Staying Cyber Safe

Students in every grade now utilize technology in the classroom. They may bring their own device or use a school-issued computer; either option increases cyber and information related risks to the school districts' information technology (IT) infrastructure. **Emerging threats and new vulnerabilities are identified every day.**

From 2018 to the present, schools in most states have reported cyber incidents on their systems. Reported incidents between 2018-2021 have risen from 400 in 2018 to an accumulated total of over 1,300.

Recent Cases

Despite cybersecurity measures put in place by many schools, they continue to be the target of threat actors. At the start of 2023, ransomware attacks hit schools across the U.S. from Nantucket to Des Moines, as described below:

- **Nantucket Public Schools**
  The hacking incident shut down all student and staff devices, as well as safety and security systems at Nantucket Public Schools, forcing early dismissal. The Superintendent directed that no school-issued devices should be used at home as it could compromise home networks.
  Source: https://www.cnn.com/2023/01/31/politics/ransomware-attack-schools-nantucket/index.html

- **Des Moines Public Schools**
  IT staff at Iowa's largest school district took 71 buildings – including 63 schools and the virtual secondary school – offline to limit the impact of a ransomware attack. For the next two days, about 30,000 students were out of school as staff worked to restore servers, the internet, networks, and websites. According to district officials, students returned to school without internet, and Wi-Fi was not restored to the buildings until almost 20 days later. Source: https://www.desmoinesregister.com/story/news/education/2023/02/17/des-moines-public-schools-confirms-ransomware-caused-cyberattack/69882337007/

In a Ransomware attack, threat actors attempt to use malicious software to encrypt their victim's files and block access to computer systems until a ransom is paid. Even after a ransom is paid to unlock files, ransomware threat actors will sometimes demand additional payments, delete victim's data, or refuse to decrypt data.

It is vital to combine strong passwords with multi-factor authentication (MFA) to help prevent theft or unauthorized use of login credentials.

It's estimated that a seven-character password that includes Numbers, Upper- and Lower-Case Letters, and Symbols can be cracked in 31 seconds by a professional, and those are typically the people targeting schools.

Source: https://www.techrepublic.com/article/how-an-8-character-password-could-be-cracked-in-less-than-an-hour/#:~:text=Due%20to%20the%20progress%20in,just%2031%20seconds%20in%202022

Continued.

Hive Systems, a cyber security solutions provider, released this helpful password table to highlight the importance of strong passwords. The table shows how fast a password can be decoded by a threat actor.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	**2 seconds**	**7 seconds**	**31 seconds**
8	Instantly	Instantly	**2 minutes**	**7 minutes**	**39 minutes**
9	Instantly	**10 seconds**	**1 hour**	**7 hours**	**2 days**
10	Instantly	**4 minutes**	**3 days**	**3 weeks**	**5 months**
11	Instantly	**2 hours**	**5 months**	**3 years**	**34 years**

Source: https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=header

As ransomware attacks continue to hit schools, IT administrators should employ additional security measures, including:

- **Multi-Factor Authentication**
- **Regular Software Updates**
- **Security Awareness Training for Staff and Students**

Resources for Schools:

- Our partnership with **Vector Solutions** includes access to their online training, including **Protection Against Malware, Email and Messaging Safety**, and **Cybersecurity**. Click here to learn more about Vector Solutions.
- Policyholders with the CyberSuite endorsement have access to the latest cybersecurity tools and information through **eRisk Hub. eRisk Hub** is the cyber education, prevention and resolution portal offered through Hartford Steam Boiler (HSB). Click here to find out more.
- **The Cybersecurity & Infrastructure Security Agency** (CISA) funds student and staff training at cyber.org.

If you have any questions about cybersecurity, please reach out to Certified School Risk Manager Mike Centrone at michael.centrone@uticanational.com.

A portion of this risk management alert was provided by the Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/sites/default/files/2023-01/K-12report_FINAL_V2_508c.pdf