The Human dimension of cybersecurity

Unique challenges of WFH

Dr. Eric Haseltine

An opening comment about human nature

Defenders

- Change is the enemy
- Complexity is the enemy
- Human nature is the enemy
- Need to prioritize is the enemy
- Must fight hard for budget
- And most of all….
  - *Don't want vulnerabilities*

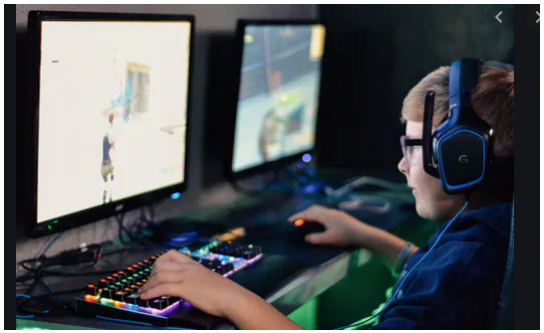
Attackers

- Change is the friend
- Complexity is the friend
- Human nature is the friend
- Can pick time, place, method of attack
- No budget needed
- And most of all….
  - ***Crave*** *vulnerabilities*

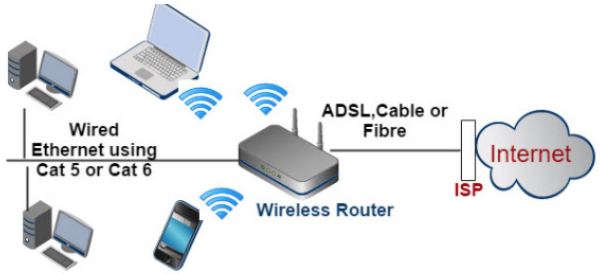
- Surface problems
- Surface solutions
- Deep problems
- Deep solutions

Surface problem 1

The environment

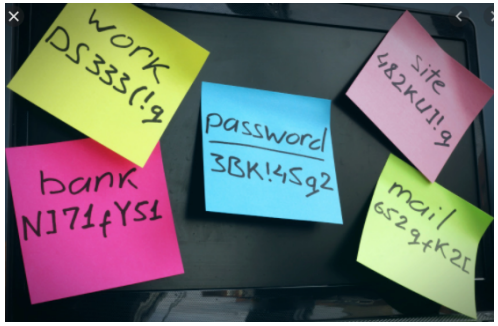


Home LANS are not Enterprise LANS



Network Diagram-Typical Simple Home Network

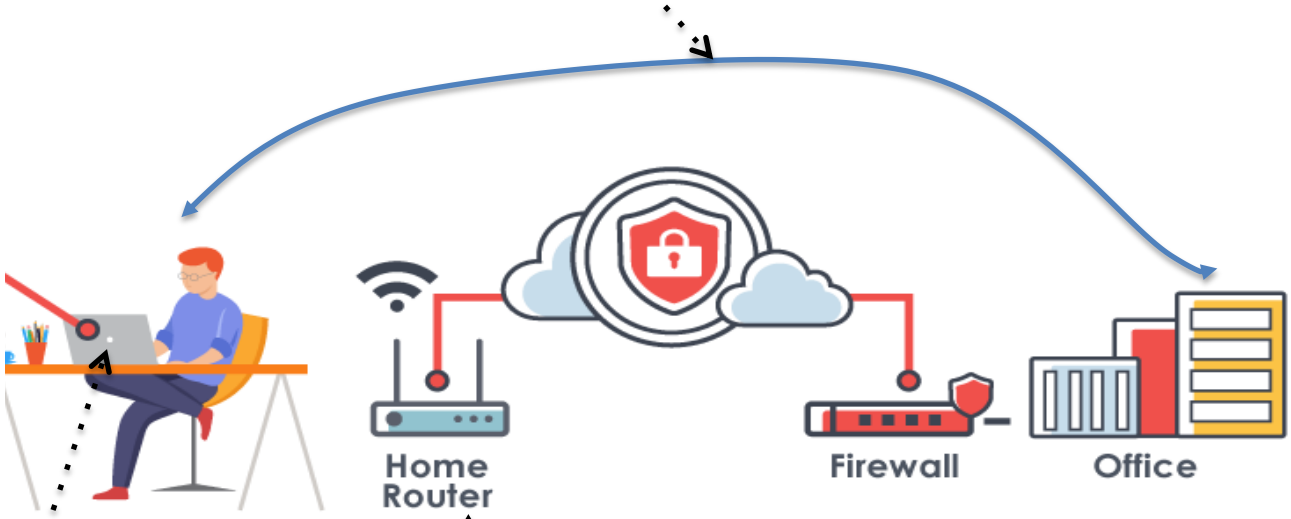
- Who has access & what do they download?
- How disciplined are users (e.g. phishing)?
- How secure are the router, mobile, IOT devices?
- How “patched” are all endpoints?
- Physical access to endpoint much easier (e.g. maids, friends, workers wanting bathroom)



Surface problem 2

VPN's

- Can download/upload bad stuff through enterprise



- Cheap home routers security sucks
- Malware can compromise net
- Access control flaky
- Belief that VPN is safe==lax behavior

"The vast majority of organizations were not prepared for 100% work from home on a cybersecurity basis," said Sultan Meghji, CEO of Neocova. "You had a VPN designed for emergency or off hours. Now it's being used for significant use."

https://www.forbes.com/sites/waynerash/2020/06/17/your-vpn-may-be-your-greatest-security-risk-during-covid-19/?sh=dd25e931a6df

Surface solutions

- Supply staff with work-only PC's/routers
- Ultra-thin, "stateless" clients (pixels and clicks)
- Use MFA everywhere
- Use "self-protecting data" systems (e.g. Keyavi)
- **Above all…focus on "High Value Targets" with "Crown jewels"**

But, let's get real

Workers

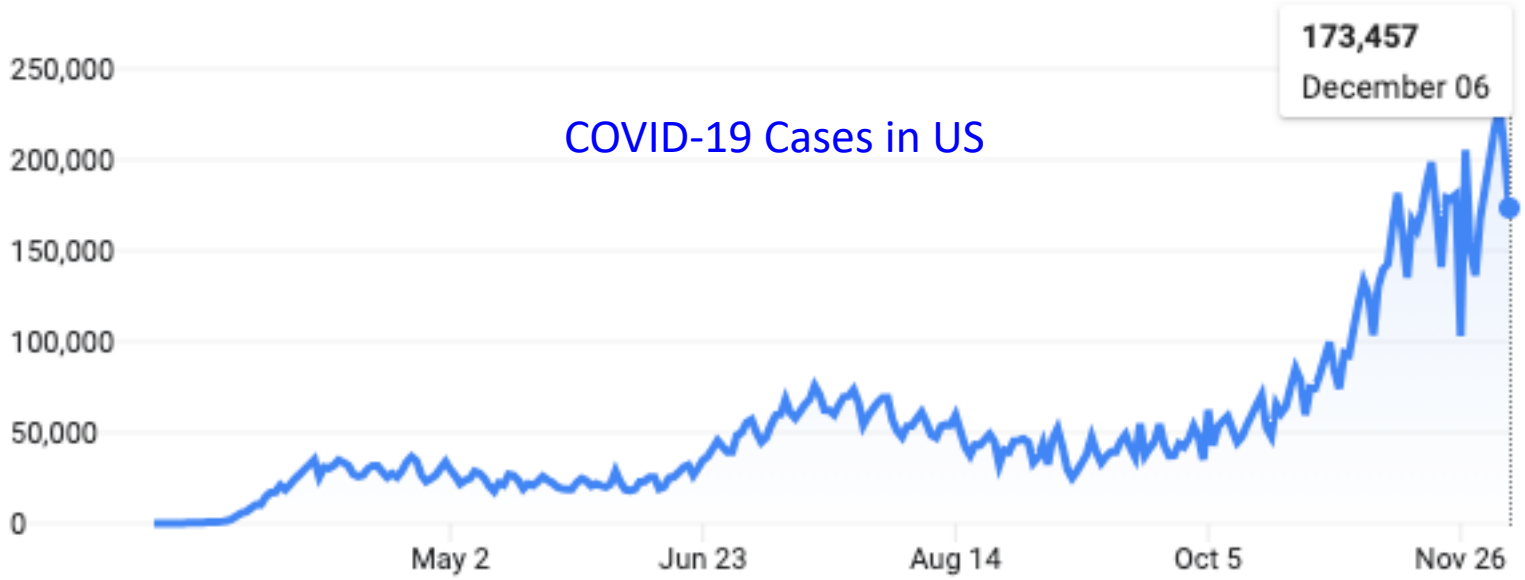
What we *want* to be true

What is *actually* true

Bosses

Deep problem 1

Most people don't really care about security



…***even*** when it's life or death

…therefore

- Employees..and their families..will be lax, negligent and sometimes actively circumvent whatever “surface solutions” you deploy

Deep problem 2

CFO's don't believe it's a problem worth $$$

…therefore won't fund endpoint fixes, ***especially*** when $$$ is extremely tight due to COVID-19 impacts

Deep solution 1

Employees

- Measure & monitor home behavior with fast feedback
  - 24/7 Pen testing (e.g. phishing, MFA testing)
  - Local monitors and canary tokens
- Make security tech work hard so your workers don't have to
  - Heavy emphasis on Human Factors/UI
  - Treat people as they ***are***, not as you ***wish*** them to be
- Involve workers --& their families--in identifying problems and solutions
    - Like it or not, families are de facto employees now
- Spend lots of time and $$ on "High Value Targets" (C-Suite, Sys Admins)
  - "Bad guys" will target them most

…Speaking of the C-suite

Deep solution 2

Convincing the "suits"

- Don't bother justifying loss avoidance with WFH
  - They'll think you are nakedly self-serving
  - Losses can't be quantified, Sony notwithstanding
  - CFO's don't get fired with breaches/spills: ***CSO's*** and ***CIO's*** do
- Focus instead on revenue generation
  - Example:
    - Securing user data builds consumer confidence in brand, especially where kids/families are concerned
    - Security as competitive weapons to increase market share
      - Competitors likely to have nasty spills by not adapting to WFH
      - Educate C-suite about unique security challenges of WFH because, they don't get it
    - Can lead to premium pricing if consumer confidence high

One last point

- CFO's probably won't fall for revenue generation argument (even though it's worth trying)
- But you can plant the idea insidiously by convincing them their home is the #1 target of bad guys who know all about WFH
  - When you go there to install "surface fixes" a light-bulb may go off in their head about rank and file employees
  - Ditto for COO, CFO
  - So, sell your ideas by explicitly ***NOT*** selling them

Bottom line

Surf human nature, don't fight it

Vs.