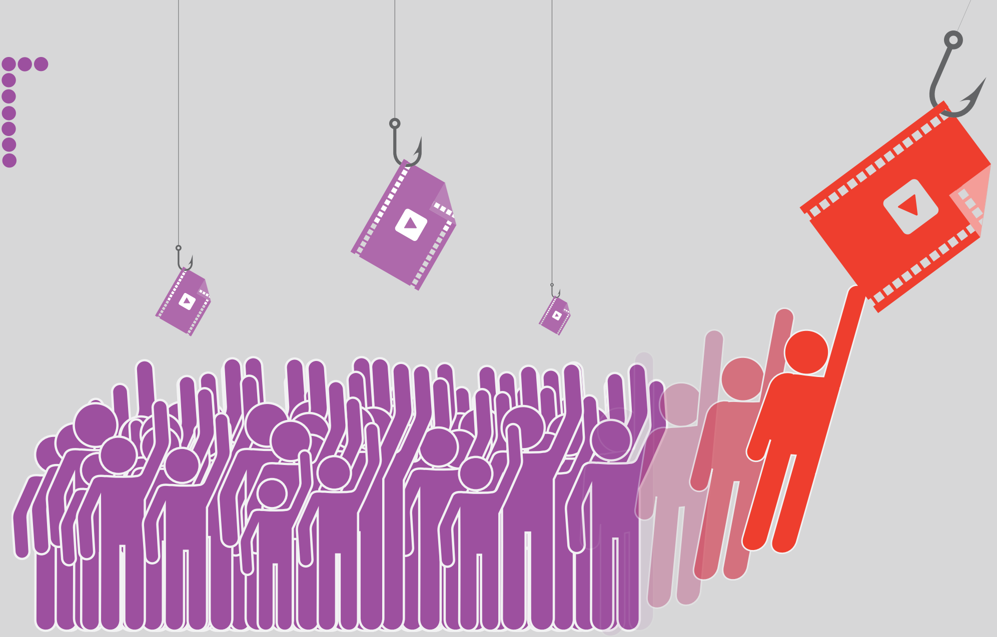
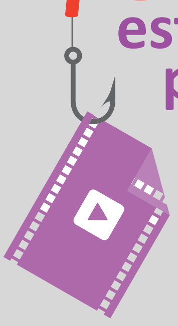
DON'T TAKE THE BAIT



Creators aren't the only ones harmed by content theft. Criminals also prey on users of these sites for identity theft and other malicious scams.

$70M
estimated per year



Baiting Internet users with stolen creative content is big business. Criminals make millions of dollars every year by stealing their personal information and taking control of their computers. And this figure is only what content theft sites earn for installing malware. It does not include revenue made by malware operators from identity theft schemes, ransomware, and other scams once the malware is installed.

How Digital Thieves Rip Off Consumers

- Stealing bank and credit card information and selling it on underground Internet exchanges.
- Finding personal information that makes it easier to sell a person's identity online.
- Locking a user's computer and demanding a ransom fee.
- Hacking a computer and controlling it to commit ad fraud, spamming, denial of service attacks, and extortion.

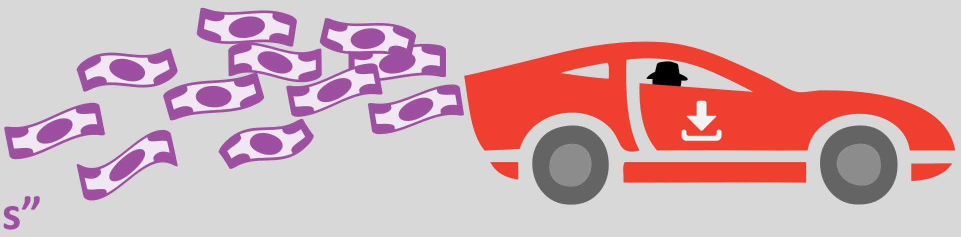
Internet users who visit content theft sites are at a high risk of exposure to malware, according to "Digital Bait," a new report by RiskIQ commissioned by the Digital Citizens Alliance.

1/3
content theft sites distribute malware

28X
more likely to have malware than legitimate sites

Merely visiting a content theft site can place a users' computer at risk – invisibly downloading malware even if the user doesn't click on a link.

45%
of malware is delivered through "drive-by downloads"



Online criminals have become more sophisticated in how they use content theft to generate illegal revenue streams. It's not just a threat to creators and legitimate advertising companies. They're targeting users, too. Don't take the bait!

#FollowTheProfit

To see the full Digital Citizens report and research by RiskIQ, go to www.digitalcitizensalliance.org.

RISKIQ®

digitalcitizens alliance