Cisco Umbrella Implementation at ECC

- Cisco Umbrella uses the internet’s infrastructure to block malicious destinations before a connection is ever established.
- Umbrella uses DNS (Domain Name Service, see ‘Tip of the Month’ below for more information on DNS) to stop threats over all ports and protocols in order to stop malware before it reaches our endpoints (computers) or network:
  - Umbrella routes requests to risky domains for deeper URL and file inspection
  - Even if devices become infected in other ways, Umbrella prevents connections to attacker’s servers:

- Having a secure DNS solution like Umbrella will help to keep Ransomware, Malware, and other threats in check and provide a safer computing environment for El Camino
- **NOTE:** For improving your DNS security posture at home, see the Tip of the Month article below!
The Top 5 Riskiest Airport WiFi Systems:

- **San Diego**: It scored a perfect 10 on Coronet's scale. They found an SSID called SANfreewifi carrying out an ARP poisoning attack. Coronet estimates you had a 30% chance of connecting to at least a medium-risk Wi-Fi access point at the time they studied the airport.

- **John Wayne Airport in Santa Ana, AKA Orange County**: It's the airport to get to the happiest place on Earth, but you will not be happy if you don't use a VPN there and get hacked.

- **Houston Hobby Airport**: This is the smaller airport to Houston Intercontinental, AKA George H W Bush airport. Hobby often has cheaper fares, but that doesn't mean you should cheap out on your protection. Maybe just tether to your wireless carrier there.

- **Southwest Florida International Airport in Fort Myers**: Oh all those spring breakers flying through and looking to 'gram. A feast of data for the hackers. You really want to make sure you're using https there.

- **Newark Liberty International Airport**: If you can hack it there, you'll hack it anywhere. It's up to you to secure your ports!

The safest WiFi Systems:
- Chicago-Midway International Airport
- Raleigh Durham International Airport
- Nashville International Airport
- Washington Dulles Airport

Full article:

---

Data Breach Watch

U.S. Higher Education Breaches For September 2018:
- N/A

Other Significant U.S. Breaches:
- British Airways
- GovPayNow.com
- MongoDB Server
- Newegg
- Chegg
- Facebook

Tip of the Month
This 30-second change to your computer settings is the easiest way to stop hackers

- As we are all too familiar with, many scams start with phishing — tricking people into clicking on nefarious links through legitimate-looking emails. An easy way to block these attacks: Change the Domain Name System (DNS) that your computer uses.
- Most computers connect to the DNS that’s automatically set by their internet service providers, but there are safer alternatives. Every URL — like elcamino.edu — has a unique numeric address that is the IP address attached to that site. When you click a URL, it is looked up through the DNS, which translates the words in the URL that make sense to humans into the IP address, or numbers, that computers and routers understand. Your computer then connects to the site with the IP address it found in the DNS lookup.
- The DNS services that your internet service provider connects to automatically are likely not as secure as they could be. Cybersecurity specialists recommend changing your DNS service to one of a handful of alternative options from either Google GOOG, security company Cloudflare, or Quad9 — a new DNS from the nonprofit Global Cyber Alliance, an international group that fights malicious online activity. The Google, Cloudflare and Quad9 DNS services are all free (I have been using OpenDNS for years on my home systems). You can set up a new DNS with just a few clicks.
- You will have to Google how to change the DNS settings on your specific operating system/version, but there are many good examples on the internet
  - Google – 8.8.8.8, 8.8.4.4
  - CloudFlare – 1.1.1.1, 1.0.0.1
  - Quad9 – 9.9.9.9
  - OpenDNS - 208.67.222.222, 208.67.220.220
- Another side benefit to changing your default DNS settings at home is SPEED! ISP’s (Internet Service Providers) DNS servers are notoriously slow and sometimes even unreliable.
- CAUTION: These DNS suggestions are for your personal home systems and NOT your systems here at ECC! We have very specialized DNS settings at ECC that utilize the Cisco Umbrella DNS protection services and these settings should never be changed. Next month, we will talk more about Cisco Umbrella and how it helps to protect our systems on campus – so stay tuned!
- DISCLAIMER: ECC is not responsible for any changes that you may make on your home computers.

Cyber Security Trivia

The trivia question for this month is:

- This enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority:
  a. Security Identifier (SID)
  b. public key infrastructure (PKI)
  c. Internet Assigned Numbers Authority (IANA)
  d. Private Branch Exchange (PBX)
e. Trusted Computing Platform Alliance (TCPA)

- Email your answer to: pyoder@elcamino.edu

**Write in with your IT security questions:**

- If you have any questions about cyber security, please send them to:
  
  pyoder@elcamino.edu

**All current and previous issues of the Monthly E.C.C. Information Security Briefing are posted online at:**

- [http://www.elcamino.edu/about/depts/its/techservices/infosec.aspx](http://www.elcamino.edu/about/depts/its/techservices/infosec.aspx)

*Paul T. Yoder*
*Information Systems Security Specialist*
*El Camino Community College District*
*pyoder@elcamino.edu*