AUDIO ENHANCEMENT®

Cybersecurity Tips from Audio Enhancement

In this day and age, technology is everywhere, including the classroom. It makes our lives and jobs easier, and allows for new ways for teachers to teach and students to learn. Audio Enhancement's products are dedicated to making classrooms more effective, through Classroom Audio Systems, VIEWpath (Video Interactive Education Window), SAFE (Signal Alert for Education) System, and EPIC (Education Paging and Intercom Communications) System. However, it is imperative for all users to be cautious while using any technology, especially online. Here are some important cybersecurity tips to maximize online safety for your school.

1. **Use a strong password.** The main reason systems get hacked is because of weak or default passwords. Change default passwords immediately and create a strong password, consisting of at least eight characters and a combination of upper and lowercase letters, numbers, and special characters.
2. **Change your password regularly and keep it private.** Update your password periodically to avoid hackers. Don't use the same password for multiple sites or devices, and don't share it with anyone.
3. **Update firmware.** When security updates are available, update firmware to ensure the system is secure.
4. **Change default settings.** There are two ports used to communicate and to view video feeds remotely (HTTP and TCP ports). These ports can be changed to any set of numbers between 1025-65535. Change the default ports to prevent outsiders from guessing which ports you are using.
5. **Disable auto-login on SmartPSS.** If you are using a computer that is used by multiple people, disable auto-login on SmartPSS. This prevents the wrong people from logging in with your credentials.
6. **Check the system log regularly.** Monitor your account regularly for suspicious activity. Check the system log, which will show you which IP addresses were used to log in to the system and what was accessed.
7. **Keep devices out of reach of unauthorized people.** Install devices in a lockbox, a locking server rack, or in a room to prevent unauthorized physical access to your system. Never leave a device unattended by unauthorized people. If you have to leave the room for whatever reason, make sure to log out of the system.
8. **Isolate NVR and IP camera network.** Make sure to use different networks for your NVR and IP cameras, and your public computer network. This prevents any outsiders from getting access to the security system network.
9. **Enable HTTPS/SSL (secure browsing).** Setting up an SSL certificate to enable HTTPS (secure browsing) will encrypt all communications between your devices and recorder.
10. **Remember it can happen to anyone.** Everyone is a target for hackers, and being educated in cybersecurity can go a long way to protect your school. It is the responsibility of each user of technology to practice cybersecurity.