Questions, Issues,

Concerns, Suggestions

Welcome at any time

Even Now

Sun City Computer Club

Cyber Security SIG

May 3, 2018

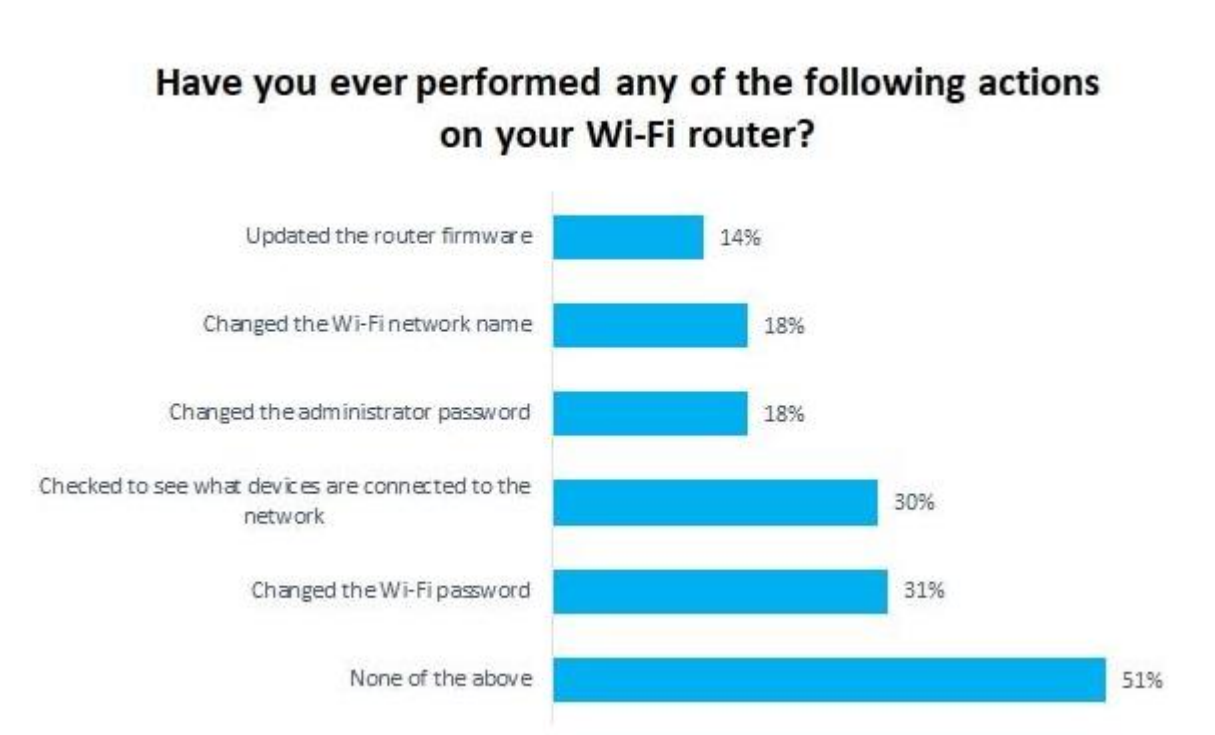
SCCCCyber@gmail.com

Current Issues

- Orangeworm healthcare
- FDA Medical Device Action Plan
  190,000 devices, 18,000 firms
- Cybersecurity Tech Accord
  Strong defense, No offensive development,
  Capacity building, Collective action
  $8 trillion by 2022
  Not Amazon, Apple, Google, Intel
- Remote Detonator SSID
- Amazon packages to car trunk
- Austrian Ski Lift
- Nasdaq servers in Sweden shutdown by noise

Current Issues

- Amazon Echo Alexa Skill
- Hotel locks Master key
- “Calculator” App removed from Apple store
- April update for Windows 10
- Automobile CAN bus
- Drupal



No one we know

VPN

- Virtual Private Network VPN
- Network
- Private Network
- Virtual Private Network

- Privacy
- Avoid firewalls, blocking proxies, etc.
- Faked presence in another country
- Most secure your device <-> your device
- Less secure Vendor’s endpoints
- No standard
- Vendor offerings may interfere
- Proprietary vs Open Source
- Addons Torrent
- EULA Terms of Service
- https://www.top10vpn.com and others

Encrypted tunnel embedded in Internet

- 1-2-3-4
- Steganography
- Hash
- Symmetric
- Asymmetric

cryptography

- 1-2-3-4
- Algorithm
- Key
- Plain text
- Cypher text

cryptography

symmetric

- Plain text, algorithm, key, cypher text
- Algorithm usually public
- Key space is important
- Reversible with the one key
- Does not scale
- E.g. RC4,SEAL DES,3DES,RC5,Rijndael
- One-time pad
- Cryptanalysis
- Control

CIA

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

Asymmetric

- Public & private key
- Intractable problem
- Symmetric key exchange in presence of advisory
- Thousands of times slower
- E.g. RSA, El Gamal, ECC
- Public key distributed and verified via Digital Certificate
- Signing via digital signature

VPN Considerations

- Should you pay?
- Interoperability
- Device coverage
- Browser addon?
- How to pay
- Vendor claims
- Standard encryption
- Speed
- Data protection inside tunnel only

- Questions, suggestions, comments?
- The**amnesic**incognito**live**system

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer

SCCCCyber@gmail.com