Questions, Issues,
Concerns, Suggestions
Welcome at any time
Even Now

# Sun City Computer Club

Cyber Security SIG

January 17th, 2019



- Printers exposed to Internet
- Govt shutdown cyber issues
- WhatsApp phone number
- Weather channel App
- Non-testimonial device access
- Oklahoma Securities Commission
- 773M 21M
- Chromecast/SmartTV/GoogleHome Leaking sensitive Information Wi-Fi, Bluetooth parings, alarms, etc. etc.
- Play video, rename device, ...

### PewDiePie

## **ATTENTION**



YOUR Chromecast/Smart TV is exposed to the public internet and is exposing sensitive information about you!

To find out more about what to do and how to fix this, visit

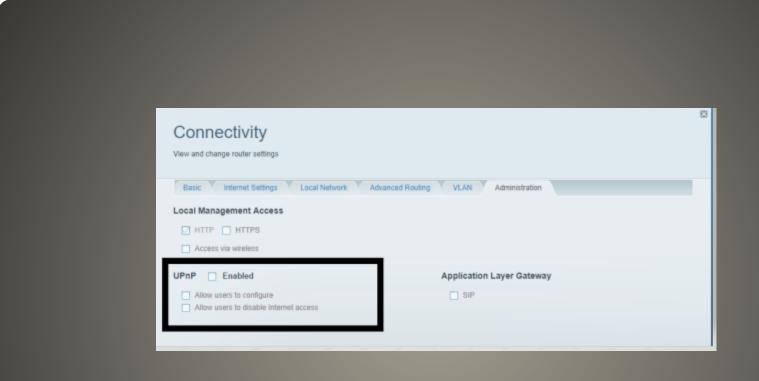
https://bit.ly/CastHack for more information

You should also Subscribe to Pewdiepie

Greetings from @HackerGiraffe and @j3ws3r Made by rosk2006



### **PewDiePie**



UPnP

https://www.grc.com ShieldsUP!



Port Authority Edition - Internet Vulnerability Profiling



#### **Greetings!**

Without your knowledge or explicit permission, the Windows networking technology which connects your computer to the Internet may be offering some or all of your computer's data to the entire world at this very moment!

- For orientation and background, please examine the page links provided below for important information about Internet vulnerabilities, precautions and solutions.
- First time users should start by checking their Windows File Sharing and Common Ports vulnerabilities with the "File Sharing" and "Common Ports" buttons below.
- For orientation and information about the Port Authority system, click the Home or Help icons in the titlebar . . .

Click here to check your router now...

GRC's Instant UPnP Exposure Test



Please see Explain this to me! below for information about Windows File Sharing and Internet port vulnerabilities.





by Steve Gibson, Gibson Research Corporation.

#### Universal Plug n'Play (UPnP) Internet Exposure Test

This Internet probe sends up to ten (10) UPnP Simple Service Discovery Protocol (SSDP) M-SEARCH UDP packets, one every half-second, to our visitor's current IPv4 address in an attempt to solicit a response from any publicly exposed and listening UPnP SSDP service. The UPnP protocols were **never** designed to be exposed to the public Internet, and **any** Internet-facing equipment which does so should be considered defective, insecure, and unusable. Any such equipment should be disconnected immediately.

Your equipment at IP:



Is now being queried:

THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!

(That's good news!)

- Router and WAP don't show UPnP ports
- Disable UPnP disables future openings
- Disable UPnP, power cycle, check firmware, update firmware if applicable, power cycle, check UPnP settings, check grc.com

## Universal Plug and Play UPnP

- Routers, Wireless Access Points, IoT devices
- Cell Phone location data brokers
  - T-Mobile > Zumigo > microbilt > Bail bond > Motherboard
- Weather Forecast-World Weather Accurate Radar
- USB-C authentication
- Reverse proxy
- Windows 10 patch

### **Current Issues**



## Fuze card

- If you didn't initiate a download, don't install it
- If you don't still need it, remove it
- If you do still need it, keep it updated

## Consider

- Tortoise and Hare
- Chicken Little

Computer Club, Help Center, SIGs, Presentations, FirstTime Cyber Security SIG meetings, NEWSBLOG Internet

• Questions, suggestions, comments?

SCCCCyber@gmail.com