Parenting, Media, and Everything In Between

How to Protect Your Kid from "Fortnite" Scams

The popular game has become an easy way for scammers to trick kids into sharing way too much information. By Frannie Ucciferri 11/2/2018

Topics: Digital Citizenship, Gaming, Marketing to Kids, Privacy and Internet Safety

You were just getting used to your kid's obsession with *Fortnite*, and now, all you hear about is V-Bucks. V-Bucks, like Robux on Roblox, are *Fortnite*'s in-game currency. Players use them to buy the fun "skins" (characters and outfits) and "emotes" (those hilarious dances like "Flossing" and "Take the L") that kids will say they *totally* need to make *Fortnite* even cooler. For the record: You don't need V-Bucks to play *Fortnite*, and if you do spring for them, they cost real money. Also, online scammers are all over V-Bucks.

Fortnite's incredible popularity among kids has made it an easy target for rip-off artists trying to make some actual bucks while the game is hot. A recent study from online security company ZeroFox discovered more than 4,700 fake *Fortnite* websites, and the company sent out more than 50,000 security alerts about *Fortnite* scams in a single month. Kids are particularly vulnerable to requests to turn over personal information, including names and email addresses or even credit card numbers. Here's how you can spot the scam and protect your kids.

What to watch out for

- **V-Bucks generators.** "V-Bucks generators" are one of the biggest online *Fortnite* scams. These are often websites that offer people points for watching or clicking on ads, and these points can supposedly be traded in for free V-Bucks within *Fortnite*. Not only do these free V-Bucks never appear, these sites often try to collect people's *Fortnite* usernames and passwords or have them take surveys where they submit personal data under the pretense of verifying that they're human.
- **Fake domains.** Similar to V-Bucks generators, there are also tons of sites that offer free V-Bucks or trick people into buying fake ones. These fake domains mimic developer Epic Games' and *Fortnite*'s real styles, colors, and fonts to fool people. Some even put "Fortnite" in the URL. These sites also collect personal information, but they often go a step further in directly charging a credit card or bank account.
- **Social media scams.** One of the most popular ways that scams are spread is through social media. Fake sites and V-Bucks generators often encourage people to share their links to get more points, which helps expose the scam to more people. Plus, these links often direct users to suspicious apps and malware that can also target your kid's personal information.
- **YouTube video scams.** Similar to link-sharing scams on social media, there are tons of YouTube videos offering free V-Bucks and more. These fake videos and accounts have millions of views and send gamers to other sketchy sites.
- **Fake Android apps.** After Epic Games made the controversial decision not to offer their Android app in the Google Play Store, scammers took advantage by putting up fake *Fortnite* apps. Although they're designed to look like *Fortnite*, they're really data theft and malware distributors in disguise.

Tips to avoid getting scammed

Talk to your kids about how to spot and avoid *Fortnite* scams and other scams online. Here are some tips to keep your kid's information private and your money safe:

- **Be cautious when you give out private information.** Tell kids to check with you before filling out forms, quizzes, registration pages, and the like on a website or app. For older kids, teach them to think carefully about why a site or app might want your data.
- **Only spend real money through official platforms.** PlayStation, Xbox, Epic Games' official website, and the official *Fortnite* app are the only places to buy V-Bucks. Anything else is a scam.
- **Double-check URLs and domain names.** Talk to kids about scams and how some sites or apps look very similar to the official ones but are designed to trick you into giving up money or information. Domain names and URLs might have only one letter or symbol that's different from the original, so look carefully.

About Frannie Ucciferri

As associate managing editor, Frannie Ucciferri makes sure each of Common Sense Media's more than 30,000 reviews and 700 curated lists is as complete and comprehensive as possible. Frannie is a graduate of UC Berkeley,... Read more