Summer School

School’s out for summer! Well, for the kids anyway. That means it’s time to plan camps, vacations and creative ways to make sure your kids don’t sit in front of a screen for the next three months... We are all guilty of a little too much (or a lot of) eyeball-numbing, brain-sucking, internet-surfing time. But as the deep dark place of the internet becomes an even deeper darker place, this summer is a good time to sit down with your kids and refresh ways to stay safe online.

There is a breadth of fun and educational resources that will help educate your young digital citizen.

- The FBI Cyber Surf Islands transports adventurers to enchanting digital islands to learn more about protecting their information. This game is designed for grades 3-8, includes multiple lessons and final quiz at the end of each grade level.
- The Federal Trade Commission Friend Finder is a great tool for those all-too-eager youth making their way onto social media. This game provides examples of just how manipulating bad actors can be and how to spot the thieves, bullies and creeps.
- NSteens.org, a website sponsored by NetSmartz Workshop, National Center for Missing & Exploited Children, and Sprint, features games, comics and videos for preteens and teens. Users can explore topics such as cyberbullying, gaming and posting etiquette.

Summer is not only a good time to get your kids in-line for online, but it is also a good time to review what you can do as a parent.

- Support their decisions and turn mistakes into teachable moments
- Know the privacy settings and protection features of the websites they frequent
- Teach them how to tell what a safe website looks like, and to be extra cautious when downloading, clicking and posting online
- Keep the family computer in an open environment so you can monitor their activity
- Have rules that ensure they are not spending too much time online and are, most-importantly, safe
- Encourage them to be leaders online, report when they see something is not right, and lead their friends by example

See the complete list for parenting tips.
InfoSec Academy Update

Thank you to all of you who participated in the Texas InfoSec Academy. The contract expired April 27. DIR is in the process of evaluating responses to the DIR Academy RFO. DIR Academy will expand training opportunities beyond security education to other areas including the state data portal. We hope to have a contract in place in a few months. We will keep you informed. If you have access to the Texas InfoSec Academy OLA Libraries, you can continue to access them until June 30, 2017. If you have any questions, please send an email to: infosecacademy@dir.texas.gov.

Gartner Webinars

The next webinar, “IAM as a Service (IDaaS) Is Ready for Your Organization: Are You Ready for It?”, will be held Tuesday, June 20 from 1 pm – 2 pm CST.

Discussion Topics:

- The forces driving and inhibiting IDaaS adoption
- How the market is evolving, and which vendors are delivering IDaaS
- How organizations that are moving forward with IDaaS should prepare

IDaaS as an IAM delivery method has been gaining in popularity, and more providers are entering the market. The functionality and time-to-value offered has been steadily improving. But is IDaaS right for your organization? This webinar provides the information you need to make an informed decision for your organization and understand the market offerings.

This webinar will be hosted by Gregg Kreizman, Research VP

To register for this webinar, please visit the link below and click on the green "Attend" button and complete the required fields. You will receive a confirmation email with a calendar invitation containing a link to attend the session. You will also be able to download the presentation on the day of the webinar.

https://www.gartner.com/webinar/3718818

If you have any issues registering for or attending the session, please email Joe Martin at Gartner (joe.martin@gartner.com) or Robin Goad at Gartner (robin.goad@gartner.com).

WannaCry Lessons

On May 12, 2017, tech blogs and IS news feeds ignited with the news of a new ransomware attack that was spreading like wildfire through both private- and public-sector networks. Agencies like the British National Health Service (NHS) and Telefonia, Spain’s largest telecommunications provider, were affected. Even private companies like Fedex felt the toll of this malicious software. In the first few hours alone, somewhere between 230,000 to 390,000 computers in more than 150 countries were infected with this newly-discovered ransomware. Its name was WannaCry (WNCRY/WannaCrypt).

This bad business taught us all some hard lessons.

1) **Patch.... PATCH!!** Everyone always says it but clearly not everyone did it. This ransomware successfully attacked so many systems due to unsupported or unpatched operating systems. Like I said, PATCH!

2) **Forgetfulness is no excuse.** Systems left in the past often mean unmonitored access points. WannaCry demonstrated just how important consistent asset management is. Bad actors prey on your human error. It is critical to take a step
back and look at your system from the outside. If you were trying to sneak into your systems, where would you look first?

3) **Build some walls with network segmentation.** Patching old systems often comes with a slew of technical challenges. For this reason, new systems are often built on top of the old and unsupported. Many do not realize the risk of unpatched systems and a lack of network segmentation. Network segmentation and well-planned network architecture could have saved some organizations a world of pain.

4) **Cybersecurity protects real life.** It is important to remember while cybersecurity is digital and you may be fighting the good fight behind a computer screen, people’s lives hang in the balance. WannaCry’s attack on health care services in the UK, was a clear display that there are consequences that go far beyond bitcoin.

5) **Don’t forget about Availability!** WannaCry gave organizations a swift kick in the rear and reminded them that availability in the CIA three-legged stool, is essential to the success of everyday business. The cost of this ransomware is estimated to be over $8 billion dollars due to business interruption, lost income and time spent restoring.

---

**Information Security Officer Spotlight**

**Jehoshaphat Tetteh**  
Network Administrator and ISO at Texas Southern University

**Tell us about your background.**

I grew up in Ghana, at a time where we had limited access to computers. Thus, I had almost no exposure to computers until my final years in high school when I was gifted a programmable scientific calculator by a family friend. With this calculator, I started to write small programs. Discovering and enjoying the power of programming led me to develop an interest in computers and the field of information technology. Despite my seemingly late introduction to computers, I pursued a college education in IT. After high school, I completed a two-year diploma course in information systems management and worked as an IT technician, gradually assuming more of a network administration role. In 2002, I joined the International Research Center WARDA (now AfricaRice), as a Network Administrator. I immigrated to the United States in 2006 and in 2012 earned my bachelor’s degree in computer science from Kean University in New Jersey. I then worked as a Lead Network Administrator, managing a team of five IT staff for a large New Jersey based federal and state funded non-profit until 2014 when moving to Houston, Texas.

**What Agency do you Work for?**

I work for Texas Southern University as network administrator and have taken on many of the responsibilities of the information security officer (ISO), a role that is being developed at the University. Texas Southern University is an HBCU located in Houston, with a student population of more than 9,200 undergraduate and graduate students from across the world.

**How did you get into the security field?**

I became interested in network security while managing the network infrastructure for a non-profit in New Jersey. I realized the implications of the growing cybersecurity threats impacting my organization. From that point forward, my interest in network security grew and I sought to become more engaged in the security field.

**Who are your users/customers, and what is one of the most challenging areas for you?**

At Texas Southern University, we serve a variety of users including faculty, staff, visitors, and consultants but our main customers are the students. One of the challenging areas for
me is being able to create the right balance between security and convenience for our constituency - finding a way to merge the appropriate security levels without sacrificing the user experience requires great effort and attention.

**What do you like best about your job?**

I enjoy that Information Security is a very broad field that requires dealing with people, processes and technology. Though dealing with people and getting them to understand the benefits of a strong information security posture can be very challenging, it is also rewarding to see them achieve that level of maturity. I also really enjoy getting upper management to embrace security solutions and implement risks mitigation steps that strengthens our security position.

**What other career would you have liked to pursue?**

When I was younger, I had an interest in languages. I can fluently speak French, English and three local African dialects. I once contemplated a career as a translator/interpreter but my interest shifted when I was introduced to computer programing.

**What has been the greatest challenge that you have faced, and how did you resolved it?**

One of the greatest challenges I faced in my IT career was to coordinate the relocation efforts of all IT operations after a war crisis disrupted all scientific research activities at the WARDA’s headquarters (now AfricaRice) in Bouake, Ivory Coast. All scientists and their supporting staff were relocated from Ivory-Coast to Mali, a more stable neighboring country. Though I had joined the research center just three weeks prior, I was tasked with coordinating all networking activities at the new location. That was indeed a huge challenge for me. We successfully got the network up and running within an acceptable timeframe. Two years later, when returning to our former headquarters in Bouake, Ivory Coast the war erupted again and we unfortunately lost one of our scientists.

**Where did you grow up?**

I grew up in three different West African countries: Ghana, Burkina-Faso and Ivory Coast (or Cote d’Ivoire). This gave me the opportunity to appreciate different West African cultures and learn French, English and three local African dialects.

**What are your hobbies?**

- Participating in church youth activities;
- Counseling and advising the youth;
- Playing the piano;
- Chasing after my two very energetic toddlers.

**People would be surprised to know that you**

I am a war survivor. Early on the morning of September 19, 2002 in Bouake, Ivory Coast, as I was waiting for our company bus to transport me to work, when rebel troops attacked. We had not been aware that rebels had taken control of part of the town the previous night. I managed to get home safely that morning. Our residential compound was also later attacked twice. Fortunately, there were no casualties during the attacks.

**Do you have a favorite book you would recommend?**

I would recommend the book of Ecclesiastes, also known by many biblical scholars as a book of wisdom. It teaches how to live a fulfilled life while abiding by simple life principles.

**What is the best advice you have received?**

Be humble and respect other’s point of view even when it sharply differs with mine. Due to divergent backgrounds, people tend to see, understand and articulate things differently.