CALIFORNIA SCHOOLS
RISK MANAGEMENT

SAFETY MATTERS

RISK MANAGEMENT NEWSLETTER

IN THIS ISSUE **OCTOBER 18 2024**

ENHANCING CYBERSECURITY AWARENESS IN OUR SCHOOL COMMUNITY

OBJECTIVE Managing cyber risks requires building a culture of cyber readiness. Learn about cyber threats and things that can help prevent them.

The importance of cyber readiness is crucial in today's digital age, as a failure to stop an attack can lead to significant financial losses, damage to reputation, and breaches of personal and sensitive information. Recognizing and mitigating these risks through robust cybersecurity measures is essential for protecting individuals, our campuses, and national security.

UNDERSTANDING CYBER THREATS

In our continuously evolving digital world, the safety and security of our online environment are paramount. As part of our commitment to ensuring a secure educational atmosphere, we want to emphasize the importance of cybersecurity awareness within our school community. Understanding how to combat cyber threats, such as phishing, smishing, vishing, and pharming, are crucial steps toward safeguarding our personal information and the school's digital infrastructure.

SAFETY MATTERS
RISK MANAGEMENT NEWSLETTER

CALIFORNIA SCHOOLS RISK MANAGEMENT

Phishing

This is a fraudulent attempt, typically made through email, to steal personal information. Always be wary of emails asking for sensitive information.

Smishing

Similar to phishing, but conducted via SMS (text messaging). Be cautious of text messages that request personal details or direct you to suspicious websites.

Vishing

This method involves phone calls or voicemails from scammers pretending to be from reputable organizations to trick you into sharing personal information.

Pharming

This tactic redirects users from legitimate websites to fraudulent ones to steal sensitive data. Ensure you are visiting the correct website by double-checking the URL (uniform resource locator).

CYBERSECURITY IS EVERYONE'S JOB

The National Initiative for Cybersecurity Education (NICE) working group has a Workforce Management Guidebook, which describes that another common misunderstanding is that organizations need to hire more technical cybersecurity professionals. Without a doubt, these skilled individuals are very important...However, the largest "attack surface" of the organization is the people who perform common functions including the leadership team, finance team, human resources, operations teams, support staff and facilities.

Therefore, cybersecurity is everyone's job. This mindset is a critical component. When we build an awareness at the individual level, we increase the ability to address cyber risks. Mindset will drive appropriate behaviors contributing to the resilient workforce that every organization needs.

HOW TO AVOID BAD ACTORS

The following recommendations are ways to avoid bad actors when using the Internet and any other communication resources:

- Pay attention to the sender and subject of the message every time. If they look suspicious, delete the emails or text message (SMS);
- Do not click the suggested links in an email or message from an unknown sender;
- Never reply to a message requesting personal information;
- Watch for mistakes in the text, if you find them, most likely the letter is a hoax;
- Files attached to an unknown message that have .exe, .msi, .bat, .pif, .com, .vbs, .reg, and .zip extensions can install malicious software, there is no point to open them.
- Do not use unlicensed software, and do not download software on unfamiliar websites;
- Use trustworthy browsers and antiviruses.
- Do not trust every first caller, and always recheck the information.

SAFETY MATTERS
RISK MANAGEMENT NEWSLETTER

CALIFORNIA SCHOOLS RISK MANAGEMENT

SAFEGUARDING OUR DIGITAL PRESENCE

1. Use Strong Passwords

Simple passwords can be guessed. Make passwords random and unique for each account. You can also use multiple word phrases to ensure a longer password.

2. Turn on Multifactor Authentication (MFA)

Use MFA on any site that offers it. MFA provides an extra layer of security in addition to a password when logging into accounts and apps, like a face scan or a code sent by text or email.

3. Understanding Your District Cybersecurity Policy

Familiarize yourself with the school district's policies on cybersecurity. These policies are designed to protect both the students and the school's digital resources and provides guidelines on the proper use of technology.

4. Update Software

When devices, apps or software programs (especially antivirus software) notify us that updates are available, we should install them as soon as possible. Updates close security code bugs.

By fostering an environment of awareness and vigilance, we can work together to build a safer digital community for our students. We encourage parents to discuss these topics with their children and for teachers to integrate cybersecurity awareness into their curriculum where appropriate.

Let us all commit to being proactive in our approach to cybersecurity. Should you have any questions or require further information, please do not hesitate to contact the school's IT department.

Together, we can create a secure and positive digital environment for everyone.

RESOURCES

The Cybersecurity and Infrastructure Security Agency (CISA)

National Cybersecurity Alliance (NCA)

Federal Virtual Training Environment Public

CISA Cybersecurity Training and Exercises

Cyber.org - Empowers K-12 educators to teach cyber confidently, resulting in students with the skills and passion needed to succeed in the cyber workforce.

REMS: Cybersecurity for K-12 Schools and School Districts

This California Schools JPA fact sheet is not intended to be exhaustive. The discussion and best practices suggested herein should not be regarded as legal advice. Readers should pursue legal counsel or contact their insurance providers to gain more exhaustive advice.