EDTECH SPOTLIGHT: CYBERSECURITY

Cybersecurity stretches beyond the boundaries of district technology teams. Depending on the severity of a cyberattack, districts can lose money, lose data, lose network time, and, ultimately, lose teaching time. This topic impacts our whole society, not just our immediate educational communities. You don't need to be a "*techie*" to know that the speed and function of your Google Classroom, Zoom meeting, or Teams meeting are vitally important to your everyday function in your remote and in-person teaching environment. Yet, the disruption of those applications, among others, is exactly what cybercriminals are trying to accomplish. Hackers are working harder than ever to gain access to the data-rich educational environment. **Is your district prepared to prevent and address a cyberattack?**

Did You Know?

*"Cybersecurity is the art of protecting **networks**, **devices**, and **data** from unauthorized access or criminal use **and** the practice of ensuring confidentiality, integrity, and availability of information."*

"Cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes."

As our society and K-12 education increasingly use email, online tools, applications, and platforms, we also increase our collective risks for cyberthreats and cyberattacks. We encourage school leaders to proactively protect their infrastructure and work to increase individual user awareness of cybersecurity and how to prevent cyberattacks in school and out of school.

Test Your Cybersecurity Knowledge *(answers below)*

Match the term in the left-hand column to its definition on the right➔

1. Distributed Denial of Service (DDoS)
2. Ransomware attacks
3. Email spoofing / email phishing

Definitions

a. A type of malicious software that can deny you access to a computer system until you pay the ransom.

b. The practice of sending fake emails that copy or resemble those from reputable sources with the goal of stealing your confidential data.

c. Attacks to websites and online services with the goal of overwhelming them with more traffic than the server or network can accommodate, making the website or online service nonfunctional.

Answers: 1c, 2a, 3b

Is your district cyber ready? Some questions to consider:

Planning & Prevention

- Does our district have cybersecurity measures in place? What are they? Have we budgeted for them?
- How do we prevent Distributed Denial of Service (DDoS), ransomware attacks, or email spoofing?

Awareness & Education

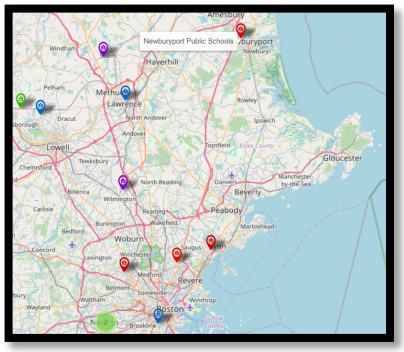
- Are our staff and students savvy, cybersafe users in the building and at home?
- Would our staff or students know a phishing email link if they saw one?

Identification & Action

- How would I know if our district has had a cyberattack?
- As a school leader, what should I do if I suspect a cyberattack?

According to the December 2020, Cyber Threats to K-12 Remote Learning Fact Sheet, "The Cybersecurity and Infrastructure Security Agency (CISA) has seen **an increase in malicious activity with ransomware attacks against K-12** educational institutions. Malicious cyber actors are targeting school computer systems, **slowing access, and rendering the systems inaccessible to basic functions, including remote learning**."

View the K12 Cyber Incident Map online



K-12 Cyber Incident Map

indicates that MA schools continue to be targeted in recent cyberattacks.

IS YOUR DISTRICT CYBER READY?

PLANNING & PREVENTION

PLANNING

ASSOCIATED COSTS

- Basic cybersecurity including firewall, filters, antivirus, and malware protection annually
- Identity and Access Management (e.g. Active Directory), Single Sign-On (SSO), mobile device management (MDM) and endpoint protection
- Continued cybersecurity mitigation costs
- Unexpected cybersecurity costs (cyberattack response and possible data recovery)
- Plan for purchasing network services, communications services and related equipment through the statewide contract ITT72 Category 2 to 9.

ESTABLISH DISTRICT POLICIES

- Engage with your Internet Service Provider to review their cybersecurity protocols
- Review software applications, platform user agreements, and 3rd party software for compliance with data privacy/cyber safety requirements
- Keep a clear and detailed inventory of devices accessing your network
- Provide and enforce secure email and browser settings for users on your network
- Check to see if your district meets the Minimum Baseline of Cybersecurity for Municipalities
- Run frequent and regular backups of your data
- Require educators and students to participate in cybersecurity education annually
- Encourage network users to change passwords regularly

PREVENTION

TEST YOUR TECHNOLOGY WITH MA OFFICE OF MUNICIPAL AND SCHOOL TECHNOLOGY (OMST)

- Request a free Cybersecurity Health Check

USE OTHER AVAILABLE RESOURCES

- Explore CISA's Cyber Essential Toolkits for actionable recommendations
- Request free cyber hygiene services from CISA
- Review the Education Network Security Recommendations Checklist

SOFTWARE and SOFTWARE (PATCH) UPDATES

- Keep antivirus current and run it regularly
- Keep all admin, educator, and student software up to date
  - ✓ For example, Zoom should be checked regularly for necessary updates. Many software updates provide protection from malicious software (malware).
- Use multi-factor authentication (MFA) where possible
  - ✓ MFA is how your online banking requires you to enter a code that is sent to your email or cell phone in addition to having to enter your password.
- Educate the end users of your devices and network
- Use application whitelisting

AWARENESS & EDUCATION

AWARENESS & EDUCATION

INCREASE YOUR AWARENESS

- Read about Cybersecurity News and Events
- Learn more about how schools can defend against cyberthreats by joining the Multi-State Information Sharing and Analysis Center® (MS-ISAC®)
- Check out the K-12 Cybersecurity Resource Center
- Review the CISA Cyber Essentials, which includes information for you, your staff, and your system

EDUCATE STAFF AND STUDENTS

- Conduct annual cybersecurity classes for both staff and students, think about including families as well. Make being a cyber-savvy community a priority!
- Promote a culture of cybersafe behaviors at home and at school by ensuring staff and students know what to do in the event of a cyberattack (e.g. What do I do if we suspect a ransomware attack?)

TRAINING RESOURCES

- Watch a cyberattack unfold
- Cyber.org has posted multiple educational videos like Video Call Safety, Phishing, and Making Strong Passwords.
- Learn about cybersecurity, cyber code, hackers and more at PBS's Nova Labs.
- Play the Cybersecurity Lab game (grades 6-10) – includes an educator guide
- Explore Common Sense Education's Digital Citizenship lessons by grade, like the 6th grade "Don't Feed the Phish" lesson.

IDENTIFICATION & ACTION

IDENTIFICATION & ACTION

WHAT'S THE PROBLEM?

- Identify the symptoms of what has happened for your IT Department.
  - Has the network has slowed to a halt?
  - Is there a student that is locked out of their computer and the message on the screen requests a ransom to allow it to be unlocked?
  - Did a teacher call to mention they clicked on an email attachment they thought was legitimate, but realized too late it was a hoax?

ACTION

STOP! Do not continue clicking. Do not pay a ransom. Power down the infected device.

Immediately contact:

- Your IT Department
- Your Internet Service Provider (ISP)
- Law Enforcement & School Resource Officer (SRO)

Any additional concerns, contact k12edtech@mass.gov.

Please note: DESE is providing this information as a service to educators, schools, and districts and may revise or supplement it from time to time. The publication of this information does not constitute an endorsement or recommendation by DESE of any resource, product, curriculum, or system. DESE welcomes comments, additional information, and suggestions; please contact Jacqulyn.m.gantzer@mass.gov.

updated March 16, 2022