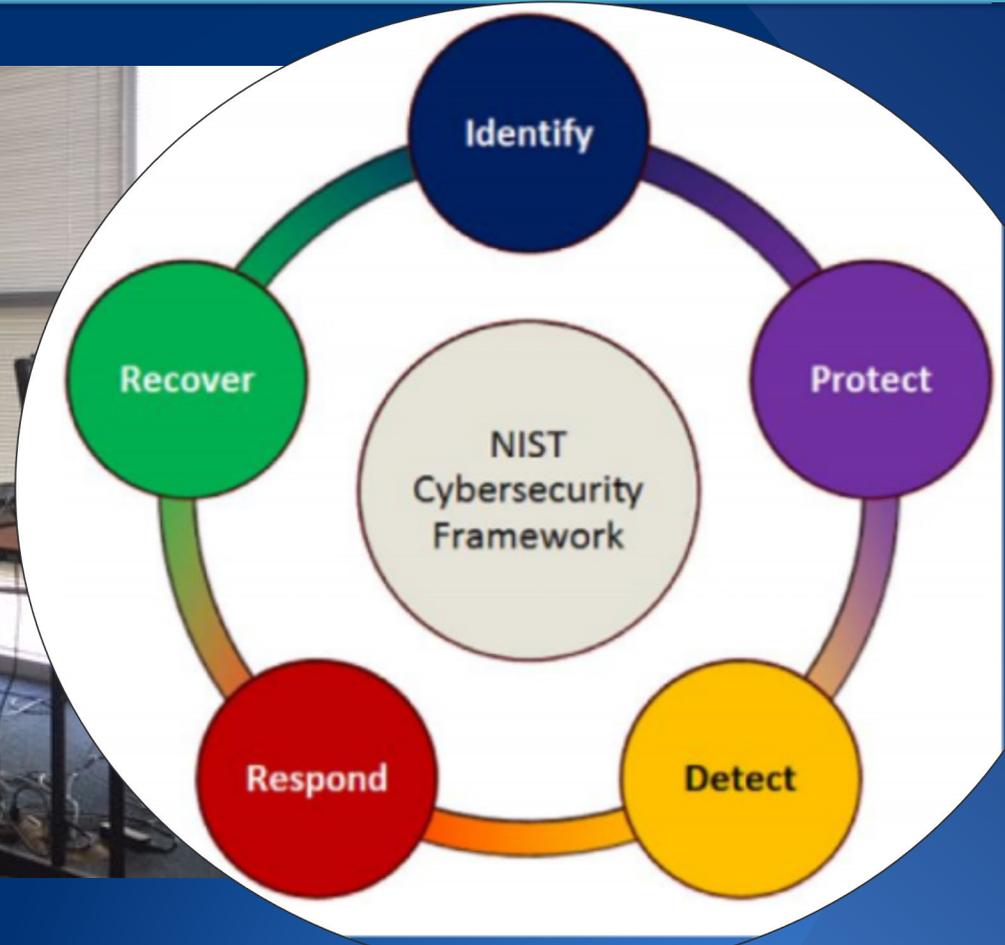
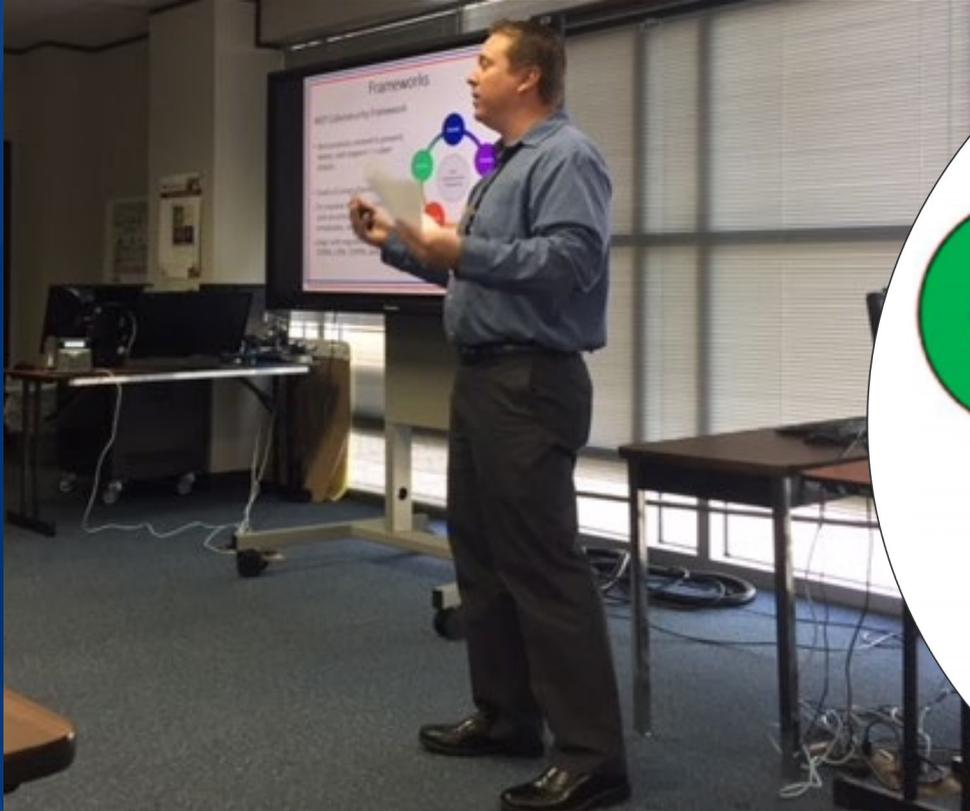


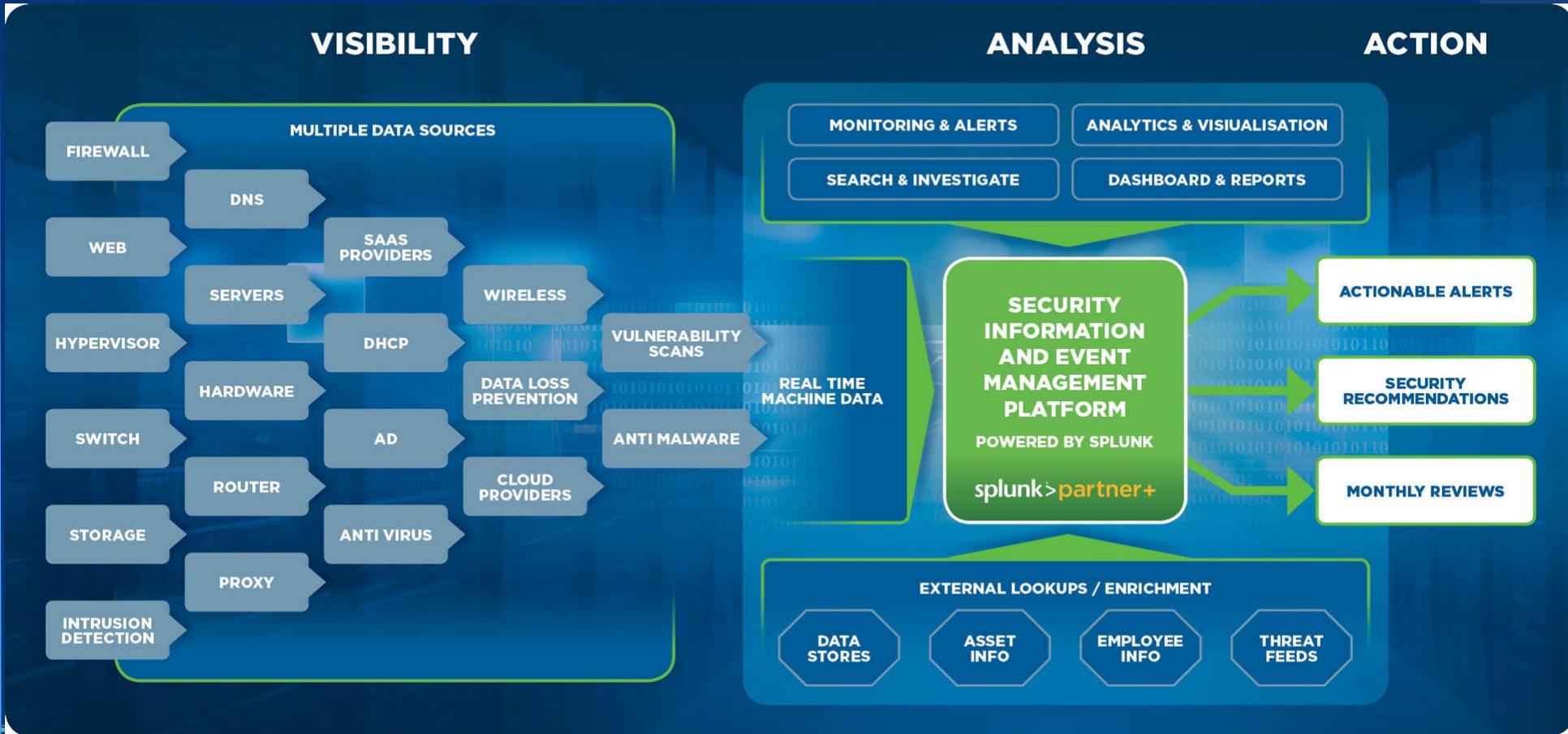
Internet Advisory Committee



On **Tuesday, November 27th**, **James Costello, Jennifer Miller, Eric Pina Greg Rhodes, and Frankie Jackson** spoke to the Internet Advisory Committee, the purpose being to make recommendations, provide feedback, and disseminate information as it relates to the protection, privacy, and security of students, employees, and personal data. The presentation can be found in this [link](#).

SIEM Solutions

This week we met with both LogRhythm and Splunk to discuss what their SIEM solutions could provide for the district. In the field of computer security, security information and event management (SIEM) solution combines security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.



Meeting with Cybersecurity Professionals

This week, **James Costello**, also attended meetings with other districts to discuss the state of cybersecurity, what is working, and what can be done better. The following meetings this week discussed the following items:

InfraGard: Education SIG Meeting

- Nessus Vulnerability Scanning
- BARK for schools

MS-ISAC

- New and ongoing attacks that are being seen in our environment.

TLE Focus Group

- Student Data Privacy



MULTI-STATE

Information Sharing & Analysis Center

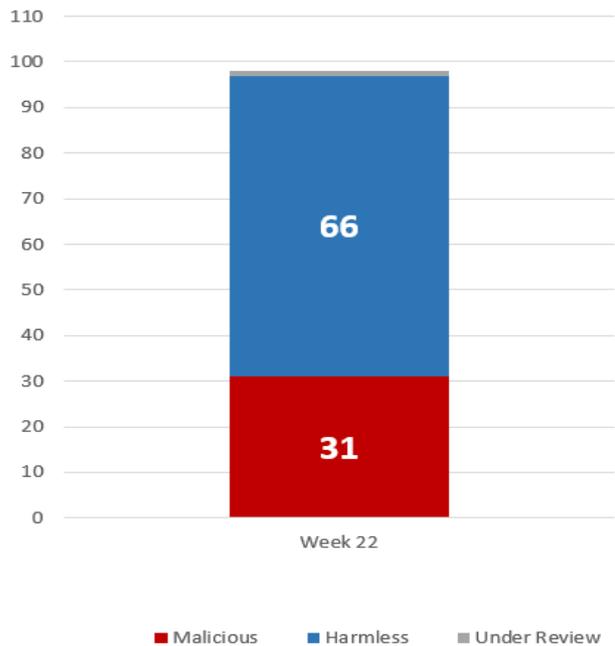


Phish Alert Button Review

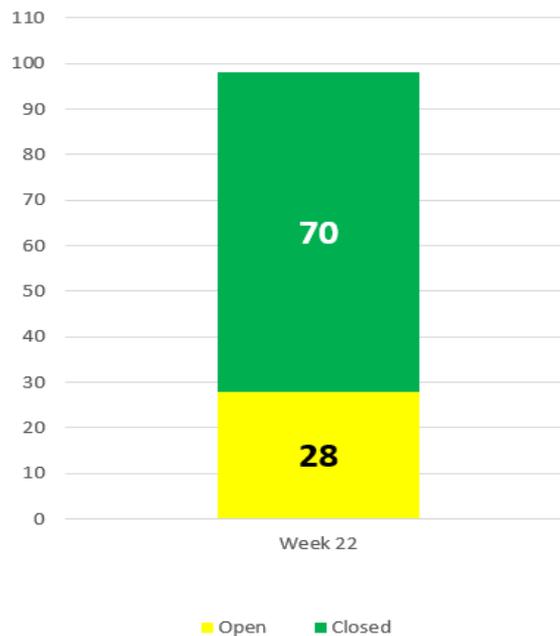
Phish Alert

This week, 98 emails were reported through the PhishAlert button in Outlook. These messages were forwarded for review and removed from the customer's mailbox immediately. James Costello and Eric Pina continued to review these email messages and analyze the threat they posed to the district's network system. A weekly breakdown of the information will be reviewed. This week **67%** of the reports were found to be harmless emails. **71%** of the issues were closed within the week and **60%** were closed within 1 day. Our team is working to review these issues quickly and efficiently.

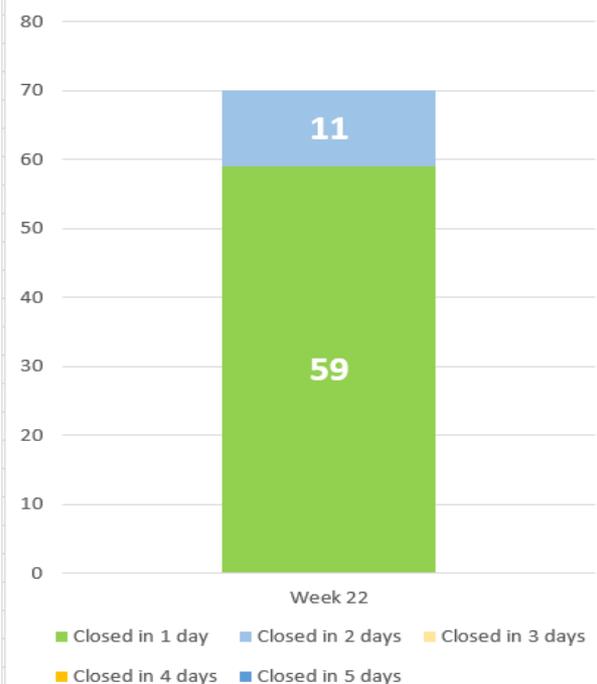
Malicious / Harmless



Open / Closed



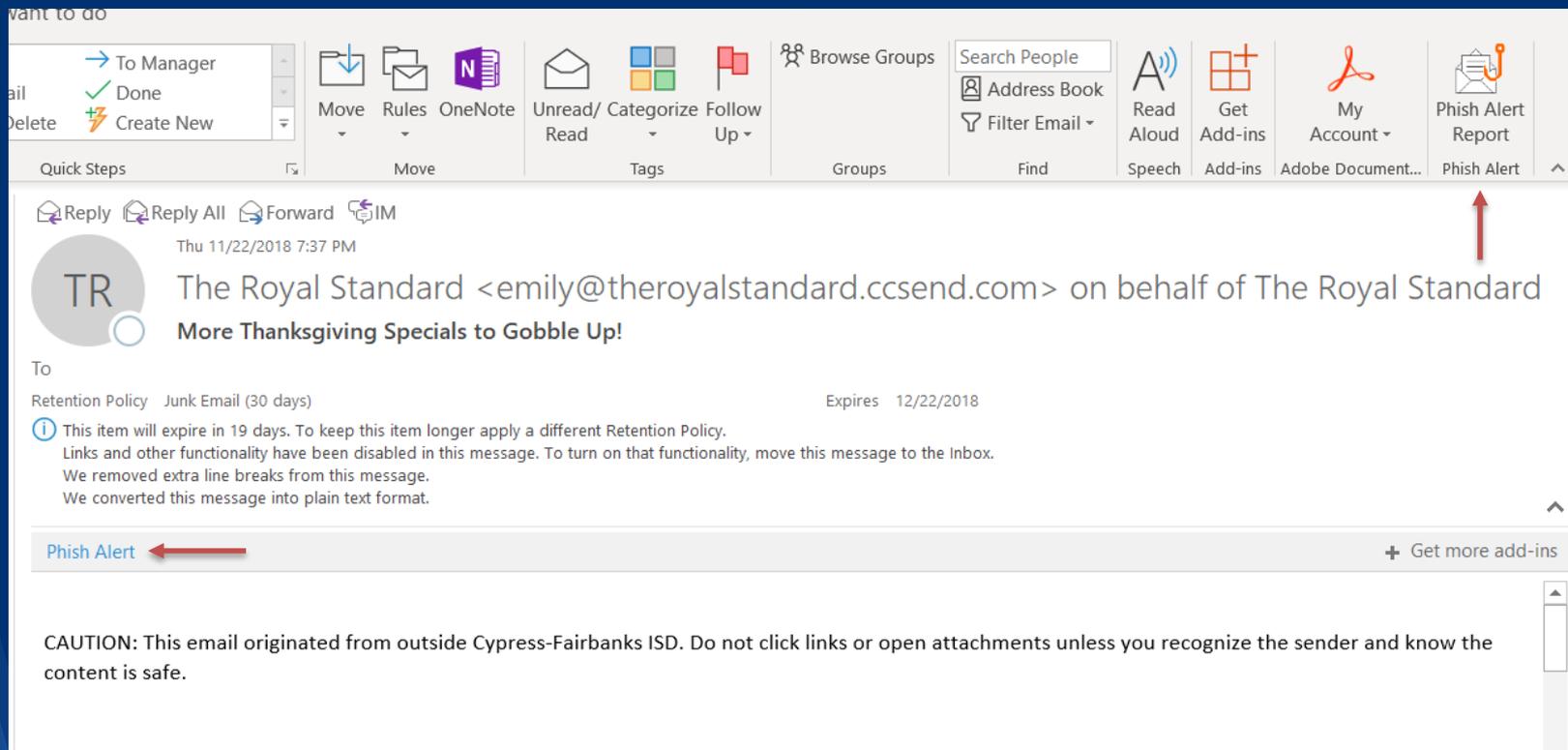
Age of Those Closed This Week





Phish Alert Button v2 Update

This week, CFISD technology services teams made updates to the KnowBe4 Phish Alert Button. These updates allowed the Phish Alert Button to be available on the Outlook Application for smart phones (Android and iOS), and also created an additional PAB report Icon for our users running the latest versions of Microsoft Office. These additional methods are all in an effort to assist our staff in reporting potentially malicious emails attempting to attack our systems.



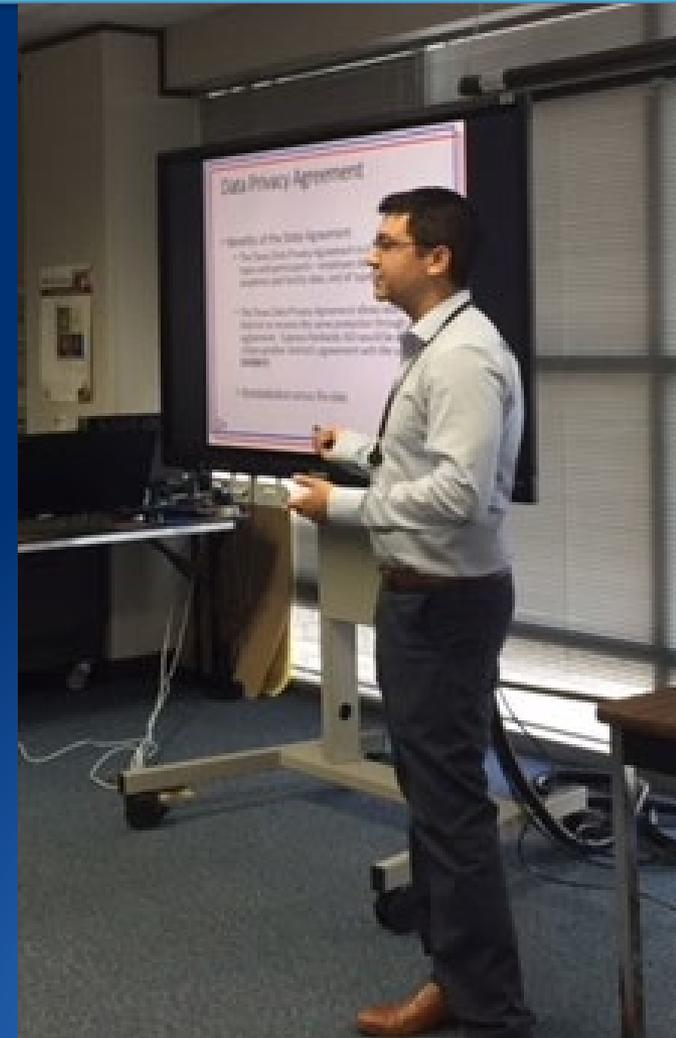


Internet Advisory Committee Meeting

On **Tuesday, 11/27**, CFISD conducted the first Internet Advisory Committee meeting of the 2018-2019 school year. **James Costello, Jennifer Miller, and Eric Pina** from the Cybersecurity Services team presented on the topics of security frameworks, the Trusted Learning Environment, and the Texas Data Privacy Agreement. **Eric Pina** shared with the attendees the benefits CyFair ISD will experience by transitioning to the Texas Data Privacy Agreement.

These benefits include:

- The Texas Data Privacy Agreement includes all data types and participants – employee data, as well as academic and facility data, and all types of documents.
- The Texas Data Privacy Agreement allows additional districts to receive the same protection through one agreement. Cypress-Fairbanks ISD would be able to utilize another district's agreement with the signature in Exhibit E.
- Standardization across the state.



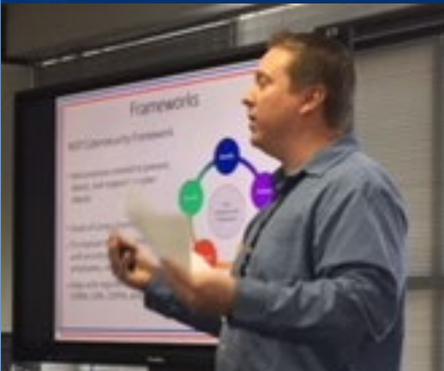


Internet Advisory Committee

On **Tuesday, November 26, 2018**, the Internet Content Advisory Committee met for its inaugural meeting of the 2018-19 school year. **Jennifer Miller, James Costello, Eric Pina, Greg Rhodes, and Frankie Jackson** presented information regarding multiple cybersecurity initiatives. This committee will provide recommendations to the Governance Authority Meeting on December 10, 2018. The purpose of this committee is to make recommendations, provide feedback, and disseminate information as it relates to the protection, privacy, and security of students, employees, and personal data. The membership of this committee is made up of Instructional Technology Representatives, Technology Services Representatives, Curriculum Coordinators/Coaches, Campus Appointee(s), and Librarians.

Today's Agenda

- Committee Development Jennifer Miller
- Security Frameworks James Costello and Jennifer Miller
- Trusted Learning Environment Status Jennifer Miller
- Website Access - Vimeo and Archive.org Greg Rhodes
- Content Filter RFP Greg Rhodes and Paula Ross
- LEARN Network Update Frankie Jackson and Paula Ross
- KnowBe4 Training James Costello
 - 1819 Know Be 4 District Instructions
 - Training series distribution
 - Training series participation
 - Reminder process
- Process implementation Eric Pina
 - Resource Approval or Utilization Process
 - Qualys SSL Server Test
 - Technology Services Responsible Use Policy
- Data Privacy Agreement Eric Pina
- Campus/Department Questions James Costello and Jennifer Miller



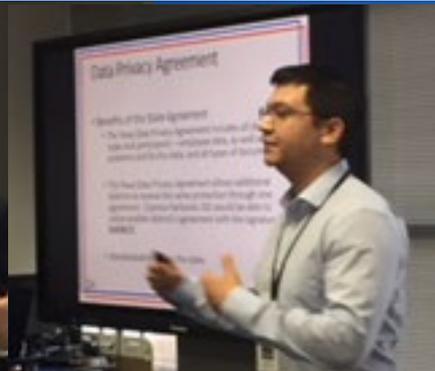
James Costello



Greg Rhodes



Frankie Jackson



Eric Pina



Jennifer Miller



KnowBe4 Updated Applications and Training

Phish Alert Button

On **Wednesday, November 27, 2018**, a new Phish Alert Report Button was implemented. **James Costello**, **Eric Pina**, and **Jennifer Miller** continue to review additional tools that can be utilized to increase our Cybersecurity awareness in the district. This new version of the Phish Alert Report Button was implemented so that employees using the Outlook app on their mobile devices can report malicious emails. Unfortunately, due to the multiple versions of Office 365 versions in use in the district some employees were not able to see the new Phish Alert Report button. **Kimberly Osborn**, NMO team, assisted and over the weekend, Phish Alert Buttons versions 1 and 2 were implemented. This will allow our employees to benefit from the new application, but also ensure all versions are supported.

By the end of the week, 3,769 reports had been made using the Phish Alert Button this semester. This button allows all employees the opportunity to report malicious emails quickly and efficiently.

KnowBe4 Training

Additionally, KnowBe4 Training will continue to be distributed every other Monday to increase the cybersecurity awareness of all employees. To date, over 25,710 sessions have been completed using the KnowBe4 curriculum.





CYPRESS FAIRBANKS
INDEPENDENT SCHOOL DISTRICT
LEARN • EMPOWER • ACHIEVE • DREAM

Updated Phish Alert Button to Report Suspicious Email Messages

Over 3,500 reports have been made using the Phish Alert Button. On Thursday, November 29, 2018, you will notice that the Phish Alert Button has been updated in the Outlook application. The Phish Alert Button is now larger and located in the row of icons at the top of your window.

If you receive a suspicious email, please click the **Phish Alert Report** button. A prompt will appear verifying that you would like to report the email as suspicious. To report the suspicious email, click **Report Phishing**. The email will be removed from your Inbox and sent to our Cybersecurity team for review.

In addition, if you use the Microsoft Outlook application on your mobile phone, you will notice the Phish Alert Button is now available on your mobile device.

Questions and/or concerns may be addressed to the Customer Care Center.



Phish Alert Report
Phish Alert

Phish Alert V2 ×

Report Suspicious Emails

Are you sure you want to report this as a phishing email?

Subject: Just in! This is on our watch list today
From: BrightTALK

Report Phishing

Performance Excellence