of the company, you can be confident that is a scam. I would caution you however that merely because the name looks legitimate does not mean that it is. Often scammers will create phony, but very legitimate appearing domain names.

The [Google Safe Browsing Transparency Report](#) is a terrific free service where you can type in the URL and learn if Google's research indicates it is a scam.

You can also use [Whos.com](https://whos.com) which is a free service that will tell you who owns a particular URL and how long it has been in service. If your Walmart website has only been around six months and is owned by someone in Nigeria, it certainly is a scam.

Finally, Google now is using AI to provide enhanced protection when using Google Chrome to recognize scam websites and warn you about them.

Social Media Ads

Scammers also purchase ads on Facebook, Instagram, TikTok and other social media platforms which enable them to use social media's algorithms to specifically target vulnerable victims such as people living in parts of the country experiencing particularly hot weather, homeowners, and older people looking for bargains.

How to avoid social media ad scams

As always, if the claims in an ad about a particular air conditioner's capability or its price appear too good to be true, you should immediately be skeptical. Trust me, you can't trust anyone. Never click on the ad to buy an air conditioner directly from the ad. Instead do your own research and search for independent reviews of the particular air conditioner as well as its availability at major retailers with which you are familiar.