

The background is dark gray with a subtle grid pattern. In the corners, there are decorative light blue circuit-like lines with small circles at the ends, resembling a stylized circuit board or network diagram.

# **CYBERCRIMES: NEW PRIVACY CONCERNS, NEW LAWS, NEW PROBLEMS, & NEW SOLUTIONS**

**DONALD H. FLANARY III,  
Flanary Law Firm, PLLC**

State Bar of Texas 44TH ANNUAL ADVANCED CRIMINAL LAW July 23-26, 2018 San Antonio





# CYBERCRIMES



**BE AFRAID, BE VERY AFRAID!!!**

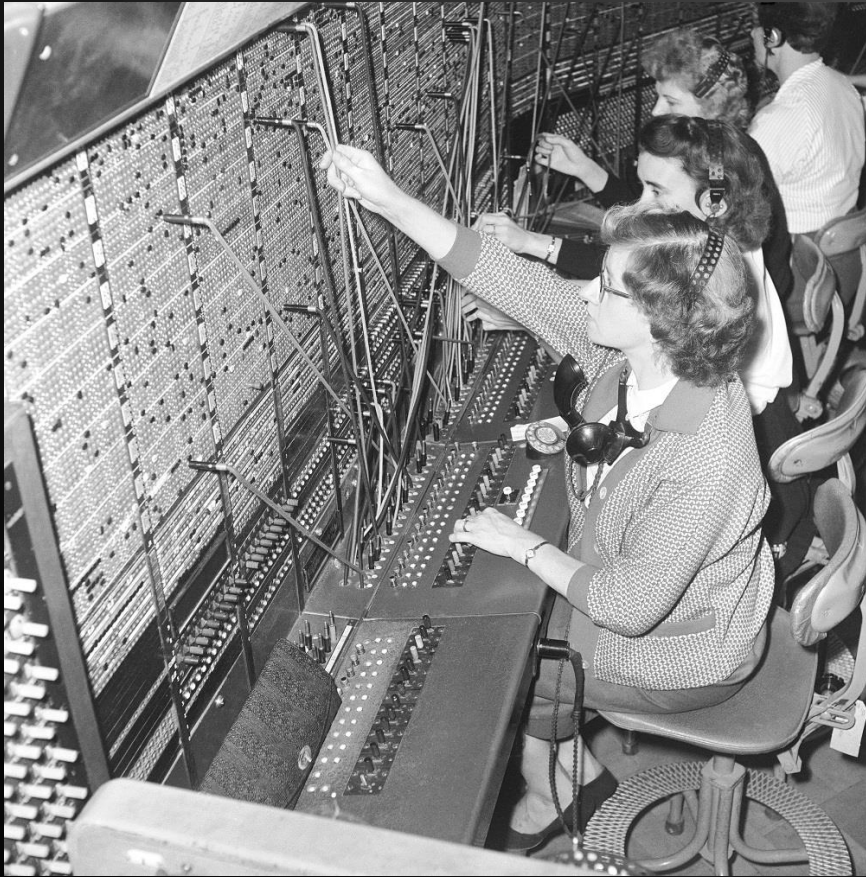




## TOP 5 CYBERSECURITY FACTS:

1. Cyber crime damage costs to hit \$6 trillion annually by 2021
  2. **Cybersecurity** spending to exceed **\$1 trillion** from 2017 to 2021
  3. Cyber crime will more than triple number of **unfilled cybersecurity** jobs which is predicted to reach **3.5 million** by 2021
  4. Human attack surface to reach 6 billion people by 2022
  5. Global **ransomware damage** costs exceeded **\$5 billion** in 2017
- 
- 

# HISTORY OF HACKING





**CYBERCRIME IS THOUGHT OF AS MODERN  
WARFARE...**



**BUT HACKING HAS BEEN AROUND LONGER  
THAN YOU THINK...**

# 1878 EARLY TELEPHONE CALLS

In 1878, Bell Telephone Company was forced to kick a group of teenage boys off the telephone system in for **repeatedly** and **intentionally misdirecting** and **disconnecting** customer calls.



# 1903

## WIRELESS TELEGRAPH

- The discovery of **electromagnetic waves** in the late 19th century paved the way for the invention of the **wireless telegraph**.
- In 1903, magician and inventor Nevil Maskelyne **disrupted** the first public demonstration of Marconi's 'secure' wireless telegraphy technology by **sending insulting Morse code messages** discrediting the invention.



# 1939-1945

## MILITARY CODEBREAKING

During the WWII, huge military operations were dedicated to **breaking the codes and ciphers** used by the Axis Powers to transmit top-secret information.

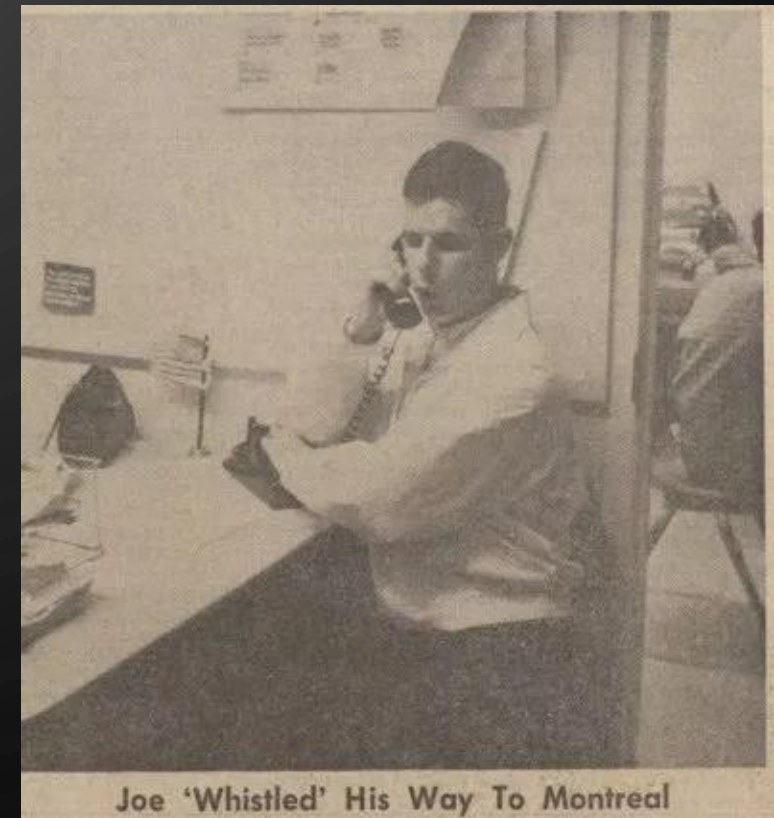
Allied powers developed an electromechanical device capable of deciphering **the German encrypted message "Enigma" machine.**



# 1957-1980

## THE RISE OF THE PHONE PHREAKS

- Phone hackers, first emerged in the late 1950s and would listen to tones to figure out how calls were routed. Joe Engressia, aka **Joybubbles**, was a blind seven-year-old boy with perfect pitch.
- In 1957 he **heard a high-pitched tone on a phone line** and began **whistling** along to it at a **frequency of 2600Hz**
- Other phreakers included John Draper, known as '**Captain Crunch**' for his use of a whistle found in a box of Cap'n Crunch cereal, and **Apple founders Steve Wozniak and Steve Jobs**, who in 1975 began building '**blue boxes**', electronic devices that communicated with phone lines.



# 1970-1995

## KEVIN MITNICK

- One of the most notorious hackers in internet history
- From the 1970s until 1995 Mitnick **penetrated some of the most highly-guarded networks** in the world, including those of Motorola and Nokia.
- Mitnick used elaborate **social engineering schemes**, tricking insiders into handing over codes and passwords and using the codes to access internal computer systems.
- He was driven by a desire to learn how such systems worked, but became the most-wanted cyber-criminal of the time. Mitnick was jailed twice, in 1988 and 1995, and was placed in solitary confinement.



# SOCIAL ENGINEERING

- Social engineering is **person-to-person communication** used to elicit **unauthorized information** or **access** to a system.
- Over time, telephone companies, notably Bell Telephone, **created automated systems to decrease human interaction**, thereby increasing call volume and decreasing costs through automation.

The background is a dark gray with a subtle pattern of concentric circles. In the four corners, there are stylized white circuit board traces and nodes, resembling a digital or technological theme.

# REMEMBER WARGAMES?

# REMEMBER WARGAMES?



The background is dark gray with faint concentric circles. Cyan circuit-like lines with circular nodes are positioned in the corners: top-left, top-right, bottom-left, and bottom-right.

# HACKING/CRACKING TRICKS AND TOOLS



# FOUR TYPES OF MALICIOUS ACTIVITY

- **Hacking**
  - **Cracking**
  - **Extortion**
  - **Destruction**
  - **Theft and Conversion**
- 
- 



Hacker  
Cracker  
Pengen  
Tahu Aja ..

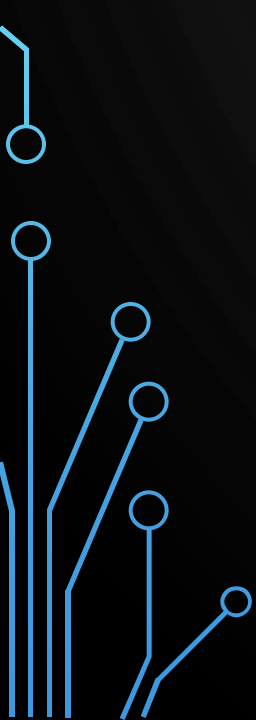

Hacking uses software and **person-to-person techniques** to **obtain access**.

Cracking involves **modifying or deploying software** to **alter** the system to **create access**.

**Hacking** is like the **key** whereas **Cracking** is like the **hammer**.



# CRACKING IS WHAT MOST PEOPLE THINK OF WHEN THEY THINK OF HACKERS

- Cracking involves **creating and injecting ready-made or custom-built computer code** to change how the system operates or processes data/requests.
  - As cracking involves altering the nature of the system, it **damages its functionality**, either recklessly or negligently.
  - Cracking requires a great deal of **knowledge** and **skill** to crack a computer system.
- 
- 

# CRACKING AND HACKING FOR SALE

- **Cracking and hacking** services can be **purchased online**, either through the darkweb or social media.
- Services range from **off-the-shelf software** to **custom-created code** and services.



There are a many hacking tools available online. **Chinese and Eastern European** criminal conglomerates **sell software packages** and services designed to **illegally hack computer systems**.

# CHINESE CYBERCRIME GANGS

- Chinese cybercrime gangs are involved in the entire gamut of cybercrimes, from **selling illicit software** to hack or disable a website to **custom service requests** tailored for the client. **Prices are negotiable**, typically with a fifty percent deposit due on agreement; the balance due on completion



# ETHICAL HACKING – PENTESTING OPERATING SYSTEMS

- “Ethical Hacking” (or “White Hat Hacking”) is the deployment of tools and techniques to test the integrity of a system. This deployment by a system administrator or information security officer is called “**Pentesting**”. Pentesting, short-hand for Penetration Testing, is ethical hacking used to discover system and security weaknesses.



# Ethical Hacker Vs. Hacker

Ethical Hacker	Hacker
Done legally with permission of the relevant organization	Done illegally without the consent of the relevant organization
Done in an attempt to prevent malicious attacks from being successful	Done in an attempt to make malicious attacks possible
Disclose any vulnerabilities discovered	Exploit discovered vulnerabilities

# PENETRATION TESTING – “PENTESTING”

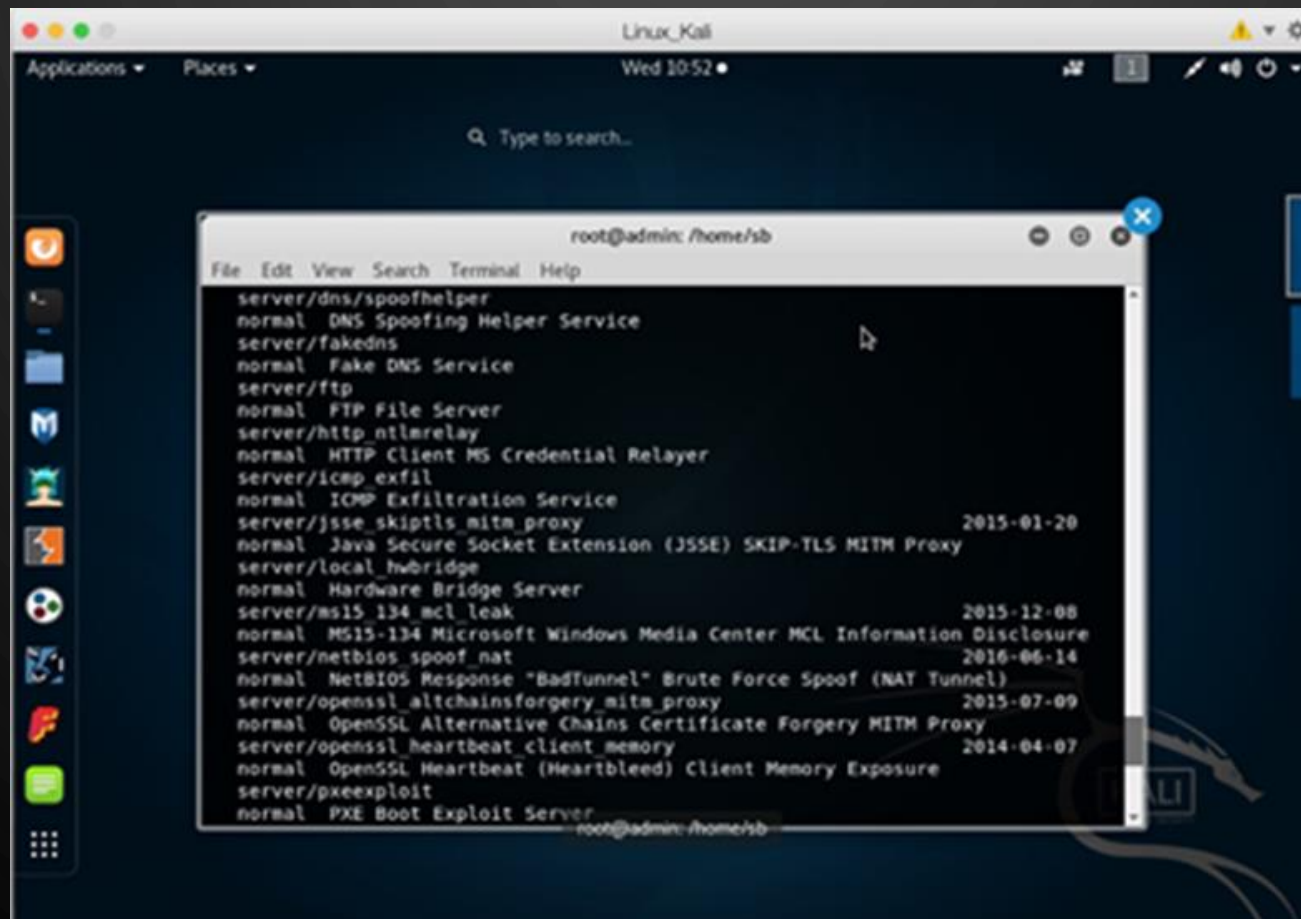
- One of the more popular pentesting facets is the [pentesting operating system](#). These operating systems are used to hack computers. Examples include Parrot OS, Network Security Toolkit, Pentoo Linux, Samurai Web Testing Framework, BlackBox, Caine OS, and Kali Linux. [The most popular is arguably Kali Linux.](#)

# Pentesting Operating Systems

## Kali Linux -

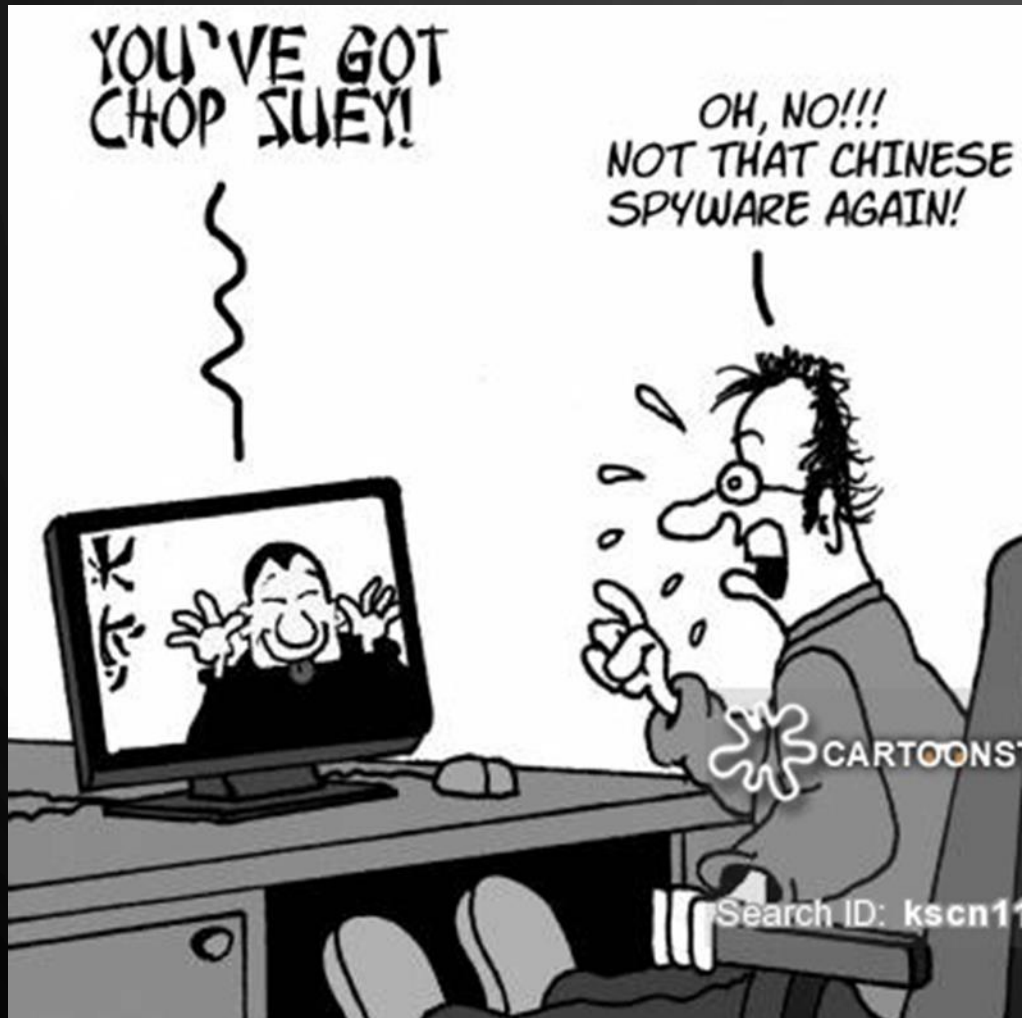


The software is a **command line application**. A flashing prompt is displayed in what is known as a terminal. The user **must** know the commands to use the software. **If you do not know the command lines, you cannot use the software.** Careful study and practice is needed to utilize the software.

A screenshot of a Linux desktop environment. The desktop background is dark blue with a faint dragon logo in the bottom right corner. A terminal window is open, displaying a list of services and their descriptions. The terminal window has a title bar that reads "root@admin: /home/sb". The list of services includes: server/dns/spoofhelper (normal DNS Spoofing Helper Service), server/fakedns (normal Fake DNS Service), server/ftp (normal FTP File Server), server/http\_ntlmrelay (normal HTTP Client MS Credential Relay), server/icmp\_exfil (normal ICMP Exfiltration Service), server/jsse\_skip\_tls\_mitm\_proxy (normal Java Secure Socket Extension (JSSE) SKIP-TLS MITM Proxy, dated 2015-01-20), server/local\_hwbriidge (normal Hardware Bridge Server), server/ms15\_134\_mcl\_leak (normal MS15-134 Microsoft Windows Media Center MCL Information Disclosure, dated 2015-12-08), server/netbios\_spoof\_nat (normal NetBIOS Response "BadTunnel" Brute Force Spoof (NAT Tunnel), dated 2016-06-14), server/openssl\_alchiansforgery\_mitm\_proxy (normal OpenSSL Alternative Chains Certificate Forgery MITM Proxy, dated 2015-07-09), server/openssl\_heartbeat\_client\_memory (normal OpenSSL Heartbeat (Heartbleed) Client Memory Exposure, dated 2014-04-07), and server/pxeexploit (normal PXE Boot Exploit Server). The terminal window also shows a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help".

```
Linux_Kali
Wed 10:52
Type to search...

root@admin: /home/sb
File Edit View Search Terminal Help
server/dns/spoofhelper
normal DNS Spoofing Helper Service
server/fakedns
normal Fake DNS Service
server/ftp
normal FTP File Server
server/http_ntlmrelay
normal HTTP Client MS Credential Relay
server/icmp_exfil
normal ICMP Exfiltration Service
server/jsse_skip_tls_mitm_proxy
normal Java Secure Socket Extension (JSSE) SKIP-TLS MITM Proxy 2015-01-20
server/local_hwbriidge
normal Hardware Bridge Server
server/ms15_134_mcl_leak
normal MS15-134 Microsoft Windows Media Center MCL Information Disclosure 2015-12-08
server/netbios_spoof_nat
normal NetBIOS Response "BadTunnel" Brute Force Spoof (NAT Tunnel) 2016-06-14
server/openssl_alchiansforgery_mitm_proxy
normal OpenSSL Alternative Chains Certificate Forgery MITM Proxy 2015-07-09
server/openssl_heartbeat_client_memory
normal OpenSSL Heartbeat (Heartbleed) Client Memory Exposure 2014-04-07
server/pxeexploit
normal PXE Boot Exploit Server
root@admin: /home/sb
```



The American, Russian, and Eastern European markets traffic on **Darknet** markets.

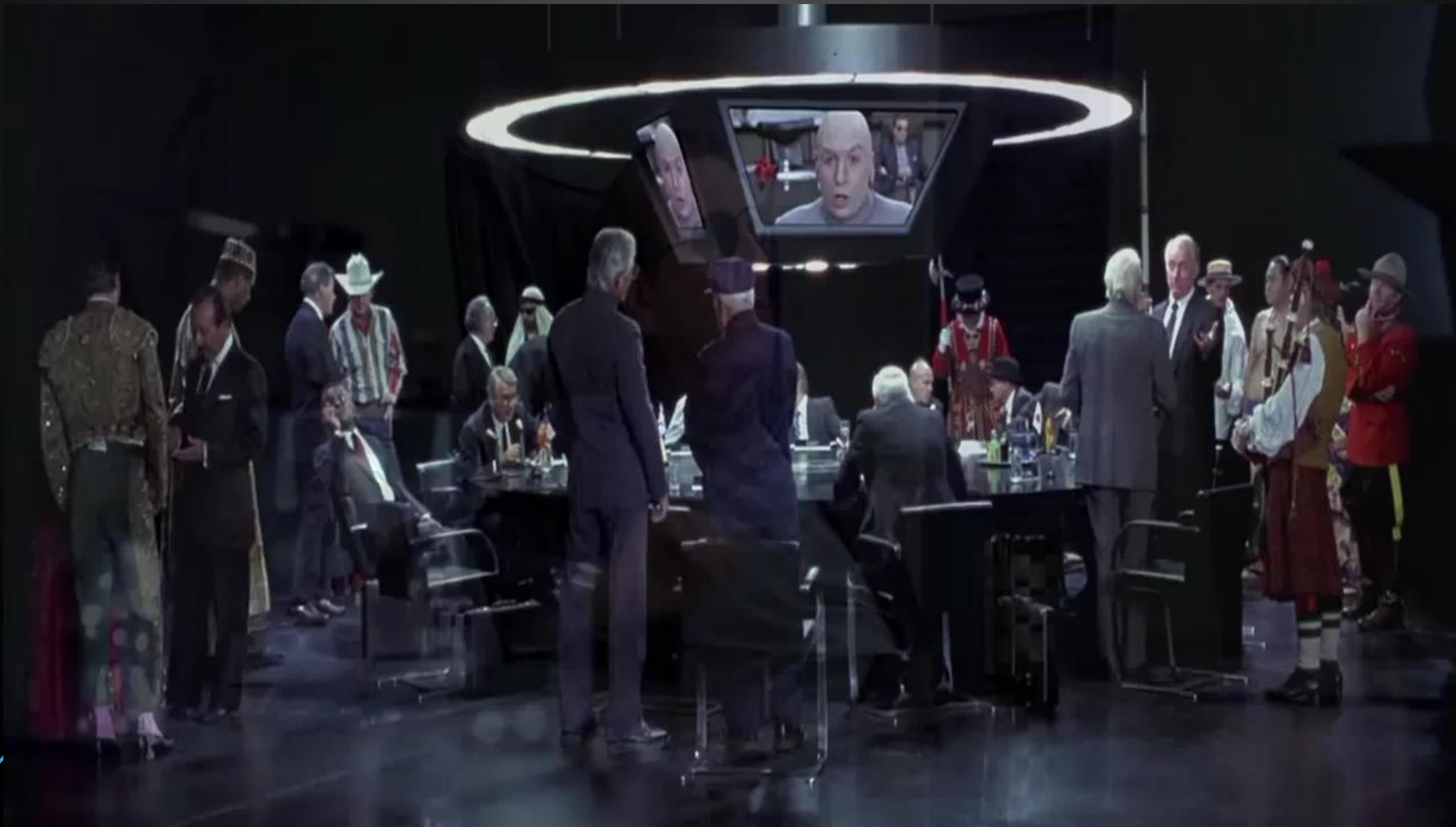
Chinese cybercrime gangs are involved in the entire gamut of cybercrimes, from selling illicit software to hack or disable a website to custom service requests tailored for the client.

The image features a dark gray background with a subtle pattern of concentric circles. In the four corners, there are stylized, light blue circuit board traces with small circular nodes, resembling a digital or technological theme.

**EXTORTION!!!**

**MUHAHAHAHAHA!!!**

**EXTORTION!!! MUHAHAHAHAHA!!!**



**Extortion** of existing computer resources primarily takes two forms: making existing victim-owned **software unusable** and **brute threats**. The former is known as **Ransomware**, which is designed to **encrypt a systems data pending a payment** for release.

## YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

**To unlock the computer you are obliged to pay a fine of \$200.**

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your  in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address [fine@fbi.gov](mailto:fine@fbi.gov).



OK

# RANSOMWARE

- **Ransomware** is malicious software that either prevents a user from accessing a computer system or encrypts existing data until a ransom is paid (usually in **Bitcoin**).
- **Ransomware** is designed to encrypt a system's data pending a payment for release. Oftentimes the data is not released, but is destroyed or remains encrypted.
- **Ransomware** is commonly delivered via email or through visiting a website



The worst ransomware attack in history was **WannaCry**, launched in 2017. In **four days** WannaCry had spread to over **250,000** computers.

WannaCry encrypts the hard drive, preventing access to user files.  
WannaCry demanded \$200 in bitcoin to release the data back to the user.

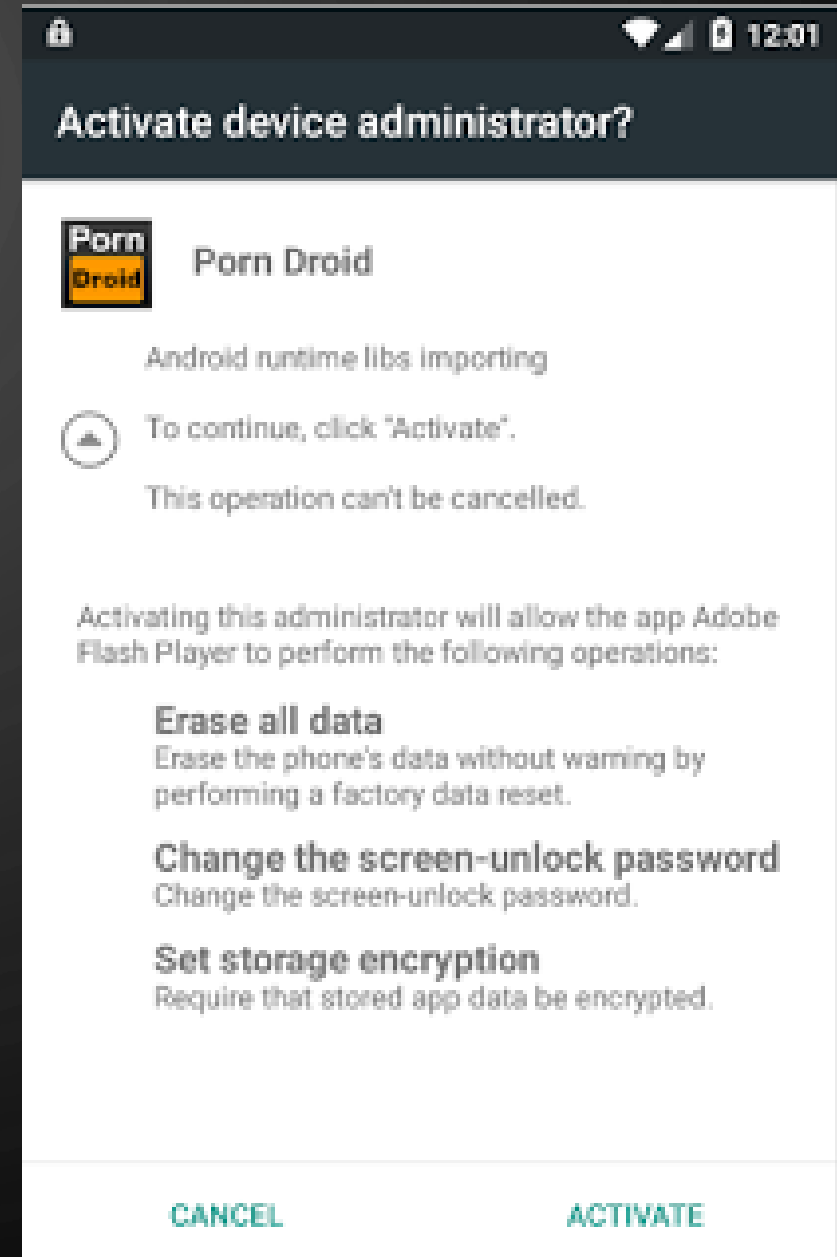




Computer security software company, Symantec believes WannaCry is linked to **The Lazarus Group**, a cybercrime group suspected of ties with **North Korea**.

# RANSOMWARE ON CELL PHONES

- Ransomware is evolving from computers to cell phones. “**Porn Droid**” targeted Android users. Hackers could remotely lock the phone by changing the PIN.





The ransom was commonly **\$500**. Software security company Symantec estimates about 3% of “hostages” pay the ransom, usually negotiated down to \$200. Symantec estimated one specific ransomware group was **generating \$34,000 daily**.

# Extortion

**Behzad Mesri**, who went by “Skote Vahshat” allegedly **stole 1.5 terabytes of data** from HBO in an effort to extort **\$6 million** worth of Bitcoin.

Included in the stolen data were unaired Emmy-award winning fantasy drama episodes of **Game of Thrones** (GOT)



# HBO®



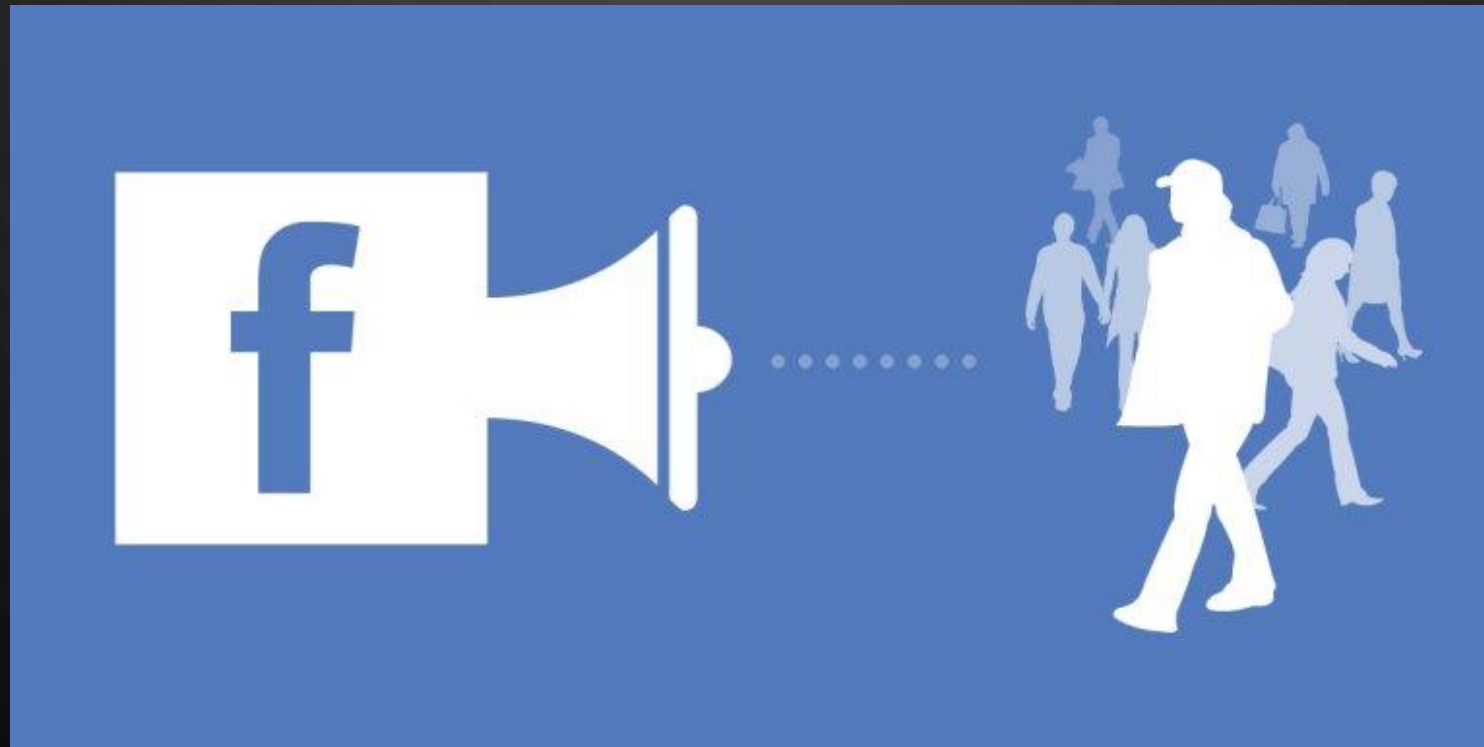
# BLACKMAIL ATTACKS

- Blackmail attacks are an emerging threat where a **hacker obtains access to Facebook, Google Drive, or a webcam** to threaten the victim with **revealing personally embarrassing photos or information** (such as sexting or pornography habits). The goal of the attack is to **convince the victim that the attacker has access to cellphone photos, online photos, and social media accounts**. Sometimes the hacker does have access; often it's a bluff. The attacker threatens to disclose this information if payment is not rendered within a specific time.

# WHAT IS THE BEST SOLUTIONS TO CAMERA HACKING?

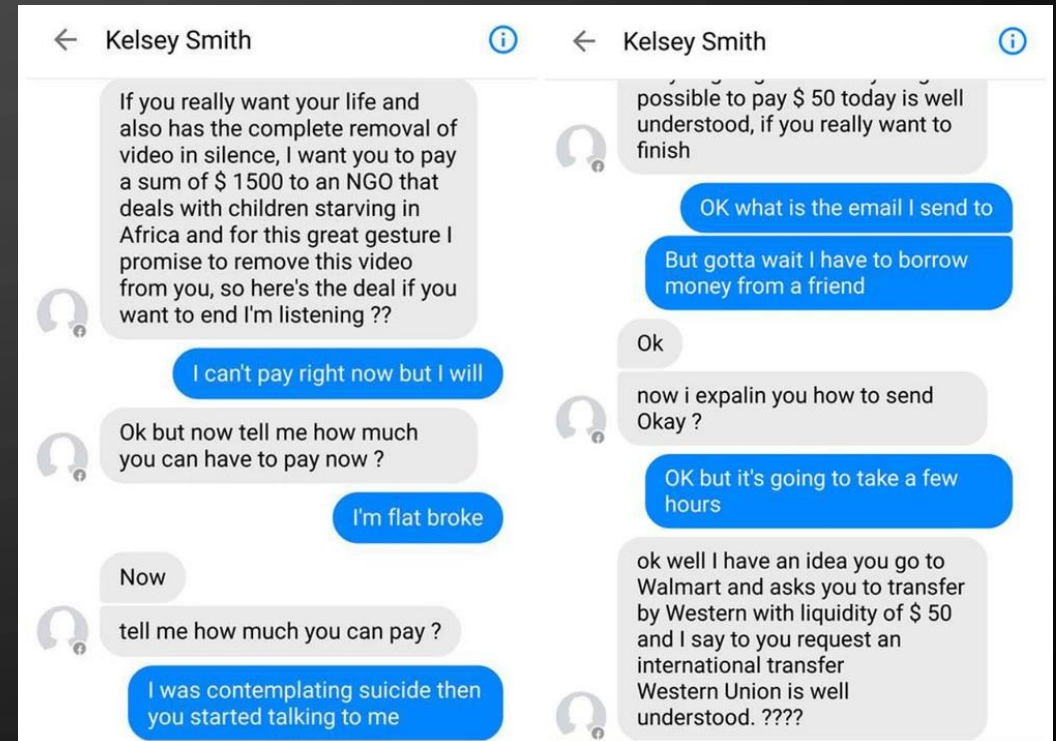


**THINK ABOUT WHAT INFO YOU SHARE ON  
SOCIAL MEDIA!!**





# Actual Blackmail Attempt



# DESTRUCTION



**Malware** is used to harm/disable a computer or an information system. Generally, malware consists of **worms** and **viruses**.



A **worm** can spread itself to a computer system, whereas a **virus** is usually introduced to a system via a “carrier”, such as a legitimate document sent from one computer to another. **Viruses** can also spread through **infected websites** or **emails**



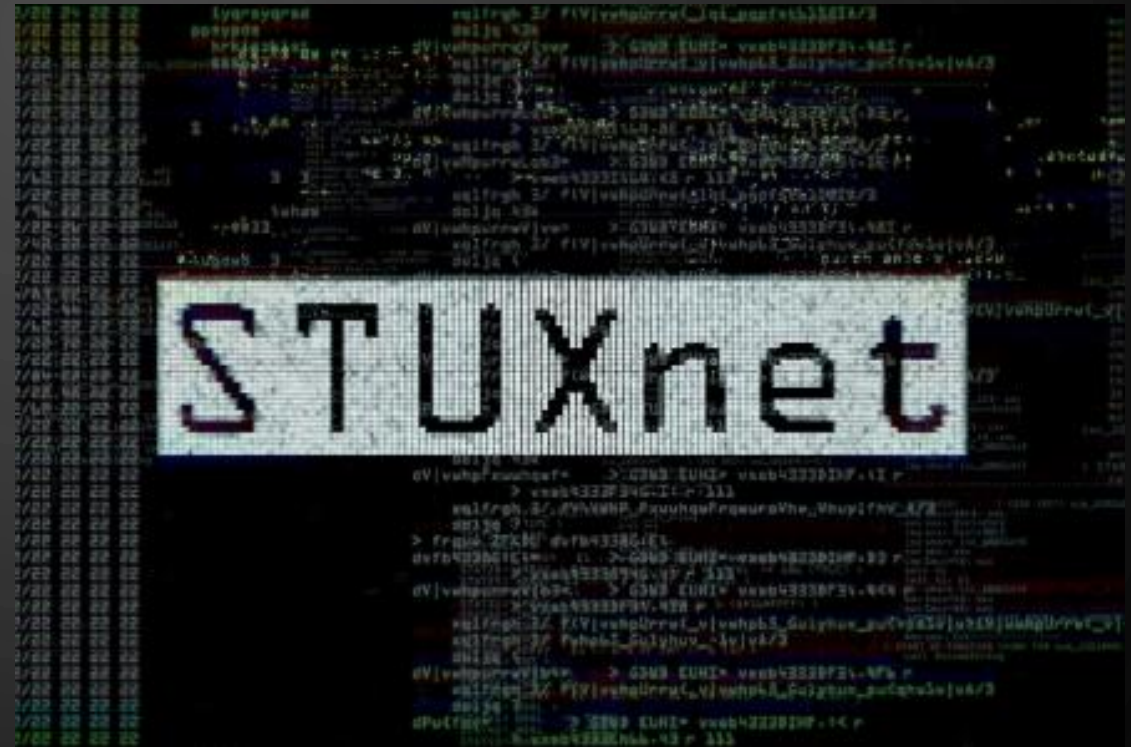
A **worm** harms a system by making copies of itself. These copies **deplete system resources**, such as **consuming hard drive space** (until the disk will no longer read/write) or **sapping system resources**, such as memory and bandwidth.



The most famous and effective worm of all time was **Stuxnet**.

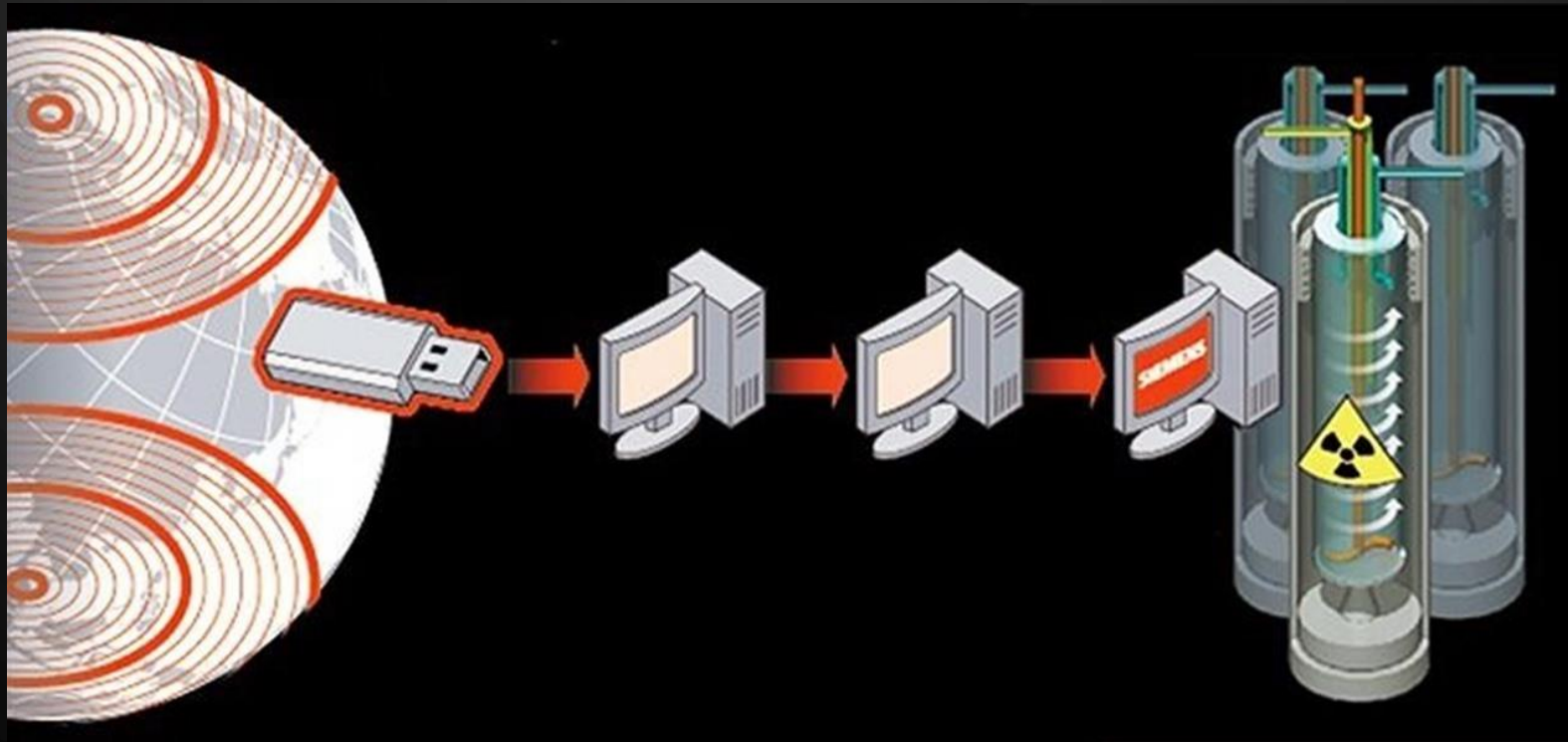
The NSA and Israeli Unit 8200 attacked the **Iranian uranium enrichment program**.

Considered the **first digital weapon**, the worm had one purpose: **alter the programmable logic controllers found on specific Siemens-manufactured uranium centrifuges**.

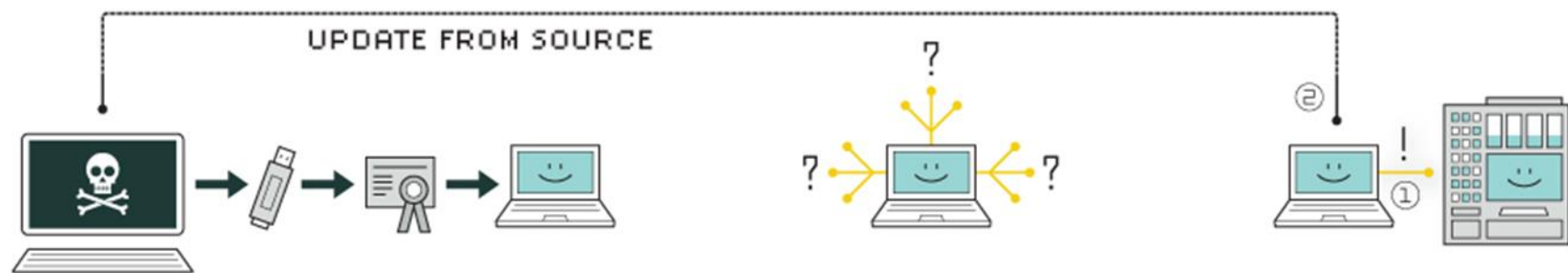


# STUXNET ATTACKED IRANIAN NUCLEAR PROGRAM

Stuxnet had to **replicate** itself to files and computers **across the world** until it found its way to the **Natanz nuclear facility** system.



# HOW STUXNET WORKED



## 1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

## 2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

## 3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



## 4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



## 5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



## 6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

# The Massive Iranian Hacking Incident of 2018



In March of 2018, the Trump administration confirmed another cyber-attack when it announced that accounts belonging to roughly **8,000 different professors at hundreds of U.S. and foreign universities, private companies and even government entities** were successfully broken into.

# THEFT AND CONVERSION

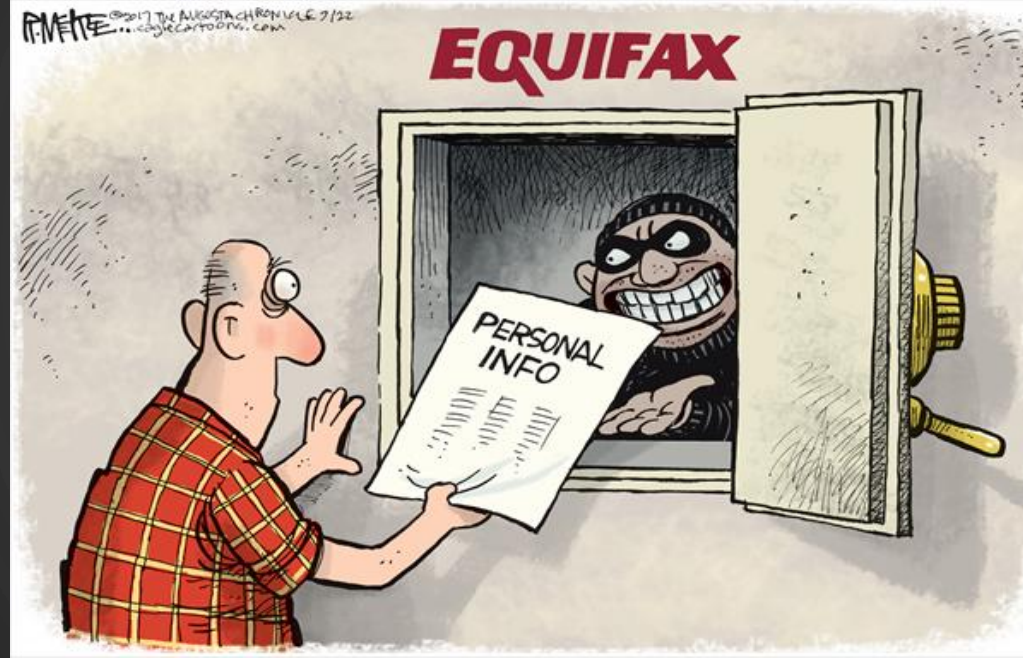
- Conversion of property is rampant on the online black markets known as **Darknet Markets**.
- Darknet vendors **sell active memberships to online services**, such as entertainment websites Netflix, Hulu, HBO Now, and Crunchyroll.
- Other account types are available, including music services such as Spotify and pornography memberships.

# THEFT AND CONVERSION

- These account credentials are harvested through various **passive and active means**, such as phishing scams and trolling low-security website communities.
- Many **users use the exact same usernames and passwords** across different sites.
- Some sites become “**honeypots**” for harvesting usernames and passwords for service sites, such as Netflix and Hulu.
- These **credentials are sold online** for usually \$5 for unlimited access to Netflix until the actual owner changes the password.
- Other services, like HBO, Spotify, and pornography credentials, are also available.

In 2017, the [Equifax web application tool](#), which is used by many major corporations, was **compromised** after the company failed to promptly install a security fix. Hackers took advantage of that flaw and stole personal data.





Roughly **2.4 million** of those affected by the breach only had their name and a portion of their **driver's license numbers leaked**, but millions of others had **private information stolen**, including full names, social security numbers, birthdates, address, and credit card numbers along with expiration dates.



March of 2018, Equifax reported that total number of American affected by the massive breach reached **147.9 million.**



# The Dark Web

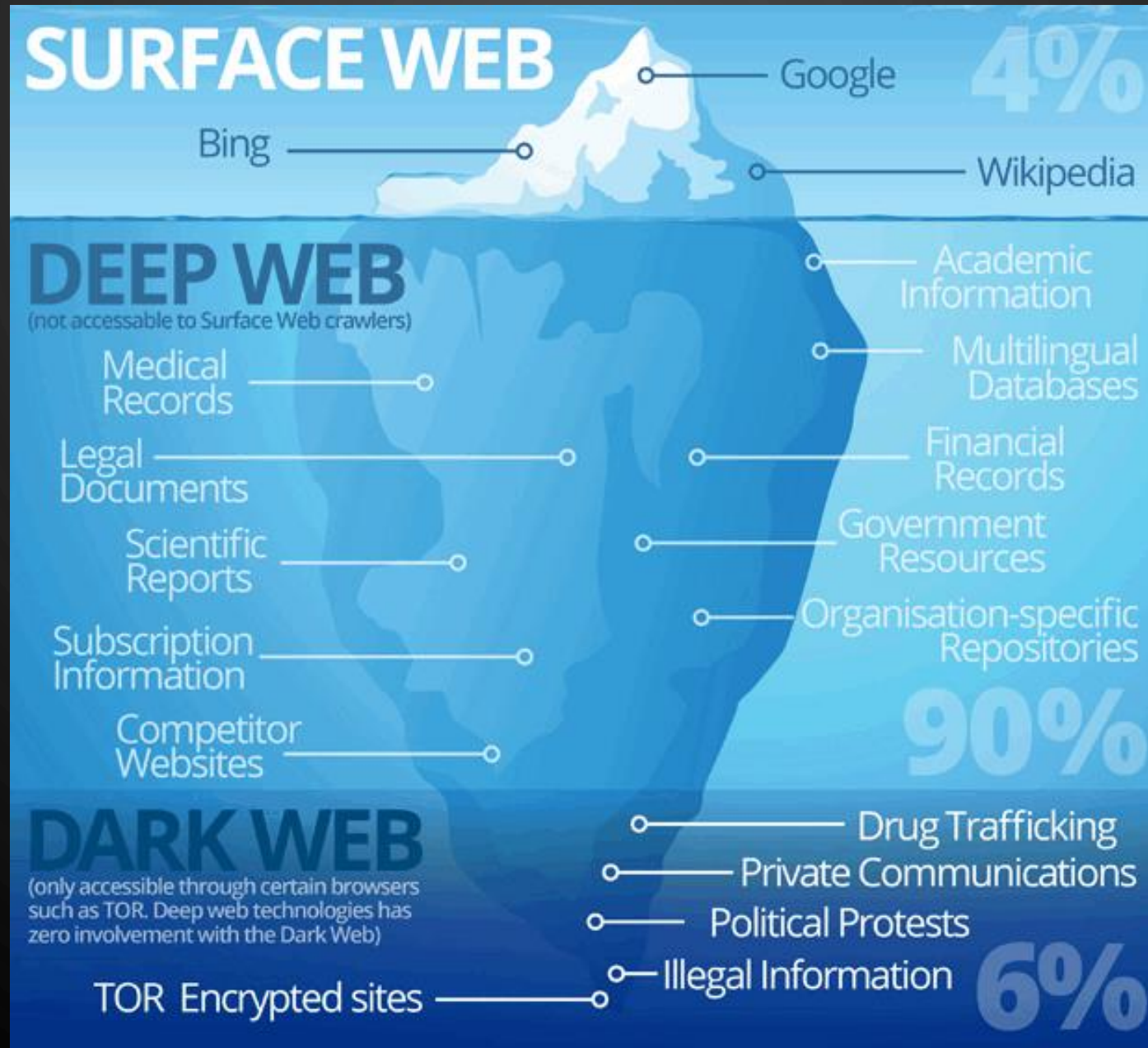
## DEEP WEB vs. DARK WEB

- **Deep Web**: It's all the data behind firewalls. Think user databases, business intranets, web archives, password-protected websites, etc.
- **Dark Web**: refers to a set of accessible, albeit anonymously hosted, websites that exist within the Deep Web.

# ONLY 4% OF THE INTERNET IS PUBLIC



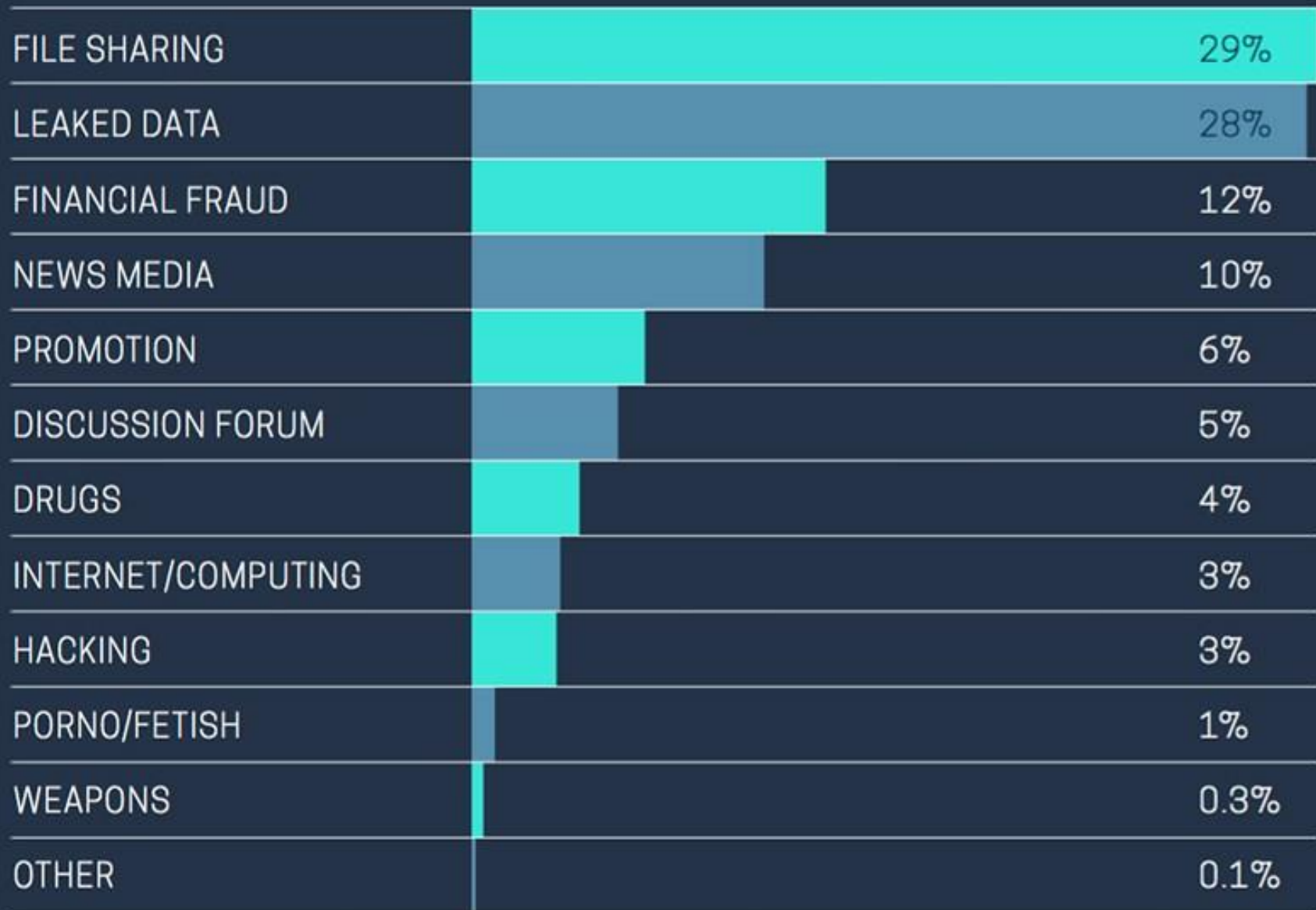
# 90% IS SECRET FOR A REASON = DEEP WEB



# Internet > Deep Web > Dark Web



# WHAT IS ACTUALLY IN THE DARK WEB?





# WHAT IS THE DARK WEB?



## ACTORS

Those who lurk beyond the shadows of the Darknet

**Public**

- Politically Oppressed
- Socially Disenfranchised
- Whistle Blowers
- Illicit Product/Service Buyers

**Government**

- Agencies
- Contractors
- Researchers

**Criminals**

- Drug Cartels
- Organized Crime
- Human Trafficking

**xHATs**

- Script Kiddies
- White Hats
- Gray Hats
- Black Hats

**Terrorists**

- Political Terrorists
- Environmental Terrorists
- Religious Terrorists

## CRYPTOCURRENCY

Greasing the wheels of the Darknet



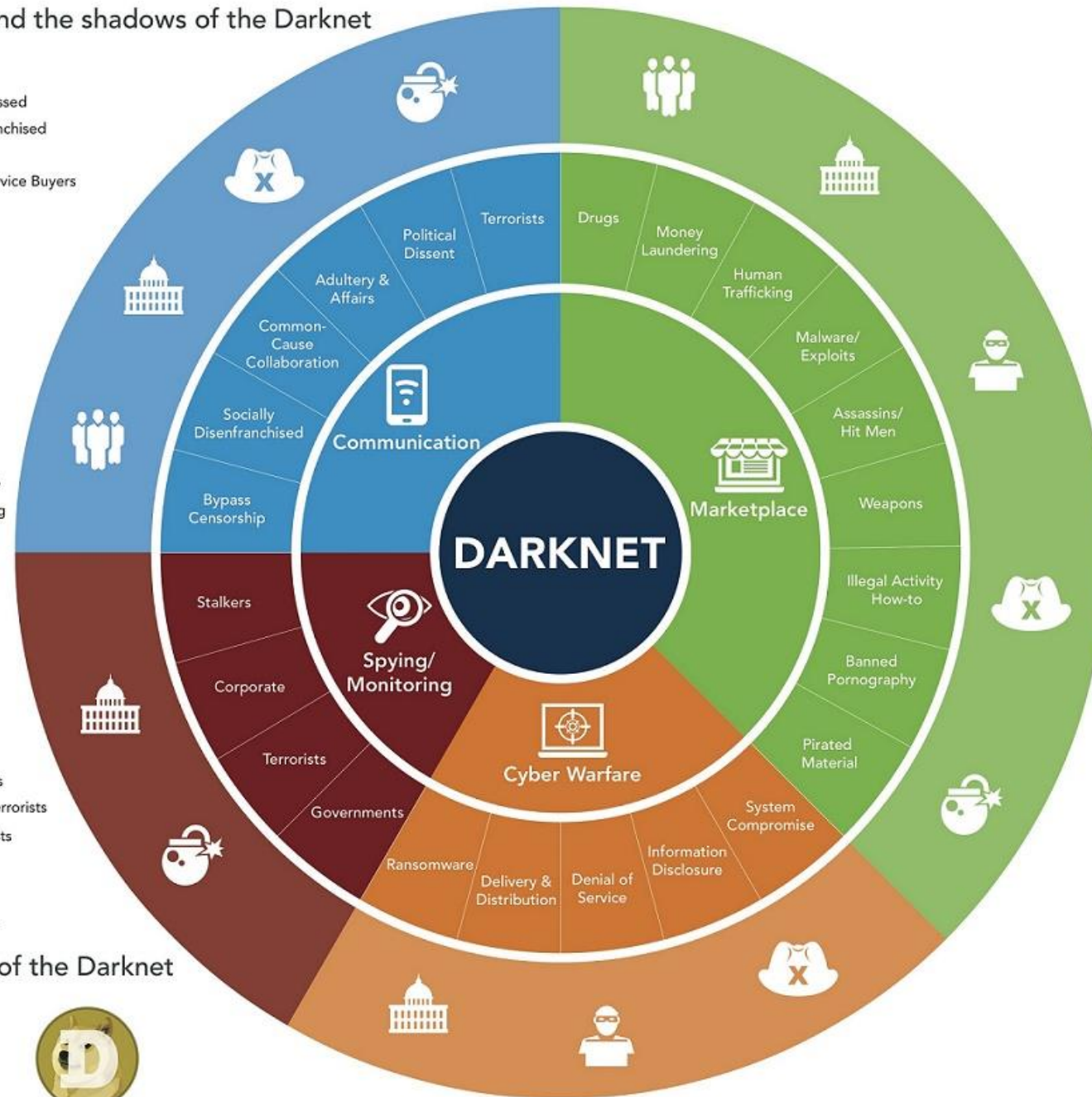
Bitcoin



Litecoin



DogeCoin





Most Darknet markets are on the Deepweb. The Darknet takes advantage of the Deepweb system. The Deepweb allows for sites that want traffic to be configured and hide in the vastness of the Deepweb. These “hidden services” hide the IP address, and ultimately the physical address, because IP’s are assigned and known.

## Darknet Markets

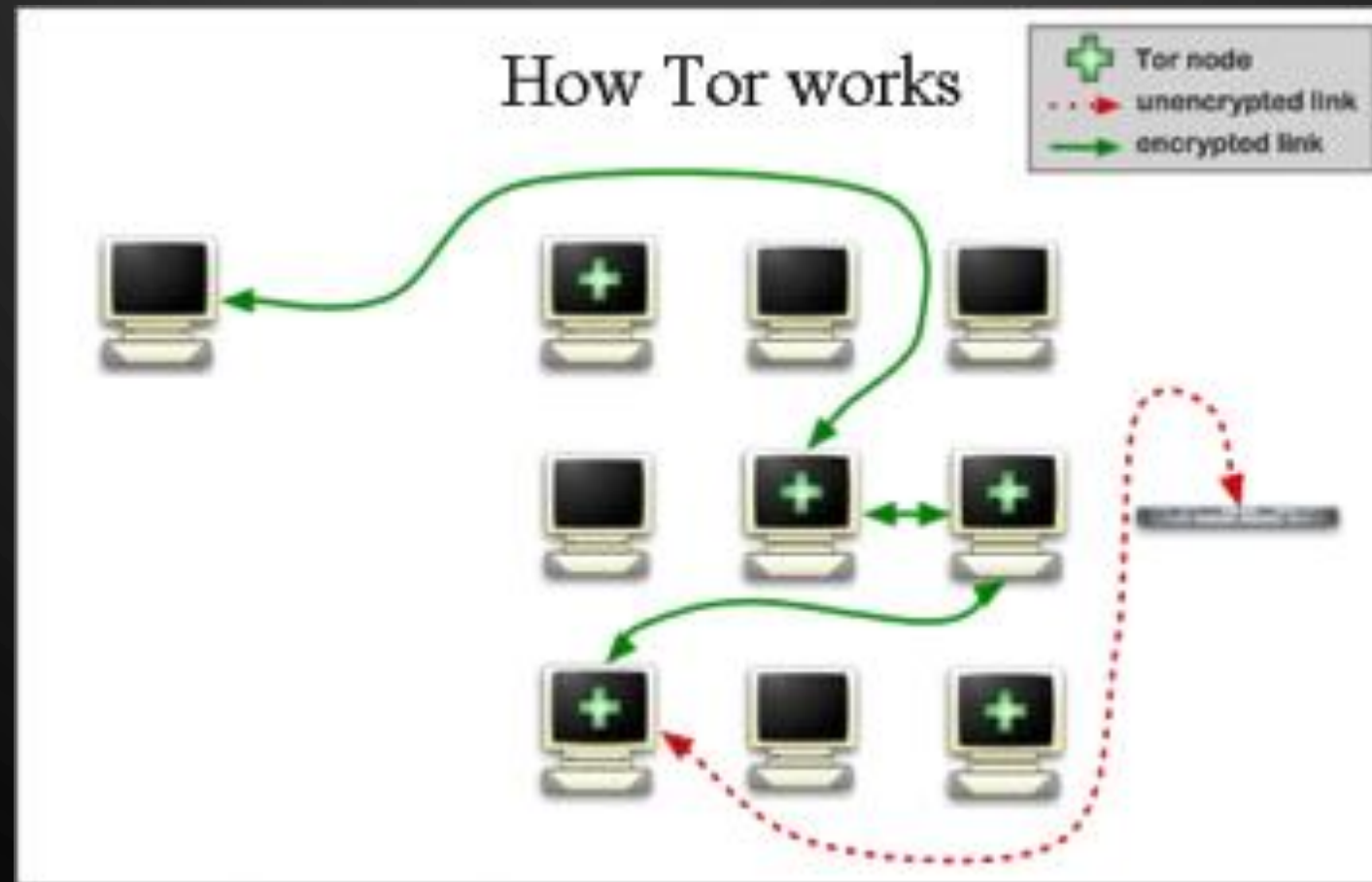


Tor Browser Icon


Tor can be used to connect to **Darknet markets.**

Darknet markets are **online retailers**, similar to eBay, that matches **private buyers with sellers for illegal transactions.**

**Tor**, a software developed in the 1990's to support government espionage. The **United States Navy developed Tor** to help people use the internet **anonymously** throughout the world; regardless if a country's internet was **monitored** and **restricted**.



# SILK ROAD IS GONE BUT...

 **AlphaBay Market**

Logged in as  
Current balance: BTC 0.0000  
[Autoshop](#) [Logout](#)

USD 320.41 CAD 425.97 EUR 297.92 AUD 449.27 GBP 210.56

HOME SALES MESSAGES LISTINGS BALANCE ORDERS FEEDBACK FORUMS CONTACT

Search Results

BROWSE CATEGORIES

☐ Fraud10520

☒ Drugs & Chemicals36550

- ☐ Benzos2920
- ☐ Cannabis & Hashish10856
- ☐ Dissociatives816
- ☐ Ecstasy5525
- ☐ Opioids2852
- ☐ Prescription2499
- ☐ Steroids1038
- ☐ Stimulants6004
- ☐ Tobacco155
- ☐ Weight Loss108
- ☐ Other648
- ☐ Paraphernalia264
- ☐ Psychedelics2865

☐ Guides & Tutorials4682

☐ Counterfeit Items1922


☐ Digital Products4350

☐ Jewels & Gold587

☐ Weapons633

☐ Carded Items1014

Search Results [\[Save Search\]](#)



[MS] [Sticky] ALL YOU HAVE TO KNOW TO BE SAFE! \*FREE(TO MAKE THIS COMMUNITY SAFER)

Item # 51105 - Other / Other - Nesquik7 (4930)


Views: 14991 / Bids: Fixed price

Quantity left: Unlimited (2046 automatic items)

Buy price

USD 0.00

(0.0000 BTC)



[FE 100%] [Sticky] 1g Best MDMA Crystals 84%+ Pure!

Item # 29299 - Ecstasy / MDMA - DrugsFromGermany (1184)


Views: 14721 / Bids: Fixed price

Quantity left: Unlimited

Buy price

USD 20.43

(0.0638 BTC)



[FE 100%] [Sticky] ISALE!5g Amphetamine Paste 100%Speed 74%Pure A++

Item # 16885 - Stimulants / Speed - DrugsFromGermany (1184)


Views: 13949 / Bids: Fixed price

Quantity left: Unlimited

Buy price

USD 21.51

(0.0671 BTC)



[MS] [Sticky] FB's MED. WEED - PURPLE KUSH (8.5/10) & PINK KUSH (9/10) [7 GRAMS]

Item # 12192 - Cannabis & Hashish / Buds & Flowers - ferrisbueller (350)

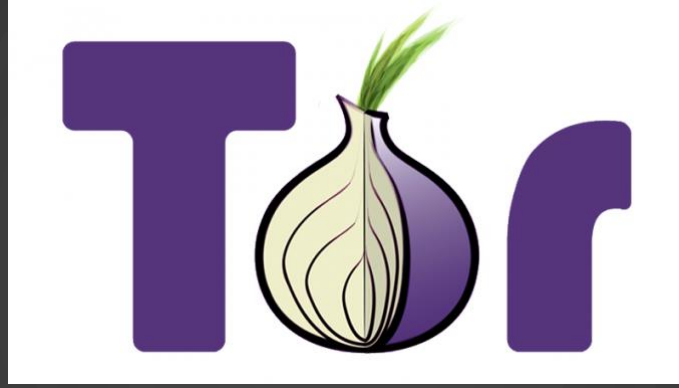
Views: 15595 / Bids: Fixed price

Quantity left: Unlimited

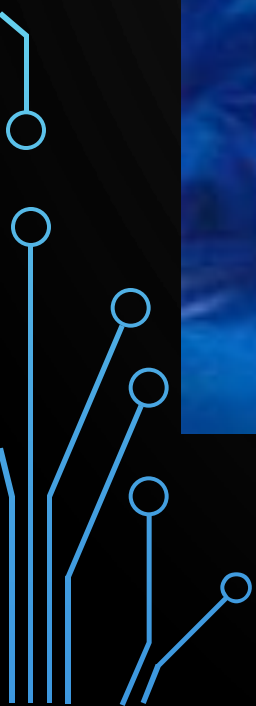
Buy price

USD 70.00

(0.2185 BTC)



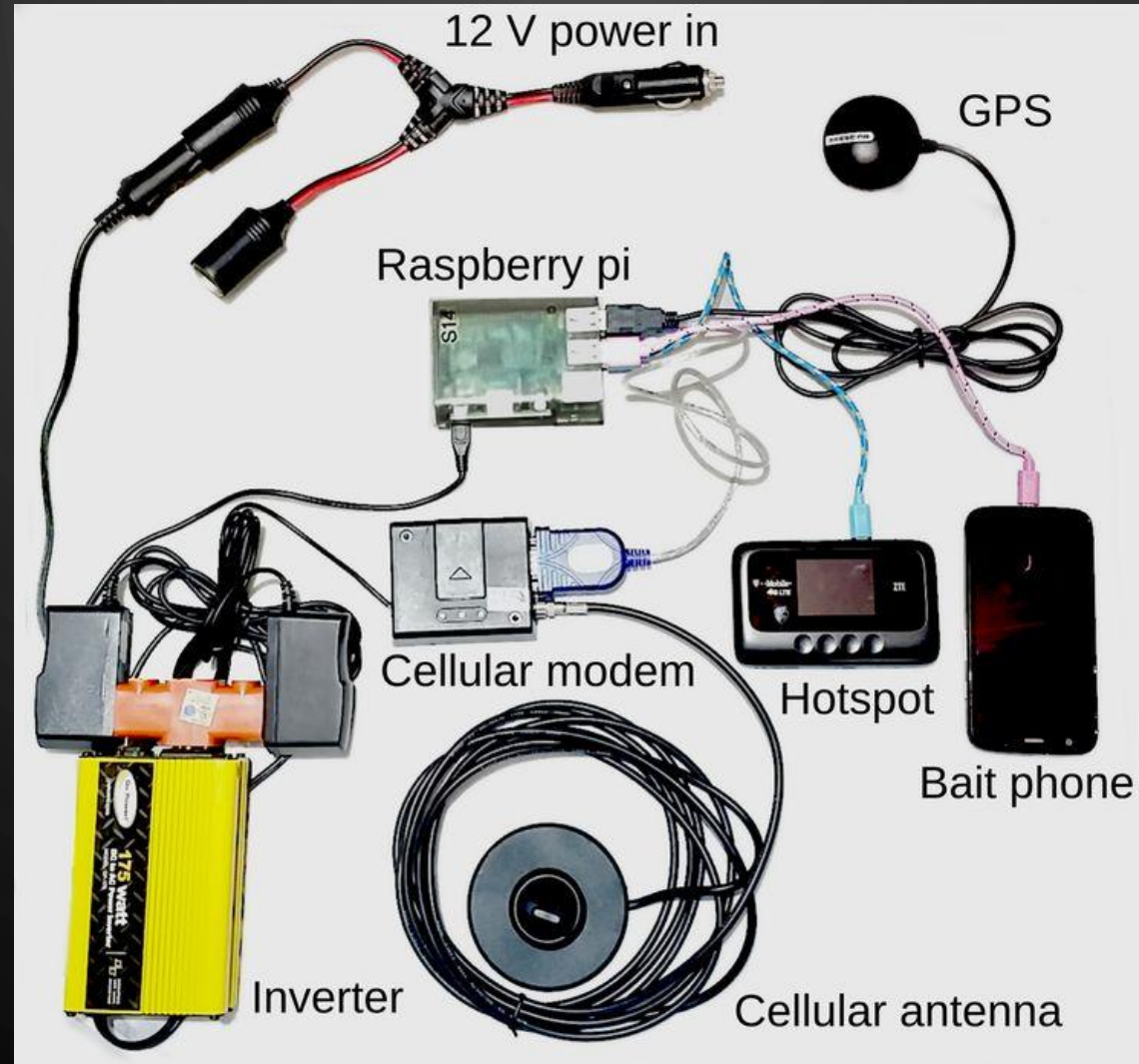
- Commonly purchased items include:
  - drugs,
  - hacking software,
  - hacking services,
  - stolen passwords and logins,
  - fake documents (such as prestigious degrees),
  - credit card information,
  - hacker appliances,
  - firearms, and illegal 3D printed items (such as serialized firearm parts).



# IMSI CATCHERS ACT AS WI-FI



# MAKE YOUR OWN IMSI



# IMSI CATCHERS



# BUY ONE ONLINE



Sourcing Solutions ▾

Services & Membership ▾

Help & Community ▾

One Request

☰ Categories ▾

Products ▾

What are you looking for...

🔍 Search

👤 [Sign In](#) | [Join Free](#)  
My Alibaba

About 1493 results: VoIP Products (1116) , Other Telecommunications Products (12) , Modems (5)

Home > Products > Telecommunications > Communication Equipment > Other Telecommunications Products (98941) 📧 [Subscribe to Trade Alert](#)



IMSI catcher

FOB **Reference** Price: [Get Latest Price](#)

**US \$1,800** / Unit | 1 Unit/Units (Min. Order)

✉ [Contact Supplier](#)

💬 [Leave Messages](#)

♥ [Add to Favorites](#)

Payment: This supplier also supports Western Union payments for offline orders.

🔍 [View larger image](#)

ZOOM

Share to: [f](#) [t](#) [in](#) [p](#)

**BE AFRAID, BE VERY AFRAID!!!**



# LAWS TO FIGHT CYBERCRIMES



# COMPUTER FRAUD AND ABUSE ACT (CFAA 1986)

## The Computer Fraud And Abuse Act



The CFAA criminalizes entering a computer without **authorization, or exceeding authority** within a computer system; **recklessly/negligently damaging** a computer through intentional access; **computer extortion; trafficking in passwords**; and **intentional damage** through knowing transmission.



# 18 USC 1030 FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

1. Computer Espionage
  2. Obtaining Information by Unauthorized Computer Access
  3. Trespassing in Government Cyberspace
  4. Computer Fraud
  5. Causing Computer Damage
  6. Trafficking in Computer Access
  7. Extortionate Threats
- 
- 

# 18 U.S.C. § 1030 (a)(1): OBTAINING NATIONAL SECURITY INFORMATION

Whoever having **knowingly accessed** a computer **without authorization** or **exceeding authorized access**, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with **reason to believe that such information so obtained could be used to the injury of the United States**, or to the advantage of any foreign nation willfully **communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted**, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it...

# LATEST MUELLER INDICTMENT OF RUSSIANS

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

VIKTOR BORISOVICH NETYKSHO,  
BORIS ALEKSEYEVICH ANTONOV,  
DMITRIY SERGEYEVICH BADIN,  
IVAN SERGEYEVICH YERMAKOV,  
ALEKSEY VIKTOROVICH  
LUKASHEV,  
SERGEY ALEKSANDROVICH  
MORGACHEV,  
NIKOLAY YURIEVICH KOZACHEK,  
PAVEL VYACHESLAVOVICH  
YERSHOV,  
ARTEM ANDREYEVICH  
MALYSHEV,  
ALEKSANDR VLADIMIROVICH  
OSADCHUK,  
ALEKSEY ALEKSANDROVICH  
POTEMKIN, and  
ANATOLIY SERGEYEVICH  
KOVALEV,

Defendants.

CRIMINAL NO.

(18 U.S.C. §§ 2, 371, 1030, 1028A, 1956,  
and 3551 et seq.)

RECEIVED

JUL 13 2018

Clerk, U.S. District & Bankruptcy  
Courts for the District of Columbia

\*\*\*\*\*  
INDICTMENT

The Grand Jury for the District of Columbia charges:

COUNT ONE  
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

# 18 U.S.C. § 1030 (a)(2): ACCESSING A COMPUTER AND OBTAINING INFORMATION

Whoever **intentionally accesses** a computer **without authorization** or **exceeds authorized access**, and thereby obtains—

- (A) information contained in a **financial record of a financial institution**, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- (B) **information from any department or agency of the United States**; or
- (C) information from **any protected computer**

# 18 U.S.C. § 1030 (a)(3): TRESPASSING IN A GOVERNMENT COMPUTER

Whoever **intentionally, without authorization to access any nonpublic computer** of a **department or agency of the United States**, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

## 18 U.S.C. § 1030 (a)(4): COMPUTER FRAUD

Whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

# 18 U.S.C. § 1030 (a)(5): CAUSING COMPUTER DAMAGE

- Whoever :
- (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
- (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
- (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

# 18 U.S.C. § 1030 (a)(6): TRAFFICKING IN COMPUTER ACCESS

Whoever knowingly and with intent to defraud traffics in any password or similar information through which a computer may be accessed without authorization, if--

- (A) such trafficking affects interstate or foreign commerce; or
- (B) such computer is used by or for the Government of the United States

# 18 U.S.C. § 1030 (a)(7): EXTORTIONATE THREATS

Whoever with **intent to extort** from any person any money or other thing of value, **transmits in interstate or foreign commerce** any communication containing any--

- **(A) threat to cause damage to a protected computer;**
- **(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information** obtained from a protected computer without authorization or by exceeding authorized access;  
or
- **(C) demand or request for money or other thing of value in relation to damage to a protected computer,** where such damage was caused to facilitate the extortion;



# 18 U.S.C. § 2252— CHILD PORNOGRAPHY STATUTES

- Possession, Receipt, and Distribution of Child Pornography
  - Topic for another Presentation
- 
- 
- 

## FBI's IC3

In 2000, the FBI established the Internet Fraud Complaint Center to serve as a tool for the public to easily report suspected internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners.

In 2003, it was renamed the Internet Crime Complaint Center, or “IC3”, to better reflect the vast amount of cyber crimes that are referred to it



Report  
**Internet Crime**  
to the **FBI**  
**[www.ic3.gov](http://www.ic3.gov)**



# Fight Online Sex Trafficking Act 2018

## Stop Enabling Sex Traffickers Act 2018

FOSTA and SESTA **toughen penalties for web services that facilitate prostitution.** The goal was to **reduce sex trafficking** occurring legally online under previous laws that protected forums from content posted by third parties.

The most infamous sex-trafficking website was **www.backpage.com**. The site primarily hosted sex work advertisements. The site, and others, has undoubtedly been used to promote forced and coerced sexual activities from both adults and minors.



# KILLING PERSONAL ADS – FOSTA-SESTA

- In April of 2018, **President Trump signed into law a set of CONTROVERSIAL BILLS** with the intention of fighting online illegal sex trafficking
- House Bill – FOSTA (Fight Online Sex Trafficking Act)
- Senate Bill – SESTA (Stop Enabling Sex Traffickers Act)
- Both were hailed by advocates as a victory for sex trafficking victims



## THE PROBLEM – WHAT ABOUT “SAFE HARBOR?”

- Section 230 of the 1996 Communications Decency Act holds:
  - “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”

## THE PROBLEM — WHAT ABOUT “SAFE HARBOR?”

- FOSTA-SESTA **creates an exception to Section 230 that means website publishers *would* be responsible if third parties are found to be posting ads for prostitution — including consensual sex work — on their platforms.**

## THE PROBLEM – WHAT ABOUT “SAFE HARBOR?”

- In response, numerous websites took action to censor or ban parts of their platforms in response — not because those parts of the sites actually were promoting ads for prostitutes, but because policing them against the outside possibility that they *might* was just too hard.

# THE PURPOSE – ELIMINATING BACKPAGE

- FOSTA-SESTA were intended specifically to fight Backpage.com & similar sites



# BACKPAGE.COM

- Backpage has long been known for its advertisements for sex workers (though these were formally removed from the site last year).
- As of late 2015, the site operated in nearly 900 cities around the world, and an independent appraiser valued it at as much as \$626 million.

# BACKPAGE.COM

- Backpage saw numerous controversies related to illegal sex work; authorities have arrested individuals using it to pay for sex, and Backpage has aided law enforcement in investigations into ads on its site
- But despite numerous attempts, authorities have continuously failed to hold Backpage accountable for the illegal content published on its site, largely because of Section 230

# THE FIGHT TO TAKE BACKPAGE DOWN

- In 2016, California Attorney General Kamala Harris announced the charges against Carl Ferrer, Michael Lacey and James Larkin in October and called the site “the world’s top online brothel.” Ferrer, the Backpage CEO, faced 11 counts related to pimping; Lacey and Larkin, newspaper publishers who founded the site in 2004 and sold it a decade later, each faced one count of pimping conspiracy.
- In December of 2016, California’s Superior Court dismissed all charges, citing the Communications Decency Act specifically in the dismissal

# THE FIGHT CONTINUED

- In January 2017, a Senate investigation ultimately found Backpage to be complicit in obscuring ads for child trafficking.



Backpage CEO, COO & Former owner being sworn in at Capitol Hill in January 2017

# THE FIGHT CONTINUED

- A month later, a documentary of survivors called *I Am Jane Doe* **focused on Backpage**, arguing that the safe harbor provision protecting Backpage from liability for ads on its sites should be done away with.

I AM  
JANE  DOE

SPEAK OUT. FIGHT BACK.

## THE FIGHT CONTINUED

- FOSTA and SESTA were created last year in response to the backlash, with the bill's creator specifically naming Backpage in an attempt to ensure that future lawsuits like the one dismissed in 2016 could move forward.

# FOSTA-SESTA SKEPTICISM

- Law Professor Eric Goldman warned “The bill would expose Internet entrepreneurs to additional unclear criminal risk, and that would chill socially beneficial entrepreneurship well outside the bill’s target zone”
- Critics argue that supporters of the bill fail to acknowledge the ways the internet makes it easier for sex workers to do their work safely, while also making it easier for law enforcement to document and gain evidence about illegal activity

# FOSTA-SESTA SKEPTICISM

- A coalition of sex workers, advocates, sex trafficking survivors, and even the Department of Justice have all strongly opposed the idea that FOSTA-SESTA is an effective deterrent to sex trafficking
- Critics argue that the bills endanger adults who want to do their job consensually & safely



# FOSTA-SESTA AT WORK

- FOSTA-SESTA **does not differentiate between various kinds of sex work & related content**
- This is big for states like **NEVADA**, where sex work can be done legally
- Despite these concerns, Congress overwhelmingly voted to pass both bills into law

# FOSTA-SESTA AT WORK

- Instead of directly targeting websites known to facilitate sex trafficking, the FOSTA-SESTA hybrid essentially sets up a template for “**broad-based censorship**” across the web.
- This means websites will have to decide whether to overpolice their platforms for potential prostitution advertisements or to underpolice them so they can maintain a know-nothing stance, which would likely be a very tricky claim to prove in court.

# FOSTA-SESTA AT WORK

- The bill's language penalizes any websites that “**promote or facilitate prostitution,**” and allows authorities to pursue websites for “knowingly assisting, facilitating, or supporting sex trafficking,” which is vague enough to threaten everything from **certain cryptocurrencies to porn videos to sites for perfectly legal escort services.**
- In short, the bills don't actually PREVENT sex work advertisements, they just let website owners know they have to SELF-POLICE

# FOSTA-SESTA SIDE-EFFECTS

- 2 days after SESTA passed in the Senate, **Craigslist removed its entire personals selection**
- Another longstanding escort service, Cityvibe — which **tacitly hosted** sex workers advertising under the guise of legal services like escorting and massages — **shut down altogether**



## FOSTA-SESTA SIDE-EFFECTS

- Furry-centric dating site Pounced.org also shut down overnight, leaving a lengthy note explaining that specific language in FOSTA undermined Section 230 in a way that made “sites operated by small organizations like pounced.org much riskier to operate.”

# FOSTA-SESTA SIDE-EFFECTS

- “We don’t promote prostitution or sex trafficking...We’re a personals site for the furry community. ... The problem is, with limited resources and a small volunteer staff, our risk for operating the site has now significantly increased.”
  - Pounddog.com letter

## FOSTA-SESTA SIDE-EFFECTS

- Internet freedom advocates have argued strenuously against FOSTA-SESTA
- One of the biggest fears surrounding the bill combo is that it could create room for more bills that attempt to create even more exemptions in Section 230

The background is dark gray with faint concentric circles. Cyan circuit-like lines with circular nodes are positioned in the corners: top-left, top-right, bottom-left, and bottom-right.

# **ELECTRONIC DEVICES & PRIVACY**

## **Electronic Device Searches & Case Law**

# *Riley v. California – Data is Different*

Privacy concerns of modern cell phones are much higher than other belongings

cellphones today “...are in fact minicomputers”  
that can easily be called “...cameras, video  
players, rolodexes, calendars, tape recorders,  
libraries, diaries, albums, televisions, maps, or  
newspapers.”

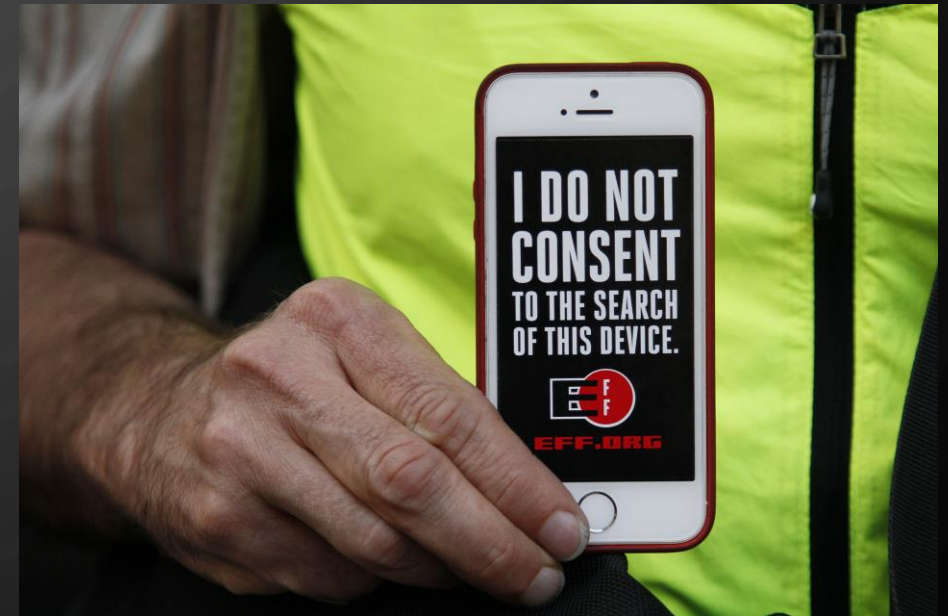
Must have a warrant to search a cell phone

Get a  
warrant.

*Riley v. California*, 573 U.S. \_\_\_\_ (2014)

## Does *Riley* apply to border searches?

From 2011 to 2017, the Department of Homeland Security (DHS) received roughly 250 complaints regarding individuals' laptops and phones being searched without a warrant as they crossed the United States border.



Lawyers have also been experiencing warrantless electronic searches of their belongings when traveling through the border. In April of 2017, the American Bar Association asked DHS to “require a subpoena based on probable suspicion” or a “warrant based on probable cause” before U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) search and review the content of lawyers’ laptop computers, cell phones, or other electronic devices



vs.



# CELL PHONE SEARCHES & THE BORDER

- For the first time since *Riley*, a federal appellate court ruled in *United States v. Kolsuz* that **forensic searches** of electronic devices **at the border require individualized suspicion** that the traveler is involved in criminal wrongdoing. *United States v. Kolsuz*, 2018 WL 2122085 (4th Cir. May 9, 2018), as amended (May 18, 2018)



# CELL PHONE SEARCHES & THE BORDER

- United States v. Kolsuz involved a traveler found with firearm parts in his luggage and charged with arms smuggling
- After defendant was detained at Washington Dulles International Airport, Customs & Border Protection officers took his phone, manually examined his recent communications, and then transported the device elsewhere for intensive forensic review
- That month-long search, per the court, “yielded an 896-page report that included Kolsuz’s personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, along with a history of Kolsuz’s physical location down to precise GPS coordinates”

# CELL PHONE SEARCHES & THE BORDER

- The month long forensic search yielded nearly 900 pages of Defendant's person data, including:
  - Contact lists / Call logs
  - Emails / Messenger conversations
  - Photos / Videos
  - Calendar
  - Web browsing history
  - GPS history, etc.



# CELL PHONE SEARCHES & THE BORDER

- While defendant chose not to challenge the manual search or the seizure of his phone, **Kolsuz moved to suppress the forensic report** on the grounds that investigators **should have been required to obtain a warrant first**
- The **district court denied the motion** and (relying in part on the report) convicted him at trial, Kolsuz appealed the denial
- Although the *Kolsuz* court ultimately affirmed the conviction based on the good-faith exception, the Fourth Circuit ruled that **authorities may no longer conduct forensic searches of electronic devices at the border without some degree of individualized suspicion**

# WHAT ABOUT THE FIFTH CIRCUIT?

- In March, the 5<sup>th</sup> Circuit decided *US v. Molina-Isidoro*
- In that case the defendant, Maria Isabel Molina-Isidoro's, cell phone was manually searched at the border, and data from the search was used to support a prosecution for attempting to import methamphetamine into the country



# WHAT ABOUT THE FIFTH CIRCUIT?

- The court held that the non-forensic search of defendant's cell phone at the border was supported by probable cause and thus, at a minimum, the border patrol agents had a good-faith basis for believing the search did not run afoul of the Fourth Amendment
- Accordingly, the court affirmed defendants' drug-related conviction and sentence



# BORDER SEARCHES & THE ELEVENTH CIRCUIT

- In March of 2018, the Eleventh Circuit decided [United States v. Vergara](#), where they rejected a child pornography defendant's argument that device searches require a warrant in the wake of *Riley*
- In *Vergara*, the defendant was returning home to Florida following a cruise to Cozumel, and had 3 phones in his possession
- Upon return, CBP agents manually searched one phone for about five minutes, discovering a picture of two topless female minors

# BORDER SEARCHES & THE ELEVENTH CIRCUIT

- CBP notified DHS, who decided to have all three phones forensically examined and found more than 100 images and videos of child pornography
- Veragara moved to suppress the evidence collected as a result of the warrantless searches, which was denied by the trial Court
- In a brief opinion, the Eleventh Circuit affirmed the denial and emphasized that Riley “expressly limited its holding to the search-incident-to-arrest exception” and that border searches “have long been excepted from warrant and probable cause requirements”
- Judge Jill Pryor stressed in dissent that *Riley*’s reasoning sweeps more broadly

# BORDER SEARCHES & CIVIL SUITS?

- The **number of electronic searches conducted at the border has skyrocketed** in the past few years, and so have complaints to DHS
- In September of 2013, the **EFF and the American Civil Liberties Union (ACLU)** **sued the federal government on behalf of 11 travelers** whose smartphone and other electronic devices were searched at the U.S. border without a warrant, arguing that the First and Fourth Amendments are violated when these border searches are done

# BORDER SEARCHES & CIVIL SUITS?

- In May of 2018, the **government sought to dismiss the case**, arguing that that the Fourth and First Amendments **do not provide protection from warrantless and suspicionless search** of electronic devices at the border and that the Plaintiffs **lacked standing to sue**
- The judge **rejected the arguments**, holding that the Plaintiffs **had standing to sue and that the case could move forward**
- The case, *Alasaad v. Nielsen*, is still pending in a U.S. District Court for the District of Massachusetts

# TEXAS PENAL CODE CYBERCRIMES



# TPC § 33.02(a). BREACH OF COMPUTER SECURITY

A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

Class B misdemeanor

# TPC § 33.02(b-1). BREACH OF COMPUTER SECURITY

A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses:

- (1) a computer, computer network, or computer system without the effective consent of the owner; or
- (2) a computer, computer network, or computer system:
  - (A) that is owned by: (i) the government; or (ii) a business or other commercial entity engaged in a business activity;
  - (B) in violation of: (i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or (ii) a contractual agreement to which the person has expressly agreed; and
  - (C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.

# PENALTIES

- Class C - less than \$100;
- Class B -  $\$100 < \$750$ ;
- Class A -  $\$750 < \$2,500$ ;
- State jail felony -  $\$2,500 < \$30,000$ ;
- 3<sup>rd</sup> Degree -  $\$30,000 < \$150,000$ ;
- 2<sup>nd</sup> Degree -  $\$150,000 < \$300,000$ ;
  - or  $< \$300,000$  and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility;
  - or the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system; or
- 1<sup>st</sup> Degree -  $> \$300,000$ 
  - Or the actor obtains the identifying information of another by accessing more than one computer, computer network, or computer system.

## TPC § 33.022. ELECTRONIC ACCESS INTERFERENCE

A person, other than a network provider or online service provider acting for a legitimate business purpose, commits an offense if the person **intentionally interrupts or suspends access** to a **computer system or computer network without the effective consent of the owner.**

3<sup>rd</sup> Degree Felony

## TPC § 33.023. ELECTRONIC DATA TAMPERING

A person commits an offense if the person **intentionally alters data as it transmits between two computers in a computer network** or computer system through deception and without a legitimate business purpose.

A person commits an offense if the person **intentionally introduces ransomware onto a computer, computer network, or computer system** through deception and without a legitimate business purpose.

## TPC § 33.024. UNLAWFUL DECRYPTION

- A person commits an offense if the person **intentionally decrypts encrypted private information** through deception and without a legitimate business purpose

# ELECTRONIC DATA TAMPERING/ UNLAWFUL DECRYPTION PENALTIES

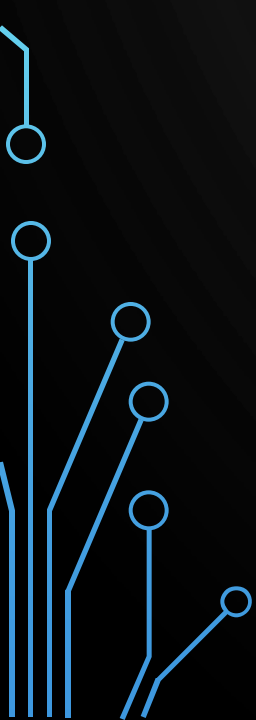
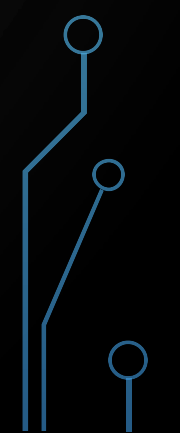
- Class C - less than \$100;
- Class B -  $\$100 < \$750$ ;
- Class A -  $\$750 < \$2,500$ ;
- State jail felony -  $\$2,500 < \$30,000$ ;
- 3<sup>rd</sup> Degree -  $\$30,000 < \$150,000$ ;
- 2<sup>nd</sup> Degree -  $\$150,000 < \$300,000$ ;
- 1<sup>st</sup> Degree -  $> \$300,000$

# OTHER TEXAS CYBERCRIME STATUTES

- TPC § 33.021. ONLINE SOLICITATION OF A MINOR
  - *Ex Parte Ingram* **Pre-2015 version upheld on writ but still ripe on direct Appeal**
- TPC § 33.07. ONLINE IMPERSONATION
- TPC § 21.15. INVASIVE VISUAL RECORDING
  - *Ex Parte Thompson* **RULED UNCONSTITUTIONAL - Amended**
- TPC § 21.16. UNLAWFUL DISCLOSURE OR PROMOTION OF INTIMATE VISUAL MATERIAL – Revenge Porn
  - *Ex Parte Jones* **RULED UNCONSTITUTIONAL\***



## *EX PARTE JONES*

- 12-17-00346-CR, 2018 WL 1835925 (Tex. App.—Tyler Apr. 18, 2018),
  - Petition for discretionary review filed 6/1/18.
- 
- 

# EX PARTE JONES - BACKGROUND

- Jones was charged by information with **unlawful disclosure of intimate visual material** (AKA the “revenge pornography” statute).
- On September 6, 2017, Jones filed an Application for Writ of Habeas Corpus, in which he argued that Texas Penal Code, Section 21.16(b) is **UNCONSTITUTIONAL ON ITS FACE**
- The trial court DENIED Jones's application, and the appeal followed

# EX PARTE JONES – THE “REVENGE PORN” STATUTE

- Section 21.16(b) sets forth, in pertinent part, as follows:
- A person commits an offense if:
  - (1) **without the effective consent** of the depicted person, the **person intentionally discloses visual material** depicting another person with the person's **intimate parts exposed or engaged in sexual conduct**;
  - (2) the visual material was **obtained** by the person or created **under circumstances** in which the depicted person had a **reasonable expectation** that the visual material would remain **private**;
  - (3) the disclosure of the visual material **causes harm** to the depicted person; and
  - (4) the disclosure of the visual material **reveals the identity** of the depicted person in any manner.

# EX PARTE JONES – ISSUE ONE – IT'S OVERBROAD

- Jones first argued that the statute was **OVERBROAD**
- **First Amendment—The Statute's Regulation of Free Speech**
  - “Because the **photographs** and **visual recordings** are inherently **expressive** and the First Amendment applies to the distribution of such expressive media in the same way it applies to their creation, we conclude that **THE RIGHT TO FREEDOM OF SPEECH** is implicated in this case.”

# EX PARTE JONES – ISSUE ONE – IT'S OVERBROAD

- Statute's Regulation of Speech: Content-Based or Content-Neutral?

- “The State CONCEDED at oral argument that 21.16(B) is subject to **STRICT SCRUTINY** analysis. We agree.”
- “Section 21.16(b)(1) penalizes only a subset of disclosed images, those which depict another person with the person's intimate parts exposed or engaged in sexual conduct. Therefore, we conclude that Section 21.16(b)(1) **discriminates on the basis of content.**”

# EX PARTE JONES – ISSUE ONE – IT'S OVERBROAD

- “The **State argues** in its brief that the expectation of privacy and the nonconsensual nature of the disclosure causes any **visual material** covered by [Section 21.16\(b\)](#) to be **unprotected speech** because it is contextually obscene. **We disagree.**”
- “Here, [Section 21.16](#) does not include language that would permit a trier of fact to determine that the visual material disclosed is obscene. Moreover, if, as the State argues, any visual material disclosed under [Section 21.16\(b\)](#) is obscene, the statute is wholly redundant in light of Texas’s obscenity statutes.”

## EX PARTE JONES – ISSUE ONE – IT'S OVERBROAD

- “Because [Section 21.16\(b\)](#) does not use the least restrictive means of achieving what we have assumed to be the compelling government interest of preventing the intolerable invasion of a substantial privacy interest, it is an invalid content-based restriction in violation of the First Amendment.”

## EX PARTE JONES – ISSUE ONE – IT'S OVERBROAD

- “Section 21.16 is **extremely broad**, applying to any person who discloses visual material depicting another person’s intimate parts or a person engaged in sexual conduct, but where the disclosing person has no knowledge or reason to know the circumstances surrounding the material’s creation, under which the depicted person’s reasonable expectation of privacy arose.”

## EX PARTE JONES – ISSUE ONE – IT'S OVERBROAD

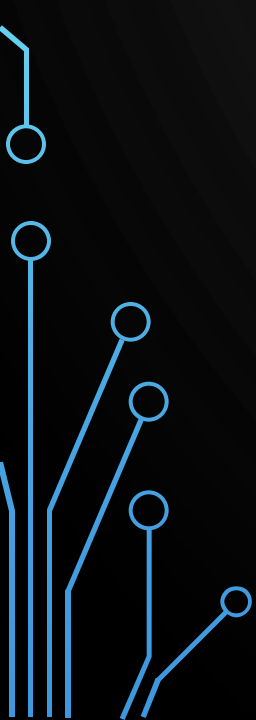

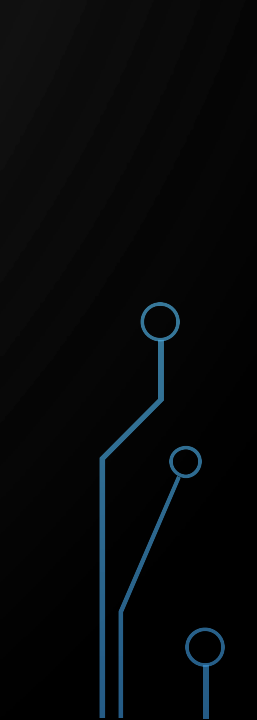
- “Furthermore, its application is not attenuated by the fact that the disclosing person had no intent to harm the depicted person or may have been unaware of the depicted person’s identity. Accordingly, we conclude that the criminal prohibition [Section 21.16\(b\)](#) creates is of ‘**alarming breadth**’ that is ‘**real**’ and ‘**substantial**’.”

## EX PARTE JONES – IN SUMMATION

- “We have concluded that [Section 21.16\(b\)](#) is an **invalid content-based restriction** and **overbroad** in the sense that it **violates rights of too many third parties** by restricting more speech than the Constitution permits. Accordingly, we hold that [Texas Penal Code, Section 21.16\(b\)](#), to the extent it proscribes the disclosure of visual material, is **unconstitutional on its face** in violation of the Free Speech clause of the First Amendment. Jones’s first issue is sustained.”



# TEXAS DPS COMPUTER INFORMATION TECHNOLOGY AND ELECTRONIC CRIME (CITEC) UNIT

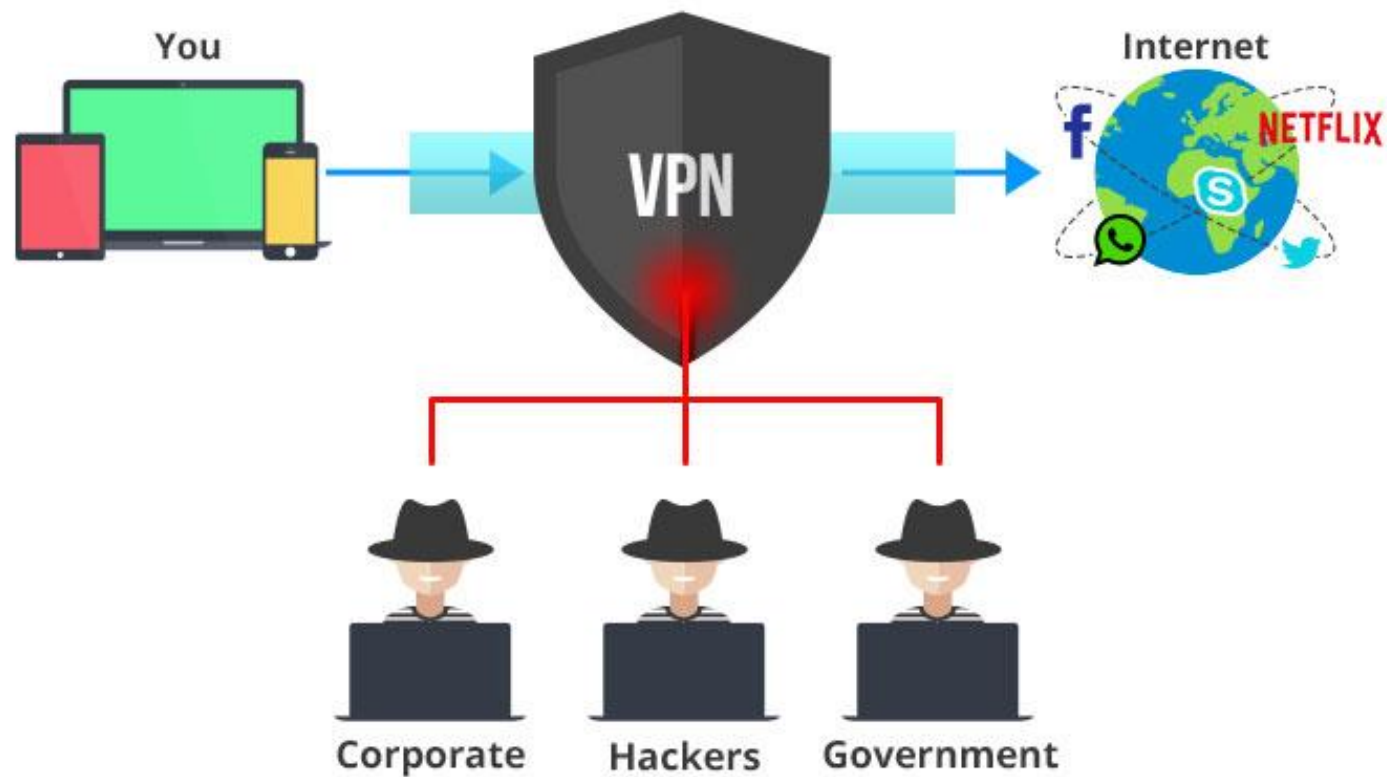
- CITEC Unit investigates non-traditional crimes where computer systems and the Internet are used to facilitate the crime or store evidence of a crime:
    - Network intrusions (hacking)
    - Denial-of-service attacks
    - Web site defacements
    - Identity theft/fraud
    - Electronic terroristic threats
    - Tampering with governmental records.
- 
- 
- 

# HOW TO STAY SAFE ON THE INTERNET?

- **Use a VPN**
- **Use different, ever changing, long passwords**
- **Use the Tor Browser**
- **Get a faraday bag**
- **Get a Cryptophone**
- **By some DuckTape**

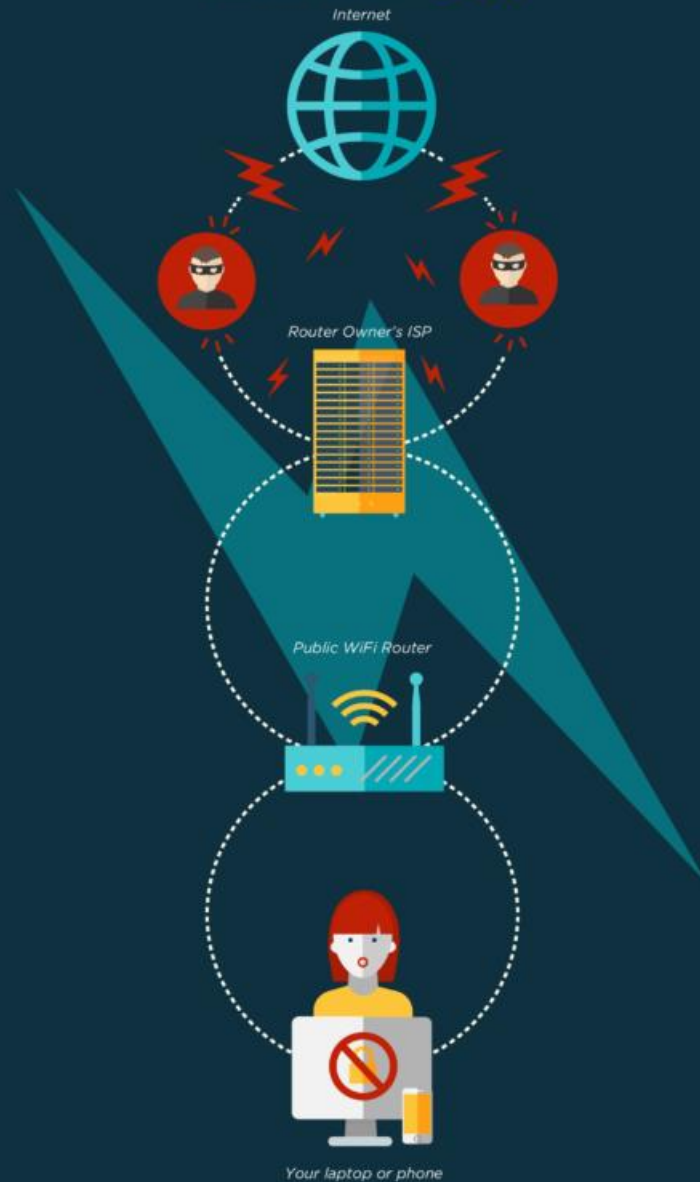
# USE A VPN

## How **VPN** works?

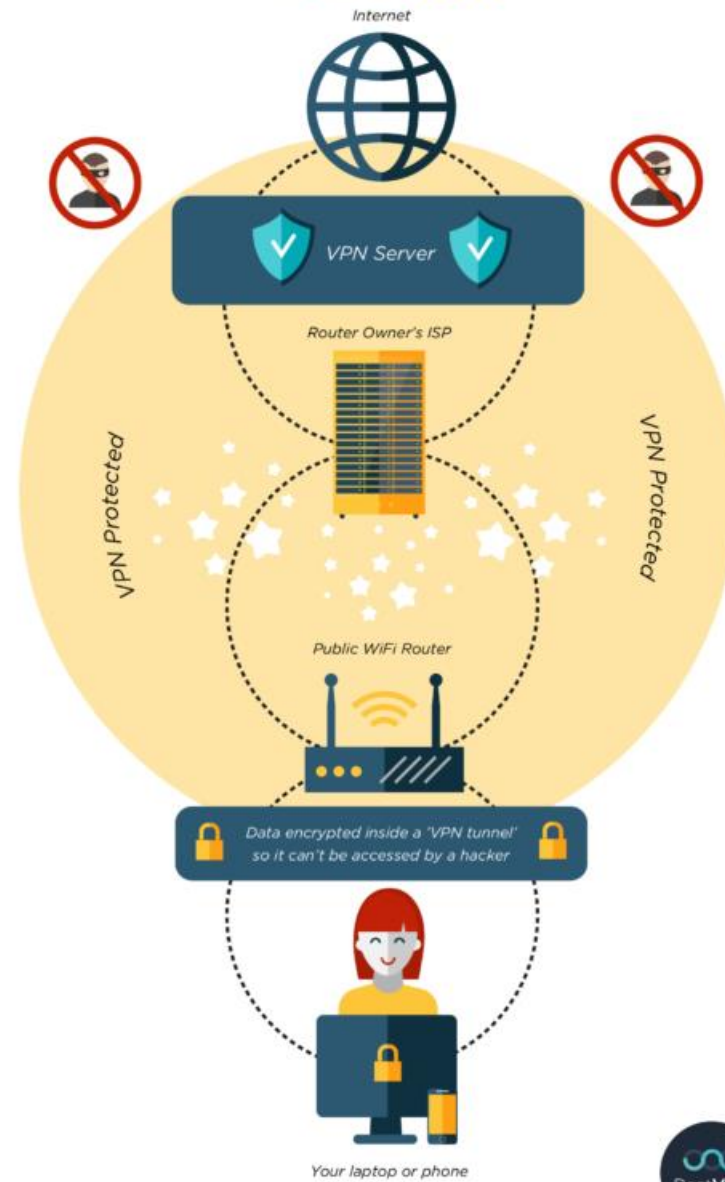


# HOW VPN PROTECTS YOU WHEN USING PUBLIC WIFI

## WITHOUT VPN



## WITH VPN



# 5 WAYS TO USE YOUR VPN



## Defeat Censorship

Watch the content you want from any country on Earth, at blazing fast speeds. Access any website or app without geographic restrictions or censorship.

## Increase Online Security

ExpressVPN encrypts your data and protects your online activity, passwords, and sensitive information from prying eyes.





## Stay Private

When connected to ExpressVPN, your ISP only sees encrypted traffic passing to our VPN servers, but they cannot decipher the data or know the websites you have visited.

## Access Hidden Internet Hacks!

With ExpressVPN, you can change your IP address and location to get better deals on everything from flights to car rentals.

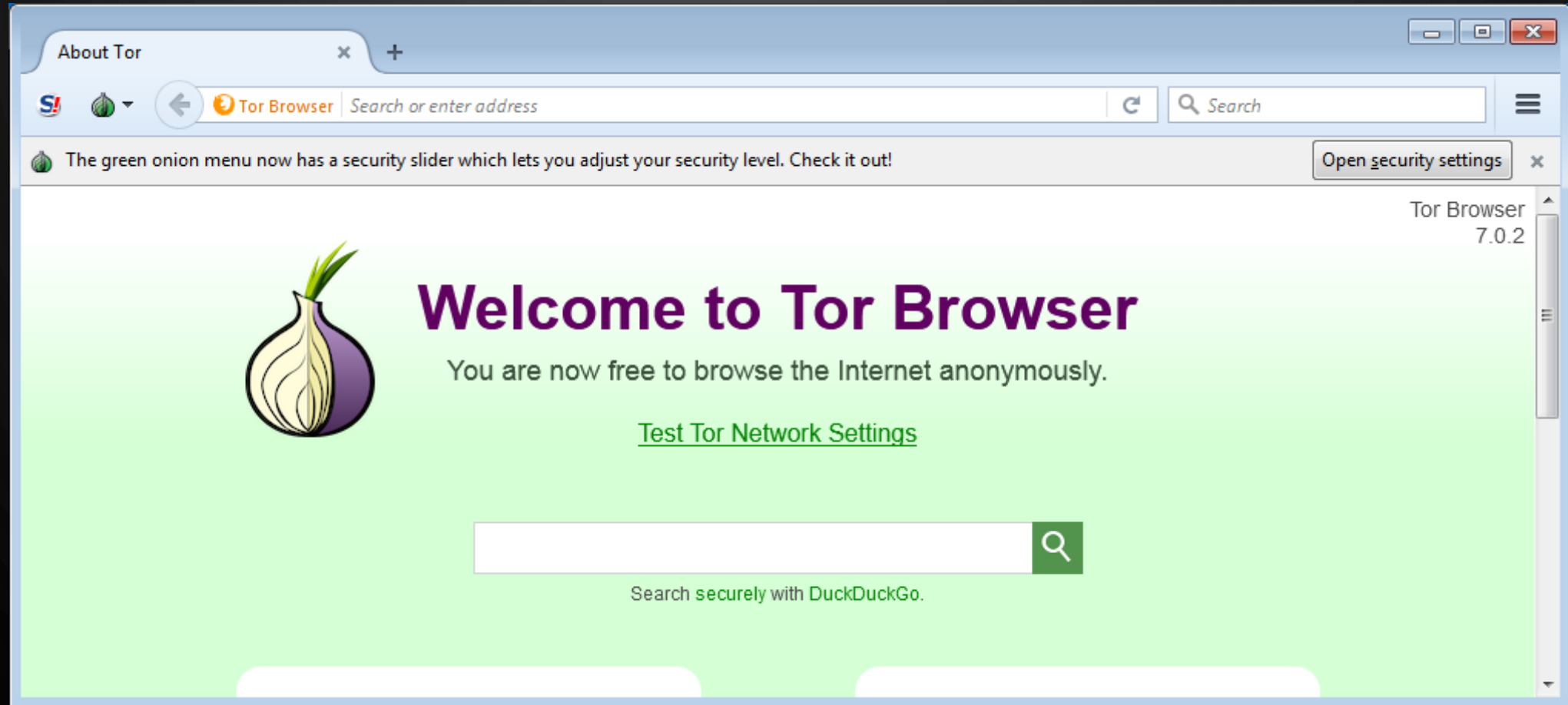


## Protect All Your Devices

Download easy-to-use VPN apps for Windows, Mac, iOS & Android.



# USE THE TOR

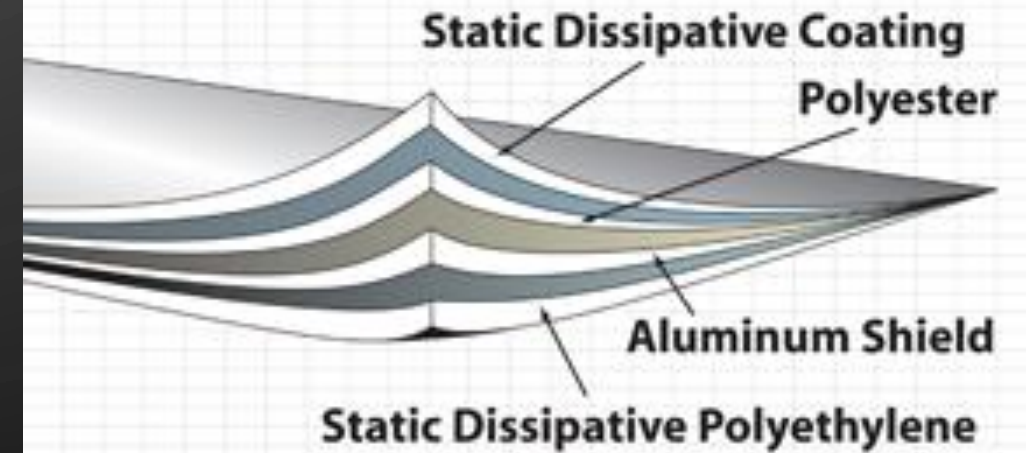


# GET A FARADAY BAG

## Black Hole Faraday Bags Window Sizes



## Metal-In Static Shielding Film



# GET A FARADAY BAG!!!



MISSION  
DARKNESS

## FARADAY BAGS DELIVER MILITARY-GRADE PROTECTION

Shield your Sensitive Data

- ✓ **Block Phone Hacking**  
Your phone holds passwords, emails, & your most important data. Protect it!
- ✓ **Stop Tracking & Camera Access**  
Hackers can view your location and access your camera. Don't let them!
- ✓ **Protect Forensic Evidence**  
Law enforcement & military seize critical evidence. Shield it properly!





## MD SHIELDING



Digital Forensics



Wireless Testing



Personal Security



Anti-Hacking



Travel Data Privacy



Passp/ID Protection

Plus, download the free Mission Darkness Faraday Bag testing app ("Faraday Test" for iOS, "MD Faraday Bag Tester" for Android) to confirm signal cutoff!

# GET A CRYPTOPHONE!



# CONSLUSION



**BE AFRAID, BE VERY AFRAID!!!**





**KEEP  
CALM**

**AND**

**BE AFRAID,  
BE VERY AFRAID**