



Phil Archer

The Monthly Brief

Volume 9 Issue 4

April 2021

AMAZON TEXT SCAMS

Who doesn't like to win prizes, especially if they are the latest Apple AirPods or a brand-new Apple Watch. That's why scam artists are using offers of free gifts as bait to trick you. The latest scheme making the rounds implements [spoofed Amazon text messages to rip you off](#).

If you received a notification from Amazon that you have won their sweepstakes, it's going to be a scam. Typically the text will claim you've won expensive tech (like AirPods or an Apple Watch) from Amazon. The Better Business Bureau is reporting the messages are often from the numbers (714) 883-6385 and (714) 507-5880, but there are more.

 The message might even include your real name or one close to yours. As with most text message scams, this one will instruct you to click on a link to claim your prize.

The link will take you to a malicious site and once you enter your details to "claim the prize" the crooks capture your information. Here are some tips to avoid text message scams:

Be Skeptical of unsolicited texts offering prizes or rewards. At best it's click bait, at worst you can get malware on your device.

Don't follow links in suspicious texts. These can lead to fake websites and efforts to trick you out of personal ID info.

Ignore instructions to reply "Stop" or "No" to opt out. This signals a working number and you'll get even more messages.

[Learn more about text scams and how to report them to Amazon.](#)

*BBB; Amazon; Komando

Follow Us On Facebook

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 a minute, and their tools are only getting better. A general rule is that your password should be at least 11 characters. But if it's 12 characters using numbers, upper and lowercase letters and symbols, it will take a hacker 34,000 years to crack.

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 suggest various security measures to implement.

Another great way to secure your accounts is to use a password manager that creates and stores all your passwords for you. You only have to remember the master password, but you will have to maintain any subscription fees. Wondering if your password has been cracked or exposed to the Dark Web before? The [amazing HaveIBeenPwned](#) website can answer that question for you.

*Komando.com; HIBP ;HSIMPW

2020 TOP 3 FRAUDS

2020 was a tough year. Between the pandemic and the economic crisis, we all had our hands full. But scammers didn't take any time off and it was a busy year for fraud. How busy? The [FTC got 2.2 million reports](#), with victims reporting losses of nearly \$3.3 billion. How did they do it? Well lets start the countdown!

#3 Phone Scams. The phone remains the most common way scammers are reaching us, using calls and now text messages are seeing a sharp increase. Many of these texts were related to the pandemic including [stimulus relief](#) (look for that again soon), [economic relief](#), or "[waiting packages](#)."

#2 Online Shopping. Go figure with everyone stuck at home there was a wave of reports about sellers failing to deliver on promises—or just failing to deliver period. The FTC received more than 350,000 reports, with losses totaling over \$245 million, and an average loss of \$100. [Learn how to protect yourself from online shopping fraud.](#)

#1 Imposter Scams. Crooks pretended to be nearly everything from government officials, to known businesses like Amazon, to a family member or friend needing help. With 500,000 reports and losses totaling \$1.2 billion, the average loss was \$850! Most common were government imposters and COVID-19 stimulus scams, proving once again, that scammers follow the headlines. [Here are some common imposter scams.](#)

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