Cybersecurity & Stewardship

What Every Church Needs to Know

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

Bobb Hawkey
Director IT Strategy & Transformation

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 wifi 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 know control over.

Why Data Matters So Much

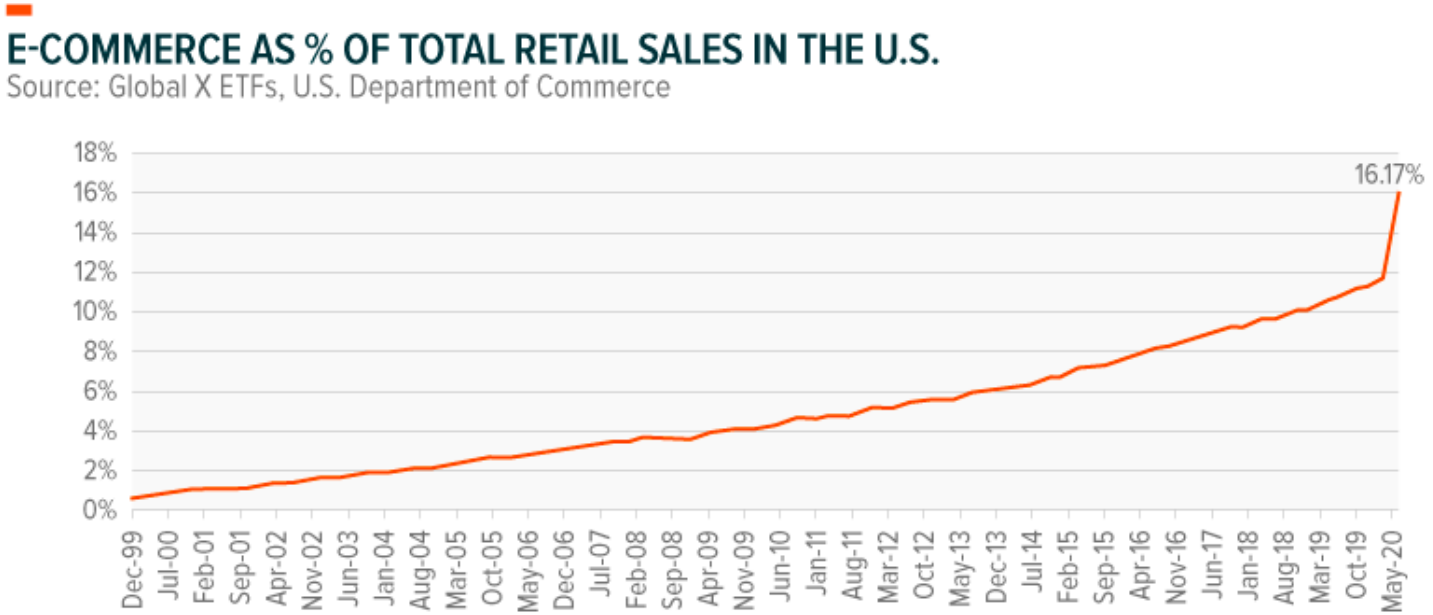
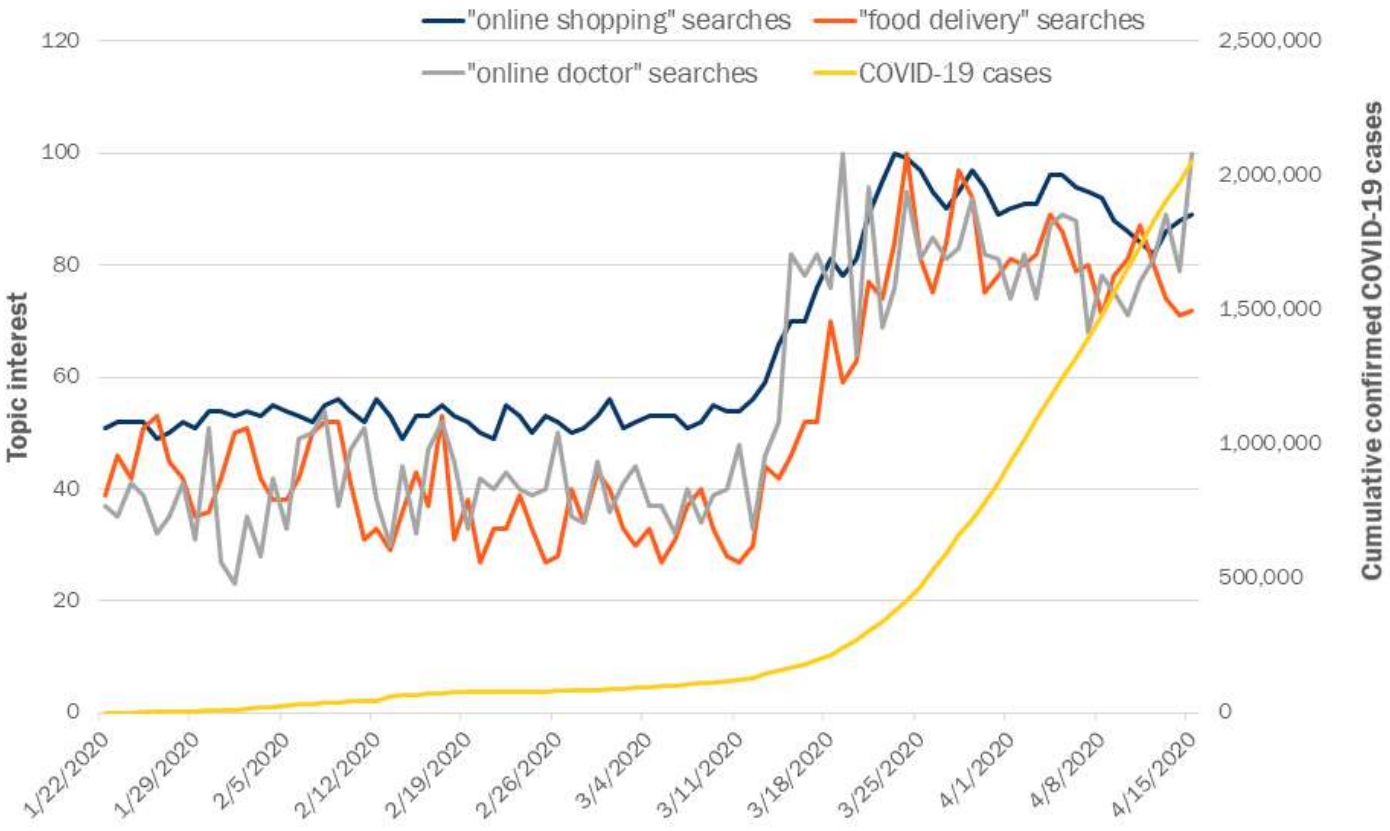


Figure 1. Worldwide Google searches and COVID-19



Source: Google Trends topic interest over time (normalized to index with scale 0-100); Johns Hopkins Coronavirus Resource Center

BROOKINGS

Sensitive Data Types

- PII (Personally Identifiable Information) – Any data that permits the identity 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

The definition of sensitive PII is a bit progressive – even though that is from the Department of Homeland Security. Various governing agencies view this differently.

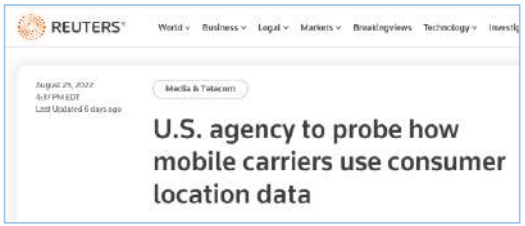
U.S. law on data privacy in regards to consumer protection is very limited, but California and other states have developed their own. The expectation is that a GDPR (General Data Protection Regulation)-like national privacy policy will come into law in the near future.

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, like. May be used in targeting.
- DEI: Discloses your race, religion, etc. Potential for bias.
- Geolocation: Knows your location, tracks your patterns historically, predictive tracking. Various risks.

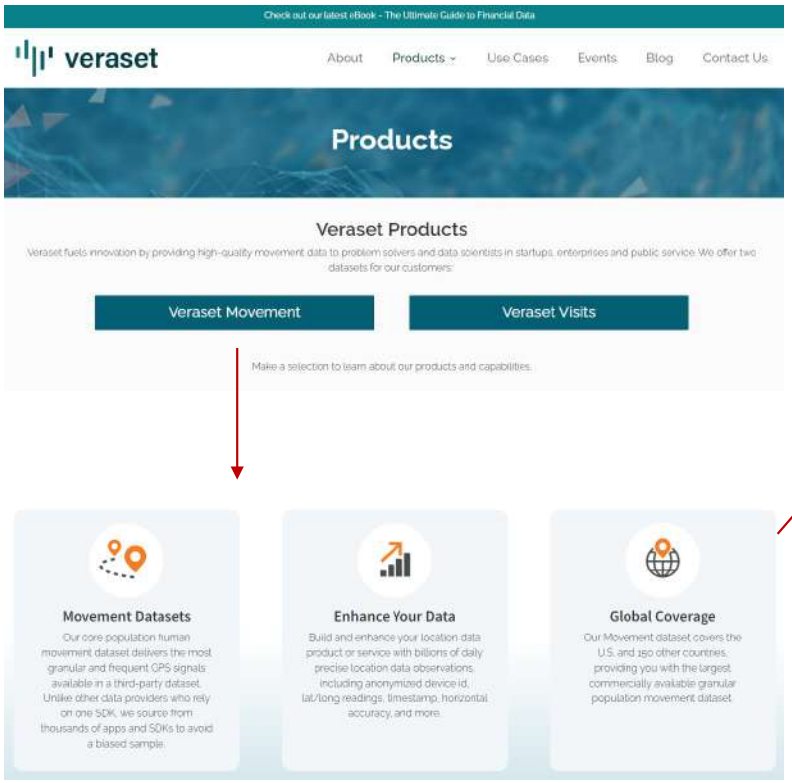
Geolocation



How is Geolocation Data Captured?

1. GPS (Global Positioning System)
2. Cellular Networks
3. Internet Usage
4. Transaction Data
5. Geotagging
6. Map applications
7. Point of Sale

Monetization of Data - Example



Case Studies:

Adtech
Real Estate & Retail
Financial Services & Economists
Social Impact
City Planning, Mobility, & Transportation
Geographic Information Systems

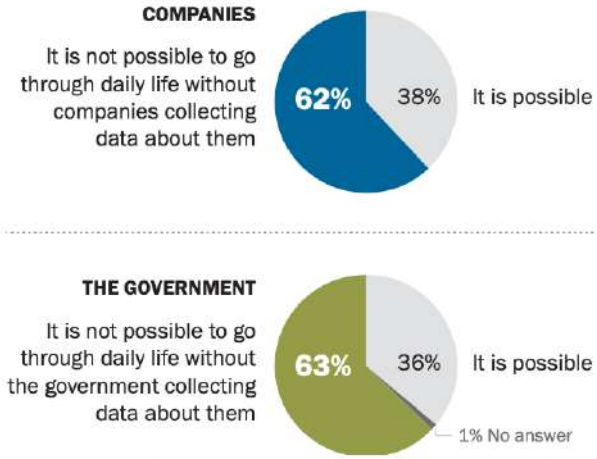
Socio-Economic Trends

- Join mobility data with aggregate demographics to understand who is visiting and how that changes over time

Concerns Around Data Collection

Roughly six-in-ten Americans believe it is not possible to go through daily life without having their data collected

% of U.S. adults who say ...



Note: Respondents were randomly assigned to answer a question about whether they think it is possible to go about daily life without having personal information collected from them by "companies" or "the government."
Source: Survey conducted June 3-17, 2019.
"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

PEW RESEARCH CENTER

Majority of Americans feel as if they have little control over data collected about them by companies and the government

% of U.S. adults who say ...

		Companies	The government
Lack of control	They have very little/no control over the data __ collect(s)	81%	84%
Risks outweigh benefits	Potential risks of ___ collecting data about them outweigh the benefits	81%	66%
Concern over data use	They are very/somewhat concerned about how __ use(s) the data collected	79%	64%
Lack of understanding about data use	They have very little/no understanding about what __ do/does with the data collected	59%	78%

Note: Those who did not give an answer or who gave other responses are not shown.
Source: Survey conducted June 3-17, 2019.
"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

PEW RESEARCH CENTER

This Why Data Matters So Much

Your congregants are trusting you not only with their offerings, but with their personal data. This puts the ownness 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.

1. Communicate clearly with your congregation.
2. Secure the experience at every step.
3. Give users the right to opt out.
4. Restrict access to any data.

The World At Large

What is Eroding their Trust?

Corporations Under Attack - 2021

- Lockbit ransomware attack on July 30th; contained immediately.
- Confirmed ransomeware attack and data breach on March 7th, all US systems impacted.
- Tokyo headquarters suffered ransomware attack, disrupting business operations.
- DarkSide ransomware attack in February with 1,300 individuals data exposed.
- DoppelPaymer ransomware impacted internal and externally facing systems.
- Babuk ransomware stole 500 GB of contract and financial data.
- Conti ransomware attack encrypted thousands of devices and stole data.
- BlackByte group encrypted systems and held them at ransom.
- Clop ransomware operators exfiltratrad data through a vulnerability.

National Disruptions

CYBERSCOOP

Another European nation hit by hackers, Montenegro grapples with ongoing ransomware attack

NATO Countries Hit With Unprecedented Cyber Attacks

Montenegro, Estonia and new NATO applicant Finland are just three of the countries being hit hard by sophisticated cyber attacks. What's happening and who's next?

September 04, 2022 - Dan Lohmann

"Earlier this month, both Finland and Estonia were victims of a cyberattack, though Estonian officials said they successfully thwarted the attack that targeted the country's public and private institutions.

"The attack followed the removal of a Soviet war monument from an eastern Estonian city bordering Russia.

"Killnet, a Russian-backed hacking group, claimed responsibility for the attempted attack against Estonia, Reuters reported."

And back in April, *Balkan Insight* reported that cyber attacks hit Romanian websites and the Czech Republic.

The Wall Street Journal reported earlier this year that Finland and Sweden were also being hit by cyber attacks: *"Authorities in Sweden and Finland have raised alert levels for cyberattacks, concerned they face increased hacking risks because of the war in Ukraine and the two Nordic countries' subsequent applications to join NATO.*

"Since Russia invaded Ukraine in February, cybersecurity officials in Sweden and Finland haven't seen an increase in attacks targeting critical infrastructure, though they say the countries are becoming more interesting targets for hacking groups with Russian ties.

"The two Nordic countries applied to join the North Atlantic Treaty Organization on Wednesday, after decades of neutrality."

U.S. Risks

Vulnerable U.S. electric grid facing threats from Russia and domestic terrorists

60

BY BILL WHITAKER
AUGUST 28, 2022 / 7:01 PM / CBS NEWS

On the night of April 16, 2013, a mysterious incident south of San Jose marked the most serious attack on our power grid in history.

For 20 minutes, gunmen methodically fired at high voltage transformers at the Metcalf Power substation. Security cameras captured bullets hitting the chain link fence.

And what the former commandos found looked familiar. They discovered the attackers had reconnoitered the site and marked firing positions with piles of rocks. That night they broke into two underground vaults and cut off communications coming from the substation.

Jon Wellinghoff: Then they went from these vaults, across this road, over into a pasture area here. There were at least four or five different firing positions.

They aimed at the narrow cooling fins, causing 17 of 21 large transformers to overheat and stop working.

Jon Wellinghoff: They hit them 90 times, so they were very accurate. And they were doing this at night, with muzzle flash in their face.

Bill Whitaker: If they had succeeded, what would've happened?

Jon Wellinghoff: Could've brought down all of Silicon Valley.

Hackers Targeting School Districts

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.

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

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

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.

HOME > DIGITAL > NEWS

Sep 6, 2022 8:31am PT

L.A. Unified School District Hit by Ransomware Attack

Bad Actors

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.
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.
Insider Threat	“Insider Hacker” are authorized to find vulnerabilities in the company’s network and help fix them.
	“Insider Cracker” find and exploit flaws for some personal gain.
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 what ever goals they have set.
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.
	“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.

Stats on Cybersecurity Stats

Profitability of cyber crime:

- University of Surrey (UK), Michael McGuire

~$1.5 Trillion every year

Illicit, illegal online markets	$860 billion
Trade secret & IP theft	$500 billion
Data trading	$160 billion
Crimeware, cybercrime-as-a-service	$1.6 billion
Ransomware	$1 billion

Revenue on Silk Road (2011-2013):

- Congressional Research Service

~$1.2 Billion

Price of Malware Installation Kit on Dark Web:

- Fortune

~$1

Average Time for a Data Breach Detection:

- Symantec

~196 Days

Malware Attacked Blocked on Windows (2018):

- Symantec

~144 Million

New Malicious Programs Registered Daily for Macs:

- MacKeeper

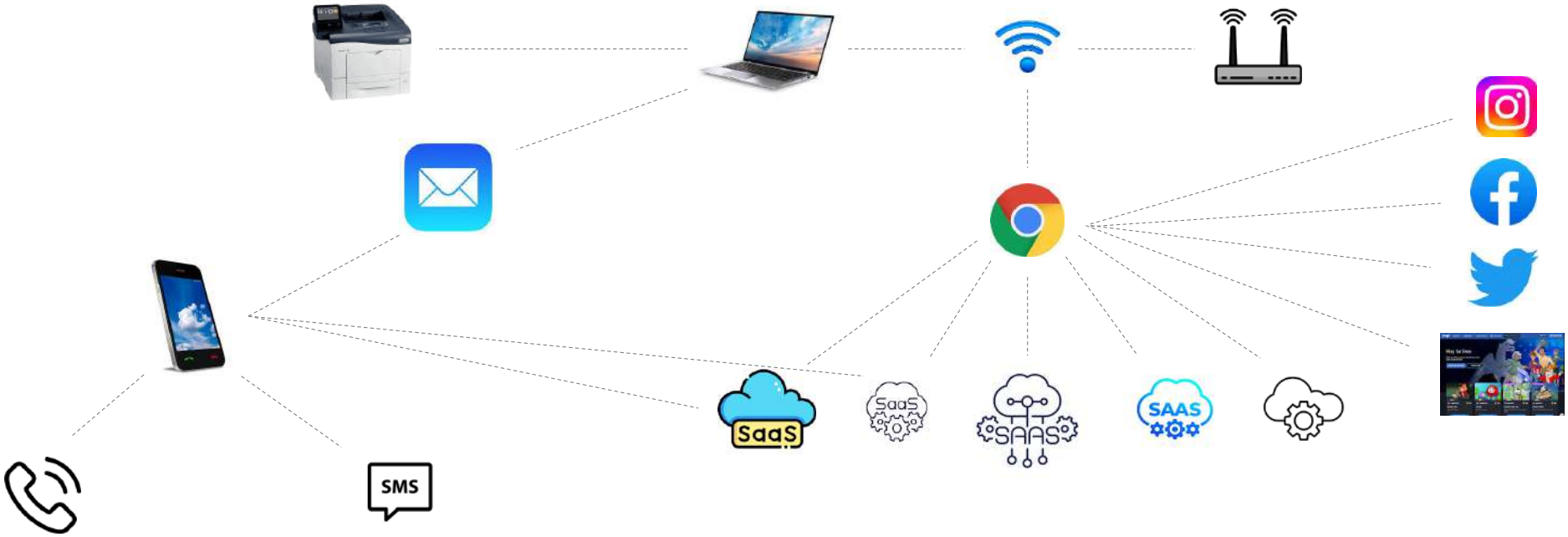
~250,000

How They Will Attack

And How You Can Protect Yourself and Your Organization

Attack Surface

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



The Most Vulnerable Parts of this Network?

People are always the weakest part of the security network – we trust people, we are afraid and will react, we multi-task. Most cyberattacks will target people.

Because of this, people are often the primary focus on attacks by bad actors.

Network Attacks

Direct Access to your Network:

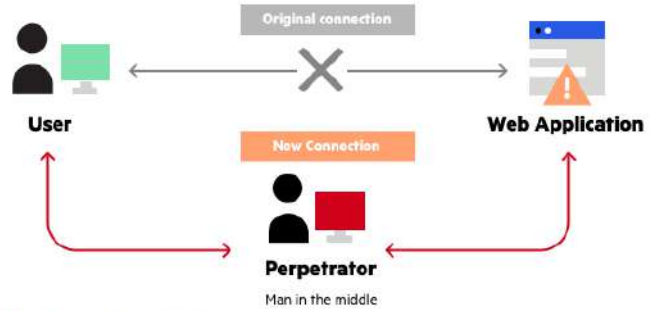
Secure access to ethernet ports, keep access points protected.

Ensure there your network is encrypted: Virtual Private Network (VPN)

Restrict material delivered over the network: Web Filtering, Firewall

Monitor for False Networks

Man in the Middle:



Man in the middle attack example

Physical Security

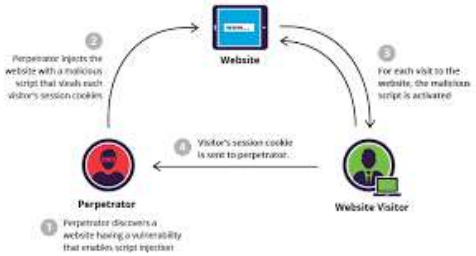
By gaining access to non-public areas of the church, bad actors may gain access to church assets and/or sensitive data.

Web Attacks

While your network is a target, a widen 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

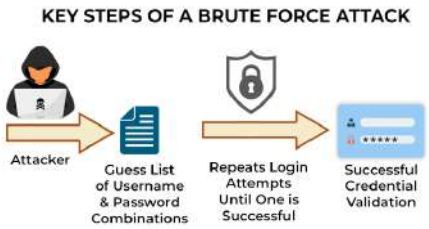


Only use secure websites (HTTPS)

Restrict the use of cookies

Clear cookies periodically

Brute Force Attack

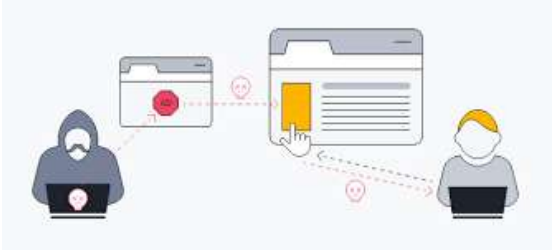


Use complex passwords

Change passwords periodically

Do not repeat passwords

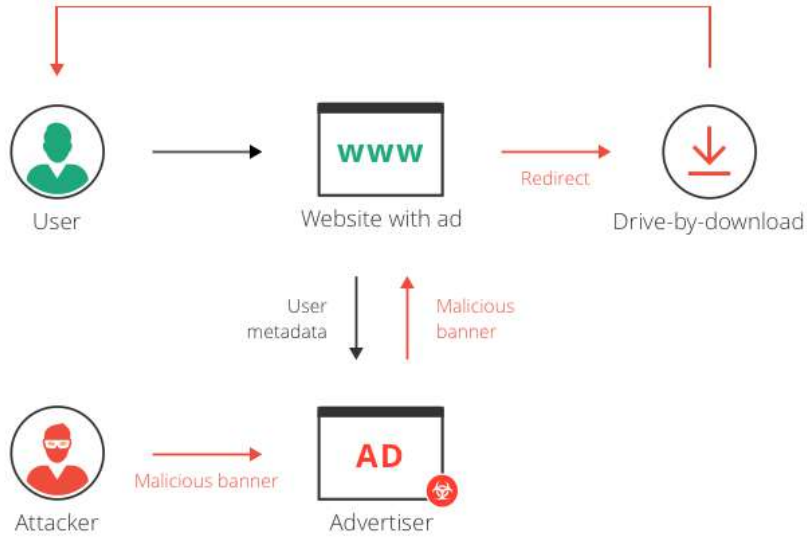
Malvertising



Malvertising (Malicious Advertising)

On-line advertising is actually 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.



The New York Times

London Stock Exchange

Spotify

The Atlantic

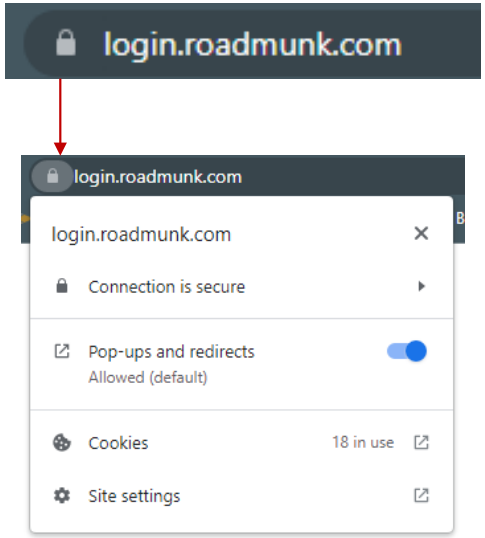
How to Protect Against Malvertising:

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

Payment Security & Compliance

The best practices for any digital organization that takes payments is to have a certified website that indicates a level of payment security and compliance to the user.

- SSL Security Certificate (Secure Sockets Layer) keeps an internet connection secure and helps to safeguard any sensitive data that is being sent between the two systems. This would be the connection between a congregant's browser on their mobile device to the application.
- HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by an SSL certificate. You can actually view the details by clicking on the lock symbol in a domain.
- See if they have a Better Business Bureau accreditation; this seal will also help to build confidence for your congregants.



It is helpful to make sure any checkout / payment confirmation process is clearly secure, and as a user they understand how their information will be safe. When reviewing applications, think about if you would feel safe submitting your information.

Leveraging a third-party payment vendor that is highly recognizable goes a long way in easing concerns.

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 that infects a network and can lock a system and block access, sometimes with threats to publish or delete personal data.

Bots are similar to worms, but are much more versatile and can be modified within hours of a new exploit publication.

Ransomware-As-A-Service

This takes the SaaS (Software-as-a-Service) operating model, and enables anyone willing to pay a subscription to use already-developed ransomeware. Typically, a percentage of each successful ransom payment is attributed back.

This has enabled even the most novel hackers to execute highly sophisticated attacks.

In the U.S. alone, ransomware attacks have increased by 139% year-over-year.

In Q3 of 2020, there were 145.2 million cases, accounting for 72.7% of global cases.

- ***Ensure you have up-to-date antivirus software on your devices.***
- ***Update your browsers.***

Social Engineering

This is when bad actors will use public or common information about you in order 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.

They will do this by trying to establish one of two key feelings:

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

Phishing Attacks

This is a form of social engineering in which the bad actor sends a fraudulent message that is designed to trick you into revealing sensitive information or load malicious software onto your device or infrastructure.

- Collect data – Passwords, Credit Card Numbers
- Click link to malicious website
- Opening file to download malicious software

This is a form of social engineering in which the bad actor sends a fraudulent message that is designed to trick you into revealing sensitive information or load malicious software onto your device or infrastructure.

Spear Phishing

Targets a specific organization or individual, leveraging, appearing to come from a well-known company or appearing to be someone withing an organization.

Whaling

Focuses on high-profile employees to encourage the performance of a secondary action, like adjusting of payroll or the transferring of funds.

Vishing / Smishing

The practice of sending voice or text messages pretending to be from reputable companies.

Impersonation

These are a techniques that manipulate victims into divulging their information. Bad actors work to build trust with the victim by establishing a credible story so that the victim isn't suspicious, tending to rely on impersonation, manipulation, and trust.

Pretexting

This approach goes after impersonating individuals in a position of power, leveraging feelings of urgency and fear to exploit victims.

- Auditors contacting IT staff to let them into the building.
- Executives contacting Human Resources to adjust their payroll distribution.
- CFO contacting Accounts Payable to distribute a payment to a vendor.
- Customers contacting Customer Service to redistribute pension payments to a new checking account.

Quid Pro Quo

This approach relies on psychological reciprocity – if someone gives us something or does us a favor, we feel obliged to return it.

- IT offers to fix our device to improve how it functions, but they need our log-in ID and password.
- A service agent can remove malware from our device, but they need to confirm our identity with a series of questions.
- HR will help us update our payroll information, but they need our Social Security Number, drivers license number.

Email Fraud Example


STATESCOOP

ODERNIZATION | EMERGING TECH | DATA & ANALYTICS | DIGITAL SERVICES | WATCH

CYBERSECURITY

Lexington, Ky., loses $4M in housing assistance to email scheme

AUG 29, 2022 | STATESCOOP

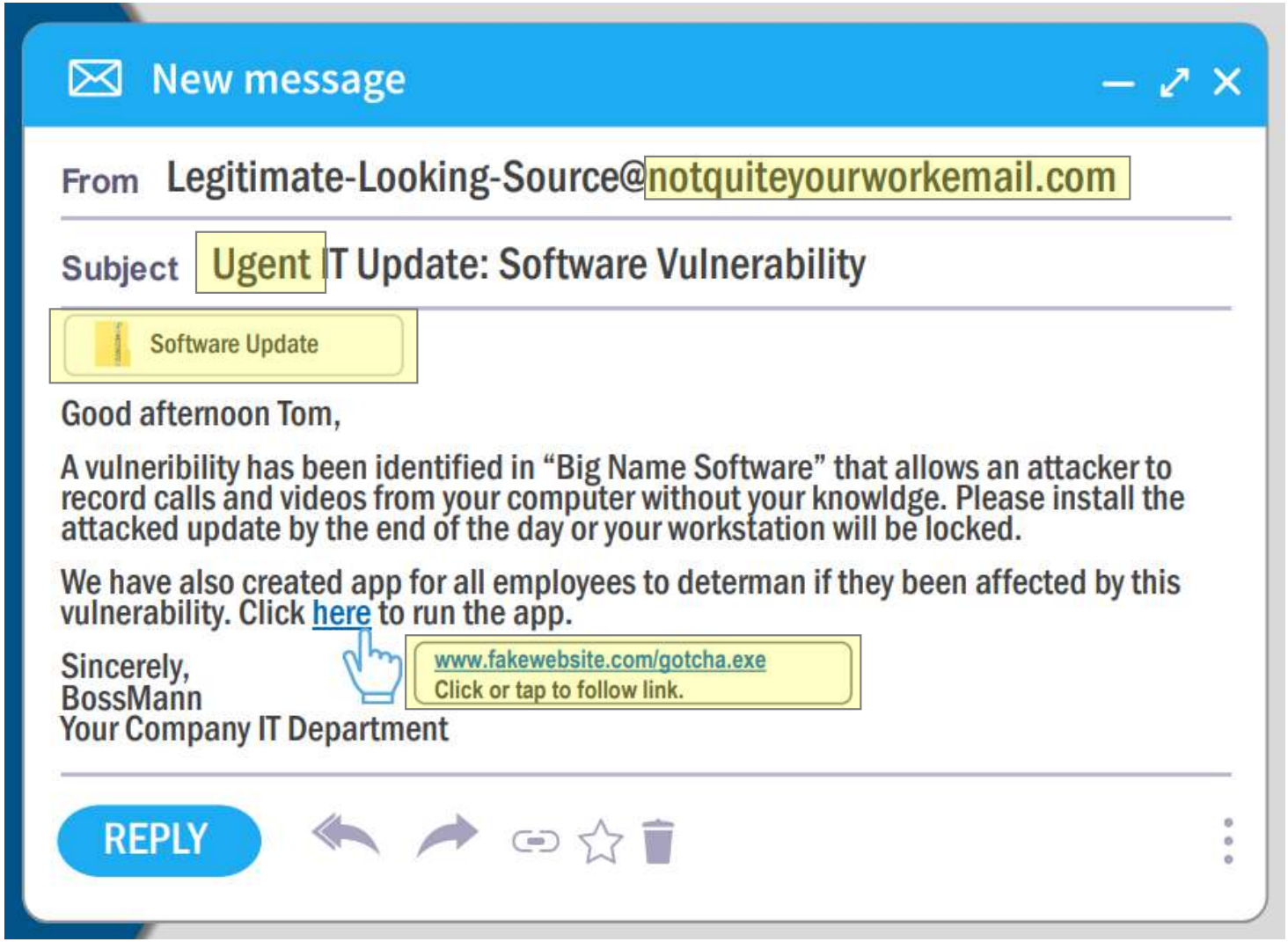
According to FBI Internet Crime Center:

BEC (Business Email Compromise) scams caused nearly *$2.4 billion* in losses in 2021.

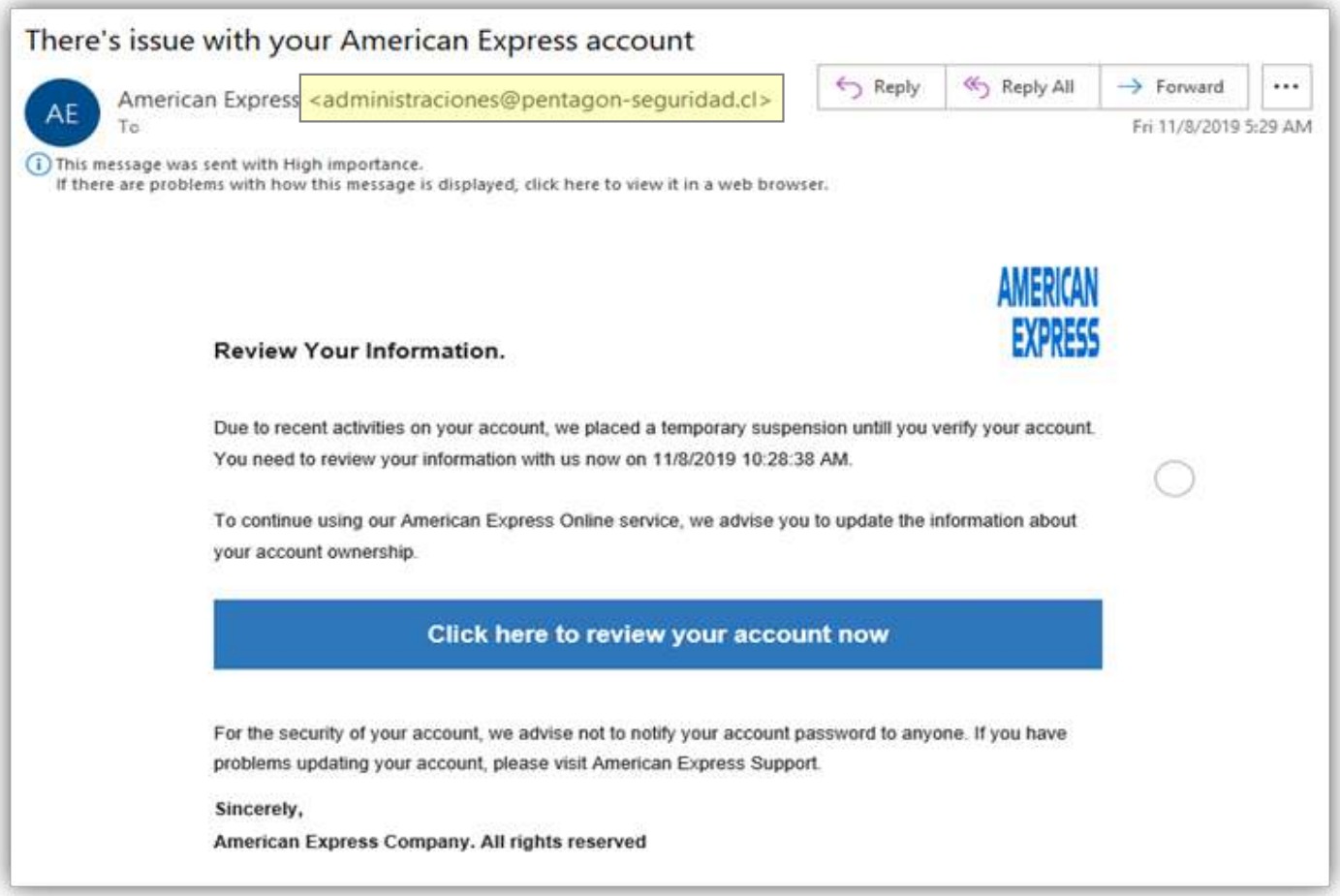
This is almost the same revenue as the Republic of Congo.

A malicious actor impersonated an email account of Community Action Council, a local housing group that works with the city. 3 wire transfers of funds for emergency rental assistance and transition housing were sent to a private bank account.

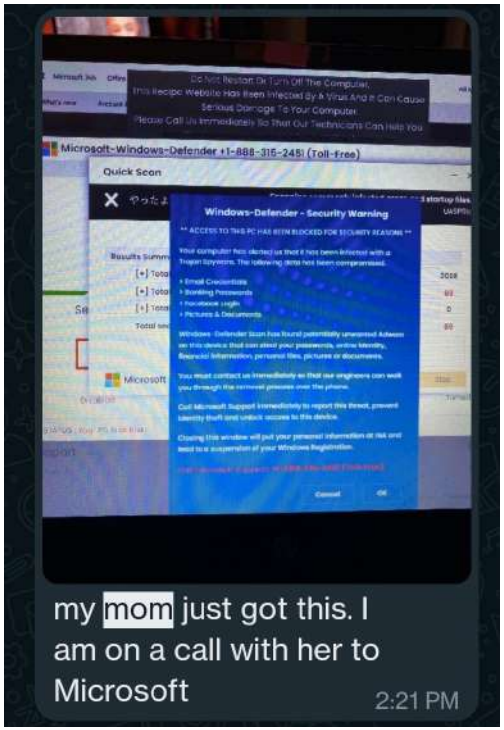
The Community Action Council notified that they never received the money. While this continues to be investigated, it appears that no one in municipal or CAC seems to be involved, and it was caught early enough that funds were frozen at the bank.

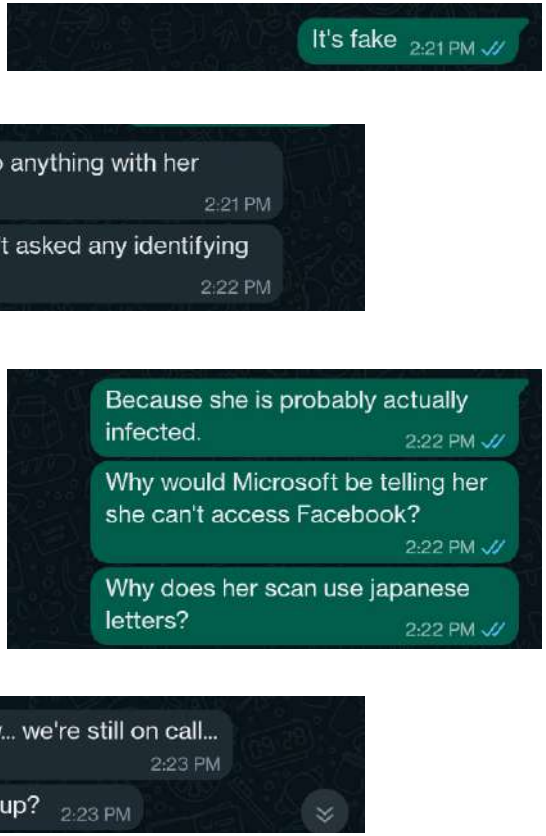

New message
From Legitimate-Looking-Source@notquiteyourworkemail.com
Subject Ugent IT Update: Software Vulnerability
Software Update
Good afternoon Tom,
A vulneribility has been identified in "Big Name Software" that allows an attacker to record calls and videos from your computer without your knowldge. Please install the attacked update by the end of the day or your workstation will be locked.
We have also created app for all employees to determan if they been affected by this vulnerability. Click here to run the app.
www.fakewebsite.com/gotcha.exe
Click or tap to follow link.
Sincerely,
BossMann
Your Company IT Department
REPLY

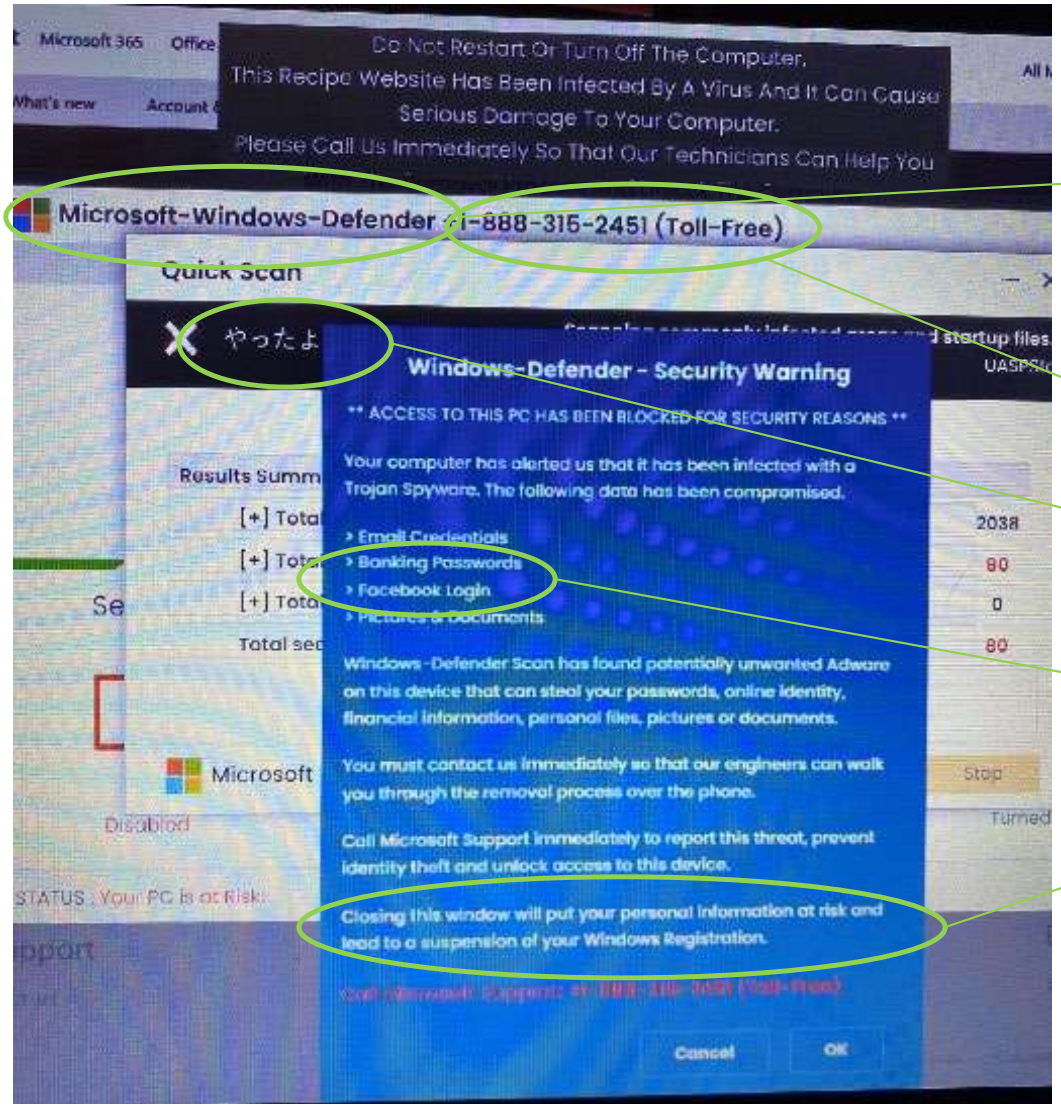

IRS
Claim Your Tax Refund Online
We identified an error in the calculation of your tax from the last payment, amounting to $ 419.95. In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.
Please click "Get Started" below to claim your refund:
Get Started
We are here to ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.


There's issue with your American Express account
AE
American Express <administraciones@pentagon-seguridad.cl>
To
Reply
Reply All
Forward
Fri 11/8/2019 5:29 AM
This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.
AMERICAN EXPRESS
Review Your Information.
Due to recent activities on your account, we placed a temporary suspension untill you verify your account.
You need to review your information with us now on 11/8/2019 10:28:38 AM.
To continue using our American Express Online service, we advise you to update the information about your account ownership.
Click here to review your account now
For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.
Sincerely,
American Express Company. All rights reserved

Real Life Incident During COVID







1. Old windows logo – this is the current one:

2. There is “Microsoft Defender”. The name “Windows Defender” actually is not used.

3. My mother-in-law did not have Microsoft Defender as a product on her laptop.

A quick Google of this phone number, and it is not linked to any Microsoft service number.

These are Japanese kana.

Microsoft does not store your banking passwords in a core application, and Facebook is a different company; these are trigger words to strike fear.

Microsoft is not going to suspend your registration for a breach on a personal device.

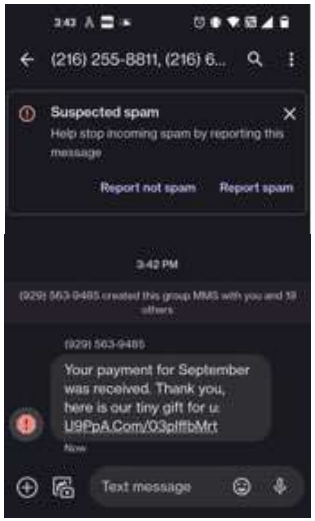
Other Things to be Aware Of

Additional Means of Attacking

Smishing & Social Media Scams

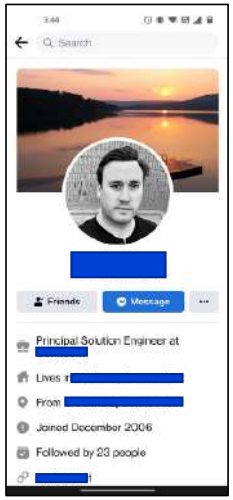
With new technology comes new ways of trying to get us to click a link to malware:

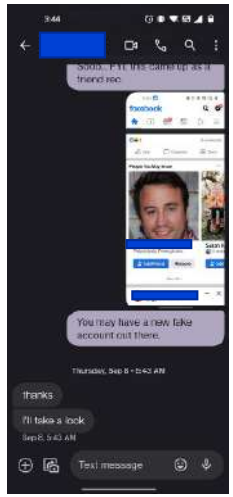
Smishing is “SMS Phising” – sending you text messages in order to try to influence you to click a link or give personal information.



Social Media

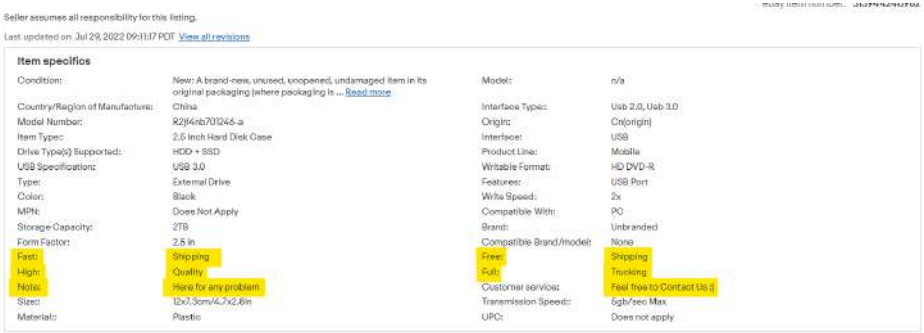
1. Pay close attention to who you are ACTUALLY messaging with. Bad actors will impersonate customer service and send you to sites with malware.
2. Be mindful of false accounts of friends, and of others creating one of you. This is a quick way to build trust.

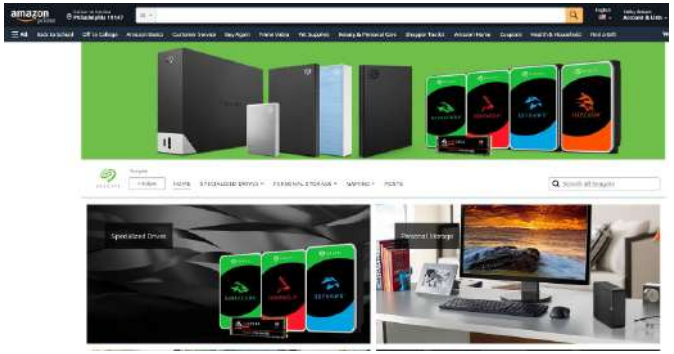




Baiting

Bad actors will make an attractive offer or promise to lure a victim into a trap.





USB “Thumb” Drives

USB Drives have been a convenient means of storing and sharing files between laptops for many years. Around 10-15 years, some companies began disabling USB ports from connecting to USB drives; now, that practice is generally universal for corporate devices.

Initially, the risk was data leakage, so USB ports were disabled to protect data.

Later, USB drives became a device to transfer malware or ransomware.

Alternatives to Using Thumb Drives

1. Secure Thumb Drives
2. Share File via Trusted Cloud Document Storage

https://www.cisa.gov/uscert/ncas/tips/ST08-001

Skimmers

A skimmer is a small device that a bad actor will place in front of a card scanner to copy and steal credit card information from you as you use your card.

When you insert your card, the machine is reading your information, but so is the skimmer.

This is often leveraged gas stations and ATMs. This has been a tactic in cities for a little bit but has spread to rural areas as well.

4 Things You Can Do To Protect Against Skimmers:

1. Use Chip Readers
2. Use Contactless Payment on Credit Card
3. Google Pay or Apple Pay
4. Go inside to pay

Google Pay

Pay

Credit Card Scanning

There is also noise around the technology these non-strip payments methods leverage. Here is some more about them:

RFID (Radio Frequency Identification)

- Concerns have been that a card reader in a pocket can pick up the RFID signal from your card to steal information.
- Transmits your account number and an encrypted one-time code.
- This does not send your name, billing address, or 3-digit security code needed for on-line transactions.
- Thief would need to be within inches of your card and need to crack bank's complex algorithm to create a new one-time code.

NFC (Near Field Communication)

Google Pay

Pay

- A version of RFID, works in very similar manner.
- Requires an additional authentication from user to verify identity on phone to enact payment.

If You Are Concerned:

1. Keep NFC turned off on your phone until you want to make a payment.
2. Purchase RFID blocking lifewear.

False QR Codes

One of the newest attack surfaces came about due to the COVID pandemic, as well – QR codes.

Restaurants, cafes, bars have moved away en masse from paper menus to digital menus that you pull up from scanning a QR code with your mobile phone.

Bad actors have started to put QR codes that link to malicious websites in order for unsuspecting users to scan them.

1. When out, make sure that a sticker has not been put over top of the menu QR code. Same with posters, ads, etc.
2. Don’t scan QR codes from unknown providers.

Collecting Offerings

Ensuring the Safety of Your Congregation & Building Confidence in Your Security

Leveraging Cloud Applications to Collect Offerings

We are in a great era where there are so many new technologies that can support our business processes. Instead of spending the time and energy to create something unique, leverage an existing system and adjust to its processes – this will save you time, money, and headache.

There are a number of platforms that are designed specifically for collecting offerings within a church:

Tithe.ly FellowshipOne planning center

Not only can they collect giving, but they have additional capabilities to support end to end church management. **This is not an endorsement, simply an example.**

If this level of technology is too much, there are other applications leveraged by the wider non-profit world to collect donations that could fit an easier need:

givelify DonorDrive

give lively donorbox

The key is to understand your business needs, find something that fits them the best, is price sensitive, and is secure. When thinking about the cost of the technology, also think about it will save work and reduce overhead costs and eliminate errors and/or risk.

Evaluating Vendor Security

In IT, we tend to rely on certain security certifications being completed by any vendor where we may store sensitive data. When selecting a vendor, make sure you know:

- What security certifications do they have? Are they willing to share them? (Requires an NDA – Non-Disclosure Agreement; ask for a mutual one to protect you, as well).

SOC 2 Type II Compliance - (System & Organization Controls) The American Institute of Certified Public Accountants that is used as standards during an audit. SOC 1 refers to financial reporting, a SOC 2 refers to security access controls. The “Type” refers to the depth of the report – a Type I ensures the proper controls exist, a Type II monitors to ensure the controls are actually followed.

ISO 27001 Certification – (International Organization for Standardization) ISO is a worldwide federation of national standards bodies for more than 160 countries. The 27001 standard is for cybersecurity.

CSA STAR – (Cloud Security Alliance) This is an assurance framework specifically focused on cloud service providers. This is based on meeting ISO 27001 Certification as well as meeting criteria in the Cloud Controls Matrix (CCM) by CSA.

OWASP ASVS – (Open Web Application Security Project Application Security Verification Standard) This is an application specific standard, where as the others look at the organization, its practices, and its controls as a whole.

Providing WiFi to Your Congregation

If you are going to use a cloud-based application to collect offerings from your congregants, you may think about providing a wifi network. Based the distance to wireless towers, the type of materials the church is built out of, your congregants may not have a good signal on their mobile devices – having a wifi network they can use should only help in additional offerings.

However, there are some things you should do in order to protect your network, and to protect your congregants as they use the network.

- **Set Up Separate Networks** – keep the network you manage finances limited to very few people, with complex password that is not given out; have a separate private network for laypeople if you need it, and a network for your congregation to access.
- **Use Different Passwords for Each Network** – Public networks are a risk for ANY device that is linked to it. Do not have a network without a password, even the network set up for your congregation. Do not use default passwords or SSID (Service Set Identifier).
- **Keep Firmware Up To Date** – This will help to minimize risk of a security vulnerability for those using network.
- **Use WPA2 Encryption on Wifi Network** – Wireless Protected Access 2 will help to encrypt data on network.
- **Set Up a Web Filtering Capability** – Will help block adware, spam, viruses, and spyware on wifi network.

Transparency, Consent, & Preferences

One of the keys to leveraging new technologies is to find a balance between protecting your congregants as they use technology within the church, while also ensuring it is a seamless digital experience. We need to meet them where they are, make them feel secure, and make the experience as seamless as possible.

People want data transparency: they want to know how will you use their data, with whom will you share this data and when.

This does not need to be overly complicated, but some things to think about establishing are:

- Privacy Policy – Disclose the types of information you will collect from users and why. Consider also specifically stating how you will not use the data. Describe the methods of collection and how users can limit the data they share, opt-out, or remove data.
- Security Statement – Articulate what you are doing to protect your congregant's sensitive data and other information during transactions on the website. This is a statement of commitment, not a specific list of technologies in use which may help at attacker.
- Consider capturing a consent of the user to store their data, and consider capturing preferences from them on how they wish to be communicated with.

Protecting the Church

Creating an Action Plan to Protect your Congregants, your Church, and Yourself

Key Areas of Focus for the Church

While there are a lot of threats out in the world, there are definitive actions that every organization – large or small – can take to protect themselves.

Assume it is not an “if” but a “when” that you will be a victim of a cyberattack, and have a plan:

- Take preventative measures to protect your congregants, your church, and yourself;
- Have cybersecurity insurance;
- Have a response plan;
- Train your employees and staff;
- Find a security advisor within your church leadership

Let’s rehash some of the protection methods we learned earlier to help secure your organization.

Creating Physical Security

1. Keep doors and windows locked.
2. Keep sensitive hard copy records locked away – filing cabinets with locks, safes, etc.
3. Minimize access privileges to areas with sensitive information.
4. Locking cables for assets that remain within the building.
5. Do not right down passwords, sensitive data and leave out in open space.
6. Do not leave devices out in plain sight – in cars, congregation areas, etc.
7. For secure areas, educate about tailgating and piggybacking – known people only.

Technology Security

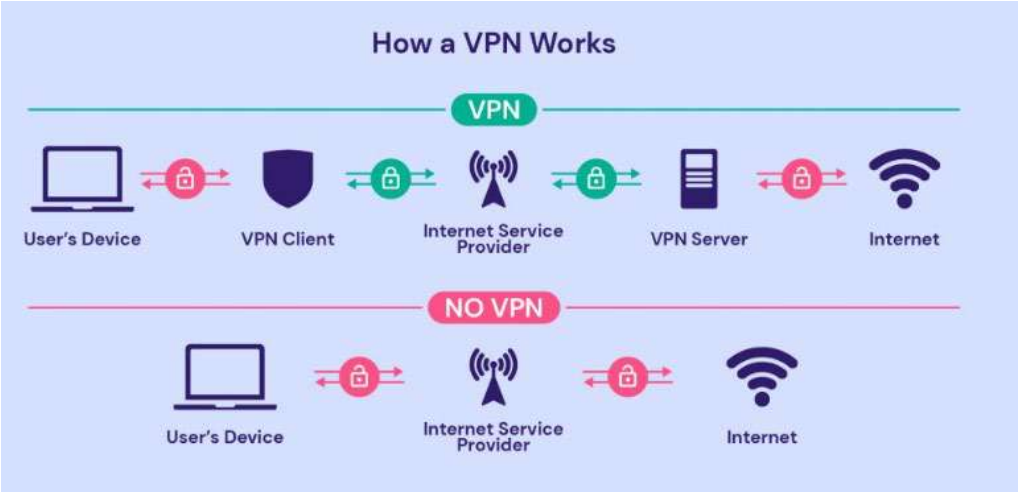
1. Keep Software, Browsers, Operating Systems Up-To-Date with Patches.
2. Set-up Time-out for Log-ins on Sensitive Applications.
3. Have unique accounts and passcodes for every employee.
4. Encrypt devices.
5. Ensure Website is Secure (HTTPS).
6. Ensure there is Next Gen Anti-Virus on devices running Church business.
7. Keep Software, Browsers, Operating Systems Up-To-Date with Patches (yes, a REPEAT).
8. Leverage a VPN (Virtual Private Network).
9. Leverage a Firewall and/or Web Filtering.
10. Have cloud based data-back-ups.
11. Use multi-factor authentication to Church assets (at least two-factor).
12. Work with a security advisor to evaluate your end-to-end.

VPN (Virtual Private Network)

A VPN will encrypt any data that is being transmitted over the internet when activated.

VPN technology has become readily available for individuals and small businesses in recent years. Here are some vendors to investigate:

NordVPN
Private Internet Access
Express VPN
Surfshark
CyberGhost



As an example, NordVPN is regularly $49.99 a year for a single device, $99.99 for up to 10 devices. This includes built in malware and ad blockers

Firewall

Slightly more complicated, you can also look into small local firewall equipment. This has started to become available in the last couple of years in supporting personal use and small businesses.

A firewall is a network security system that will monitor and control incoming and outgoing network traffic. In general, this is a barrier between your trusted network and an untrusted network like the internet.

Watchguard has tabletop “firebox” appliances. Equipment can cost just under $500, with annual subscription costs.

Firewalla has various options, from $200 to $500 with no subscription costs.

Content filtering
Monitor and control internet usage
Built-in VPN server and client
Ad blocker
Vulnerability Scan
Intrusion Detection

Cybersecurity Insurance

General liability policy will not cover losses in a cyberattack – this can be just as devastating as fire or theft.

When thinking about cybersecurity insurance, you have to think about both first and third party coverage:

- First pays for your losses;
- Third covers your constituents who may sue because of a data breach.

1. Regular back-ups stored in a secure, off-site location and are encrypted.
2. Limit remote access using two-factor authentication.
3. The number of PII records you are storing.
4. Provide anti-fraud training to employees.
5. Controls in place around requesting financial account details.
6. Required SPF (Sender Policy Framework) on incoming emails.
7. Endpoint protection (Next Gen Anti-Virus).

Staff Education

1. Reminder that the weakest link in the security equation.
2. This is one of the most important requirements for cybersecurity insurance.
3. Ensure annual confirmation of security policy.
4. Periodic training on phishing.
5. Consider security education tools like Ninjio.

Privacy & Security Policy

1. Password security of 15 characters, 4 types (Capital, Lower, Number, Unique).
2. Consider leveraging a password manager application.
3. Lock devices while not in use, shut down overnight.
4. Do not leave devices out in plain sight – in cars, congregation areas, etc.
5. Limit Use of Personal Devices for Church Business, as possible.
6. Limit Use of Church Devices for Personal Use, as possible.
7. Have a response plan – know what to do, who to contact, and how to quickly cut off further damage.

Consider conducing training or table-top exercises with employees and staff to help ensure everyone knows what to do in the event of an attack or a data breach.

Questions to Develop Privacy Guidelines

1. What categories of data are you collecting? (Names, contact information, biographical data, hobbies, health conditions, visual images, etc.)
2. What information should be off-limits? How can you ensure it stays that way?
3. How is personal information being collected? (Employee documents, guest and membership cards, website forms, social media analytics, event registrations, etc.)
4. Do you have the appropriate consent for each of the various collections? Do people have opt-in or opt-out options regarding data collection?
5. Is the data used appropriately? (A donor who submits information is not necessarily giving permission to use that information in a marketing campaign. A volunteer who submits information for a background check is not necessarily giving permission to receive text announcements.)
6. Does the church limit access to personal information? (The fewer people, the better.)
7. Is the information shared? If so, what is being shared with whom? (Consider prayer lists that are included on social media, in phone chains, in emails or text messages.)
8. How does the church protect personal data from being hacked, stolen, or misused? (Create strong, unique passwords. Keep software updated. Have sufficient firewalls and virus protection on all your computers.)
9. How will the church respond if someone requests a copy of all their personal information?
10. How will the church respond if there is a breach in security?
11. Is your data current? (To keep information relevant, periodically remove information on deceased members or those who now attend elsewhere.)
12. How will you dispose of unused/unnecessary data? (Deletions of electronic data can usually be recovered; rewriting cannot. Paper files with personal information should be burned or shredded.)

How to Protect Yourself

Additional Considerations in Daily Life

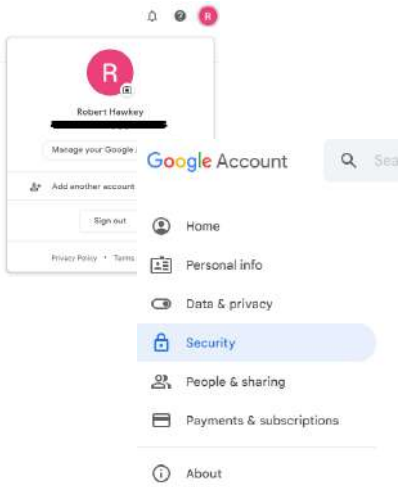
Protecting Your Mobile Device

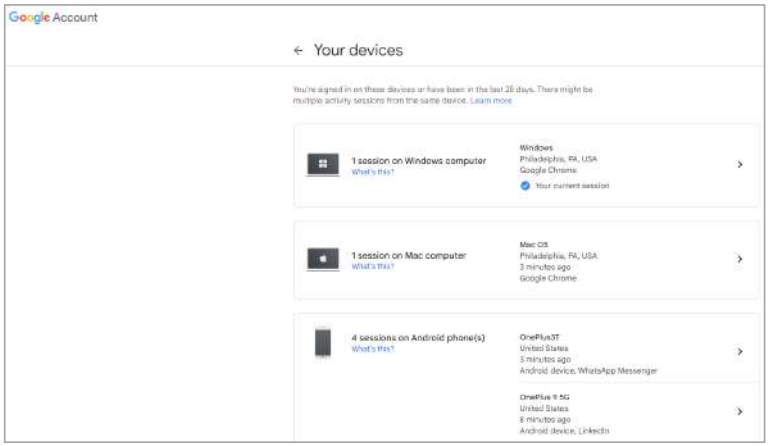
Some quick rules for protecting the one piece of technology you rely on the most…

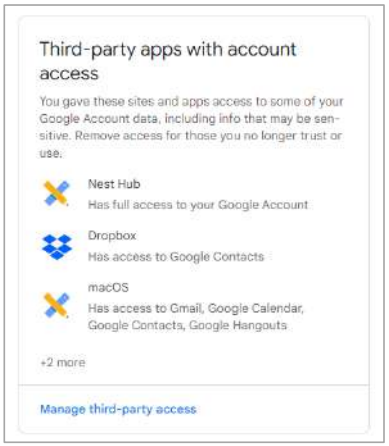
- Never leave your phone unattended.
- Change your phone's default passcode.
- Manage your Bluetooth security.
- Protect passcodes and credit card data – use a protected app for storage, or don't store at all.
- Keep up with software updates.
- Turn off autocomplete feature – prevents storage of critical personal data.
- Regularly delete browsing history, cookies, and cache.
- Use a security application.
- Manage your app permissions.
- Enable "Find My Device".
- Beware public charging stations.

Know How to Secure Your Accounts

Check what devices have access to your email accounts. Whether Apple or Google, make sure you know how to manage your account and settings.







Additional Tips for Personal Data Security

1. Think About Physical Security and Access to Data and Devices.
2. Pay Attention to Insecure Websites (HTTPS).
3. Lock down your social media accounts. Have a public and private account, if necessary.
4. Scrub old devices of data before recycling them – this isn't just about removing SIM card from phone.
5. Use password manager to manage all your passwords. Don't repeat passwords, or use simple or old passwords that may have been previously compromised. Random is best if you have a password manager.
6. Don't scan or print sensitive or personal data on a public printer.

Thank You!


Robert Hawkey
Digital Strategist, Business
Architect, CX Evangelist, Techn...

Ransomware in the Real World

Cryptolocker – early September 2013 to late May 2014

Originated in a .zip file attachment in an email, with an executable file that appeared as a PDF file.
This would encrypt files across local hard drives and mapped network drives, sending a message to the user of the encryption, demanding payment of $400 worth of Bitcoin.
After missing payment deadlines, the cost would continue to increase.
Traced movement is 41,928 Bitcoin between 10/15/13 and 12/18/13, equilvalent to $27 million at the time – this would be worth close to $1 billion in 2022.

Wannacry – May 2017

Targeted Microsoft Windows operating system by encrypting data and demanding ransom in Bitcoin. It was propagated through EternalBlue which was an exploit developed by the NSA – it was stolen and leaked by a different group a month earlier. Wannacry infiltrated organizations that had not applied patches to their Windows operating system.
The attack only lasted for just over 7 hours until a kill switch was discovered, but it infected 200,000 computers across 150 countries, causing an economic loss up to $4 billion.

NotPetya – June 27, 2017

A cybersecurity attack by Russia on Ukraine on Constitution Day, this infected the computer and triggered a reboot. Upon startup, the payload encrypts the master file table and displays a ransom message in Bitcoin. This also took advantage of EternalBlue. While this targeted Ukraine (80%), it proliferated based on global economy, taking down Merck for multiple weeks and many other companies.
Total estimated damages were estimated to be more than $10 billion.