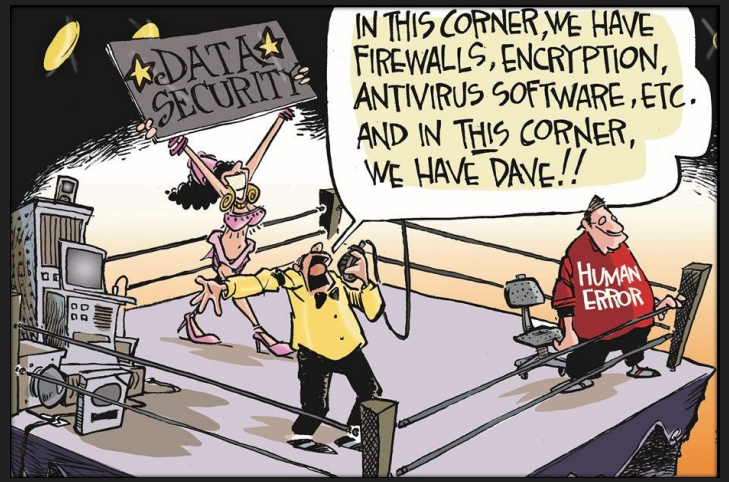
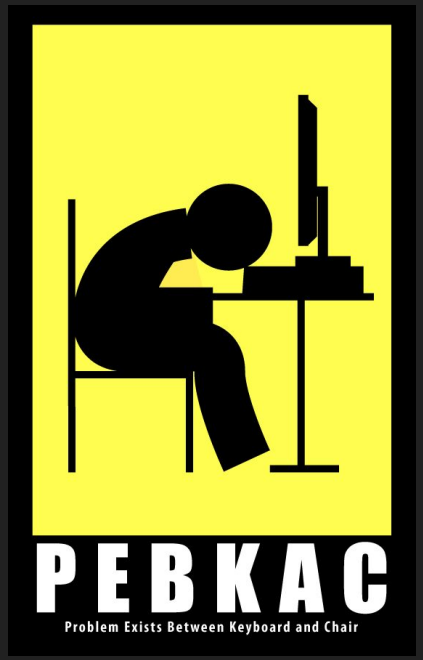
Plenty of Phish in the Sea

The l33test of attack vectors



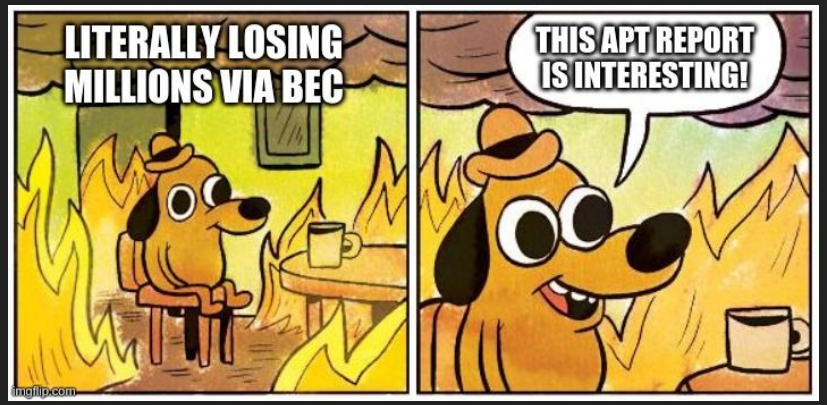


Threat of Phishing

Threat of Phishing (it’s high… it’s very high)

- 74% of U.S. orgs phished in 2020 - up from 60%
  - 30% higher than the global avg
- Becoming more sophisticated
- RaaS relying more and more on phish
- 11% PhishAlarm failure rate

*according to ProofPoint’s 2021 State of Phish Report



- 1.9B loss (for 2019) - FTC

Does it Look Like a phish? (unreliable)

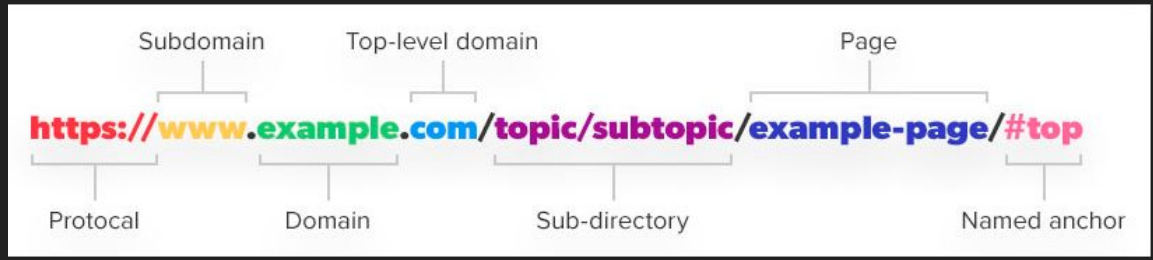
What to look for:

- Pay attention to the sender
- Hover-over links - where does it go?
    - @John, remember to ask Q

Does it Look Like a phish?

What to look for:

- Pay attention to the sender
- Hover-over links - where does it go?
  - @John, remember to ask Q
- Rarely contains specifics
- Typos
- Something weird...



Steps of Social Engineering (SE)

1. The rouse - story of why you're being contacted
2. The connection - emotional, attempt to establish trust
3. Some point of pressure or fear - time, debt, people
    - together with the connection -> gets victim to react
4. The ask
    - why we say **never** do certain actions/give information without

Ex: Silent Librarian

Dear Graduate Student,

Our records show that your access [univ3] library databases is about to expire. Due to new security precautions established to protect [univ3] Library system, you have to renew your library account on a regular base, so please use the following link

Click Here http://go.[univ2].edu/[shortened]

After your successful authentication, your access will be restored automatically and you will be redirected to the library homepage. If you are unable to log in, please contact the library help desk for immediate assistance. We apologize for any inconveniences this may have caused.

Office 365

Operation did not complete successfully because the file was created on IOS device.

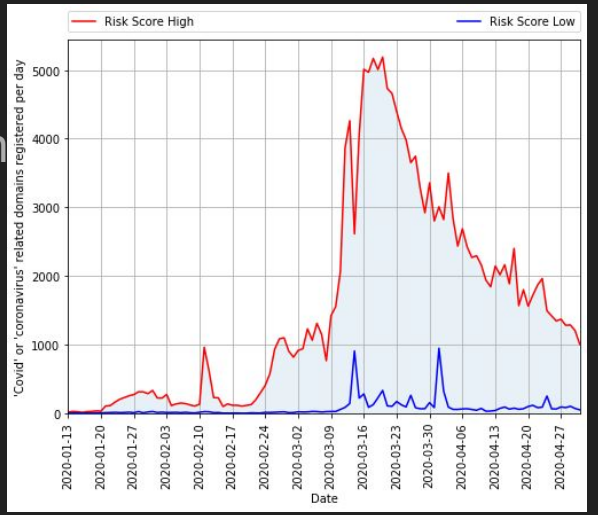
To view and edit document click **Enable Editing** and then click **Enable Content**.

Important Notes on Social Engineering

- **EVERYONE** is vulnerable to being socially engineered
- It is **NOT** the fault of the victim
- SE is an **emotional** problem, not an intelligence one

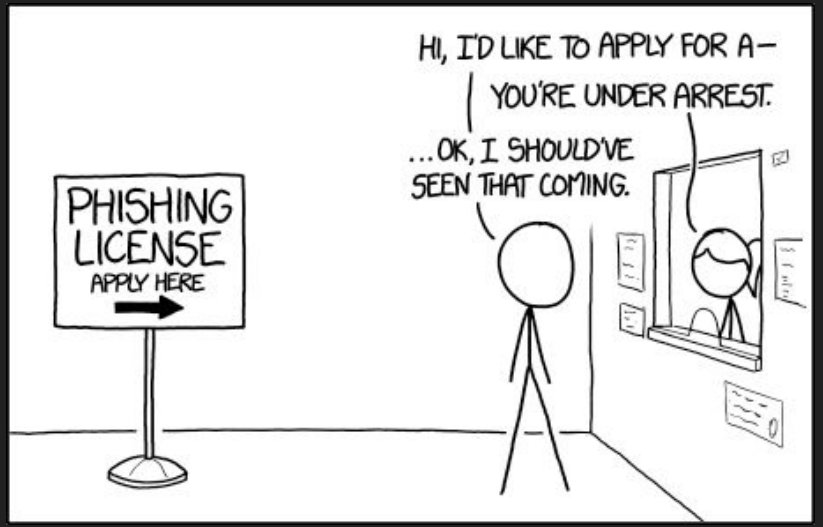
Important Notes on Social Engineering

- **EVERYONE** is vulnerable to being socially engineered
- It is **NOT** the fault of the victim
- SE is an **emotional** problem, not an intelligence one
- Attackers **do not** care - They are vicious people willin to harm others for their benefit



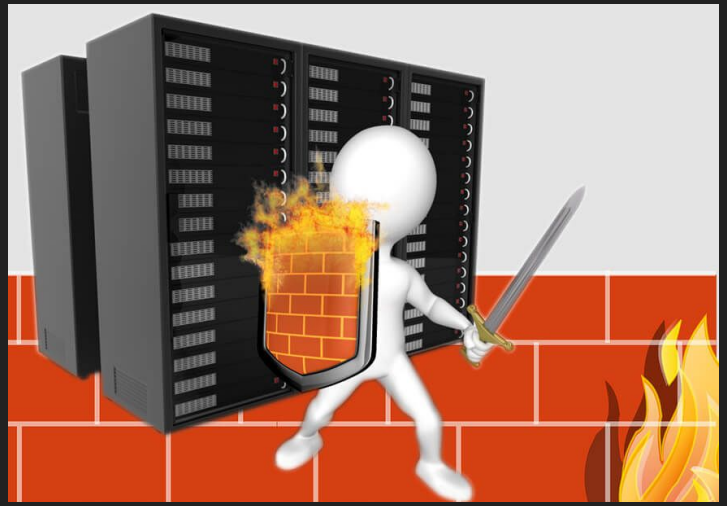
Advice

- Remember: you have **NO IDEA** who is on the other side
- Be aware of how SE/phishing operates
- Use an AV (or similar software)
- Set **clear** guidelines
- Take 5!
- Research



Investigation 🕵️

- Report to authority (... send urself a backup too)
- Take note of sender - notify org if possible
- Investigate links **carefully**
  - Can sometimes alert phisher
  - Defang URLs if sharing
    - https://sarlacklab.000webhostapp.com/
    - h**xx**ps://sarlacklab**[.]**000webhostapp**[.]**com/
- Malware? 😋
  - Move to sandbox!!!
- Share findings!
  - compromised accounts, domains, rouses, URLs, malware signatures, etc



Investigation Tools:

phishing@wpi.edu

https://www.virustotal.com/gui/home/url

https://o365atp.com/

https://app.any.run/

http://phishtank.org/index.php

https://urlhaus.abuse.ch

https://twitter.com/explore

Orgs to Bother:

- Proof Point
- Great Horn
- KnowBe4

Volunteer work 😎

phishing@wpi.edu

https://thecyberwire.com/podcasts/hacking-humans

https://darknetdiaries.com/

https://hub.wpi.edu/news/678/phishingirsimpersonation-scam

Layer 8 Con

@humanhacker, @abuse_ch, @PhishStats, @securitydoggo, @ActorExpose, @Cryptolaemus1