fissea

Federal Information Systems Security Educators' Association

AWARENESS • TRAINING • EDUCATION

FISSEA Security Awareness, Training, & Education Contest

Entry Form

Please review the rules before completing this entry form (pay attention to the due date). No late entries will be accepted. Be sure to fill this form out completely and email it with your entry to fissea-contest@nist.gov. Please submit an entry form with each entry.

Name of submitter: Kimberly Blake

Name(s) to be printed on award certificate if your entry is selected as the winner:

IHS Policy and Security Awareness Team

Organization: Indian Health Service

Please list how the organization should be listed under the name(s) on the award certificate if your entry is selected as the winner:

IHS Division of information Security

Address: 5600 Fishers Lane
Rockville, MD 20857

Phone: 301.443.6895

Email Address: cybersecurity@ihs.gov

Type of Entry:
Please list the entry type below: it should be one of the 6 categories (poster, newsletter, website, motivational item, video, training scenario)

Newsletter

Title of Entry: Internet of Things-out-to-Getcha!

Description of Entry (use up to but no more than 500 words):

Note: Please also put the URL for any entries (videos or websites) that are publically available.

Internet-connected devices are growing increasingly common in the home, from climate control and home-monitoring systems, to everyday stuff like toothbrushes and toasters. The technological phenomenon of ubiquitous interconnectivity has been termed the *Internet of Things*, and many people look at it as an opportunity to gain convenient and programmable control over everyday life.

However, as with all things connected through the Internet, interconnected everyday stuff creates endless handholds for criminals to infiltrate or rob us of our privacy, property, and even our premises.

Though the Internet of Things offers a whole new landscape of exploitation, it is, as yet, rarely the subject of cybersecurity training. IHS developed the “Internet of Things-out-to-Getcha!” tip sheet for National Cybersecurity Awareness Month (NCSAM) to provide timely, fresh, and meaningful IT security education for a user population who is otherwise bombarded with the same old password security, phishing awareness, and malware prevention material.

National Cybersecurity Awareness Month

National Cybersecurity Awareness Month

INDIAN HEALTH SERVICE
PHS · 1955

OCTOBER 2016

WEEK 4

The Internet of Things

Each year, manufacturers think up new ways to connect mundane, physical objects to the digital world. From toys to thermostats, toasters to TVs, and even toothbrushes to toilets, we're connecting, monitoring, and managing everday tasks online.

The Internet of Things (IoT) is a growing phenomenon forcing major changes in the way we operate in our daily lives. With our expanding footprint of interconnectivity comes an expanding surface area of vulnerabilities for hackers to exploit. Why would a hacker exploit your toothbrush, and why should you care?

Halloween Cyber Tricks?

Hacking IoT devices like toothbrushes or coffee makers may seem like a benign prank, but these vulnerabilities can put your and your loved ones' personal information and safety at risk!

- IoT devices have been hijacked in order to send spam or host illicit pornography.
- Personal information has been compromised by IoT devices like: the Samsung smart fridge that exposed email credentials; climate-control systems that resulted in the 2013 Target credit card breach; and even barbie dolls that were connected to smart phones.
- Hackers have demonstrated the deadly potential to take over IoT products like: automobile engine and break systems; medical devices like Wi-Fi enabled pacemakers and drug-infusion pumps; and Wi-Fi enabled sniper rifles.
- Information about daily lives gained from Internet connected thermostats and door locks can provide burglars valuable information about your habits.

NANCY!
I'm so glad you passed by!!!
I need help!!
My goodness, Sally!
What's wrong???
How can I help??
Some jerk unlocked my door, turned my TV on super loud, overflowed my toilet, turned my AC down to 42 degrees, and turned my refrigerator up to 75! I think I have a mean-spirited burglar!
Scariest of all, I think the creep is stalking me right now in MY OWN CAR! I keep seeing it following me!!
Oh my LANDS, honey! I'm calling the police right now. Do you have any idea who it might be?
Actually, YES! I'm pretty sure it's my wireless toaster

NCSAM Tips of the Week!

- Consider first whether your toothbrush or toaster needs to be "smart." If it does, make sure to purchase the ones with built-in security, and let the other companies know why you won't buy their unsecured products.
- Change the default passwords and give each device a unique password. Look for encryption options, enable security features, and apply patches or "firmware" updates when recommended.
- Never connect IoT devices at work without IT approval, and limit the number of devices that connect to the Internet at home. Software is available to enable a group of smart devices within the home (like light bulbs and door locks) to communicate with each other rather than the Internet.