

Mississippi Department of Education

Office of Technology and Strategic Services

Office of Information Security and Data Privacy

Guidance for Districts and Schools in Information Security and Data Privacy Best Practices

All questions may be directed to the author:

**Virgil John *Henry* Vaughn,** Information Security and Data Privacy Officer
Office of Technology and Strategic Services

**MISSISSIPPI DEPARTMENT OF EDUCATION**
P.O. Box 771 | Jackson, MS | 39205-0771
Tel 601-359-2029 | Fax 601-359-2027
hvaughn@mdek12.org

Information Security and Data Privacy Best Practices

2019

We have seen several Distributed Denial of Service (DDoS) incidents across the state during testing periods. What do we need to do?

Thankfully, the best ways to protect ourselves against DDoS are the same ways we protect ourselves from other types of attacks.

         To stop attacks at the application layer, you need to keep your applications and OS’ up-to-date. Knowing what vulnerabilities are on your network is key to positioning the layers of your layered defenses properly.

o   <https://nvd.nist.gov/>

o   <https://www.us-cert.gov/ncas>

         To stop attacks at the network layer, you need to harden your defenses, implement redundancies, and engage vendors for emergency mitigation response.

o   Make use of blacklisting and whitelisting at the firewall level

o   Drop foreign IPs that are known hostile to the U.S.

o   Employ IPS/IDS or SEIM technology to increase your visibility on your network

o   Segment your networks and segregate the testing traffic

o   Consider a secondary ISP for redundancy

         Ensure your anti-virus and anti-malware systems are up-to-date and properly implemented across your network.

         Restrict the usage of portable media, or at the very least scan it on insertion to workstation.

         Issue credentials on a 1:1 basis

         Educate your users

o   <https://www.dhs.gov/stopthinkconnect>

o   <https://staysafeonline.org/ncsam/about-ncsam/>

o   <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns>

# Bibliography

Arnold, A. (2019, 05 23). *5 Essential Cybersecurity Best Practices To Follow As A Remote Employee*. Retrieved from Forbes: https://www.forbes.com/sites/workday/2019/05/23/how-upskilling-programs-provide-opportunity-and-solve-the-battle-for-top-talent/#2c491ff362d0

Johansen, A. G. (2019). *10 cybersecurity best practices that every employee should know*. Retrieved from Norton: https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

National Institute of Standards and Technology. (2019). *Advanced DDoS Mitigation Techniques*. Retrieved from NIST: https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques

National Institute of Standards and Technology. (2019, 06 27). *Before Connecting an IoT Device, Check Out a New NIST Report for Cybersecurity Advice*. Retrieved from NIST: https://www.nist.gov/news-events/news/2019/06/connecting-iot-device-check-out-new-nist-report-cybersecurity-advice

National Institute of Standards and Technology. (2019, 05 14). *Getting to V1.0 of the NIST Privacy Framework: Workshop #3*. Retrieved from NIST: https://www.nist.gov/news-events/events/2019/07/getting-v10-nist-privacy-framework-workshop-3

Oltsik, J. (2019, 07 08). *Must-have features in a modern network security architecture*. Retrieved from CSO: https://www.csoonline.com/article/3406475/must-have-features-in-a-modern-network-security-architecture.html

University of California Berkeley. (2019). *Top 10 Secure Computing Tips*. Retrieved from Berkeley: https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips