SOUTH SAN ANTONIO INDEPENDENT SCHOOL DISTRICT

Agenda Item Summary

Meeting Date: May 25, 2025

Agenda Section: Presentation / Report

Agenda Item Title: Cybersecurity Report

From: Israel De Leon; Director of Technology

Description: Cybersecurity threats can cause major damage to the district. The school district has implemented a cybersecurity annex to the district EOP. Information provided is to educate key personnel in on prevention and to take proactive measures that may harm the district Technology infrastructure.

Recommendation: To provide a safe and secured learning environment.

Funding Budget Code and Amount:

INFORMATION
TECHNOLOGY

Phishing Emails

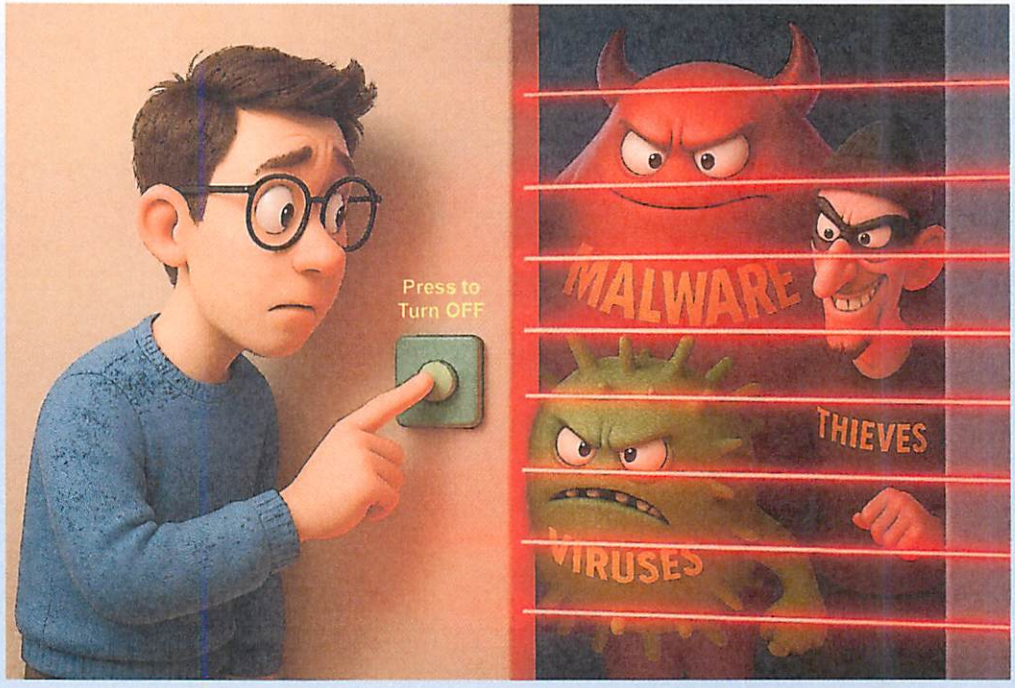
The Basics

Understanding Phishing

- **Phishing Attacks**
  - These emails are designed to trick you into revealing sensitive information (like passwords, credit card details, or social security numbers) or to take a specific action that compromises your security.
- **Malicious Links**
  - Clicking on a link in a phishing email can send you to a fake website that looks legitimate but is designed to steal your login credentials or install malware on your device.
- **Malicious Attachments**
  - Opening an attachment in a phishing email can install viruses, ransomware, or other malware on your computer or phone.
- **Requests for Information**
  - Some phishing emails directly ask you to reply with sensitive personal or financial information.

INFORMATION TECHNOLOGY

It Take Just One Click



INFORMATION TECHNOLOGY

Phishing Email Dangers

- **Think of it like a fake key**
  - These emails try to trick you into giving away your "keys" – your usernames and passwords for important school systems like attendance, grades, or even your email. Once they have those keys, they can sneak into those systems and cause real problems.
- **They can steal student and staff info**
  - Just like a thief might steal personal files, phishing emails can trick you into sharing sensitive information about our students, their families, or our staff. This could be anything from contact details to confidential records, and that's a serious privacy concern.
- **They can break our computers and networks**
  - Sometimes, clicking a bad link in a phishing email is like letting a tiny bad guy into our computers. This "bad guy" could be a virus that messes up files, slows down our systems, or even locks us out completely, disrupting learning and school operations.
- **They can cost the school money and time**
  - Dealing with a successful phishing attack – like fixing hacked accounts or recovering lost data – takes a lot of time and resources. This means less time and money for what really matters: our students' education.
- **They can damage our school's reputation**
  - If our school gets hit by a phishing attack and sensitive information is leaked, it can make parents and the community lose trust in our ability to keep things safe.

INFORMATION TECHNOLOGY

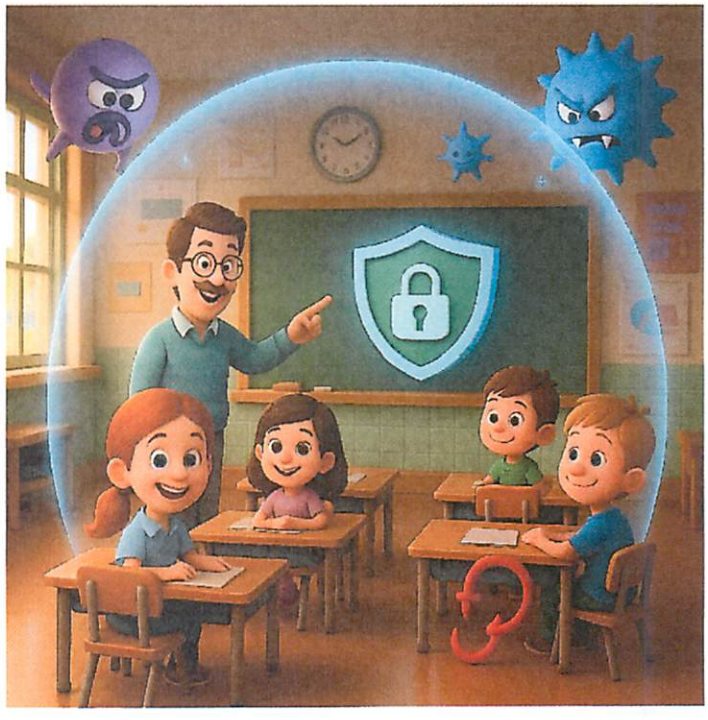
How can you help prevent attacks

- Think Before You Click
- Check the Sender's Email
- Beware of Generic Greetings
- Watch out for Urgent or Threatening Language
- Look out for Typos and Bad Grammar
- Hover over Links to make sure URLs match
- Report Suspicious Emails
  - Better to be safe than sorry

INFORMATION TECHNOLOGY

REMINDER

We are the Frontline Protection For our Student



INFORMATION TECHNOLOGY