



Phil Archer


The Monthly Brief

Volume 12 Issue 4

April 2024

AMAZON PHONE SCAMS

Did you get a call or text about a suspicious purchase on Amazon? Well, it's a scam.

 This new and complicated scam starts with a call or text message about a suspicious charge on your Amazon account. But it's not really Amazon. It's a scammer.

The caller ID is fake making it appear it's from Amazon so you'll answer. Once in contact, the scammer creates fear by telling you your account or identity was used to commit criminal fraud. Worse yet you're a suspect. To avoid arrest they ask for your personal identity info, account verification, and payment of a fine or fee. **Don't do it!**

No one legitimate will tell you this or ask for a payment to fix it. If there's a problem with your account or identity, always talk with someone you trust — especially if the stranger on the phone says it's serious or involves a crime or claims to be from the government. That's always a scam.

Hang up and log into your account to verify it's status. Visit the [Amazon security guide](#) to identify if a call, email, or text are legit.

Get a free instant copy of your credit report at [AnnualCreditReport.com](#) and check for accounts you don't recognize.

If someone stole your identity to open fake accounts go to [IdentityTheft.gov](#) and submit a report, Then put an extended fraud alert on your credit report. Do not transfer money or drain your savings to protect it from fraud.

Learn more about [text scams](#) and how to protect yourself. *FTC, Amazon, Security.org

Comments or Questions?

Subscribe: philarcher@sa18.org

Password Security



It seems the [rules for creating the best passwords are always changing](#). It's no longer safe to just have a mix of letters and numbers. On average, it takes a hacker about two seconds to crack an 11-character password that uses only numbers.

Cybercriminals use sophisticated software that can run thousands of password combinations in seconds, and AI is taking it to next level. A strong password should not be less than 11 characters. 14 or more is best, using numbers, upper and lowercase letters and symbols. Avoid using any words found in a dictionary, names, characters, products, or organizations.

With your current passwords in mind, how long do you think it would take a hacker to crack them? If you are unsure, check out the [How Secure Is My Password? tool](#). By putting in some of your passwords, the system will tell you how long it will take a hacker to crack. The site will also provide you with helpful tips on making your password stronger and [information on password managers and security keys](#). Using a password manager to create complex passwords and complete logins automatically is a great way to secure accounts. They work on computers or mobile devices, but some have subscription fees. Both [Apple](#) and [Google](#) currently offer these services at no cost.

Wondering if your password has been cracked or exposed to the Dark Web before? The [Have I Been Pwned](#) website can answer that question for you. *Komando; ;HIBP, Security.org

ANNUAL FTC SCAM REPORT

Every year the FTC shares the information on reported scams in a [data book](#) so everyone can spot and avoid them. [In their latest summary report](#), the FTC received 2.6 million reports of fraud, with victims reporting losses of nearly \$10 billion. That's roughly \$7 billion more than 2020 and an indication that criminals aren't taking any time off.

1 in 4 people reported losing money to scams, with a median loss of \$500 per person. Email was the #1 contact method in 2023, especially when scammers pretended to be a business or government agency to steal money.

The report includes info on other emerging trends, including these takeaways:

Imposter scams remained the top fraud category, with scammers pretending to be your bank's fraud department, the government, a relative in distress, a well-known business, or a technical support expert. [Here are some common imposter scams](#).

Scams starting on social media accounted for the highest total losses at \$1.4 billion – an increase of 250 million from 2022. But scams that started by a phone call caused the highest per-person loss (\$1,480 average loss).

Of people who reported their age, younger adults (20-29) reported losing money more often than older adults (70+). However, when older adults lost money, they lost the most

To find out more and see what's happening in your area, visit the [FTC's interactive dashboards](#). To learn more about reporting fraud visit [ReportFraud.ftc.gov](#) *FTC