October 2023

DPO NEWSLETTER

NYSED Data Privacy and Security Updates

Volume 2 Issue 3

October is Cybersecurity Month

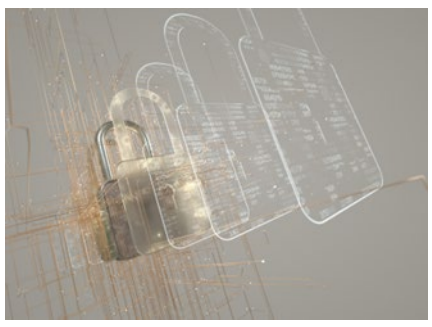
The theme for Cybersecurity Awareness Month this year is "It's easy to stay safe online."

To stay safe online CISA, our Nation's cyber defense agency, suggests that everyone take four simple steps, which are: (1) use strong passwords and a password manager, (2) turn on multi factor authentication, (3) think before you click, and (4) keep your software updated.

Today, we are going to focus on passwords and password managers. Over the years, guidance regarding password length, complexity, and duration has changed many times. The rules for passwords are easy.

- Make them as long as possible.
- Use passphrases, which are a combination of words, numbers, and symbols, that you can easily remember.
- Do not reuse the same password for different websites for applications.
- If you have a difficult time remembering your passwords, consider using a password manager such as Dashline, 1Password, NordPass, Bitwarden, or Keeper.
- **Do not** store your passwords or any other personally identifiable information in your browser. (Yes, we know it is very convenient, but it is also very risky.)

Research your available options and use free trials before deciding which password manager will suit your needs. NYSED does not endorse any of these products.



Cybersecurity Training From CISA

CISA will be holding the 2023 National Summit on K-12 School Safety and Security on November 1-2, 2023. This is a free, virtual event. You can find additional information here and register for the event here.

October 2023 marks the 20th Anniversary of Cybersecurity Awareness Month!

Old Hardware

As with all personal computers, the moment will come when the operating systems for district owned devices such as tablets (Apple or Android) and Chromebooks cannot be updated. This does not mean that the tablet or Chromebook is no longer operational. It means that the device's hardware cannot support the current operating system ("OS"), leaving the device exposed to unknown vulnerabilities that are discovered and patched automatically in the current OS version. Thus, continuing to use older devices introduces additional risk into your environment because threat actors could attempt to access your network and all data contained therein through the vulnerable device.

Wondering when this day will arrive? Keep reading. For Apple products, it could be anywhere between 7 to 9 years from the device's release date. For android tablets, Samsung announced that as of August 2023, its brand of devices will obtain a total of 4 years of automatic updates. And on September 14, 2023, Google announced that all Chromebooks released after 2021 will automatically receive security updates for 10 years, a significant change from their prior policy.

In light of this information, districts need to decide the procedure and timeline for deploying software patches. Best practice is to test a patch before deploying it in production to avoid incompatibility issues or 'bugs' so that it can be resolved before the patch is widely deployed. However, when a patch is developed for a critical zero-day vulnerability, you need to determine how long it will take you to test the patch and if the delay caused by testing is worth the increased risk of a device being compromised, especially when the patch to mitigate the zero-day vulnerability can be automatically updated on the newer devices.

According to the Zero-Day Tracking Project, as of September 19, 2023, 68 'zero-day vulnerabilities' have been discovered in 2023, which is 16 more zero-day vulnerabilities than were discovered in all of 2022. While zero-day vulnerabilities cannot be completely avoided, the potential for a devastating attack can be mitigated by expediently deploying a developed patch designed to defeat the zero-day vulnerability.

A perfect but disappointing example of what can transpire when a patch is not timely implemented to protect and upgrade the operating system occurred on July 29, 2017, when Equifax had delayed deployment of a zero-day vulnerability patch into its production environment. This patch was released by the developer *months* earlier. The delay in patching led to the personally identifiable information of approximately 143 million people being compromised.

Bottom line: Older devices are not being automatically patched and when you do patch, most especially for a zero-day vulnerability, it must be done so expediently!

There is still room in the October 11, 2023, FERPA training being conducted by U.S.D.O.E.'s Privacy Technical Assistance Center (PTAC). You can register by using our form or by emailing privacytraining@nysed.gov