

Safer Schools Ohio addresses cyber threats

Last fall, a cybercriminal group known as The Dark Overlord (TDO) targeted dozens of schools, threatening violence and releasing personal information of student and school personnel unless a ransom was paid. Numerous schools were shut down for one to three days while law enforcement investigated. It was determined that the group operates from overseas and that the threats were not credible. Safer Schools Ohio recommends that schools take these steps to help mitigate further threats by TDO:

- ◆ Conduct audits to ensure patches are issued for any vulnerabilities within school computer systems
- ◆ Install and maintain firewalls and antivirus software to help mitigate malware from access to the network
- ◆ Immediately report to local law enforcement any suspicious activity detected on computer networks
- ◆ Never pay a ransom demand – there is no guarantee the information will be returned to its original state
- ◆ Train school staff, students and parents to recognize phishing emails containing malicious documents or links that could download malware that would steal personally identifiable information
- ◆ Ensure that passwords are complex, contain uppercase and lowercase letters, numbers and symbols unique to each site accessed and implement two-factor authentication when possible.

