US Census Scams – In person, over the phone, email, and social media

Identity thieves and other scammers are using another tool to obtain personal information: the 2020 U.S. Census Bureau questionnaire.

Every 10 years, the Census Bureau collects personal information to tally the people living in the United States. Census officials may try to contact you by phone, letter, and in person.

Be careful, not all people who say they’re census officials will be legitimate.

The caller could be a scammer, trying to collect your personal information for their own purposes.

The census is known to collect your personal information. Scammers view this as an opportunity to get enough personal information from you to commit identity theft and other frauds.

Here’s a list of the census scams you should be aware of, along with steps you can take to help you avoid becoming a victim.

Phone scams

Census officials may approach you in one of three ways: a phone call, a letter in the mail, or a knock at your door. **They will not reach out to you via email.**

If you’re contacted by phone, there are ways to verify that the caller is legitimate.

It’s not always easy to tell. Here are three phone scams to be aware of.

1. **Phone spoofing**

   Scammers may call you, and the call may look like it’s from the Census Bureau. But there’s a problem. Scammers can manipulated the caller ID to make it look legitimate.

   How will you know the caller is a real census worker or not?

   Callers should identify themselves and the name of the survey. If you don’t answer, they should leave a message with the case ID associated with your survey.

   You can call the Census Bureau to verify a caller’s name is in the [Census Bureau’s online staff directory](https://www.census.gov/2020census/). 

2. **Asking sensitive questions outside the scope of the census**
Legitimate census callers will ask you for some personal information. That does not include:

- your Social Security number
- bank and credit account numbers
- passwords

If a caller asks you for this type of sensitive data — information that may allow them to impersonate you, often for financial gain — you can be sure it’s a scam.

The questions on the census aren’t extensive or sensitive. The questions involve the number of people in your household along with other identifying characteristics. The idea is to get an accurate read on the U.S. population.

The census questionnaire asks basic questions related to these five facts.

- The number of people in your home.
- Their identifying characteristics: gender, age, race, ethnicity.
- Their relationships to one another.
- Your address and phone number.
- Whether you rent or own your home.

3. Delinquency scams

If you haven’t completed a census questionnaire and have already received a letter, you may receive a follow-up phone call from a census taker. Legitimate callers will not claim that you will go to jail if you fail to fill out the census. Other threats or warnings, such as the police are going to come to your home, are also false.

If the caller tells you that you can pay a fine as a remedy, with a prepaid debit card, for example, it’s a scam.

Mail scams

The Census Bureau usually contacts you through the mail. Make sure that letter you received is from a census representative. Here are a few ways to spot scammers.

4. A survey without a proper census ID

In your census invitation to respond, you’ll receive a unique census ID that’s 12 characters (numbers and letters). If you don’t receive a census ID, the survey is not from the Census Bureau.

5. Postcards with QR codes
Some scammers will send you a postcard with a QR code. It will ask you to scan the code with your cell phone to access the survey page. But here’s the problem. When you scan the code, you may upload malware. Don’t do it.

6. Fake invitation mailings

If your invitation mailing doesn’t look like the invitation letter on the Census Bureau page, don’t respond.

7. Envelope lacks usual identifiers

If you receive a survey or letter by mail, the envelope can help verify whether it’s legitimate. If the return address doesn’t say “U.S. Census Bureau” or “U.S. Department of Commerce,” then it’s not legitimate.

The return address on the envelope you receive also should say Jeffersonville, Indiana.

In-person scams

You may be visited by a census taker. That’s normal. Keep in mind a census taker may come back to your door up to six times. The census taker should leave a door hanger with a contact number.

If you have a policy of not to answering the door for strangers or because of COVID-19, you may want to fill out the census questionnaire online, as detailed below.

There also are a few details that can help you spot a scammer at your door.

8. A field rep doesn’t have proper ID or equipment

A real census taker should show you an ID badge that includes their name and photograph, a U.S. Department of Commerce seal, and an expiration date. The representative also should have an official bag and bureau-issued electronic device with its logo.

9. Visits outside of census times

Census takers are only supposed to knock on doors from 9 a.m. to 9 p.m.

Census takers may attend local community events with computer tablets to help individuals respond online.

If you still don’t know if the person at your door is really with the Census Bureau, call 844-330-2020 to speak with a census representative. If you believe the visitor is not legitimate, call Security or if you live off campus, your local police department.
Online scams

Scammers may try to get your personal information by posing as the census bureau online. They may contact you using social media, or in an email. They may ask you to click on a link to a fake survey or download an attachment that could contain malware or other malicious viruses. Here are a few online scams to watch out for.

10. Phishing scams

Phishing happens when a malicious third party pretends to be someone they aren’t. Their objective is to get your personal information. The scammer will attempt to direct you to a fake website that may look like it’s a trusted entity, like the Census Bureau, your bank, creditor, or other entity that you might expect to receive legitimate emails from. But when you enter your personal information, the scammer will have it to use for illegal purposes.

11. Malware scams

Scammers may send you a seemingly legitimate email with a link to the census survey. Don’t click on that link. You could be downloading malware onto your computer or device. Remember the Census Bureau will not request information over email.

12. Social media scams

Scammers may also target social media platforms. Social media scams are similar to phishing emails. You may see a posting from what appears to be a legitimate source like the Census Bureau. But when you click on that link, or download the document, the scammers may infect your device with malware or steal your personal information.

13. Census job scams

Scammers sometime post fake census jobs. They post a fake job application for a temporary position. This may not seem suspicious because the Census Bureau sometimes hires temporary workers. Don’t pay any application fees or give out your personal or financial information.

For more information on scams and avoiding fraud, visit the US Census Bureau website.