SECURITY ALERT

CYBER ACTORS TARGET K-12 DISTANCE LEARNING EDUCATION TO CAUSE DISRUPTIONS AND STEAL DATA

2020 has brought the whole world online. Teleworking, gatherings with friends and family, and virtual school has become the norm. With more people online, it's important to watch out for cyber attackers in all areas - especially schools doing distance learning.

According to the National Cyber Security Alliance, "K-12 educational institutions are experiencing more disruptions of distance learning efforts by cyber actors via ransomware, malware, video conference disruptions, and distributed denial-of-service attacks."

Malicious cyber actors are expected to continue seeking opportunities to exploit the evolving remote learning environment. Phishing, obtaining personal information and requesting to perform tasks are just some of the ways these attackers are presenting to students, parents, faculty, IT personnel, and other individuals involved in distance learning.

- **Learn more.**
- **Contact okisac@omes.ok.gov for questions and assistance.**

BE AWARE OF THESE ATTACKS AND PREPARE YOUR ORGANIZATIONS BY REMEMBERING TO IMPLEMENT THESE PRACTICES:

- PATCH OPERATING SYSTEMS, SOFTWARE, AND FIRMWARE AS SOON AS MANUFACTURERS RELEASE UPDATES.
- REGULARLY CHANGE PASSWORDS TO NETWORK SYSTEMS AND ACCOUNTS, AND AVOID REUSING PASSWORDS FOR DIFFERENT ACCOUNTS.
- USE MULTIFACTOR AUTHENTICATION WHERE POSSIBLE.
- AUDIT USER ACCOUNTS WITH ADMINISTRATIVE PRIVILEGES AND CONFIGURE ACCESS CONTROLS WITH LEAST PRIVILEGE IN MIND.
- IDENTIFY CRITICAL ASSETS SUCH AS STUDENT DATABASE SERVERS AND DISTANCE LEARNING INFRASTRUCTURE; CREATE BACKUPS OF THESE SYSTEMS AND HOUSE THE BACKUPS OFFLINE FROM THE NETWORK.
- IMPLEMENT NETWORK SEGMENTATION. SENSITIVE DATA SHOULD NOT RESIDE ON THE SAME SERVER AND NETWORK SEGMENT AS THE EMAIL ENVIRONMENT.
- SET ANTIVIRUS AND ANTI-MALWARE SOLUTIONS TO AUTOMATICALLY UPDATE; CONDUCT REGULAR SCANS.

OKLAHOMA
Office of Management & Enterprise Services