Technology Trends
(Cyber) Crime, Security & Warfare

Center for Learning in Retirement

CLR Fall 2020

Glen Maxson & Alan Freedman

Week 5

The What

- ~~Artificial Intelligence & Machine Learning~~
- ~~Robots & Drones~~
- ~~Autonomous Transportation Systems~~
- ~~Surveillance~~
- (Cyber) Crime, Security & Warfare
- Medical Tech
- Media (incl. Social Media)
- (Virtual) Money & Blockchain
- Communication
- Earth & Sky
- Space

Utility Scams

Warning Signs

- An unscheduled or unsolicited call or visit from someone claiming to represent your power or water company.
- Threats to cut off service unless an overdue bill or maintenance cost is paid immediately.
- A demand for payment by wire transfer, cryptocurrency, gift card or cash-reload card — scammers' favored methods.
- Payments on credit card or bank statements for utility accounts you did not open.

Do

Do call the utility, at the number listed on your bill
Do know how utilities operate
Do ask questions of anyone calling you
Do notify the utility if you've been approached by an impostor
Do notify neighbors of a suspected scammer

Don't

Don't provide personal or financial information
Don't wire money or provide credit card numbers
Don't get scared
Don't let a supposed utility employee into your home
Don't click on links in a utility-related email or text message

Taxpayer Scams

- Taxpayers should be on the lookout for new version of SSN scam
- Scams related to natural disasters
- Security Summit warns of new IRS impersonation email scam; reminds taxpayers the IRS does not send unsolicited emails
- IRS reminder: Tax scams continue year-round
- IRS warns of new phone scam using Taxpayer Advocate Service numbers
- IRS: Don’t be victim to a ‘ghost’ tax return preparer
- IRS warns of “Tax Transcript” email scam; dangers to business networks
- IRS-Impersonation Telephone Scams

Political Scams

Warning Signs

- A PAC has a name that sounds more like that of a charity. PACs registered with the Federal Election Commission (FEC) are supposed to focus on political activity.
- The PAC's website does not list the names of the people running it or provide contact information.
- A caller claiming to be a pollster or elections official asks you for personal or financial data.

Do

Do go to a candidate's official campaign website to learn about the candidate
Do check out a PAC before you donate
Do create a "refusal script" with potential responses to high-pressure fundraising requests

Don't

Don't make donations or provide personal or financial information to organizations that contact you out of the blue
Don't give in to pressure to contribute by a particular method
Don't give to a PAC that does not ask about your citizenship status
Don't provide private information to political canvassers

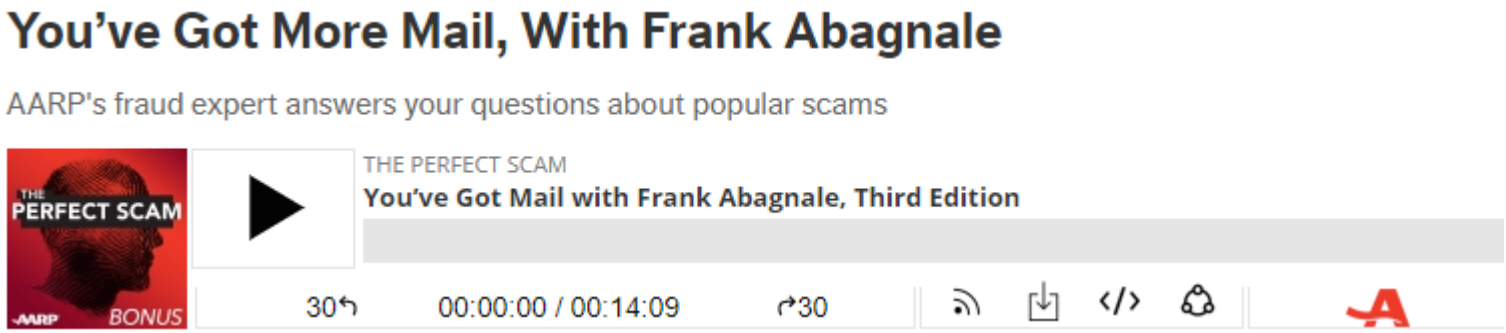
COVID-19 Scams

Advice from the Justice Department on dodging fraud during the pandemic

- Independently verify the identity of any company, charity or individual that contacts you regarding COVID-19
- Check the websites and email addresses offering information, products or services related to COVID-19
- Be wary of unsolicited emails offering information, supplies or treatment for COVID-19 or requesting personal information
- Do not click on links or open email attachments from unknown or unverified sources
- Make sure the anti-malware and antivirus software on your computer is up to date.
- Ignore offers from suspicious sources for a COVID-19 vaccine, cure or treatment
- Check online reviews of any company offering COVID-19 products or supplies
- Research any charities or crowdfunding sites soliciting donations tied to COVID-19 before making a donation
- Be wary of any business, charity or individual requesting payments or donations in cash or by wire transfer, gift card or using the mail
- Be cautious of “investment opportunities” related to COVID-19, especially those based on claims that a small company's products or services can help stop the virus

And So Many More…

AARP's weekly podcast *The Perfect Scam* profiles America's biggest scam stories. Hosted by Emmy award winning investigative journalist Michelle Kosinski, and leading fraud expert Frank Abagnale, the series introduces listeners to compelling personal stories from scam victims and their families.

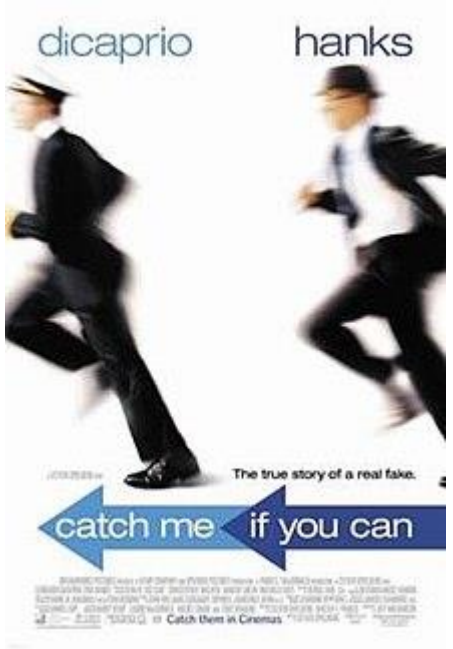


What is Cyber…?

- **Cyber-**, from "cybernetic", from the Greek for "skilled in steering or governing“
- relating to, or involving computers or computer networks (such as the Internet)
- things made possible by the spread of computers…

A Word About Cyber

[Frank Abagnale: "Catch Me If You Can“](#)
Talks at Google



What is Cybercrime?

- **Cybercrime**, or **computer-oriented crime**, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet. "
- Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming.

What is Cybersecurity (Computer Security)?

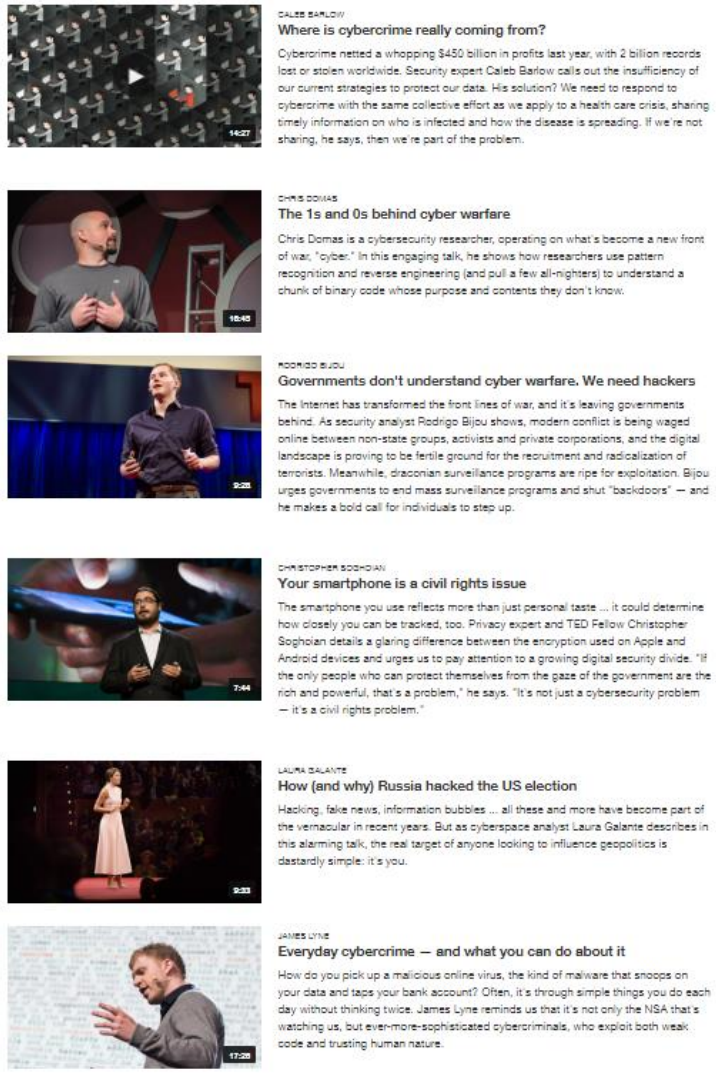
- **Cybersecurity**, **computer security** or **IT security** is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.
- Cybersecurity includes controlling physical access to system hardware, as well as protecting against harm that may be done via network access, malicious data and code injection.
- Due to malpractice by operators, whether intentional or accidental, IT security personnel are susceptible to being tricked into deviating from secure procedures through various methods of social engineering.

What is Cyberwarfare?

- **Cyberwarfare** is the use or targeting in a battlespace or warfare context of computers, online control systems and networks.
- It involves both offensive and defensive operations pertaining to the threat of cyberattacks, espionage and sabotage. [There has been controversy over whether such operations can be called "war“].
- Powers have been developing cyber capabilities and engaged in cyberwarfare, both offensively and defensively, including the United States, China, Russia, Israel, the United Kingdom, Iran and North Korea.

Cybercrime

- Where is **cybercrime** really coming from? Caleb Barlow
- Mikko Hypponen: Three types of online attack | TED Talk
- Top Five Emerging Cybersecurity Challenges | Srini Sampalli | TEDxDalhousieU



Where is **cybercrime** really coming from? Caleb Barlow (9.5 min)

Where is **cybercrime** really coming from? Caleb Barlow

- 2016 – 2 billion records lost/stolen
  - Months before stolen records reported
- Espionage a small portion of the problem – where is it coming from?
  - 80% from sophisticated gangs
  - 445 billion dollars in illegal profits (>GDP of 160 nations)
- Dire Wolf – 2 personalities (small and large transactions)
- The Dark Web* – anonymous under-bully of the Internet
- How do we ‘stop’ this? New approach…
  - Change the economics for the bad guys – altruistic effort to respond to attack
  - Need to democratize threat intelligence information – rapid response
  - Use healthcare response to a pandemic – open and collaborative*

*Pandemic response shows value of collaboration across sectors

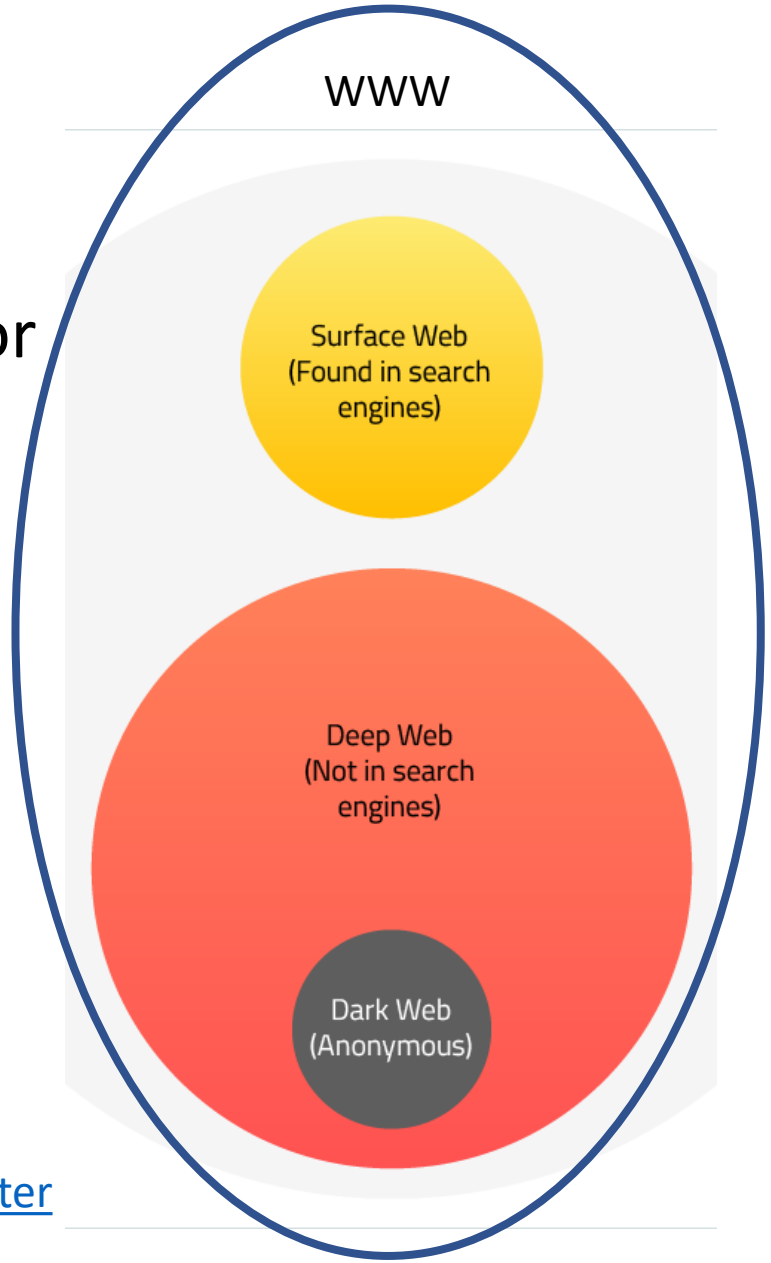
Dark Web versus Deep Web (10.5 min)

The **Dark Net** isn't what you think. It's actually key to our **privacy** | Alex Winter

Dark Web versus Deep Web

- The part of the internet indexed by Google and other search engines is known as “Visible Web” or “Surface Web.” (4% or the World Wide Web)
- The Deep Web is effectively walled off from ‘indexation’ – unreadable sites, internal sites, or sites requiring authentication to access (96%)
- Included within the Deep Web is the Dark Web (aka DarkNet). Pages in the Dark Web are anonymous, encrypted, and require special software to access - TOR (The Onion Router) and the Tor browser.

Excellent Video about the Dark Web:
The **Dark Net** isn't what you think. It's actually key to our **privacy** | Alex Winter



Top Five Emerging **Cybersecurity** Challenges | Srini Sampalli (10 min)

Top Five Emerging **Cybersecurity** Challenges | Srini Sampalli

- 2016 – Cyber Threats - Malicious online attacks, 758 million (24/sec)
- 5 challenges
  - Mobile Tech – knows a lot about you a hacker can use to build a digital profile
  - Ransomware – encrypts your files, pay up or lose your data (600% increase)
  - Internet of Things (IoT) – tech connected to the Internet – attack surface
  - Big Data – 60 seconds*
  - 1.7 mb of new information per person per second
  - The 'Weak Link' is US. (social engineering, simple passwords)