

PRIVACY & SECURITY UNDER ATTACK



Dave Hatter, CISSP, CCSP, CSSLP, Security+, Network+, PMP, ITIL V3

"Doomsday" Dave



"Privacy is one of the biggest problems in this new electronic age" – Andy Grove

"We believe the customer should be in control of their own information. You might like these so-called free services, but we don't think they're worth having your email, your search history and now even your family photos data mined and sold off for God knows what advertising purpose. And we think some day, customers will see this for what it is." – Tim Cook

If you're not paying with money, you're paying with data. You're the product
NOT the customer

My goals for today

- Educate you
- Motivate you
- Provide actionable advice
- Have fun

Ripped from the headlines

PC #Amplify #WorkFromHome Reviews Best Products How-To News Newsletters

PCMag editors select and review products [independently](#). If you buy through affiliate links, we may earn commissions, which help support our testing. [Learn more.](#)

Home > News > Networking

T-Mobile to Share Customers' Web Browsing Data With Advertisers Unless They Opt Out

The upcoming policy doesn't mention the risk of third-party advertisers combining T-Mobile customer information with their own stockpile of tracking data, which could de-anonymize users' activities.

BGR TECH ENTERTAINMENT DEALS BUSINESS SCIENCE LIFESTYLE

TECH

Google finally reveals the terrifying amount of data Gmail collects on iPhone

CPO MAGAZINE HOME NEWS INSIGHTS RESOURCES

Over a Billion Android Phones Turned Into Perfect Spying Tools by Security Flaws

gt government technology MAGAZINE NEWSLETTERS EVENTS PAPERS NAVIGATOR GovTech Biz Emerging Tech Gov Experience SPECIAL:

Cell Data Offers Look at California Pandemic Travel Patterns

Through a compilation of cellphone location tracking data, Google has painted a picture of how Californians have changed their travel habits as a result of the ongoing COVID-19 pandemic.

n p r CINCINNATI PUBLIC RADIO NEWS 93.2 89.3 105.1 SIGN IN

NEWS ARTS & LIFE MUSIC SHOWS & PODCASTS SEARCH

NATIONAL SECURITY

China Wants Your Data — And May Already Have It

Thousands of Android and iOS Apps Leak Data From the Cloud

https://www.wired.com/story/ios-android-leaky-apps-
Search
Socials Email Training CS PMI PM Security GitHub KCR IIT Tools 800-171 Azure Python MS 55KRC CIL

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY SIGN IN

LILY HAY NEWMAN SECURITY 03.04.2021 10:00 AM

Thousands of Android and iOS Apps Leak Data From the Cloud

It's the digital equivalent of leaving your windows or doors open when you leave the house—and in some cases, leaving them open all the time.

Reviews Gear Gaming Entertainment Tomorrow Audio Video Deals Buyer's Guide

Latest in Gear



Your fitness tracker probably has security issues

Hackers could theoretically track you or manipulate your health data.

Ripped from the headlines

NEWS ANALYSIS

Smart lighting security flaw illuminates risk of IoT

The latest smart home security nightmare sheds light on the risk you take each time you add another connected system to your network.



Electronics & Computers / Computers & Internet / Privacy / Gifts That Snoop? The Internet Of Things Is Wrapped In Privacy Concerns

Gifts That Snoop? The Internet of Things Is Wrapped in Privacy Concerns



About Issues Our Work

Amazon's Ring Is a Perfect Storm of Privacy Threats

BY MATTHEW GUARIGLIA | AUGUST 8, 2019

naked security by SOPHOS

PRODUCTS > FREE TOOLS > Q FREE SOPH

Smart speakers mistakenly eavesdrop
up to 19 times a day

BUSINESS

CULTURE

GEAR

IDEAS

SCIENCE

Share



BRIAN BARRETT SECURITY 02.07.17 08:03 PM

How To Stop Your Smart TV From Spying on You



Walgreens says mobile app leaked users' personal data

US pharmacy store says mobile app exposed names, prescription details, and shipping addresses.



Join Extra Crunch

A 'stalkerware' app leaked phone data from thousands of victims

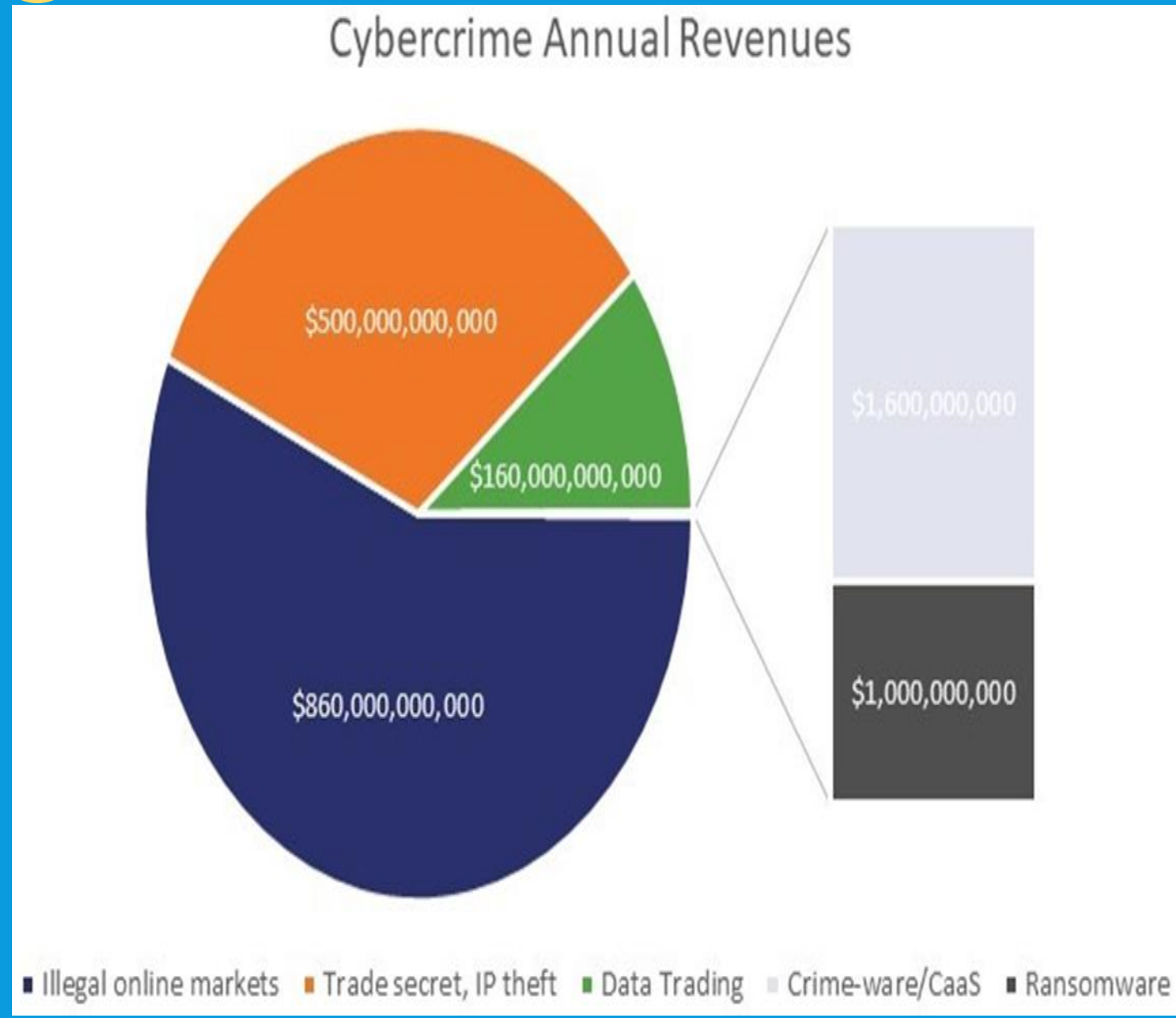
Why now?

- Increasing use of technology in all facets of life
- Massively scalable computing resources available on-demand (cloud)
- Untraceable worldwide communications (encryption)
- Virtual international currency (cryptocurrency)
- Ever increasing number of connected devices
- And...

Crime is going digital

<https://www.thesslstore.com/blog/2018-cybercrime-statistics/>

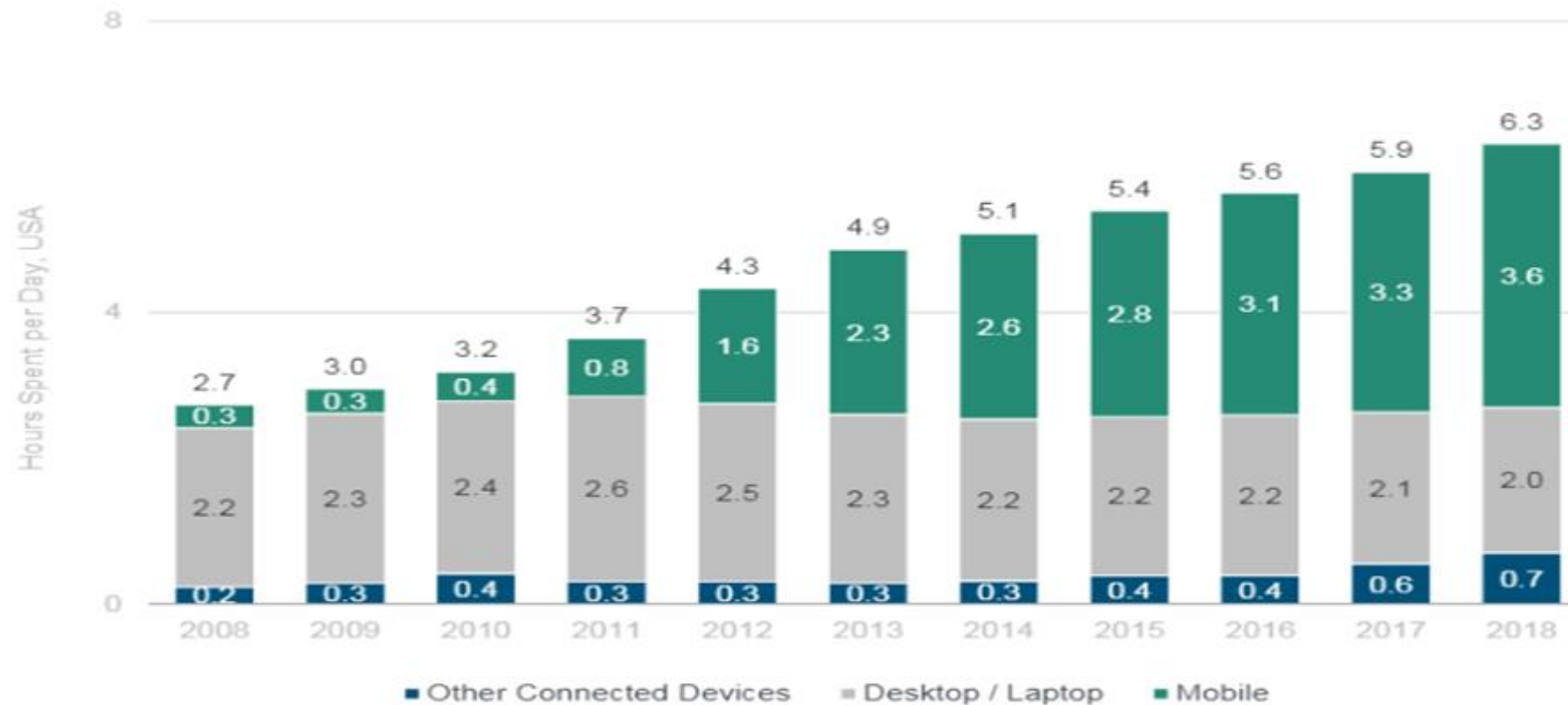
- Cyberattacks are increasing in frequency, sophistication, impact and cost
- A study by Dr. Michael McGuire puts value of the cybercrime economy at \$1.5 trillion
- Could hit \$10 trillion by 2025
- Cybercriminals are rarely prosecuted



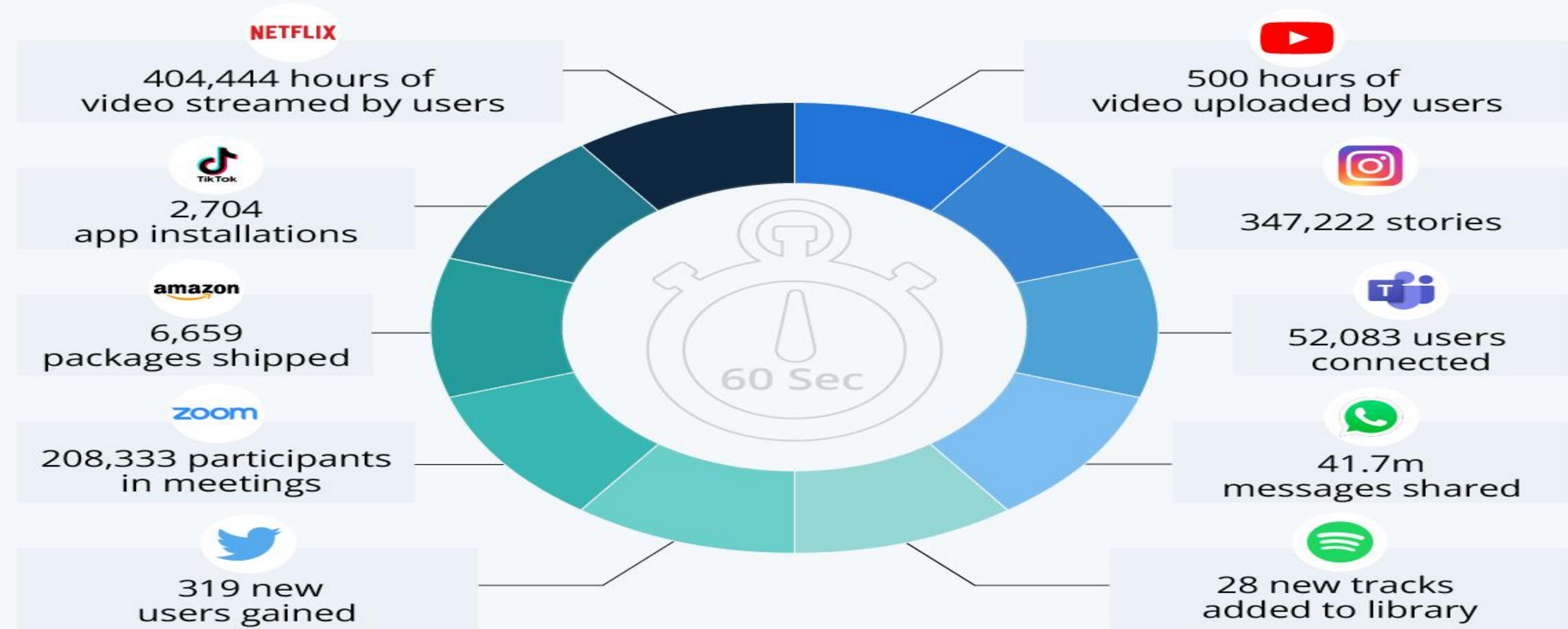
More data is being created

Accelerating +7% vs. +5% Y/Y

Daily Hours Spent with Digital Media per Adult User, USA

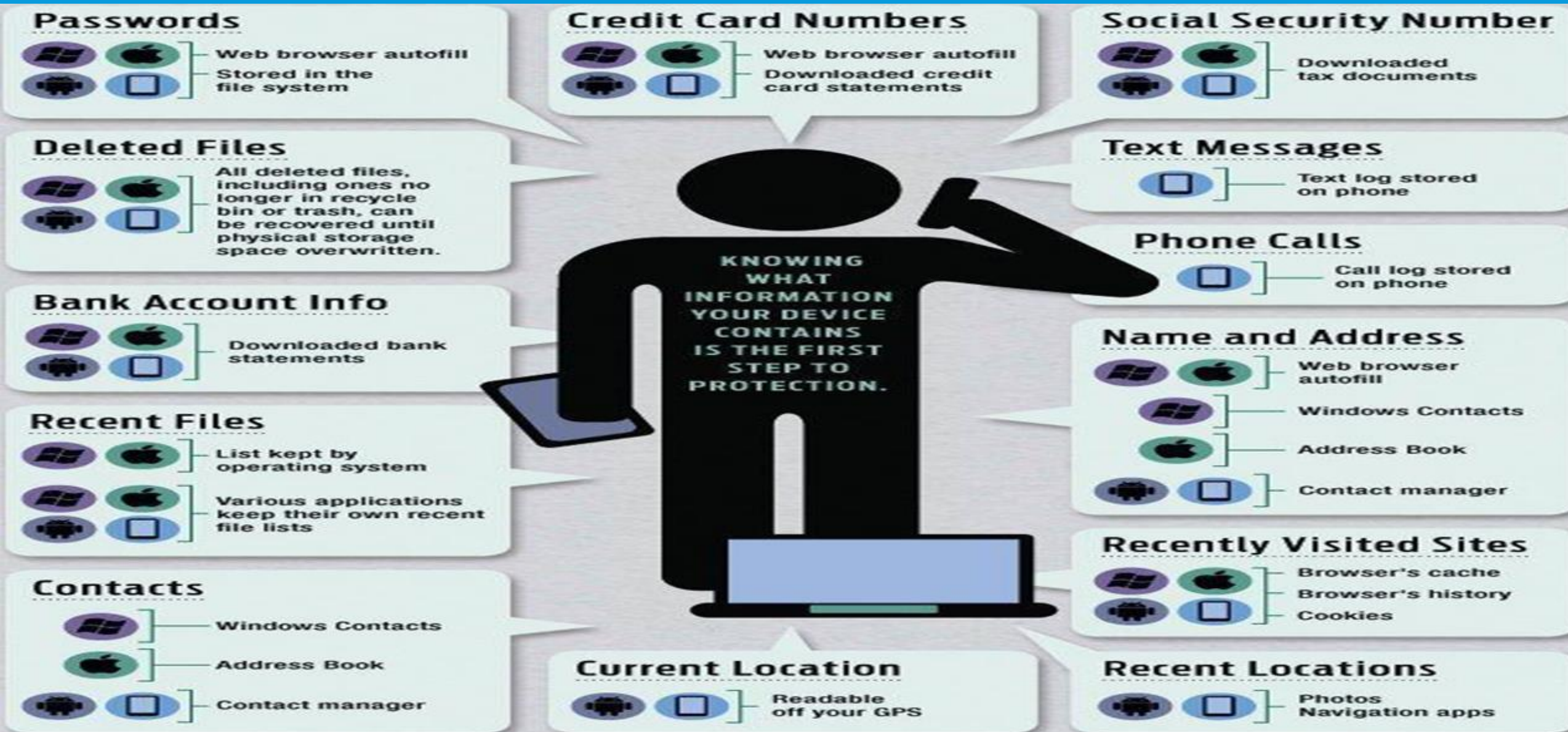


2020 Internet Minute



Source: Visual Capitalist

And... pervasive data collection



Data is increasingly valuable

Your identity is a steal on the Dark Web.
Here are what the most common pieces of information sell for:



Social security number



\$1

Online payment services login info
(e.g. Paypal)



\$20-\$200

Credit or debit card
(credit cards are more popular)



\$5-\$110

With CVV number
\$5

With bank info
\$15

Fullz info*
\$30

Drivers license



\$20

Loyalty accounts



\$20

General non-financial institution logins



\$1

Diplomas



\$100-\$400

Passports (US)



\$1000-\$2000

Subscription services

\$1-\$10

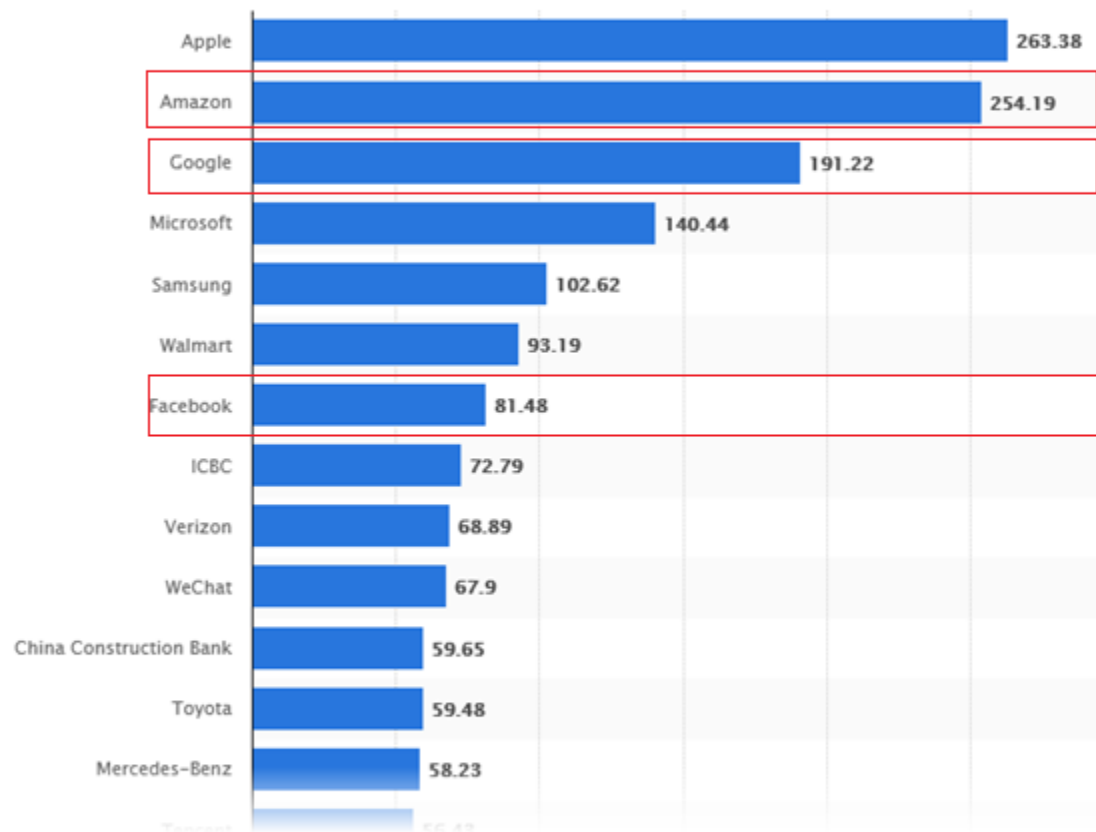
Medical records

\$1-\$1000**

And.. data is increasingly valuable

Most valuable brands worldwide in 2021

(in billion U.S. dollars)



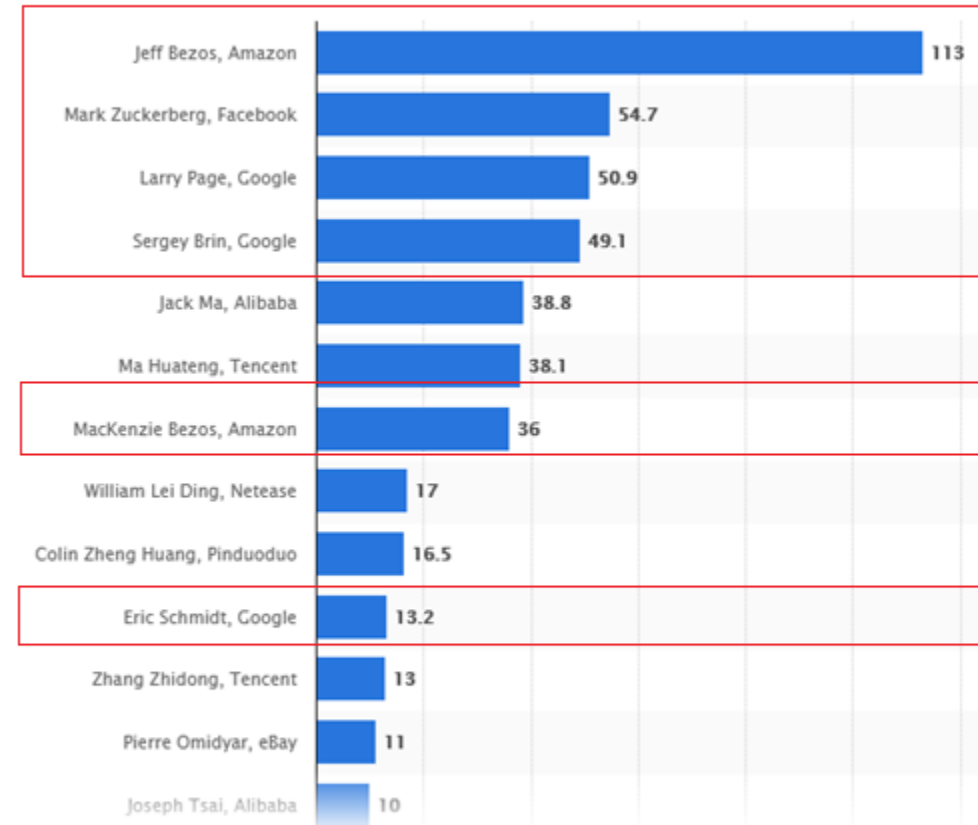
Expand statistic

© Statista 2021

Show source

Leading internet billionaires as of March 2020, by net worth

(in billion U.S. dollars)



Expand statistic

© Statista 2021

Show source

Additional Information

Additional Information

Who does Facebook Own?

- Instagram
- WhatsApp
- Oculus VR

CNN BUSINESS Markets Tech Media Success Video

Facebook is facing an existential crisis

by Dylan Byers @CNNMoney

🕒 March 19, 2018: 10:40 AM ET



Facebook suspends data firm with Trump ties



CNNMoney Sponsors

SmartAsset Paid Partner

These are your 3 financial advisors near you

This site finds and compares 3 financial advisors in your area

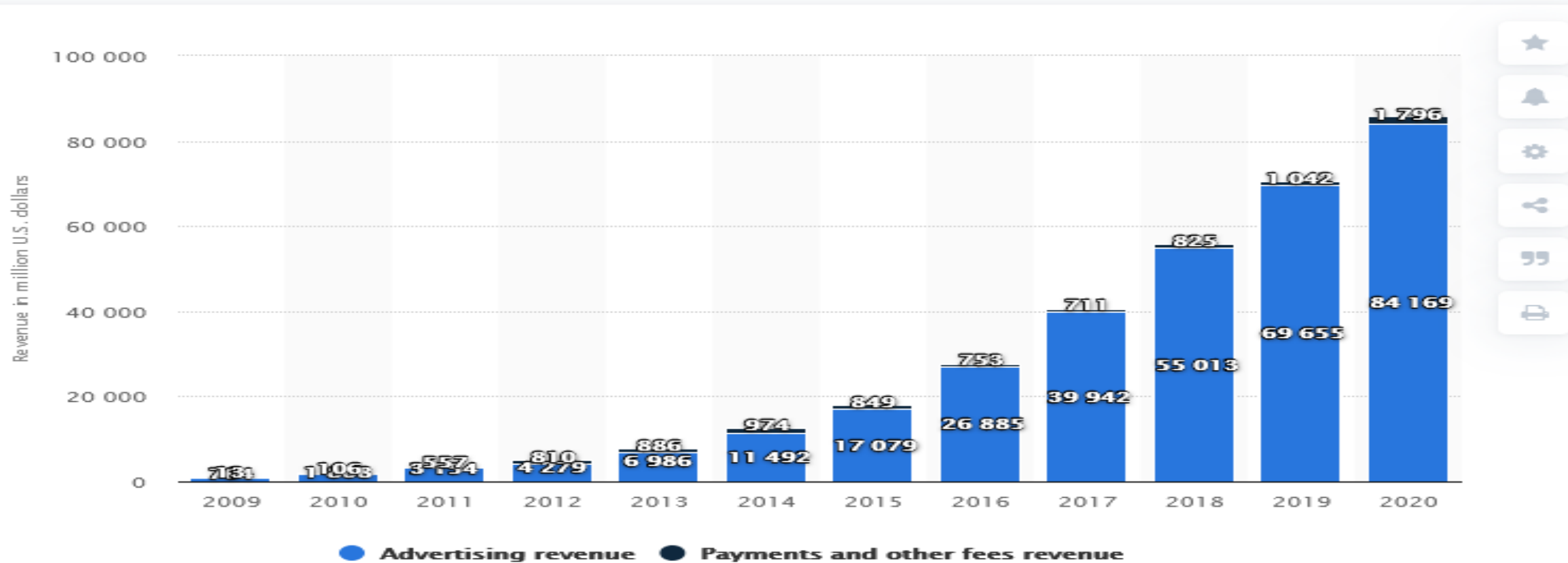
Check this off your list before retirement: talk to an advisor

Answer these questions to find the right financial advisor for you

Find CFPs in your area in 5 minutes

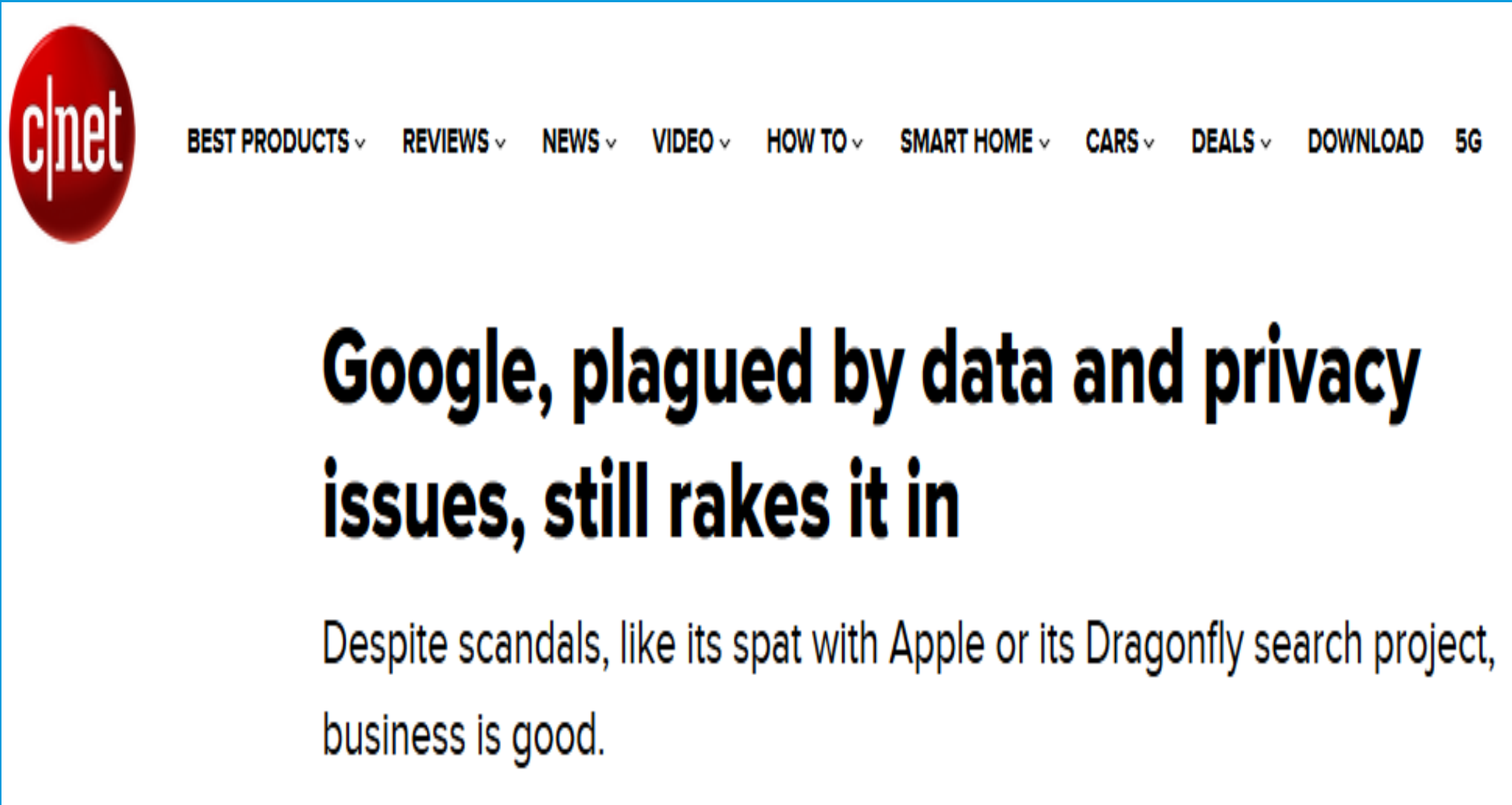
And.. data is increasingly valuable

Facebook's annual revenue from 2009 to 2020, by segment
(in million U.S. dollars)



Who does Alphabet (Google) Own?

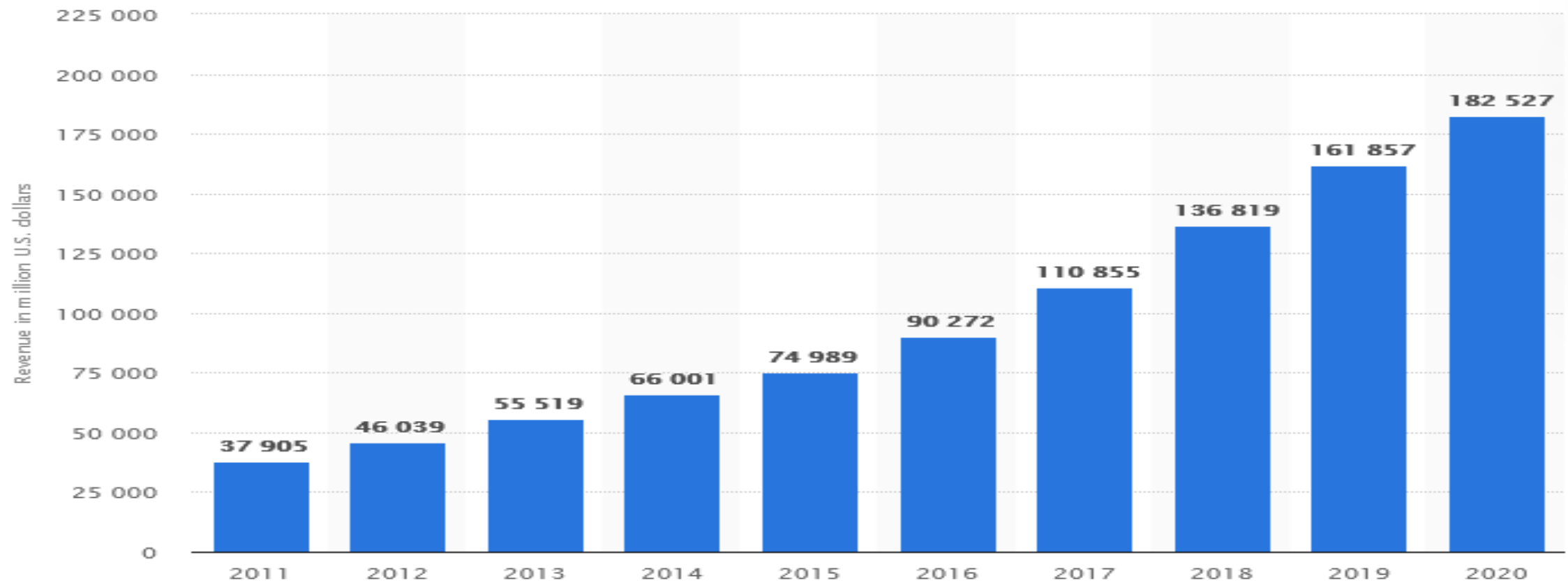
- Android
- YouTube
- Gmail
- GSuite
- Fitbit
- Blogger
- Picasa
- Nest
- Zagat
- Boston Dynamics



And.. data is increasingly valuable

Annual revenue of Alphabet from 2011 to 2020

(in million U.S. dollars)



© Statista 2021

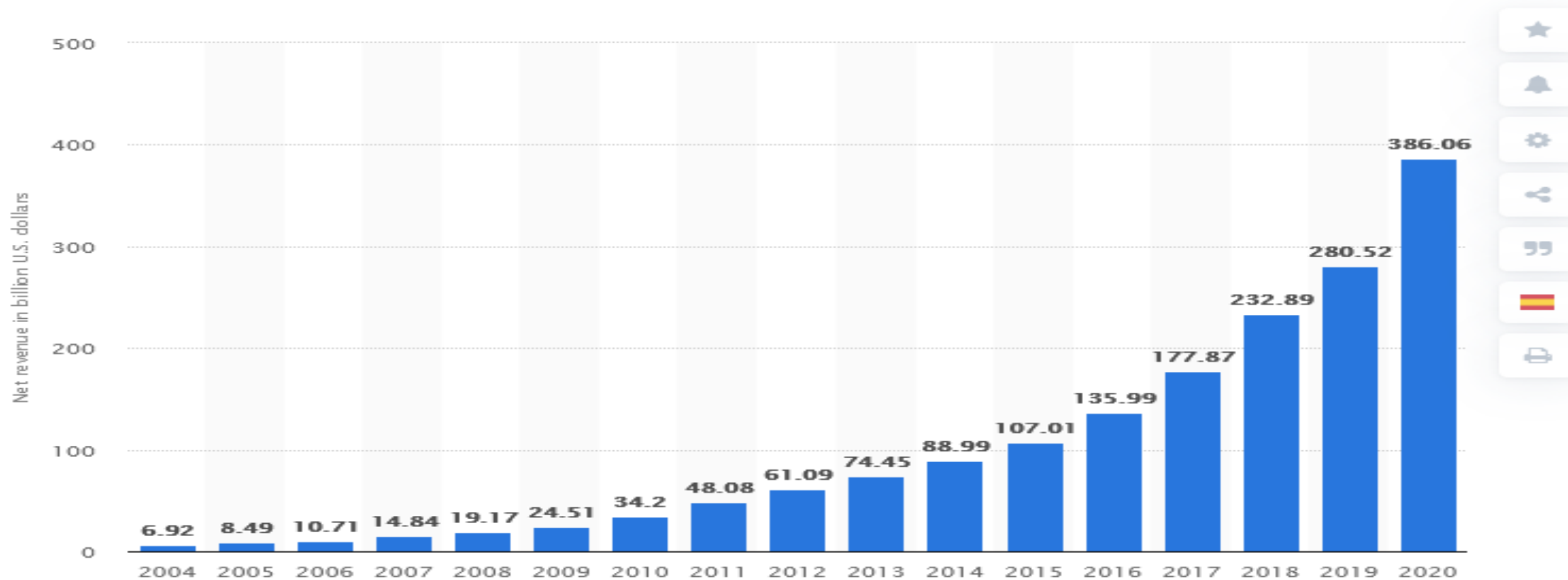
[Additional Information](#)

[Show source](#)

And.. data is increasingly valuable

Annual net revenue of Amazon from 2004 to 2020

(in billion U.S. dollars)



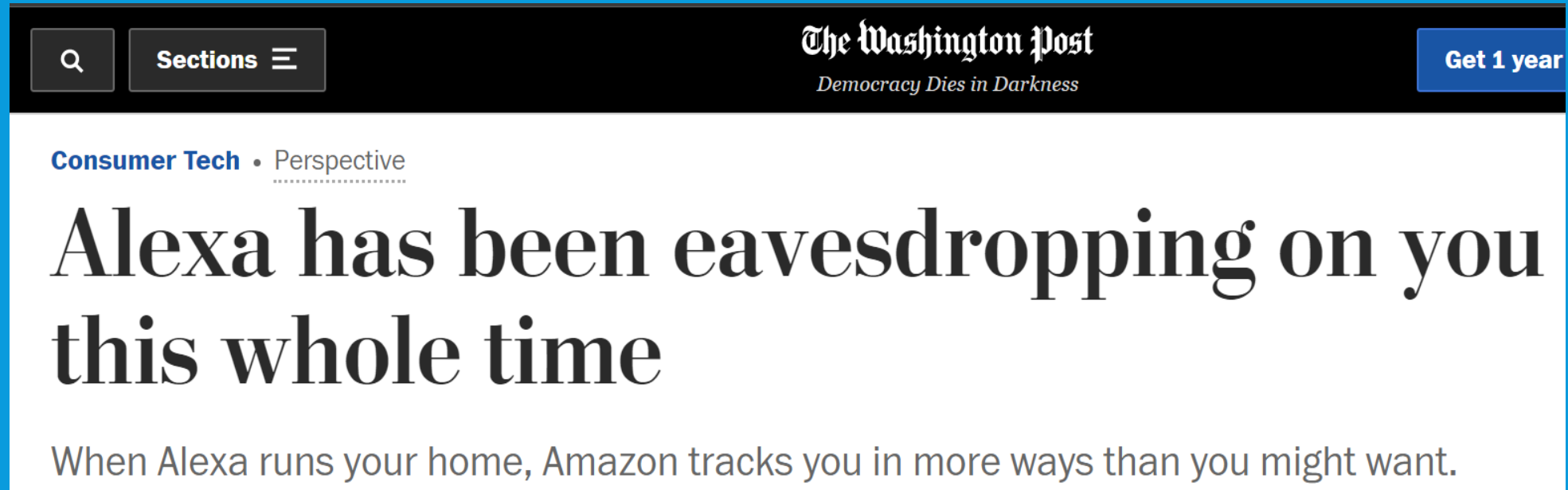
© Statista 2021

[Additional Information](#)

[Show source](#)

Who does Amazon Own?

- AWS
- Whole Foods
- Ring
- Zappos
- PillPack
- Twitch
- Kiva
- Audible



The Washington Post
Democracy Dies in Darkness

Get 1 year

Consumer Tech • Perspective

Alexa has been eavesdropping on you this whole time

When Alexa runs your home, Amazon tracks you in more ways than you might want.

This screenshot shows the top portion of a news article from The Washington Post. The masthead includes the newspaper's name and tagline, a subscription button, and a search icon. The article is categorized under 'Consumer Tech' and 'Perspective'. The headline is 'Alexa has been eavesdropping on you this whole time', followed by a sub-headline that reads, 'When Alexa runs your home, Amazon tracks you in more ways than you might want.'



Subscribe →

The Guardian

News Opinion Sport Culture Lifestyle

My life in data

‘They know us better than we know ourselves’: how Amazon tracked my last two years of reading

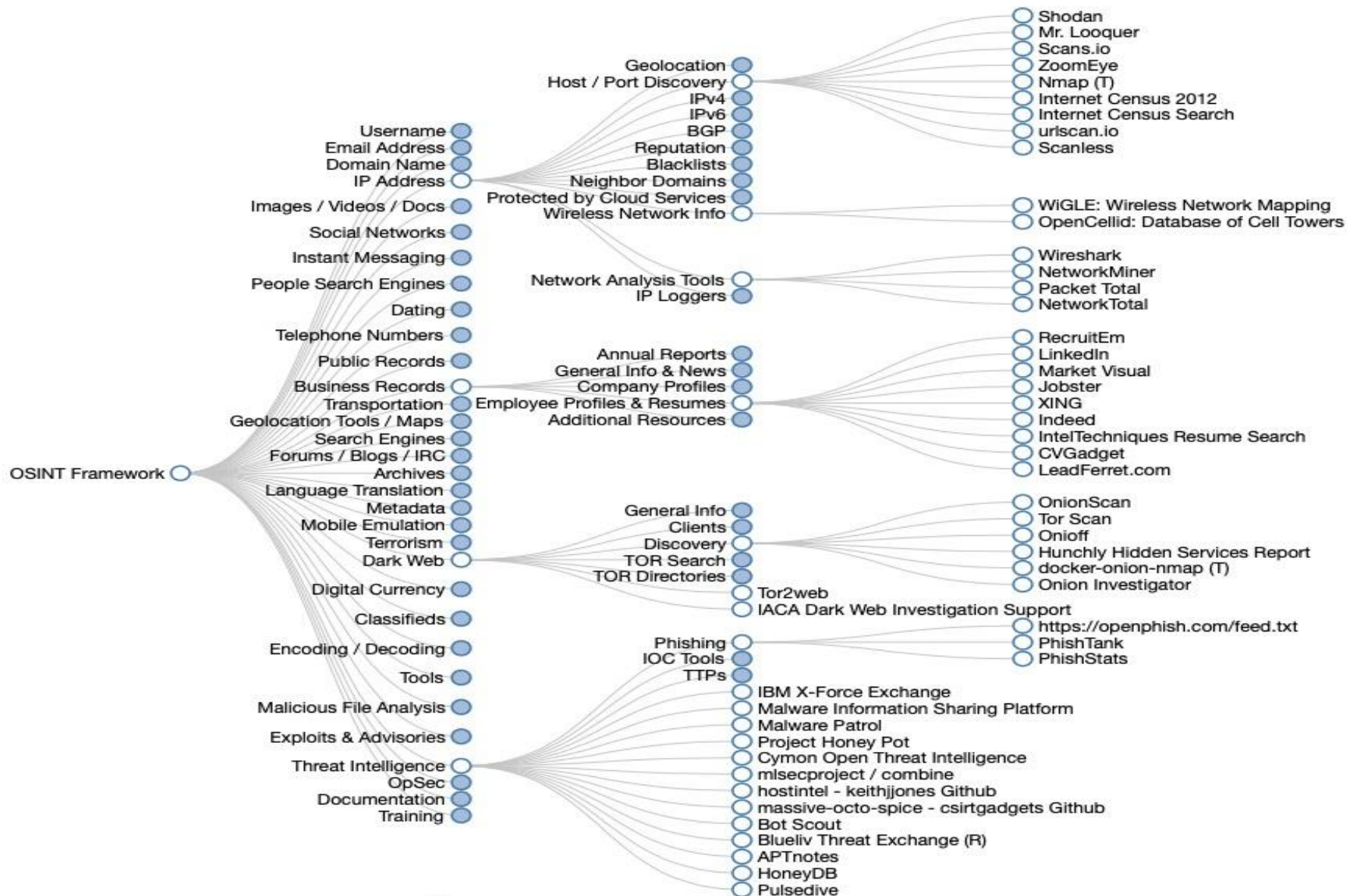
This screenshot shows the top portion of a news article from The Guardian. It features a yellow 'Subscribe' button with a right arrow, the newspaper's name, and a navigation bar with links to 'News', 'Opinion', 'Sport', 'Culture', and 'Lifestyle'. The article is titled 'My life in data' and '‘They know us better than we know ourselves’: how Amazon tracked my last two years of reading'.

Eliminate the middleman?



CUTTING OUT THE MIDDLEMAN

And... Open-Source Intelligence



And... Shodan



The screenshot shows the Shodan website homepage. At the top, there's a browser address bar with 'https://www.shodan.io'. Below it is a navigation bar with links like 'Shodan', 'Developers', 'Monitor', and 'View All...'. A search bar with the Shodan logo is on the left, and links for 'Explore', 'Pricing', and 'Enterprise Access' are on the right. A red button says 'Try out the new beta website!' and a blue button says 'Help Center'. The main content area features a large black box with the text 'The search engine for Security' and 'Shodan is the world's first search engine for Internet-connected devices.' Below this are two buttons: 'Create a Free Account' and 'Getting Started'. To the right is a large graphic of a globe made of a wireframe mesh, with several red circular icons and IP addresses (67.20.69.105, 50.87.75.184, 104.18.61.231) overlaid on it.

https://www.shodan.io

Shodan Developers Monitor View All...

SHODAN

Explore Pricing Enterprise Access

Try out the new beta website! Help Center

New to Shodan? Login or Register

The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



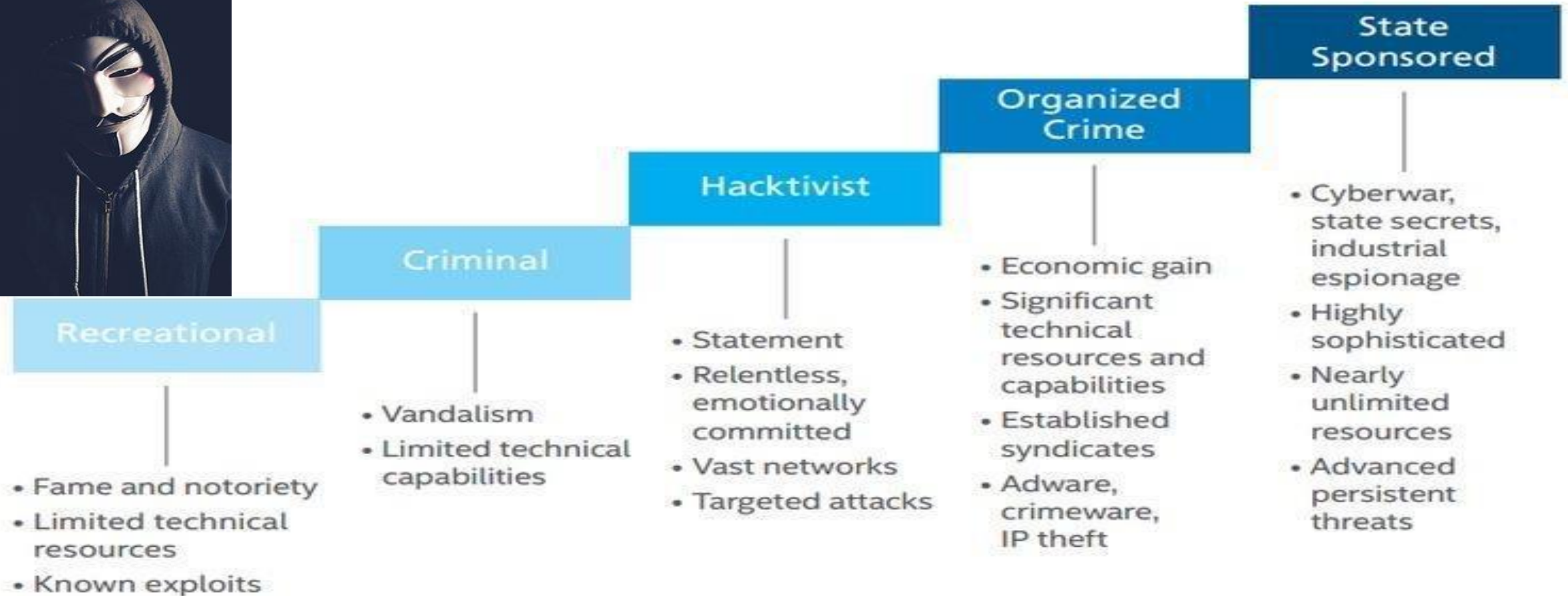
Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

And... Threat Actors



Changing Attacker Profiles



INCREASING RESOURCES AND SOPHISTICATION

The expansion of attacker types, their resources, and their sophistication.

And... the attack surface grows daily



THE EXPLOSION OF IOT DEVICES

**30.73
BILLION**

IoT devices expected by 2020¹

**75.44
BILLION**

IoT devices expected by 2025

AN EASY TARGET

IoT devices are inherently vulnerable and relatively easy to hijack. Why?

- They're leaving security up to the owner
- They're not regularly patched
- They're not running security software
- They're not designed with security in mind



EVERYTHING IS CONNECTED!

IoT devices are in our homes and offices, and on our bodies



22 Million

Amazon Echos sold in 2017²



1 Per Second

how often Google says it has sold a Google Home device since October 2017³



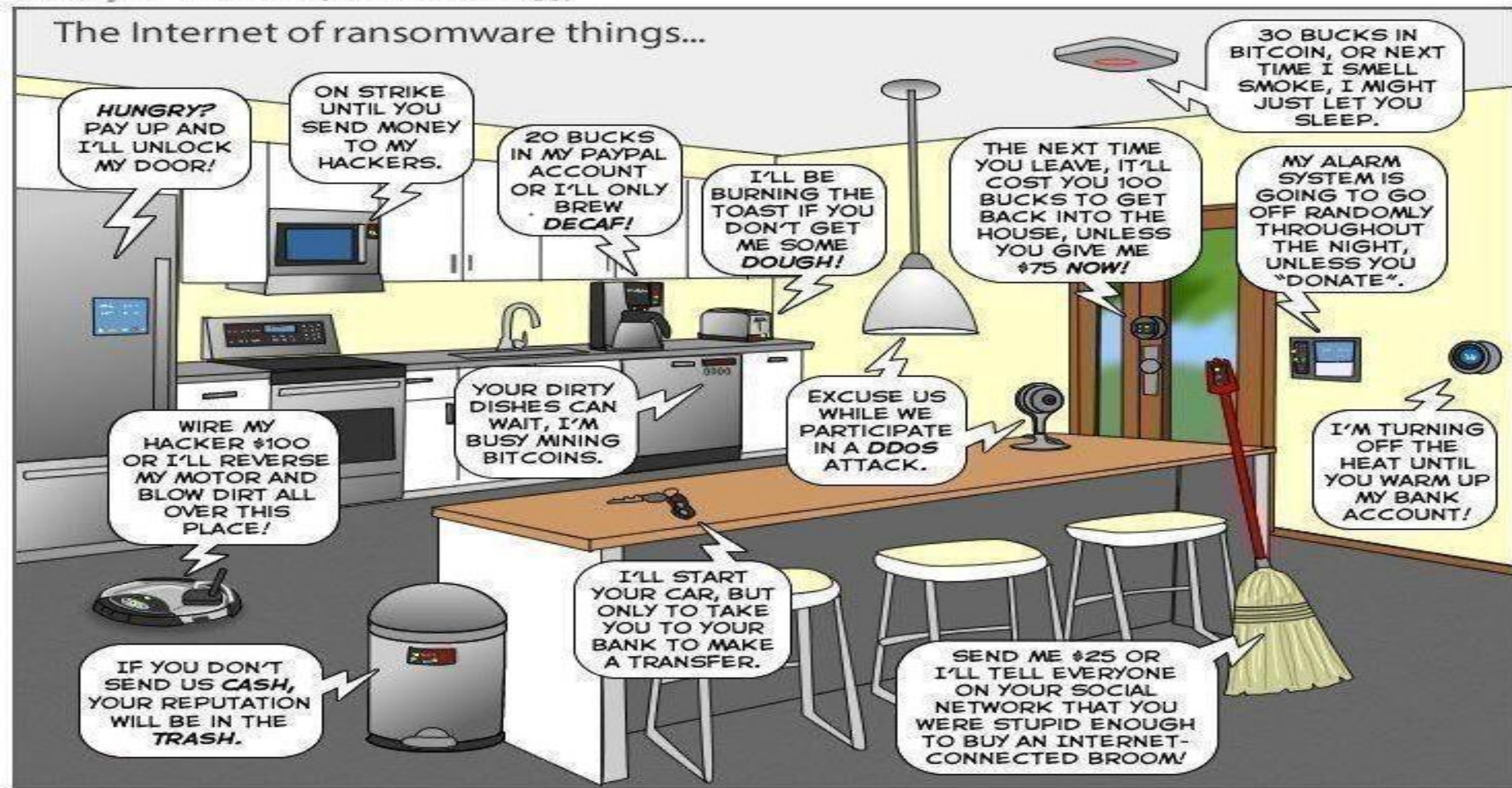
\$310.4 Million

wearable devices sales in 2017⁴

And... Security is often an afterthought

- People working remotely are at higher risk
- IoT devices are creating more attack points
- An attack can open an organization to devastating attacks and crippling consequences
- An organization can incorporate cybersecurity into business practices and processes, OR react to security failures
- Be proactive and be prepared, or be sorry

The Internet of ransomware things...



Privacy != Security

- Privacy: Control of your personal information and how it's used
- Security: how your personal information is protected

Privacy myths

- It's impossible maintain some privacy in today's world
- My data (or the data I have access to) isn't valuable
- I have to be a technical wizard to protect myself
- I have nothing to hide

Cybersecurity myths

- My organization is too small or insignificant to be a target
- Cybersecurity requires a huge financial investment
- Attacks are sophisticated or technically complex
- New software and devices are secure out-of-the-box
- Compliance with industry standards is sufficient
- Security is an IT issue

It's a matter of when, not if...

- "No locale, no industry or organization is bulletproof when it comes to the compromise of data." – Verizon 2016 Data Breach Investigation Report
- "Fundamentally, if somebody wants to get in, they're getting in. Alright, good. Accept that." – former director of the CIA and National Security Agency Retired Gen. Michael Hayden
- Cybercrime is "the greatest threat to every profession, every industry, every company in the world." – IBM CEO Ginni Rometty
- "There are two kinds of companies in the United States. There are those who've been hacked ... and those who don't know they've been hacked." – Former FBI Director James Comey

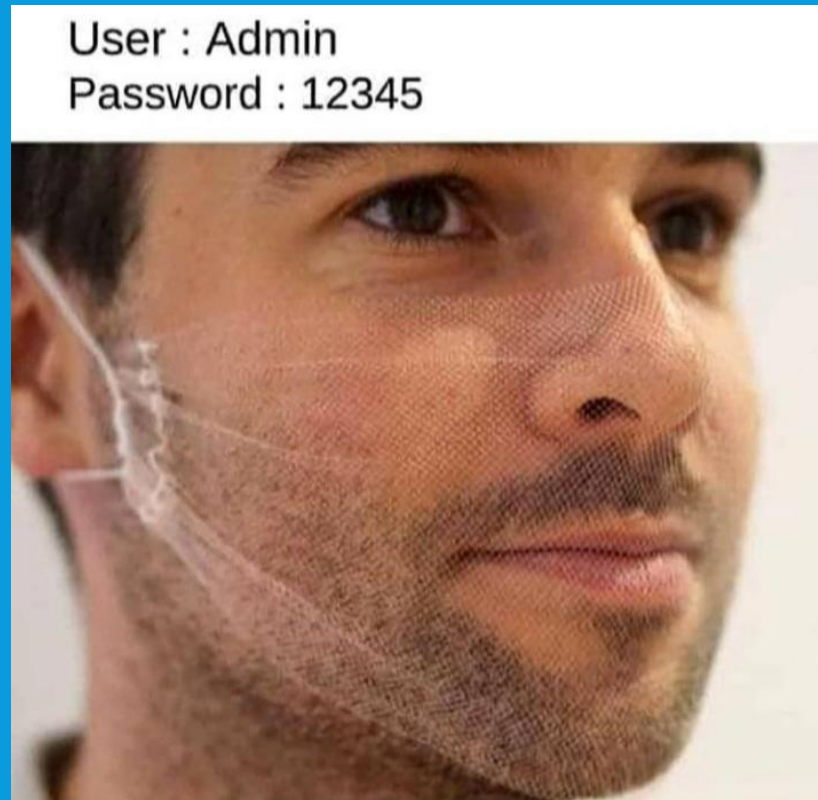
Guiding principals of security

- Impenetrable security is nearly impossible and very expensive
- Focus on risk
- Take a layered approach
- Invite security to the party from the beginning
- Threats emerge and evolve constantly
- Education and awareness are critical
- Maintain a very healthy dose of skepticism/paranoia

3 simple steps to remember

- Stop
- Think
- Protect — Be a human firewall

Threats: Poor credential management



Threats: Unpatched Software

- A Ponemon Institute survey found 57% of security breaches were due to vulnerabilities in unpatched software
- 34% of these cybercrime victims were aware of holes but didn't patch them in time.
- 37% of breach victims don't perform regular scans to find vulnerabilities in their own systems
 - Patching gaps are an issue:
 - Unaware of the updates that are available
 - Know updates are available, but don't have the resources or strategies implement the patches

Threats: Spoofing

- "Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security." – Techopedia
- Spoofing leads to:
 - Phishing
 - Vishing (Voice based)
 - Smishing (Text based)
 - Doppleganger or Lookalike websites

Threats: Phishing

- "Cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords." – Phishing.org
- Types of Phishing include:
 - Spear phishing
 - Whaling
 - Vishing
 - Smishing



Threats: Phishing

From: Dave Hatter <pm772858@gmail.com>

Sent: Wednesday, October 30, 2019 1:23 PM

To: Jeff Bethell <jbethell@fortwright.com>

Subject: Hey Jeff

Hey Jeff , i need you to help me get some gift cards at the store right now for some council members / staff appreciation gifts , let me know if you can do that right away because there is a sharp deadline for this request .

Dave Hatter

Mayor

Sent from my mobile device

Threats: Phishing

JW

Joyce Woods

To: David Hatter; y

Inbox

You replied on 3/3/2016 2:02 PM.

----- Original Message -----

From: Dave Hatter [mailto:dhatter@fortwright.com]

Sent: Wednesday, March 02, 2016 4:09 PM

To: Joyce Woods <jwoods@fortwright.com>

Subject: RE: Question

Thanks for the information. I need you to initiate 2 wire transfers today for an international payment and a local payment also. Let me know what information is required.

Sent from my iPhone

Sorry Dave,

I just got your message. I have been working on other things. If you mean the General Fund Checking Acct, the balance today is \$4,285,408.72.

Joyce

From: Dave Hatter [mailto:dhatter@fortwright.com]

Sent: Wednesday, March 02, 2016 12:35 PM

To: Joyce Woods <jwoods@fortwright.com> <mailto:jwoods@fortwright.com> >

Subject: Question

Are you available? I need to ask you a quick question What is the present balance in the operating checking account? Reply as soon as possible.

Sent from my iPhone

JW

Joyce Woods

To: David Hatter; y

From: Dave Hatter [mailto:dhatter@fortwright.com]

Sent: Wednesday, March 02, 2016 12:35 PM

To: Joyce Woods <jwoods@fortwright.com>

Subject: Question

Are you available? I need to ask you a quick question What is the present balance in the operating checking account? Reply as soon as possible.

Sent from my iPhone

Threats: Phishing

Mail - David Hatter - Outlook

https://outlook.office.com/mail/inbox/id/AAMkAGRmNDY5MGVhLWJiOTMtNGlyNS1iNDZiLTc2YWfkZThiNDE2NQBGAAAAAAj91TVN85gQbrRM1ehWXssBwBumyDpLKyoQaLSPgd6x4pIAAAAAEMAABumyDpLKyoQaLSPgd6x4pIAAOs3yuBAAA%3D

To see favorites here, select ☆ then ☆, and drag to the Favorites Bar folder. Or import from another browser. [Import favorites](#)

Outlook

Search

New message

Reply all

Delete

Archive

Junk

Sweep

Move to

Categorize

Happy New Year!

Getting too much email? [Unsubscribe](#)

JH

J. Holloway <jholloway@fortwright.com>

Thu 12/12/2019 11:09 AM

David Hatter

**** WARNING: This e-mail is from an EXTERNAL sender. Be wary of any links or attachments. If this e-mail is unexpected and you are being asked to open an attachment or enter information or credentials into an online form STOP NOW. Call the sender via a known phone number to determine if this is legitimate. Even if you expected this email, if it is regarding any type of financial transaction like a wire, call the sender via phone to validate the information and talk to your supervisor before conducting any financial transaction. ****

Good Day Dave,

Original URL:
<http://cardpayments.microransom.us/XYWNj0aW9uPWgN...>
Click or tap if you trust this link.

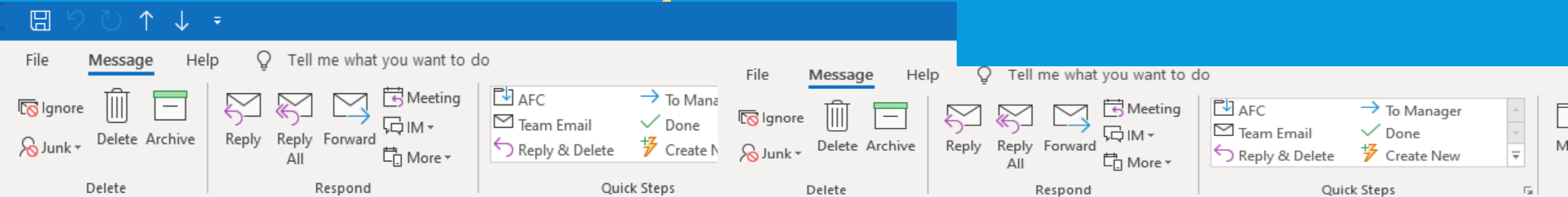
holiday, warm wishes for the new year!

[Here is your card](#)

With Gratitude,

<https://nam11.safelinks.protection.outlook.com/?url=http%3A%2F%2Fcardpayments.microransom.us%2FXYWNj0aW9uPWgNsaWNrJneVybD1ozzdHRwaczovL3NIIV3dVvZWQtbG9n%3A%3D&data=04&ad=US&u=https%3A%2F%2Fcardpayments.microransom.us%2FXYWNj0aW9uPWgNsaWNrJneVybD1ozzdHRwaczovL3NIIV3dVvZWQtbG9n%3A%3D>

Threats: Phishing



RE: Divorce papers



Brown & Booth LLP <Booth@brown-booth-law.com>
To: Dave Hatter

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

WARNING: This e-mail is from an external sender. Be suspicious of any links or attachments. If you are not expecting this e-mail, or about any type of financial transaction like a wire, call the sender via phone to validate all the information.

Dave

My name is Keith Booth and I am a senior partner at BROWN & BOOTH LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft, please contact me as soon as possible:

http://www.brown-and-booth-law.com/papers/divorce_Hatter.doc

Thank you
Keith L. Booth

RE: Divorce papers



Brown & Booth LLP <Booth@brown-booth-law.com>
To: Dave Hatter

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

WARNING: This e-mail is from an external sender. Be suspicious of any links or attachments. If you are not expecting this e-mail, or about any type of financial transaction like a wire, call the sender via phone to validate all the information.

Dave

My name is Keith Booth and I am a senior partner at BROWN & BOOTH LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft, please contact me as soon as possible:

http://www.brown-and-booth-law.com/papers/divorce_Hatter.doc

Thank you
Keith L. Booth



Original URL:
<http://addto.password.land/xywns0aw9upwqnsawnrjnvybd1orgdhrwnczovl3nlby3cvyzwqtb9naw4ubmv0rl3bhz2vzl2findfly2jkngzhjnjly2lwawvudf9pzd01ntgxmdaxmjemy2ftcgfpz25fcnvux2lkpti3mjyyndu=>
Click or tap to follow link.

Threats: Phishing

Outlook

Search

New message

Delete

Archive

Move to

Categorize

Favorites

Inbox

111

Sent Items

1

Drafts

9

Add favorite

Folders

Inbox

111

Drafts

9

Sent Items

1

Deleted Items

251

Junk Email

Archive

Notes

Conversation Hist...

You have been approved for a \$2,321.00 USD from FAFSA

Federal Student Aid

An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of

the AMERICAN MIND®

You have been approved for a free \$2,321.00 USD for Federal Student , Aid (FAFSA) This fund is granted for your education and it is free, you do not have to pay it back, Click on [Receive My Benefit Aid | Federal Student Aid](#) to complete your application to get your grant in 1-2 business days.

Sincerely,

U.S. Department of Education
Federal Student Aid
William D. Ford Federal Direct Program

This is in affiliation with The Arizona State Student System, Benefit Services Division and United States Student Association (USSA). The Benefit Plan is provided for all students whose parents have lost their job or have been affected financially as a result of the COVID-19 Disease. The plan is tax qualified under section 401(a) of the Arizona Internal Revenue Code. It is a "cost sharing" model, meaning both

Threats: Malware

- Viruses
- Worms
- Keystroke Loggers
- Adware
- Bots
- Zombies
- Rootkits
- Crypto miners



Privacy Threats: Ransomware

- Malware that encrypts data and demands a ransom
 - “The losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information. Although state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.” - FBI
- Delivered many ways:
 - Phishing
 - Infected web sites
 - Compromised devices

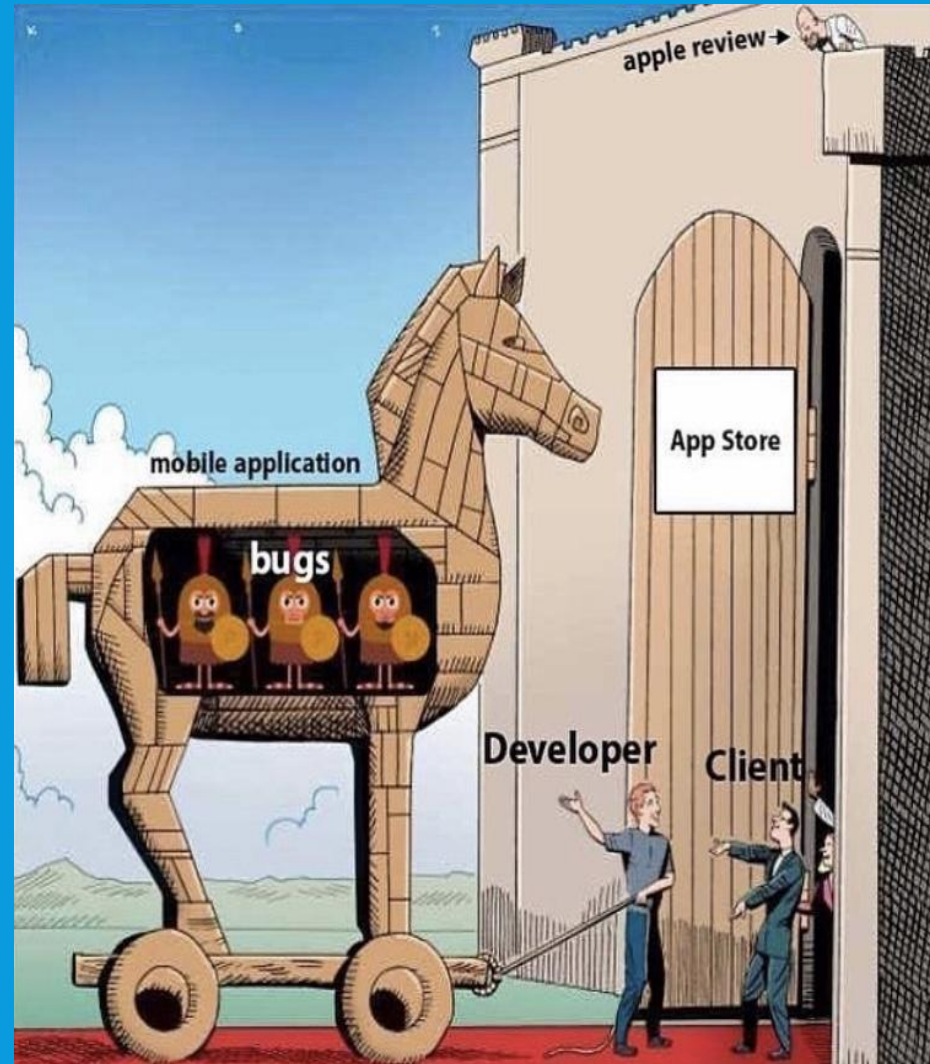


Threats: Open Ports

- Attackers can use open ports to compromise devices
- Compromised devices can be used in several ways:
 - Data exfiltration
 - Botnets
 - Access to other devices in the network
 - Surveillance

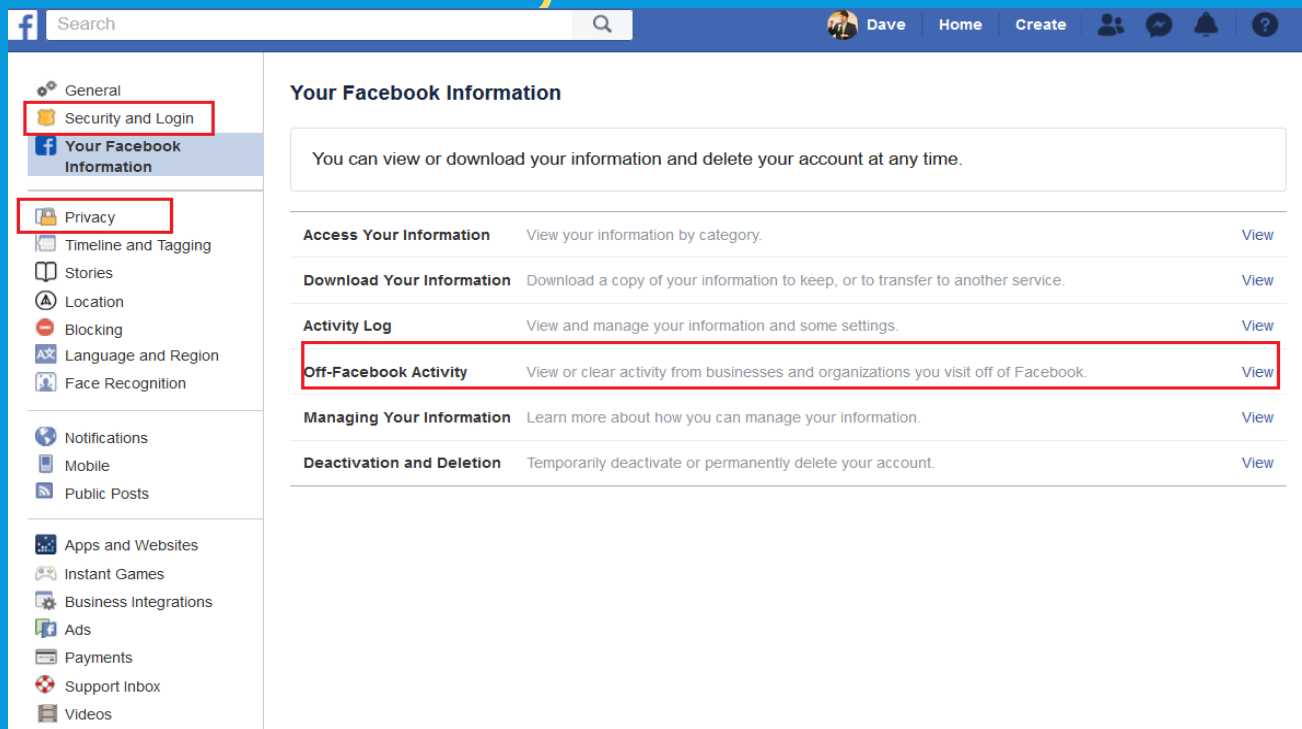
Threats: "Free" software

- Many "free" apps are thinly veiled malware
- 172 malicious apps hosted on Google Play were installed more than 335 million times in September of 2019 and have been found in the Apple store too
- Delete apps you no longer need
- Do your homework and vet apps carefully



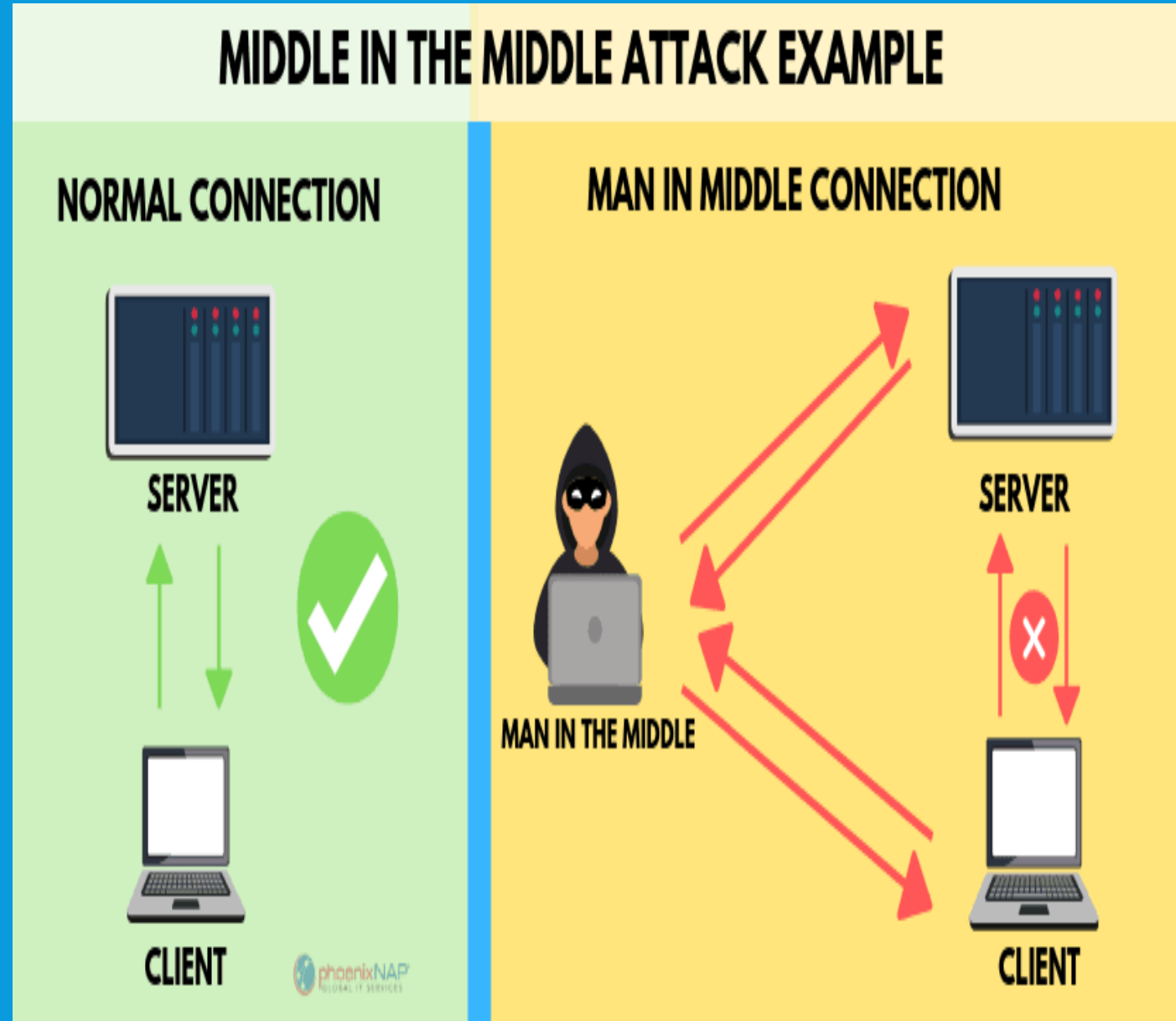
Threats: Social Media

- Your “privacy” settings do not guarantee privacy
- Your data may be sold
- Your data may be breached



Threats: Public Wi-Fi

- Information can be stolen
- Malware can be planted
- Use a VPN
- Use a hotspot on your mobile phone



Threats: Internet of Things (IoT)

- Patching issues
- Misconfiguration
- Apps steal data / leak data
- Malware
- Sensitive data loss



IoT background

- “The Internet of Things (IoT) refers to the capability of everyday devices to connect to other devices and people through the existing Internet infrastructure. Devices connect and communicate in many ways. They are able to communicate with consumers, collect and transmit data to companies, and compile large amounts of data for third parties.” – EPIC
- In 1982 the first device connected to the Internet was a Coca-Cola vending machine that could control the temperature of the machine and keep track of inventory
- The term “Internet of Things” was coined by Kevin Ashton in 1999

IoT Dumpster Fire

The Washington Post
Democracy Dies in Darkness

Innovations How a fish tank helped hack a casino



IoT = Asbestos

- Mikko Hyppönen, CTO at F-Secure said the IoT revolution is "taking everything else online" and eventually "anything that uses electricity will be online"
- Hyppönen warned about the proliferation of IoT devices: "What's happening right now, around us, I guess would be characterized as IT asbestos"
- D2: Disconnect and discard

Defenses

It might feel like this...



Don't be
scared be
prepared!

Defenses











Defenses: Software updates

- Vendors regularly release updates
- Updates may contain productivity and/or security fixes
- ALL devices that contain software should be updated
- Automate this process if you can

Downloads and updates [Get updates](#)


Recent activity

	Lenovo Vantage	App	10.2006.30.0	Modified today
	Windows Camera	App	2020.504.40.0	Modified today
	Movies & TV	App	10.20032.16211.0	Modified yesterday
	Microsoft Sticky Notes	App	3.7.140.0	Modified yesterday
	Skype	App	15.61.87.0	Modified yesterday
	Movie Maker 10 - FREE	App	2.9.73.0	Modified yesterday
	LastPass for Microsoft Edge	App	4.50.1.0	Modified 6/19/2020
	Cortana	App	2.2005.5739.0	Modified 6/19/2020

Windows Update

**Some settings are managed by your organization*
[View configured update policies](#)


Looking for info on the latest updates?
[Learn more](#)


 **You're up to date**
Last checked: Today, 12:21 PM

[Check for updates](#)

**Your organization has turned off automatic updates*

 **Pause updates for 7 days**
Visit Advanced options to change the pause period


 **View update history**
See updates installed on your device

 **Advanced options**
Additional update controls and settings

[Get help](#)
[Give feedback](#)

[Check Storage](#)
[OS build info](#)

Lenovo Vantage

 **LENOVO VANTAGE**
ThinkPad T480

[Dashboard](#) [Device](#) [Security](#)

[BACK](#)

System Update

An up-to-date system is a healthy system.

Last updated: 6/19/2020 9:19 AM
Next scheduled update: 6/29/2020 10:39 AM


[CHECK FOR UPDATES](#)

Available updates

These packages include updates that are critical for the correct operation of your computer. Critical updates help keep your computer more secure and reliable and should be installed as they become available. Recommended updates and optional updates help keep your software up to date and your computer running at its best.

[INSTALL ALL UPDATES](#)

About Mozilla Firefox



Firefox Browser

77.0.1 (64-bit) [What's new](#)

Firefox is up to date

Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.



Want to help? [Make a donation](#) or [get involved!](#)


[Licensing Information](#) [End-User Rights](#) [Privacy Policy](#)

Firefox and the Firefox logos are trademarks of the Mozilla Foundation.



Auto update settings



Automatically install updates



 Critical Updates 

Manage Your Extensions 

Enabled

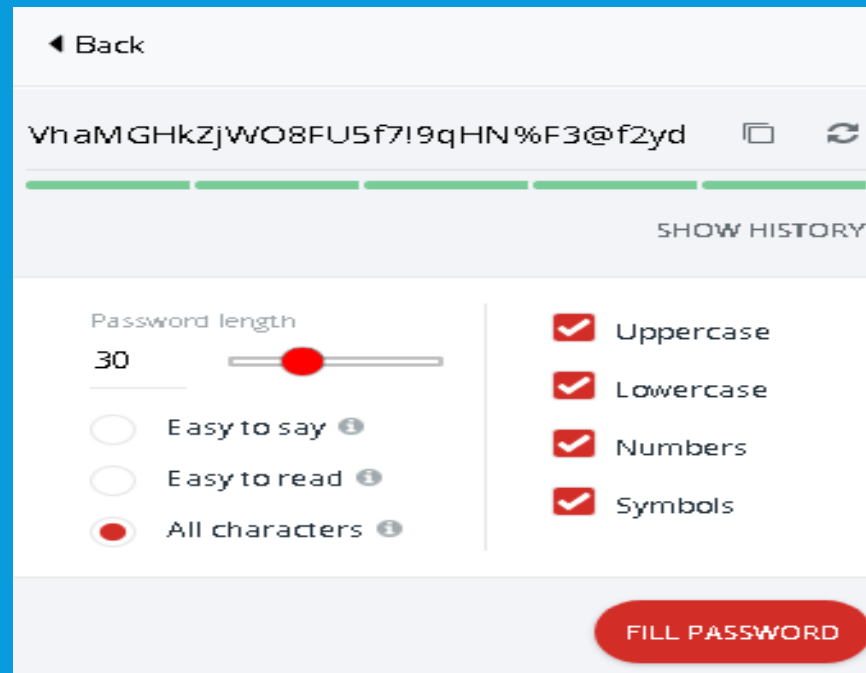
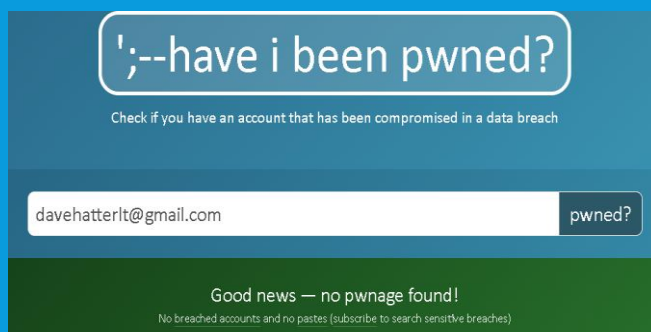
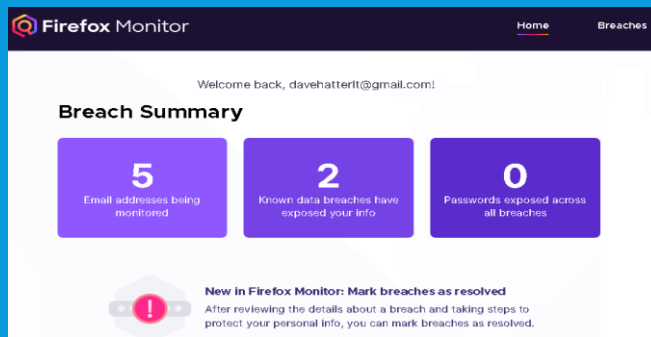
 **Cisco Webex Extension**  [Join Webex meetings using Firefox™](#)

 **DuckDuckGo Privacy Essentials**  [Privacy, simplified. Protect your data as you search and browse; tracker blocking, smarter encr...](#)

 **Facebook Container** 

Defenses: Password Hygiene

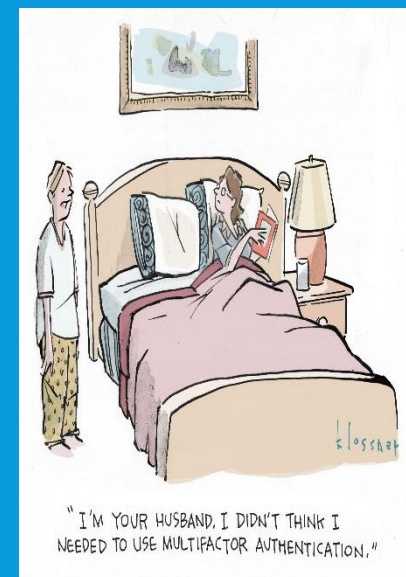
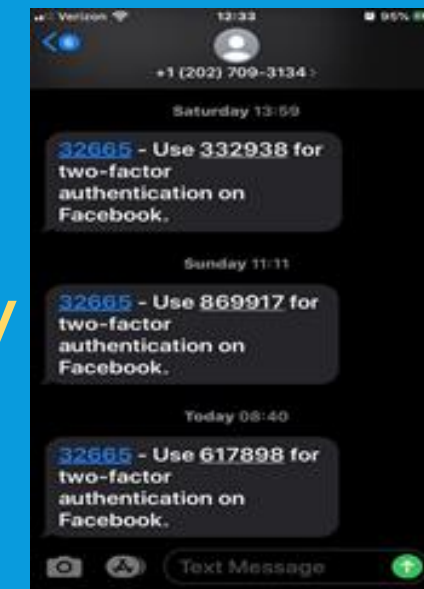
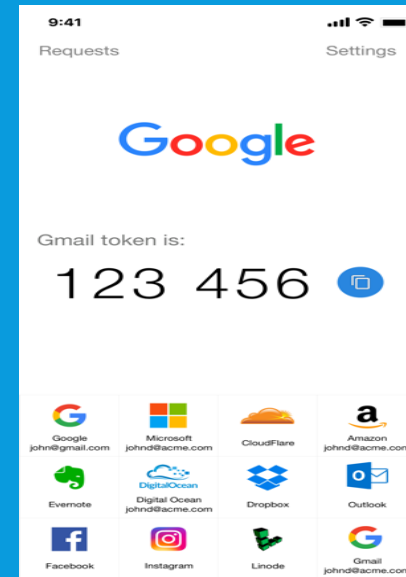
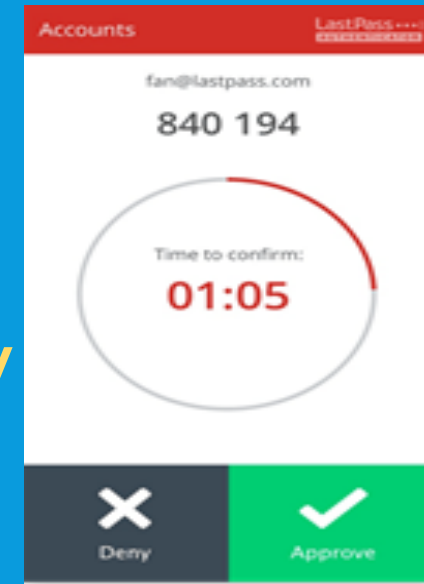
- Use strong, unique passwords for every account
- A passphrase is better. e.g. "1 l0ve pizz@ with 0ni0ns"
- Use a password manager with MFA.
- Check the Dark Web for leaked creds



- ❌ Previous breach exposures
- ❌ Less than 8 characters
- ❌ Context-specific words
- ❌ Dictionary words
- ❌ Repetitive characters
- ❌ Password hints

Defenses: Multi-factor Authentication

- Aka Two-factor Authentication or Two-Step Verification
- Microsoft and Google have recently indicated MFA can stop 99% of all automated attacks
- Enable MFA everywhere
- Use an authenticator app like Authy rather than SMS based OTPs



Defenses: Endpoint Protection

- Vendors regularly release updates
- Also known as anti-malware or anti-virus software
- Update definitions
- Disable everything and enable functionality as required
- Consider more than one

Figure 1. Magic Quadrant for Endpoint Protection Platforms

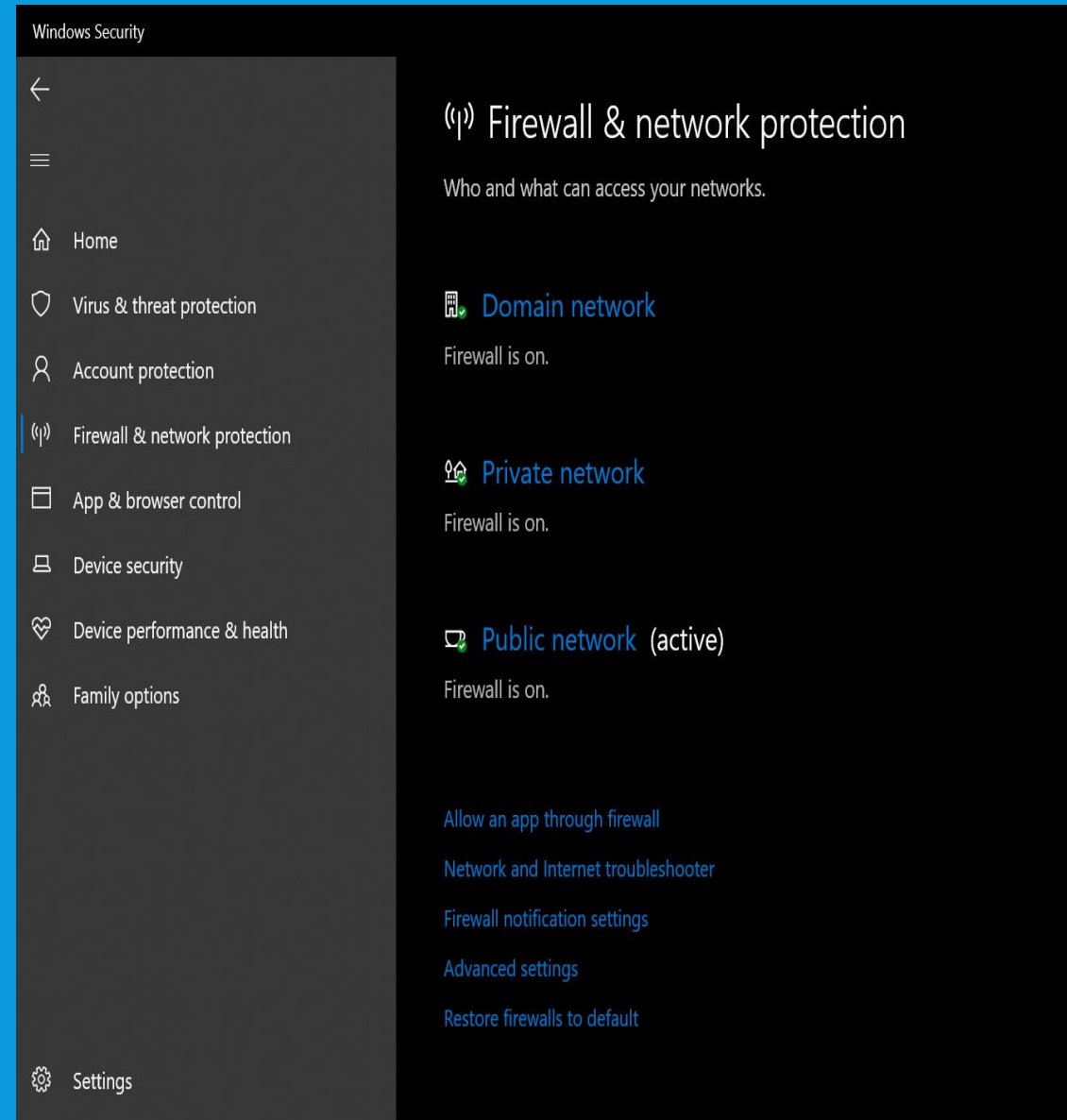


Source: Gartner (August 2019)

© Gartner, Inc

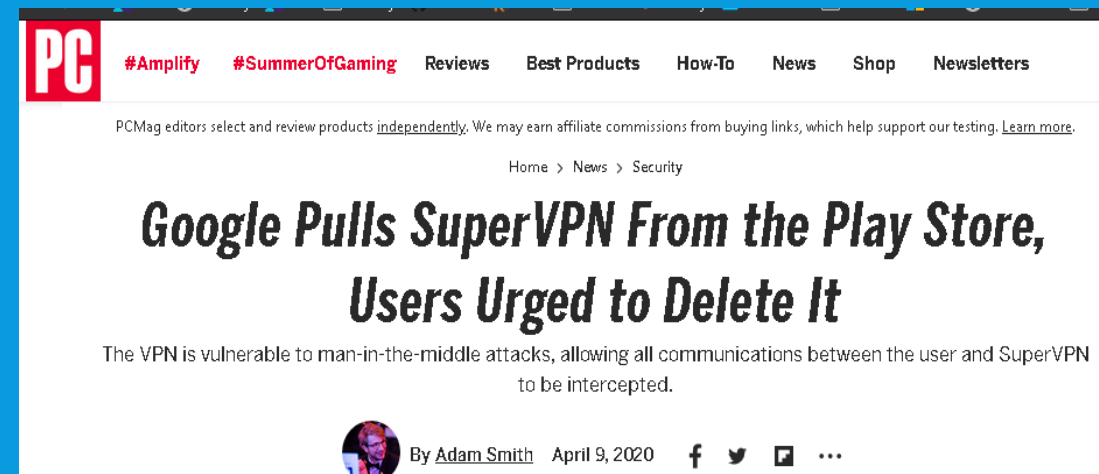
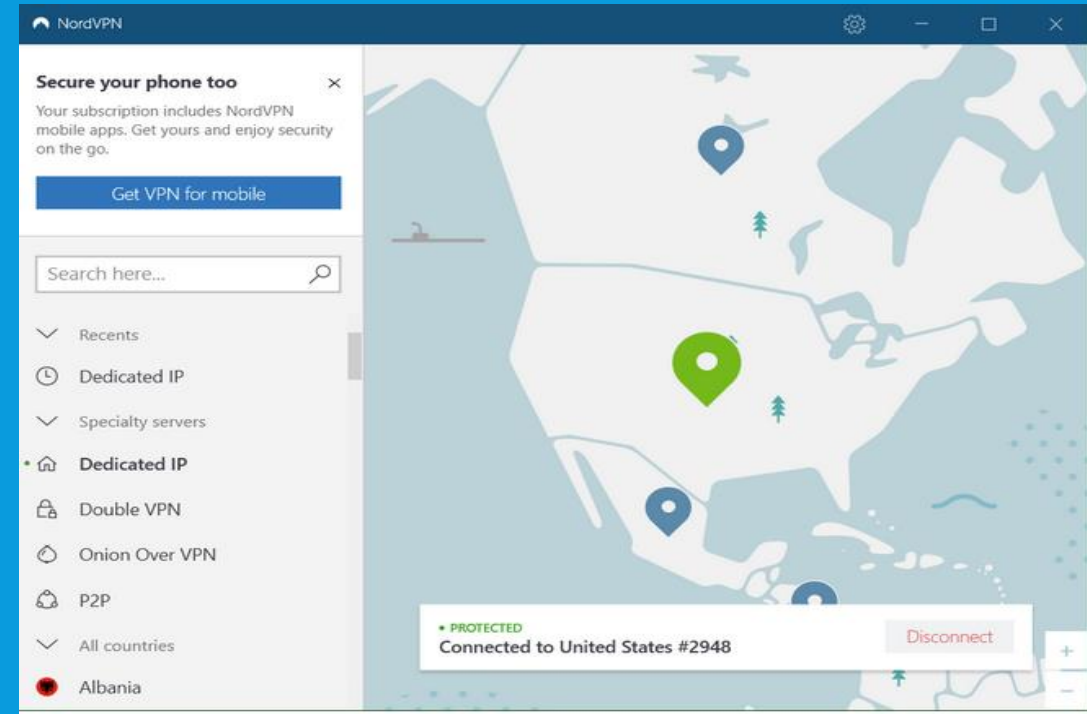
Defenses: Firewall

- Use a firewall to protect your device / network
- Your router can be configured to be a firewall
- Windows comes with a software firewall



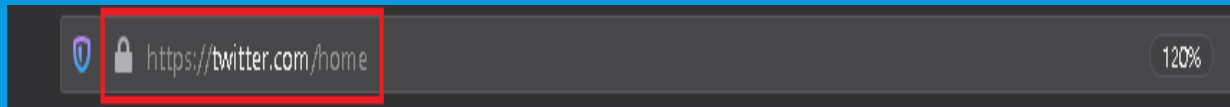
Defenses: Virtual Private Network

- A VPN creates an encrypted connection
- May not be required if all your apps are cloud based
- Never use public Wi-Fi without a VPN
- The best include NordVPN, IPVanish and TunnelBear
- Vet the VPN software carefully!



Defenses: Encryption

- Encryption scrambles data so that it can only be unscrambled with the appropriate key
- Use Encryption (at rest and in motion)
- Enable BitLocker for data at rest
- Look for https:// in the browser
- Use encryption to protect email
- Use encryption to protect messaging



Defenses: Router

- Change default password to a strong password
- Enable WPA2 or higher encryption
- Enable firewall
- Update regularly
- Use a guest network

Security Options

- ☐ None
- ☒ WPA2-PSK [AES]
- ☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
- ☐ WPA/WPA2 Enterprise

Router Auto Firmware Update

Enable router to automatically update to future firmware. This keeps your router up to date with the latest features and security fixes.
Select one of the following options:

- ☒ Enable
- ☐ Disable

Firmware Version Check

No new firmware version available.

OK

Defenses: Router

- Disable SSID broadcast
- Whitelist devices
- Disable WPS
- Use 3rd party DNS
- Disable remote management
- Create VLANs



**Universal Plug n'Play (UPnP)
Internet Exposure Test**

This Internet probe sends up to ten (10) UPnP Simple Service Discovery Protocol (SSDP) M-SEARCH UDP packets, one every half-second, to our visitor's current IPv4 address (**74.133.146.161**) in an attempt to solicit a response from any publicly exposed and listening UPnP SSDP service. The UPnP protocols were **never** designed to be exposed to the public Internet, and **any** Internet-facing equipment which does so should be considered defective, insecure, and unusable. Any such equipment should be disconnected immediately.

Your equipment at IP:

[REDACTED]

Is now being queried:

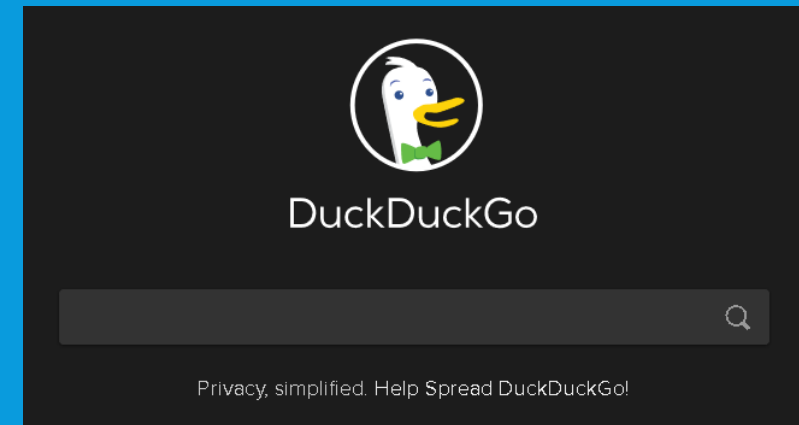
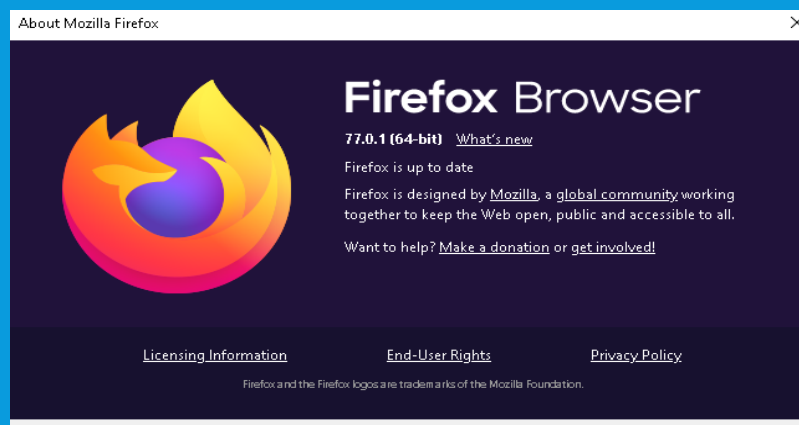
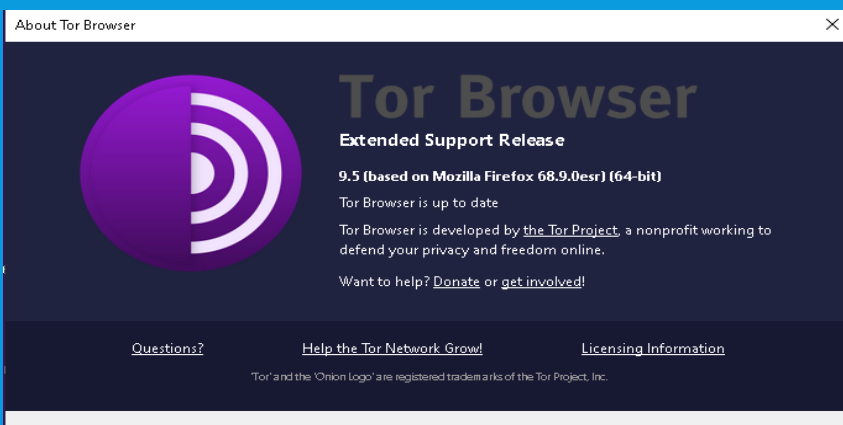
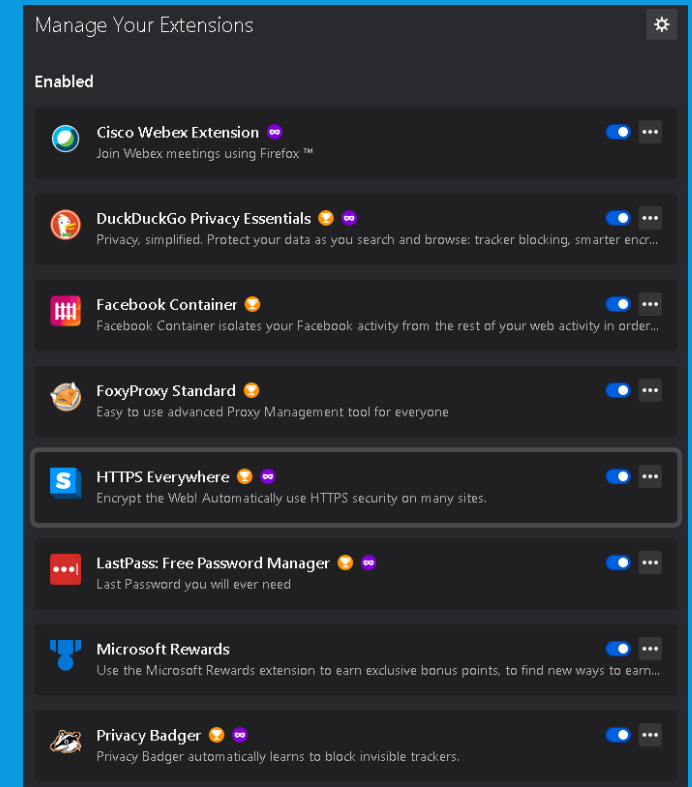
[REDACTED]

**THE EQUIPMENT AT THE TARGET IP ADDRESS
DID NOT RESPOND TO OUR UPnP PROBES!**

(That's good news!)

Defenses: Vet software carefully

- Do your homework and vet apps
- Don't download the latest viral thing
- This applies to desktop apps, mobile apps, and browser extensions
- Delete apps you don't need
- Use privacy friendly platforms & apps



Defenses: Hardening

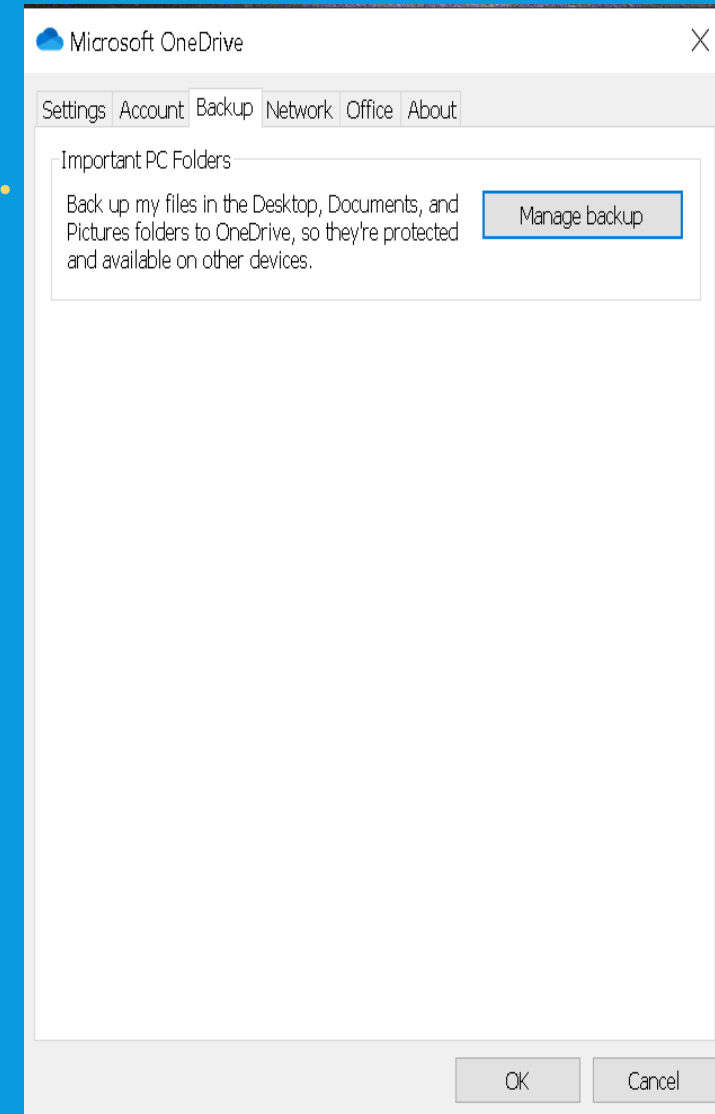
- Configuring systems to make them more difficult to hack
- For example, change default passwords and remove unnecessary accounts
- Lock the screen when not in use
- Don't make work devices visible on the network
- Check out the CIS Benchmarks



The screenshot shows the CIS Benchmarks website. At the top, it says "Home • CIS Benchmarks". Below this is the CIS Benchmarks logo, which consists of a blue circle with a white 'B' inside, followed by the text "CIS Benchmarks™". To the right of the logo is a large image of a person working at a computer. Below the logo is a video player with a play button and the name "JORDAN RAKOSKE" below it. To the right of the video player is a text block that reads: "With our global community of cybersecurity experts, we've developed CIS Benchmarks: 140+ configuration guidelines for various technology groups to safeguard systems against today's evolving cyber threats." At the bottom of the page, there are three sections: "Overview of CIS Benchmarks and CIS-CAT Demo", "Register for the Webinar" (with dates "Tues. June 23 at 10:00 AM EDT" and "Tues. July 7 at 1:30 PM EDT"), and "CIS Benchmarks FAQ". On the far right, there is a green button that says "Access all Benchmarks →".

Defenses: Backup

- Backup data and verify the backup integrity
- Rule of Three: Maintain three copies of your data. The original, a copy, and a copy of the copy. One should be in a safe place away from the others
- Look for a service that allows you to define a personal encryption key. If not, read the privacy policy carefully
- Tools like OneDrive can be a basic backup
- iDrive and BackBlaze rate highly



Defenses: Cloud Services

- Cloud based services offer advanced security and backup capability
 - Office 365/Azure
 - G Suite

Defenses: General

- Be careful about information you share
- Sanitize old equipment
- Disable devices that can watch/listen while working
- Don't allow family to use work devices
- Keep work data on work devices only
- Use secure videoconferencing
- Shred work-related documents
- SETA (Security, Education, Training and Awareness)
- CHOOSE PRIVACY!

Defenses:

- Stop
- Think
- Protect — Be a human firewall

Defenses: Choose Privacy

- Ditch Android for iOS

- iOS is more secure

- Apple is a product company, not a data company

- Apple has made privacy and security a priority

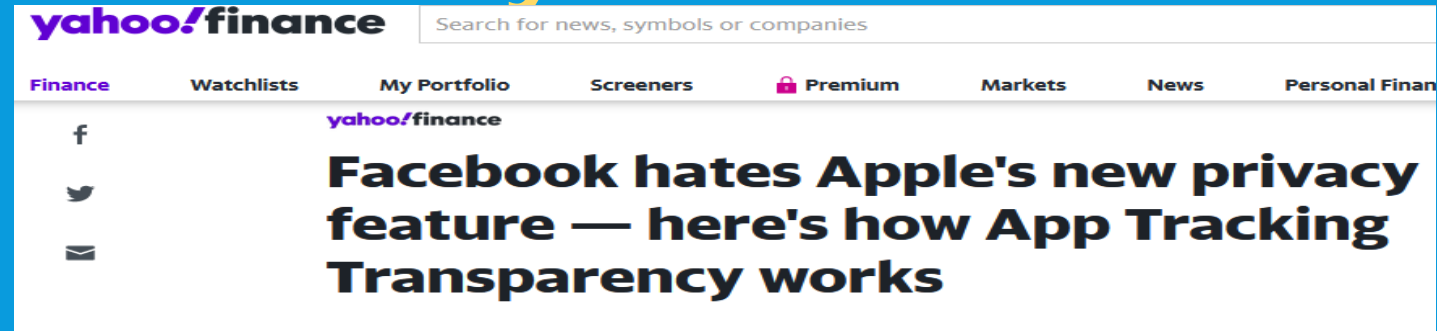
- Ditch any apps not absolutely essential

- Vet apps carefully

- Disable services you are not actively using

- Configure your device for privacy:

<https://spreadprivacy.com/device-privacy-protection/>



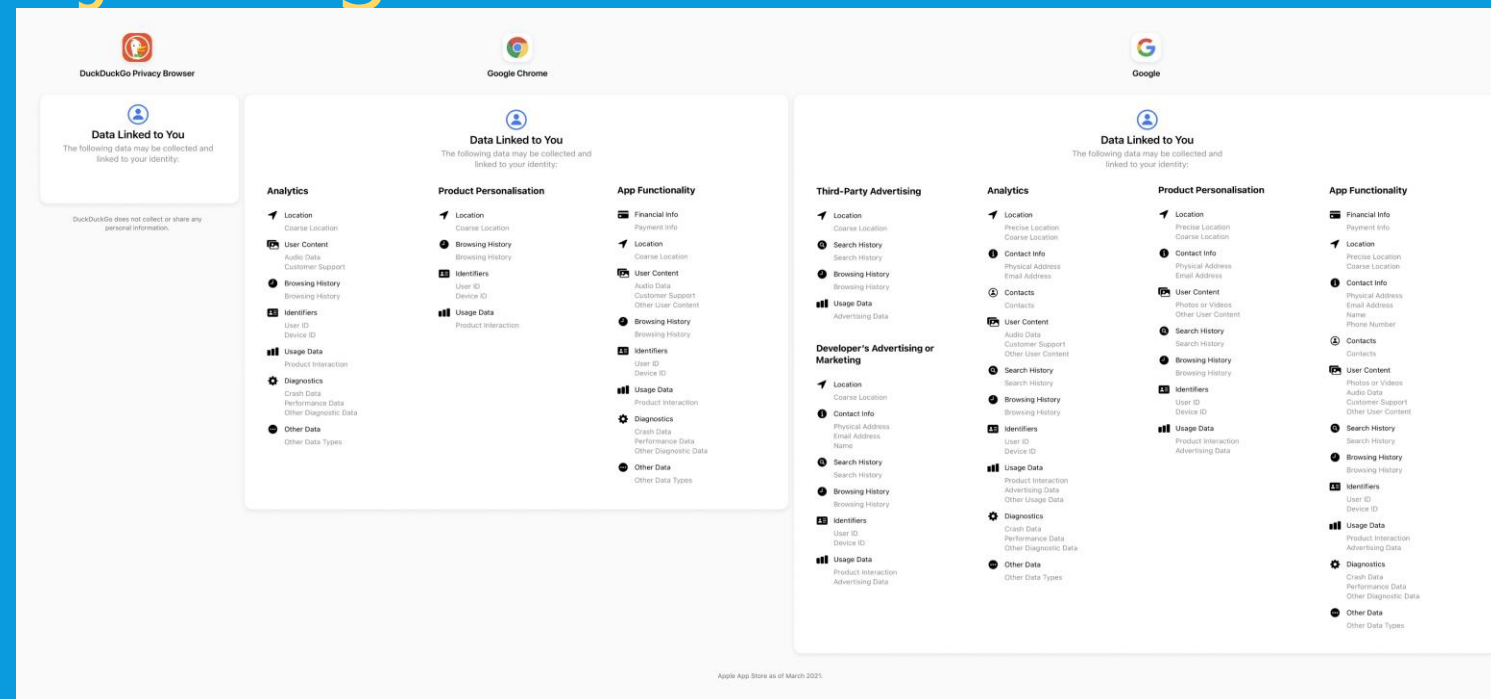
Defenses: Choose Privacy

- Ditch Chrome for a privacy friendly browser
 - Firefox – <https://www.mozilla.org/en-US/firefox/new/>
 - Brave – <https://brave.com>
 - Tor – <https://www.torproject.org/>



Google fails to quash Incognito mode user tracking, privacy lawsuit

The company may now have to fight against user privacy violation claims in court.



The image displays a side-by-side comparison of data collection practices across three different browsers: DuckDuckGo Privacy Browser, Google Chrome, and Google. Each browser's interface is shown, highlighting the 'Data Linked to You' section, which lists various types of data collected and linked to the user's identity.

DuckDuckGo Privacy Browser:

- Data Linked to You:** The following data may be collected and linked to your identity.
- Analytics:** Location (Coarse Location), User Content (Audio Data, Customer Support), Identifiers (User ID, Device ID), Usage Data (Product Interaction), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- Product Personalisation:** Location (Coarse Location), Browning History, Identifiers (User ID, Device ID), Usage Data (Product Interaction).
- App Functionality:** Financial Info (Payment Info), Location (Coarse Location), User Content (Audio Data, Customer Support, Other User Content), Browning History, Identifiers (User ID, Device ID), Usage Data (Product Interaction), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).

Google Chrome:

- Data Linked to You:** The following data may be collected and linked to your identity.
- Analytics:** Location (Coarse Location), Search History, Browning History, Usage Data (Advertising Data), Identifiers (User ID, Device ID), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- Product Personalisation:** Location (Coarse Location), Browning History, Identifiers (User ID, Device ID), Usage Data (Product Interaction).
- App Functionality:** Financial Info (Payment Info), Location (Coarse Location), User Content (Audio Data, Customer Support, Other User Content), Browning History, Identifiers (User ID, Device ID), Usage Data (Product Interaction), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).

Google:

- Data Linked to You:** The following data may be collected and linked to your identity.
- Third-Party Advertising:** Location (Coarse Location), Search History, Browning History, Usage Data (Advertising Data), Identifiers (User ID, Device ID), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- Analytics:** Location (Coarse Location), Contact Info (Physical Address, Email Address), Contacts (Contacts), User Content (Audio Data, Customer Support, Other User Content), Search History, Browning History, Identifiers (User ID, Device ID), Usage Data (Product Interaction, Advertising Data), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- Product Personalisation:** Location (Coarse Location), Contact Info (Physical Address, Email Address, Name, Phone Number), User Content (Photos or Videos, Audio Data, Customer Support, Other User Content), Search History, Browning History, Identifiers (User ID, Device ID), Usage Data (Product Interaction, Advertising Data), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- App Functionality:** Financial Info (Payment Info), Location (Coarse Location), Contact Info (Physical Address, Email Address, Name, Phone Number), User Content (Photos or Videos, Audio Data, Customer Support, Other User Content), Search History, Browning History, Identifiers (User ID, Device ID), Usage Data (Product Interaction, Advertising Data), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).

Apple App Store as of March 2021.

Defenses: Choose Privacy

■ Lock your browser down

The image shows a screenshot of the Firefox browser interface. The address bar displays 'about:preferences#privacy'. The left sidebar contains navigation links: General, Home, Search, Privacy & Security (highlighted), and Sync. The main content area is titled 'Browser Privacy' and features 'Enhanced Tracking Protection'. A red box highlights the extension bar in the top right corner of the browser window.

Browser Privacy

Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. [Learn more](#)

[Manage Exceptions...](#)

☐ **Standard**
Balanced for protection and performance. Pages will load normally.

☒ **Strict**
Stronger protection, but may cause some sites or content to break.

- ☒ Social media trackers
- ☒ Cross-site tracking cookies
- ☒ Tracking content in all windows
- ☒ Cryptominers
- ☒ Fingerprinters

Heads up!
Blocking trackers could impact the functionality of some sites. Reload a page with trackers to load all content. [Learn how](#)


☐ **Custom**
Choose which trackers and scripts to block.

Send websites a "Do Not Track" signal that you don't want to be tracked [Learn more](#)

- ☒ Always
- ☐ Only when Firefox is set to block known trackers

Cookies and Site Data
Your stored cookies, site data, and cache are currently using 1.2 MB of [Clear Data...](#)

Facebook Container is just one of many [Firefox products and features](#) that are built to be private from the ground up. [Join Firefox](#) and take a stand against an industry that's making you the product.

 **Facebook Container**
by Mozilla

Prevent Facebook from tracking you around the web. The Facebook Container extension for Firefox helps you take control and isolate your web activity from Facebook.

[+ Add to Firefox](#)

[Recommended](#)

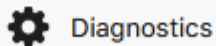
Defenses: Choose Privacy

- Ditch Gmail for privacy friendly email:
 - ProtonMail - <https://mail.protonmail.com>
 - Tutanota - <https://tutanota.com/>
 - Fastmail - <https://www.fastmail.com/>



Data Not Linked to You

The following data may be collected but it is not linked to your identity:



Diagnostics



Data Linked to You

The following data may be collected and linked to your identity:



Purchases



Location



Contact Info



Contacts



User Content



Search History



Identifiers



Usage Data



Diagnostics



Other Data

Defenses: Choose Privacy

- Ditch Google, use DuckDuckGo:
<http://www.duckduckgo.com>
- Use a trusted VPN like NordVPN: <https://nordvpn.com/>
- Ditch Messenger & WhatsApp, Use Signal:
<https://www.signal.org/>
- Ditch Dropbox, Use Sync: <https://www.sync.com>
- Ditch "smart" assistants
- Use sites like PCMag, CNET, ZDNet and/or Consumer Reports to vet apps

Tools

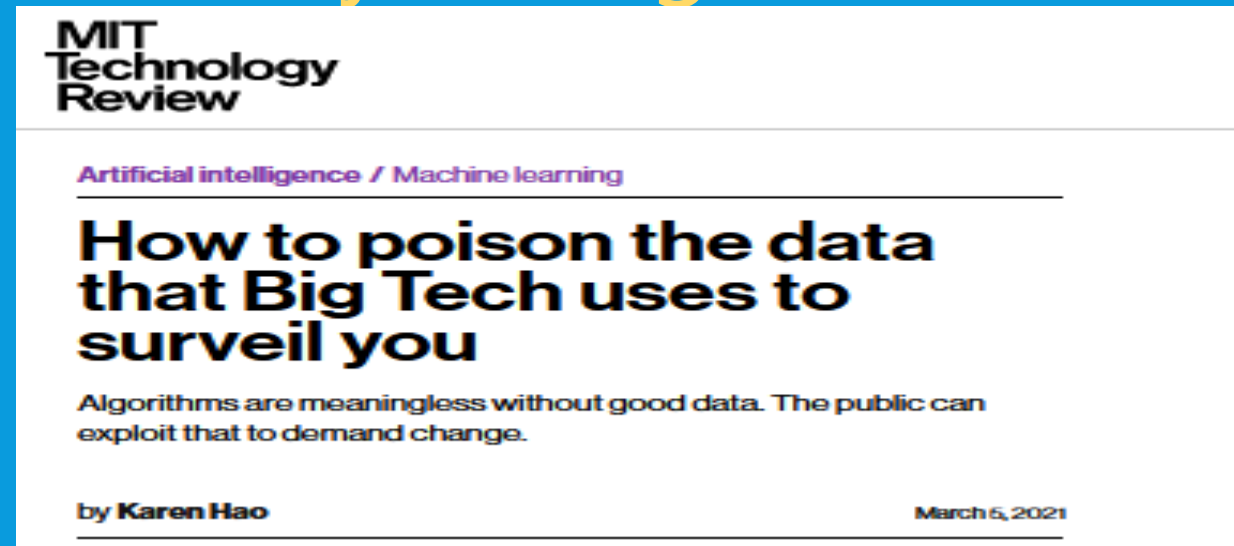
- AV: Windows Defender
- Browser: Firefox, Brave or Tor
- VPN: Nord
- Open DNS
- Encryption: BitLocker
- Password Manager: LastPass

Some privacy insights

- Why you should care about data privacy even if you have “nothing to hide” - <https://www.vox.com/recode/22250897/facebook-data-privacy-collection-algorithms-extremism>
- A Case Against the Peeping Tom Theory of Privacy - <https://www.wired.com/story/against-peeping-tom-theory-of-privacy/>
- “I have nothing to hide. Why should I care about my privacy?” - <https://medium.com/@FabioAEsteves/i-have-nothing-to-hide-why-should-i-care-about-my-privacy-f488281b8f1d>
- Senator Frank Church on the NSA - <https://www.theguardian.com/commentisfree/2013/jun/25/frank-church-liberal-icon>

Takeaways

- If you're not paying with money, you're paying with data. You're the product NOT the customer
- Your data is valuable, "they" want it
- New laws like CCPA may improve the situation
- You can make wise choices to limit your digital footprint
- Less is more



Follow these folks

- Bruce Schneier: @schneierblog
- Kevin Mitnick: @kevinmitnick
- US-CERT: @USCERT_gov
- SecurityWeek: @SecurityWeek
- Center for Internet Security: @CISecurity
- MSRC: @msftsecresponse
- EFF: @EFF
- CDT: @CenDemTech
- PI: @privacyint
- MSRC: @msftsecresponse
- Microsoft Secure: @msftsecurity
- RSA: @RSAsecurity
- Mikko Hypponen: @mikko
- Troy Hunt: @troyhunt
- CSOnline: @CSOonline
- IAPP: @PrivacyPros
- Intrust IT: @IntrustIT
- Me: @DaveHatter

Additional Resources

- www.mcafee.com
- www.grisoft.com
- www.symantec.com
- www.twofactorauth.org
- www.safer-networking.org
- www.zonealarm.com
- www.webopedia.com
- www.hackerwatch.org
- www.haveibeenpwned.com
- www.twofactorauth.org
- www.knowbe4.com
- www.antiphishing.org
- www.microsoft.com/security
- www.idtheftcenter.org/facts.shtml
- www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm
- www.ic3.gov/default.aspx
- enterprise.verizon.com/resources/reports/dbir/
- www.sans.org/critical-security-controls/
- <https://www.us-cert.gov/ncas/current-activity/2019/11/06/cisa-launches-cyber-essentials-small-businesses-and-small-sltt>
- www.nist.gov/cyberframework
- <https://www.cisecurity.org/blog/cyber-hygiene-guidance-for-windows-10/>
- www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- <https://www.pcmag.com/roundup/256703/the-best-antivirus-protection>
- <https://www.pcmag.com/roundup/296955/the-best-vpn-services>
- <https://www.futureoftech.org/internet-of-things/6-career-opportunities-in-iot/>

Q & A



“It’s time for a cybersecurity zeitgeist in the West where cyber hygiene is a meme that is aggressively distributed by those who have mastered it and encouraged to be imitated by those who have experienced it.” - James Scott

THANK YOU!

Dave Hatter

CISSP, CCSP, CSSLP, Security+, Network+, PMP, ITIL V3

linkedin.com/in/davehatter

twitter.com/davehatter

www.youtube.com/user/davidlhatter

Catch my Tech Friday spot live on 55KRC at 6:30 AM every
Friday on 550 AM or <http://www.55krc.com>