THE BOARD OF PENSIONS
OF THE PRESBYTERIAN CHURCH (U.S.A.)

Cybersecurity and Stewardship

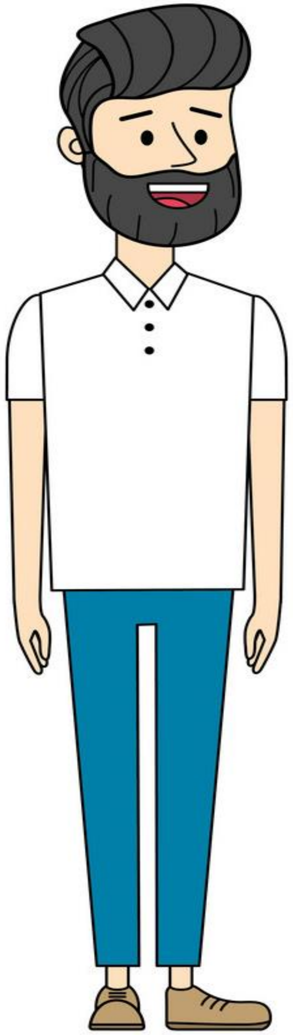
Enhancing Your Church's Cyber Strategy

Nick Kotoulas
Assistant Director, Information Technology

Who am I?

Nick Kotoulas, Assistant Director of the IT Service Desk at the Board of Pensions PC(USA), has over 14 years of experience in the field of information technology. Nick works with his team of service support specialists to help users successfully navigate technology systems at the Board. As a certified ITIL Strategic Leader and Managing Professional, and with a degree from Drexel University in Info Tech, Nick prides himself on his passion for cloud computing, technology trends, and user support and education.

Contact: **Nkotoulas@pensions.org**



Why are we here?

Cybersecurity & stewardship?

What is the real connection between stewardship and cybersecurity? And why is this something that everyone should be thinking about?

In stewardship, you must collect...

Your congregants will be:

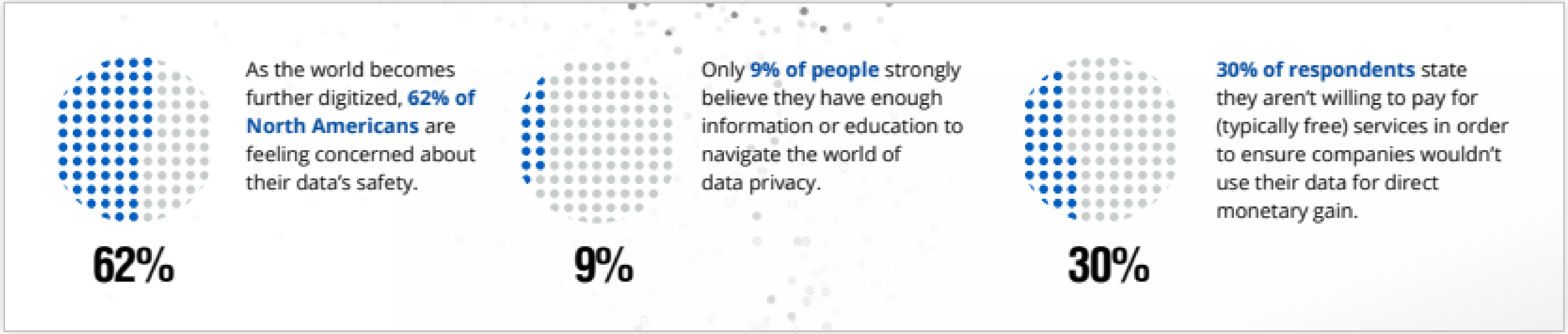
- ✓ giving you their data for stewardship
- ✓ giving their data to any vendor that is processing data on your behalf
- ✓ accessing that vendor's technology on a personal device
- ✓ accessing that technology over the Wi-Fi network within your church

This is why cybersecurity matters to your congregation.

Sharing data requires trust

The complexity of the modern technology space is finding a balance between privacy and convenience.

While it is easier and easier to accomplish day-to-day transactions through technology, this requires more and more of your personal data to be entered, processed, and stored in technology that you have little to no control over.



62%

As the world becomes further digitized, **62% of North Americans** are feeling concerned about their data's safety.

9%

Only **9% of people** strongly believe they have enough information or education to navigate the world of data privacy.

30%

30% of respondents state they aren't willing to pay for (typically free) services in order to ensure companies wouldn't use their data for direct monetary gain.

Sensitive data types

- **PII (Personally Identifiable Information)** – any data that permits the identification of an individual
- **Sensitive PII** – any data considered PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual
  - Social Security Number, Driver’s License, State Identification Number
  - Citizenship, Immigration Status, Ethnic, Religious, Sexual Orientation
  - Biometric Identifiers, Mother’s Maiden Name, Criminal History, Medical History
- **PHI (Protected Health Information)** – any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity and can be linked to a specific individual
- **PCI DSS (Payment Card Industry Data Security Standard)** – requirements intended to ensure all companies that process, store, and transmit financial information maintain a secure environment

Trends in data

As of July 2024, 20 states in the U.S. have passed comprehensive consumer data privacy laws, including California, which was the first state to do so.

These laws often share common provisions, such as the right to access and delete personal information and opt out of the sale of personal information; however, the laws vary by state.

Meanwhile, more and more data is being collected, bought and sold, and used in ways that may not always be in a consumer's best interest. With that, while some data is not always considered sensitive by all parties, this doesn't mean that individuals do not take it seriously.

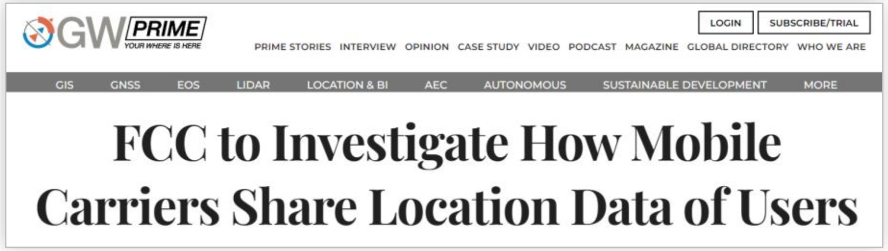
Concerns around:

- **Tendencies**: hints at your behaviors, and what you may prefer or like may be used in targeted ads or interests
- **DEI**: discloses your race, religion, etc. and creates the potential for bias.
- **Geolocation**: knows your location, tracks your patterns historically, predictive tracking; these pose various risks.

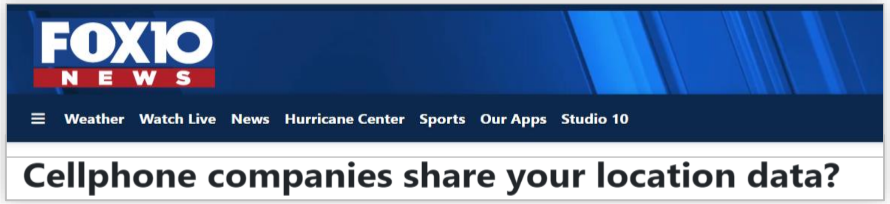
Geolocation

How is Geolocation data captured?

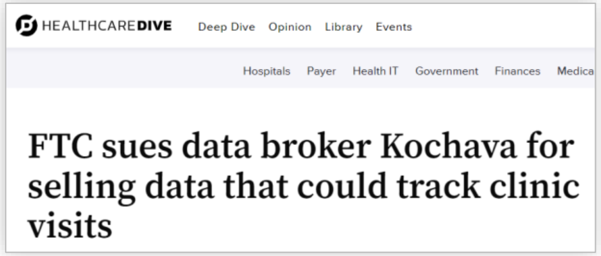
- GPS (Global Positioning System)
- cellular networks
- internet usage
- transaction data
- geotagging
- map applications
- point of sale


GW PRIME
YOUR WHERE IS HERE
LOGIN
SUBSCRIBE/TRIAL
PRIME STORIES INTERVIEW OPINION CASE STUDY VIDEO PODCAST MAGAZINE GLOBAL DIRECTORY WHO WE ARE
GIS GNSS EOS LIDAR LOCATION & BI AEC AUTONOMOUS SUSTAINABLE DEVELOPMENT MORE

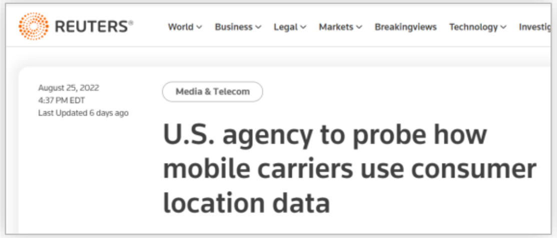
FCC to Investigate How Mobile Carriers Share Location Data of Users


FOX10 NEWS
Weather Watch Live News Hurricane Center Sports Our Apps Studio 10

Cellphone companies share your location data?

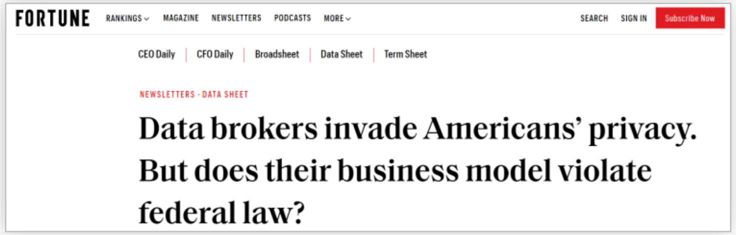

HEALTHCAREDIVE
Deep Dive Opinion Library Events
Hospitals Payer Health IT Government Finances Medica

FTC sues data broker Kochava for selling data that could track clinic visits


REUTERS
World Business Legal Markets Breakingviews Technology Investig
Media & Telecom

August 25, 2022
4:37 PM EDT
Last Updated 6 days ago

U.S. agency to probe how mobile carriers use consumer location data


FORTUNE
RANKINGS MAGAZINE NEWSLETTERS PODCASTS MORE
SEARCH SIGN IN Subscribe Now
CEO Daily | CFO Daily | Broadsheet | Data Sheet | Term Sheet
NEWSLETTERS · DATA SHEET

Data brokers invade Americans' privacy. But does their business model violate federal law?

This is why data matters so much

Your congregants are trusting you not only with their offerings, but with their personal data. This puts the onus on each church to:

- ✓ protect your congregation
- ✓ protect the stewardship your church has received
- ✓ protect yourself and your family

Online transactions have become the new norm coming out of the COVID lockdowns, but this has also led to a tremendous increase in nefarious behaviors by bad actors.

By building trust with your congregants, they are more likely to support the church.

- ✓ Communicate clearly with your congregation.
- ✓ Secure the experience at every step.
- ✓ Give users the right to opt out.
- ✓ Restrict access to any data.

What’s been going on lately?

Corporations under attack - 2023

Boeing: In December, a cybercrime gang leaked internal data from Boeing after a ransomware attack.

ICMR Indian Council of Medical Research: In October, 815 million records were breached.

23andMe: In October, 20 million records were breached.

Redcliffe Labs: In October, 12,347,297 records (7TB) were breached.

Corporations under attack - 2023

MOVEit: In May, the file transfer platform MOVEit was hacked, affecting at least 160 schools, as well as government agencies, financial institutions, and other organizations.

T-Mobile US: In January, a data breach that began in November 2022 exposed personal customer information for 37 million customers.

ChatGPT: In March, a cyberattack exposed users' first and last names and email addresses.

Activision: In February, the video game publisher Activision confirmed a data breach that occurred in December.

Corporations under attack - 2024

Disney: In July, “NullBulge” accessed internal Slack messages from employees, amounting to around 1.2 TB of data.

AT&T: In July, AT&T paid $370,000 to hackers to delete 70 million records of customer data, former and current.

Truist Bank: In October 2023, employee information was discovered online for sale.

Tile: In June, Life360, the company behind the Tile Tracker device, disclosed a breach resulting in 450,000 records of customers and Tile device IDs leaked.

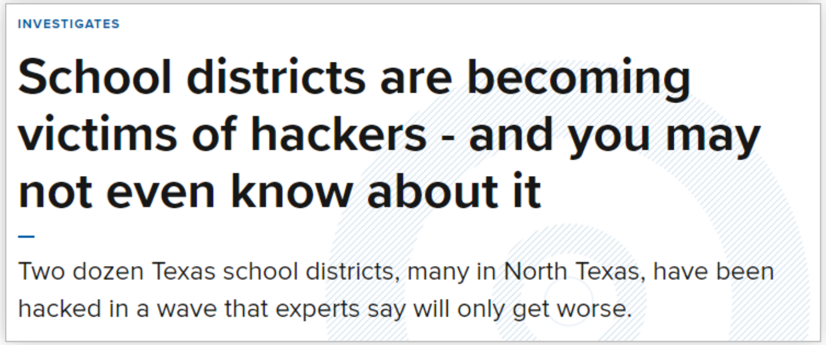
Corporations under attack - 2024

Ticketmaster: In May, 560 million customer records, including payment information, email data, and order history was offered for sale.

Dell: In May, 49 million customers were impacted when home addresses and order data was compromised.

CDK Global: In June, U.S. dealerships faced over $1 billion in losses when “Blacksuit” disrupted the Dealer Management Systems (DMS) with ransomware attack.

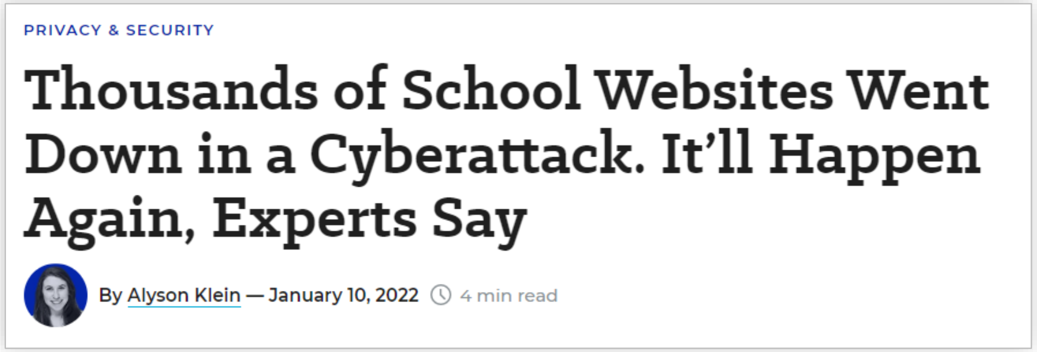
Hackers targeting school districts



INVESTIGATES

School districts are becoming victims of hackers - and you may not even know about it

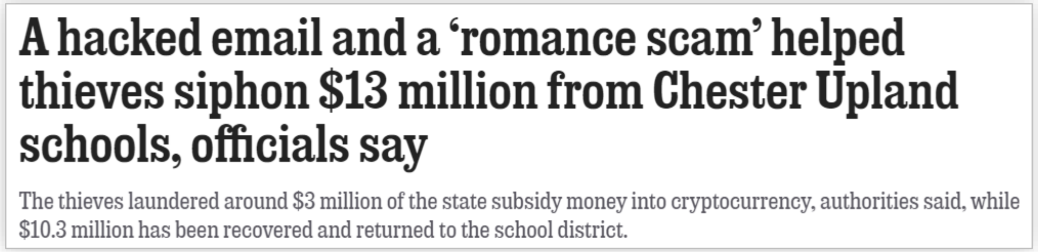
Two dozen Texas school districts, many in North Texas, have been hacked in a wave that experts say will only get worse.



PRIVACY & SECURITY

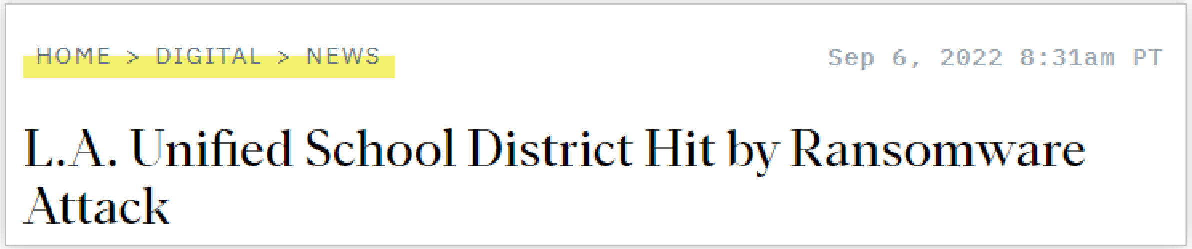
Thousands of School Websites Went Down in a Cyberattack. It'll Happen Again, Experts Say

By Alyson Klein — January 10, 2022 4 min read



A hacked email and a 'romance scam' helped thieves siphon $13 million from Chester Upland schools, officials say

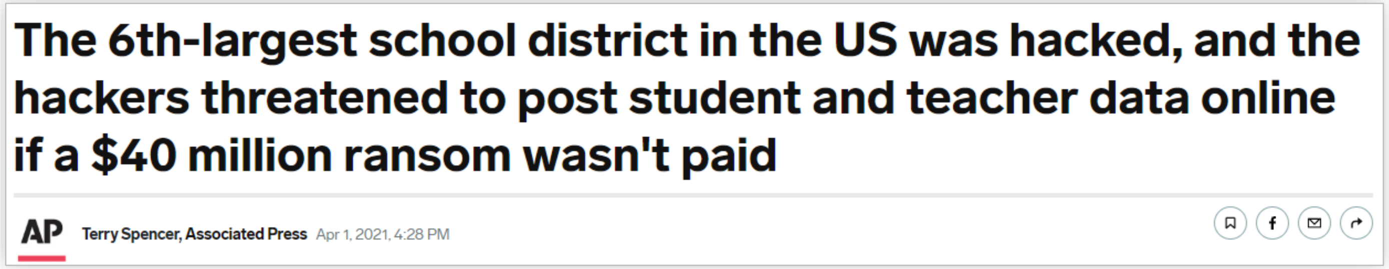
The thieves laundered around $3 million of the state subsidy money into cryptocurrency, authorities said, while $10.3 million has been recovered and returned to the school district.



HOME > DIGITAL > NEWS

Sep 6, 2022 8:31am PT

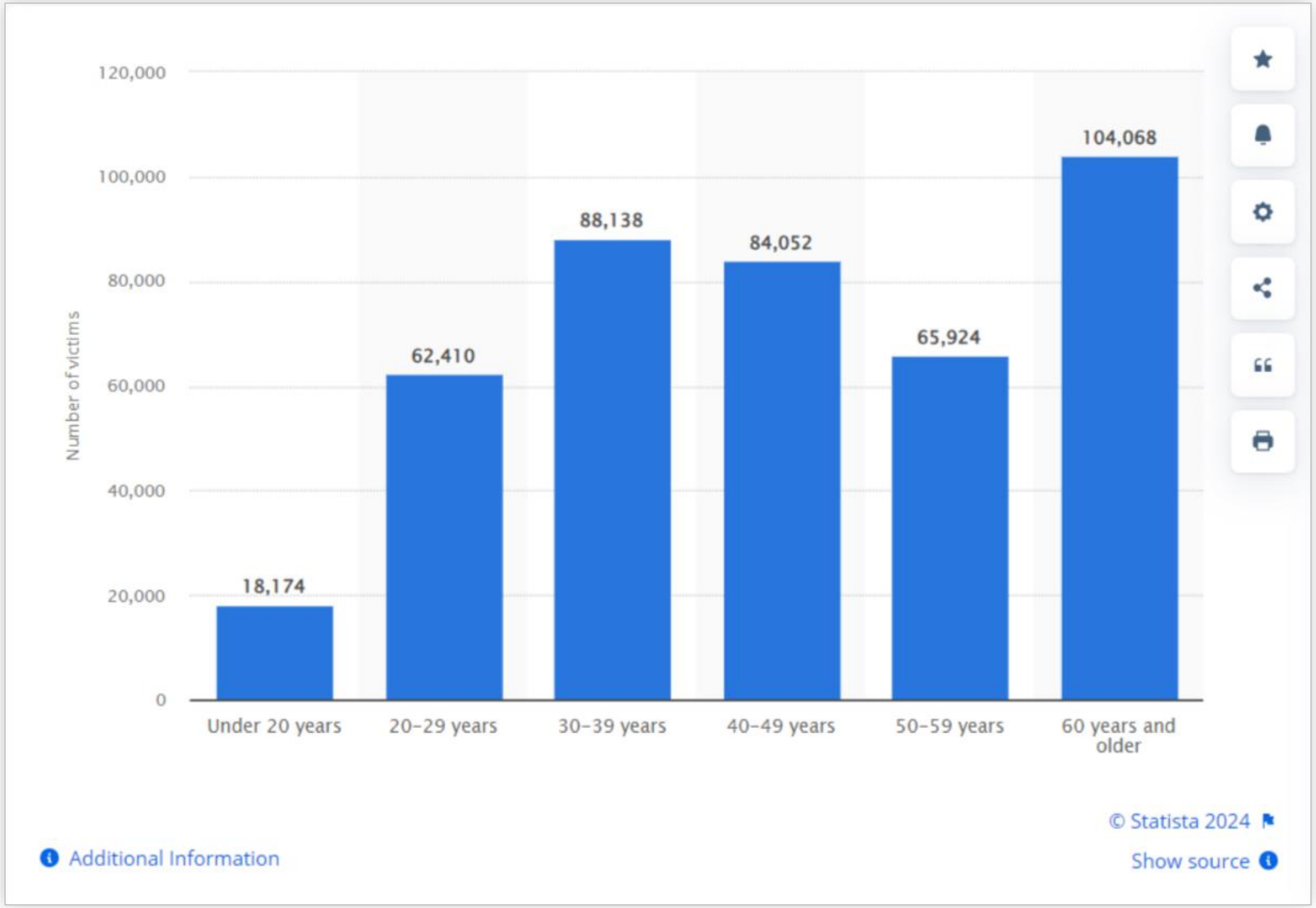
L.A. Unified School District Hit by Ransomware Attack



The 6th-largest school district in the US was hacked, and the hackers threatened to post student and teacher data online if a $40 million ransom wasn't paid

AP Terry Spencer, Associated Press Apr 1, 2021, 4:28 PM

Cyber crime victims (USA)



Who is after our data, and why?

Types of hackers

Not all hackers are ill-intentioned. Here is how they tend to be categorized.

Black Hat	Financial gain. These are the hackers you hear about in the news.	☹
White Hat	Desire to combat black hats, help businesses.	☺
Grey Hat	Flip flop between black and white – really looking at personal enjoyment.	😐
Red Hat	Vigilante justice.	😐
Blue Hat	Vengeful and aggressive, but only if you make them.	☹
Green Hat	New hackers, wanting to learn how to be full-blown hackers.	😐
Script Kiddies	Chaos and disruption. Download, watch videos, deploy.	☹

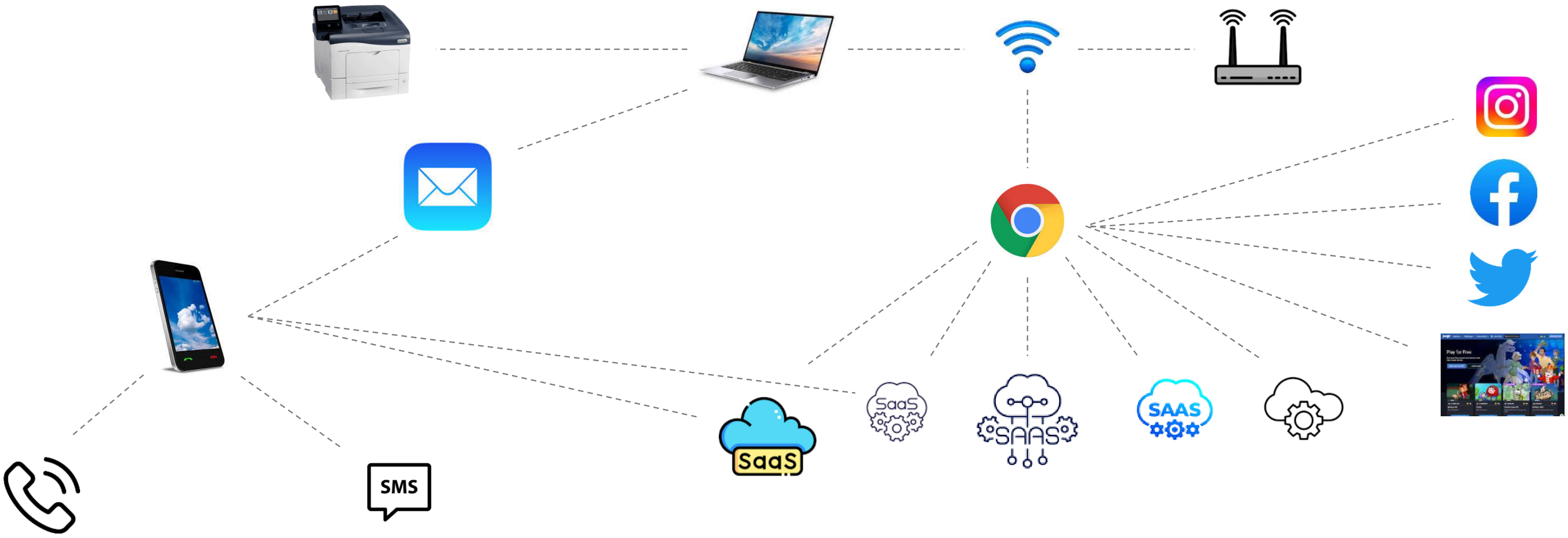
Who are the “bad actors” & why do they attack?

Profiteers	“**Show Me the Money**,” these are individuals simply looking for financial gain.	**Script Kiddies** **Black Hat**
Nation State	“**License to Hack**,” these actors work for the government to disrupt or compromise target governments, organizations, or individuals to gain access to valuable data or intelligence or create incidents.	**Black Hat** **White Hat**
Insider Threat	“**Insider Hackers**” are authorized to find vulnerabilities in the company’s network and help fix them. “**Insider Crackers**” find and exploit flaws for some personal gain.	**White Hat** **Green Hate, Blue Hat, Black Hat**
Ideologues	“**Hacktivists**” commit cyber crime to further their own beliefs and ideologues. Include anti-capitalists and anti-corporate idealists and attacks are inspired by political and social issues. “**Terrorists**” want to create panic to achieve whatever goals they have set.	**Red Hat** **Script Kiddies, Blue Hat, Red Hat**
Thrill Seekers	“**Thrill Seekers**” are out for the challenge of breaking into a network. This can be for entertainment, for bragging rights, or simply for practice.	**Green Hat**
Grey Hat	“**Trolls**” tend to be thrill seekers that have evolved a bit and are now simply attacking a system for recreation. They intend to cause harm and spread dis- and/or misinformation.	**Script Kiddies, Green Hat, Blue Hat**

How will they attack?

Attack surface

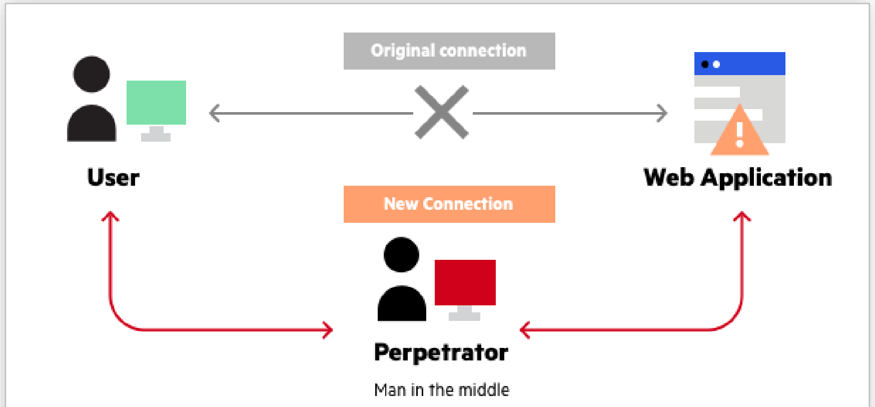
An “**attack surface**” is the collection of all possible points where an unauthorized user can access a system and extract data



Network attacks

Direct access to your network:

Man in the middle:



Man in the middle attack example

- ✓ Secure access to ethernet ports, keep access points protected.
- ✓ Ensure that your network is encrypted: **Virtual Private Network (VPN)**
- ✓ Restrict material delivered over the network: **Web Filtering, Firewall**
- ✓ Monitor for false networks.

Physical security

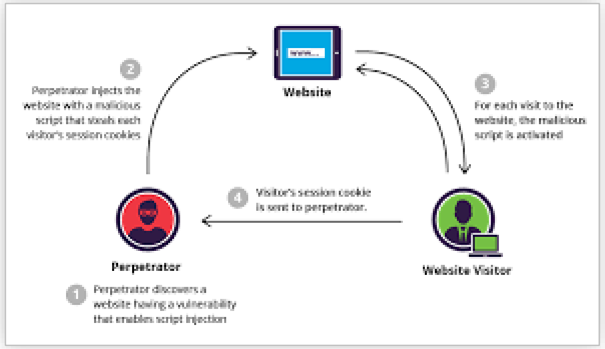
By gaining access to non-public areas of the church, bad actors may gain access to church assets and/or sensitive data.

Web attacks

While your network is a target, a wider net is often cast by leveraging the web as an attack surface. Bad actors will use websites to gain access to your devices, obtain your personal information and credentials, introduce malicious software, etc.

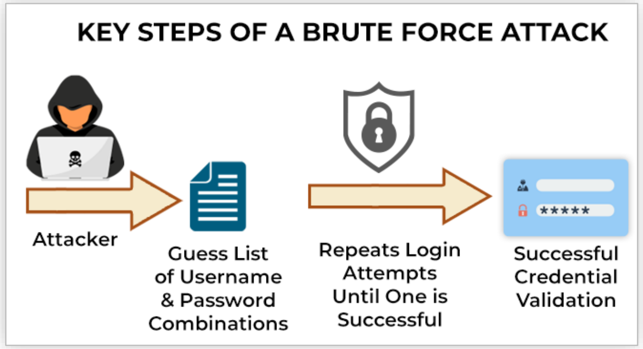
Most attacks will target the site itself, but there are some that will directly go after you as an end user.

Cross-site scripting


Website
2 Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3 For each visit to the website, the malicious script is activated
4 Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1 Perpetrator discovers a website having a vulnerability that enables script injection

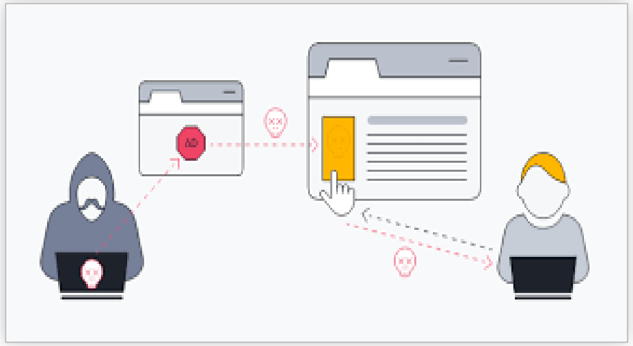
- Only use secure websites (HTTPS)
- Restrict the use of cookies
- Clear cookies periodically

Brute force attack


KEY STEPS OF A BRUTE FORCE ATTACK
Attacker
Guess List of Username & Password Combinations
Repeats Login Attempts Until One is Successful
*****
Successful Credential Validation

- Use complex passwords
- Change passwords periodically
- Do not repeat passwords

Malvertising



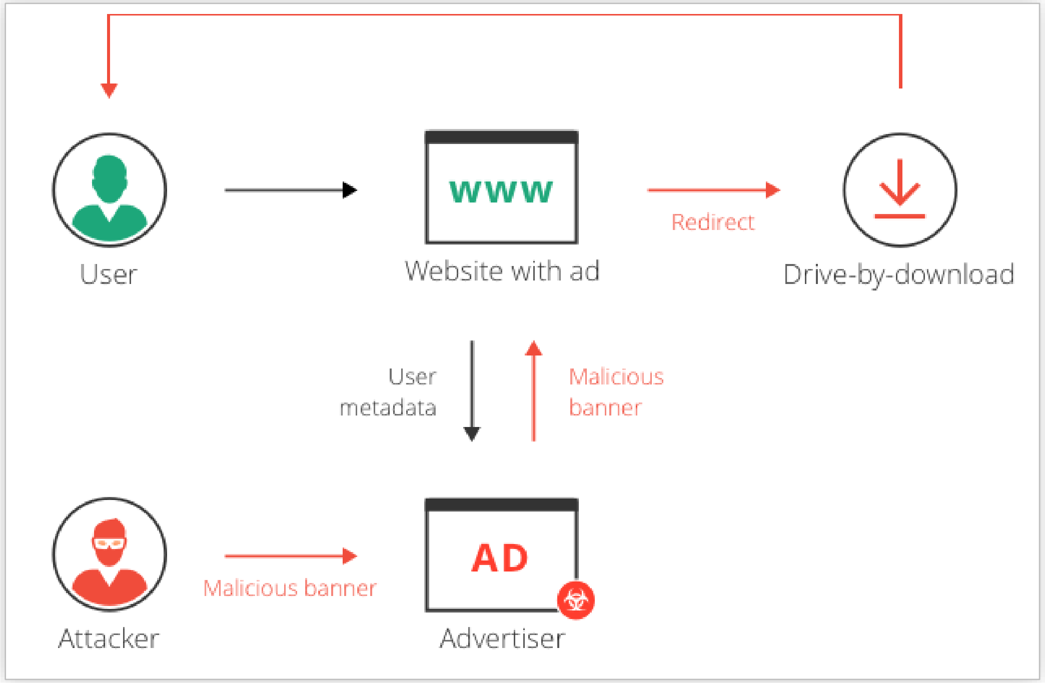
Malvertising (malicious advertising)

Online advertising is a rather complex system: ad exchanges, ad servers, retargeting networks, content delivery networks.

All of this means there are multiple interactions between different servers, which creates a lot of opportunity for attackers to place malicious content.

How to protect against malvertising:

- Ensure you have up-to-date antivirus software on your devices.
- Update your browsers.
- Do not click on ads, click bait, etc.
- Enable ad blockers.



London Stock Exchange

The Atlantic
EST. 1857

The New York Times

Spotify

Malware (malicious software)

Malware is any intrusive software that has been developed to steal data and/or damage or destroy computers and computer systems.

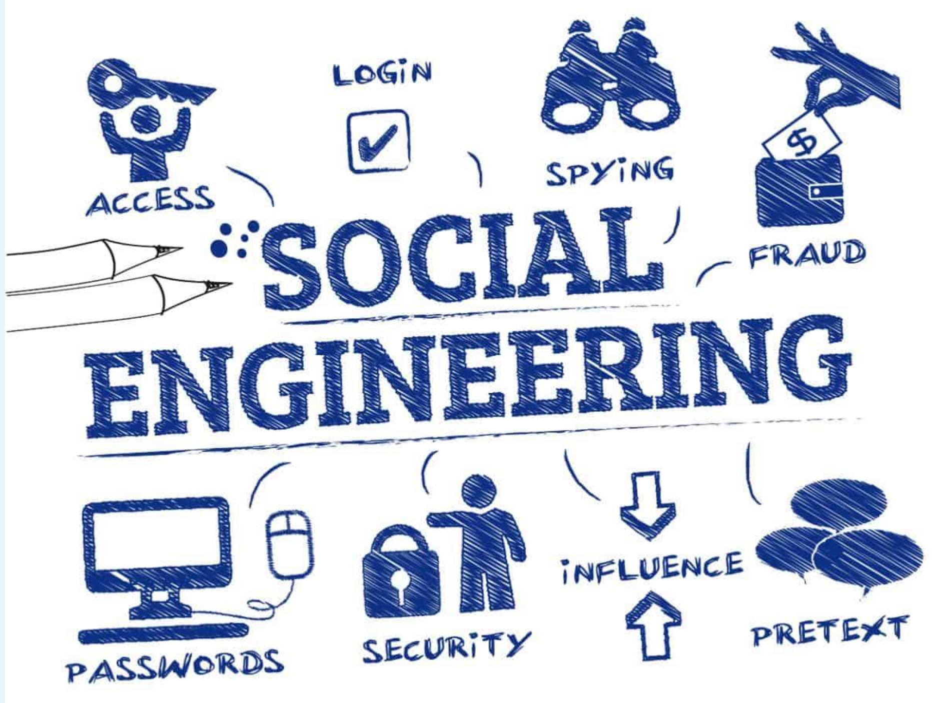
- Virus is attached to a program or file so that it can transfer from computer to computer, but it must be triggered by the activation of their host.
- Worm is very similar to a virus; however, once entering a system, a worm can run and self-replicate without a triggering event and spread from computer to computer with no assistance.
- Trojan Horse is a program that looks like a genuine application, but it does not replicate itself. It creates a backdoor entry to your computer for a bad actor to access the network.
- Spyware is designed to track all of your computer activities, from user information to browsing habits, and transmits all of the data back to a remote entity. Targets sensitive data and can grant remote access.
- Adware automatically displays advertisements online to generate revenue. It is not always malicious; however, in some cases it may install additional programs, including Trojan Horses and spyware.
- Ransomware infects a network and can lock a system and block access, sometimes with threats to publish or delete personal data.
- Bots are like worms but are much more versatile and can be modified within hours of a new exploit publication.

Social engineering

This is when bad actors will **use public or common information** about you to deceive you into divulging personal or confidential information that will allow them to either breach your company or steal your identity or personal assets.

Where did they get the data?

- public information
- social media
- geolocation
- dark web
- spyware



How do they attack?

- pretexting
- tailgating
- phishing
- baiting
- quid pro quo

Pretexting

Just like hackers can **impersonate brands** to get your information, they will also **impersonate people.**

Attackers will create a fake identity to prey on your trust and good will to gain information or money.

Some examples:

- fake social media accounts
- impersonating IT
- impersonating customer service

Physical intrusions

- **Tailgating** - when someone attempts to follow you into a building to gain access or convinces you to allow them access without a building or guest pass
- **Dumpster diving** – digging through a person's garbage to obtain documents with personal & confidential information
- **Shoulder surfing** – looking over a target's shoulder while they are accessing information on a device; most commonly happens at airports, coffee shops, or public workplaces

‘Phishing’ for information

- **Phishing** is when attackers use a means of contact, mostly **email**, to trick victims into providing sensitive information or clicking a malicious link.
  - Phishing is the most common type of social engineering attack.
- Messages are composed to attract the victim’s attention.
  - Social engineers will try and **pique your curiosity**, **appeal to urgency**, or **gain your trust** to convince you to send them personal information.

Baiting & quid pro quo

- **Baiting** exploits your curiosity or proactive nature.
  - **viruses** disguised as software updates
  - **flash drives** left in public areas
  - **new browser games** full of spyware

- Similar to baiting, **quid pro quo** promises something in return for your personal information.
  - fake contests or raffles
  - free products or coupons
  - free software or games

Time to dive in!

All bets are off (vishing)

- Hotel and Casino giant MGM Resorts reported losses from a recent vishing attack that exceeded $110 million.
- Vishing involves a convincing phone call, rather than an email, to trick targets into divulging sensitive information.

- A bad actor tricked an employee (part of the support team) to reset the password and MFA for an employee's account.
- Many bad actors do homework on the organization and compile data including job titles and names of employees, the infrastructure, etc.

Teachable takeaways

- Don’t give out sensitive information or act until you’re 100% sure of the person’s identity.

- Always verify before you trust by taking an additional step, such as calling the person back on a trusted line or speaking to them in person.

- Keep current job information on professional networking sites as generic as possible to protect yourself and your organization.

Everything. Gone. (pig butchering)

- The “Pig Butchering Scam” has become the scourge of the internet.

- A long con that tricks victims into sending money to fraudulent investment platforms, it has exploded to becoming the costliest scam out there, with victim losses totaling tens of billions of dollars worldwide.

- It’s a highly sophisticated con typically ran by organized crime rings involving 3 stages: targeting the victim, fattening the victim, targeting the victim, and butchering the victim.

Teachable takeaways

- Scammers use psychological manipulation techniques such as flattery and relatability to gain your trust. Never send money or cryptocurrency to anyone you haven't met in real life or don't personally know and trust.

- Never join an investment site, or download an app, at the direction of someone you've only met online. Even if it seems real, it could be a fraudulent app that scammers are in control of.

- There's no such thing as "guaranteed returns." Never believe anyone or any site that promises returns or requests minimum investment amounts.

Clouded judgement (personal cloud storage)

- Android game developer, Ateam, recently announced 900,000 customer records had their personal data exposed.
- The breach occurred due to Ateam employees' improper use of the cloud storage service, Google Drive.

- Company sensitive data was loaded on a personal cloud storage account instead of a corporate cloud storage account.
- Cloud storage, while convenient, comes with inherent risks and must be used with caution.

Teachable takeaways

- Be sure to follow your organization’s policy regarding the use of cloud storage services such as Google Drive, Dropbox, or OneDrive.

- In addition to the threat of your personal cloud account being breached, the cloud storage service itself could succumb to a vendor-wide attack.

- Storing company data, especially sensitive data, on a personal cloud account is inherently risky and should be avoided.

Generative A.I. (garbage in, garbage out)

- 23andMe suffered a data breach resulting in the theft of user genetic information including ethnicity and family relationships.

- The rapid implementation of public generative artificial intelligence (G.A.I.) models, such as ChatGPT, has led to two types of risks:
  - Input risk – sensitive data is stored into G.A.I. that can be stolen by hackers.
  - Output risk – information generated by G.A.I. is wrong or biased.

Exercise extreme caution with G.A.I. tools!

Teachable takeaways

- The risks associated with public generative artificial intelligence tools, such as ChatGPT, fall into two broad categories: input and output risk.

- Public G.A.I. input risk lies in the fact that information you use to prompt, upload, or have analyzed may not be kept secure and therefore may be exposed to hackers and the general public.

- Public G.A.I output risk lies in the fact that information is generated by unknown public sources. This could lead to misinformation, miscommunication, and even legal issues.

Thank you for attending!

Let's take a few moments to walk through the handouts and guides provided.

1717

THE BOARD OF PENSIONS

OF THE PRESBYTERIAN CHURCH (U.S.A.)