From: POLITICO"s Weekly Education
To: Goins, Anthony
Subject: Hacking the classroom — Asking the cyber experts — Getting kids cyber savvy
Date: Monday, September 21, 2020 9:03:50 AM

Sep 21, 2020 View in browser

POLITICO's Weekly Education: Coronavirus Special Edition newsletter logo

BY **JUAN PEREZ JR.**

Presented by Comcast

Editor's Note: Welcome to Weekly Education: Coronavirus special edition. Each week, we will explore how the pandemic is reshaping and upending education as we know it across the country, from pre-K through grad school. We will explore the debates of the day, new challenges and talk to movers and shakers about whether changes ushered in now are here to stay.

This newsletter is a weekly version of POLITICO Pro's daily Education policy newsletter, Morning Education. POLITICO Pro is a policy intelligence platform

that combines the news you need with tools you can use to take action on the day's biggest stories. Act on the news with POLITICO Pro.

VIRTUALLY VULNERABLE — The FBI blasted a warning to private industry this summer, saying new cyberattacks are likely in store as the nation's schools begin a semester of virtual learning. It was a prescient prediction.

— **Ransomware targeting the Fairfax County school system near Washington, D.C., led officials to loop in federal authorities this month.** Some worried the offensive had links to dozens of cyber-criminal attacks against school systems and businesses. In Florida, a cyberattack attributed to one tech-savvy Miami-area teenager blocked thousands of students and staff from classes during their first week of online learning. Other cyberattacks on the nation's fourth-largest school district have been traced to Russia, Ukraine, China, Iraq and elsewhere.

— **Colleges and universities have long been high-profile targets for hackers and thieves. But the pandemic is laying bare vulnerabilities and privacy concerns in K-12 schools.** Industries reported 9.3 million devices had some kind of encounter with malware in the past 30 days, according to statistics compiled by Microsoft Security Intelligence. The vast majority, more than 5.7 million, targeted the education sector.

— **The challenge is just another aftershock caused by the shift schools have had to make to distance learning.** The taxing spring semester of virtual classes left no doubt that schools must adjust their technology plans, and a flurry of high-profile attacks may raise awareness about information security problems. Today's threats from state-sponsored or amateur hackers are not going to disappear.

Industries targeted by cyberattacks in the last month

Annette Choi/POLITICO

IT'S MONDAY, SEPT. 21. One of the late Ruth Bader Ginsburg's notable education influences was the majority opinion she wrote when the high court ruled unconstitutional the exclusion of women from the state-funded Virginia Military Institute, the last same-sex military academy in the country. While Virginia "serves the state's sons," she wrote in *United States vs. Virginia* in 1996, "it makes no provision whatever for her daughters. That is not equal protection." The court agreed with her 7-1. (h/t our colleague Bryan Bender)

Here's your daily reminder to send tips to today's host at jperez@politico.com and also colleagues Nicole Gaudiano (ngaudiano@politico.com), Michael Stratford (mstratford@politico.com) and Bianca Quilantan (bquilantan@politico.com). Share your event listings with educalendar@politicopro.com . And don't forget to follow us on Twitter: @Morning_Edu and @POLITICOPro. Did someone forward this newsletter?

Sign up. Did you miss last week's issue? It was all about how the pandemic is affecting pre-K.

HOW IS VIRTUAL EDUCATION GOING FOR YOU OR YOUR FAMILY? Tell us, and we may publish your response in our next special edition of the newsletter, which publishes Sept. 28.

AND JOIN US for a town hall discussion on inequalities in education this Thursday. Register to attend.

A message from Comcast:

With an uncertain school year underway, Comcast's Internet Essentials Partner Program is helping communities work together to connect low-income students to the Internet. Since 2011, Comcast has connected more than 8 million low-income families so they can have the tools they need to be ready for anything. Learn more.

HACKED

FLASHBACK TO THE FBI'S SUMMERTIME WARNING — The stark overview, first obtained by POLITICO Pro's cybersecurity team , found growing numbers of ransomware offensives targeting schools well before the pandemic. These attacks often use email phishing scams to block access to critical, sensitive systems until hostages pay up. The government concluded the risks could only grow as schools transitioned to online instruction.

— **"Cyber actors are likely to increase targeting of K12 schools during the COVID-19 pandemic** because they represent an opportunistic target as more of these institutions transition to distance learning," the bureau warned. "This shift has created greater risks for schools, as they now must depend on remote tools."

— **Many K-12 schools already were grappling with a lack of dedicated funding and resources to help vet and improve cybersecurity defenses** before the surge of online classes in the spring, according to one analysis from the Morphisec cybersecurity firm.

— “**And as a result, many failed to employ even the most basic security protocols and left gaping vulnerabilities unpatched,”** Morphisec said. “Now they’re increasingly exposed to third-party technology vendors with security vulnerabilities and IT teams operating remotely.”

QUOTABLE

Herbert Lin

Herbert Lim, a cyber policy and security scholar at Stanford University’s Hoover Institution and Center for International Security and Cooperation, is pictured. | Courtesy of Stanford University

WHY IS THIS HAPPENING? Your host asked Herbert Lin, a cyber policy and security scholar at Stanford University’s Hoover Institution and Center for International Security and Cooperation, to address some basic questions about the state of security in the education industry. The following is a summary of our wide-ranging chat.

Why target ordinary school systems with cyberattacks?

“Here’s the way the syllogism goes. It’s not that the schools have anything that’s potentially ‘valuable’ in the usual sense of the term. But if you hold a school’s records hostage for ransom, for example, then the school district is highly motivated to solve the problem because parents are going to get really, really upset if their kid’s educational records can't get submitted to colleges, they don't have their grades, and all that other sort of stuff. So this applies a lot of pressure.”

Generally speaking, who is responsible for school cyberattacks?

“I’ll tell you that this question of computer-savvy students mucking with the computerized grading systems and computerized aspects of education goes back a very, very long way. I was an undergraduate at MIT, and there were people who were hacking grading systems for classes, too. Sometimes it’s outsiders. If there’s a ransomware demand, it’s usually because they want money. Sometimes it’s people who don’t like the school district, and you can easily imagine some poorly adjusted teenager being mad at a teacher and crashing the school system because of that.”

Why isn’t school cybersecurity at the level it should be?

“It’s just like insurance. How many people would buy automobile insurance if it wasn’t mandated by law? The problem is that security costs money. You pay for security because you want something to not happen. It’s not that something good happens with security, it's that something bad doesn’t happen. Many people say ‘That’s not really a threat to me. I don’t have anything that they would want.’

"Well that’s not true, as it turns out.”

Advertisement Image

FIRST LOOK

Daisley Kramer helps her kindergarten daughter, Meg, with schoolwork at home in San Anselmo, Calif. | Ezra Shaw/Getty Images

PARENTS CONCERNED, CONFUSED ABOUT PRIVACY — New research out today from the Center for Democracy and Technology suggests families are concerned about their children's digital privacy, but they don't have much understanding of the issue.

— **Some key findings:** Student data privacy and information security are "mid- to low-level concerns" of parents, the organization concludes based on an Edge Research survey of a nationally representative sample of approximately 1,200 parents. Parental concerns, however, grow as they learn more.

— **Parents see themselves as most responsible for their child's data privacy and security, along with school administrators, according to the center's research.** But parents report low awareness and involvement in their school's data privacy plan or the way schools collect information about their

child. And they largely trust schools to use student data appropriately.

— **"Parents see a clear role for technology when it comes to educating their children, both during the pandemic and beyond,"** said the center's president and CEO, Alexandra Givens.

— **"Yet, many feel ill-equipped to safeguard their children from data breaches and other safety risks." Givens added.** "And far too many children are unable to utilize education technology at all due to internet access inequalities. As we bring more students online, we need to make sure families are supported and their data is protected."

FOR YOUR RADAR

TEACHING KIDS TO BE CYBER SAVVY — The Cyber Innovation Center, via its CYBER.ORG academic initiative, is rolling out plans to address an ongoing concern: the nation's shortage of cybersecurity knowledge and skills among school-age children.

— **There are few state educational standards that detail what cyber knowledge students should have and be able to use at each grade level,** officials say, nor are there any national standards. CYBER.ORG — which receives support from the Department of Homeland Security — is setting out to change that during the coming year, with help from a group of businesses, schools and government agencies.

— **Their K-12 Cybersecurity Learning Standards Initiative** aims to create benchmarks states can easily adopt and to expand a future pool of eligible workers in the field. A 2017 study, highlighted by the Center for Strategic and International Studies, concluded there will be 1.8 million unfilled cybersecurity jobs across the globe by 2022.

— **The initiative's work is set to accelerate in October and stretch through next year.** The learning standards are expected to be published by August of next year.

A message from Comcast:

For nearly a decade, Comcast has connected more than 8 million low-income families to the Internet at home through its Internet Essentials program.

With an uncertain school year underway, Comcast's Internet Essentials Partner Program is helping communities work together to connect low income students to the internet. And WiFi-connected "Lift Zones" in community centers nationwide will provide a safe space for students and families to get online, participate in distance learning and do their schoolwork. Learn more.

SYLLABUS

— How an epic series of tech errors hobbled Miami's schools: Wired

— Is online learning worse than being in school? Majority of teens say yes: Education Week

— D.C. school leaders struggle to reopen buildings for small groups this month as staff reluctance persists. Washington Post

— How one district got its students back into classrooms: New York Times

— Oregon Department of Education issues ban on hate symbols in public schools: The Oregonian

— 751 Arizona teachers have resigned or retired since the beginning of the school year: Arizona Republic

Follow us on Twitter

Jennifer Scholtes @JAscholtes
Michael Stratford @mstratford
Nicole Gaudiano @ngaudiano
Bianca Quilantan @biancaquilan
Juan Perez Jr. @PerezJr

FOLLOW US

To change your alert settings, please log in at https://login.politico.com/_login?base=https%3A%2F%2Fwww.politico.com

This email was sent to anthony.goins@nebraska.gov by: POLITICO, LLC 1000 Wilson Blvd. Arlington, VA, 22209, USA

Please click here and follow the steps to unsubscribe.