BACK TO SCHOOL... THE 4 CYBERSECURITY TRAININGS YOU MUST DO WITH ALL EMPLOYEES

It's back-to-school season! If your staff has not had a refresher course on your cybersecurity practices sometime in the last year, now is the perfect time to get them up to speed. After all, they can't defend themselves from cyber threats if they don't know how.

Cyberthreats come in all shapes and sizes, but an overwhelming majority of successful cyber-attacks can be attributed to human error. A lack of training can open your school up to hackers and other cyberattacks by way of phishing e-mails, weak passwords, unsafe browsing, and more. In many cases, insurance won't cover your claims if your employees have not undergone regular training.

Finally, no one wants to associate with an organization that isn't keeping their information protected. If you've never trained your team on cybersecurity and are unsure of which topics to cover, don't worry because we've put together a list of the most important topics to discuss.

#1 PASSWORD SECURITY

Nearly every employee has their own login to access network data and applications. When selecting the passwords for this login, employees need to use strong, unique passwords that utilize letters, numbers, punctuation and other special characters and are not shared between accounts. You should also ensure that your employees regularly change their passwords. For an extra layer of security, you can utilize multi-factor authentication.

#2 E-mail

Your employees should be cautious of any e-mails that come from addresses outside of the organization. When your employees go through their e-mail, they should not open e-mails from people they don't know or have not communicated with in the past. Unless they know exactly where the e-mail has come from, they should not open any links or attachments within it.

#3 SOCIAL MEDIA

Personal accounts should never be set up through a school e-mail address. When posting on social media, your employees should be cautious about what they post in regard to work. They shouldn't disclose private information about your school or your students on social media. If they did, it could be devastating to your school's reputation as well as your cybersecurity.

#4 PROTECTING SCHOOL DATA

At the end of the day, your cybersecurity practices are in place to protect student and staff data, and your employees have a legal and regulatory duty to protect sensitive information. A reckless disregard for protecting this information can quickly cause trouble and has the potential to bring forth fines and lawsuits. Establishing strong cybersecurity practices and ensuring your team is aware of them through training is the best way to protect your organization from cyber threats.

By implementing training on these four topics, you'll be on your way to developing a cyber-secure culture.

"Did you try unplugging it and plugging it back in?"

AUGUST 2022 • VOL.5

IKON INSIGHTS

TECHNOLOGY NEWS FOR K-12 SCHOOLS

Brought to you by IKON Business Group, Inc.

IN THIS ISSUE

This monthly publication provided courtesy of IKON Business Group.

IKON is a premium IT consulting company focused on providing K-12 schools with customized technology solutions and personalized support.

Get More Free Tips, Tools and Services on Our Website: www.ikonbusinessgroup.com (212)334.6481

HOW K-12 SCHOOLS CAN QUICKLY ELIMINATE TECH PROBLEMS

Now more than ever, we depend on technology to run our schools and our lives. When the "internet goes down," most schools are at a standstill until they are back online, costing precious learning time.

It's not just the BIG problems but things like file access, password protection, being able to print and recovering files or versions of files that were accidentally overwritten or deleted. All of these are common needs in today's schools.

Every school must have a way to get back up and running quickly should something happen or even ELIMINATE tech problems before they start.

That's why we've created a list to help you determine how ready your K-12 school is for these issues so you can stay focused on learning and not have to worry about these all-too-common occurrences.

Continued on pg. 2

Continued from pg. 1

CHECK OFF ALL THAT APPLY:

- ☐ Does your IT company answer their phone LIVE and respond to emergencies promptly?
- ☐ Is your IT company easy to reach and highly responsive (responding within an hour) when you need them for non-emergencies?
- ☐ Do you know if your IT company proactively monitors, patches and updates your computer network's critical security settings daily? Weekly? At all? How do you know for sure? Hint: Most don't!
- ☐ Does your IT company offer proof that they are backing up ALL your data, laptops and devices?
- ☐ Does your IT company meet with you regularly (at least once a quarter) to report what they've been doing, review projects and offer new ways to improve your network's performance instead of waiting until you have a problem to make recommendations?
- ☐ Does your IT company provide detailed invoices that clearly explain what you are paying for?
- ☐ Does your IT company explain what they are doing and answer your questions in terms that you can understand, NOT in "geek speak" and routinely ask if there's anything else they can help with, no matter how small?
- ☐ Does your IT company proactively discuss cybersecurity with you, make recommendations for protecting your network from ransomware and offer employee training, so they don't fall victim to a scam?
- ☐ Has your IT company provided you complete network documentation, or do they hold the "keys to the kingdom" refusing to give you admin passwords so you're totally helpless if something goes wrong and you can't get a hold of them?
- ☐ Do techs arrive on time and dress professionally, and do you look forward to working with them, or do you cringe every time you have to make that call?

If your current IT company or technician does NOT check the boxes on every point, you could be paying for substandard support. This could jeopardize your data and your network's security and cost you countless hours in lost productivity and instruction time because you and your staff are spending time dealing with problems that shouldn't exist. If that's the case, then it's time you see what else is out there and make sure you're getting what you pay for.

To schedule a free 10-minute discovery call to see how we can get rid of your tech issues, visit bit.ly/meetwithikon.

IT SECURITY TIP: WHY YOU MIGHT WANT TO COVER UP YOUR WEBCAM

Here's a disturbing, but very real, tactic for hackers: spying on you via your device's camera. Some simply watch you for fun. Others attempt to catch incriminating photos and then blackmail you by threatening to release the photos or video (which they have) to all your Facebook friends, LinkedIn connections or e-mail address book (which they also have) unless you pay a ransom. If you pay, they can come back and ask for MORE because they now know you care AND that you'll pay.

As always, follow the various security strategies we've been sending you via these newsletters. As a backup, you can buy stickers that cover your camera with a slider so you can uncover it when you want to actually use it to take a picture or join a web meeting. These are really inexpensive and can be found on Amazon for under $10. Just search for "webcam cover slider."

Have questions about cybersecurity or the technology at your school? We're here to help.

FREE ON-DEMAND WEBINAR:

HOW TO CREATE A TECHNOLOGY PLAN FOR K-12 SCHOOLS

Technology planning for schools can often be a difficult, drawn-out, and confusing process... but that shouldn't be the case!

Rather than implementing technology in an ad-hoc manner - and risk wasting valuable time and resources - it's important for school leaders and their IT staff to perform their proper due diligence in putting a technology plan in place ahead of time.

In this webinar, we'll discuss the keys to creating a successful technology plan, including:

1. Identifying the key stakeholders that should be a part of your technology planning committee
2. Outlining your school's vision, priorities and student learning goals and identifying the technology solutions that can help you achieve them
3. Evaluating your current technology environment, taking inventory of the current hardware and software systems in place, and identifying any potential issues and areas for improvement
4. Understanding and defending against cybersecurity risks
5. Maintaining adherence to compliance mandates, such as CIPA, FERPA and ADA
6. Creating a budget and timeline for implementing technology and identifying potential funding sources
7. Finding the right technology vendors that align with your needs and budget

Scan to Watch

Get your copy today at: https://www.ikonbusinessgroup.com/7voipquestions/