TECH TIMES: CYBERSECURITY AWARENESS

GREAT THINGS ARE HAPPENING @WACOISD WITH TECHNOLOGY SERVICES

CYBERSECURITY AWARENESS MONTH

TIPS TO SECURE YOUR VIDEO CONFERENCING WITH STUDENTS:

K-12 school districts are increasingly incorporating distance learning tools as a means of delivering curricula. Advances in information technology as the increased availability of video conferencing software and video conferencing capabilities incorporated into other products have rapidly made distance learning more feasible. However, schools and school districts must balance the convenience, usability, speed, and stability of these platforms with increasing risks to both school IT networks and individual users.

The Cybersecurity Infrastructure Security Agency recommends the following for all users that use video conferencing tools.

1. Only use organization-approved software and tools for school-related work, including school-provided or - approved distance learning and collaboration tools to host/initiate and schedule meetings.
2. Consider sensitivity of data before exposing it (via screen share or upload) to video conference and collaboration platforms. When sharing a screen, ensure only information that needs to be shared is visible; close or minimize all other windows and consider turning off alerts for incoming messages (e.g. emails and direct messages). If displaying content from organizational intranet sites in public meetings, hide the address bar from participants before displaying the content. Use common sense—do not discuss content you would not discuss over regular telephone lines. When having sensitive discussions, use all available security measures (e.g., waiting rooms and strong passwords), ensure all attendees of the meeting are intended participants.
3. When joining meetings initiated by third parties that use collaboration tools not approved by your school, do not attempt to install software—join web (browser) based session instead. Do not use school email addresses to sign up for unauthorized/free tools.
4. Ensure that your visual and audio surroundings are secure and do not reveal any unwanted information (e.g., confirm that whiteboards and other items on the wall are cleared of sensitive or personal information; confirm that roommates or family members are not within earshot of sensitive conversations). If available, make use of background replacement or blurring options in the collaboration tool.
5. Move, mute, or disable virtual assistants and home security cameras to avoid inadvertently recording sensitive information. Do not have sensitive discussions with potential eavesdroppers in your space or in a public area. Consider using headphones.

VIDEO CONFERENCING:
Guidelines to Keep You and Your Students Safe

TIP 1:
ONLY USE SCHOOL / DISTRICT-APPROVED TOOLS

Only use secure software and tools to host video conferences with your students and school community. **Remember:**

1. **Do not host school business via unapproved tools.** Use only tools that have been provided or approved by your school or district.
2. **Carefully review meeting invitations.** Be wary of links sent by unfamiliar addresses.

TIP 2:
SECURE YOUR MEETING FOR ATTENDEES

Take security precautions appropriate for an educational setting. **Remember:**

1. **Only make meetings "public"** when necessary for the planned audience.
2. **Have a plan to terminate a meeting** if needed.
3. **Require a meeting password** and use features such as a waiting room to secure private meetings.
4. **Provide a link to the meeting directly to your students** and share passwords in a separate email.

TIP 3:
SECURE YOUR STUDENT OR SCHOOL'S INFORMATION

Only share data necessary to accomplish the goals of your meeting, consistent with privacy and legal guidance from your school or district. **Remember:**

1. **Manage screensharing, recording, and file sharing options.**
2. **Protect sensitive information** especially when screensharing and displaying school information.

TIP 4:
SECURE YOURSELF AND YOUR STUDENTS

Take precautions to avoid unintentionally revealing information and to ensure your home network is secure. **Remember:**

1. **Don't reveal information unintentionally.** Check your visual and audio surroundings to safeguard personal information.
2. **Consider your surroundings.** Move, mute, or disable virtual assistants and home security cameras.
3. **Check and update your home network.** Change default settings and use complex passwords for your Wi-Fi network.

05/13/2020

For more information, visit cisa.gov/telework and schoolsafety.gov.

GOOGLE MEETING TIPS

SEESAW MEETING TIPS

ZOOM MEETING TIPS

IMPOSTER SCAMS

PASSWORD PROTECTION

OFFER SCAMS

HOW TO SPOT AN IMPOSTER SCAM

3 things you can do to help avoid the deception

Imposter scams use a variety of tricks to gain your trust and steal your money, but they often start with a simple call, email, or message impersonating a person or company you know to trick you into giving them your money.

Here are a few common scenarios to look out for and what you can do to help avoid them:

Family Imposters
"I received a message from a 'family member' asking me for money ASAP..."
Scammers may hack social media accounts to impersonate a relative in need.
How to avoid: Before sending any money, always call your relative to confirm their actual situation.

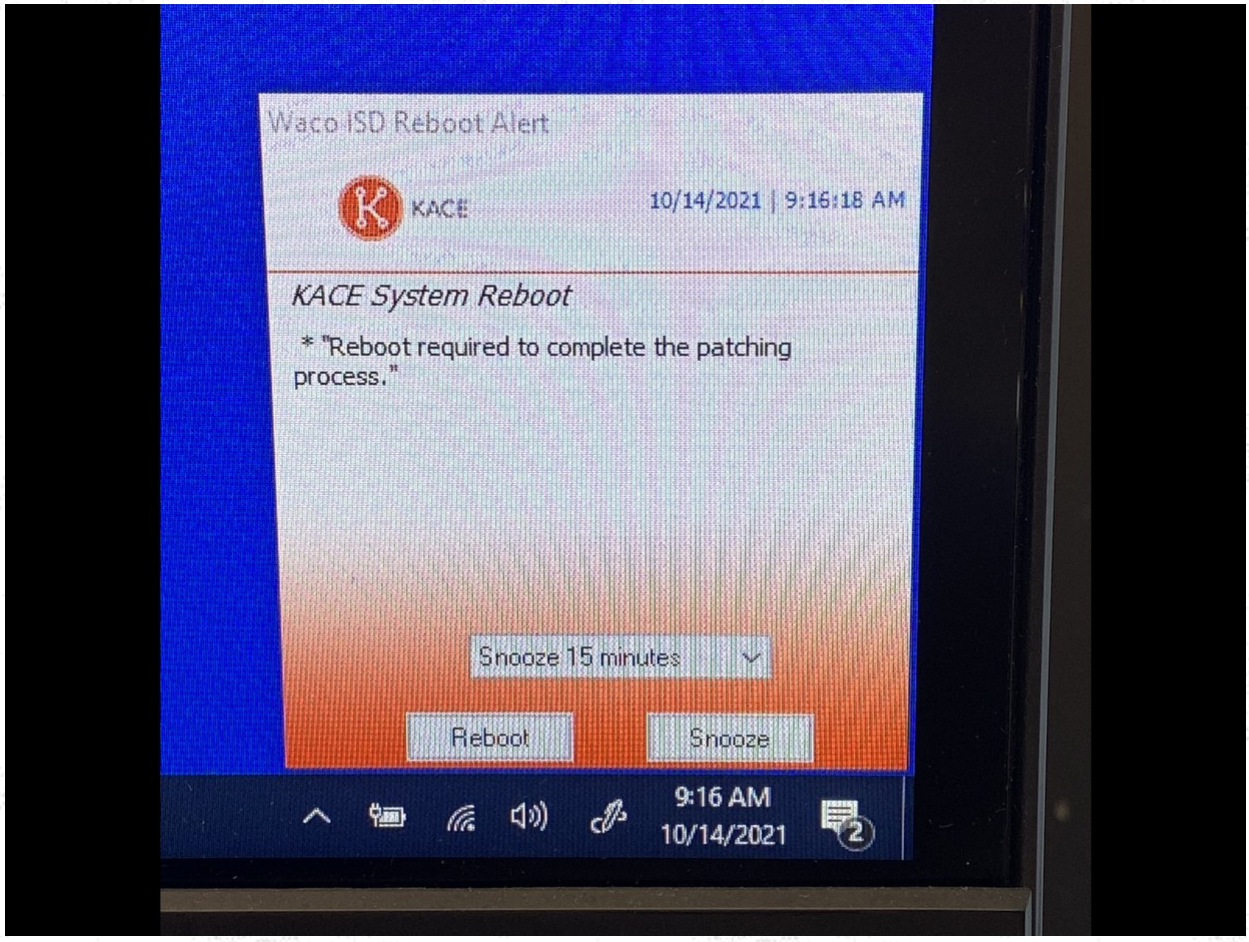
Financial Imposters
"Someone from 'Wells Fargo,' who already knew some of my personal information, asked for my access code..."
Scammers can spoof their caller ID number and use bits of your personal information to convince you to reveal your access code and steal your money.
How to avoid: Don't ever share your temporary access codes or PIN with anyone who calls you unexpectedly. Your bank or the government will never ask you for this information.

Refund Imposters
"I got a call from an online company about a 'refund' for something I don't remember..."
Scammers often impersonate well-known retail and tech support companies to gain access to your personal device or bank account.

How to avoid: Never give control of your device to a stranger. Never send money to anyone claiming to be from companies asking for payment or offering a refund for something you didn't order.

SHOW ME MORE ABOUT IMPOSTER SCAMS

KACE ??? IS THAT SAFE??



Short answer... Yes. KACE is our systems deployment appliance that allows us to monitor your system and keep it updated with the latest drivers and operating systems. This allows you to continue to operate seamlessly in the classroom without the dreaded "blue screen of death" for a computer. Well at least a minimal chance of that occurring. We all know that at any point, for no apparent reason, it can just stop. That is frustrating to say the least, but if we are updating our systems, the likelihood of that happening is lessened.

So when you see a KACE Alert... Please make every attempt to do what it asks. Your technical life will hopefully be better. :) If, your device struggles with updates, please take a deep breath & make sure to contact the helpdesk by clicking the button below...

WACO ISD HELPDESK

Click here to be taken directly to the Helpdesk work order system.

STUDENT TECHNOLOGY SUPPORT

Click here to be taken directly to the Helpdesk work order system.

WACO ISD TECHNOLOGY SERVICES

@jerrynallen_

112 South 6th Street, Waco, T...

helpdesk@wacoisd.org

(254) 755-9599

wacoisd.org