CITY OF BRYAN
The Good Life, Texas Style.™

EDUCATING FOR A CAREER IN CYBERSECURITY

CHAMPION
National Cybersecurity Awareness Month

This week's topic is "Educating for a Career in Cybersecurity" – according to Forbes magazine, there will be 3.5 million unfilled positions. This is up from a study by the Center for Cyber Safety and Education that there will be a shortage of 1.8 million information security workers in 2022.

1. **What does a cybersecurity expert really do?** Cybersecurity analysts help prevent attacks through their expertise and knowledge of databases, networks, hardware, firewalls and encryption. Cybersecurity analysts may also regulate access to computer files, develop firewalls, perform risk assessments and test data processing systems to verify security measures.
2. **How long does it take to become a security engineer?** The job of a Security Engineer is a highly technical one, so employers will likely expect you to have a bachelor's degree in Computer Science, Cyber Security or a related field.
3. **Security Engineers like to fix systems and Security Analysts like to break them.** Analysts are more concerned with probing for risks and weaknesses (pen testing, auditing, etc.); engineers are more intent on building robust security solutions (firewalls, IDS, etc.).
4. **Can I make a living at being a cybersecurity expert?** According to Salary.com, the median salary for a Cyber Security expert is $125,101 (2017 figures). Overall, you can expect to take home a total compensation of $112,000 – $145,000 with 10 years of experience. This includes a base annual salary, bonuses, profit sharing, tips, commissions, overtime pay and other forms of cash earnings, as applicable.

To interest YOUR kids in a career path in the "cyber aware" world, start by grooming them to be more socially self-aware. Google developed a neat tool called Interland. The included links are vetted and will take you to the Interland game.

SHARE WITH CARE

Teachers and parents understand how early digital mistakes can do lasting damage to one's reputation. But it can be harder to convince preteens that a seemingly harmless post today could in the future be misunderstood by unintended audiences. These activities use concrete examples to teach children how to maintain a positive online reputation by managing their privacy and protecting their personal information.

DON'T FALL FOR FAKE

It is important for kids to understand that the content they find online isn't necessarily true or reliable, and sometimes may involve malicious efforts to steal their information. Phishing and other online scams encourage Internet users of all ages to respond to mysterious pitches from people they don't know, or from people pretending to be someone they do know.

SECURE YOUR SECRETS

Online privacy and security issues don't always have clear right and wrong solutions. Protecting your personal and private information—all the stuff that makes you you—means asking the right questions and finding your own educated answers.

IT'S COOL TO BE KIND

The digital world creates interesting challenges for kids. Social cues can be harder to read online, anonymity can encourage negative behavior, and online bullying is easily repeated and leaves a digital footprint. But, the Internet can amplify kindness. Learning to convey kindness and empathy—and how to respond to negativity and harassment—is essential for building healthy relationships and reducing feelings of isolation that can sometimes lead to bullying, depression, academic struggles, and other problems. Research shows that rather than simply telling kids not to be negative online, effective safety education addresses the underlying causes of negative behaviors. These activities encourage children to interact positively from the start and teach them how to deal with negativity if it happens.

WHEN IN DOUBT, TALK IT OUT

One piece of advice that appears consistently throughout these lessons applies to any online activity. If a child comes across something questionable, they should be taught to talk to a trusted adult about it. Below is a list of situations in which the "when in doubt, talk it out" principle might be most useful:

- **They suspect that their account may have been compromised.** (Discussion opportunity: What can you do to make your account security even stronger?)
- **They need help from a trusted adult remembering a password.** They are unsure whether something is a scam, or suspect they might have fallen for one.
- **What are the warning signs?**
  - Someone tries to discuss something online with them that makes them uncomfortable.
  - They receive suspicious contact from a stranger.
  - They want to discuss online acts of kindness and unkindness.
  - They are concerned that they may have shared something online that they should not have.
  - Foster open communication in your home and remind children that you're always there for backup.

Additional Resource: *Be Internet Awesome: Google's Digital Citizenship Safety Curriculum*