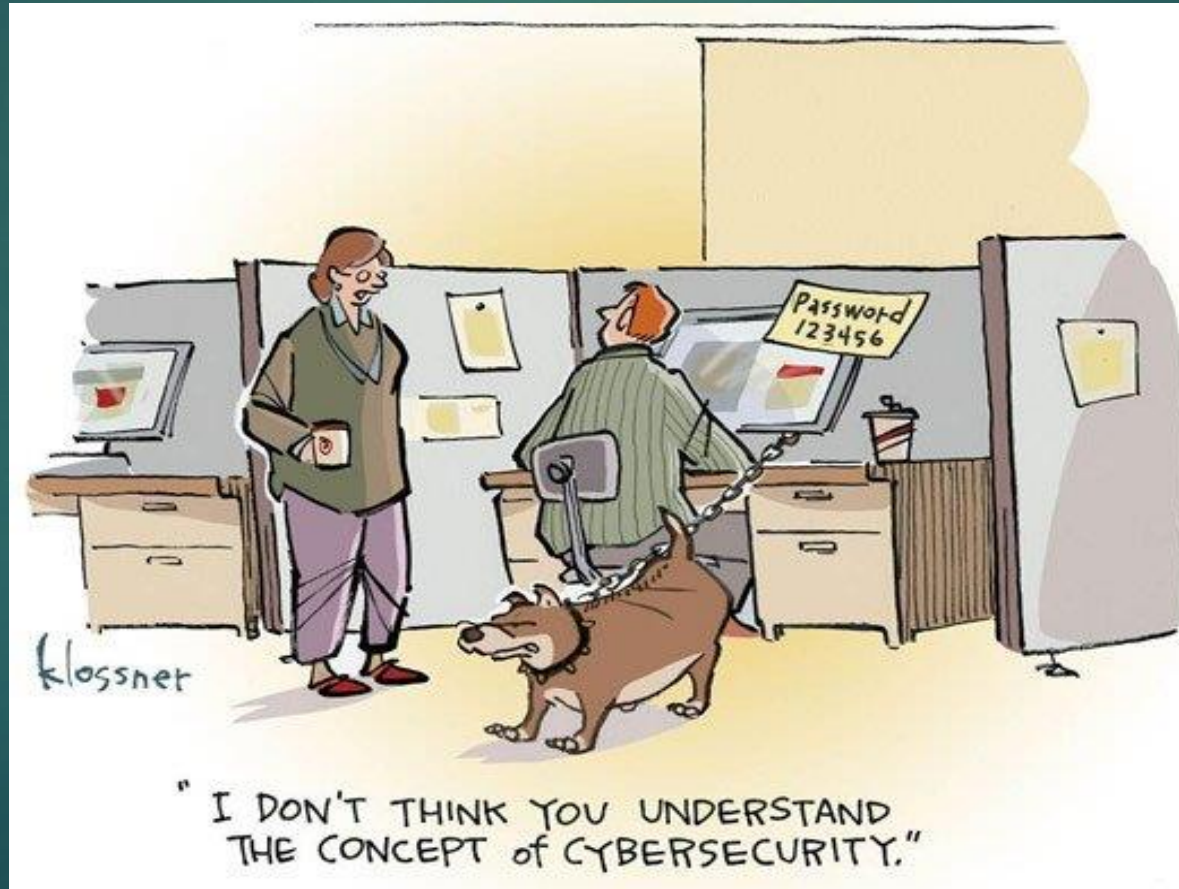


TAMIDS- Tutorial Series

1

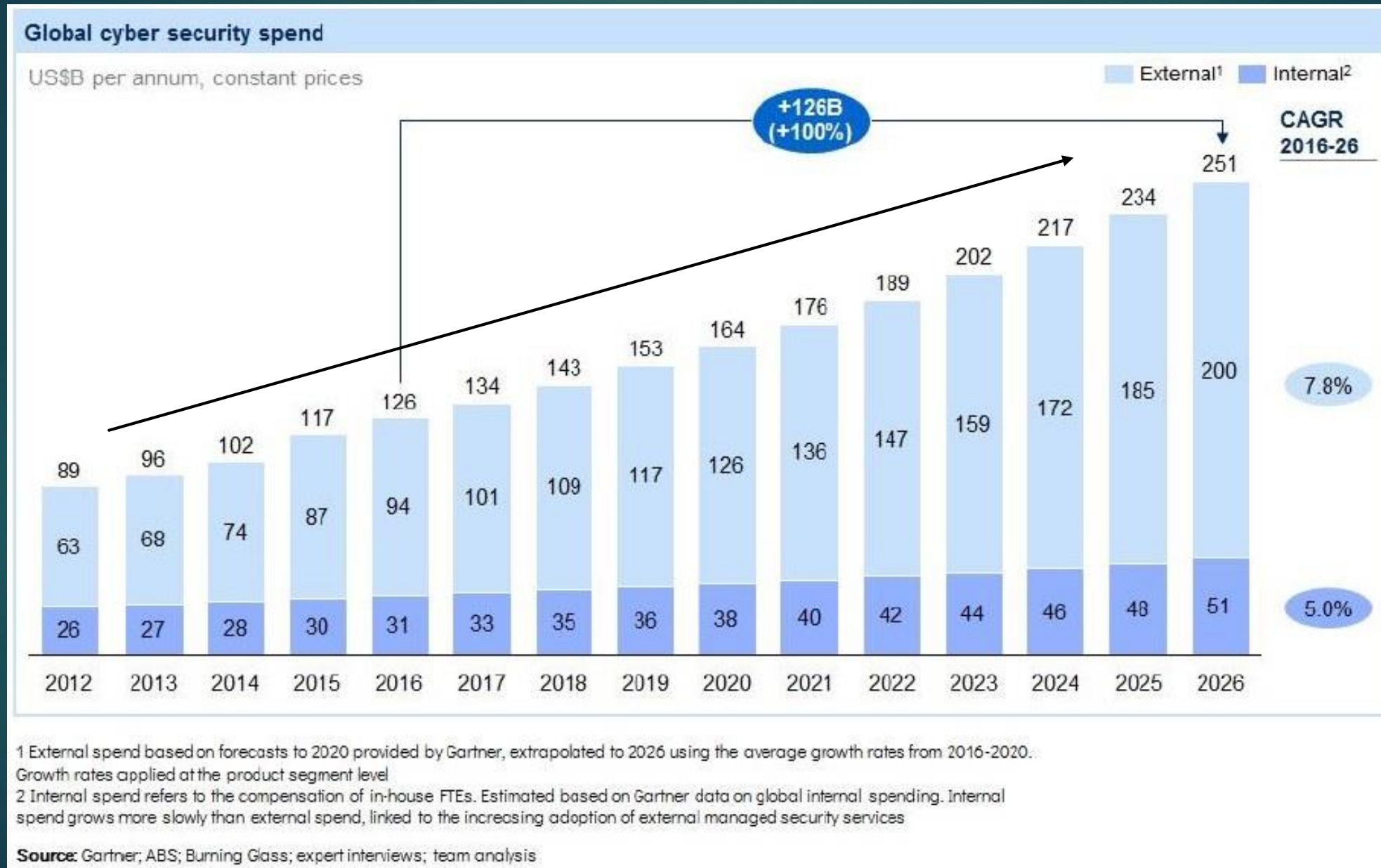
“MANAGE YOUR DIGITAL FOOTPRINTS”

DR. RAVI SEN, DEPARTMENT OF INFO & OPS MANAGEMENT, TAMU



Cybersecurity Spending (in billion US \$)

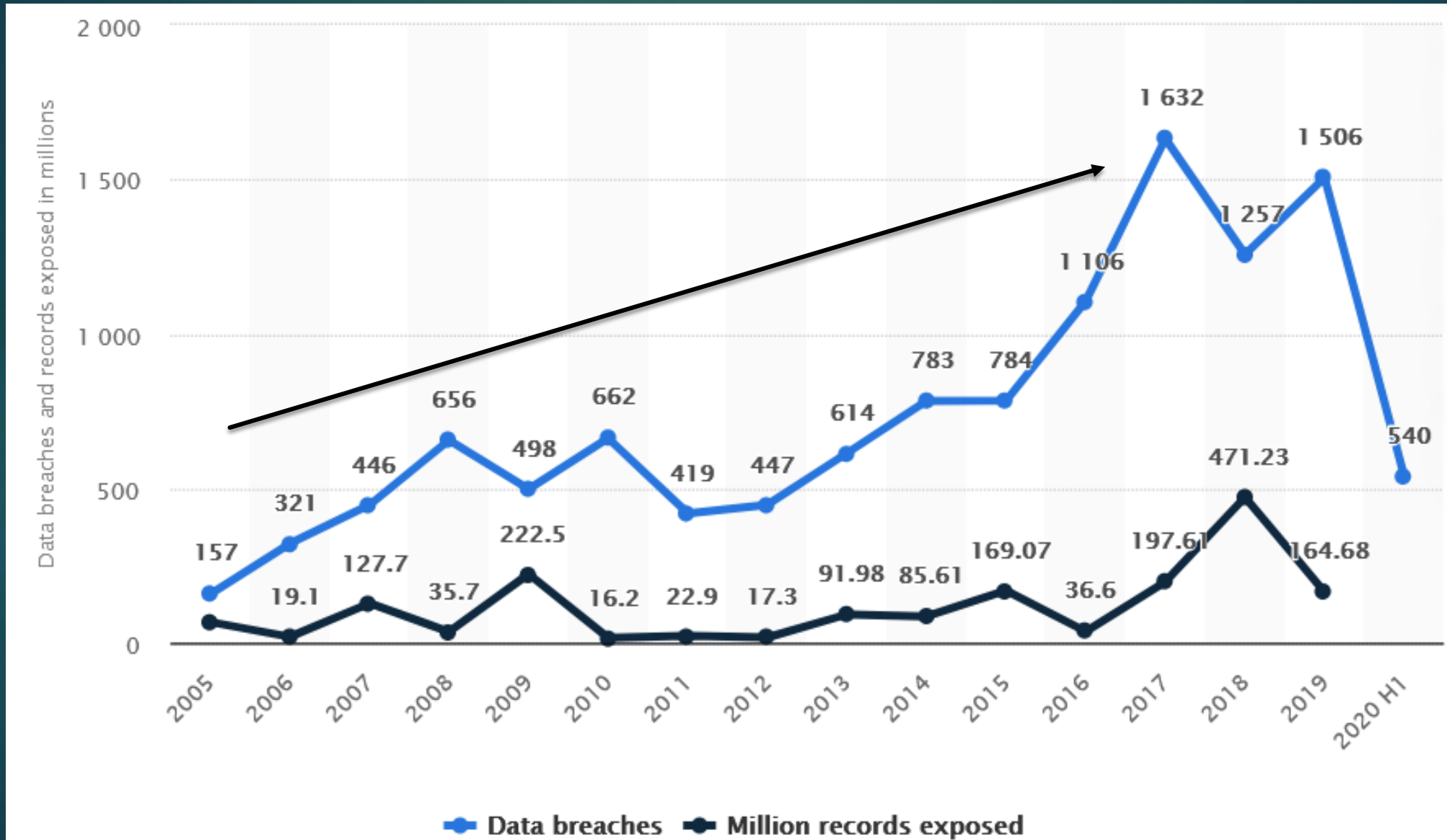
2



Annual Number of Data Breaches & Exposed Records in the USA (2005- 1st Half of 2020)

[Image via Statista.com. ©Statista 2021]

3



Who All Share the Blame?



Vulnerable Software, Complex Operating Environment

5

Targeting Industries &
Protected Data

Weak, not clear

Delayed Updates
Delayed Patching
Weak Credentials



Clueless, Careless,
Unaware Users



Release First
Patch Later

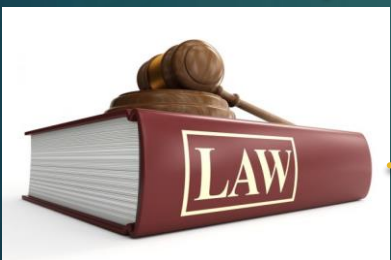
Bad Code

Information

Asymmetry



Asymmetric
Conflict



Laws & Regulations

Targeting Threat Agents



Market for SW
Vulnerabilities

We play an important role in strengthening cybersecurity.

But do we know it? For example-

Top 10 most popular passwords (2020)

Source: <https://nordpass.com/most-common-passwords-list/>

7

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213
11. ↑ (12)	1234567	165,909	Less than a second	2,516,606

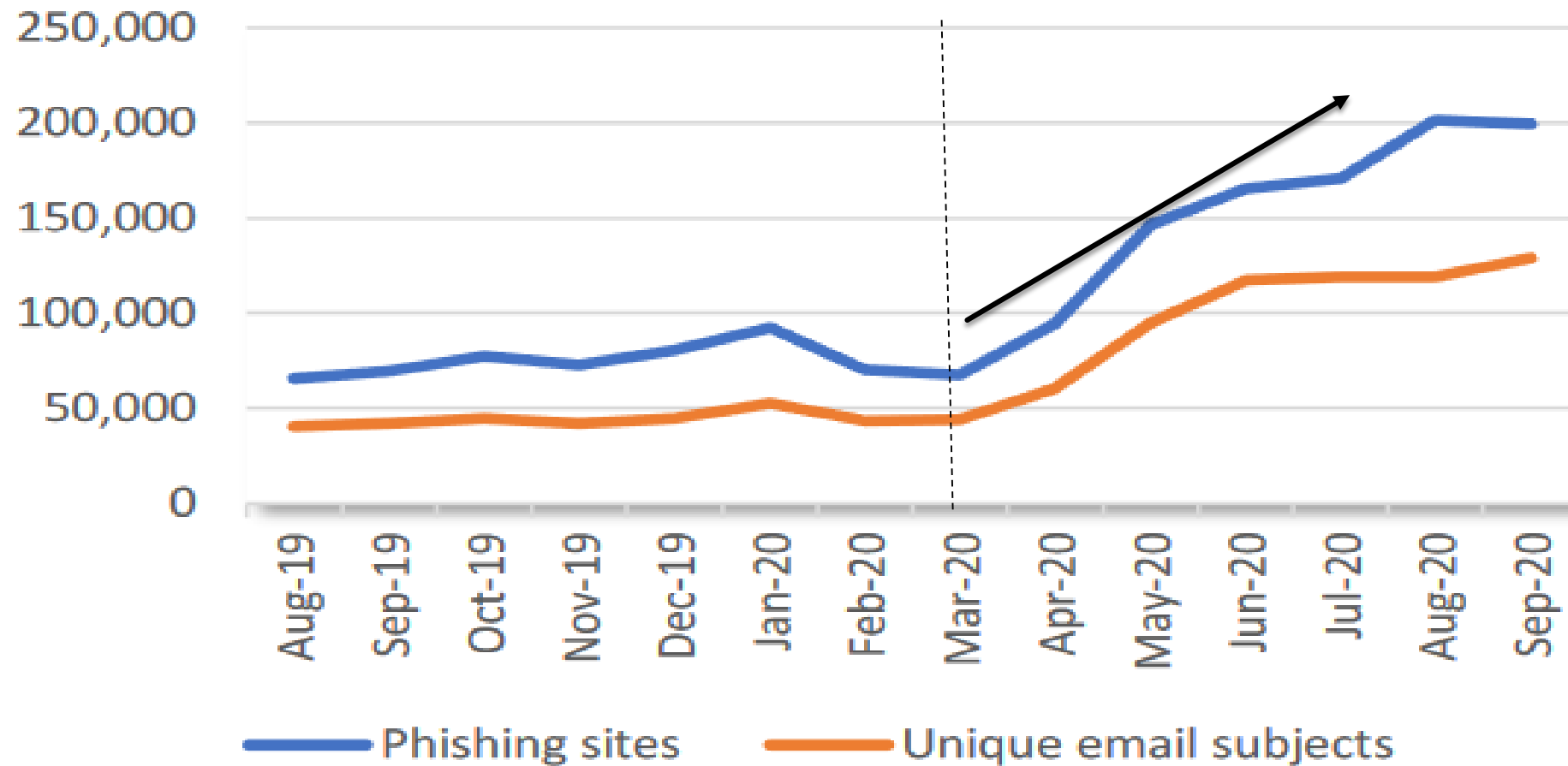
So What? How does this relate to my digital footprints?

8

- ▶ Let us take a look at one of the most common attacks
- ▶ **Phishing attacks**- Almost 147,000 in first half of 2020

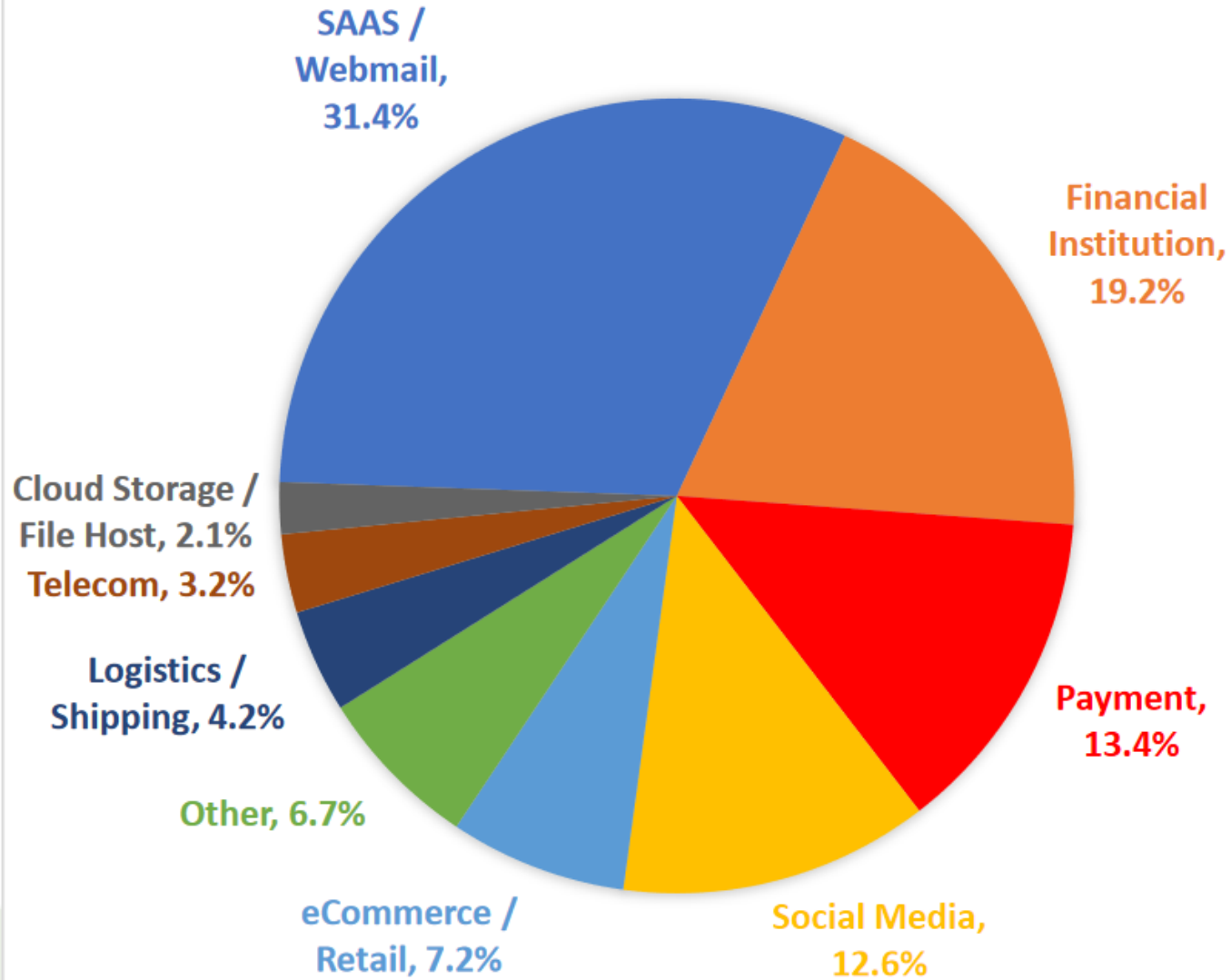
[Source: APWG Phishing Activities Trend Report Q3-2020 available at https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf]

Phishing Activity, 3Q 2019 to 3Q 2020



Source: APWG Phishing Activities Trend Report Q3-2020
[https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf]

MOST-TARGETED INDUSTRY SECTORS, 3Q 2020



Source: APWG Phishing Activities Trend Report Q3-2020
[https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf]

Types of Phishing Attacks

11

- ▶ **Vishing** is a type of attack done through Voice over IP (VoIP), e.g. IRS scams
- ▶ **SMiSHing** is done over the phone but in the form of text messages
- ▶ **Social Media Deception** – Fake profiles are used to befriend victims while posing as a current or former co-worker, job recruiter, or someone with a shared interest on social media, especially LinkedIn.
 - ▶ Goal is to trick the victim into providing sensitive information or downloading malware to their device.
- ▶ **Pretexting** – Attackers focus on creating a good pretext, or a false but believable fabricated story, so that they can use it to pretend to need certain information from their target in order to confirm their identity.
- ▶ **WaterHoling** – An attack strategy where attackers gather information about a targeted group of individuals within a certain organization, industry, or region as to what legitimate websites they often visit.
 - ▶ Goal is to look for vulnerabilities in these sites in order to infect them with malware.
 - ▶ Eventually individuals in the targeted group will visit those sites and then become infected.

Types of Phishing Attacks

12

- ▶ **Deceptive phishing**

- ▶ Goal is to replicate a legitimate company's email correspondence and prompt victims into handing over information or credentials

- ▶ **Spear phishing** attacks are specifically tailored to one victim.

- ▶ Using knowledge gained from your social media profiles and other public information, a scammer can craft a legitimate-looking email to trap the victim into responding.

- ▶ **Whaling** is an attempt to go after the “big fish.”

- ▶ First attackers will target high-level employees and executives to gain access to their email accounts or spoof them.
 - ▶ Example- An attacker will use an executive's email or make one that appears similar and attempt to collect W2s and W9s of the employees to gain private information such as social security numbers and addresses.

Business Email Compromise (BEC) Attack

13

In a BEC attack, a scammer impersonates a company employee or other trusted party, and tries to trick an employee into sending money, usually by sending the victim email from fake or compromised email accounts

In Q3 2020, scammers requested-

- Funds in the form of gift cards in 71% of BEC attacks
 - The average amount of gift cards requested by BEC attackers was **\$1,205**
 - Gift cards for eBay, Google Play, Amazon, Apple iTunes, and Steam Wallet made up 72% of the gift card requests
- In 6% of the attacks they requested payroll diversions
- In 14% they requested direct bank transfers
 - The average amount requested in wire transfer BEC attacks was **\$48,000**



Above: global locations of BEC criminals, summer 2020

Source: APWG Phishing Activities Trend Report Q3-2020
[https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf]

Cybersecurity- The Human Factor

15

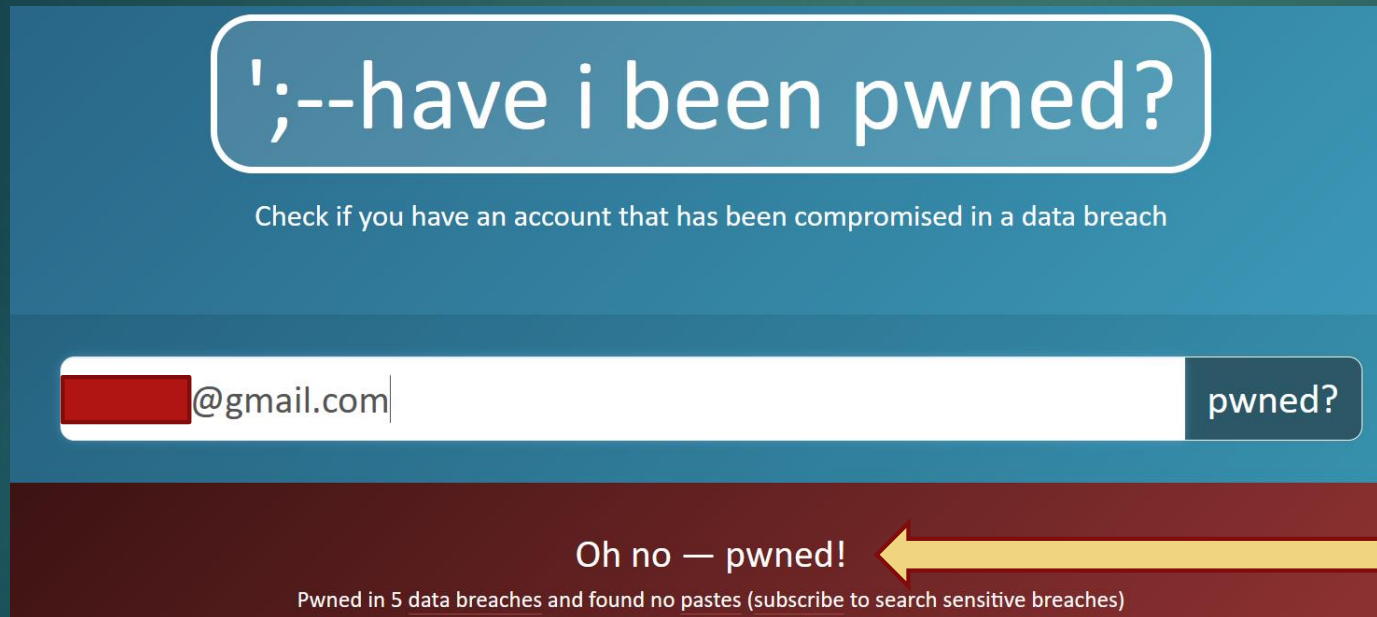
- ▶ Digital footprints can be used to extract relevant information, e.g.
 - ▶ Contacts
 - ▶ Relationships
 - ▶ Profession & Career
 - ▶ Audio
 - ▶ Video
 - ▶ Likes & dislikes
 - ▶ Interests & hobbies
 - ▶ Travel and location
 - ▶ Etc.
- ▶ The information can then be used to-
 - ▶ Craft social engineering attacks
 - ▶ Craft phishing attack

A simple test- Who knows my emails?

Are your email details safe?

16

- Have I Been Pwned? <https://haveibeenpwned.com/>



The screenshot shows the 'have i been pwned?' website interface. At the top, the title is in a blue rounded rectangle. Below it, a subtitle says 'Check if you have an account that has been compromised in a data breach'. A search bar contains a redacted email address followed by '@gmail.com'. To the right of the search bar is a button labeled 'pwned?'. Below the search bar, a red banner displays the message 'Oh no — pwned!' with a yellow arrow pointing from the right. Underneath the banner, smaller text reads 'Pwned in 5 data breaches and found no pastes (subscribe to search sensitive breaches)'.

1. People Data Labs (PDL) – October 2019
2. Evite- April 2019
3. MyFitnessPal- February 2019
4. Verification.io- February 2019
5. Yatra.com- September 2013



**Change
Password
asap!!**

Are your email details safe?

17

- Firefox Monitor? <https://monitor.firefox.com/>

Results for: [REDACTED]@gmail.com

**This email appeared in 4
known data breaches.**

Alert me about new breaches

1. Evite- April 2019
2. MyFitnessPal- February 2019
3. Verification.io- February 2019
4. Yatra.com- September 2013



**Change
Password
asap!!**

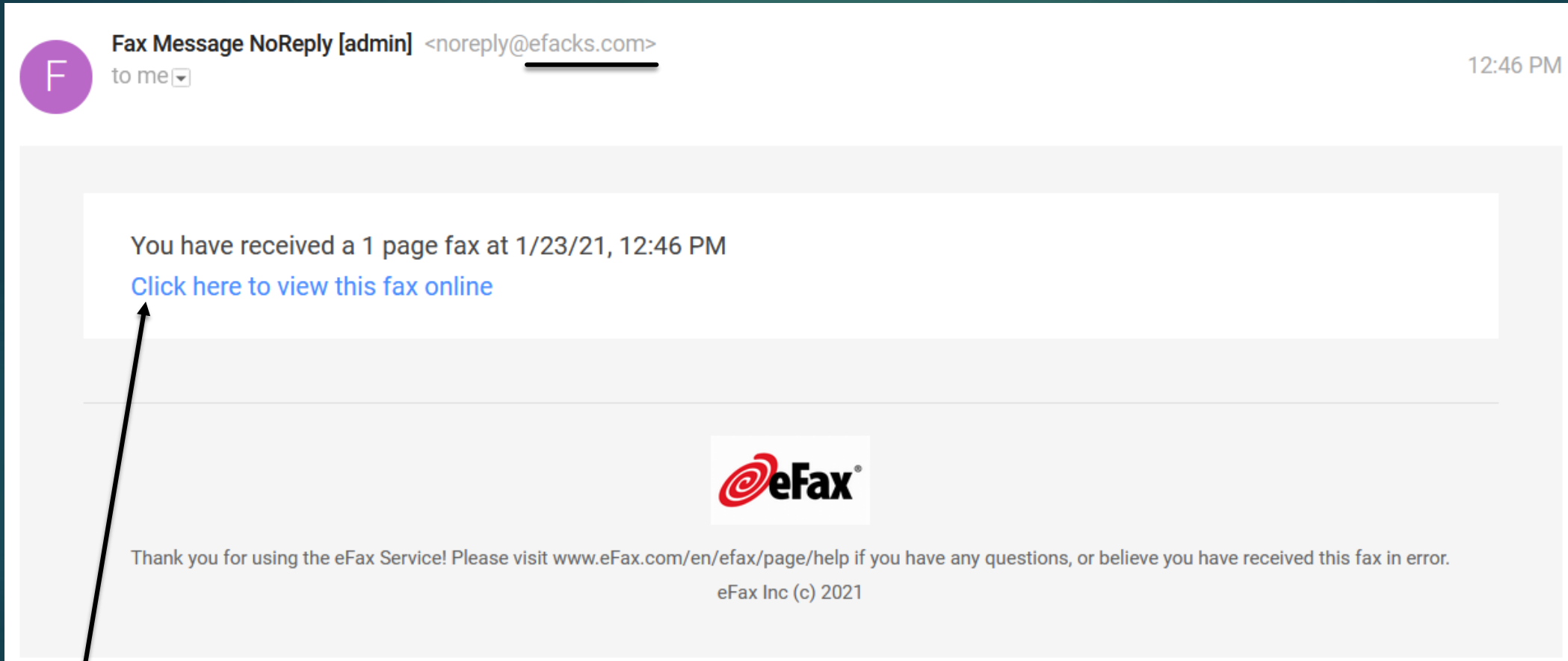
PHISHING?

- ▶ One should be suspicious of any emails asking to check or renew your credentials even if it seems to come from a trusted source.
- ▶ Do not click on suspicious links or open any suspicious attachments.
- ▶ Be very suspicious of mails from people you don't know- especially if they ask to connect to links or open files (if in doubt phone your security officer).
- ▶ Mails that create an image of urgency or severe consequences are key candidates for phishing - in these cases always verify via an external channel before complying.
- ▶ Mails sent from people you know, but asking for unusual things are also suspect - verify by phone if possible.

Let us take a simple quiz

Phishing Attack?

19



<http://efax.hosting.com.mailru382.co/efaxdelivery/2017Dk4h325RE3>

Phishing Attack?

20

<https://drive.google.com.download-photo.sytez.net/AONh1e0hVP>



TK <tk867530@gmail.com>
to me ▾

12:51 PM

hey, do you remember [THIS PHOTO!](https://drive.google.com.download-photo.sytez.net/AONh1e0hVP)

Phishing Attack?

21



Dropbox <no-reply@dropboxmail.com>
to me ▾

12:54 PM



Hi,

Your Dropbox is full and is no longer syncing files. New files added to your Dropbox folder won't be accessible on your other devices and won't be backed up online.

Upgrade your Dropbox today and get 1 TB (1,000 GB) of space and powerful sharing features.

Upgrade your Dropbox

<https://www.dropbox.com/buy>

For other ways to get more space, visit our [Get More Space](https://www.dropbox.com/help/spave/get-more-space) page.

Happy Dropboxing!

- The Dropbox Team

P.S. If you need the biggest plan we've got, check out [Dropbox for Business](https://www.dropbox.com/business).

<https://www.dropbox.com/business>

<https://www.dropbox.com/help/spave/get-more-space>

Phishing Attack?

22



Sharon Mosley <sharon.mosley@westmountdayschool.org>

to me ▾

12:59 PM

Good day adad ahah,

Please find attached the 2021 financial activity report for your perusal.

Thanks & Regards,

Ms. Sharon Mosley
Westmount Day School



Phishing Attack?

23



Google <no-reply@google.support>

to me

1:00 PM

Someone has your password

Hi,

Someone just used your password to try to sign in to your Google Account.

Information:

Saturday, January 23, 2021 at 1:00:18 PM GMT-06:00

Slatina, Romania

Firefox browser

Google stopped this sign-in attempt. You should change your password immediately

CHANGE PASSWORD



<https://myaccount.google.com-securitysettingpage.ml-security.com/signonoption>

Best,

The Mail Team

Phishing Attack?

24



Google <no-reply@google.support>
to me

1:05 PM



Government-backed attackers may be trying to steal your password

There's a chance this is a false alarm, but we believe we detected government-backed attackers trying to steal your password. This happens to less than 0.1% of all Gmail users. We can't reveal what tipped us off because the attackers will take note and change their tactics, but if they are successful at some point they could access your data or take other actions using your account. To further improve your security, based on your current settings, we recommend:



[Change password](#)

<https://google.com/amp/tinyurl/y7u8ewlr>



Hi adad ahah
affa@gmail.com

Triplt wants to

 View your email messages and settings 

Allow Triplt to do this?

You may review this app's [terms of service](https://www.tripit.com/uhp/userAgreement) and [privacy policies](https://www.tripit.com/uhp/privacyPolicy). You can remove this or any other app connected to your account in [My Account](https://security.google.com/settings/security/permissions)

CANCEL

ALLOW

<https://www.tripit.com/uhp/userAgreement>

<https://www.tripit.com/uhp/privacyPolicy>

<https://security.google.com/settings/security/permissions>

More Examples of digital footprints causing problem

26

- ▶ Resetting credentials [e.g. Sarah Palin's Gmail]
- ▶ Tarnishing reputation
 - ▶ E.g. Deepfake, online postings, embarrassing pics, participation in groups flagged as extremists etc.
- ▶ Bullying
- ▶ Identity theft
- ▶ False representation
- ▶ Blackmail
- ▶ Etc.

Types of Digital Footprints

[Source: <https://blogs.informatica.com/2016/01/15/10-digital-footprints-value-insurance/>]

27

- ▶ Social Media footprints
- ▶ Web site visit footprints
- ▶ Mobile App usage footprints
- ▶ Vehicle Telematics data footprints
- ▶ Health data footprints
- ▶ Travel data footprints
- ▶ Location data footprints
- ▶ Biometric data footprints- e.g. voice & video

Why do you allow your digital footprints to be captured? We don't ask the right questions

28



- Who, other than the intended recipient, will receive or have access to my information?
- Will it be shared by the intended recipient with other parties?
- What is the scope of this information?
- Is the information being shared directly or indirectly?
- Do I benefit from the sharing of my data? Are these benefits tangible or intangible?
- How much do I value my privacy?

Why do you allow your digital footprints to be captured?

- ▶ Lack of understanding
- ▶ Convenience- e.g. You don't have to repeatedly log in or submit personal details to web sites.
- ▶ Professional reasons- Contribute to your online reputation
- ▶ Cultural reasons



Who is recording your digital footprints?

30

- ▶ **Advertisers**- anyone with product(s) and/or service(s) to sell
- ▶ **Publishers**- companies that publish online advertisements (e.g. search engines, online magazines/newspapers, blogs etc.)
- ▶ **Data Aggregators**- compile information from databases (public or private), and partner websites on individuals and sell that to advertisers to target ads (e.g. BlueKai, OutBrain, Rio etc.)
- ▶ **Nation States**
- ▶ **Vendors of IoT & smart devices, e.g.**
 - ▶ **Voice**- e.g. Amazon Echo and Google Home
 - ▶ **Video**- Surveillance cameras, YouTube, TikTok
 - ▶ **Biometrics**- Sleep Number now collects more than 8.5 billion full-body biometric data points every night by measuring a customer's movement, breathing rates, heartbeat and sleep habits.

Who knows what about you? **Google**

31

- ▶ Who you are (your looks, age, what you sound like, your political and religious beliefs, your health, your family, your pets, etc.)?
- ▶ Where you have been?
- ▶ Who your friends are?
- ▶ Your likes and dislikes
- ▶ Your future plans
- ▶ Your online search and browsing history
- ▶ Location etc.

Who knows what about you? Google

32

► **Google-** <https://takeout.google.com>

How your ads are personalized

Ads are based on personal info you've added to your Google Account, data from advertisers that partner with Google, and Google's estimation of your interests. Choose any factor to learn more or update your preferences. [Learn how to control the ads you see](#)



45-54 years old

Who knows what about you? Facebook

33

- ▶ **Off-Facebook Activities**- Even when you're not on Facebook, the app can track some of your activity, such as what you search for or purchase online. Many websites use fragments of code known as *Facebook Pixel* to advertise to you after you've left their page too.
- ▶ **Apps & Web Activity**- Noticed how many websites and apps offer you the option to quickly sign in with Facebook instead of creating an account from scratch? That's thanks to Facebook being able to interact with your app and web activity. it may have access to your:
 - ▶ **Contacts** – To help suggest friends in the “**People You May Know**” feature.
 - ▶ **Networks and Connections** – Who you interact with online and how.
 - ▶ **Transactions and Usage** – What you do, like, and buy on Facebook and its affiliated companies (WhatsApp, Instagram, etc.).
- ▶ **Device Information**
 - ▶ Device type
 - ▶ IP address
 - ▶ Battery life
 - ▶ Location
 - ▶ Mouse movements (this is to help detect bots)
- ▶ **Information that you provide**- posts, everything you 'like' or comment on, the events you attend or show interest in, the locations you 'check-in' to, etc.
- ▶ When you are logged in, Facebook can track your browsing activities

Who knows what about you? **Amazon**

34

- ▶ **Amazon.com**: Addresses, payment cards, milestones, purchase history, cart contents, search history, wish list, and browsing history on Amazon (and Amazon-owned sites like Zappos and Diapers.com).
- ▶ **Kindle** (digital books) and **Audible** (audio books): Reading history, browsing history, your location on various books, and what passages you've highlighted in Kindle.
- ▶ **Fire tablets**: Amazon's tablets run a custom version of Android, and collects data on your interactions with the device
- ▶ **Prime Video** (streaming video): Watch, browse, and search history
- ▶ **Twitch** (streaming game videos): Watch, browse, and search history
- ▶ **Ring** (smart doorbells and security gear): For customers with a paid recording plan, Amazon stores videos for 30 to 120 days depending on location, or until a customer manually deletes the video. Recordings for those who don't subscribe to a plan are deleted automatically.

Who knows what about you? **Amazon**

35

- ▶ **Eero** (wi-fi routers): Eero's device knows every Web site you go to, but the company says it doesn't collect or store this information. (Eero [detailed its practices](#) in a blog post after the Amazon acquisition.)
- ▶ **IMDB** (movie and TV database): Your taste in movies, favorite actors, genres etc.
- ▶ **Goodreads** (book-centric social network): The focus may be on books, but Amazon is also building a social graph of the service's bookworm members, in addition to getting more details on what sort of topics members are interested in.
- ▶ **Whole Foods** (grocery store): Your grocery list, purchase behavior, address, payment method
- ▶ **Alexa**
- ▶ **Key** by Amazon- To have your amazon delivery left in your garage
- ▶ **Amazon Go**- Just walkout shopping

Who knows what about you? **Twitter**

36

- ▶ What devices you use Twitter on
- ▶ Location and Time- When and where you was when I tweeted
- ▶ The advertising topics you are interested in
- ▶ Applications you have downloaded on your smartphone
- ▶ Every tweet you have ever posted

Who knows what about you? Tesla

37

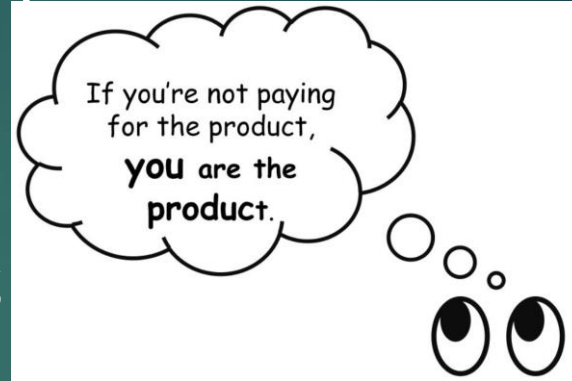
- ▶ Vehicle's location
- ▶ **Car's personal settings**, e.g. contacts you've synced from your phone, addresses you've plugged into the navigation system, and even your favorite radio stations
- ▶ **It knows** your speed, your mileage, and where and when you charge the battery.
- ▶ **It also monitors** airbag deployments, braking and acceleration, which helps in accident investigations.
- ▶ **And it knows when Autopilot**, Tesla's assisted-driving feature, is engaged or disengaged, and whether you have your hands on the wheel as you should
- ▶ **Tesla is constantly in record mode**, using cameras and other sensors to log every detail about what they encounter while driving, even when Autopilot is turned off.
- ▶ **Most important, Tesla uses data** from its vehicles to crowdsource advanced technology features like high-precision maps and improvements to Autopilot.

Value of Your Digital Footprints?

38

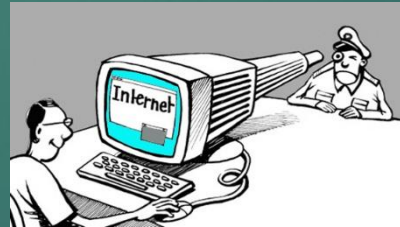
▶ To **monetize** your online activity

- ▶ Follow you
- ▶ Understand you
- ▶ Customized product & services
- ▶ Sell/Trade your data



▶ **Surveillance**

- ▶ Law enforcement
- ▶ Nation states



▶ **Forensics**

- ▶ Lawsuits
- ▶ Solve a crime



Value of Your Digital Footprints?

39

▶ Cyberattacks

- ▶ Phishing
- ▶ Blackmail/Extortion
- ▶ Data theft
- ▶ Cyberstalking
- ▶ Cyberbullying



▶ Background Checks

- ▶ Job applicants
- ▶ Contractors
- ▶ Political opponents
- ▶ Potential love interest/spouse

Managing Your Digital Footprints

40

- ▶ **Find out the extent of your digital footprints**
 - ▶ According to Allstate's research, the average consumer thinks they have 50 or fewer online accounts -- when in reality, the average is 152
 - ▶ **Delete** accounts that you no longer use or need
- ▶ **Develop Secure Browsing Habits**
- ▶ **Mobile Apps**

Extent of Your Digital Footprint?

41

- ▶ **Facebook**
- ▶ Google
- ▶ Instagram
- ▶ Snapchat
- ▶ Twitter

Facebook- What does it know about you?

42

- ▶ Download your data from Facebook
 - ▶ <https://www.facebook.com/help/1701730696756992>
- ▶ Turn off personalized ads:
 - ▶ **Settings → Privacy Shortcuts → Ad Preferences → See Your Ad Settings.**
Then, select each option and turn it off as needed.
- ▶ Manage which third-party websites, apps, services, etc., are associated with your Facebook account
 - ▶ Select **Manage Your Off Facebook Activity** under 'View or clear your off-Facebook activity' in *Privacy Shortcuts*. Then, you can look at each activity and choose to turn them off.
- ▶ **Stop Facebook from tracking your Google searches**
 - ▶ **Settings → Privacy Shortcuts → Your Facebook Information → View or clear your off-Facebook Activity → More Options → Manage Future Activity → Manage Future Activity** → Then, **toggle OFF** the 'Future Off-Facebook Activity' option.

Extent of Your Digital Footprint?

43

- ▶ Facebook
- ▶ **Google**
- ▶ Instagram
- ▶ Snapchat
- ▶ Twitter

Google Settings

- ▶ Get Your data from Google [<https://takeout.google.com>]
- ▶ Autofill Service- Disable
- ▶ Usage & Diagnostics- Disable
- ▶ Google Activity Controls
 - ▶ Web & App Activity
 - ▶ Location History
 - ▶ Search History
 - ▶ Browsing History
 - ▶ YouTube History
 - ▶ Ad Personalization

Extent of Your Digital Footprint?

45

- ▶ Facebook
- ▶ Google
- ▶ **Instagram**
- ▶ Snapchat
- ▶ Twitter

The extent of your digital footprints?

46

► Instagram

- Pull up Instagram's website and log in
- Click on the person icon in the upper-right corner
- Click on the gear-like icon to the right of the "**Edit Profile**" button
- In the menu that pops up, click on **Privacy and Security**
- Scroll down a bit on the subsequent **Account Privacy** page, and you should see a header for **Data Download**, followed by a "Request Download Link" Click on that link.

Extent of Your Digital Footprint?

47

- ▶ Facebook
- ▶ Google
- ▶ Instagram
- ▶ **Snapchat**
- ▶ Twitter

The extent of your digital footprints?

48

▶ Snapchat

- ▶ Log into your Snapchat account
- ▶ Click '**My Data**'
- ▶ Click '**Submit Request**' at the bottom of the page
- ▶ If your email is clearly verified by Snapchat, they will send you a downloadable link when the information is ready via your email
- ▶ Follow that link sent to your email and download the ZIP file
- ▶ Click download and your file will be ready to open with the compatible software

Extent of Your Digital Footprint?

49

- ▶ Facebook
- ▶ Google
- ▶ Instagram
- ▶ Snapchat
- ▶ **Twitter**

Extent of Your Digital Footprint?

50

► **Twitter**

- Open your profile from a web browser.
- Click your picture in the top-right corner next to the Tweet button.
- Select “*Settings and Privacy*”
- Choose “*Your Twitter Data*” from the left menu.
- Dig through this information.

Managing Your Digital Footprints

51

- ▶ Find out the extent of your digital footprints
- ▶ **Develop Secure Browsing Habits**
- ▶ Mobile Apps

Secure Browsing

52

- ▶ Browse in “INCOGNITO” mode
- ▶ Enable “DO NOT TRACK”
- ▶ **DELETE** search and browse history on exit
- ▶ **OPTOUT** of ad personalization from your current browsers-
 - ▶ <https://optout.aboutads.info/>
 - ▶ Ask for a website to remove you from a database directly
- ▶ Use the “right to be forgotten” if the option is available

Secure Browsing

53

- ▶ Use false or 'Burner' Information
- ▶ Use VPN (e.g. NordVPN)
- ▶ Use secure browsers on mobile devices e.g.
DuckDuckGo
- ▶ Use secure search engine (e.g. DuckDuckGo) with popular browsers such as Chrome, Firefox, MS Edge
- ▶ Fine tune browsers for security and privacy with plugins for URL filtering, content blocking, anonymous/incognito browsing etc.

Managing Your Digital Footprints

54

- ▶ Find out the extent of your digital footprints
- ▶ Develop Secure Browsing Habits
- ▶ **Mobile Apps**

Popular Apps with Security Concerns

55

- ▶ **Voice Assistants** (e.g. Siri, Alexa, Google Voice)- collect not only behavioral data, but voice searches, and they can record them at any point in time, meaning any time you talk about something,
- ▶ **WhatsApp**- has had some major security breaches with phishing texts and phone calls, that even though were ignored, still installed spyware,
- ▶ **Facebook Messenger**
 - ▶ Doesn't provide end-to-end encryption by default
 - ▶ Accessing user SMS, photos, contacts, and camera without permission
- ▶ **Pokémon Go**- ability to access contacts, camera, and even the user's location without permission
- ▶ **Free VPNs**- HolaVPN is one that should never be downloaded due to security reasons. "When you are a free Hola user, you automatically allow other Hola users to reroute their Internet traffic through your computer and network. These other users will access and browse the Internet using your IP address. All their Internet activities will be linked to your unique IP address, which could get you into significant trouble depending on what those other users are doing online

More Concerns about Mobile Apps

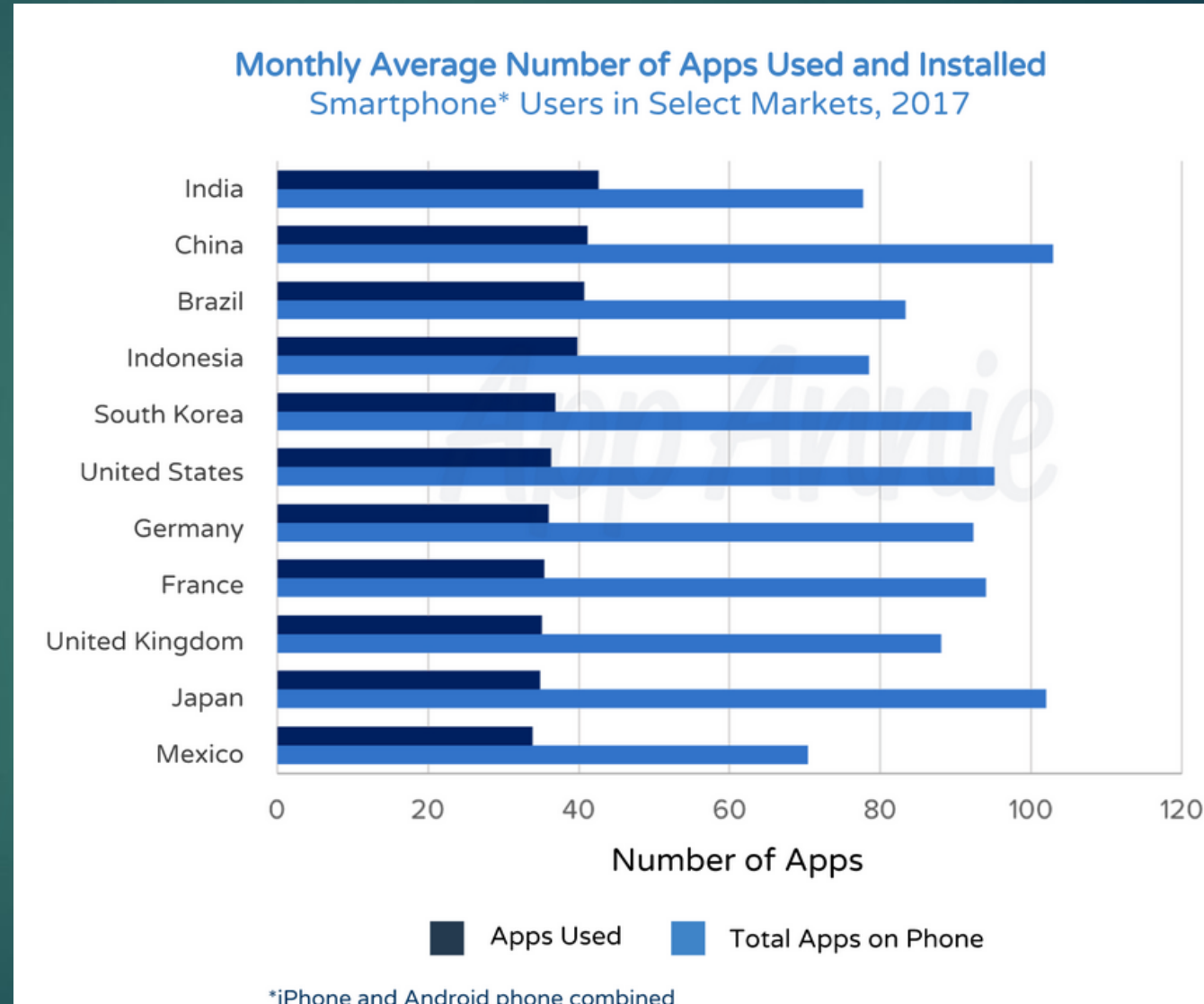
56

- ▶ **Uninstalling an app remove permissions?** No, not necessarily because most apps leave behind directory structure along with log files and other data to let them know if they were previously installed.
- ▶ According to a study, 33 percent of Android apps request more permissions than they actually need.
- ▶ A research that has been conducted revealed that out of 83 percent users paid attention to the permission, 97 percent of them couldn't correctly identify what the app permission were used for, and 42 percent didn't know what those permissions are.
- ▶ Both Android and iOS leave the explanation to developers to explain why they need to see personal data
- ▶ **Which App Does What?** For example, an app that does battery saving, what does it actually do? If it works as marketed, it should save battery and do nothing else. Does it really need to know the user's location or contact information?
- ▶ **What Business Model?**

Mobile Apps

57

- ▶ Lots of Apps on your device
- ▶ Approximately 305 are used regularly
- ▶ **MINIMIZE** the number of apps on your mobile devices



Source: <https://www.appannie.com/en/insights/market-data/app-annie-2017-retrospective/>

Mobile Apps

58

▶ **Manage App Permissions- Android**

▶ SETTINGS → PRIVACY → PERMISSION MANAGER

▶ Set APP permissions for-

▶ Body Sensors

▶ Calendar

▶ Call Logs

▶ Camera

▶ Contacts

▶ Location [*“Allow all the Time”, “Allow Only When Using the app”, “Deny”*]

▶ Microphone

▶ Phone

▶ Physical Activity

▶ SMS

▶ Storage

Mobile Apps

59

► **Manage Permissions- iPhone**

- Has excellent access controls- passcode, biometrics, Two-Factor authentication
- **Settings** —> Privacy. A list of different categories, such as Location Tracking, Bluetooth, Contacts, Microphone, Photos, and more will appear. You can click on each specific category to see which apps have access to that data. You can grant or revoke permissions as you see fit.
- **Location:** To view your location history: Open the Settings app —> Click “Privacy” > Choose “Location Services”—> Scroll down and select “System Services” —> Click “Significant Locations > Choose “History.”
- **Stop Sharing Location**
 - Go to “Find My” app.
 - Click on the “People” tab.
 - Select the designated contact's name.
 - Choose “Stop Sharing My Location”
 - Confirm by tapping “Stop Sharing Location.”
- **Turn off location services for specific apps:** Go to “Settings” —> “Privacy” —> “Location Services.” For each app listed, you'll be prompted to choose one of the options: “Never,” “Ask Next Time,” or “While Using the App.” If you don't want a specific app to track you at all, select “Never.”

Working from Home?

- ▶ Be Aware of
 - ▶ Coronavirus related phishing attacks
 - ▶ Emails from people you do not know
 - ▶ More than 2 million phishing websites emerged in 2020 alone
 - ▶ People who you know but asking for suspicious things- call them
- ▶ Ensure anti-virus is in place and fully updated
- ▶ Home Wireless Router
 - ▶ Strong password
 - ▶ Restrict devices by filtering for MAC addresses
 - ▶ Don't broadcast SSID

Working from Home?

61

- ▶ **Use TAMU** (rather than personal) **computers** where possible - As far as possible, do not mix work and leisure activities on the same device.
- ▶ **Connect** to the internet via **secure networks**
 - ▶ **Avoid** open/free networks (e.g. restaurants & coffee shops, airports, grocery store etc.)
- ▶ **Avoid** the exchange of sensitive information through possibly insecure connections (e.g. via email).
- ▶ **Do NOT** share the virtual meeting URLs on social media or other public channels.

Some Additional Best Practices

62

- ▶ **On your personal laptop/desktop**
 - ▶ **Disable** guest account
 - ▶ Create **two** accounts
 - ▶ One with no-administrative privileges: Use this for your routine work
 - ▶ One with administrative privileges: Use this for system updates, SW installations, Patch applications etc.
 - ▶ Make sure that you are up to date with latest patches for your OS and Apps
 - ▶ Create a **backup** policy and follow it diligently
 - ▶ Use disk **encryption**
 - ▶ Ensure that Mic and Camera are used only by authorized Apps (e.g. Zoom, Skype)
 - ▶ Use **camera cover** to enhance privacy
 - ▶ Lock your screen if you work in a shared space

