Cybersecurity

Client Hijacking Attacks

CYBER.ORG

Clickjacking

- Hijacking a button or link
- What you think you clicked on is something else entirely
- Web page renders on the screen properly, looks fine
  - Transparent layer over top of web page captures your click
  - JavaScript redirect
- Many ways it can harm you:
  - Installs malware
  - Redirects to phishing site

Typosquatting/URL Hijacking

- Typo-squatting/brandjacking
  - Exploiting a user's misspelling
- Outright misspelling
  - www.cyber.org vs. www.ciber.org
- Typing error ("fat finger")
  - www.cybre.org or www.cyberr.org
- A different name altogether
  - www.cyberer.org
- Wrong top-level domain
  - www.cyber.com or www.cyber.cc

Session Hijacking

- Logging into a website provides browser with cookie or session ID that authenticates users
- Stored cookie that tells service no need for user to keep logging in – once is enough
- Attacker can steal this cookie and assume user's identity on the service/server or track you from site to site
- Session for federated services like Google or Facebook can give hackers access to other services that authenticate through those services

Prevent Session Hijacking

- Encrypt HTTP
  - Most sites are moving to HTTPS-only
  - Hides web activity from MiTM attacks
- Encrypt connection
  - VPN hides traffic from you to VPN exit
  - Still visible once data leaves VPN on other end
- Anti-malware scanner on local computer
- Prevention tools
  - Blacksheep
    (sniffs out Firesheep tool that gives hackers ability to hijack sessions)