Welcome to the SPELL JIF Virtual Safety Seminar:

Managing Virtual Safety and Security Risks in a Digital World

Wednesday, July 19, 2023

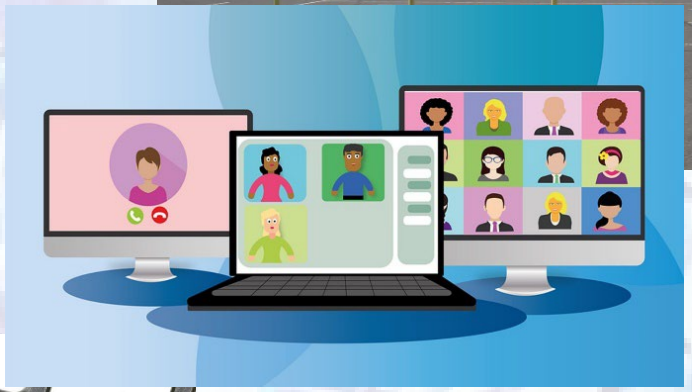
Why Virtual Safety instead of Cyber Security?

If I say, Safety

you think Organization.

If I say Virtual,

you think Instruction.



If I say Cyber,

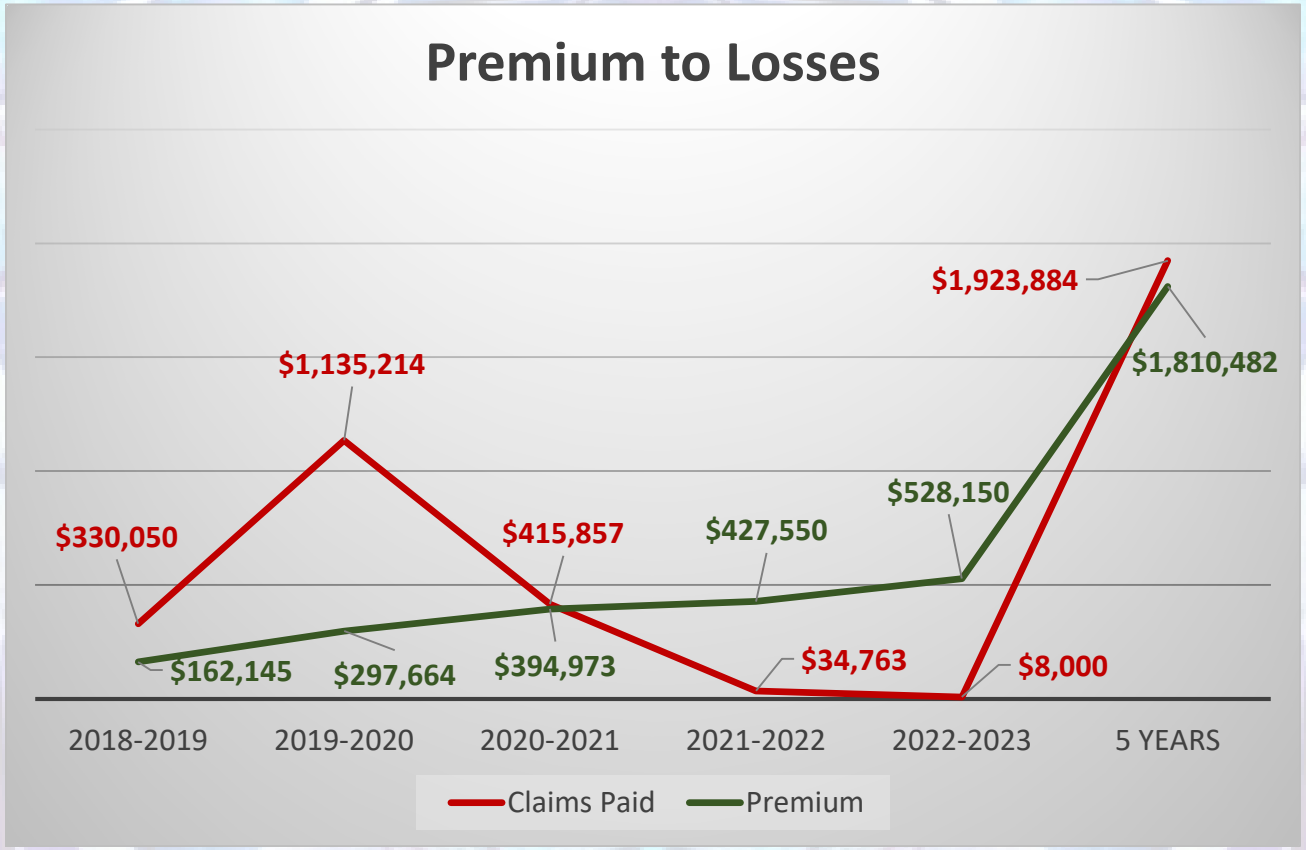
you think IT.

Why Virtual Safety instead of Cyber Security?

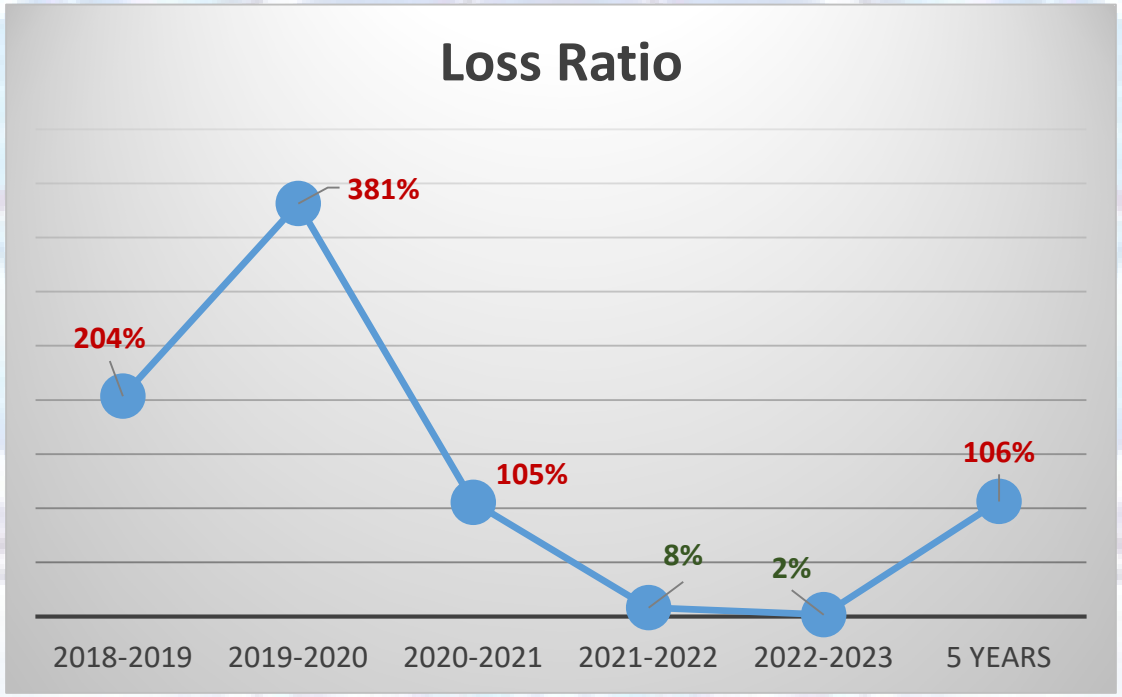
The truth is you need the combined efforts of IT and Instruction to create a Safe Organization.

We can’t afford not to get better at this.

We can’t afford not to get better at this.



We can’t afford not to get better at this.



STOLEN HARDWARE & DATA

Actual Claim Descriptions

A survey was taken in middle school in spring of 2022. The responses on this form contained some student data including Student ID, First Name and Last Name. This sheet was accidently shared with public access and was accessed anonymously.

District issued laptop and iPad stolen from an employee's car over the weekend in front of home. There is the potential that PII of students were on the devices.

A special ed. teacher's car was broken into and 8 student IEPs were stolen from her car while on vacation in Florida.

A teacher left a school laptop in his car overnight at his home. The car was broken into and the laptop was stolen.

DISGRUNTLED EMPLOYEE

Actual Claim Descriptions

District reports that on 1/31/2020 the HR Manager of the district was terminated effective 2/28/2020. The district computer was secured to ensure no data was deleted. It was discovered that on 2/3/2020, files were copied to a personal laptop.

IMPROPER ACCESS

Actual Claim Descriptions

A middle school student used her school issued laptop to search for prohibited subjects and was contacted for conversation by an unrelated adult through the chat app. This may have exposed the student's personal information.

BOE has been using the Zoom video conferencing platform for their remote learning instruction and have been doing so since their closure on March 17th. At approximately 2:10pm on Monday, 4/27 a Zoom session for their Algebra students was hacked by nine unauthorized participants.

EMAIL CHALLENGES

Actual Claim Descriptions

On 1/28/19 two BOE employees' email accounts were compromised. The users were not denied access to their accounts. One users email account was used to generate spam to other email accounts. Office 365 usernames and passwords for 2 employees may have been compromised.

School District staff member inadvertently sent personally identifiable information and highly sensitive data via e-mail to 12 families. The highly sensitive information was a list of all of the District's low income families (approximately 80).

GIVE ME YOUR PAYROLL

Actual Claim Descriptions

School District was breached and their bank logins in the business office were intercepted during payroll transfers, which led to someone creating and approving fraudulent wire transfers totaling $400,000.

An unauthorized person sent an email to the Board office directing a change to an employee's direct deposit information in order to fraudulently re-direct that employee's paychecks.

District reported that its assistant superintendent's payroll check was stolen through an email phishing scam, changing the bank via direct deposit. The Insured is working with our bank and IT team to ensure this is the only security breach.

GIVE ME YOUR PAYROLL

Actual Claim Descriptions

On 2/15/19 the district business administrator was contacted by the Superintendent who informed him that she did not receive her direct deposit and that the payment actually went to a bank which was not hers.

District reported that a payroll breach occurred with the May 30th payroll. Someone identifying themselves as the Superintendent sent an e-mail to payroll requesting a change of account form.

Potential security incident in apparent attempts to access the payroll server.

PARTNER CHALLENGES

Actual Claim Descriptions

District states that about 2 weeks ago a vendor's computer systems were compromised. The district believes their Business Office personnel computers are now compromised as it appears banking accounts and passwords may have been stolen.

On 9/3/20 at 09:54 BOE, received an email from PNC Bank advising that the password to the online banking application used to manage accounts at PNC Bank had changed, followed by 4 additional emails advising that security questions were altered.

School's telephone network provider (Xtel Communications) detected possible suspicious traffic originating from District's site. The International Calling Services have been disabled in order to prevent further incident.

PARTNER CHALLENGES

Actual Claim Descriptions

The insured received a notice from Tmobile, its cell phone vendor, notifying it that Tmobile suffered a data breach.

Third party software, RealTime, suffered a malware attack that temporarily interrupted provision of services to clients including to the insured school. Reportedly, no data was accessed or stolen.

The Difference Card had a data breach. This is a third party used to administer part of the District health insurance program. We were notified on 7/13/2022 of the breach, but were told that none of our data was included in the breach.

SYSTEMS DOWN

Actual Claim Descriptions

Superintendent arrived at school and system was locked.

District systems went down on 11/28/2022 for internet and email. No internal or external access. No access to financial, operational or instructional software. Entire school system aware.

SYSTEMS DOWN

Actual Claim Descriptions

On Thursday, April 18, 2019 at 10:58 am, The BOE experienced a Crypto lock virus which made their server that housed student database information system (Genesis) inoperable.

District servers are down and they have been inflicted with ransomware. The technology company they contract with is in charge of their backups and those may have been corrupted as well.

SYSTEMS DOWN

Actual Claim Descriptions

Network is down, which happens after a storm. When system restarted they noticed that all file backup dates were the same, but Tech noticed the Systems 3000 (Financial Package) was not operating correctly.

DDoS attack starting with internet outages around 11/23/20 and possibly progressing to Zoom class interference.

District's transportation server has been encrypted and threat actors are asking for 3 bit coin to release the data. District further contends that the threat actors have denied them access just to their transportation server.

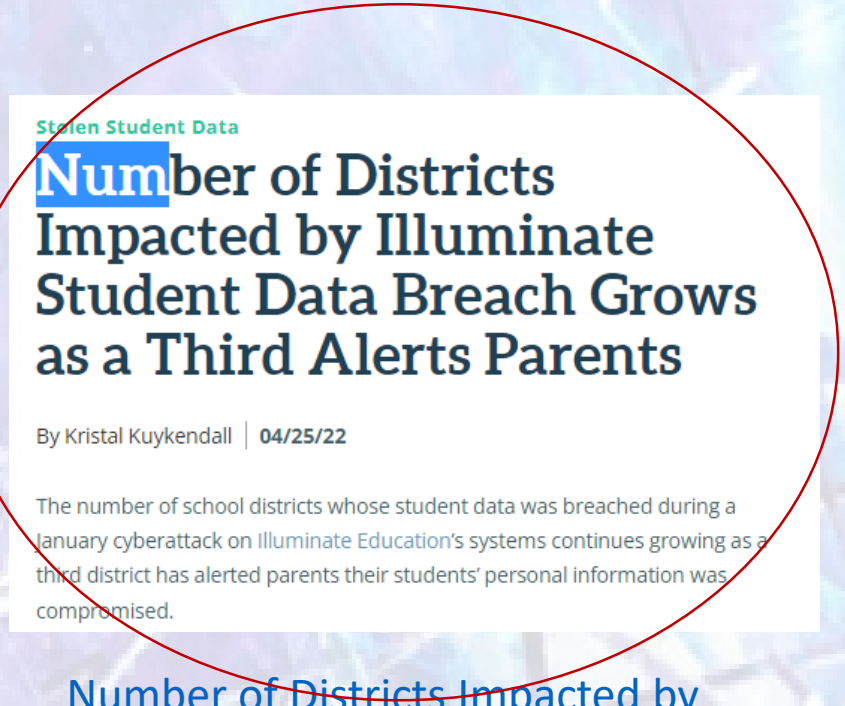
PHISHING

Actual Claim Descriptions

The District received and paid a fraudulent invoice sent by an unauthorized person who was able to compromise one or more of the school's outside vendors.

The school experienced a phishing attack and what appeared to be lateral movement through their servers and unauthorized changes such as installation of screen sharing software, HVAC overrides, errors in telephone server software and inability to access data.

Educational Software Breaches



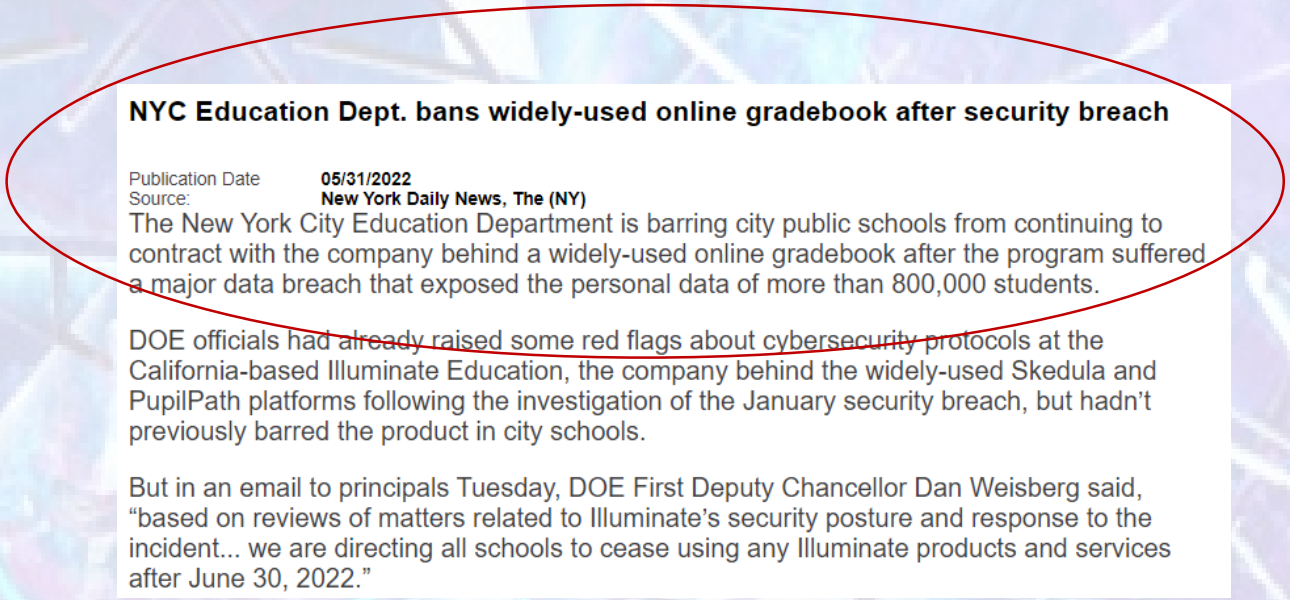
Stolen Student Data

Number of Districts Impacted by Illuminate Student Data Breach Grows as a Third Alerts Parents

By Kristal Kuykendall | **04/25/22**

The number of school districts whose student data was breached during a January cyberattack on Illuminate Education's systems continues growing as a third district has alerted parents their students' personal information was compromised.

[Number of Districts Impacted by Illuminate Student Data Breach Grows as a Third Alerts Parents -- THE Journal]



NYC Education Dept. bans widely-used online gradebook after security breach

Publication Date **05/31/2022**
Source: **New York Daily News, The (NY)**

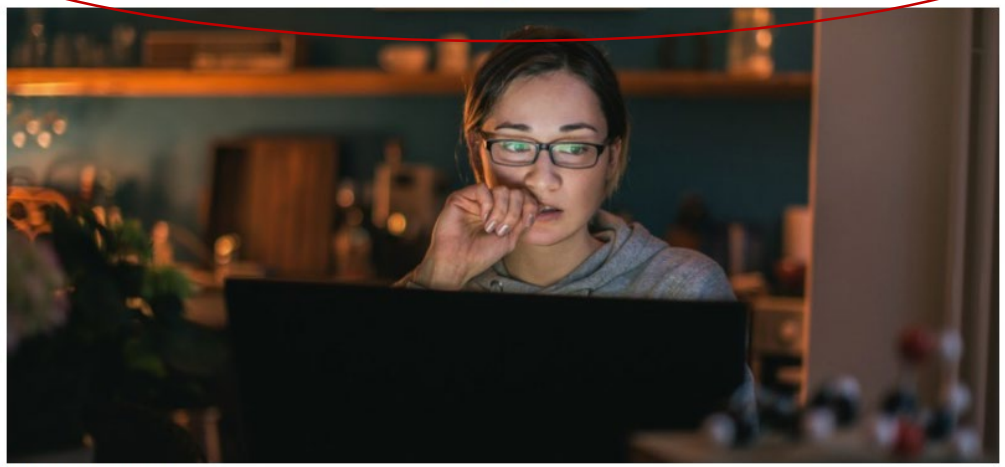
The New York City Education Department is barring city public schools from continuing to contract with the company behind a widely-used online gradebook after the program suffered a major data breach that exposed the personal data of more than 800,000 students.

DOE officials had already raised some red flags about cybersecurity protocols at the California-based Illuminate Education, the company behind the widely-used Skedula and PupilPath platforms following the investigation of the January security breach, but hadn't previously barred the product in city schools.

But in an email to principals Tuesday, DOE First Deputy Chancellor Dan Weisberg said, "based on reviews of matters related to Illuminate's security posture and response to the incident... we are directing all schools to cease using any Illuminate products and services after June 30, 2022."

[Advisen Front Page News]

Report Reveals Surveillance Abuses In Educational Technology



GUIDO MIETH/GETTY IMAGES

By Alexandra Kelley,
Staff Correspondent,
Nextgov/FCW

MARCH 31, 2022

The report was commissioned by Democratic Senators Elizabeth Warren, Richard Blumenthal and Edward J. Markey.

PRIVACY | EDUCATION | CONGRESS | ARTIFICIAL INTELLIGENCE

A report examining the use of four educational technology companies' usage of artificial intelligence was released on Wednesday, following a request from Sens. Elizabeth Warren, D-Mass., Edward J. Markey, D-Mass., and Richard Blumenthal, D-Conn. back in 2021.

The companies in question—Gaggle.net, Bark Technologies, GoGuardian and Securly Inc.—were found to have misused surveillance technology while students were using the products. The report specifically noted that software monitoring student activity may have been misused for disciplinary purposes resulting in contact with law enforcement and that schools and parents have not been made aware of the use of data being gathered by these softwares.

Additionally, some of the software companies may not have taken adequate action to understand if student activity monitoring software disproportionately targets a select racial group or LGBTQ+ students, further exacerbating the disparities marginalized groups face.

"Absent federal action, these surveillance products may continue to put students' civil rights, safety and privacy at risk," the report reads.

This report builds on increased concerns over artificial intelligence and surveillance technology's potential for biased algorithms that target vulnerable communities.

A lack of legal regulation and oversight contribute to the interest legislators have in investigating uses of artificial intelligence, particularly in the private sector. These specific concerns follow a report issued by the Center for Democracy and Technology documenting inappropriate surveillance of students.

https://www.nextgov.com/analytics-data/2022/03/report-reveals-surveillance-abuses-educational-technology/363860/

Consequences

Microsoft settles charges over data collection on children using Xbox

Publication Date 06/06/2023
Source: Dow Jones News Service

By John D. McKinnon

WASHINGTON -- Microsoft agreed to pay $20 million to settle charges that it violated children's privacy rights when they signed up for its Xbox gaming system, the Federal Trade Commission said Tuesday.

The FTC charged that Microsoft violated the Children's Online Privacy Protection Act, known as Coppa, by collecting personal information from children under 13 when they signed up for Xbox, without notifying their parents or obtaining their parents' consent.

Microsoft also improperly retained children's personal information, the FTC said.

[Advisen Front Page News]

Hackers steal social security numbers, birth dates and more on CalPERS, CalSTRS retirees

Publication Date 06/22/2023
Source: Sacramento Bee (CA)

The California Public Employees' Retirement System reported Wednesday that hackers stole the names, social security numbers, birth dates and other confidential information of roughly 769,000 retirees and beneficiaries, taking advantage of a vulnerability in a contracted vendor's cybersecurity system.

"This external breach of information is inexcusable," said CalPERS CEO Marcie Frost in a news release. "Our members deserve better. As soon as we learned about what happened, we took fast action to protect our members' financial interests, as well as steps to ensure long-term protections."

CalPERS is the largest pension system in the nation, with more than 2 million members and administering benefits to more than 1.5 million members and their families. CalSTRS, the nation's second-largest, said Thursday it, too, was hacked through the same vendor, though it denied to offer specifics on who was affected.

[Zywave | Advisen Front Page News]

Zywave | Advisen Front Page News - Thursday, July 6, 2023

E-mail This Story Print This Story

Ransomware criminals are dumping kids' private files online after school hacks

Publication Date: 07/05/2023
Source: Independent, The (UK) (Online)

The confidential documents stolen from schools and dumped online by ransomware gangs are raw, intimate and graphic. They describe student sexual assaults, psychiatric hospitalizations, abusive parents, truancy — even suicide attempts.

"Please do something," begged a student in one leaked file, recalling the trauma of continually bumping into an ex-abuser at a school in Minneapolis. Other victims talked about wetting the bed or crying themselves to sleep.

Complete sexual assault case folios containing these details were among more than 300,000 files dumped online in March after the 36,000-student Minneapolis Public Schools refused to pay a $1 million ransom. Other exposed data included medical records and discrimination complaints.

Rich in digitized data, the nation's schools are prime targets for far-flung criminal hackers, who are assiduously locating and scooping up sensitive files.

Why Virtual Safety instead of Cyber Security?

Human Failure causes nine out of ten cyber incidents. Behavior change and education are among the most effective ways to address cyber attacks.

Learn to Leap: Building a human firewall to block cyberattacks: Lessons from SoSafe

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/building%20a%20human%20firewall%20to%20block%20cyberattacks%20sosafe/building-a-human-firewall-to-block-cyberattacks-lessons-from-sosafe.pdf

Why Virtual Safety instead of Cyber Security?

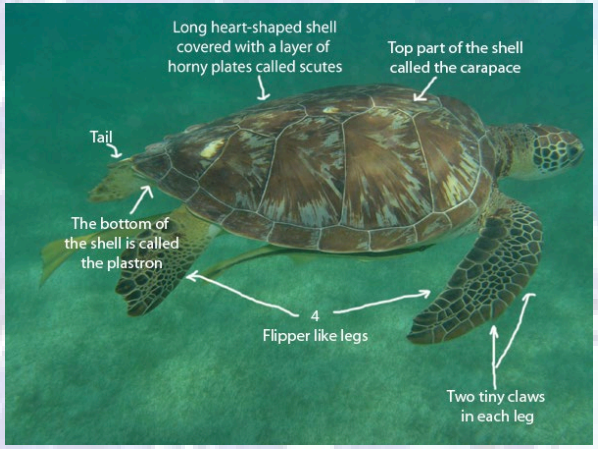
1. We are physical and virtual beings.
2. We are dependent upon safe physical and virtual space.
3. Safety is a matter of construct, awareness, rules and, more than anything else, human behavior.

Keep My Identity Safe Please

Financial Information

Residence and Work Information

Virtual Me



Physical Attributes

Health Information

Social Security, Driver's License, Credit Cards & more


ORGANIZATIONAL
PHYSICAL
PERSONAL
SAFETY
360°
EMOTIONAL
VIRTUAL
COMMUNAL

Why Virtual Safety instead of Cyber Security?

Because safety is physical and virtual.

Thank You