October 2021

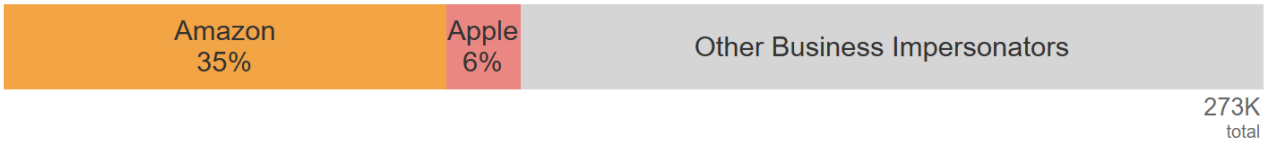
Consumer Protection Data Spotlight
FTC reporting back to you

Amazon tops list of impersonated businesses

Scammers impersonate all sorts of businesses, but reports to the FTC's Consumer Sentinel point to Amazon as a runaway favorite for scammers. From July 2020 through June 2021, about one in three people who reported a business impersonator said the scammer claimed to be Amazon. Reports about Amazon impersonators increased more than fivefold during this period.[1] About 96,000 people reported being targeted, and nearly 6,000 said they lost money. Reported losses totaled more than $27 million. The reported median individual loss: $1,000.

These impersonators get your attention with messages to call about suspicious activity or unauthorized purchases on your Amazon account. When you call the number, a phony Amazon representative tricks you into giving them remote access to your computer or phone to supposedly fix the problem and give you a refund. But then—whoops—a couple of extra zeros are keyed in and too much money is (supposedly) refunded. They tell you to return the difference. In fact, some people have reported that the "representative" even begged for help, saying Amazon would fire them if the money wasn't returned.

About **1 in 3** people who report a business impersonator say the scammer pretended to be Amazon.



Of 273,000 people who reported a business impersonator from July 2020 - June 2021, about **96,000** said the scammer claimed to be Amazon, and about **16,000** said the scammer claimed to be Apple.

These figures are based on reports to the Federal Trade Commission's Consumer Sentinel Network categorized as business imposter scams. Reports that did not indicate the business name used by the business impersonator are excluded.

To make their lies about refunding that so-called overpayment more believable, scammers have reportedly accessed people's online banking. They move money from one account to another—say, from savings to checking. Then, when people see a large deposit in their checking account, they think it's the refund, but it's all fake. If they send money, as requested, they end up sending their own (very real) money.

In another twist, scammers tell people to buy gift cards and send pictures of the numbers on the back. The scammers may call these numbers "blocking codes" or "security codes," and explain that sharing them can block the hackers who—supposedly—took over the Amazon account in question. But the only thing those numbers are good for is getting (or stealing) the money on the card. After people send pictures of the gift cards, they often report getting texts confirming a supposed account credit in the amount of each gift card purchase. That's just another trick scammers use to get their targets to buy more cards.

Another common hook are text messages that say you've won a raffle for a free product from Amazon. People who click the link to claim their free prize then have to enter credit card information to pay for "shipping." Before long, they see charges they never agreed to.

Most people who report these scams say the scammer contacted *them*.[2] But some people have reported finding bogus phone numbers when searching online for the number to call Amazon about a *real* issue. Of course, the scammers who answer calls to those phone numbers are happy to "help."

The data suggest that Amazon impersonation scams may be disproportionately harming older adults. Over the past year, people ages 60 and up were over four times more likely than younger people to report losing money to an Amazon impersonator.[3] Older adults also reported losing *more* money—their median reported loss was $1,500, compared to $814 for people under age 60.

After Amazon, Apple is the second most frequently reported company, but it's a distant second. Apple impersonators reportedly tell people their iCloud account has been compromised or that they've been chosen to get a free iPad. Sound familiar? Scammers change names but often use the same lies again and again.[4]

Here are ways to avoid some common tricks business impersonators use:

- Never call phone numbers given in unexpected calls, texts, emails, or messages on social media. And don't click any links. Those are scams.
- If you're worried, check it out. Go directly to the company's website to find out how to reach them. Don't trust the phone numbers or links that come up in search results.
- Never give anyone remote access to your devices unless **you** contacted the company first (using its real number). If someone tells you to give remote access to get a refund, it's a scam.
- Never pay by gift card. Nobody legit will ever require you to. And never send pictures of gift cards. If someone tells you they need the numbers on the back of a gift card, it's a scam.
- Talk about it. If you're getting these messages, so are people you know. Help them avoid the scam by sharing what you know.

To learn more about how to spot, avoid, and report scams—and how to recover money if you've paid a scammer—visit ftc.gov/scams. If you spot a scam, report it to the FTC at ReportFraud.ftc.gov.

1 Amazon impersonator scam reports increased from 1,794 reports in July 2020 to 9,796 in June 2021. Amazon impersonator scams are defined here and throughout this Spotlight as reports from all sources to the FTC's Consumer Sentinel Network that are categorized as business imposter scams and name Amazon as the impersonated company.

2 About 70% of Amazon impersonator scams reported from July 2020 through June 2021 identified a phone call as the method of contact, followed by text (15%), and email (8%). These percentages exclude reports that did not specify a method of contact.

3 This age comparison is normalized based on the number of loss reports per million population by age during this period. Reports from consumers under age 18 are excluded. Population numbers were obtained from the U.S. Census Bureau Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States (June 2020).

4 Prior to the increase in reports of Amazon impersonators, Social Security Administration impersonation scams were the most frequently reported imposter scam. From July 2020 through June 2021, reports about Social Security Administration impersonators totaled 80,797. The number of reports about Social Security Administration impersonators declined from 7,441 in July 2020 to 4,166 in June 2021. For more information, see the April 2019 Consumer Protection Data Spotlight, "Growing Wave of Social Security imposters Overtakes IRS Scam," located at ftc.gov/spotlight.