



Are All Downloads on Mobile App Stores Safe?

Mobile apps let us play, teach us, give us social media or music, and more. No wonder there were more than 142 billion downloads in 2022! Going to Google or Apple's mobile stores to find the app you want feels safe, but even these heavy hitters can't guarantee you're downloading something secure.

Google and Apple do their best, but they are vetting thousands of new apps submitted monthly. The vast majority of their offerings aren't a threat, but some malicious apps make it through.

What do malicious apps do?

Apps downloaded from mobile stores are typically more secure than your Web activity. On an app, you're within a contained system, whereas on the Web, you click through various links and visit websites which could have viruses or malware.

Still, a malicious app can infect your smartphone and cause several issues:

- **Ad fraud.** The app runs in the background and sends ad clicks to different websites. This runs down your battery and slows your phone activity.

- **Data theft.** If you give a malicious app permission to cross the app/data divide, it could lead to information being stolen.
- **Browser hacking.** The app may open website browsers that put you at risk of sharing sensitive data.
- Apps access all your information (SMS, camera, contacts) and take control of your device.

Keep your mobile phone safe

When looking to download a mobile app, do your research. Look at the ratings and how many downloads it has had. Application reviews can also help you verify the credibility of the app. Check the logo and the name of the creator, too. You don't want to install something from Microsoft instead of Microsoft.

Keep your mobile device's operating system current. Installing the manufacturer's updates can help cut your vulnerabilities.

Also, take a moment to review the permissions for that new app. There's no reason a calculator app needs access to your entire address book and camera. If the app asks for too much access, it can be a good idea to delete it and look for another option.

Be wary if you decide to download an app directly from a website other than the app store. This is a greater risk. Plus, know that illegally pirating software or media is a real risk for viruses.

Also, keep an eye out for common signs of a virus on your phone such as:

- other apps taking longer than usual to open or install;
- phone battery running down faster than normal;
- your monthly data usage increasing;
- your contacts receiving odd messages from you via email, text, or social media.

Worried you may have a virus on your device? We can check and see and then secure your phone. We can also help backup your data and wipe a compromised phone, if needed.

Call us today at 940-282-0290.



Don't Fall for Deepfake Voice Scams

Deepfake has gone mainstream. You've probably seen a movie or TV show with a character complaining about images or videos that look real. You should also be wary of deepfake voice scams.

Deepfake is a mashup of the words deep learning and fake. The technology uses artificial intelligence and machine deep-learning algorithms. This can create convincing representations of people for special effects or silly videos, but these fake videos or images can also be more dangerous.

Malicious deepfakes spread false information or can defame or scam people. That's what we want to talk about in more detail here: Deepfake voice scams.

What is a deepfake voice scam?

This type of scam manipulates synthesized speech to convince you someone is saying something they didn't actually say. This increasingly common scam tricks you into providing sensitive information or sending money.

Criminals first record a voice sample from their victim. They might use speeches, TikTok or YouTube videos, podcasts, or phone conversations. Then, they turn to a tool such as

ElevenLabs, Resemble, Overdub, ReadSpeaker, or Voice.ai. These platforms analyze speech patterns and create a voice mimicking the original. The bad actors can then generate a new speech that sounds like the original speaker said it. They script it, and the AI voice says it.

Examples of deepfake scams include creating a voice that mimics a family member. They'll script a request for help in an emergency situation. Or you might get a call from a lawyer claiming to need payment to help defend a family member.

You might also hear from a celebrity who wants you to donate to their charity. The fake voice might also ask for sensitive information such as banking details. After all, who wouldn't trust Liam Neeson if he called personally?

A tech support scam is another common one. The scammer creates a voice for a customer support rep from a prominent company. They request remote access to your computer to "fix" a non-existent problem. Instead, they'll steal sensitive information such as login credentials, or install malware.

How to defend against deepfake scams?

This technology does a good job, and the scam can be very convincing. Be cautious of unexpected requests for personal information or money made by phone. Be especially suspicious if the request makes an emotional appeal to you to act now.

Confirm before you share sensitive data or transfer money. For example, if you're asked to pay a lawyer to help out your grandson in an accident, check in with him first. Or, if someone calls from your internet service provider, use a trusted phone number to confirm their authenticity.

We can help you combat deepfake scams. We can install email and Web filtering, multi-factor authentication (MFA), and endpoint protection. Our IT experts can also watch networks for signs of attack and respond to cut potential damage.

Contact us today at 940-282-0290.