IT & Data Security Training and Awareness Best Practices

The below information was shared at two March webinars titled "FERPA: District Policies and Staff Access." It comes directly from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC).

Information System Users are the First Line of Defense

Hackers and data thieves are hard at work and are constantly changing their tactics and methods. Combined with the already lightning fast evolution of technology and the constant parade of security vulnerabilities, software patches and updates, an organization can quickly become lost in a sea of change. It's hard for your dedicated data security people to keep up with the changes, let alone your non-IT employees. That is why having a well-developed IT & Data Security training and awareness program is so critical. The users are the first line of defense against the majority of cyber-attacks.

Best Practices for IT & Data Security Training

IT & Data Security training does no good if users choose not to take it or if the concepts and information are not updated and repeated regularly enough. Generally, organizations require mandatory course completion as part of the onboarding process prior to account authorization and on a recurring annual basis thereafter. This ensures that the user base is informed about organizational security policies, their responsibilities to protect data and good security practices, as well as possessing an understanding of the various threats that an organization's information systems and data face. Below are some key points that we recommend as foundational to a good IT & Data Security training program:

- *The training should highlight the importance of protecting information and information systems from unauthorized use*
- *Explain the basics of Information Security: Information Security is the collection of policies, procedures and security controls that are put in place to quantify and manage risk to data*
- *Define important concepts like Confidentiality, data Integrity and Availability, what is a threat versus vulnerabilities, and pertinent statistics on current data security trends*
- *It should touch on regulatory requirements / regulations (FERPA, COPPA & other Federal and state laws) that directly affect information security controls / procedures*
- *Provide information for users on best practices (for example):*
    - ***Organizational password policy** – requirements and advice on choosing strong passwords*
    - ***Media control** – not putting confidential or sensitive data on removable media unencrypted*

    - ***Email security*** *– double checking addressees, avoiding putting sensitive information in the body of emails but rather in an encrypted attachment*
    - ***Avoiding common attack vectors*** *– Good browsing habits, avoiding unsolicited emails & attachments, careful use of wireless, combatting social engineering*
    - ***Physical security*** *– policing work areas for sensitive info, shredding un-needed paper copies, being wary of shoulder surfing and tailgating in sensitive areas*
- *Review the organization's* ***Acceptable Use Policy*** *that explains how organizational information system resources can be used (use of email, apps, personal use, conduct, etc.) and details the ramifications of failure to comply*
- *Explain the user's expectations for privacy on organizational data systems, establish that monitoring is occurring on the system and that use of the system constitutes consent to monitoring as defined by the organization's security policy*
- *Provide users with and overview of incident reporting policy & procedures that detail what to do if they believe a security incident has occurred, who to call, what to expect and what information to provide to responsible parties*

Security is everyone's responsibility. A trained and engaged user base is the best "bang for the buck" in IT & Data Security today. By building a robust, engaging and informative annual IT & Data Security training program including the recommendations in this document. An organization can greatly reduce the risk to its information systems and data, and is far more likely to more quickly recognize, identify and mitigate security vulnerabilities and incidents.

If you have questions on privacy or data security or for more information on the recommendations above, visit the PTAC website at http://ptac.ed.gov.