Cyber Security Awareness Month - 10/18/2012 Board Meeting

Cyber Security at the County

- **IT Security Team**
  24x7 support for all county systems
  Cyber security incident handlers on staff
  Integration with Sheriff's Office and District Attorneys office
  Ongoing training efforts
  - keep up with emerging threats
  - early recognition of cyber security issues

- **Protection of county data**
  Data about citizens and their interactions with county services
  Includes library patrons, dog owners, registered offenders, and health clinic patients
  Control set includes:
  - intrusion detection and prevention
  - identity management technology
  - anti-virus and anti-malware
  - regular software updates
  - regular backups
  - other best practices supporting protection of data

- **Relationships with federal, state, and local authorities**
  Investigations
  Response capabilities

- **Recent developments**
  Cloud-based security services monitoring our networks and computer systems
  Intrusion detection
  Identity protection

- **Ongoing development**
  Cyber security is an iterative activity
  Awareness Program
  Privacy Officials group
  Security Synchronization group
  Online training
  Periodic security tips in the Wednesday Wire
  Material from the MS-ISAC

Cyber Security TIPS:

1. Use unique passwords for unique accounts. Your email account password should be different than your Amazon shopping account and also different from the one you use to login to your bank.
   It's a lot like having a single key that fits your car, house, work, and a safe in your house. If someone is able to copy that one key they can access everything that shares that key.

2. Do not respond to an email that asks for personal information or that asks you to "verify your information" or to "confirm your user-id and password".
   Legitimate organizations rarely use email to solicit your personal information.

3. Kid safety - place your home computer in a common area of the house.
   Encourage your kids to ask questions and let you know if they see anything that makes them feel uncomfortable.

4. Keep your computer and your programs up to date.
   The older a program gets, the more opportunities hackers have to find the security holes in it.

5. Make sure you have anti-virus/anti-spyware that it is current and is set to scan regularly.
   Most antivirus software will do this for you automatically when installed correctly.

6. Backup your files.
   If your computer fails, and eventually it will, you will want backups of your files.

7. Do not click on links in emails. You can fall victim to a phishing attack that puts your financial accounts, personal information, and computer into the hands of a hacker.
   If a message says it's from your bank, go directly to your bank's website and avoid the links in the message. It is best to call your bank if you are unsure about the message.

8. Most importantly "Trust your gut." If something doesn't quite feel right, it probably isn't.