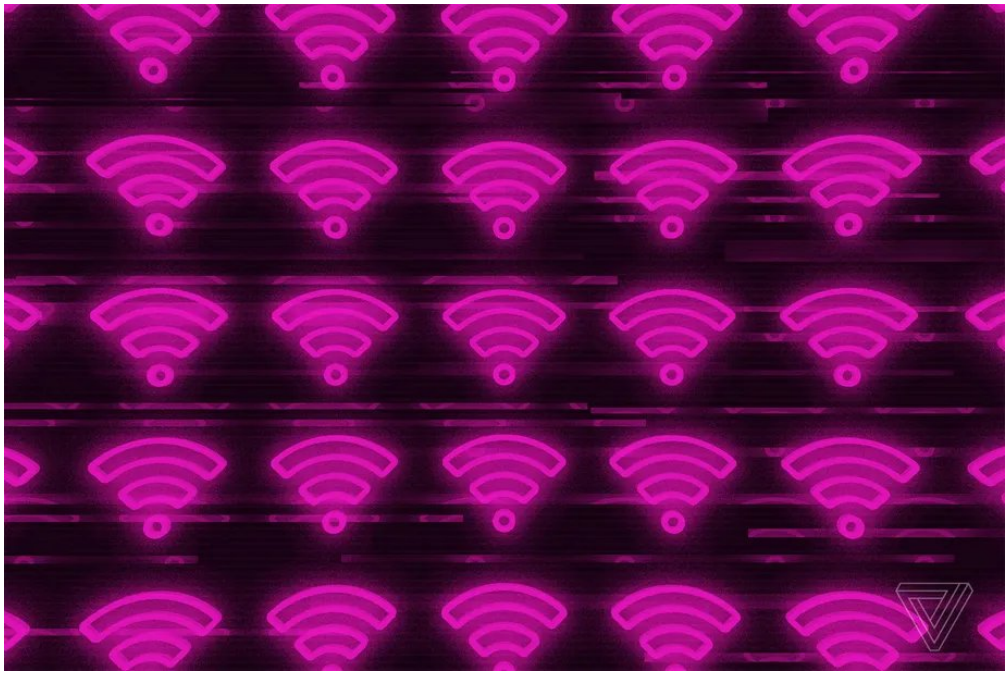
POLICY TECH CYBERSECURITY

13

Go read this report about the horrifying leaks coming from school ransomware attacks

Cyberattacks on schools put children's SSNs, birthdays, and more on the dark web

By Mitchell Clark | Sep 10, 2021, 7:13pm EDT



Illustrator by Alex Castro / The Verge

Ransomware has been a hot-button topic in 2021 due to its impact on critical infrastructure, hospitals, and computer manufacturers. However, a recent report from *NBC News* may be one of the more heartbreaking accounts of the effects hackers can have: it details how data leaks from attacks on schools can put student's most sensitive information out onto the internet, available to anyone who knows how to find

it and is willing to pay. It's a story that's well worth a read for all the details it goes into and edge cases it explores.

According to *NBC*'s report, one school district had an Excel sheet called "Basic student information" posted to the dark web after it refused to pay a ransom, according to the FBI's instructions. The article's author, Kevin Collier, breaks down the shocking information it contains:

> It lists students by name and includes entries for their date of birth, race, Social Security number and gender, as well as whether they're an immigrant, homeless, marked as economically disadvantaged and if they've been flagged as potentially dyslexic.

The school knew about the attack and informed parents about it — making it potentially one of the better scenarios. Insurance covered identity theft protection for staff, but it's unclear whether that benefit extends to students even after getting lawyers involved. In other cases, when *NBC News* asked some schools about their leaks, they seemed "unaware of the problem."

CREDIT AND IDENTITY THEFT IS ONE OF THE OBVIOUS PROBLEMS

It's hard even to comprehend how it could affect a student's social life if their grades, medical info, or free or reduced-price lunch benefit status leaked online. What's easier to understand is the impact of having their SSNs, birthdays, and names sold to unscrupulous people: *NBC* tells the story of a student whose info was used in attempts to get a credit card and car loan.

I know firsthand the hell that can come from having your credit wrecked before you even get out of high school, and I wouldn't wish it on anyone. The report cites Eva Velasquez from the Identity Theft Resource Center, who tells parents to freeze their kid's credit to keep them safe from identity theft. Parents already have enough concerns — dealing with kids who are learning remotely or figuring out how to get kids physically to school, all the while worrying that they could catch COVID while they're there. It's hard to accept that parents should also become the data security and privacy experts that school systems are missing.

PROTECTING KIDS' DATA COULD BE EASIER SAID THAN DONE

As an expert at a non-profit for protecting school's IT systems told *NBC*, "it is a solemn responsibility that schools have to care for kids, so they collect a lot of data with that." Clearly, many schools (the report mentions that 1,200 schools' info had been published by ransomware attackers this year) aren't up to the task of keeping that data safe — though doing so is easier said than done, especially while working with budgets that don't allow for the level of corporate security attackers are bypassing daily.

It's incredibly sad to imagine students having to simultaneously worry about their school using FBI-grade tech to steal personal data and hackers stealing information for their school and selling it to criminals. While it may be hard to think about, it's even more difficult to push for change if we don't know what's happening, which makes reports like *NBC*'s so essential and worth the read.