Protecting Yourself in Today's Cyber Landscape

13 November 2019

Presented by Don Boian,
Cybersecurity Outreach Director

Huntington
Welcome.®

Agenda

- Threat Landscape - Overview
- Today’s Vulnerabilities & Risks
- Data Protection
- The Basics – Get Started Today!
- Q&A

Huntington
Welcome.

Disclaimer

This presentation is intended for educational purposes only and does not replace independent professional judgment. Statements of fact and opinions expressed are those of the individual participants and, unless expressly stated to the contrary, are not the opinion or position of Huntington National Bank or its affiliates. Huntington does not endorse or approve, and assumes no responsibility for, the content, accuracy of completeness of the information presented. Professional assistance must be consulted prior to acting on any of the content in this presentation.

The Huntington National Bank is Member FDIC.

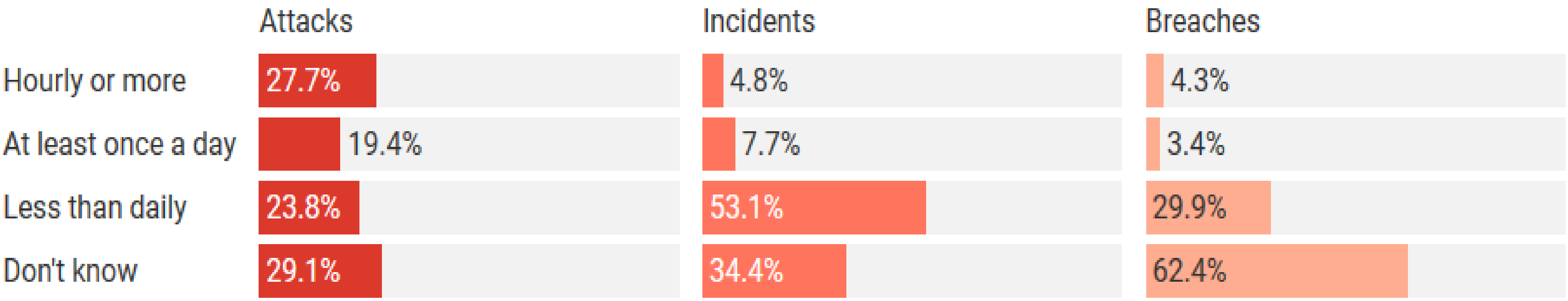
®, Huntington® and Huntington® are federally registered service marks of Huntington Bancshares Incorporated.

Welcome.

Current State of Local Government/ Municipality Cybersecurity

How frequently are local governments under cyberattack?

While many local governments know how often they're being targeted, a surprising number do not.

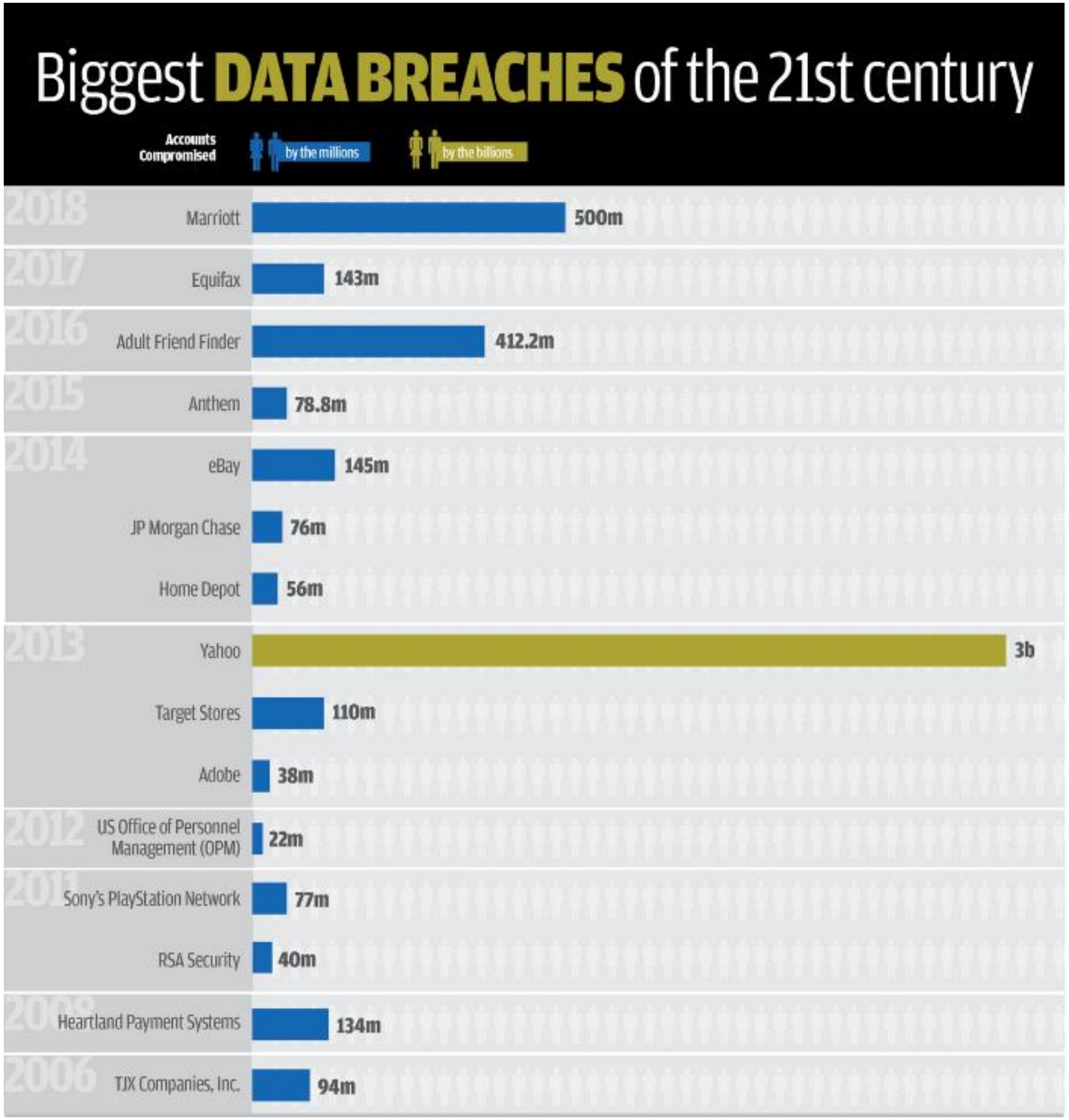


Attacks are attempts to gain unauthorized access to cause mischief or do harm. Incidents are events that compromise confidentiality, integrity or availability of a computer system. Breaches are incidents that result in confirmed disclosure of information to an unauthorized person.

Chart: The Conversation, CC-BY-ND • Source: University of Maryland, Baltimore County • Get the data

Source: https://www.govtech.com/security/Local-Governments-Cybersecurity-Crisis-in-8-Charts.html

Current Cybersecurity Threat Landscape



January – June 2019

3,816

Reported data breaches

4.1 Billion

Records compromised

Source: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

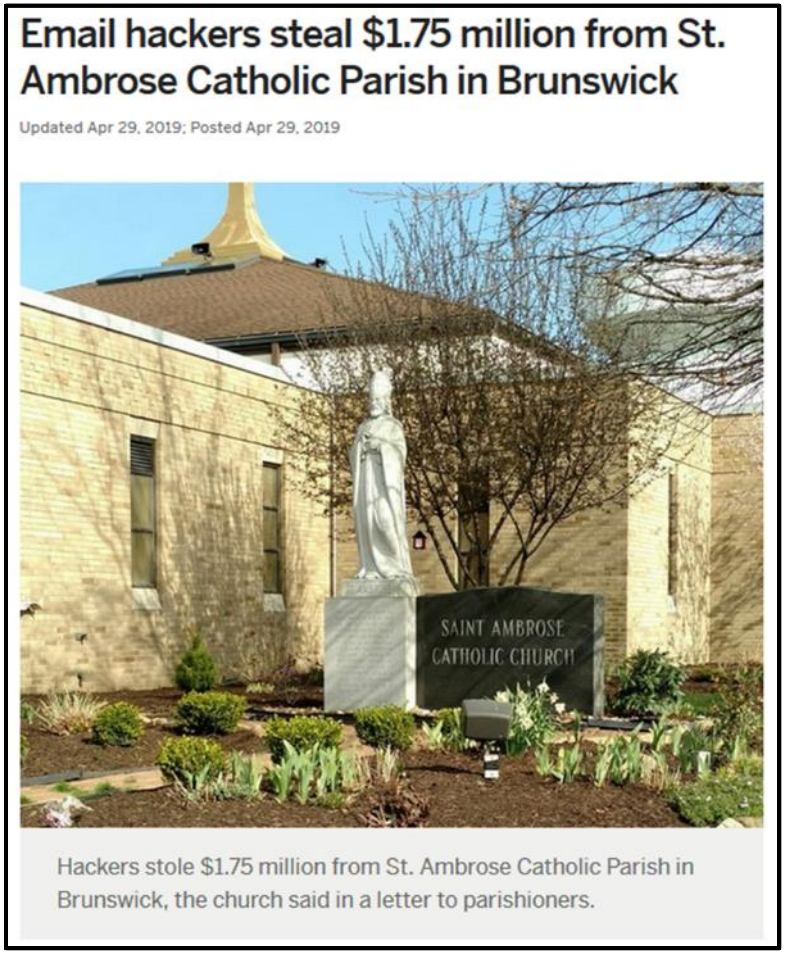
Business Email Compromise (BEC)

Business Email Compromise is defined as “a form of phishing attack where a cybercriminal impersonates an executive and attempts to get an employee, customer, or vendor to transfer funds or sensitive information to the phisher.”

BEC schemes are generally executed through two malicious techniques:

Email account compromise (EAC):
When an employee of a company has their email account compromised

Email spoofing:
Fraudster uses an email address that looks like a legitimate email address and tricks the victim



Email hackers steal $1.75 million from St. Ambrose Catholic Parish in Brunswick

Updated Apr 29, 2019; Posted Apr 29, 2019

Hackers stole $1.75 million from St. Ambrose Catholic Parish in Brunswick, the church said in a letter to parishioners.

Source: http://Cleveland.com
Source: https://www.phishprotection.com/content/business-email-compromise/

BEC & EAC: A Rising Threat

According to the FBI: Between the years of 2015-2017 …

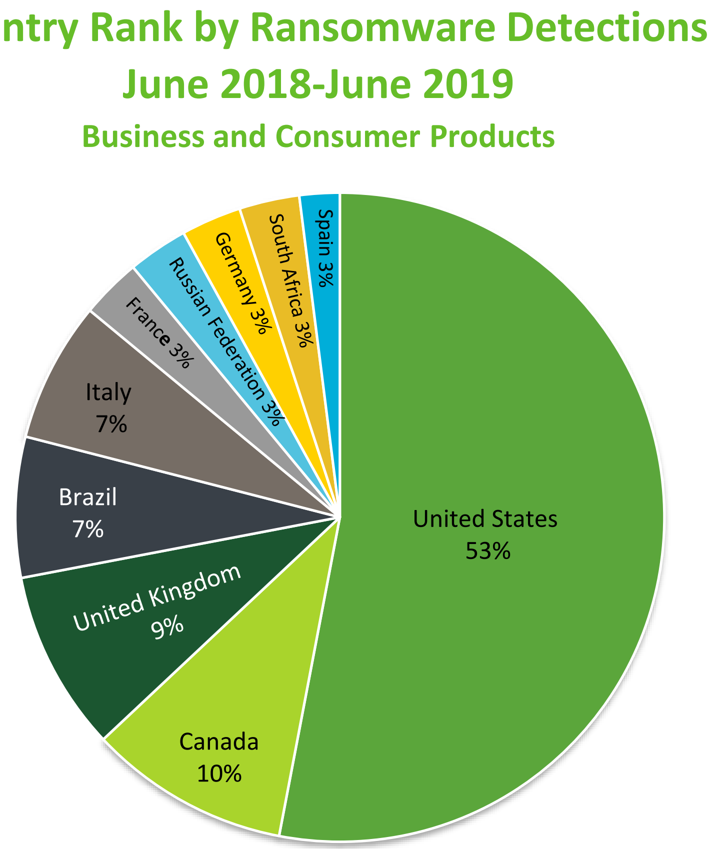
% increase in BEC/EAC victims __1,100__%.

% rise in monetary loss __2,200__%

"In May 2018 the highest number of BEC/EAC victims was reported since 2015."

Source:
https://www.securityweek.com/bec-scam-losses-top-12-billion-fbi
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1501791870.pdf
Cleveland.com/Cleveland.comp://Cleveland.com

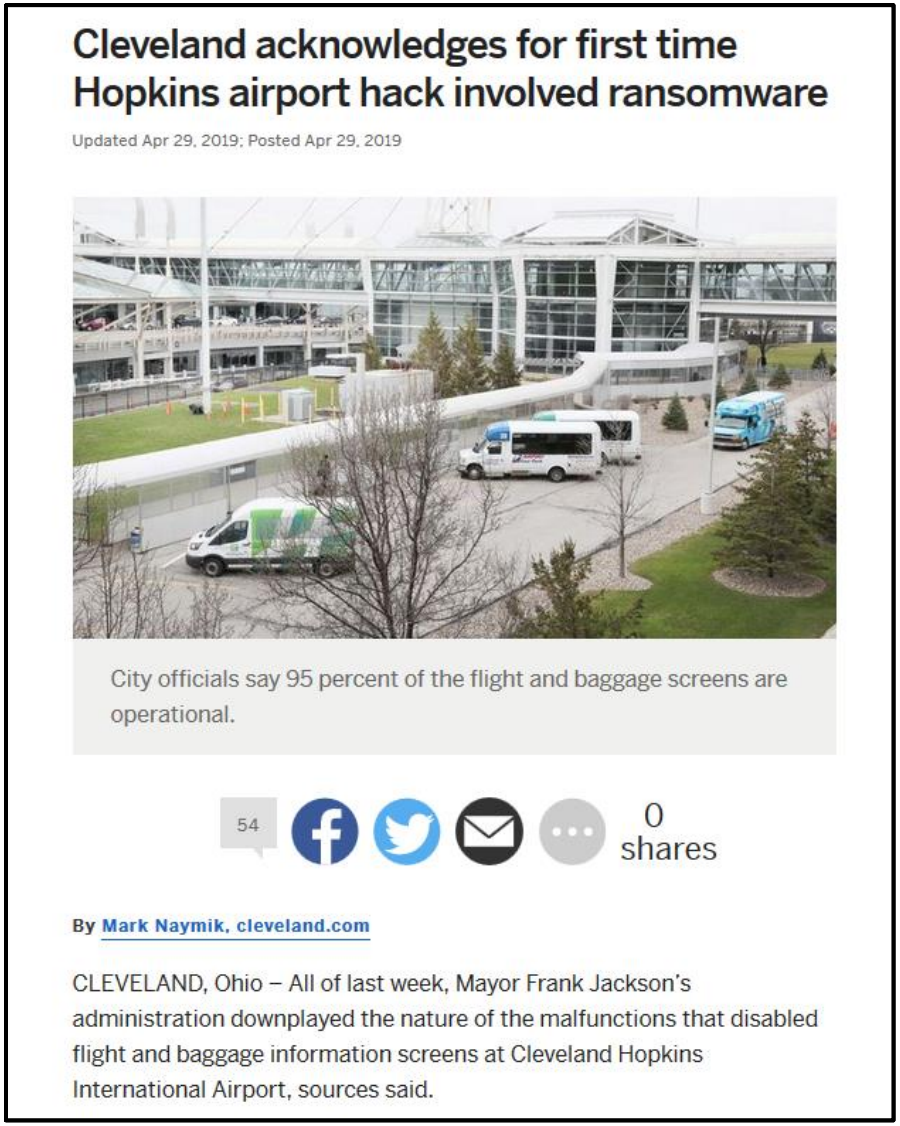
Malware and Ransomware



Ransomware detections against businesses in the second quarter of 2019 rose by a 363% year over year, while consumer detections of ransomware declined by 12% year over year and 25% quarter over quarter.

Source: https://www.bleepingcomputer.com/news/security/us-accounts-for-more-than-half-of-worlds-ransomware-attacks/

In the headlines



Cleveland acknowledges for first time Hopkins airport hack involved ransomware

Updated Apr 29, 2019; Posted Apr 29, 2019

City officials say 95 percent of the flight and baggage screens are operational.

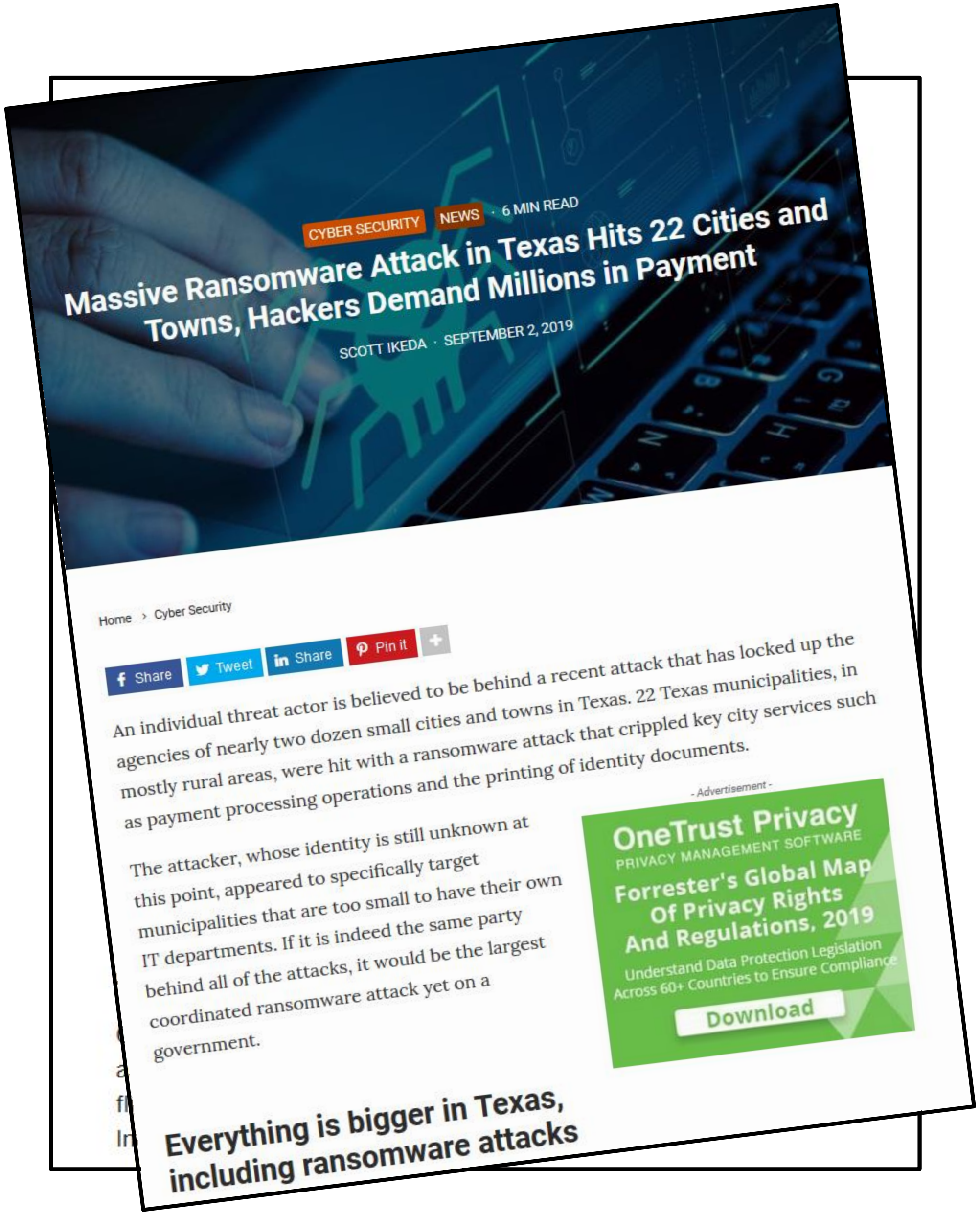
By Mark Naymik, cleveland.com

CLEVELAND, Ohio – All of last week, Mayor Frank Jackson's administration downplayed the nature of the malfunctions that disabled flight and baggage information screens at Cleveland Hopkins International Airport, sources said.

- Disruption of Flight Information Systems
  - Baggage claim
  - Gate Arrival/Departure

Source: http://cleveland.com/

In the headlines



CYBER SECURITY NEWS · 6 MIN READ

Massive Ransomware Attack in Texas Hits 22 Cities and Towns, Hackers Demand Millions in Payment

SCOTT IKEDA · SEPTEMBER 2, 2019

Home › Cyber Security

An individual threat actor is believed to be behind a recent attack that has locked up the agencies of nearly two dozen small cities and towns in Texas. 22 Texas municipalities, in mostly rural areas, were hit with a ransomware attack that crippled key city services such as payment processing operations and the printing of identity documents.

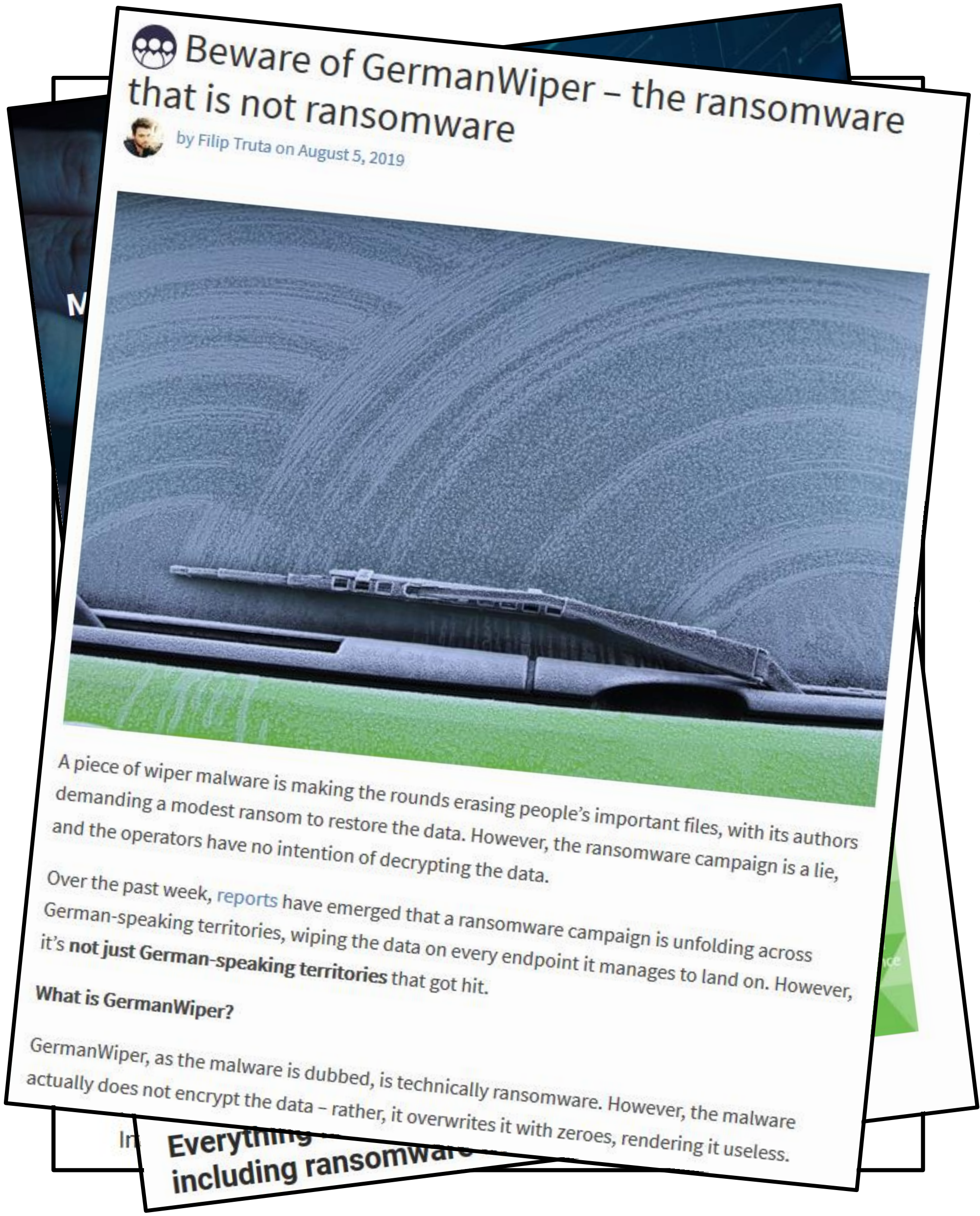
The attacker, whose identity is still unknown at this point, appeared to specifically target municipalities that are too small to have their own IT departments. If it is indeed the same party behind all of the attacks, it would be the largest coordinated ransomware attack yet on a government.

Everything is bigger in Texas, including ransomware attacks

- 22 government municipalities throughout Texas impacted by a coordinated ransomware attack on their computer networks.
- Hackers can remotely block access to important data and systems until a ransom is paid. Sometimes data is never recovered.

Source: https://www.cpomagazine.com/cyber-security/massive-ransomware-attack-in-texas-hits-22-cities-and-towns-hackers-demand-millions-in-payment/

In the headlines



Beware of GermanWiper – the ransomware that is not ransomware

by Filip Truta on August 5, 2019

A piece of wiper malware is making the rounds erasing people's important files, with its authors demanding a modest ransom to restore the data. However, the ransomware campaign is a lie, and the operators have no intention of decrypting the data.

Over the past week, reports have emerged that a ransomware campaign is unfolding across German-speaking territories, wiping the data on every endpoint it manages to land on. However, it's **not just German-speaking territories** that got hit.

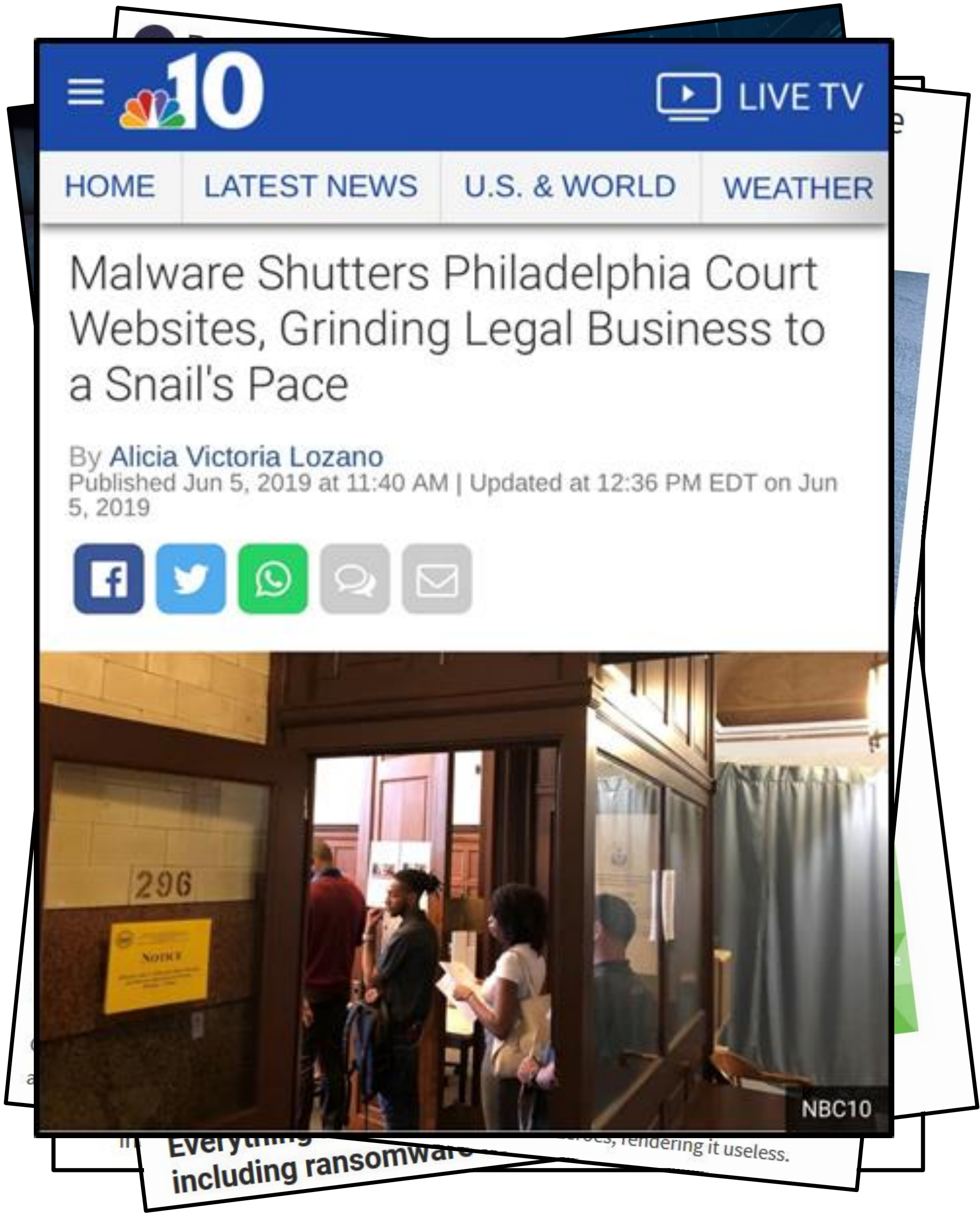
What is GermanWiper?

GermanWiper, as the malware is dubbed, is technically ransomware. However, the malware actually does not encrypt the data – rather, it overwrites it with zeroes, rendering it useless.

- A data-wiping malware, distributed via as spam email campaign, with a ransom note written in German and demanding $1,500 bitcoin payment.
- The malware pretends to be ransomware but is actually a wiper that destroys the data instead of encrypting it.

Source: https://securityboulevard.com/2019/08/beware-of-germanwiper-the-ransomware-that-is-not-ransomware/

In the headlines



Malware Shutters Philadelphia Court Websites, Grinding Legal Business to a Snail's Pace

By Alicia Victoria Lozano
Published Jun 5, 2019 at 11:40 AM | Updated at 12:36 PM EDT on Jun 5, 2019

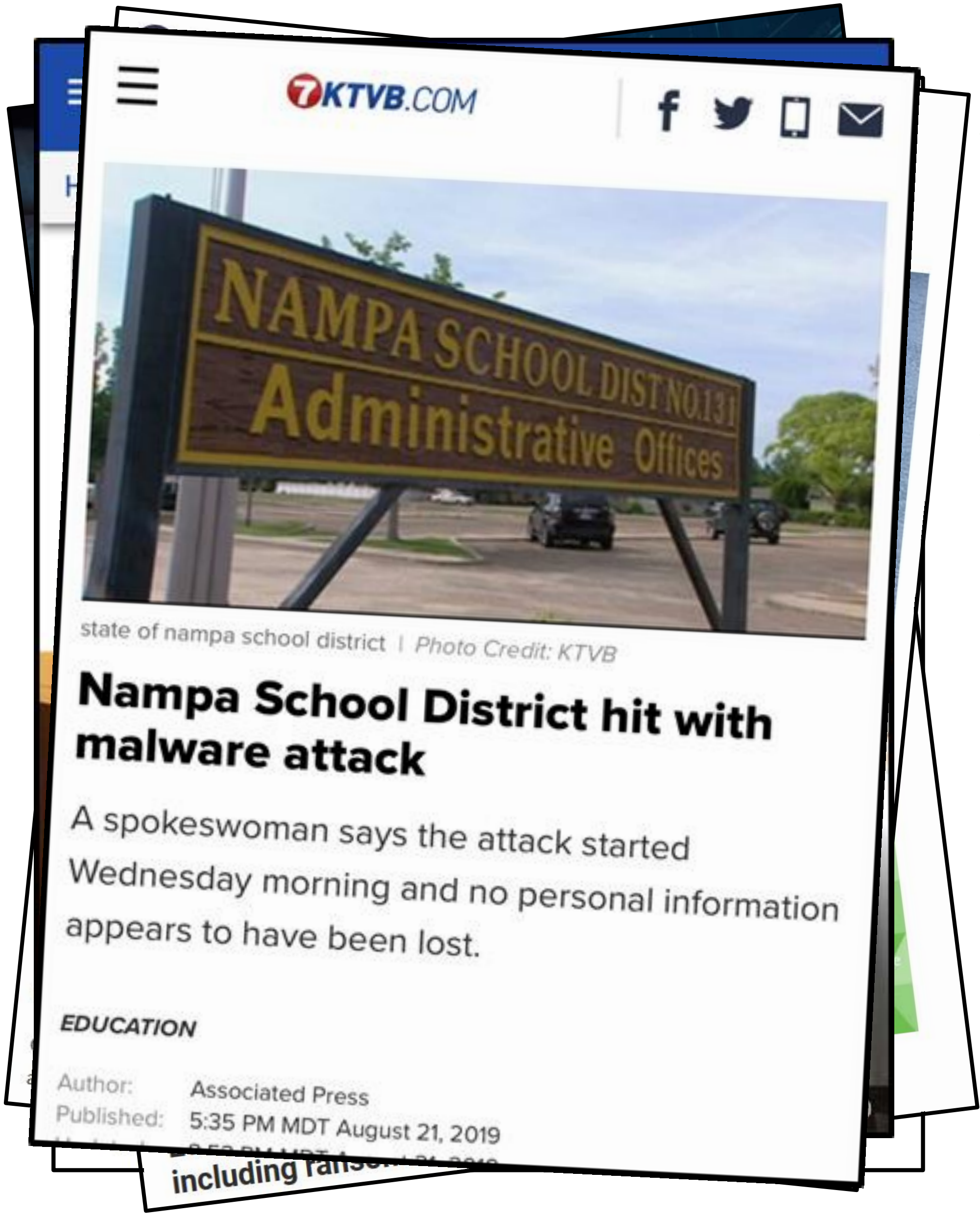
Everything
including ransomware

rendering it useless.

- City court websites were first shut down after malware was found on a “limited number” of First Judicial District computers.
- As a precaution, the electronic filing system for civil and criminal cases and several email accounts were suspended and have yet to be restored.

Source: http//www.nbcphiladelphia.com/news/local/Malware-Philadelphia-First-Judicial-District-Computers-510860591.html

In the headlines



state of nampa school district | *Photo Credit: KTVB*

Nampa School District hit with malware attack

A spokeswoman says the attack started Wednesday morning and no personal information appears to have been lost.

EDUCATION

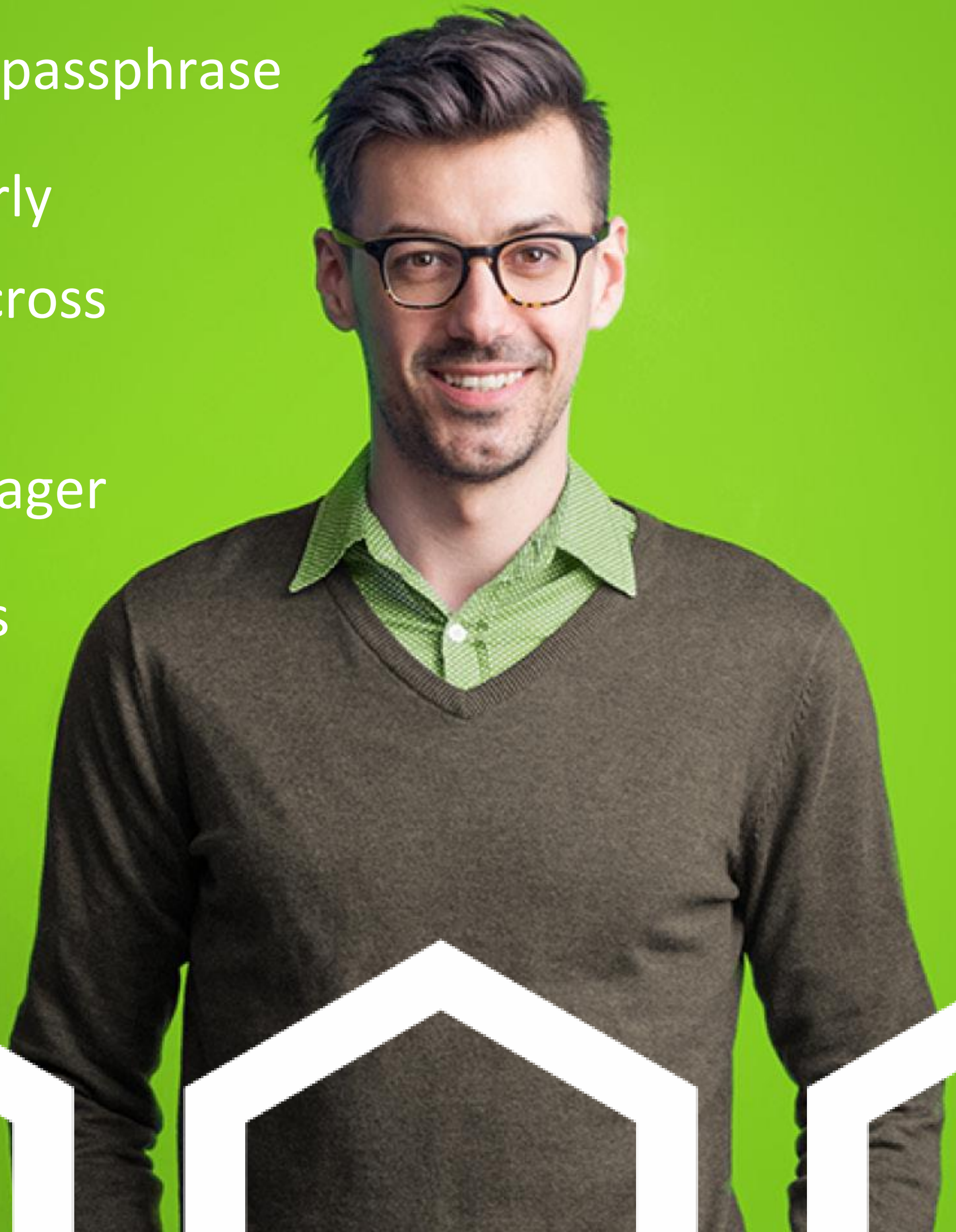
Author: Associated Press
Published: 5:35 PM MDT August 21, 2019

- The Nampa School District has shut down their internet following a malware attack.
- Teachers & Administrators are forced to use personal devices as a precaution following the attack.

Source: https://www.ktvb.com/article/news/nampa-school-district-hit-with-malware-attack/277-4092dda1-d23e-4650-b82b-361e090f33fa

Credential Security – Password Basics

- Chose a strong password/passphrase
- Change passwords regularly
- Never reuse passwords across multiple accounts
- Consider a password manager
- Change default passwords



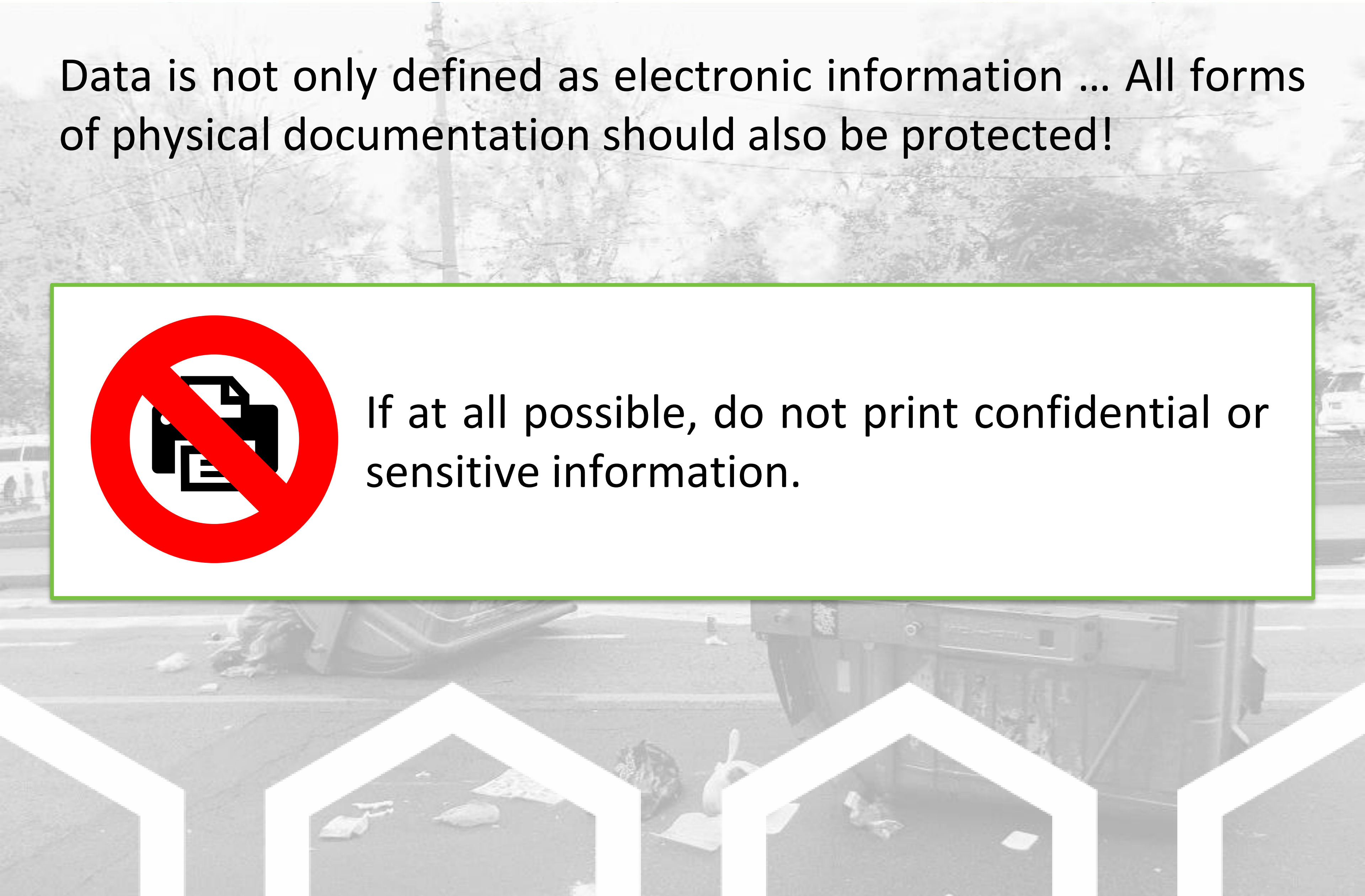
Protecting Personally Identifiable Information (and other sensitive information)

Personally Identifiable Information (PII)
PII includes: Name, emails, home address, phone number, etc.

Sensitive PII includes:	
If standalone:	*If paired with another identifier:*
Social Security Number (SSN)	Citizen or Immigration Status
Driver's License or State ID #	Medical Information
Passport Number	Ethnic or Religious Affiliation
Alien Registration Number (A#)	Sexual Orientation
Financial Account Number	Account Passwords
Credit Car Numbers	Last Four Digits of SSN
Biometric Identifiers	Date of Birth
	Criminal History
	Mother's Maiden Name
	Personal Health Information

Source: DHS Privacy Policy Directive 047-01-007

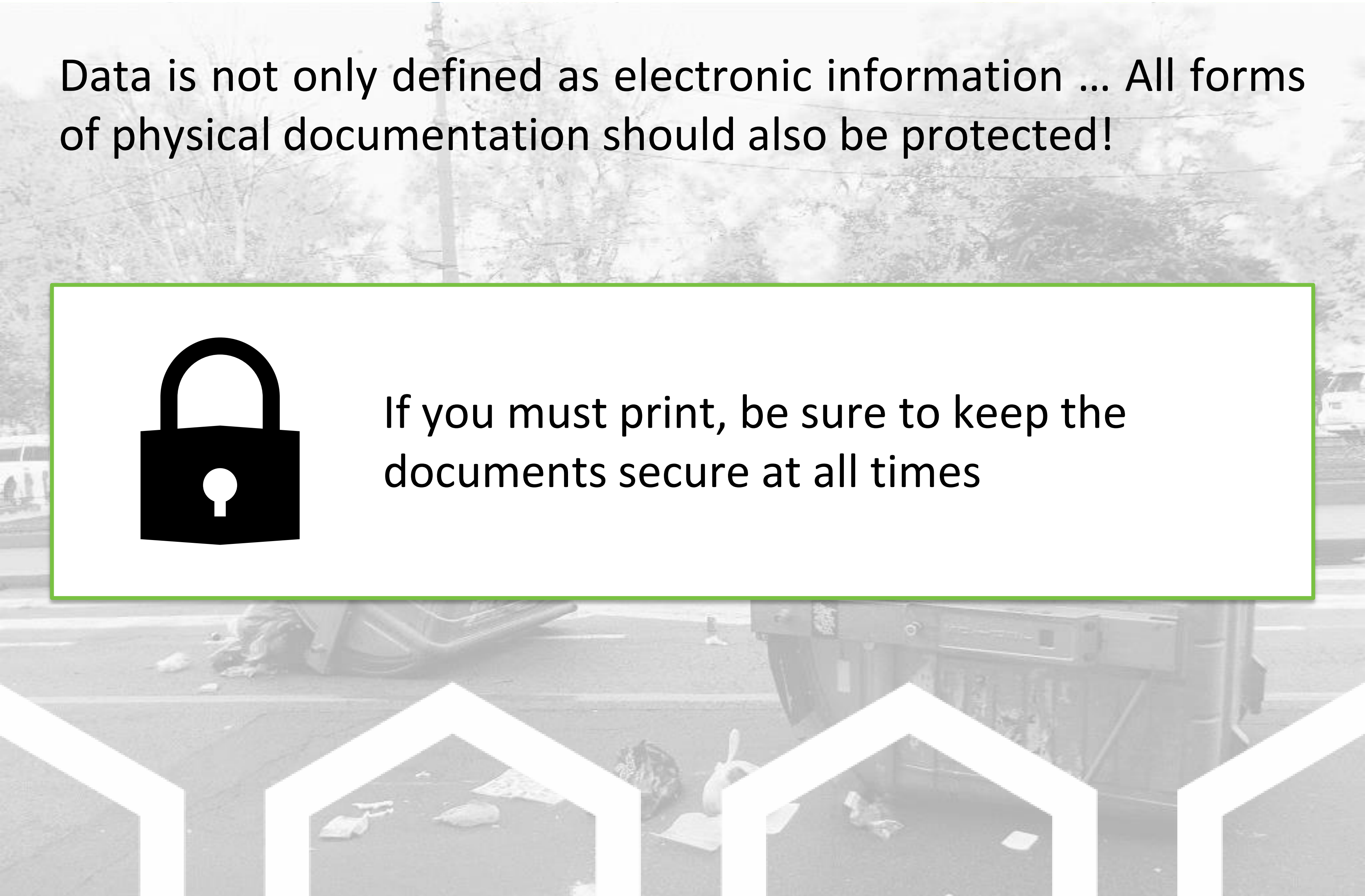
Protect ALL Forms of Information



Data is not only defined as electronic information … All forms of physical documentation should also be protected!

If at all possible, do not print confidential or sensitive information.

Protect ALL Forms of Information



Data is not only defined as electronic information … All forms of physical documentation should also be protected!

If you must print, be sure to keep the documents secure at all times

Protect ALL Forms of Information

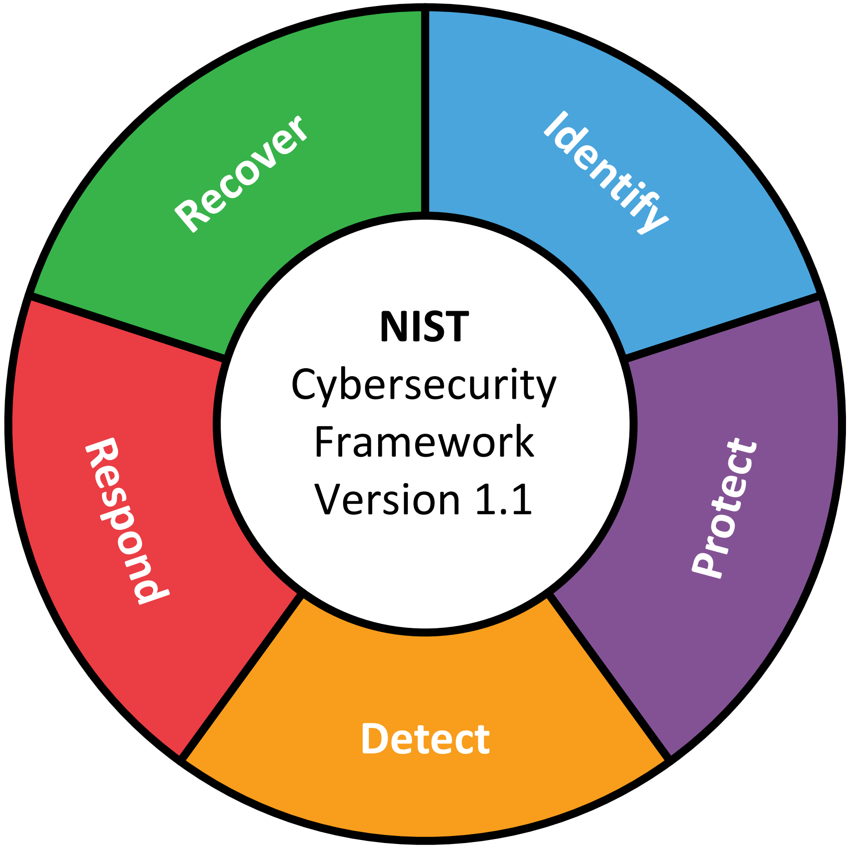
Data is not only defined as electronic information … All forms of physical documentation should also be protected!

Once you are finished with the documents, be sure to properly destroy them!

Protecting Payment Processing

- Are there appropriate checks and balances in place?
- Is there a single person (or account) that can make payments or transfer funds?
- Are critical systems isolated (or on own segment)?
- Are environmental systems on separate network segments?

The NIST Cybersecurity Framework

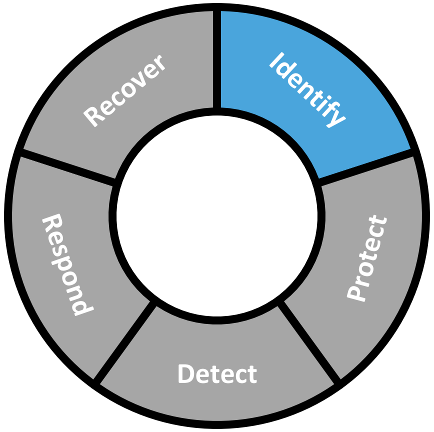


NIST
Cybersecurity
Framework
Version 1.1

Source: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

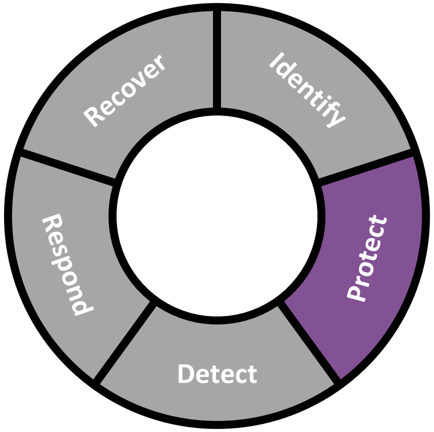
Identify

- Inventory data
- Index systems and software
- Conduct independent security assessments



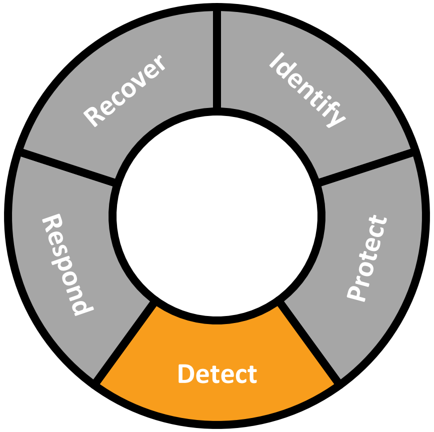
Protect

- Implement employee training/awareness
- Backup data
- Update Operating Systems and Applications
- Integrate e-mail security best practices
- Increase network defensive barriers



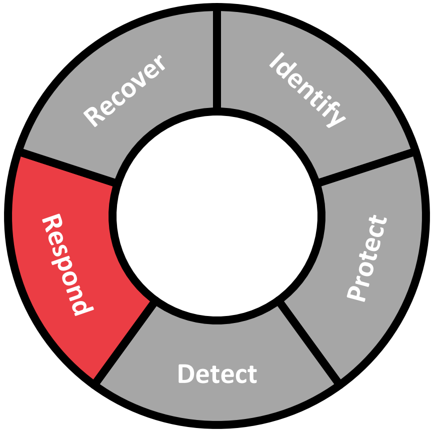
Detect

- Ensure Antivirus, endpoint encryption and data loss prevention software up to date
- Monitor your logs for anomalies
- Integrate Checks and Balances in ALL processes
  - Segregation of duties
  - Least privilege
  - Invoice/payment processing



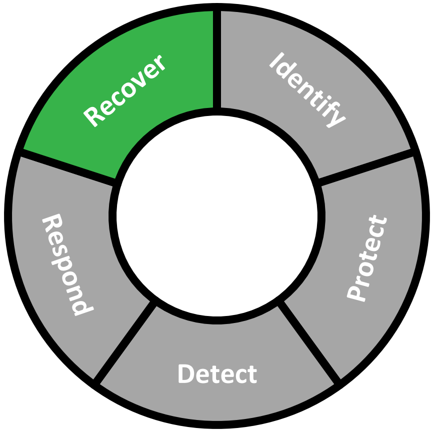
Respond

- Develop and periodically review incident response plans
- Exercise the incident response plans
- Integrate those plans with business continuity and communications plans



Recover

- Plan (and exercise) for the worst
- Cybersecurity Insurance – Purchase and/or update policies & know your coverage



Q&A

Thank you.

Appendix

Corporate Cybersecurity Basics*

1. Employee training/awareness (Phishing, BEC, Social Engineering, …)
2. Inventory sensitive data (know where it is stored and processed, know what 3rd parties have your sensitive data)
3. Backup data
4. Inventory systems and software (necessary for Vulnerability Mgt, etc)
5. Updated/Current OS and Applications (patch management)
6. Antivirus, Endpoint encryption, Data Loss Prevention - software up to date
7. Independently assess your security and that of your 3rd parties
8. Implement E-mail security (DMARC, SPF, DKIM), external banner, block spam/junk
9. Plan (and exercise) for the worst (malware, outage, breach, …)
10. Monitor your logs for anomalies (or outsource it – MSSP)
11. Increase network defensive barriers
12. Checks and Balances in ALL processes (Segregation of duties, least privilege, invoice/payment processing, …)
13. Cybersecurity Insurance – Purchase and/or update policies & know your coverage

BE BRILLANT AT THE BASICS

* Start with these, but don't stop there once you've mastered them

Personal Cybersecurity Basics*

1. Raise awareness (Phishing, Social Engineering, …) – know the threats
2. Passwords – NO reuse; Complex; Passphrase; Use a Password Manager
3. Backup data
4. Updated/Current OS and Applications – allow auto-update
5. Antivirus, Firewall, Home network – change default passwords!
6. Terms of Service; Beware of free services – YOU'RE the product
7. Geolocation/Location based services
8. Reputable applications and what they have access to
9. Home IoT Devices – Change default passwords; Security
10. WiFi Security
11. Credit Cards – Transaction Alerts (CNP); Use mobile app locking
12. Credit Reporting Bureaus - Freeze/Lock credit
13. Application Settings - Security & Privacy – periodically review/reset

BE BRILLANT AT THE BASICS

* Start with these, but don't stop there once you've mastered them