

SECURITY

Back-to-school malware is hiding in those digital textbooks

Kaspersky warns that it found more than 100,000 textbook files with malware lurking inside.

BY RAE HODGE | SEPTEMBER 3, 2019 1:41 PM PDT



Researchers warn that malicious actors are targeting students seeking to escape rising textbooks costs via online alternatives.

Jeff Greenberg/Getty Images

C|NET

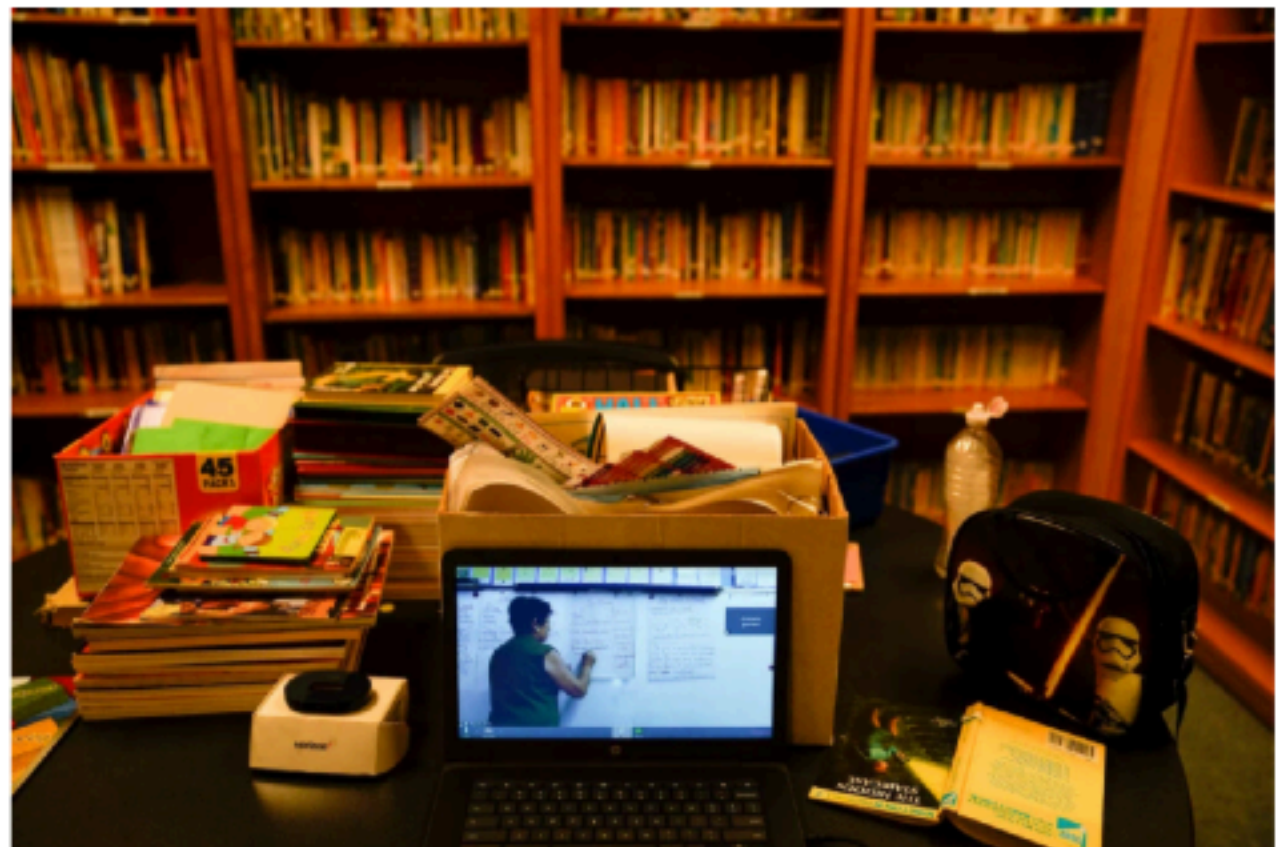
September 2019

New York Times

September 2020

Website Crashes and Cyberattacks Welcome Students Back to School

With many districts across the country opting for online learning, a range of technical issues marred the first day of classes.



Many of the nation's school districts faced technical challenges on Tuesday while starting the academic year remotely. Jae C. Hong/Associated Press



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



February 01, 2022

Alert Number
I-020122-PSA

Questions regarding this PSA
should be directed to your
local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Scammers Exploit Security Weaknesses on Job Recruitment Websites to Impersonate Legitimate Businesses, Threatening Company Reputation and Defrauding Job Seekers

The FBI warns that malicious actors or 'scammers' continue to exploit security weaknesses on job recruitment websites to post fraudulent job postings in order to trick applicants into providing personal information or money. These scammers lend credibility to their scheme by using legitimate information to imitate businesses, threatening reputational harm for the business and financial loss for the job seeker.

Since early 2019, the average reported loss from this scheme is nearly \$3,000 per victim, and many victims have also reported that the scheme negatively affected their credit scores.

FBI IC3

February 2022

security.org

March 2021



Account Takeover Fraud: A Consumer's Guide to Protecting Yourself



By Aliza Vigderman | Published March 17, 2021

Account takeover fraud is a type of cybercrime or identity theft where a malicious third-party gains access to (or "takes over") an online account, such as an e-mail address, bank account, or social media profile. In fact, our research shows it's happened to about 1 in 5 adults. In this guide, we break down exactly what account takeover is, how it happens, and most importantly, how to prevent it. Account takeover is often abbreviated as ATO or called account fraud.