CYBER CRIMINALS ARE BACK TO SCHOOL TOO

September 2021 | Issue 2021:8

CSO's Message

September marks back to school in person for much of Delaware's K-12 community. For many state employees it also means back to a physical office or workplace. The pandemic has brought many changes in how and where we work, and with that comes new opportunities for malicious cyber actors.

Rick McElroy, Principal Cybersecurity Strategist at VMware, cautions that Security Officers face several challenges as workforces return to physical locations. "Endpoint visibility will continue to be one of the biggest challenges CISOs encounter, particularly if their company is implementing a hybrid return to work model. Because employees' devices have been on an open home network for over a year, it is difficult to determine where they all stand from an endpoint protection perspective."

Realizing that a certain percentage of workers are disgruntled at return to the office mandates, cyber criminals are taking advantage of this too. Bad actors

Schools Brace for Cyber Attacks

The Cybersecurity and Infrastructure Security Agency (CISA) is launching the 2021 Back to School campaign to bring awareness of the dangers of phishing and ransomware in K12 and academic settings, and to share cybersecurity best practices. The growing frequency of hacks—averaging more than two per school day last year—has school officials worried about the potential for the theft of students' identities and the added cost to insure against attacks and repair breaches.

Educational institutions continue to report numerous cyberattacks to CISA, FBI and the Multi-State Information Sharing and Analysis Center (MS-ISAC). According to MS-ISAC, the percentage of reported ransomware incidents against K-12 schools greatly increased in the 2020 school year. MS-ISAC reported 57% of ransomware incidents during August and September involved K-12 schools, compared to only 28% of all those reported from January through July.

Malicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible for basic functions, including remote learning. Bloomberg reports that while schools are opening back up across the country for in-person instruction, many are expected to retain virtual learning as an option and that means more access points for potential intrusion with financial consequences for districts that are already facing increased costs to bring students back. In some instances, ransomware actors stole and threatened to leak confidential student data unless institutions paid a ransom. Hackers might be targeting schools to access personal identifying information of young children, laying the groundwork for identity theft years later. Parents of kindergarteners rarely if ever look at their child's credit report; it might be a decade or more before they realize there's a problem and someone has misappropriated their child's identity.

CISA warns that the federal government cannot confront the ever-growing threat of cyberattacks

are reaching out to this cohort, some offering cash or percentages of ransom payments for providing personal or financial data.

That is why it is vitally important that all state and K-12 employees respond to the annual cyber security training notification and complete the assessment by their specified deadline.

Solomon Adote
Chief Security Officer

alone. "That is why we encourage everyone—students, parents, teachers, and administrators—to explore these actionable cybersecurity resources and implement best practices."

To learn more about how administrators, teachers, parents and students can protect data in all facets of the K-12 community check out:

CYBERSECURITY | CISA

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Information & Technology publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to https://digiknow.dti.delaware.gov/pages/cybersecuritynewsletters.shtml

Department of Technology and Information
Contact us at **esecurity@delaware.gov**