EAST ALLEN COUNTY SCHOOLS

DREAM IT. DO IT.

EACS Technology Newsletter February 19, 2021

1. **For all district teachers who use media tools on projects and assignments: Have you heard of Thinglink?** With Thinglink, students and teachers can create visual learning materials, such as virtual tours, when working on projects and assignments using voice, photo, text, and video. Users can tag images, videos, and 360-degree media with information, audio, embedded videos, and web links. The free version offers interactive image editing, publishing unlimited images, publishing unlimited videos, virtual tour creation, and 1,000 views per year. Download free in the App Store here. (Has free and paid versions.)

2. For all staff: Did you click on the phishing email? During the first week of February, all staff received another phishing email test from me, and the district passed with **flying colors**! 1281 emails were sent out to staff over a 3 day period, and only 17 staff members clicked, which is a click-rate of only 1.5%! According to the phishing company, other districts and companies average a 16.9% click rate, so **EACS rocks!** Great job! There will be at least one more phishing email test this school year…

KnowBe4 Human error. Conquered.

3. For all teachers who use Canvas: Have you heard of the Canvas Betterizer Chrome Extension? Canvas Betterizer will make your time spent in Canvas more efficient by adding improvements, especially in SpeedGrader, such as automatically selecting the student grade, saving and entering comments faster, moving between student grades faster, and removing those pesky tooltips that show up in the gradebook and cover up assignment scores. Canvas Betterizer collects **no information** about you or your students. Thanks to Jessica Faroute for this one. Find Canvas Betterizer in the Chrome Store here.

4. For all Staff: More from the IDOE's Cybersecurity for Education Toolkit: Maintain Strong and Secure Passwords: Creating complex and unique passwords and changing them continuously is a great memory exercise. While using public computers or other public devices and networks, **never allow the public computer to remember or store your password**. This can open the door for others to sign in after you and access your online profiles and any other personal information that might have been saved. *(If you can avoid it, never use a public computer)* Take advantage of **two-factor verification/authentication** when it is available. These systems typically require you to enter both your password and a special code sent to your phone or email. This type of authentication offers the best protection for those of your accounts that hold personal and sensitive information about you.

Indiana DEPARTMENT OF EDUCATION