

Avoid Scams In Online Games

Plain-English how-to. ~15 minutes. Spot fake giveaways, item-duping scams, and account-recovery cons.

The five top scam patterns gamers face and the verification habits that stop them.
Print, share, and re-run quarterly.

Do This Right Now

#	STEP
1.	'Free currency / skin' sites: always scams.
2.	'Pro team scout' DMs: always scams.
3.	'Support agent' DMs you didn't ask for: always scams.
4.	Verify trade partners via steamrep.com and account age.
5.	Never share API keys or disable 2FA on request.
6.	Bookmark real login URLs; never click to log in.
7.	Audit linked third-party apps quarterly.
8.	The 30-second pause stops 90% of scams.

Why This Matters

- Gaming scams have grown into a multi-million dollar criminal industry. The FBI's IC3 reports a steady annual increase in losses tied to gaming.
- Unlike phishing for bank credentials, gaming scams exploit social pressure and excitement: a 'free Knife skin if you spin the wheel,' a 'free Steam Wallet if you watch this video.'
- The cure is pattern recognition. Once you know what scams look like, they become almost comical. The goal of this guide is to make you a pattern recognizer.