

Internal Audit

INTEGRITY, OBJECTIVITY, CONFIDENTIALITY, COMPETENCY



National Cyber Security
Awareness Month



CyberAware

We are transitioning from an Internet of connected individuals to an Internet in which everything and everyone is connected, also known as the **Internet of Things (IoT)**.

As **TECHNOLOGY ADVANCES**, more “things” become “smart” or connected:

25 million smart devices now and **50 billion before 2020**.

67% of households have between 1 and 5 home devices connected to the Internet. More than 1 in 5 households use mobile devices or apps to remotely access or control devices in the home.

Navigating the world of **IoT** starts with **STOP, THINK, CONNECT**. Make sure connected devices have security precautions, think about the consequences of the data being shared and then connect a device to the Internet with more peace of mind.

KEEP CLEAN MACHINES:

Understand how you keep IoT devices up to date - Including any software that might be needed and passwords or other ways of securing devices.

Keep your mobile phone and apps up to date - Many **IoT** devices are controlled via smartphones or tablets. Keeping your phone and associated apps up to date is an important security step.

Pay attention the WI-FI router in your home - It is the main way home **IoT** devices connect to the Internet. Use a strong password to protect your router, and name the device in a way that won't let people know it's your house. Keep router software up to date by checking with the manufacturer or with your Internet service provider (ISP) to see if the software is updated automatically.

OWN YOUR ONLINE PRESENCE:

Understand what's being collected - The functionality of most **IoT** devices requires collecting data. Take the time to understand what information your connected devices collect and how that information is managed and used.

Where does your data go - Many **IoT** devices will send information to be stored in the cloud. Understand where your data will reside and the security protecting your personal information.

Do your research - Before adopting a new smart device, research it to make sure others have had positive experiences with the device from a security and privacy perspective. (Source: StaySafeOnline.org)

Challenge Question

Which of these groups exploits cyber vulnerabilities?

- a. Criminals
- b. Governments
- c. Hacktivists
- d. All of the above

Send responses to Viviana Lauke at vlauke@fgcu.edu by **Friday, October 27th**. Correct responses will be entered into a drawing for a **\$15 Dunkin Donuts gift card**.

Internal Audit Staff

**Bill Foster, MBA, CPA, CIA,
CGAP, CFE, CRMA, CCSA**
Director, Internal Audit
590-1709

Jena Valerioti, MBA
Internal Auditor
590-1708

Viviana Lauke
Staff Auditor
745-4439



Resource Links

FGCU's Business Technology Services Department offers free training classes for Faculty and Staff.

Register for Get Secure! Training by visiting:

[BTS Training Classes](#)

Additional resources are available at:

[Get Secure](#)



<https://www.dhs.gov/stopthinkconnect>