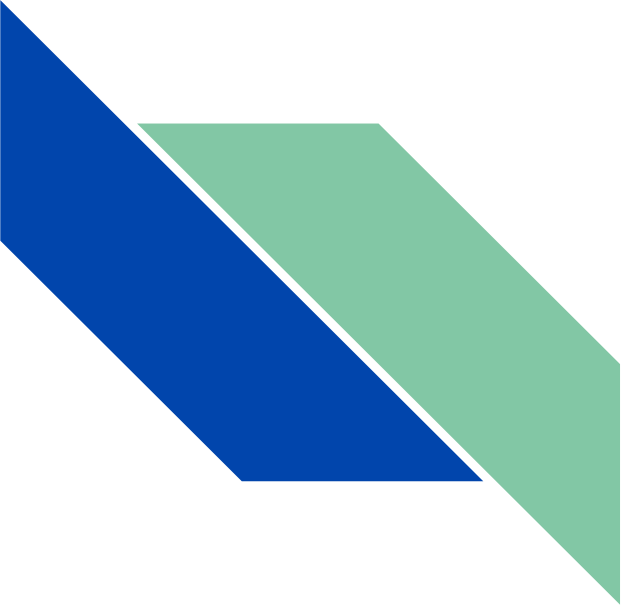
DIGITAL SECURITY + PRIVACY *in the library*

Presenter: Samantha Link

Topics Today

- SECURITY THREATS
  - Who wants personal data?
  - How does data move on the Internet?
  - Where and how is data vulnerable?
- PASSWORD PROTECTION
- PRIVACY TOOLS



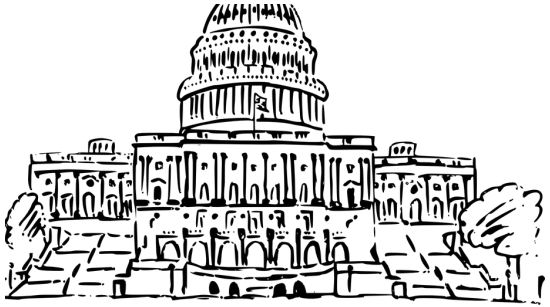
SECURITY THREATS

Who wants personal data?

COMPANIES

advertising

GOVERNMENT



investigations

INDIVIDUALS

fraud

Who wants personal data?

COMPANIES

advertising

GOVERNMENT

investigations

INDIVIDUALS

fraud

How does data move through the Internet?

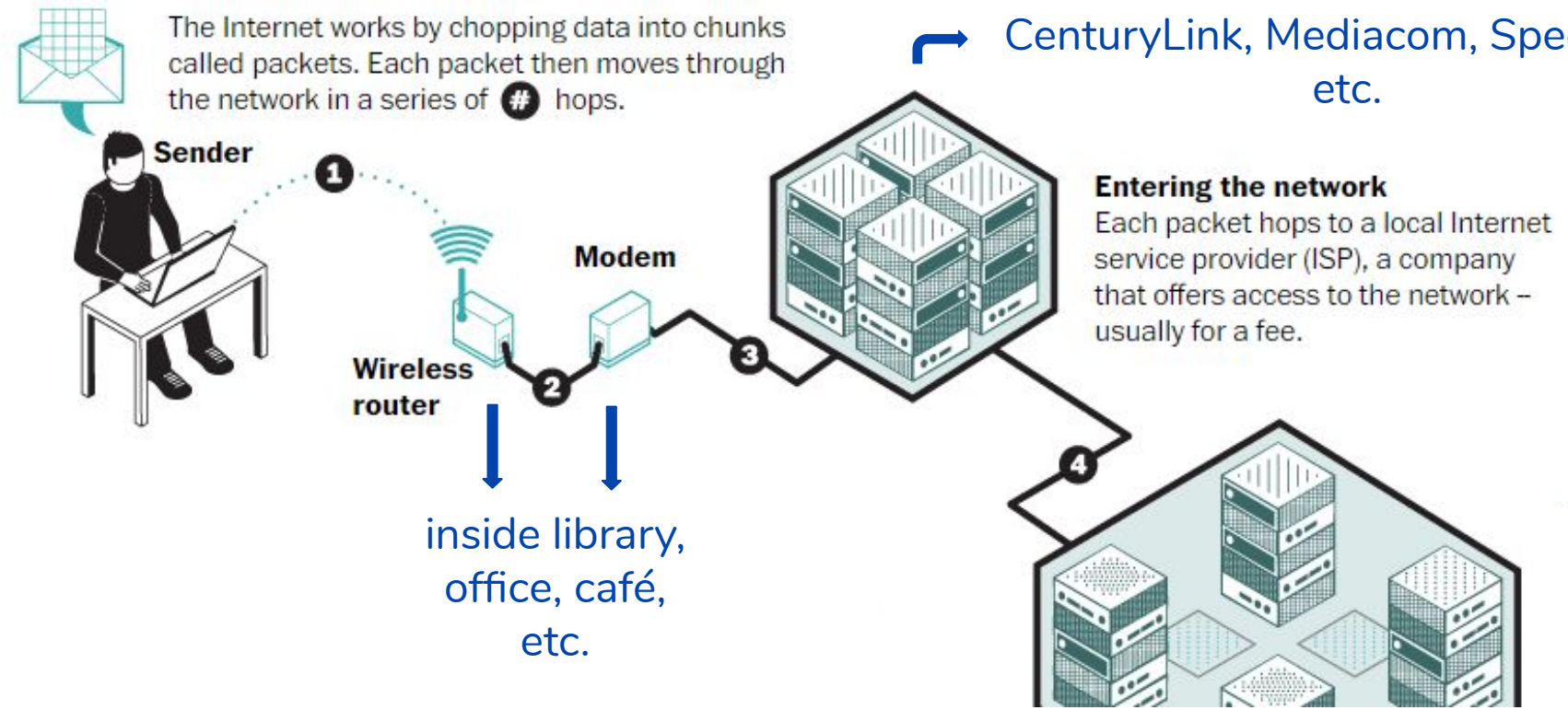
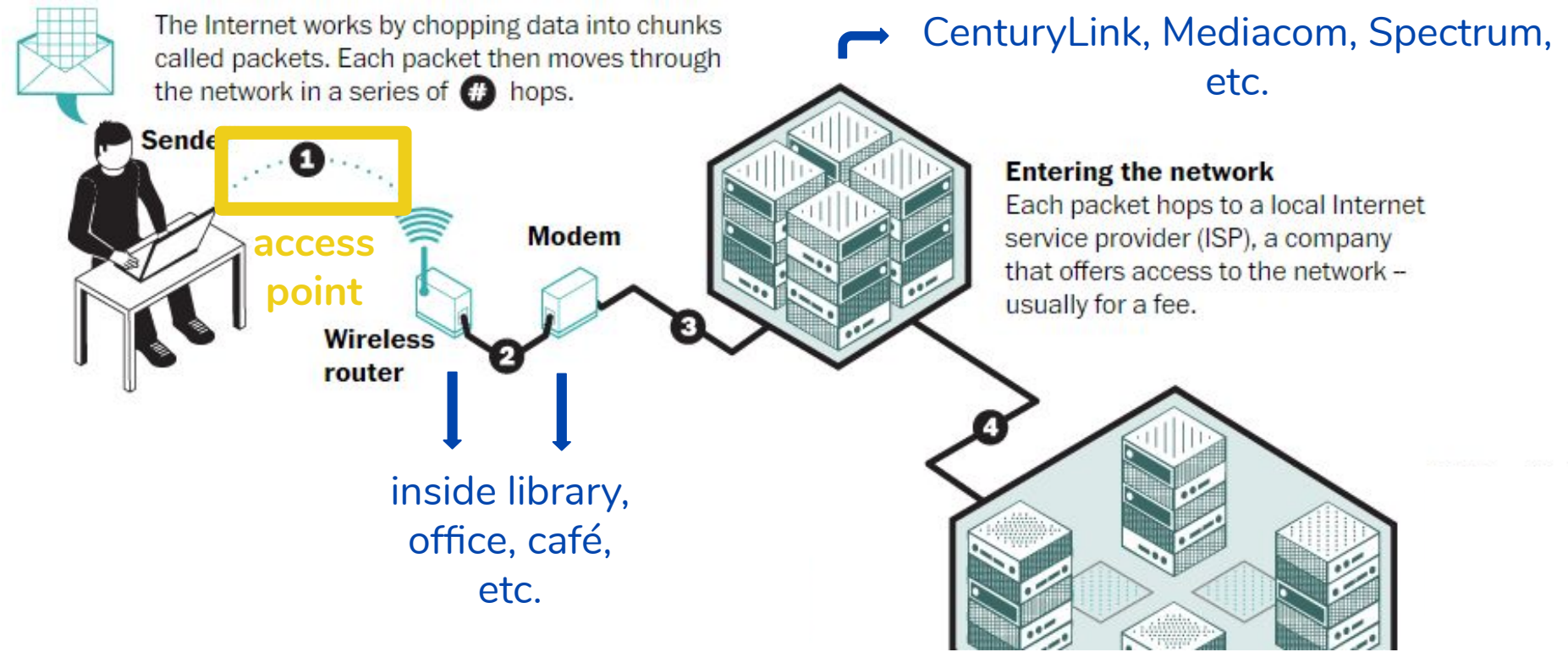


IMAGE CREDIT: Lazaro Gamio, *Washington Post*

How is data vulnerable?



CenturyLink, Mediacom, Spectrum, etc.

inside library, office, café, etc.

"THE INTERNET"

IMAGE CREDIT: Lazaro Gamio, *Washington Post*

Wardriving

McAfee Blog: "What is Wardriving?"

“While it may sound odd to worry about bad guys snatching our personal information from what seems to be thin air, it’s more common than we’d like to believe. In fact, there are hackers who drive around searching for unsecured wireless connections (networks) using a wireless laptop and portable global positioning system (GPS) with the sole purpose of stealing your information”

Wardriving

WiFi security = password-protected connection

What's a *library* to do?

We want open WiFi! Consider practical threats. We can educate patrons about security practices, strong passwords, etc.

Remember: "wired" connections (e.g. patron PCs) are quite secure; having a program to clear data upon each log-out even more so. *In your library?*

How is data vulnerable?

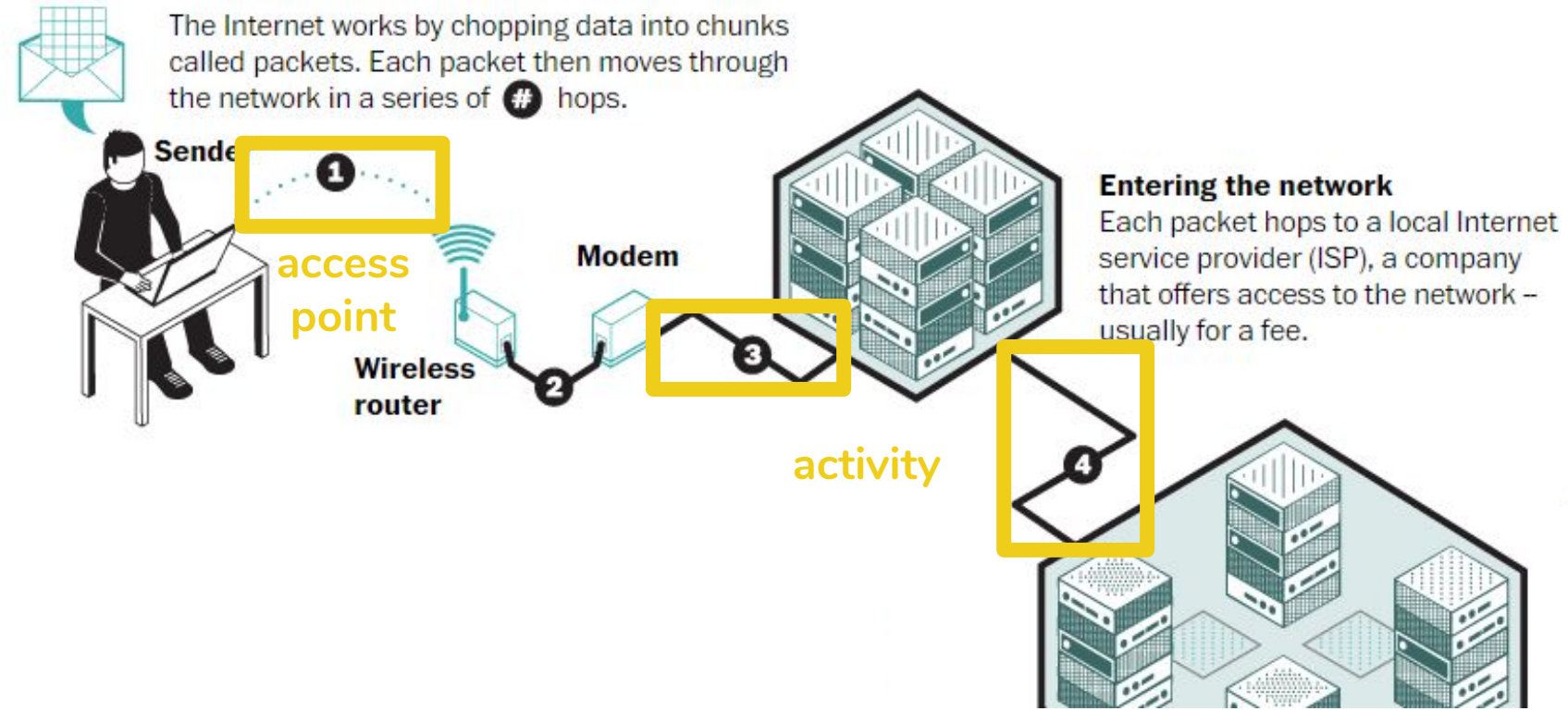


IMAGE CREDIT: Lazaro Gamio, *Washington Post*

"E-vesdropping"

Sender

Account name

Password

Social Security #

Server

Encryption over the Web

Hyper-
Text
Transfer
Protocol
Secure

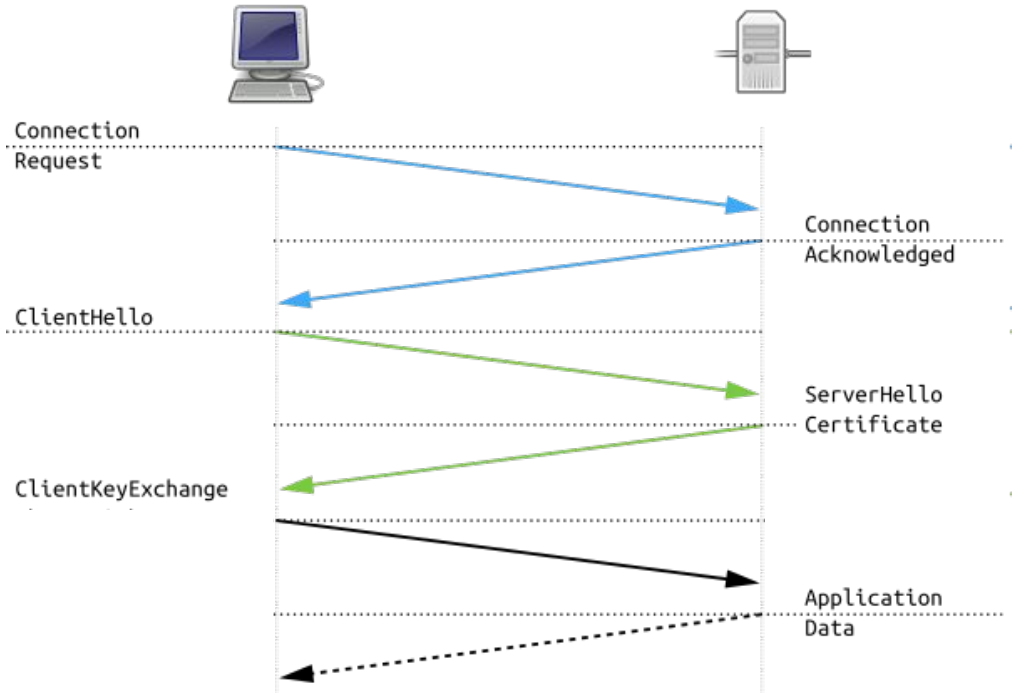


IMAGE CREDIT: Wikimedia Commons

Encryption over the Web

Sender

...11039225900287...
...65342003154354...
...92135892439243...

Server

What's a *library* to do?

Use links to HTTPS websites whenever possible

Keep all software updated!

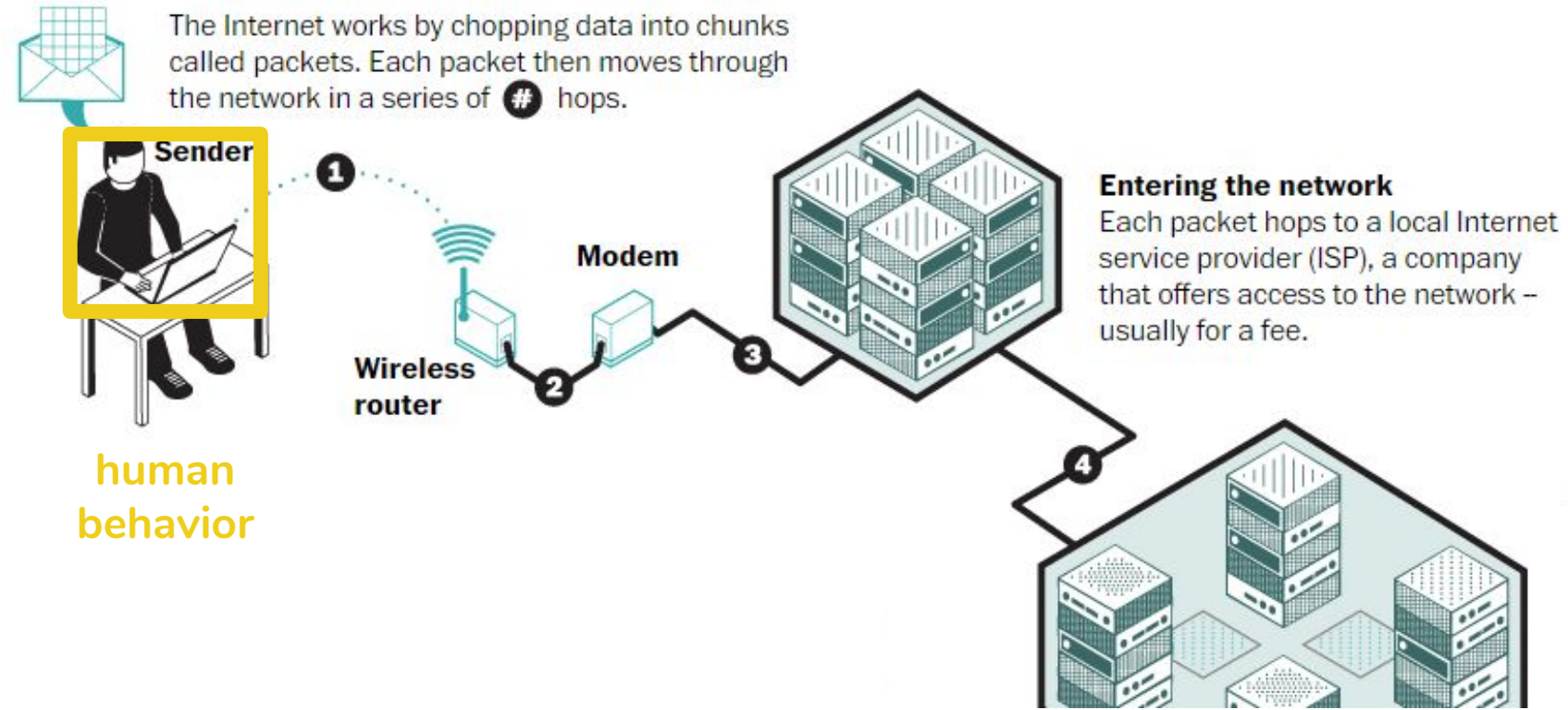
E-mail encryption

E-mail uses dedicated "protocol" requiring different encryption; also limited by correspondents' platform

Options:

- Settings within popular services (Gmail, Outlook, Yahoo)
- Dedicated service (ProtonMail, Hushmail)

How is data vulnerable?



human behavior

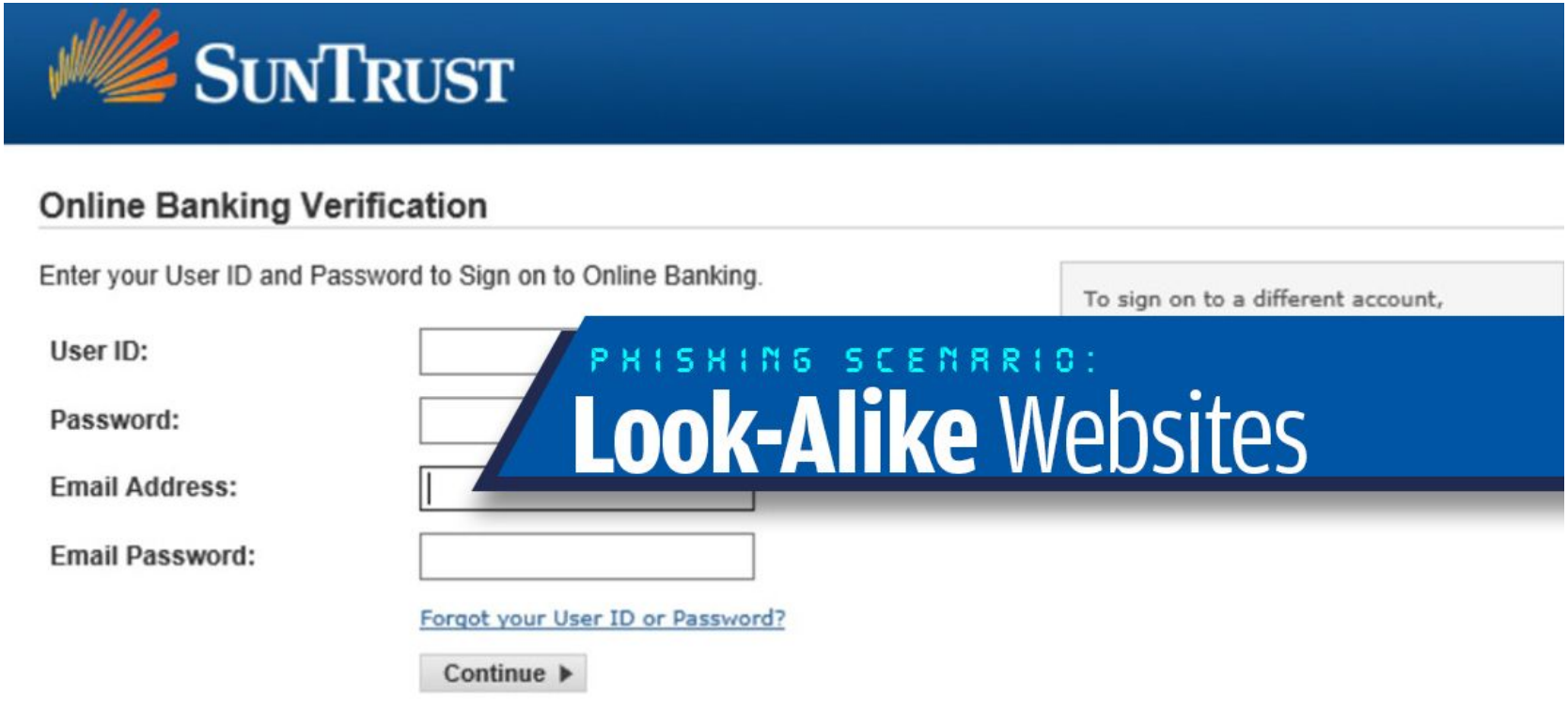
"THE INTERNET"

IMAGE CREDIT: Lazaro Gamio, *Washington Post*

Phishing

Merriam-Webster.com: “a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly”

CSO Online: 15 real-world phishing examples

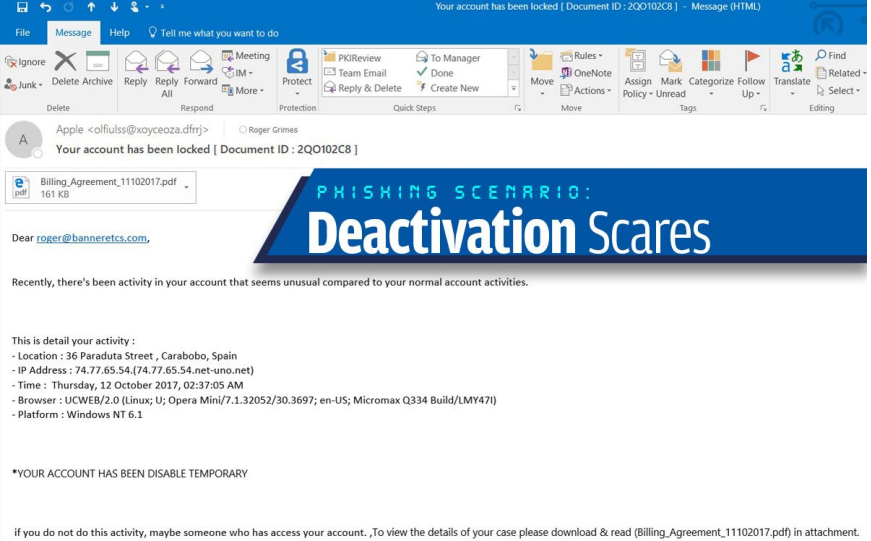


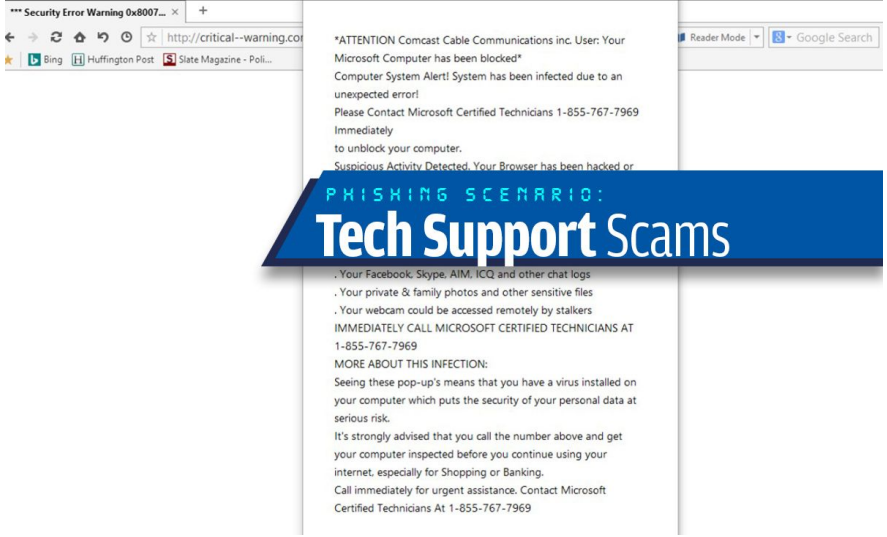
Don’t take the bait!

Do you recognize sender’s email address?

Look at link URLs before clicking — https://www.website-you-want.com?

Suspicious? Don’t click, contact IT!


Your account has been locked [Document ID : 2QO102C8] - Message (HTML)
Apple <olfiulss@xoyceoza.dfrrj>
Your account has been locked [Document ID : 2QO102C8]
Billing_Agreement_11102017.pdf
161 KB
PHISHING SCENARIO:
Deactivation Scares
Dear roger@banneretcs.com,
Recently, there's been activity in your account that seems unusual compared to your normal account activities.
This is detail your activity :
- Location : 36 Paraduta Street , Carabobo, Spain
- IP Address : 74.77.65.54.(74.77.65.54.net-uno.net)
- Time : Thursday, 12 October 2017, 02:37:05 AM
- Browser : UCWEB/2.0 (Linux; U; Opera Mini/7.1.32052/30.3697; en-US; Micromax Q334 Build/LMY47I)
- Platform : Windows NT 6.1
*YOUR ACCOUNT HAS BEEN DISABLE TEMPORARY
if you do not do this activity, maybe someone who has access your account. ,To view the details of your case please download & read (Billing_Agreement_11102017.pdf) in attachment.


*** Security Error Warning 0x8007...
ATTENTION Comcast Cable Communications inc. User: Your Microsoft Computer has been blocked
Computer System Alert! System has been infected due to an unexpected error!
Please Contact Microsoft Certified Technicians 1-855-767-7969 Immediately
to unblock your computer.
. Your Facebook, Skype, AIM, ICQ and other chat logs
. Your private & family photos and other sensitive files
. Your webcam could be accessed remotely by stalkers
IMMEDIATELY CALL MICROSOFT CERTIFIED TECHNICIANS AT 1-855-767-7969
MORE ABOUT THIS INFECTION:
Seeing these pop-up's means that you have a virus installed on your computer which puts the security of your personal data at serious risk.
It's strongly advised that you call the number above and get your computer inspected before you continue using your internet, especially for Shopping or Banking.
Call immediately for urgent assistance. Contact Microsoft Certified Technicians At 1-855-767-7969
PHISHING SCENARIO:
Tech Support Scams


THE FBI FEDERAL BUREAU OF INVESTIGATION
CYBER DEPARTMENT
All activities of this computer have been recorded
All your files are encrypted. Don't try to unlock your computer!
You have been subjected to violation
(Video, Music, Software) and illeg
contents, thus infringing Article 1,
Article 1, Section 8, Cause 8 of the
hundred minimal wages or a deprivation of liberty for two to eight years.
You have been viewing or distributing prohibited Pornographic content (Child Porno photos and etc were found on your computer). Thus violating article 202 of the Criminal Code of United States of America, Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.
Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law on Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or deprivation of liberty for four to nine years.
Pursuant to the amendment to Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine of the States.
To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $300. Payable through GreenDot MoneyPak (you have to purchase MoneyPak card, load it with $300 and enter the code). You can buy the code at any shop or gas station. MoneyPak is available at the stores nationwide.
Your IP:
Location:
SECURE PAYMENT FORM
Enter the code MoneyPak
Please enter MoneyPack code using pin pad below.
1 2 3 4 5 6 7 8 9 0 Clear
PHISHING SCENARIO:
Go Directly to Jail


PHISHING SCENARIO:
Save a Friend

How is data vulnerable?

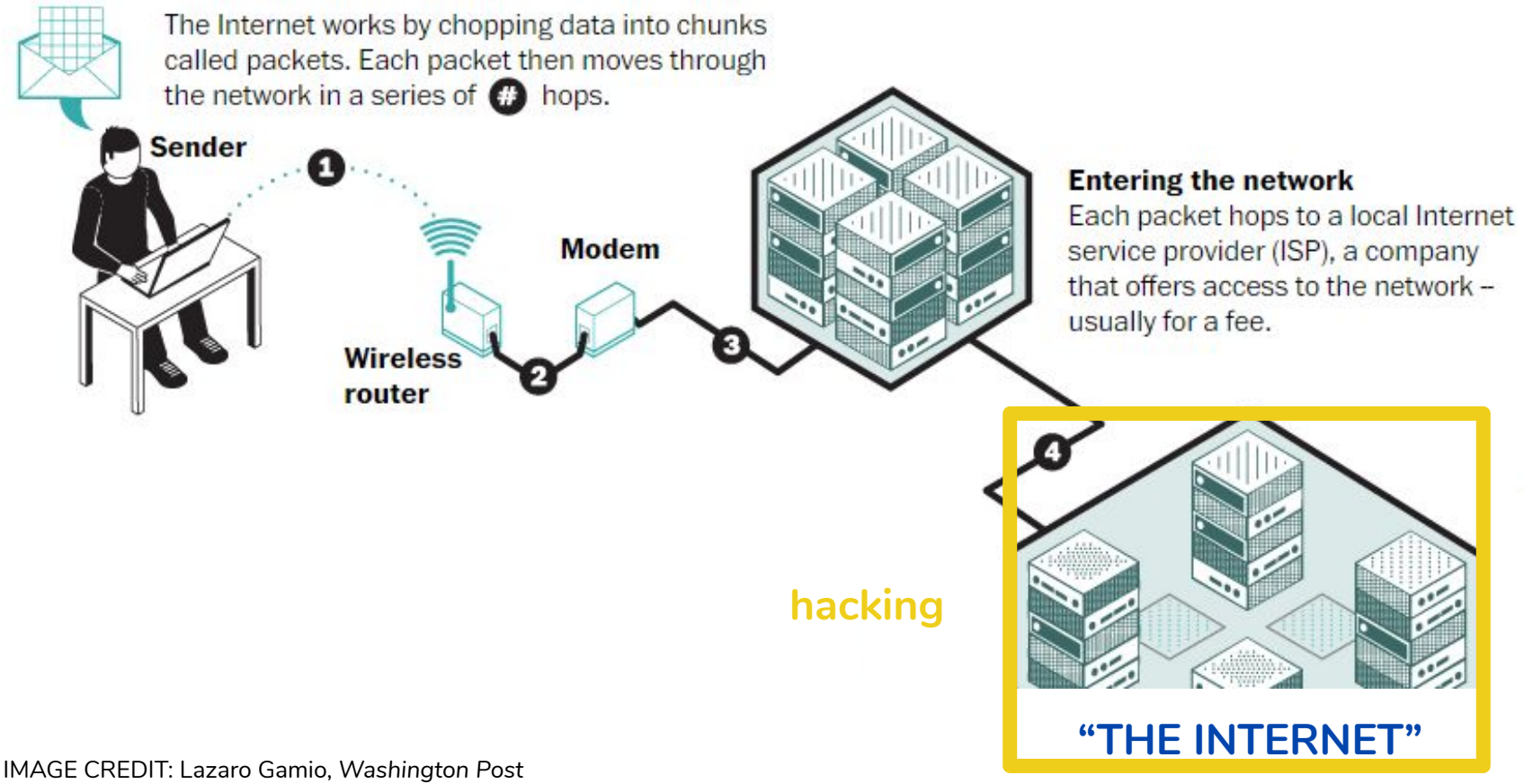


IMAGE CREDIT: Lazaro Gamio, *Washington Post*

Data breaches

FEDERAL TRADE COMMISSION
Consumer Information

MONEY & CREDIT | HOMES & MORTGAGES | HEALTH & FITNESS | JOBS & MAKING MONEY | PRIVACY, ID ONLINE SE

Home › Blog

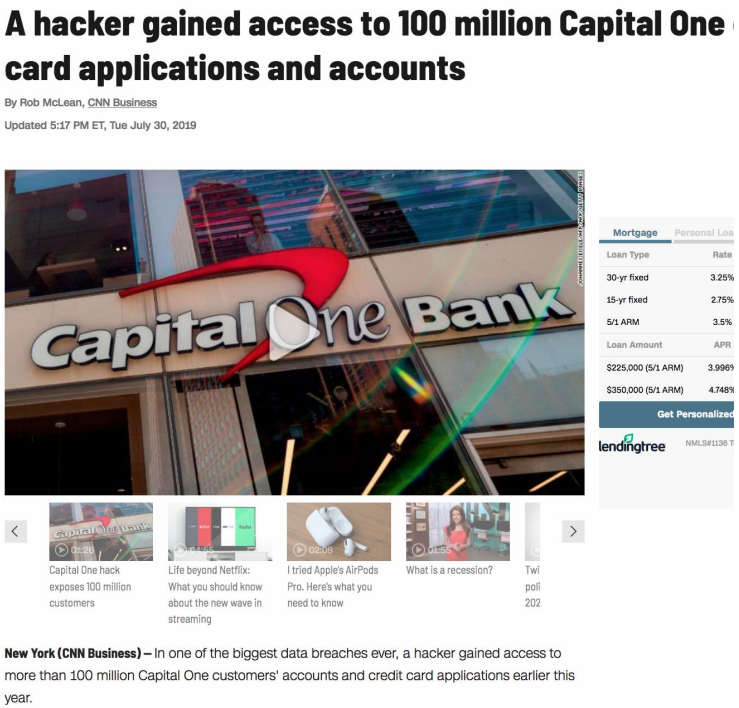
The Equifax Data Breach: What to Do

Share this page

September 8, 2017
by Seena Gressin
Attorney, Division of Consumer & Business Education, FTC

If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.

2017
Equifax credit agency



A hacker gained access to 100 million Capital One card applications and accounts

By Rob McLean, CNN Business

Updated 5:17 PM ET, Tue July 30, 2019

Capital One hack exposes 100 million customers

Life beyond Netflix: What you should know about the new wave in streaming

I tried Apple's AirPods Pro. Here's what you need to know

What is a recession?

Mortgage | Personal Loa

Loan Type	Rate
30-yr fixed	3.25%
15-yr fixed	2.75%
5/1 ARM	3.5%
Loan Amount	APR
$225,000 (5/1 ARM)	3.996%
$350,000 (5/1 ARM)	4.748%

Get Personalized

lendingtree

New York (CNN Business) — In one of the biggest data breaches ever, a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year.

2019
Capital One

Data breaches

Stay informed with

Federal Trade Commission

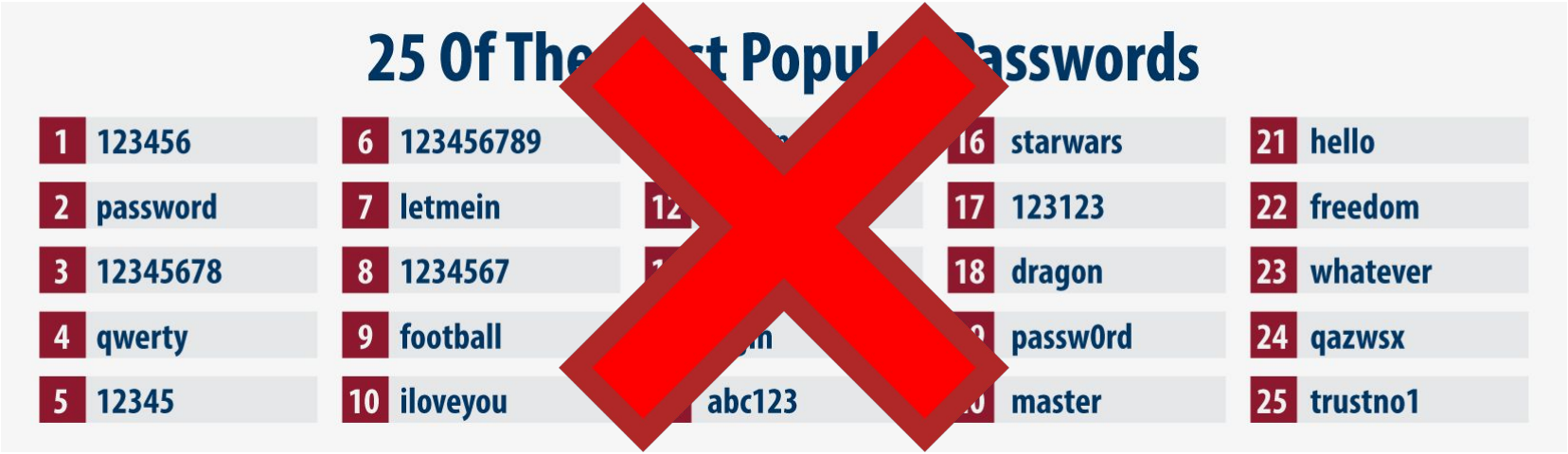
Consumer Information blog:

https://www.consumer.ftc.gov/blog

PASSWORD PROTECTION

GOAL: strong passwords

GOAL: strong passwords



GOAL: strong passwords

Current guidelines to avoid being easily guessed by humans or robots...

- 12-15 characters
- No dictionary words
- No obvious details (name, phone #, etc.)
- Different for each account
- Change if any suspicion!

GOAL: strong passwords

Turn a memorable phrase into secure password…

Example:
“Be happy for this moment; this moment is your life”
Bh4tm;tmiyl5433 (15 characters)

GOAL: password security

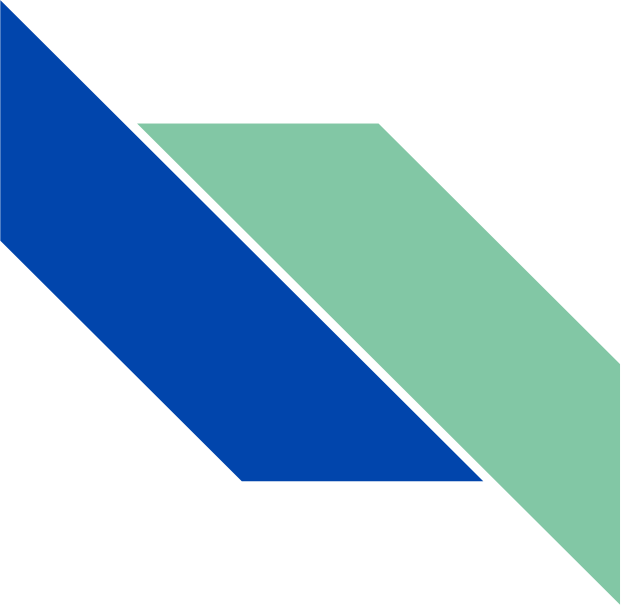
Not in plain sight! (no sticky notes on monitors)

Best practice: stored only in staff brains, with knowledge of how to reset them

GOAL: patron protection

From ALA's Privacy Tool Kit:

"Confidentiality of library records is a core value of librarianship…For libraries to flourish as centers for uninhibited access to information, librarians must stand behind their users' right to privacy and freedom of inquiry."



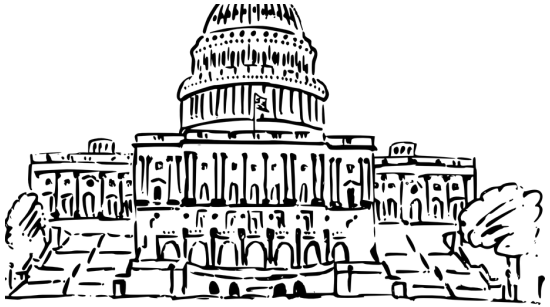
PRIVACY TOOLS

Who wants personal data?

COMPANIES

advertising

GOVERNMENT



INDIVIDUALS

https://www.acxiom.com/what-we-do/data-packages

Game Day Data Package

Plan your winning strategy with the best consumer data package in the game. We open our playbook to help you reach sports fans.

Valentine's Day Data Package

Forbes called it "America's $20 Billion Day of Love," and Acxiom can introduce you to this seasonal audience of your dreams – gift givers and big spenders.

Mother's Day Data Package

Using audience insights, Acxiom can help you target your ideal digital audience for this mother of all marketing opportunities.

Summer Fun Data Package

As temperatures heat up, so does your opportunity to reach seasonal audiences through Acxiom's data packages. Connect to vacationers, campers, boaters, beach goers and other active digital audiences.

Aug. 2012

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS

Home » News & Events » Press Releases » Google Will Pay $22.5 Million to Settle FTC Charges it Misrep
Internet Browser

Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser

Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order

July 2019

Home » News & Events » Press Releases » FTC Imposes $5 Billion Penalty and Sweeping New

FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook

FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency

July 2019

Slate: Facebook, Inc. expects 2019 earnings of $69 billion

https://slate.com/technology/2019/10/facebooks-2019-fines-and-settlements.html

2019 documentary investigating U.K. digital marketing firm Cambridge Analytica and targeted social media advertising campaigns in political elections worldwide

Directed by Karim Amer and Jehane Noujaim

“Filter bubble”

Merriam-Webster.com: “an online environment in which people are exposed only to opinions and information that conform to their existing beliefs”

Fun experiment: Try same keywords in different search engines on various computers

“Anonymize” your ads

Facebook:
https://www.facebook.com/ads/preferences

Google:
https://support.google.com/ads/answer/2662922

DuckDuckGo

https://duckduckgo.com

Free “privacy-dedicated search engine that does not collect or share personal information” such as search terms, location, etc.

“Private” browsing modes

Chrome privacy settings	Incognito window
Firefox privacy settings	Private window
Internet Explorer settings	InPrivate window
Safari privacy settings	Private window

Browser add-ons

Ghostery

“control over ads and tracking technologies”

Privacy Badger

“block invisible trackers”

More privacy tools and info

Library Freedom Project:
https://www.libraryfreedom.org

Electronic Frontier Foundation:
https://www.eff.org