Great Ways to Observe Data Privacy Month in 2023

1. Change your IU passphrase annually and keep it confidential!
   Having a unique IU passphrase that is not used for any other service or website helps protect IU. Please make sure to change your passphrase **before January 31**. To change your passphrase go to https://access.iu.edu/Passphrase, or go to One.iu.edu and search for "passphrase reset."

2. Review your employee FERPA responsibilities here: https://ferpa.iu.edu/responsibilities/index.html. Remember, casual access of student data for personal reasons or just out of curiosity is a violation. There is auditing of "high profile" records and accessing those records without legitimate educational need, can result in termination of access or employment.

3. Practice good habits regarding data retention and disposal of restricted and critical data securely:
   Clean up your email: Save only those emails you really need and unsubscribe to email list-serves you no longer need/want to receive.
   File upkeep: Delete or archive older files such as numerous drafts of the same document and outdated financial statements.
   Dispose of electronics securely: Wiping data isn't enough. When you dispose of old electronics, look for facilities that shred hard drives, disks and memory cards…
   Empty your trash or recycle bin on all devices: Make sure to permanently delete old files.

4. Stay on alert for phishing scams:
   Always verify the sender before opening attachments or links embedded in an email. For more information: https://protect.iu.edu/online-safety/personal-preparedness/email-phishing.html

5. Stay secure online. Personal Identifiable Information (PII) must be protected.
   - **Passcode Protect Devices accessing IU data:** All mobile devices must be passcode protected and meet the standards outlined in IT- 12.1.
   - **Delete apps when done:** Some applications are installed on mobile devices for specific purposes like conferences or tours that collect personal information. It's good practice to delete all apps when no longer in use and be careful what information you agree to provide.
   - **Disable Wifi and Bluetooth** on mobile devices when not in use to avoid tracking by stores and other services.
   - **Use a VPN:** Public wireless networks and hotspots are not secure. Use a virtual private network (VPN) or a personal/mobile hotspot for a more secure connection. For more information see: VPN at IU
   - **Use Secure Share for critical data to share sensitive information:** https://secureshare.iu.edu/**.** Do not send large datasets with student information through email (>100 students).