TNCC

Cybersecurity Program

Prof. Steve Foster, CISSP

Cybersecurity Project Director
2019
Highlights of TNCC Cybersecurity Program

Designated a Center of Academic Excellence in Cyber Defense CAE2y-CD by NSA/DHS

Designed two year Associate of Applied Science Degree with focus in Cybersecurity

Designed Academic Cybersecurity Career Studies Certificates

Developed Cybersecurity BS Articulation Agreement with ODU

Developed Workforce Cybersecurity Certificates

Host annual Hampton Roads Cybersecurity Conferences

https://tncc.edu/cybersecurity
VA Beach will be a Hub for (2) new undersea transatlantic fiber optic cables from Spain and Brazil.

The Military has conceded a portion of their own networks to Hackers.

Verizon is beginning to offer upstream Cybersecurity service options to its customers.

Companies banned from US Gov. (Lenova PC, Huawei Tech, Kaspersky Labs).

Drones becoming a major threat to our Homeland and National Security.

We do not have any National Cybersecurity Defense Policy or Plan to define a Cyberwar and or a response to it.

Do I have your attention yet?
Gov. Ralph Northam noted that there are approx. **37,000 currently open Cybersecurity jobs in Virginia**, paying an **average annual salary of $88,000**.

There are currently **1.1 Million Cybersecurity related open positions Nation wide**

It is expected that number will go up to **1.4 M open positions by 2020**
DARPA was created in 1958 as the Advanced Research Projects Agency (ARPA) by the Dept. of Defense (DoD) to execute R&D projects and survive a Nuclear attack during the “Cold War”.

DARPA’s involvement in the **creation of the Internet** began with an idea to link time-sharing computers into a National system.

The **first Node (using TCP/IP protocol)** was connected in 1969.
Regardless of the exact numbers, one thing is clear: there is much that can still be connected and it’s safe to assume we’ll probably reach the lower numbers of connected devices (20-35 billion) by 2020.

What is Driving The IoT

1960’s

2000

Today
Risk Exposure

- Home
- Government
- Business
- Military
- Bad Guys
- The World
Today Be Thinking About
Identity Theft Continues To Be The Fastest Growing Crime
What is Identity Theft?

Stealing Someone’s Personal Identifiable Information (PII)
Bad Guy Action Plan

How do bad guys steal your identity

- They gain access to your home or business
- They gain access to your digital devices
- They hack into your digital devices
- They steal your info. from an on-line data base
Physical Prevention Tips

- Never discard documents into a public trash bin containing **Personal Identity Information (PII)**
- Always shred important documents
- Cut up all old credit and debit cards so that the information is not legible
- Never leave important documents lying around the house or on your desk at work

**Dumpster diving or searching through your trash is fairly easy to prevent.** It basically consists of taking the extra steps to make sure your personal identity information (PII) is properly disposed.
Define and Prioritize Your **Crown Jewels**!

- **Information is a critical asset**
  - Government
  - Business
  - Military
  - Personal (legal and financial documents, family photos, etc.)

- **Our failure to protect key information can directly affect**
  - Economic & Marketplace Advantages
  - R&D
  - National Security
  - Warfighters in the field!
Digital Prevention Tips

- Develop a good Cybersecurity "Attitude"
- **Use Common Sense and be a role model**
- Know that security measures are not 100%
- Assume you have been already Hacked

**Actin Items**

- Operate your PC in the "Standard User Mode"
- ID your most important data and store it off-line: example USB Drive
- Back up your USB drive weekly *(and use encryption)*
- Enable The Restore Function on your PC
- Install Router / Firewall between your COX Cable Modem and your Home Network
- Install Anti-Virus / Firewall suite on your PC Operating System O/S
- Keep O/S, Router/FW and Anti-Virus/FW up to date with the latest patches (weekly)
- Disable **MS Macro** features MS Office suite *(instead use Word Viewer in MS Office emails)*
Digital Prevention Tips

- Never open suspicious emails and or click on embedded Web links (Phishing)
- Maintain an encrypted vault for all your passwords and change regularly
- Use 2FA or multi-factor Authentication Apps (examples below)
- Verify that you use (HTTPS://) in the URL window, especially when conducting any financial business on-line
- Do not download anything from untrusted web sites
- Reconsider using mobile devices for on-line financial transactions
- Do not use airport, restaurant, hotel, Cyber Café and or Public use PC’s for your financial transactions
- Keep a separate PC for children and Grands to use

“Be Cybersecurity Vigilant”
Student
Social Media (Digital) Activities
Provide Parental Guidance
Friend or Foe
Phishing Emails

- Social engineering techniques that persuade you to **download rouge attachments (Malware)**, **click on an rouge embedded web link (Malware)** and or **make a rouge phone call (to provide PII)**

---

**Spelling**
Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department.

**Links in email**

**Threats**

**Popular company**
Threats From Emails

- Do not open un-trusted attachments or click links
- Do not open jokes or junk mail
- Do not respond to emails requesting financial info.
- Disable HTML and **Do** use “plain text” formatting
- Disable Microsoft Word “Macro”

What Should Cyber Citizens Do

Everyone’s to Do List

- Recognition that our National Digital Infrastructure is a “National Security Priority”
- Support Passage of Congressional Legislation to protect U.S Information Systems
- Review what really needs to be connected to the Internet
- Develop a strong Cyber Security mind set and attitude
- Practice safe computing and encourage others to do the same
- Continue your education and training on Cybersecurity – be aware!

Remember

It's your responsibility to protect your own data
Do not rely on someone else to protect your data for you
Federal Laws

- The “Federal Identity Theft and Assumption Act” of 1998 makes Identity Theft a Federal Crime
- Criminal Penalties up to 15 years in prison
- [https://www.identitytheft.gov/](https://www.identitytheft.gov/)
On-Line Resources

Cybersecurity

- [http://www.consumer.ftc.gov/topics/privacy-identity](http://www.consumer.ftc.gov/topics/privacy-identity)
- [http://www.dhs.gov/topic/cybersecurity](http://www.dhs.gov/topic/cybersecurity)
- [http://www.us-cert.gov/nccic/](http://www.us-cert.gov/nccic/)
Questions?

Contact us!

Prof. Steve Foster

Email: fosters@tncc.edu

Phone: 757-258-6600