Top Scams Targeting Older Americans in 2021

Here's how to recognize and protect yourself from these costly cons

by Sari Harrar, **AARP**, April 1, 2021

1. Zoom phishing emails

Con artists registered more than 2,449 fake Zoom-related internet domains in the early months of the pandemic, just so they could send out emails that look like they're from the popular videoconferencing website, according to the Better Business Bureau.

The scheme: “You receive an email, text or social media message with the Zoom logo, telling you to click on a link because your account is suspended or you missed a meeting,” says Katherine Hutt, national spokesperson for the BBB. “Clicking can allow criminals to download malicious software onto your computer, access your personal information to use for identity theft, or search for passwords to hack into your other accounts.”

How to avoid: Never click on links in unsolicited emails, texts or social media messages, Hutt says. If you think there is a problem with your account, visit Zoom's real website at Zoom.us and follow the steps for customer support.

2. COVID-19 vaccination card scams

Many who got a COVID vaccine posted selfies on social media showing off their vaccination card. Scammers immediately pounced.

The scheme: “With your full name, birth date and information about where you received your shot, scammers have valuable data for identity theft, breaking into your bank accounts, getting credit cards in your name and more,” Hutt says.

How to avoid: If you want to inform friends and family that you got your shots, a selfie with a generic vaccine sticker will suffice. “Or use a Got My Vaccine profile picture frame on social media,” Florida Attorney General Ashley Moody suggests. And review your social media security settings to choose who can see your posts.

3. Phony online shopping websites

Phony retail websites aren't new, but they look more real today than ever before. “Fake sites are using photos from real online retailers and mimicking their look and feel,” Hutt says.

The scheme: You click on an ad online or on social media, see stuff you like at a great price, enter your credit card info … and never receive a product. “Or you receive a lower-quality item shipped directly from an overseas seller,” Hutt says.

How to avoid: Never click on an ad to go to a retailer's website. Instead, bookmark the URLs of trusted shopping websites you visit frequently and use those, suggests Tyler Moore, professor of cybersecurity at the University of Tulsa. “Don't bother with trying to figure out whether the web address is real. Attackers adapt and change them frequently.”

If you're considering buying from a new site, first check online reviews as well as the company's track record via the Better Business Bureau's online directory (bbb.org).

4. Celebrity impostor scams

Real celebs like Kim Kardashian and Justin Bieber grabbed headlines during the pandemic with social media money giveaways. Fans posted their cash-transfer app identifier (or $Cashtag, in Cash App) for a chance at free money. Right away, scammers posing as celebrities started offering fake giveaways as a way to get people's private information.

The scheme: You get a note via social media, email or text message, claiming you won! You just need to verify your account info and send a small deposit up front.

How to avoid: If you really win, you won't be asked to send money first, says Satnam Narang of Tenable, a cybersecurity firm. “The easiest way to defeat this scam is to block incoming requests on your cash-transfer app. Remember: If it sounds too good to be true, it probably is."

5. Online romance scams

They're not just lurking on dating sites. “Romance scammers are getting close to unsuspecting women and men in online prayer groups and book groups, through online games like Words With Friends and other groups people are turning to during pandemic isolation,” Nofziger says.

The scheme: Scammers typically lure their romance marks off of sites that may be monitored and onto Google Hangouts, WhatsApp or Facebook Messenger, where no one's watching. Eventually they hit you up for money.

How to avoid: Rule number one: Never send money to someone you've never met in person. And say no to requests for suggestive selfies and videos that a scammer can later use to blackmail you. “It's flattering to be told you are attractive,” Nofziger says, “but it will be used against you.”

6. Medicare card scams

Scammers are emailing, calling and even knocking on doors, claiming to be from Medicare and offering all sorts of pandemic-related services if you “verify” your Medicare ID number.

The scheme: The offers include new cards they claim contain microchips. Some posers are asking for payment to move beneficiaries up in line for the COVID-19 vaccine.

How to avoid: Hang up the phone, shut the door, delete the email. According to the Centers for Medicare & Medicaid Services, Medicare will never contact you without permission for your Medicare number or other personal information. And it will never call to sell you anything. Guard your Medicare number and never pay for a COVID vaccine. It's free.

7. Peer-to-peer (P2P) payment scams

The rise of smartphone tools like CashApp, Venmo, Zelle and PayPal, which let you transfer money directly to another person, has led to a range of frauds.

The scheme: “One of the more pervasive is the so-called ‘accidental transfer of funds’ scam,” Narang says. “A scammer sends hundreds of dollars, then sends a follow-up message requesting the money back, claiming it was ‘an accident.’ “ But the original transfer was made with a stolen debit card; those funds will eventually be removed from your account. And you're out the money.

How to avoid: Scrutinize money requests before hitting “accept.” To be extra diligent, “disable [or block] incoming requests altogether on your app and only use it for sending money,” Narang suggests. Enable it when someone you trust is about to send you cash. And ignore a notice to return an accidental deposit. Report the incident to the app's support team to resolve the dispute.

8. Social Security scam calls

Scammers are using “spoofed” phone numbers that look like they're coming from Washington, D.C., to appear credible.

The scheme: You get a scary phone call saying your Social Security number was used in a crime — and you'll be arrested soon if you don't send money to fix it. “They may say your number was used to rent a car where drugs were found and that the Drug Enforcement Agency is on their way to your house,” Nofziger says. “The caller may refer you to a local law-enforcement website where you can see the person's picture. You think you've checked it out, call them back and send money.”

How to avoid: “Don't pick up the phone unless you absolutely know who's calling,” Nofziger says. “If it's important, they'll leave a voicemail.”

9. Account takeover scam texts

Scammers are sending fake text messages alleging there's big trouble with your internet account, a credit card, bank account or shopping order on Amazon. They want you to click on links and provide personal info.

The scheme The urgent-sounding text message may have a real-looking logo. “People don't expect scammers to use text messages, so they're more likely to click,” Moore says.

How to avoid: Remember, don't click on links in emails and texts that you haven't asked for. Call your bank or credit card company to check for a problem. Installing security software on your computer and keeping it updated is also crucial, says cybersecurity expert Brian Payne, of Old Dominion University in Norfolk, Virginia.

AARP’s Fraud Watch Network can help you spot and avoid scams. Sign up for free Watchdog Alerts, review our scam-tracking map, or call our toll-free fraud helpline at 877-908-3360 if you or a loved one suspect you’ve been a victim.