vwbrown
Insurance Service

10 STEPS TO PREVENTING DATA BREACHES AT YOUR SCHOOL

1. OUTSOURCE PAYMENT PROCESSING. Avoid handling credit card data on your own. Reputable vendors, whether it's for Point-of-Sale or web payments, have dedicated security staff that can protect the data better than you can.
2. SEPARATE SOCIAL MEDIA FROM FINANCIAL ACTIVITY. Use a dedicated device for online banking. Use a different device for e-mails and social media.
3. THINK BEYOND PASSWORDS. Never reuse passwords and don't trust any website to store them securely. You can never tell when a website has already been hacked and your password has been exposed. Set up a two-factor authentication; this sends a secret code to your phone verifying your identity.
4. EDUCATE AND TRAIN EMPLOYEES. Establish a written policy about data security and communicate it to all employees. Educate employees about what types of information are sensitive or confidential and what their responsibilities are to protect that data. Also, most scams and malicious attacks arrive through e-mail, so be sure your team is prepared and alerts others when they are received.
5. STAY INFORMED. Evaluate the entire chain of events in a potential attack. From assessing your e-mail infrastructure to your user's responsiveness to your browser's vulnerability, identify where your organization is most at risk. Then, question the security posture of your business lines, vendors, suppliers, or partners.
6. STOP TRANSMISSION OF DATA THAT IS NOT ENCRYPTED. Mandate encryption of all data. This includes data at "rest" and "in motion". Also consider encrypting e-mails within your company when personal information is transmitted. Avoid using Wi-Fi networks as they may permit interception of data.
7. SECURE YOUR BROWSER. With the growing popularity of watering holes – malicious code installed or trusted websites – how do you know which websites you can trust? Forget individual patches. Focus on keeping up-to-date with the latest version of your browser. Then, test your browser's configuration for weakness.
8. SECURE YOUR OPERATING SYSTEM. It's far easier to break into older operating systems like Windows XP. Take advantage of major security improvements baked into newer operation systems.
9. SECURE YOUR ROUTER. It connects your computer to the Internet. Make sure someone can't interrupt all the data sent through it. It's important to see a strong admin password on your router and a WPA2 password on your WiFi.
10. SECURE YOUR DATA. Whether you lose data to an accident or an attack, you'll always be glad to have a backup. Ideally, your backups should be encrypted and off-site in case there's a fire, burglary, or other problem that could destroy your backup.