Protecting You, Your Organization and Community from Cyber Threats

A SESSION ON CYBER SECURITY FOR 2022 AND BEYOND

BY TIM O'BRIEN

SIMPLIFIED BUSINESS SOLUTIONS
YOUR TECHNOLOGY SIMPLIFIED

What is an I.T. Managed Service Provider?

SIMPLIFIED BUSINESS SOLUTIONS
YOUR TECHNOLOGY SIMPLIFIED
Simplified Business Solutions
TEAM-SBS
We Protect Your Business with the Latest Cyber Security Tools -
So You Can Grow IT, Worry-Free

SBS provides the Winning Playbook for Centralized and Managed Software Solutions

Service Offerings

- Virtual CIO (IT Governance and Auditing)
- Cyber Security (Assessment, Response, Detection, Removal)
- Impactful Communication (Text, Email, Phone) from one Source
- Cloud Based Solutions including Back-up, Disaster Recovery, Email
- ADA Compliant WebSites and Hosting
- Project Management & I.T. Staffing
- Device Procurement & Optimization

Who We Protect

A Community Centric MSP (Managed Service Provider/Partner) for 25 businesses - most are Community-Based or Not for Profit)

City of Harper Woods

City of St Clair Shores

Port Huron Housing - including Community Centers (Dulhut & Ross)

A Beautiful Me & The Closet

Marysville Housing

Grace Episcopal Church

St Clair Housing

Battle Creek Housing

Ferndale Housing

Kitchen Tune-up

Eastpointe Housing

Luna Pier Housing

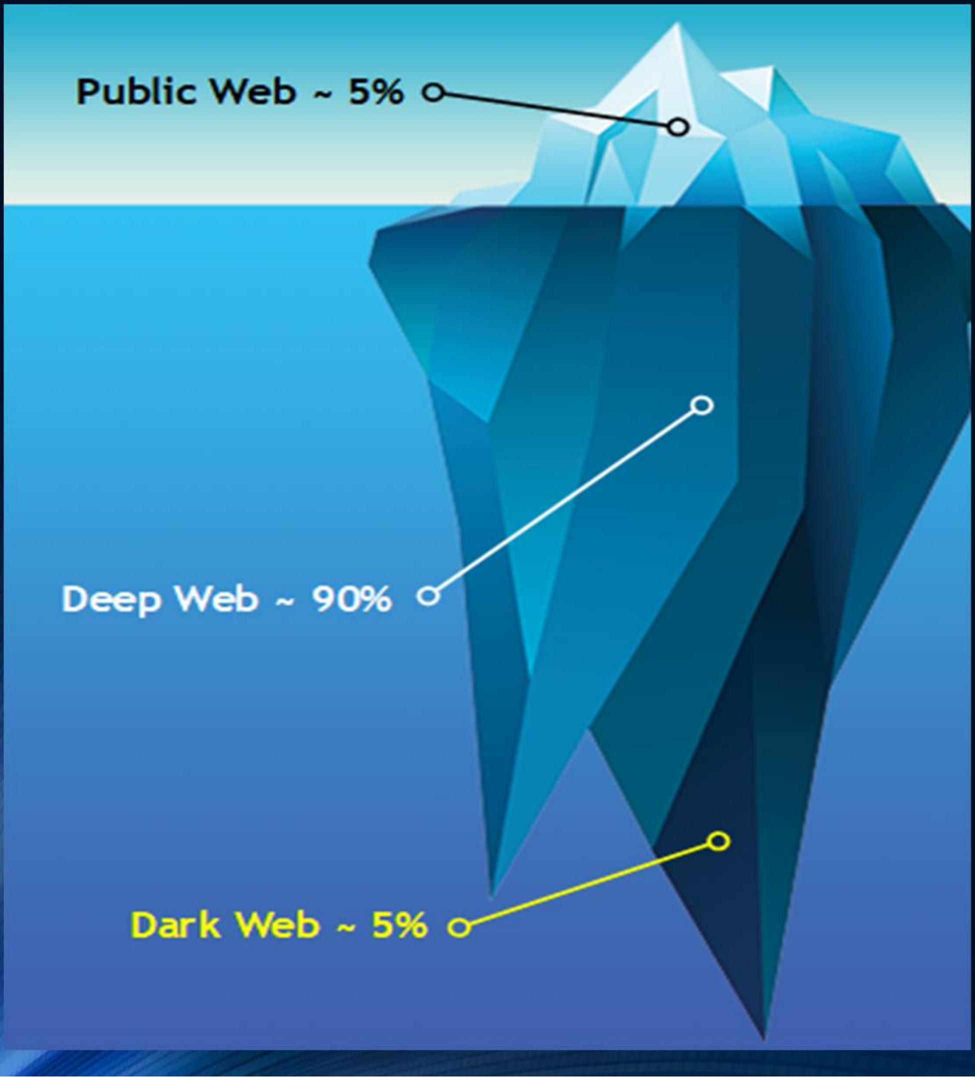
Lansing Housing

Port Huron Downtown Development Authority

Algonac Housing

Alma Housing

Approximately Only **1/3** of the Internet is Used for Good

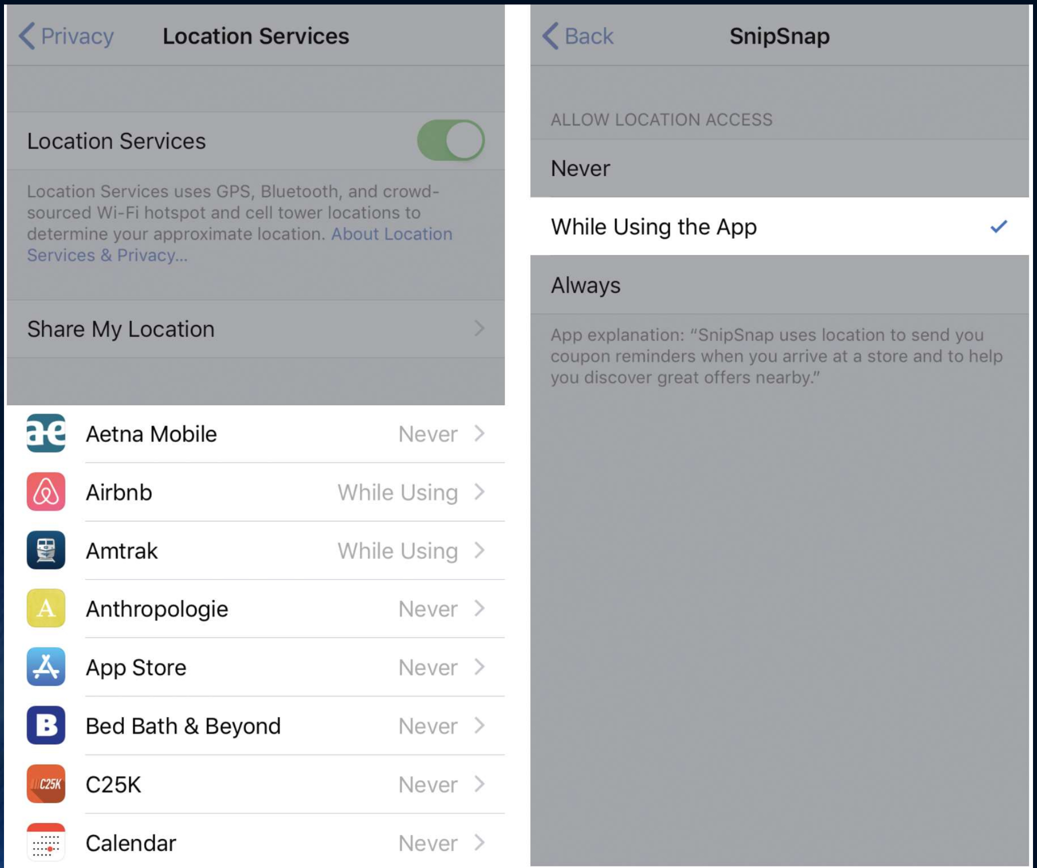


- Google, Pinterest, Facebook
- Online Banking, Venmo, Uber
- Research, Whistle Blowers
- TOR - Ransomware Affiliates
- Child Pornography, Human Trafficking

New Challenges with Privacy (IoT)

- Smart home/Wearables
- Artificial Intelligence
- Energy Management

Protecting Mobile Privacy



Location Services

Location Services ● On

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Share My Location

Aetna Mobile	Never
Airbnb	While Using
Amtrak	While Using
Anthropologie	Never
App Store	Never
Bed Bath & Beyond	Never
C25K	Never
Calendar	Never

SnipSnap

ALLOW LOCATION ACCESS

- Never
- While Using the App ✓
- Always

App explanation: "SnipSnap uses location to send you coupon reminders when you arrive at a store and to help you discover great offers nearby."

- Apple - https://www.foxnews.com/tech/how-to-stop-apple-and-google-from-tracking-you

- Google Android Device - https://support.google.com/android/answer/6179507

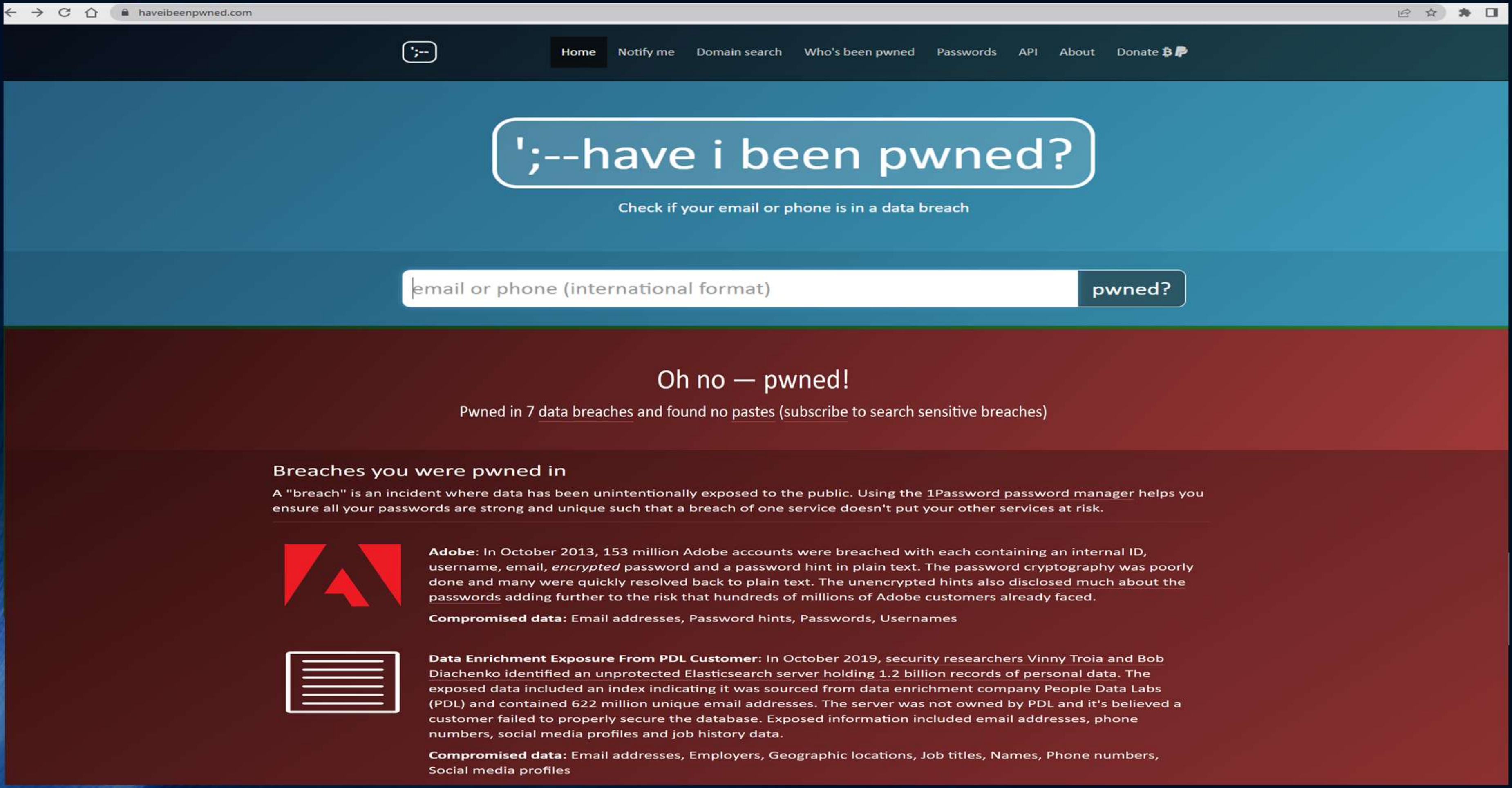
- Amazon Alexa - https://www.consumerreports.org/privacy/smart-speaker-privacy-settings/

Threats that Hit Home

- Cyber Bullying
- Social Influencers
- No Generational Boundaries

https://www.stopbullying.gov/

Have I Been Pwned?



';--have i been pwned?

Check if your email or phone is in a data breach

Oh no — pwned!

Pwned in 7 data breaches and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

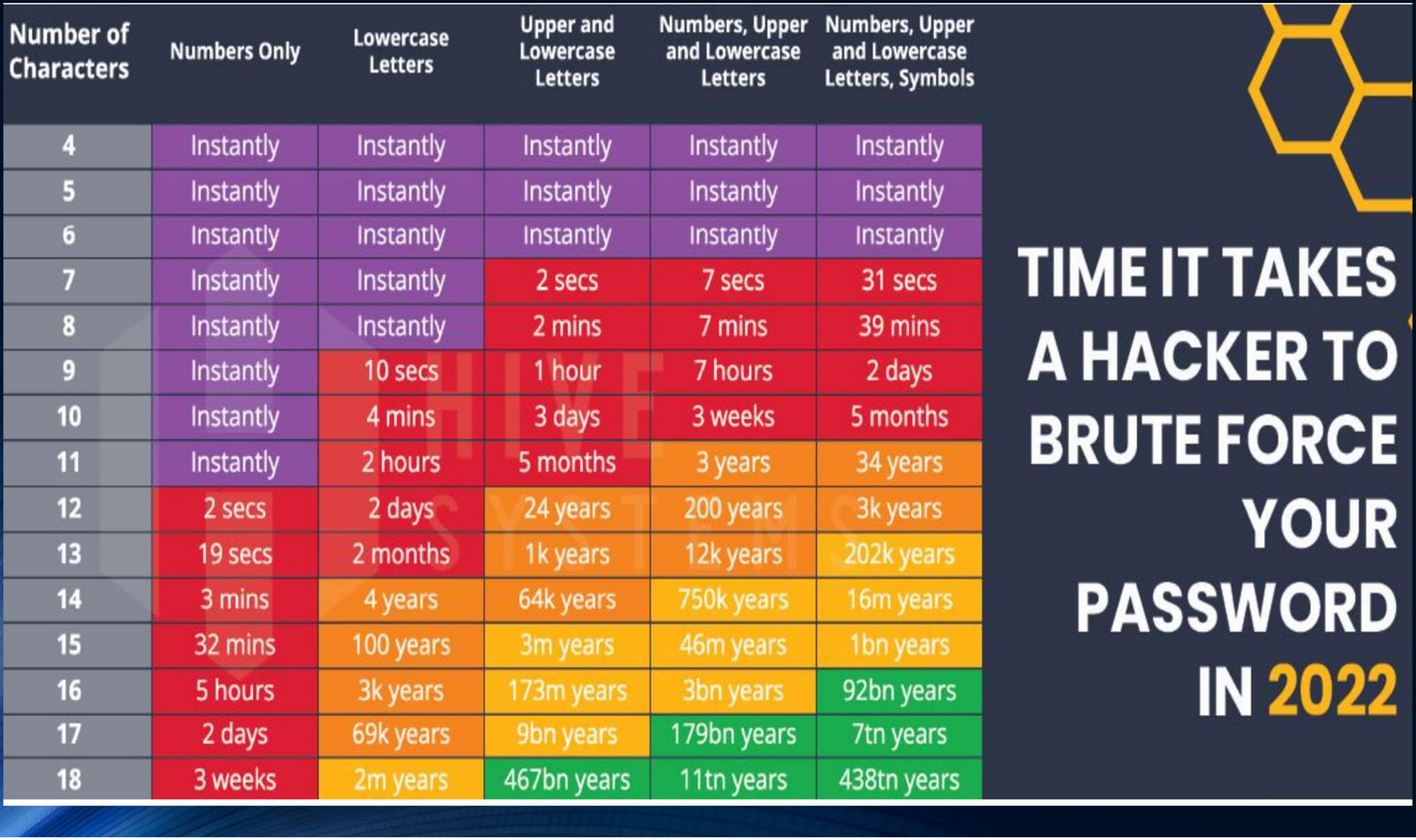
Compromised data: Email addresses, Password hints, Passwords, Usernames

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

https://haveibeenpwned.com

Tips to Protecting Your Confidentiality

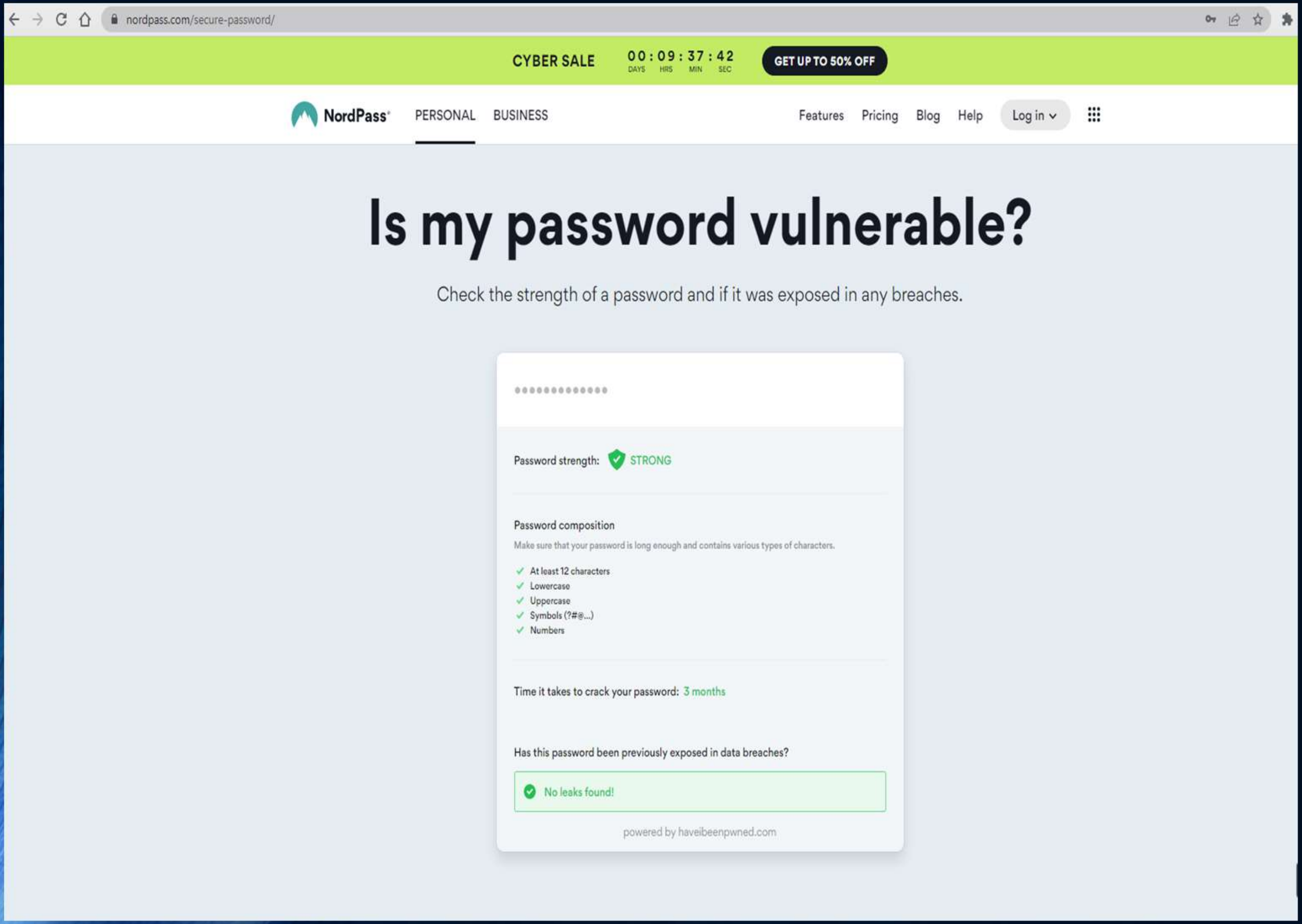


TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

How Strong Are your Passwords?



Is my password vulnerable?

Check the strength of a password and if it was exposed in any breaches.

•••••••••••••

Password strength: ✓ STRONG

Password composition

Make sure that your password is long enough and contains various types of characters.

- ✓ At least 12 characters
- ✓ Lowercase
- ✓ Uppercase
- ✓ Symbols (?#@...)
- ✓ Numbers

Time it takes to crack your password: 3 months

Has this password been previously exposed in data breaches?

✓ No leaks found!

powered by haveibeenpwned.com

https://nordpass.com/secure-password

The Don'ts -

- Reuse passwords
- Common keyword patterns
- Common names

Protecting Personal Privacy

❑Utilize Strong passphrases

❑VPN Software

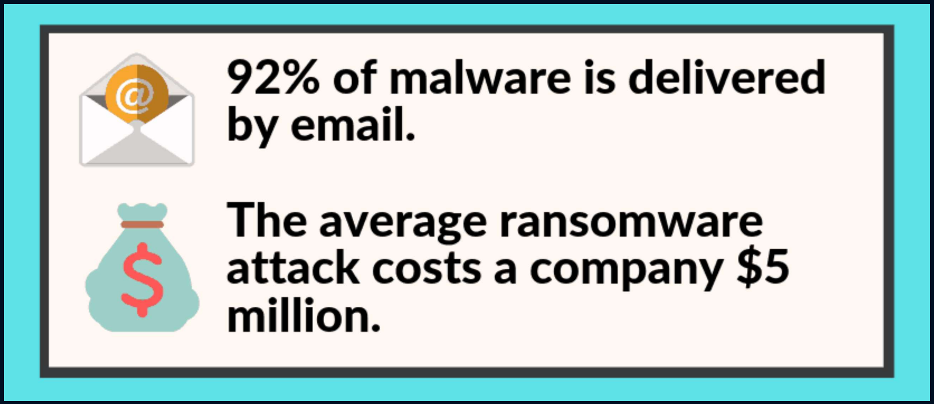
❑Reputable Anti-virus

❑Two-factor Authentication

❑Incognito/Private Browsing

❑Separate Email/Ccard for Online Banking

Threats that Lurk in the Deep – Go Phish



92% of malware is delivered by email.

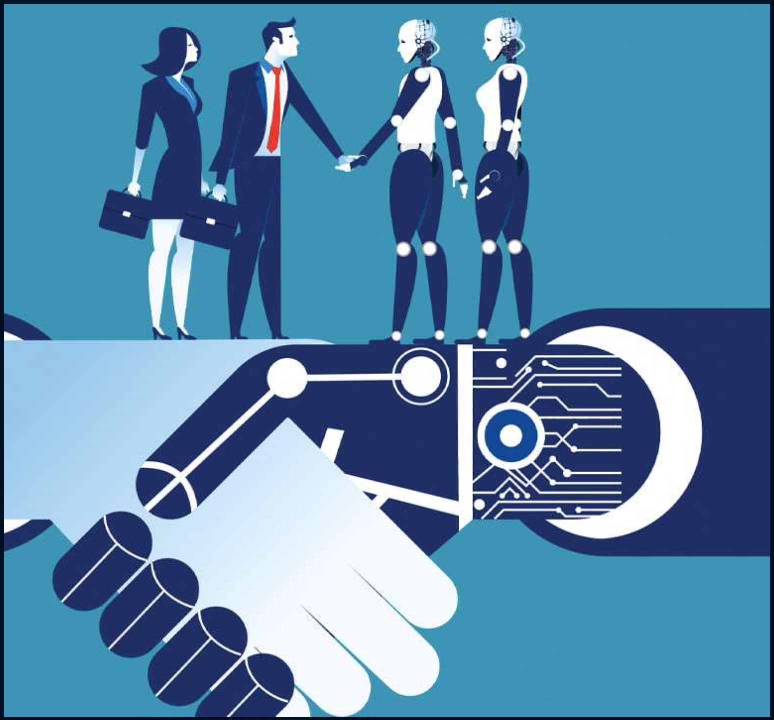
The average ransomware attack costs a company $5 million.

- Spoofing
- Phishing
- Advanced Ransomware is expected to encrypt a new business every 11 seconds and Cost Business’ upwards of $40 Billion in 2022…

https://blog.knowbe4.com/

Keeping your Business Safe

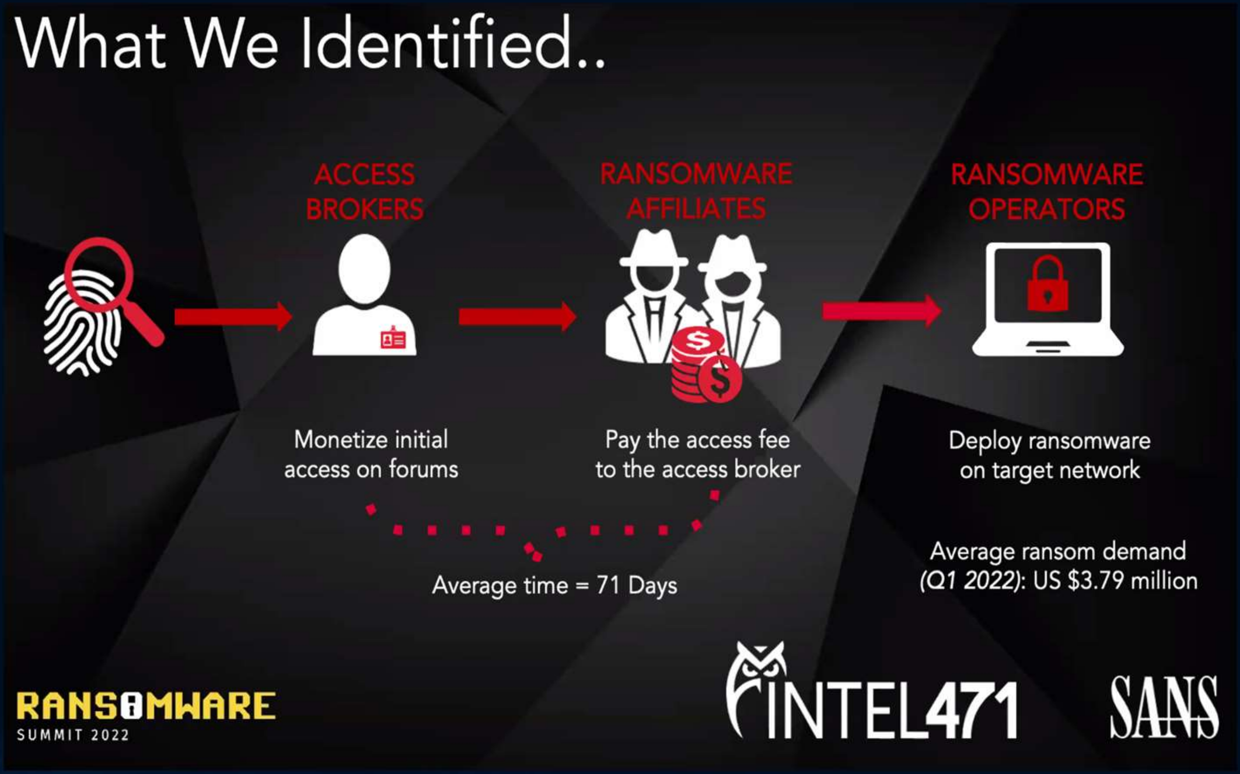
- ❑Always Verify the Source
- ❑Awareness Training
- ❑Phishing Simulations
- ❑Security Liaison Role



Advanced Threats
Ransomware in the Underground Marketplace

What can happen……

- Stolen Credentials
- Compromised Data
- Ransom
- Double/Triple Extortion



What We Identified..

ACCESS BROKERS

Monetize initial access on forums

RANSOMWARE AFFILIATES

Pay the access fee to the access broker

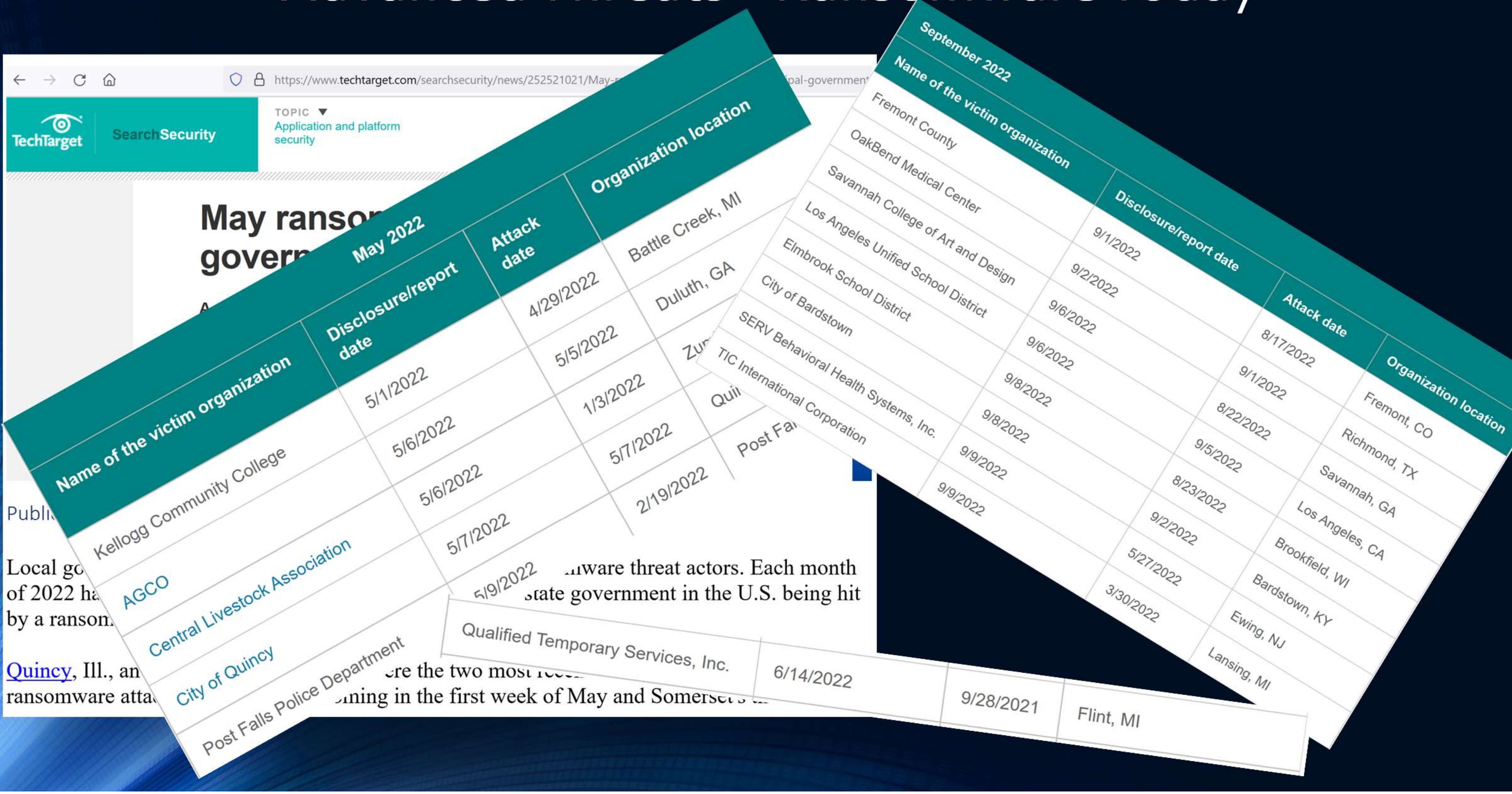
RANSOMWARE OPERATORS

Deploy ransomware on target network

Average time = 71 Days

Average ransom demand *(Q1 2022)*: US $3.79 million

Advanced Threats - Ransomware Today



https://www.techtarget.com/searchsecurity/news/252521021/May-r
ipal-government
TechTarget
SearchSecurity
TOPIC ▼
Application and platform security

May ranso
govern

A

Publi

Local go ...ware threat actors. Each month
of 2022 ha... state government in the U.S. being hit
by a ransom...

Quincy, Ill., an... ...ere the two most rece...
ransomware atta... ...ning in the first week of May and Somerset's ...

May 2022			
Name of the victim organization	Disclosure/report date	Attack date	Organization location
Kellogg Community College	5/1/2022	4/29/2022	Battle Creek, MI
AGCO	5/6/2022	5/5/2022	Duluth, GA
Central Livestock Association	5/6/2022	1/3/2022	Zu
City of Quincy	5/7/2022	5/7/2022	Qui
Post Falls Police Department	5/9/2022	2/19/2022	Post Fa

Qualified Temporary Services, Inc.	6/14/2022	9/28/2021	Flint, MI

September 2022			
Name of the victim organization	Disclosure/report date	Attack date	Organization location
Fremont County	9/1/2022	8/17/2022	Fremont, CO
OakBend Medical Center	9/2/2022	9/1/2022	Richmond, TX
Savannah College of Art and Design	9/6/2022	8/22/2022	Savannah, GA
Los Angeles Unified School District	9/6/2022	9/5/2022	Los Angeles, CA
Elmbrook School District	9/8/2022	8/23/2022	Brookfield, WI
City of Bardstown	9/8/2022	9/2/2022	Bardstown, KY
SERV Behavioral Health Systems, Inc.	9/9/2022	5/27/2022	Ewing, NJ
TIC International Corporation	9/9/2022	3/30/2022	Lansing, MI

Layering Your Security Stack

- ❑Assessment
- ❑Purchase a Business Class Firewall
- ❑VPN/DNS Filtering Software
- ❑Centralized and Advanced Antivirus
- ❑Two-factor Authentication
- ❑Simulated Training

Bonus Items

- ❑ Kiosk Security Approach
- ❑ Recycle Copier Hard Drive

Layering Your Security- Continued

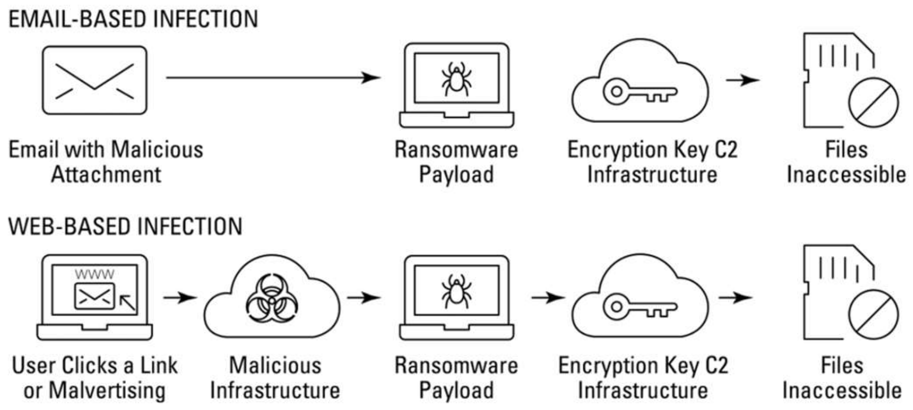


FIGURE 1-2: How ransomware works.

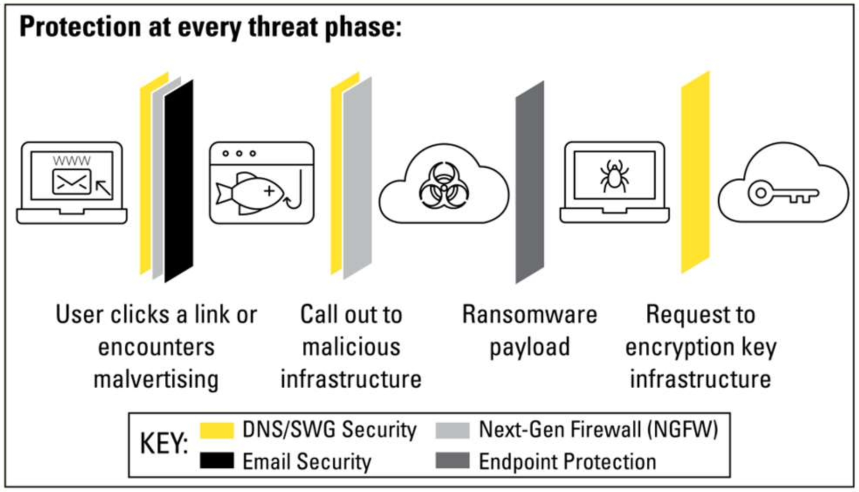

Protection at every threat phase:
WWW
User clicks a link or encounters malvertising
Call out to malicious infrastructure
Ransomware payload
Request to encryption key infrastructure
KEY:
DNS/SWG Security
Next-Gen Firewall (NGFW)
Email Security
Endpoint Protection

FIGURE 3-2: The new best-of-breed security architecture provides the best threat surface coverage possible with defense in depth.

Multiple Layered Approach is needed to help Mitigate Threats

How Do You Stack Up?

michigan municipal league

We love where you live.

□ Ensure systems are up to date and patched regularly

□ Fix any known exploits hardware/software and review common authority guidelines frequently (CISA Catalog, NIST, RSA, OFAQ, DFIR Report)

□ Implement a comprehensive password policy

□ Implement Multi-factor authentication

□ Utilize encryption techniques to safeguard data (Backups, Email)

□ Make sure unnecessary Internet facing Ports and Protocols are deactivated to prevent DDoS and other Cyber Attacks

□ Setup Performance Alerts and Reporting of any unexpected/unusual network activity via monitor Security Operations Center (SOC)

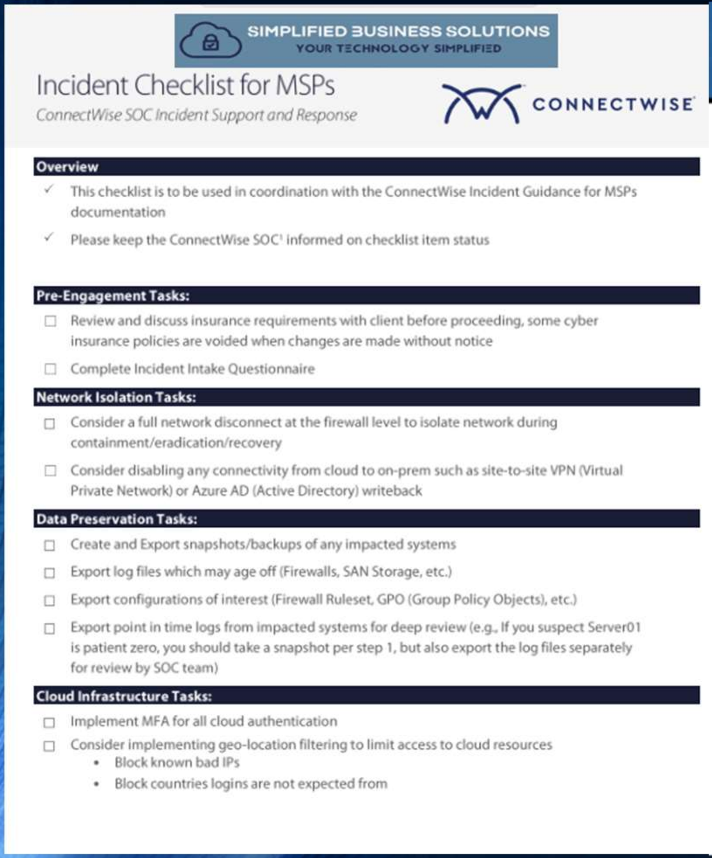
□ Install up-to-date antivirus software. Add advanced EDR to Stack.

□ Provide Awareness Training- Training to prepare staff for phishing, & ransomware attacks including testing

Tools for Your Arsenal

NEVER ASSUME you Are Protected!

Detection and Response Checklists



SIMPLIFIED BUSINESS SOLUTIONS
YOUR TECHNOLOGY SIMPLIFIED

Incident Checklist for MSPs

ConnectWise SOC Incident Support and Response

CONNECTWISE

Overview

- ✓ This checklist is to be used in coordination with the ConnectWise Incident Guidance for MSPs documentation
- ✓ Please keep the ConnectWise SOC[1] informed on checklist item status

Pre-Engagement Tasks:

- ☐ Review and discuss insurance requirements with client before proceeding, some cyber insurance policies are voided when changes are made without notice
- ☐ Complete Incident Intake Questionnaire

Network Isolation Tasks:

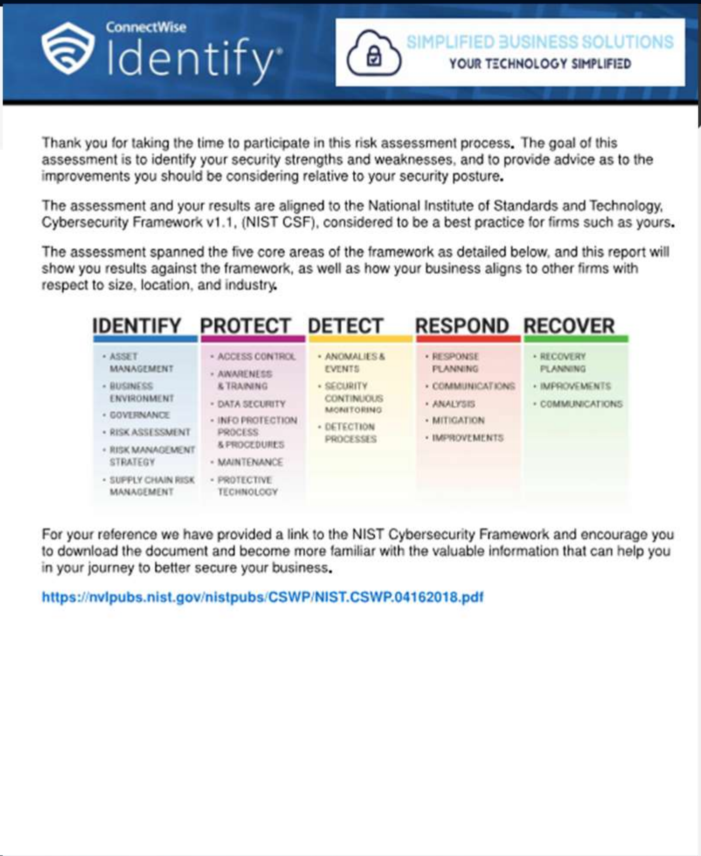
- ☐ Consider a full network disconnect at the firewall level to isolate network during containment/eradication/recovery
- ☐ Consider disabling any connectivity from cloud to on-prem such as site-to-site VPN (Virtual Private Network) or Azure AD (Active Directory) writeback

Data Preservation Tasks:

- ☐ Create and Export snapshots/backups of any impacted systems
- ☐ Export log files which may age off (Firewalls, SAN Storage, etc.)
- ☐ Export configurations of interest (Firewall Ruleset, GPO (Group Policy Objects), etc.)
- ☐ Export point in time logs from impacted systems for deep review (e.g., If you suspect Server01 is patient zero, you should take a snapshot per step 1, but also export the log files separately for review by SOC team)

Cloud Infrastructure Tasks:

- ☐ Implement MFA for all cloud authentication
- ☐ Consider implementing geo-location filtering to limit access to cloud resources
  - Block known bad IPs
  - Block countries logins are not expected from



ConnectWise Identify

SIMPLIFIED BUSINESS SOLUTIONS
YOUR TECHNOLOGY SIMPLIFIED

Thank you for taking the time to participate in this risk assessment process. The goal of this assessment is to identify your security strengths and weaknesses, and to provide advice as to the improvements you should be considering relative to your security posture.

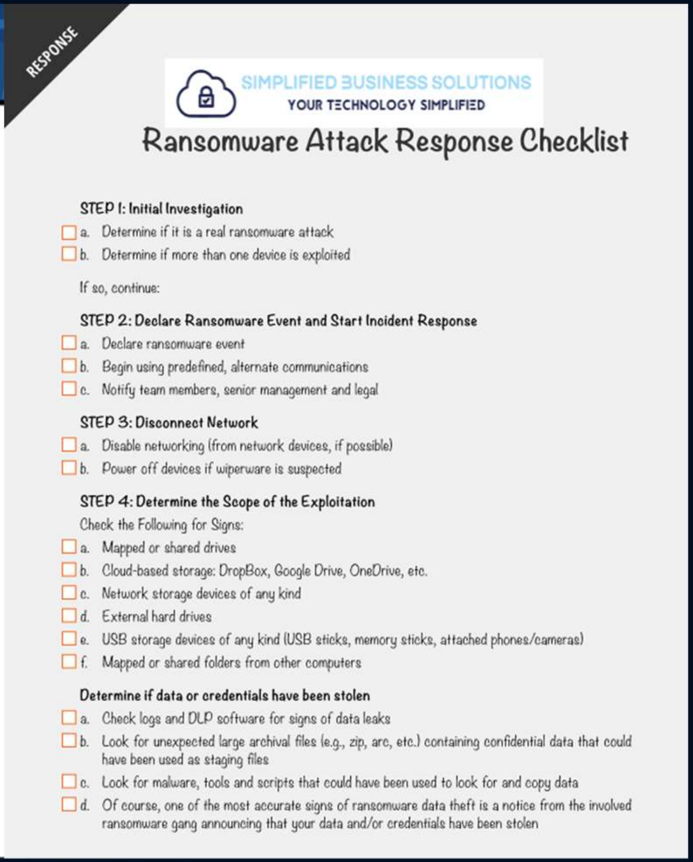
The assessment and your results are aligned to the National Institute of Standards and Technology, Cybersecurity Framework v1.1, (NIST CSF), considered to be a best practice for firms such as yours.

The assessment spanned the five core areas of the framework as detailed below, and this report will show you results against the framework, as well as how your business aligns to other firms with respect to size, location, and industry.

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• ASSET MANAGEMENT • BUSINESS ENVIRONMENT • GOVERNANCE • RISK ASSESSMENT • RISK MANAGEMENT STRATEGY • SUPPLY CHAIN RISK MANAGEMENT	• ACCESS CONTROL • AWARENESS & TRAINING • DATA SECURITY • INFO PROTECTION PROCESS & PROCEDURES • MAINTENANCE • PROTECTIVE TECHNOLOGY	• ANOMALIES & EVENTS • SECURITY CONTINUOUS MONITORING • DETECTION PROCESSES	• RESPONSE PLANNING • COMMUNICATIONS • ANALYSIS • MITIGATION • IMPROVEMENTS	• RECOVERY PLANNING • IMPROVEMENTS • COMMUNICATIONS

For your reference we have provided a link to the NIST Cybersecurity Framework and encourage you to download the document and become more familiar with the valuable information that can help you in your journey to better secure your business.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf



RESPONSE

SIMPLIFIED BUSINESS SOLUTIONS
YOUR TECHNOLOGY SIMPLIFIED

Ransomware Attack Response Checklist

STEP 1: Initial Investigation

- ☐ a. Determine if it is a real ransomware attack
- ☐ b. Determine if more than one device is exploited

If so, continue:

STEP 2: Declare Ransomware Event and Start Incident Response

- ☐ a. Declare ransomware event
- ☐ b. Begin using predefined, alternate communications
- ☐ c. Notify team members, senior management and legal

STEP 3: Disconnect Network

- ☐ a. Disable networking (from network devices, if possible)
- ☐ b. Power off devices if wiperware is suspected

STEP 4: Determine the Scope of the Exploitation

Check the Following for Signs:

- ☐ a. Mapped or shared drives
- ☐ b. Cloud-based storage: DropBox, Google Drive, OneDrive, etc.
- ☐ c. Network storage devices of any kind
- ☐ d. External hard drives
- ☐ e. USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- ☐ f. Mapped or shared folders from other computers

Determine if data or credentials have been stolen

- ☐ a. Check logs and DLP software for signs of data leaks
- ☐ b. Look for unexpected large archival files (e.g., zip, arc, etc.) containing confidential data that could have been used as staging files
- ☐ c. Look for malware, tools and scripts that could have been used to look for and copy data
- ☐ d. Of course, one of the most accurate signs of ransomware data theft is a notice from the involved ransomware gang announcing that your data and/or credentials have been stolen

Where to Start? Assume Nothing!

❑ *Partner* with the right *Technology Provider* to help Assess all things I.T.

❑ Base decisions on business need and budget, not hype or scare tactics

SIMPLIFIED BUSINESS SOLUTIONS
YOUR TECHNOLOGY SIMPLIFIED

Questions?

About Your Technology Team

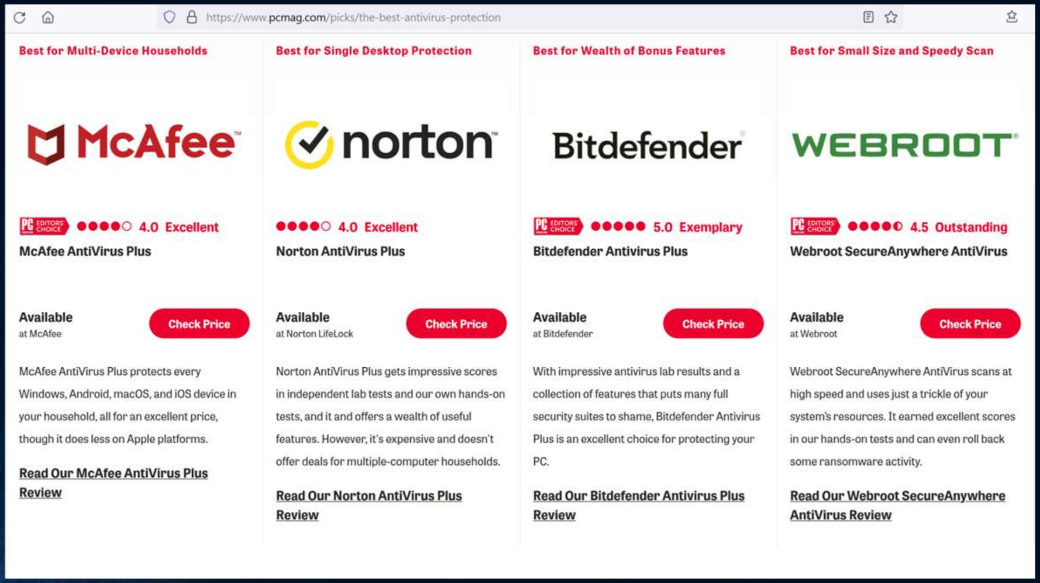
Team-SBS
Achieve business goals previously un-imagined. Our technology services will help you get I.T. done!

Founder and CIO of Simplified Business Solutions, LLC (SBS), Tim O’Brien is a Technology Specialist, holding over 25 years of experience with a unique focus on people.

Excellent customer service is how business is handled. SBS can create and manage a multitude of technological environments for any sized business, and focuses on the following industries – non-profit, local government, housing authorities, medical, financial, and automotive.

Having been in the consulting business for over 10 years, Tim saw an opportunity to provide technology support a different way. As a direct result from feedback from previously supported clients, Simplified Business Solutions, LLC was founded in the fall of 2017. SBS is redefining this thing we call "Service". We want to give the personal type of service that seems to be a lost art these days. You want to know you can call someone and get a caring human on the line, not an email ticket system or phone answering service. We have your answer…

How We Do I.T.?



https://www.pcmag.com/picks/the-best-antivirus-protection

Best for Multi-Device Households

McAfee

EDITORS' CHOICE ●●●●○ 4.0 Excellent

McAfee AntiVirus Plus

Available at McAfee — Check Price

McAfee AntiVirus Plus protects every Windows, Android, macOS, and iOS device in your household, all for an excellent price, though it does less on Apple platforms.

Read Our McAfee AntiVirus Plus Review

Best for Single Desktop Protection

norton

●●●●○ 4.0 Excellent

Norton AntiVirus Plus

Available at Norton LifeLock — Check Price

Norton AntiVirus Plus gets impressive scores in independent lab tests and our own hands-on tests, and it and offers a wealth of useful features. However, it's expensive and doesn't offer deals for multiple-computer households.

Read Our Norton AntiVirus Plus Review

Best for Wealth of Bonus Features

Bitdefender

EDITORS' CHOICE ●●●●● 5.0 Exemplary

Bitdefender Antivirus Plus

Available at Bitdefender — Check Price

With impressive antivirus lab results and a collection of features that puts many full security suites to shame, Bitdefender Antivirus Plus is an excellent choice for protecting your PC.

Read Our Bitdefender Antivirus Plus Review

Best for Small Size and Speedy Scan

WEBROOT

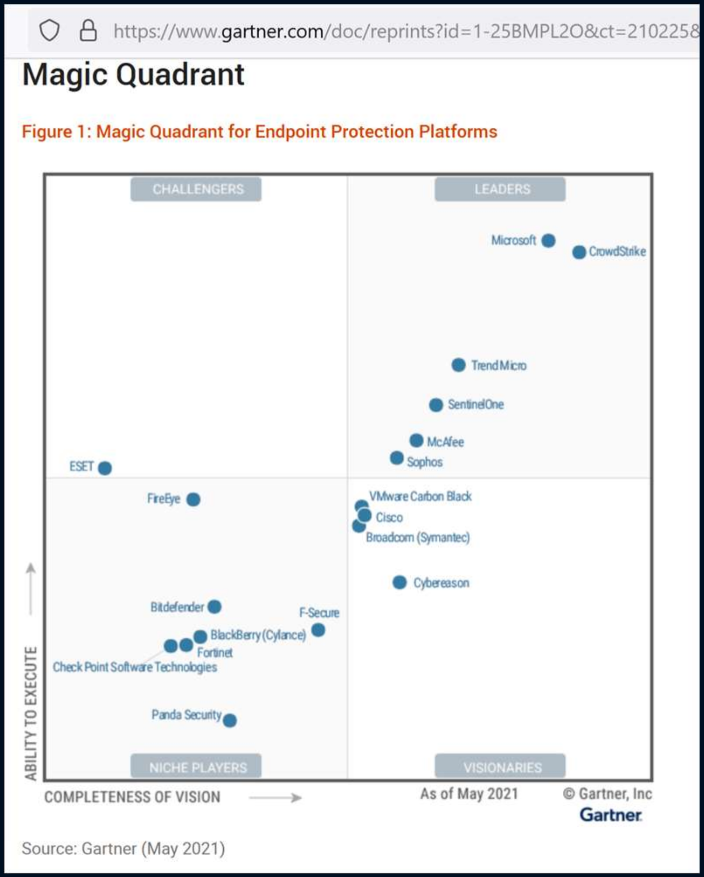
EDITORS' CHOICE ●●●●◐ 4.5 Outstanding

Webroot SecureAnywhere AntiVirus

Available at Webroot — Check Price

Webroot SecureAnywhere AntiVirus scans at high speed and uses just a trickle of your system's resources. It earned excellent scores in our hands-on tests and can even roll back some ransomware activity.

Read Our Webroot SecureAnywhere AntiVirus Review



https://www.gartner.com/doc/reprints?id=1-25BMPL2O&ct=210225&

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (May 2021)

Best in Class Software

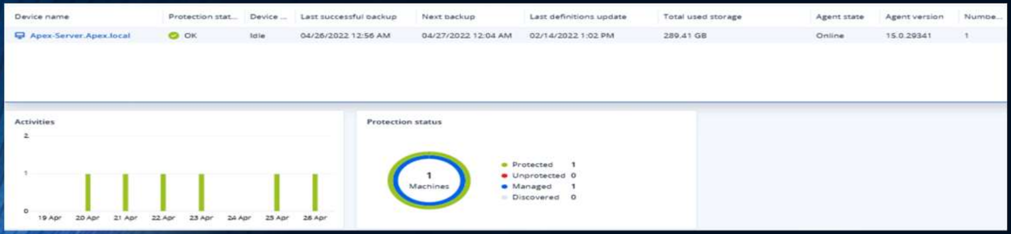
- Webroot SecureAnywhere is Editors Choice
- SentinelOne is top Advanced EDR Solution (4th of 18)
  Endpoint Detection and Response Software with advanced AI hunting and heuristics learning

What We Do - I.T.

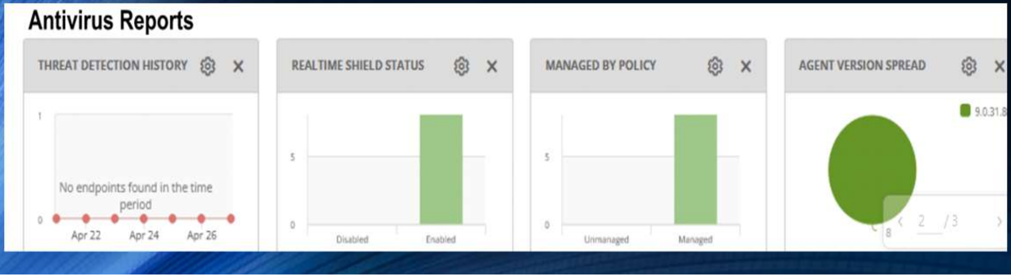
We Provide Advanced Monitored and Assessment Software Solutions

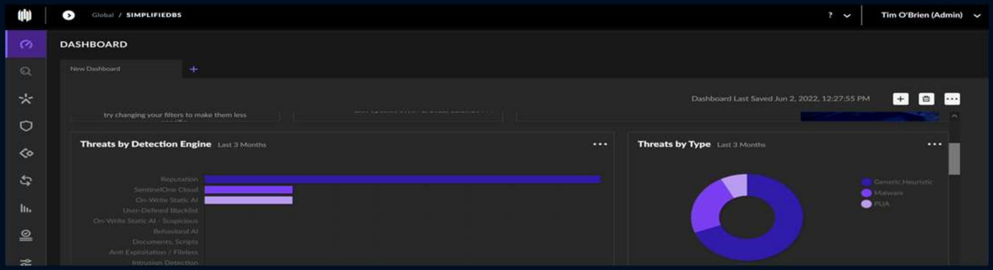
These include Best in Class -

- ✓ Monitored Endpoint Devices and Software (like Servers, PCs, Switches, Routers, SQL, Virus/Malware/Ransomware, DDoS Attack Status)
- ✓ Performance Alerts and Reporting
- ✓ Microsoft and Third Party (Dell, HP, Lenovo, Adobe, Java) Patching Software
- ✓ Self/Automated Repair and Optimization Utilities
- ✓ Advanced Security Services like EDR, and Security Operations Centers (SOC)

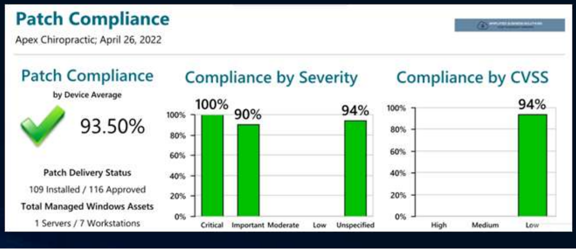


Device name	Protection stat...	Device ...	Last successful backup	Next backup	Last definitions update	Total used storage	Agent state	Agent version	Numbe...
Apex-Server.Apex.local	OK	Idle	04/26/2022 12:56 AM	04/27/2022 12:04 AM	02/14/2022 1:02 PM	289.41 GB	Online	15.0.29341	1





Global / SIMPLIFIEDBS
?
Tim O'Brien (Admin)
DASHBOARD
New Dashboard
+
Dashboard Last Saved Jun 2, 2022, 12:27:55 PM
try changing your filters to make them less
Threats by Detection Engine Last 3 Months
Reputation
SentinelOne Cloud
On-Write Static AI
User-Defined Blacklist
On-Write Static AI - Suspicious
Behavioral AI
Documents, Scripts
Anti Exploitation / Fileless
Intrusion Detection
Threats by Type Last 3 Months
Generic Heuristic
Malware
PUA



Patch Compliance

Apex Chiropractic; April 26, 2022

Patch Compliance

by Device Average

93.50%

Patch Delivery Status

109 Installed / 116 Approved

Total Managed Windows Assets

1 Servers / 7 Workstations

Conclusion - Long Term Approach to the Security Epidemic

- Stay vigilant – Always question an email communication and get verbal communication it is legitimate from the sender.
- Invest in additional awareness training, tools to improve safety and Never use/plug non-sanctioned devices into a corporate network. (Example – free USB drives from a conference)
- Develop future budgets with security in mind and Make IT Infrastructure and Security a priority in your annual budget.
- Consider adopting a Security Liaison Role and empower employees to help set guidelines throughout process to encourage ownership and forge buy-in

References

- https://www.consumerreports.org/privacy/ways-to-protect-digital-privacy/
- https://www.forbes.com/sites/forbestechcouncil/2017/06/05/13-biggest-challenges-when-moving-your-business-to-the-cloud/#585f24869b0e
- https://www.sans.org/reading-room/whitepapers/cloud/paper/38725
- https://www.nytimes.com/2018/12/10/technology/prevent-location-data-sharing.html
- https://securingtomorrow.mcafee.com/business/brief-history-cloud-computing-security/
- https://www.whizlabs.com/blog/cloud-security-risks/
- https://www.pcmag.com/roundup/300318/the-best-password-managers
- https://www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report--attacks-peak-during-the-holidays
- https://download.webroot.com/SecurityAwarenessTraining_GettingStartedGuide.pdf
- https://www.today.com/money/seven-warning-signs-your-identity-may-have-been-stolen-2D11944420
- https://www.quora.com/What-are-the-benefits-of-cloud-computing-to-consumers
- https://www.mcafee.com/enterprise/en-us/assets/white-papers/restricted/wp-sans-cloud-security-defense-in-detail-if-not-in-depth.pdf
- https://support.google.com/android/answer/6179507
- https://www.consumerreports.org/privacy/smart-speaker-privacy-settings/