Flash-n-Flush
A 90-SECOND READ · K12 CYBER FORWARD

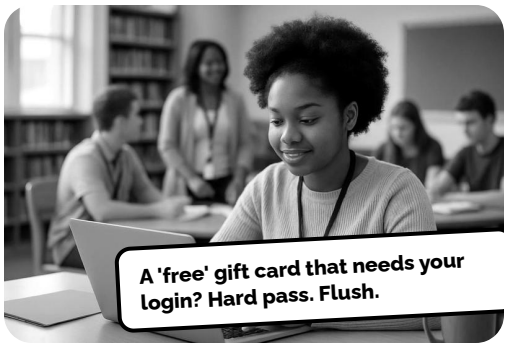
STUDENT EDITION · GRADES 6-12
December · Issue 3

SHARED BY
Your school

GIVEAWAY SEASON EDITION

Free and urgent? That's bait.

Fake giveaways, 'free' phone credits and copycat apps are built to grab one thing: your login, your personal info, or a payment from a family card. They show up in ads, pop-ups and DMs that look official.



1

Get apps from the official store only

Download apps only from your device's official app store or your school's approved list. Check the developer name and reviews. A 'free premium version' from a random link is how malware gets in.

2

Check who's really posting

Fake giveaway accounts copy real logos and photos. Check how old the account is and what it posted before. Real giveaways don't make you pay shipping or share a password to win.

3

No family cards for 'free' stuff

If a free prize needs a card number, a small fee or a login, it isn't free. Ask a parent or guardian before you enter any card info, every time.

Spot the scam

Pop-up External

Pop-up on a game tips website <free-gift-rewards.example/claim>

CONGRATULATIONS: you're today's winner

Congratulations. You are visitor #1,000,000 today and you've won a $500 gift card for your favorite game store. To claim it, install our Rewards Helper app and enter a card number to cover $1.99 shipping. Your prize expires in 02:59, then it goes to the next lucky visitor. Close this window and you lose your spot.

Spot the scam: how many red flags can you find?

Red flags I found: ◯ ◯ ◯ ◯ ◯

Look for: surprise, urgency, secrecy, an unusual payment method, a sender or link you can't confirm.

FUN FACT

Georgia, this one's about us: in the FBI's 2025 Internet Crime Report, Georgia ranked number one in the nation for money lost by victims 17 and younger, more than $3 million.

Source: FBI IC3 2025 Internet Crime Report

Your 60-second move

Scroll through your phone's apps and delete any you don't use or don't remember installing.

Who do I tell?

Name / ext. _____

Report channel _____

ANSWER

Five flags: a 'millionth visitor' claim, a too-good prize, an app to install, a card for 'shipping' and a countdown. Smart move: close the tab without tapping anything inside the pop-up, don't install anything, and tell an adult if you already entered card info.

- 'Millionth visitor' pop-ups have been a scam for decades.
- A huge prize for doing nothing is too good to be true.
- An app from a pop-up can be malware.
- A card for 'shipping' is how they get the card number.
- A countdown timer is fake pressure.

Scan for a 2-minute lesson on fake sign-in prompts
Free, no sign-in · k12cyberforward.com/learn