CYBERSECURITY tips for your district

By: Andy Orr, Senior Client Advisor, PSDLAF

Imagine walking into your office on a Monday morning and being locked out of your computer.

You check your bank statement and there are $50,000.00 less dollars in your account.

This has happened, it can happen, and it will happen again.

It is essential to remain diligent of fraudulent attempts on you and your school. This is a daily battle, and unfortunately the criminals only need one opportunity to be successful.

A Federal Bureau of Investigation (FBI) report on March 16, 2021, said, "Since March 2020, the FBI has become aware of PYSA ransomware attacks against US and foreign government entities, educational institutions, private companies, and the healthcare sector by unidentified cyber actors. PYSA typically gains unauthorized access to victim networks by compromising Remote Desktop Protocol (RDP) credentials and/or through phishing emails."[1] According to a K-12 Dive article from March 31, 2021, "a recent report from the K-12 Cybersecurity Resource Centers finds 2020 was a 'record-breaking' year for cyberattacks against U.S. schools, with 408 publicized incidents marking an 18% increase over 2019."[2]

In today's day and age, despite how diligent we all can be, criminals can find a way. Noted below are some tips to help if your identity is ever compromised, or your school is targeted in a ransomware attack.

Identity theft

Immediate recommendation:

- Freeze credit files with Equifax, Experian, Innovis, TransUnion, and the National Consumer Telecommunications and Utilities Exchange for free. Credit freezes prevent someone from applying for and getting approval for a credit account or utility services in their name, immediately.
- Review credit reports to ensure that they do not include accounts that were not authorized. The reports can be ordered for free from AnnualCreditReport.com.
  - » Due to COVID-19 issues, through April 20, 2022, Experian, TransUnion and Equifax are providing all U.S. consumers free weekly credit reports through AnnualCreditReport.com to help protect their financial health.
- If an employee discovers that someone is misusing his or her personal information, he or she can visit the Federal Trade Commission's website to report the identity theft.

The most important action is to create a preventive barrier. PSDLAF strongly recommends utilizing a credit monitoring company. While there is a cost to this service, it is well worth the investment. This article from CNBC provides some reviews and recommendations. Additionally, this article from Experian provides some important tips, including what to do if you believe you are a victim of identity theft.

While individuals can't do anything about the fact that their information may have been compromised, there is a lot that they can do to ensure that they are protecting themselves.

Ransomware
There were 50 documented instances of ransomware targeting public K-12 districts across 25 different states during 2020. The 50 incidents were a 24% increase from than the previous year, and the rate of reported attacks, specifically school districts, has continued to escalate in 2021.[3] As of May 11, there were already 44 reported attacks, almost already reaching the total for all of 2020.[4]

Immediate recommendation:

- Report the incident to your information technology group.
- Isolate the infected system and ensure any other networks are disconnected.
- Turn off all computers that are not yet infected by the ransomware.
- Ensure that all backup data is secure and off the infected network.

For further details on responding to an infection, the U.S. Cybersecurity & Infrastructure Security Agency provides valuable links and information.

Preventing infection:
Ensure that your school's staff is fully trained in preventing ransomware and can effectively identify the phishing emails that carry it. It is always easier to prevent an infection from happening than recover from it.

The U.S. Department of Justice website provides extensive preventive measures as well as details on numerous variants of ransomware. Norton Antivirus covers the main do's and don'ts of ransomware attacks in this article.

You or your school will be the target of a cyberattack – it is unavoidable – but you can ensure that the correct safety measures are put in place. By recognizing the threat and taking the necessary steps to prevent an attack from being successful, you will be better positioned when the time comes.

1. https://nylaf.avenet.net/vertical/Sites/%7B0169A75C-2F7B-4A03-8CC7-F46F662F2FD1%7D/uploads/FBI_Cyber_Division_Report_03.16.21.pdf
2. https://www.k12dive.com/news/2020-was-a-record-year-for-k-12-cybersecurity-incidents/597593/
3. https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf
4. https://www.securitymagazine.com/articles/95164-now-ransomware-is-inundating-public-school-systems

PSBA
Pennsylvania School Boards Association