



SEAC

SOUTHEASTERN ACTUARIES CONFERENCE

BEING PART OF SOMETHING THAT COUNTS

Cyber Security:
Protecting your data and your
privacy

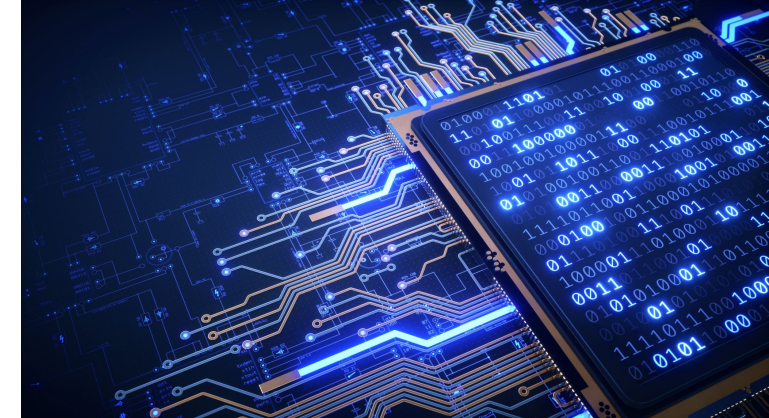
June 24, 2022, 8:30am

Kevin C. Glasgow, FLMI, FLHC, CLU®, CFE

Diligence International Group, LLC

1-800-660-4202

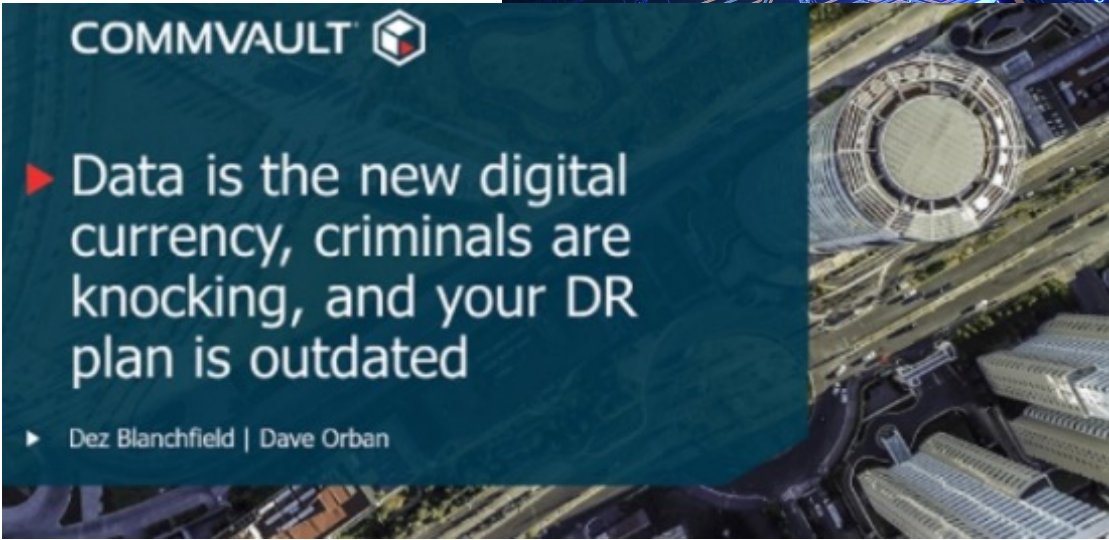
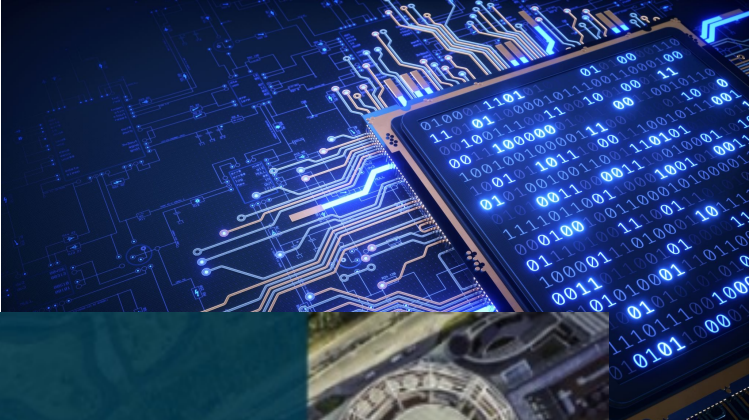
www.DIGroup-US.com



Objectives

- Define OSCINT
- Learn how to protect your data:
 - Password habits
 - Security question
 - VPNs
 - WIFI Signals
- Identify Social Engineering schemes
 - Website insights
- Understanding what a DDOS attack does

Data Is The New Currency



Data Is The New Currency

Unfortunately, data isn't always used for good purposes.

June 13, 2022

Kaiser Permanente Discloses Data Breach at WA Health Plan, 69K Impacted

Kaiser Foundation Health Plan of Washington, Virginia Mason Medical Center, and MCG Health recently reported data breaches impacting protected health information (PHI).



Source: Getty Images

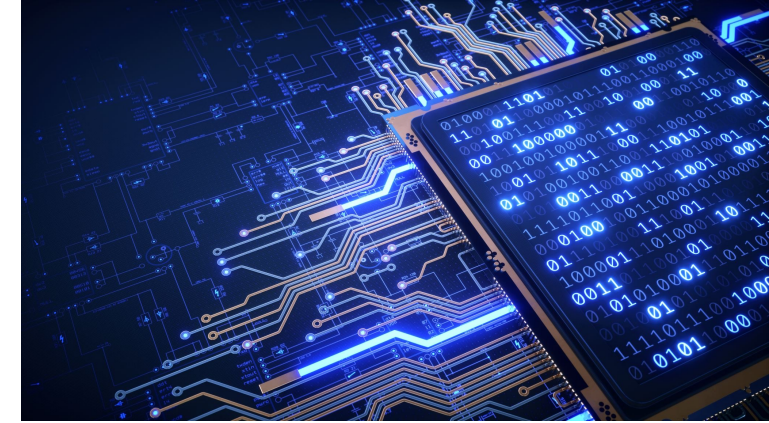


By Jill McKeon



June 13, 2022 - Kaiser Permanente notified 69,589 individuals of a data breach that occurred at

OSINT: Open-Source Intelligence

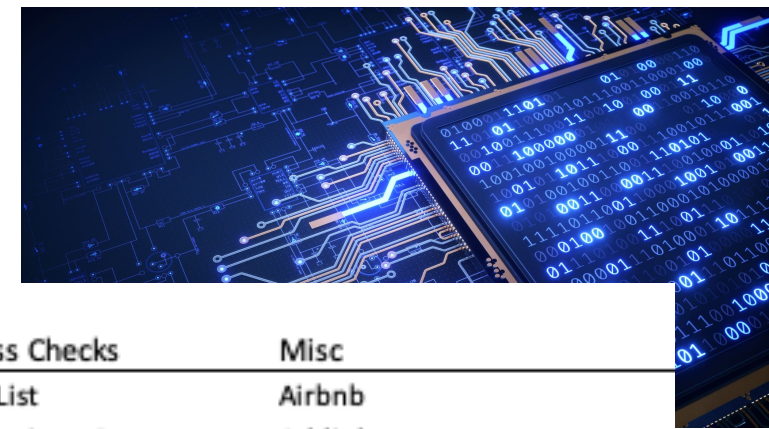


Simply put:

All information available through public source whether electronic, physical, or from other people.

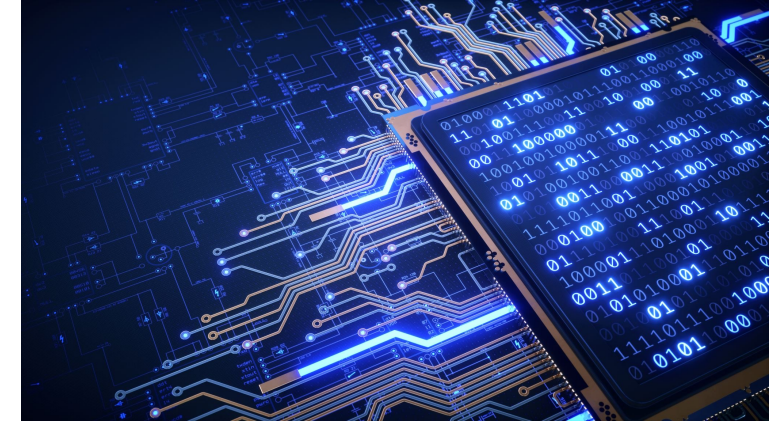
Examples:	Google	Twitter
	Facebook	Library
	Prop Tax Records	LinkedIn
	Court Records	DuckDuckGo
	Newspapers	Radio
	TV	Commercial databases

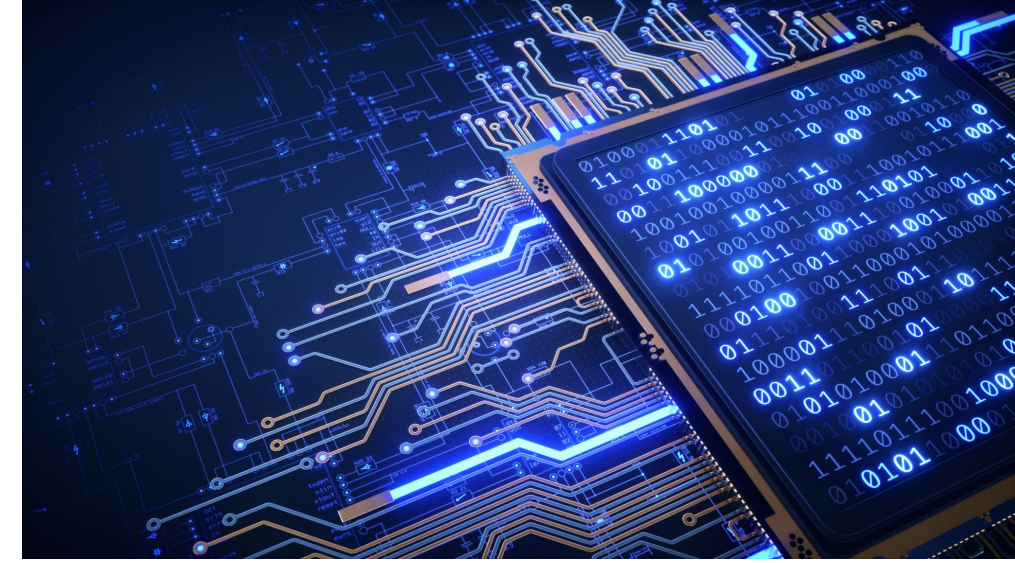
OSINT: Open-Source Intelligence



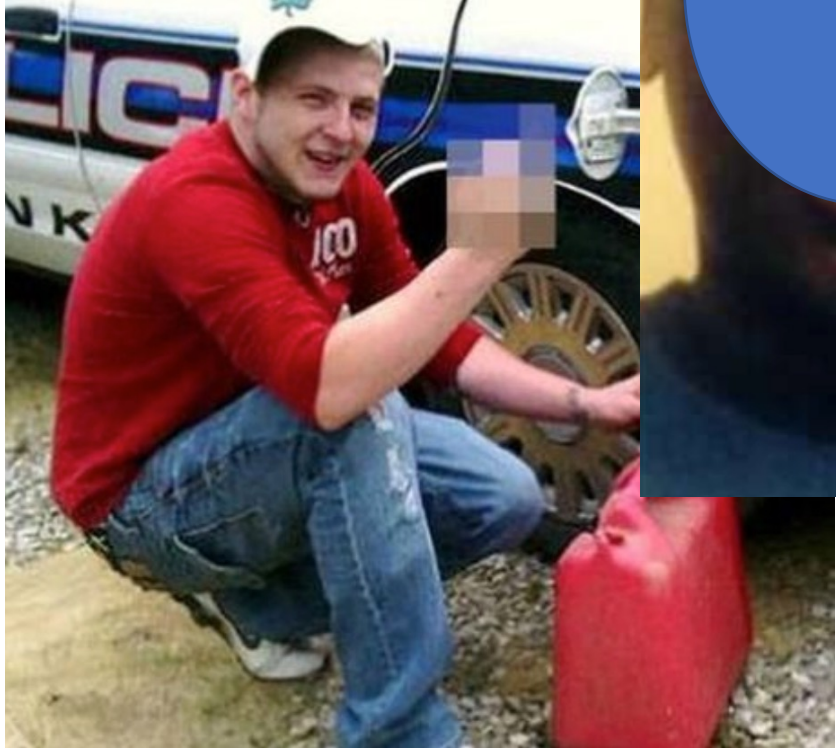
Search Engines	People	Social Media	Images	Online Communities	Classified Listings	Business Checks	Misc
Ask	Ancestry	Ashley Madison	Bing Image Search	Angelfire	Amazon	Angie's List	Airbnb
Bing	AnyWho	Blogspot	Flickr	Boardreader	American Listed	Better Business Bureau	Athlinks
Dogpile	Black Book Online (public)	Chatty Heads	Instagram	Deviantart	Clickooz	BizNar	CourtReference
DuckDuckGo	BeenVerified	Classmates	Photobucket	Domain Tools	Craigslist	Bloomberg Businessweek	dnsLytics
Google	Canada 411	Facebook	SmugMug	Google Groups	eBay	CLEAR	DomainTools
Gigablast	InfoBel	Flickr	TinEye	IMDB	Hotfrog	Corporate Information	EarthCam
Mozbot	Intelius	hi5	Webshots	Nexopia	Kijiji	Dun & Bradstreet	Fold3 (military records)
Oscobo (UK-based)	MelissaData	Instagram	Yandex Image Search	Omgili	Manta	Foursquare	Terrorism Databases
Qwant	PeekYou	LinkedIn	YouTube	Quora	PicClick	Guidestar	National Sex Offender Registry
Sputtr	Phonebook of the World	Match	What is TinEye?	Reddit	SaleSpider	Industry Canada	PageGlimpse
StartPage	Pipl	Meetup		Tumblr	Used	InsiderPages	Public Records
Yahoo	Public Records	MyLife		Typepad	VendAnything	Leadership Connect	Snopes
Yandex	Snitch.name	MySpace		Who.is		Open Corporates	State Sex Offender Registry
	Spokeo	OurTime		WordPress		Orbis Directory	U.S. Federal Inmate Lookup
	ThisNumber	Pinterest		Xanga		PIBuzz	Wayback Machine
	UserSearch	ReverbNation		Yahoo Groups		SEC Company Search	Webboar
	Webmii	Sportstats				Yelp	Whoisology
	ZabaSearch	Tagged					
	ZoomInfo	Trendsmap					
		Twitter					
		WordPress					
		YouNow					
		YouTube					

OSINT: Open-Source Intelligence





Did They REALLY Post That? Yes, They Did





Oklahoma mom tried to sell two kids on Facebook for \$4,000 so she could pay boyfriend's bail

Via ebaumsworld.com

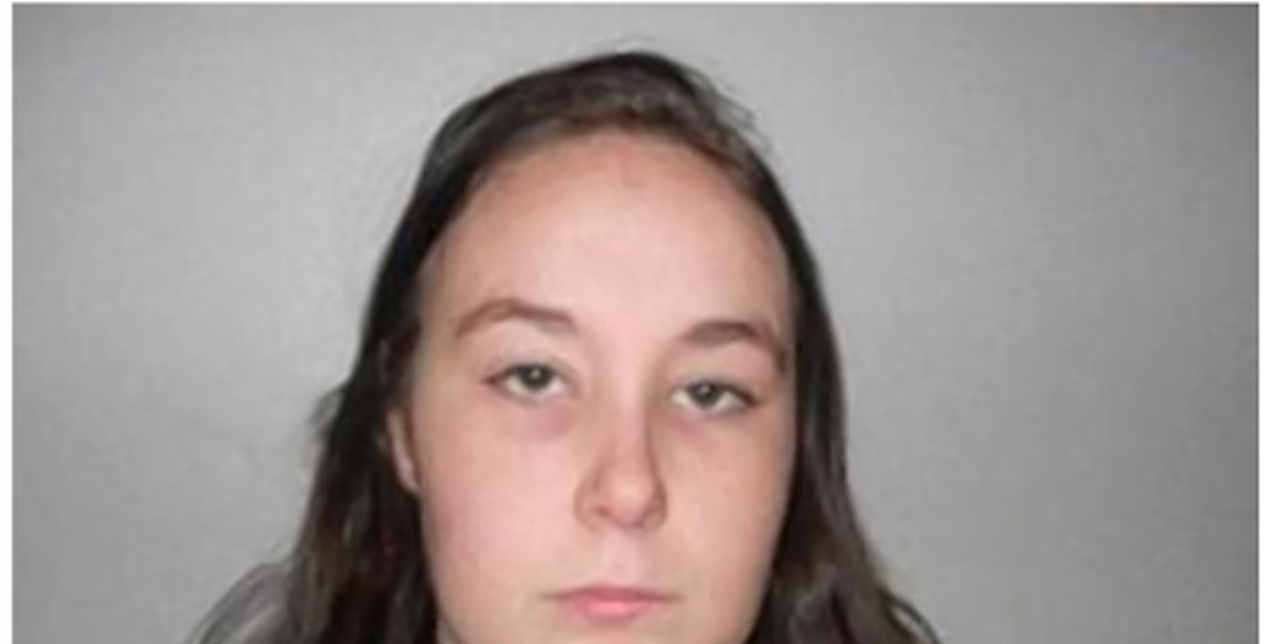
Misty VanHorn, 22, is accused of offering up for sale online her two babies, one who is 2 years old and the other who is 10 months old.

Comments (47)

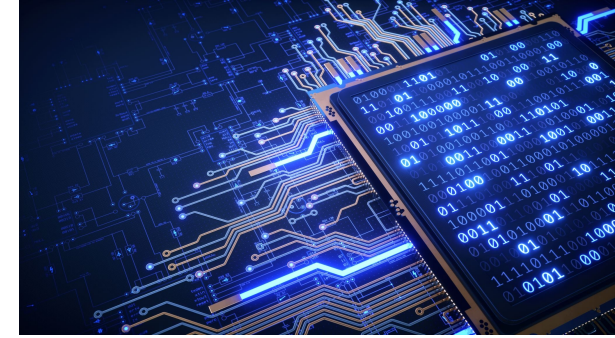
BY LEE MORAN / NEW YORK DAILY NEWS

TUESDAY, MARCH 12, 2013, 8:36 AM

f 2K t 49 p 0 g +1 s in dig e mail print



Web Tidbits – Where is it?



WWW

Websites are indexed through web service providers so they can be searched and accessed by public.

Deep Web

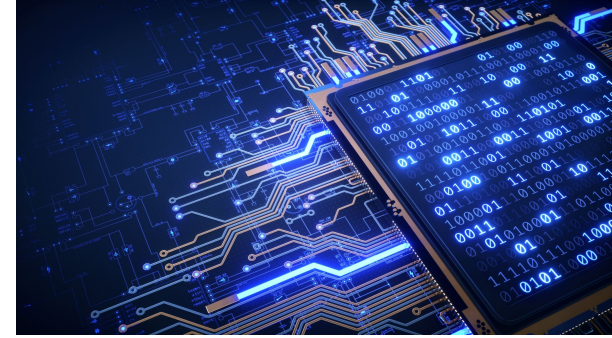
Websites are NOT indexed through web service providers but may be legit. Example may be web pages that companies use for internal purposes. Sites can still be accessed if the site address is known.

Dark Web

Websites are NOT indexed and intentionally hidden. May require TOR browser to view.

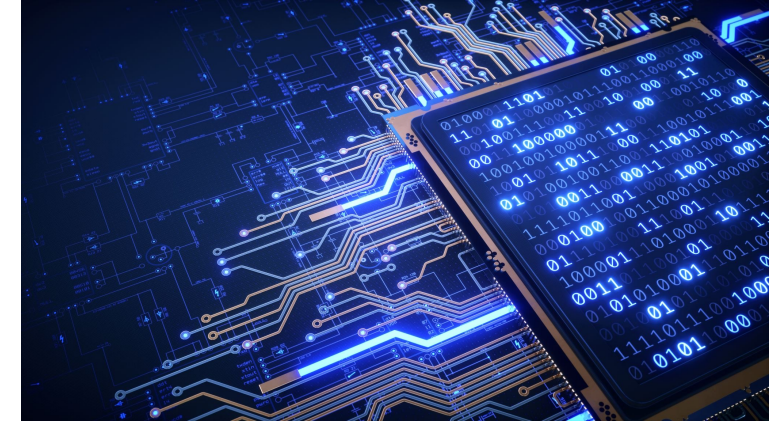
- Safe communications
- Adds additional layer of security
- Associated with illegal activity because of security, but used legitimately as well
- Over 20 billion data points for sale on Dark Web – think ID theft.

How to Protect Your Data



1. Shred documents with PII including Utility Bills
2. Password Habits
3. Security Questions
4. VPNs (Maybe)
5. Diligence with emails (Phishing and other scams)
6. Know your website

Passwords



85% of breaches are due to human element, like phishing or weak and reused passwords...

65% of people use the same password on multiple accounts¹

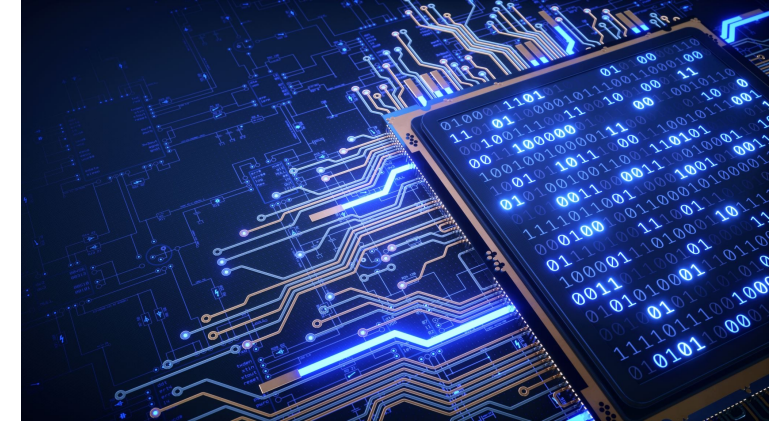
User ID:

Password:

¹<https://www.lastpass.com/resources/learning/how-secure-is-my-password>

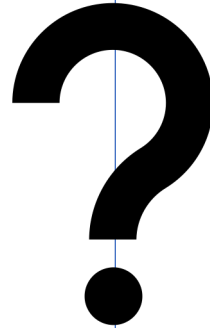
Passwords

Conventional Wisdom is Changing...



Conventional Thinking...

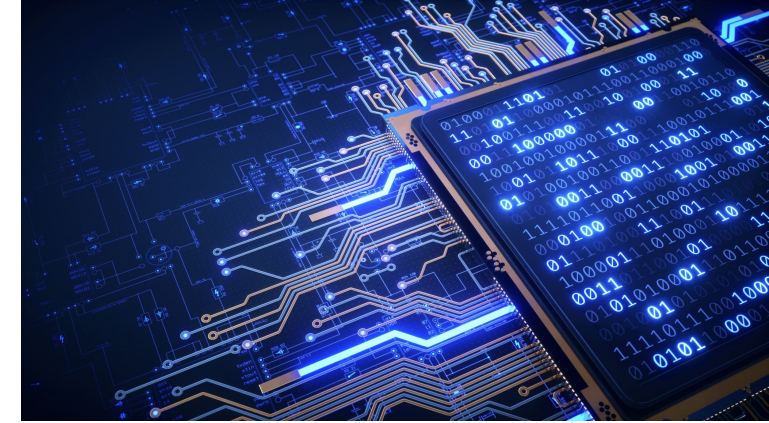
Change passwords often



Revised Thinking...

Create a **STRONG, UNIQUE** password for each account, and leave it alone


Passwords



Password Do's	Password Don'ts
Each account should have its own password	Use same password for all accounts / Reuse passwords
- Use lower, upper, numbers, and special characters	Use known dates / names such as birthdates
- Use long phrases or random words	Write them down in a place where people can see them
- Unique, Private, Random, No Patterns	Use PII
Change passwords regularly – or not (changing views)	Don't share passwords (Netflix)
Use MFA with passwords	Use security questions that have available answers
Password Vault	

Passwords

Sample Passwords

 1234 MyStreet

 Kim1925

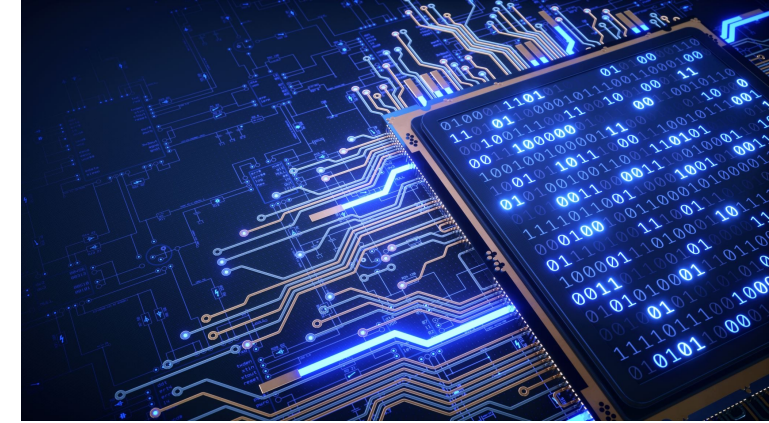
 Snickers2002

 derrick-forsake-fadeout-AXIOLOG-sums-clam-quackery

String of random words

 y3V7Ja*VyzNpggkNtwW@ctfKtWg_JovXUbiyoPK

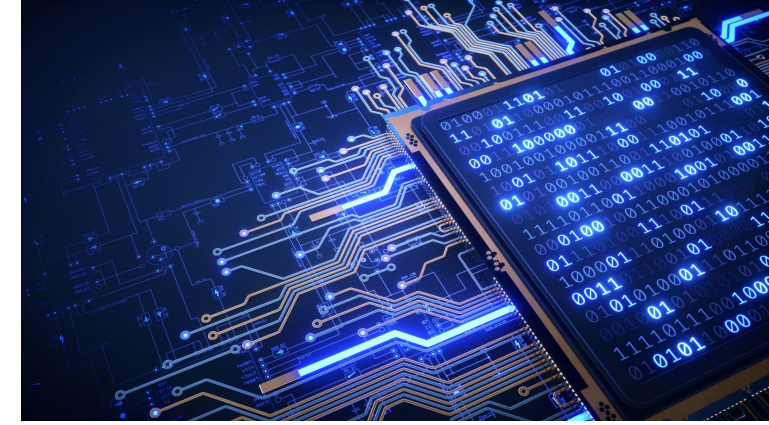
String of random characters

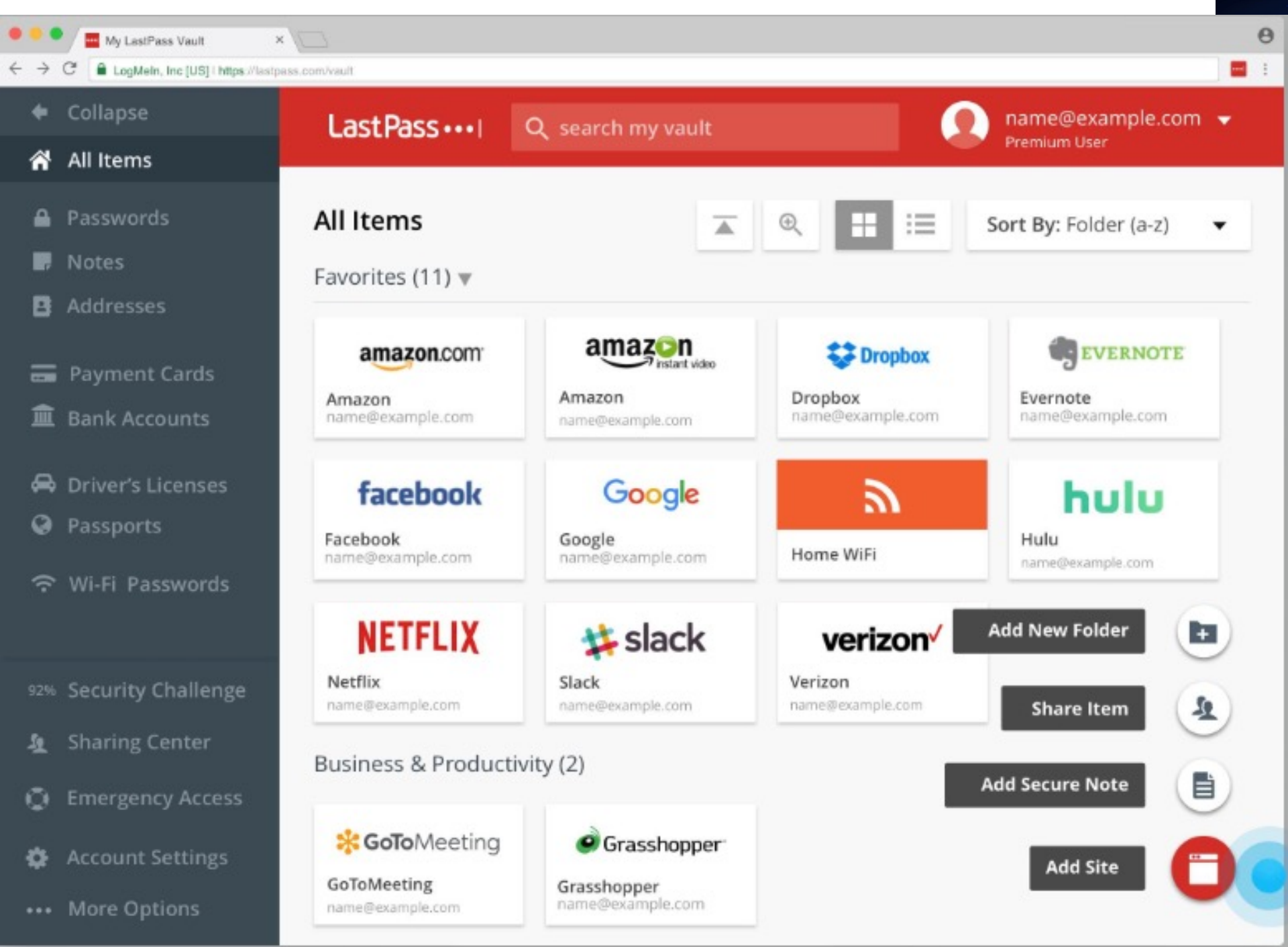


Password - Vaults

Offer Convenience and Security



- Stores Passwords in one place
- Can ensure you are on the right website
- Generates long passwords that are random
- May be local or on their server
- Some share across devices
- Some have private and shared folders
- Features and cost will vary
- iCloud Keychain (iOS and Windows, synchs across)






Password Vaults


[◀ Back](#)


CtJnFec%X@zj%PP7iv0ptViUnh6H#5L4  


SHOW HISTORY

Password length

32 

☐ Easy to say 

☐ Easy to read 

☒ All characters 

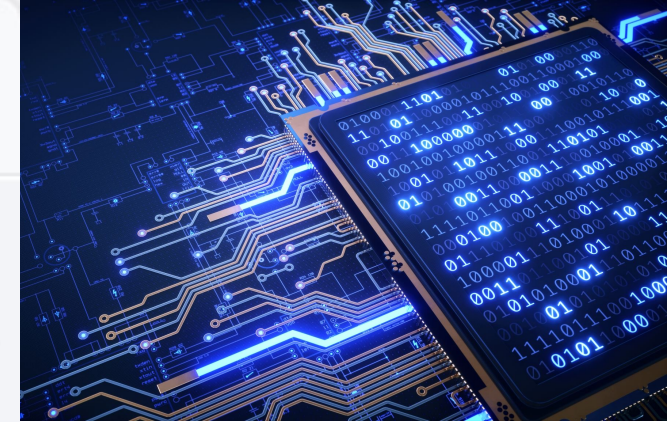
☒ Uppercase

☒ Lowercase

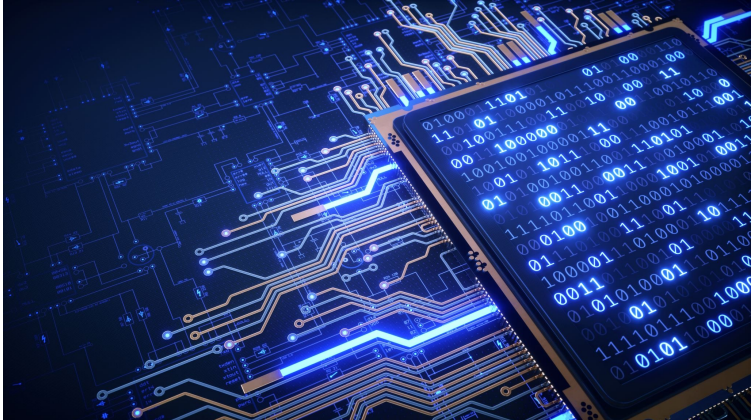
☒ Numbers

☒ Symbols


FILL PASSWORD



Password Security Questions



Lifelock by Norton helps detect identity threats



Suzanna Shaw New York, NY
Senior Product Designer

Endorsement Rating
4 ★★★★★

Profile Information


DOB:	July 27 1979
Social Security #:	455-33-18011
Phone:	+1 123 456 7890
Address:	234 Maine Street Anyplace, NY 192011
Email:	hello@suzysinaw.com

Employee Profile

Unalla Inc. New York [View Profile](#)

Unalla Inc. New York 110035



Suzanna Shaw  New York, NY
Senior Product Designer

Endorsement Rating
4     

Profile Information

DOB: July 27 1979
Social Security #: 455-33-18011
Phone: +1 123 456 7890
Address: 234 Maine Street
Anyplace, NY 192011
Email: hello@suzyshaw.com

Employee Profile

Voilla Inc. New York
Bridgeway, NY 110038

Location

Scroll for details

Play (k)



0:00 / 0:15



Password Security Questions

Here's an idea...

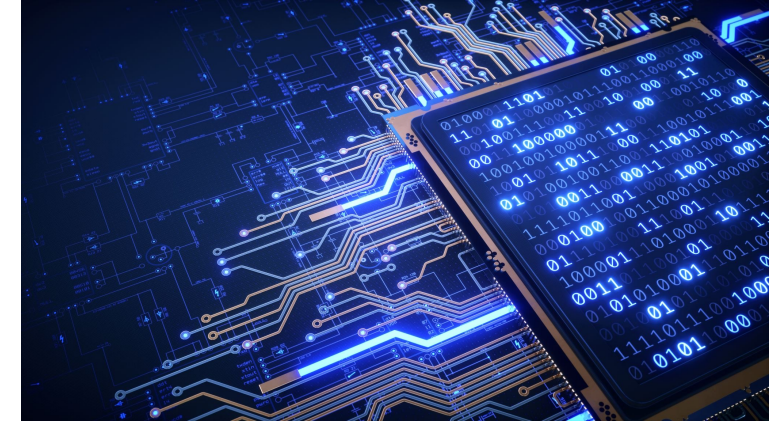
Use your password vault to
generate a random password for
your security question

Security Question

What's your mother's maiden name?

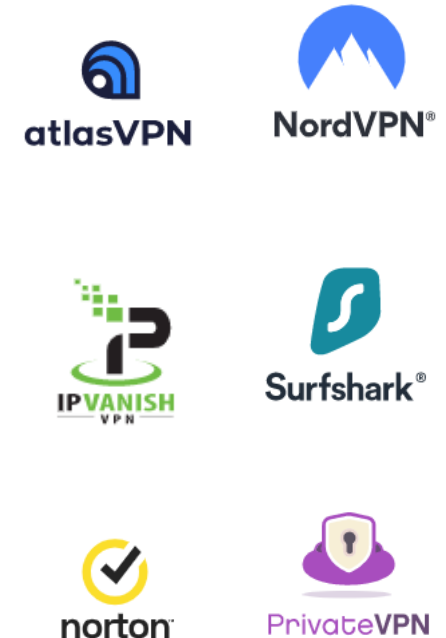
^79J7h6Hg\$gJi(k

Virtual Private Networks (VPNs)



Purpose: Allow secure communications from one computer to another over the internet

- Used by many companies to secure remote connections
- Available for personal use
- The user connects to a secured server
- Connection is encrypted
- All traffic to and from is “hidden” from hackers



VPNs

How a VPN works

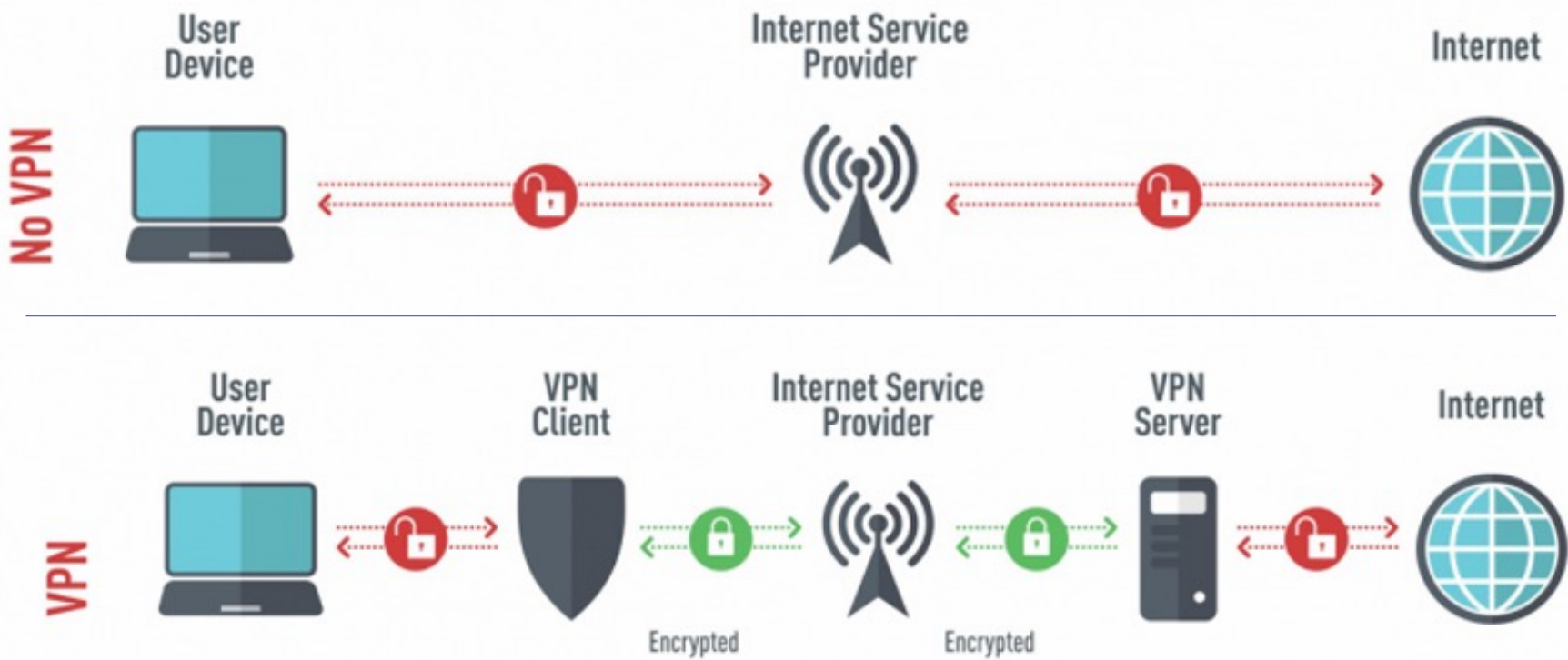
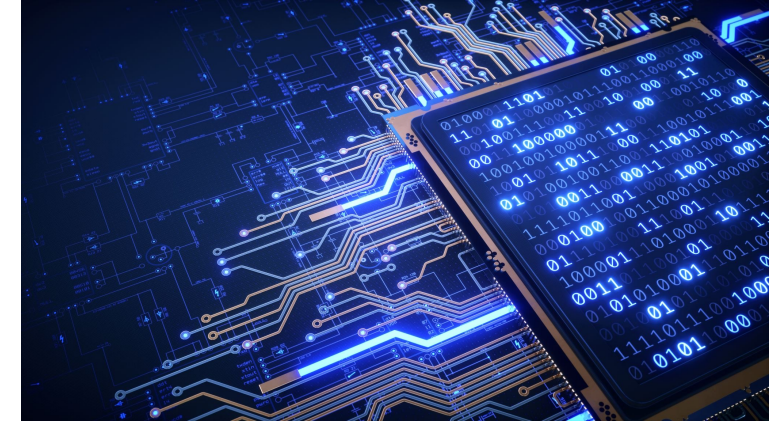


Image source: https://www.yellowstonecomputing.net/uploads/2/2/1/6/22165724/how-a-vpn-works-intographic-730x484_orig.png

VPNs

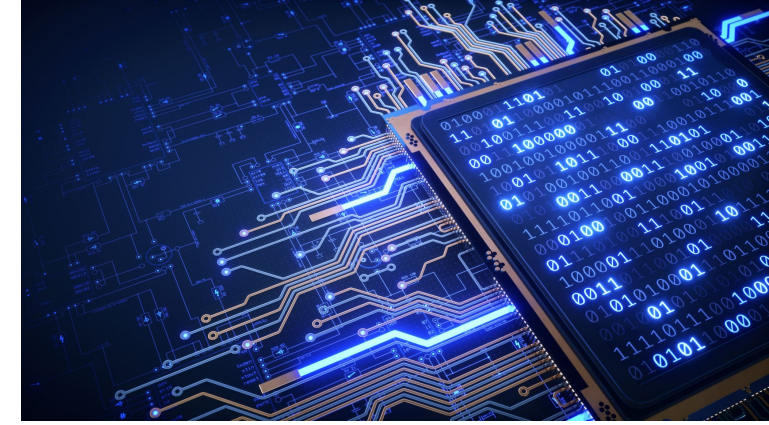


Advantages:

- All communications are encrypted and hidden from hackers
- Keeps online activity private
- You can make your connection appear to be from anywhere
 - Great for the consumer, but...
 - Fraudsters can mask their true location

Be aware: Some VPN services keep logs

Virtual Private Networks (VPNs)

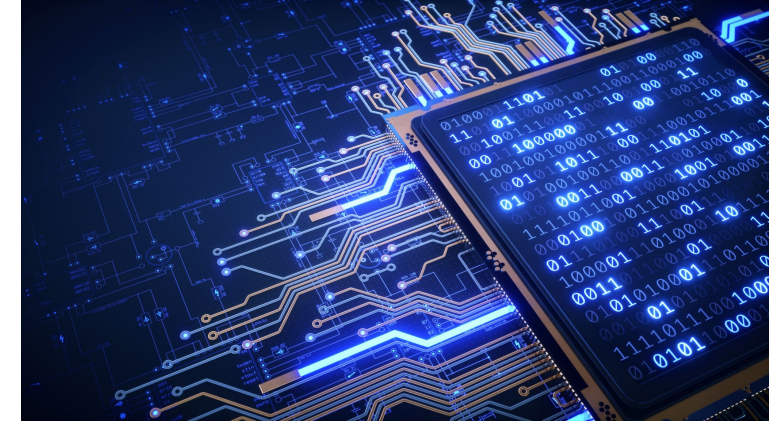


Opinion is Mixed: There isn't a consensus on usefulness depending on security of the website itself.



VPNs

WARNING



People in other countries may appear to be in the U.S.

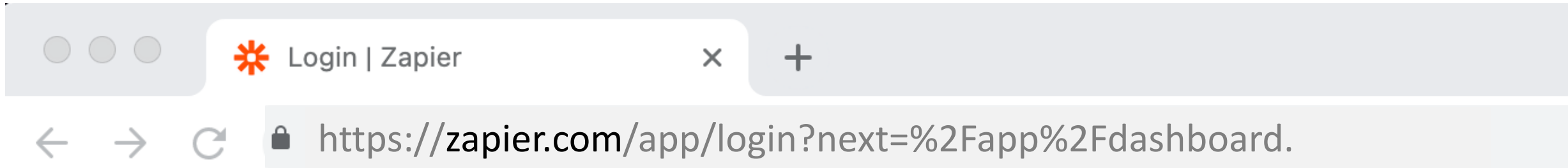
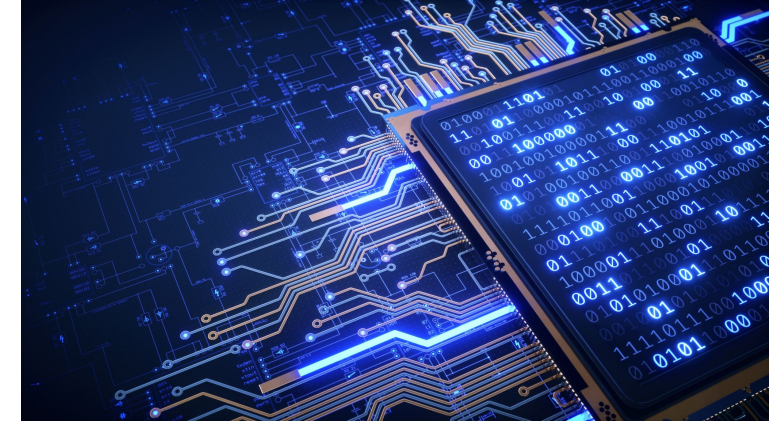
The IP address being collected on your insurance application may be masked or from a VPN.

What are the implications of this for your company?

Diligence has solutions for this...

VPNs

Know your website



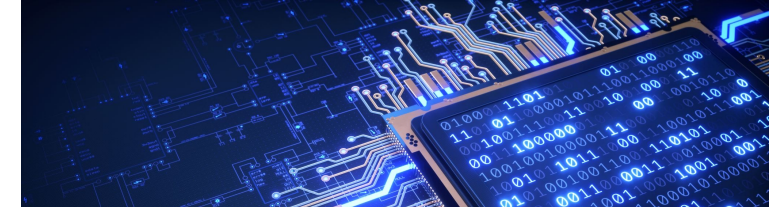
The bolded part of the address is the domain

The lock shows that the site is using SSL certificates to encrypt data in transit.

The lock does NOT mean:

- the site is trustworthy,
- the site stores data securely,
- etc.

Beware of Typos and False Sites



🔒 <https://blog.goggle.com>

ⓘ <http://goggle.com>

Welcome to the
Goggle.com Data Diary

GOGGLE: /'gägəl/ – verb
1. look with wide open eyes, typically in amazement.

Goggle was the closest Electoral College predictor
among established pollsters

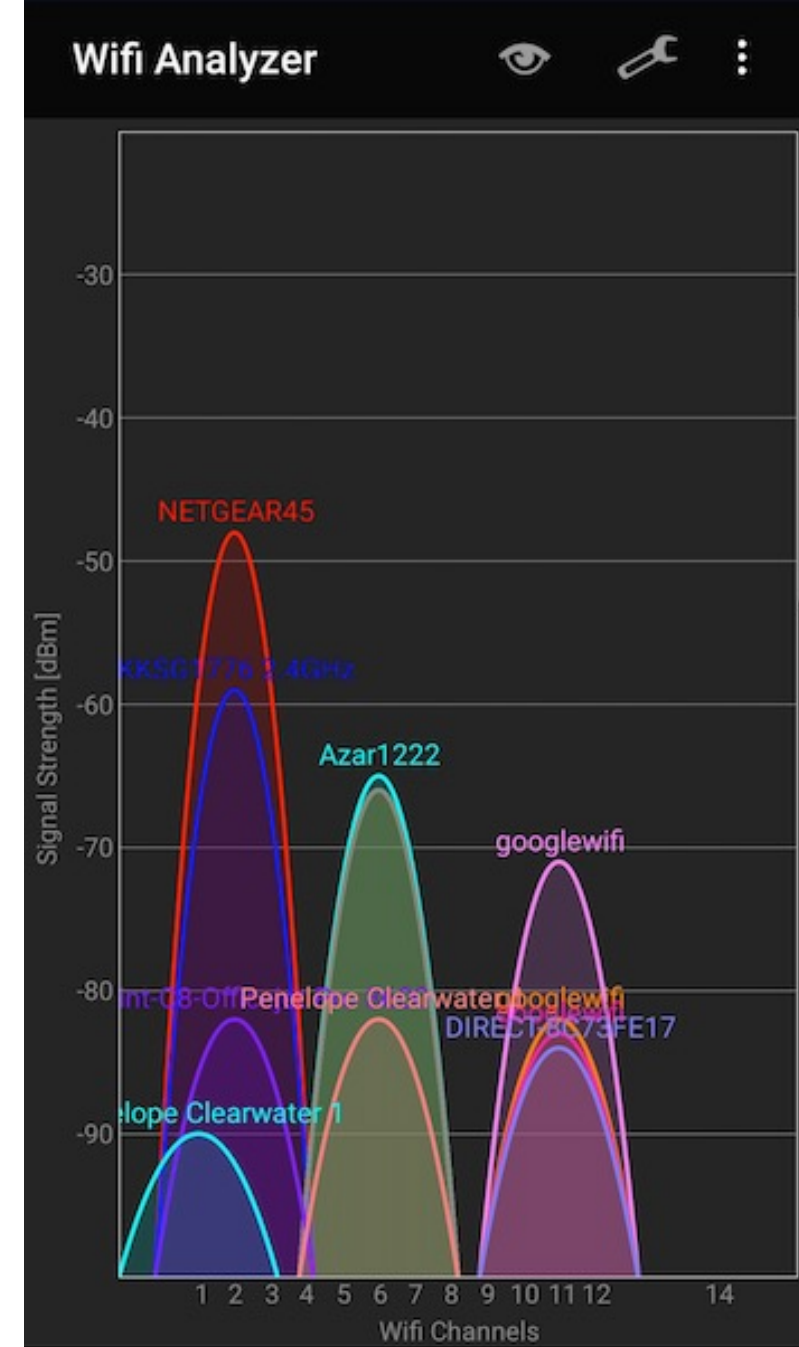
Error in Democratic and Republican vote predictions

← Democratic vote error →

WiFi Signals

Be mindful of your WIFI signal name...

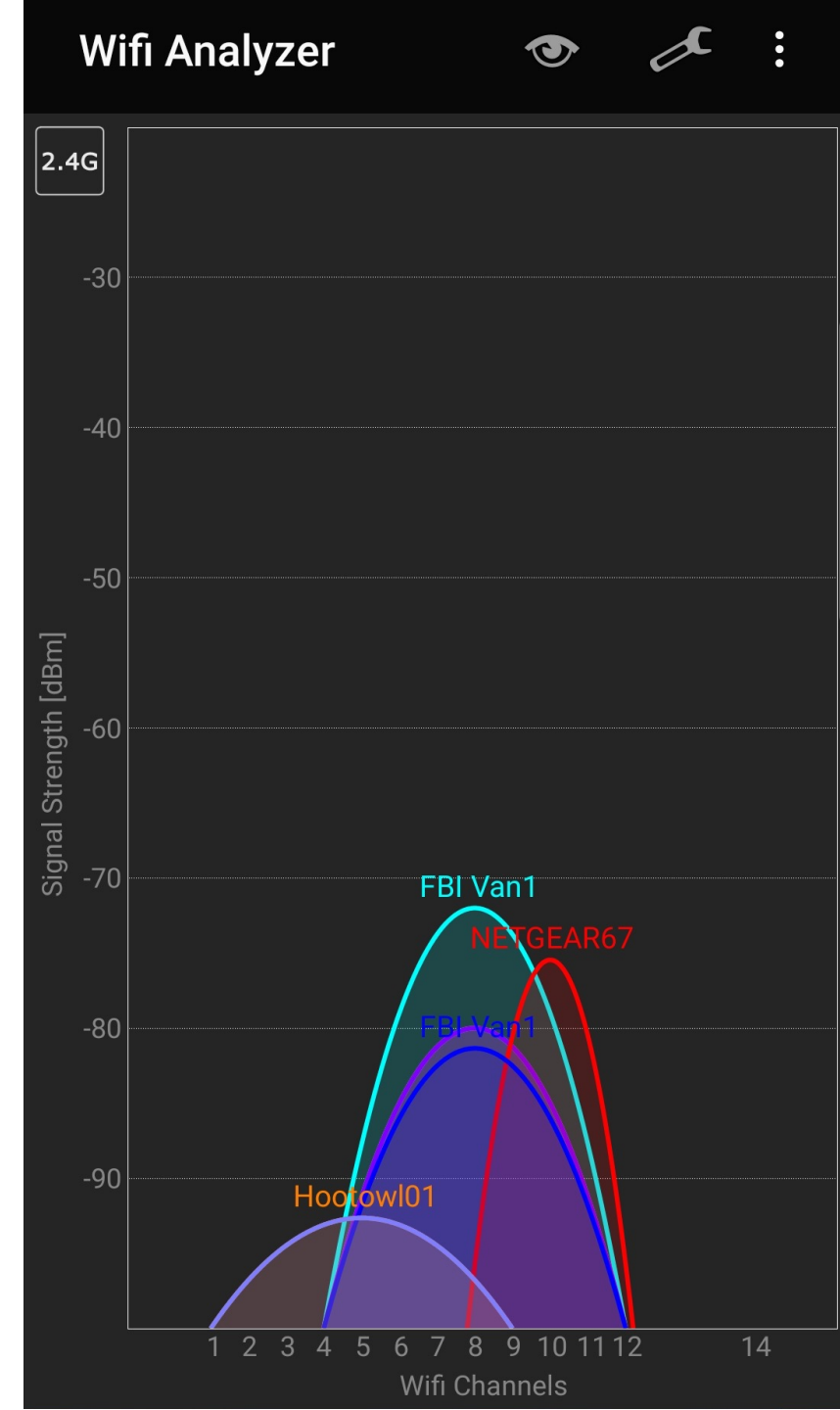
- Make sure you WIFI is password protected
- Use an obscure name - we have used this to locate "dead" people on the lam.
- Use may be liable for your internet used for illegal purposes



WiFi Signals

Be mindful of your WIFI signal name...

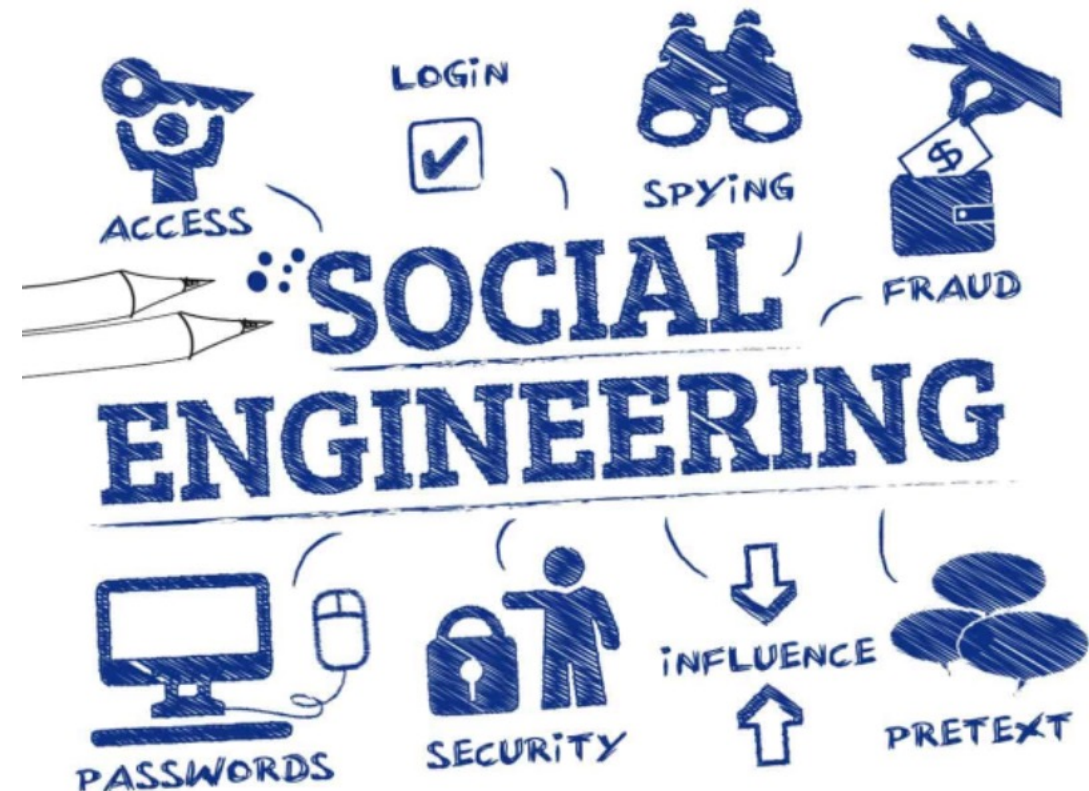
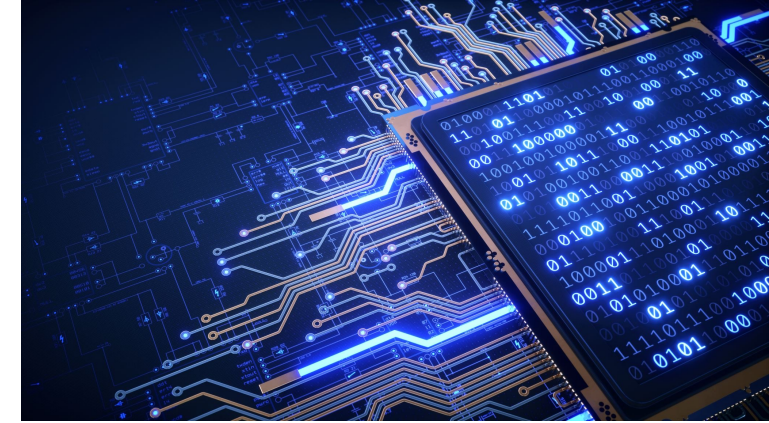
- Make sure you WIFI is password protected
- Use an obscure name - we have used this to locate "dead" people on the lam.
- Use may be liable for your internet used for illegal purposes



Social Engineering

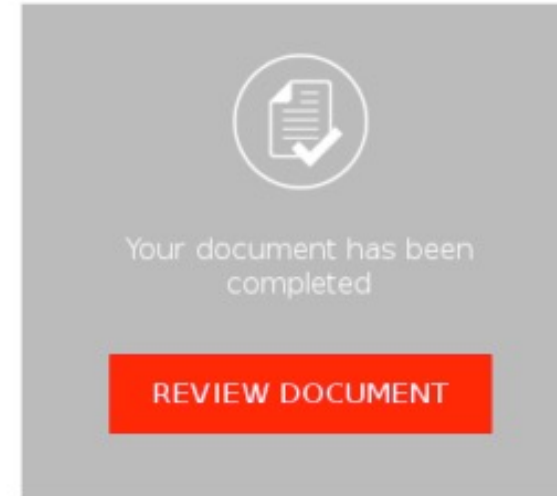
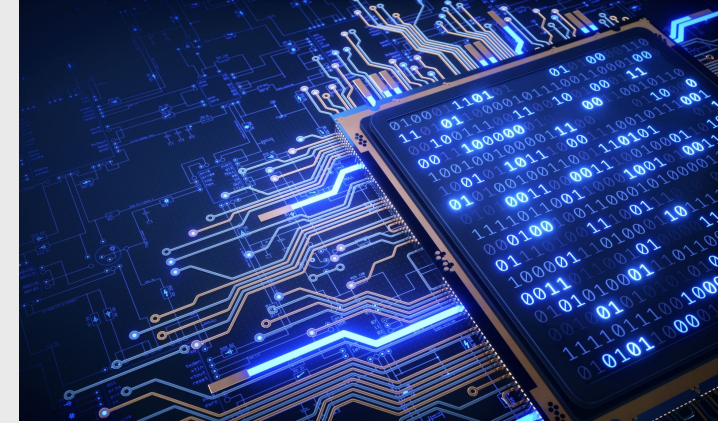
“a method of gaining unauthorized access to a computer system in which the attacker deceives victims into disclosing information or convincing them to commit acts that facilitate the attacker’s intended scheme.”

(2018 Fraud Examiners Manual, p 1.1406)



Social Engineering

- Phishing
- Spear Phishing
- Whaling
- Rock Phishing
- Pharming
- Vishing
- BEC



All parties have completed
- Accounting Invoice
Document Ready for Signature.

Please review and sign your
Accounting Invoice
via DocuSign by clicking on the
"Review Document" button above.
Signing will not be complete until you
have reviewed the agreement and
confirmed your signature. Please make
sure to fill out the TaxID if you are
requesting for credit terms. Please let us
know if you have any questions. Thank
you.

Powered by 

From: Joe Smith
To: Troy Foster
Subject: WebMail Migration

 Attachment – Webmail_Migration.pdf

Troy,

This is to inform you that we are in the processing of migrate our email infrastructure to the Windows 2003 platform, which includes an e-mail.

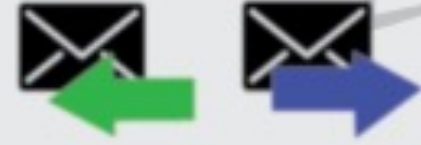
Attached is a document outlining the benefits of the migration we **request you to enter your Windows password before 8 PM** on Tuesday. **Failure to do so will result in being locked out of your email account!**

Please click [here](#) to update your password.

Thank You,
John Smith

Attachments

When an attachment comes from someone you don't know or if you weren't expecting the file, make sure it's legitimate before opening it.



Log-in Pages

Spear phishers will often forge login pages to look exactly like the real thing in order to steal your credentials.

Links

Roll your mouse pointer over the link and see if what pops up matches what's in the email. If they don't match, don't click.

**If you see something,
say something!**




Report suspected phishing emails to the information security team

There's issue with your American Express account

 American Express <administraciones@pentagon-seguridad.cl>
To

[Reply](#) [Reply All](#) [Forward](#)

Fri 11/8/19

 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.

Review Your Information.



Due to recent activities on your account, we placed a temporary suspension until you verify your account.
You need to review your information with us now on 11/8/2019 10:28:38 AM.

American Express <administraciones@pentagon-seguridad.cl>



[Click here to review your account now](#)

Hover over to find URL

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

American Express Company

Source:

<https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/>

RE: Your account has been frozen. *84654

Coinbase (nick-carlson@p4ncen.onmicrosoft.com)

To: you Details ▾

Coinbase

Coinbase

Verify your account information

Due to the upcoming new regulation in the United States on cryptocurrency, all Coinbase users are required to verify their account. Please provide the documents required for verification purpose. You will not be able to verify your identity from the Coinbase App.

Verify My Account

If you did not verify your Coinbase account, it will be closed and you need to contact our support to reopen the account.

©Coinbase2021

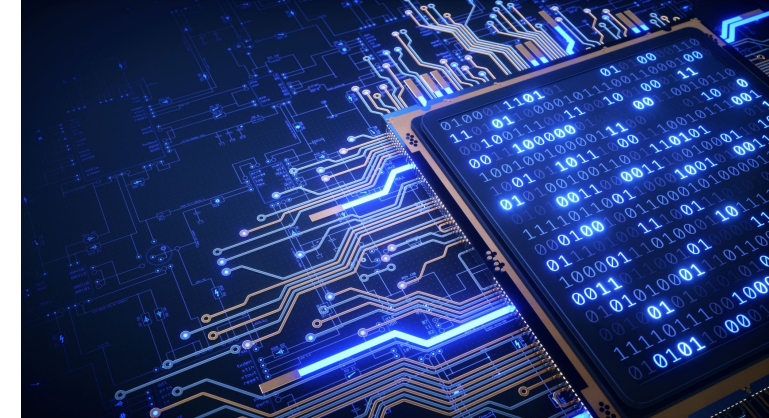
100 Pine Street, Suite 1250 | San Francisco, CA 94111 | United States
1-888-908-7930

Wrong account number

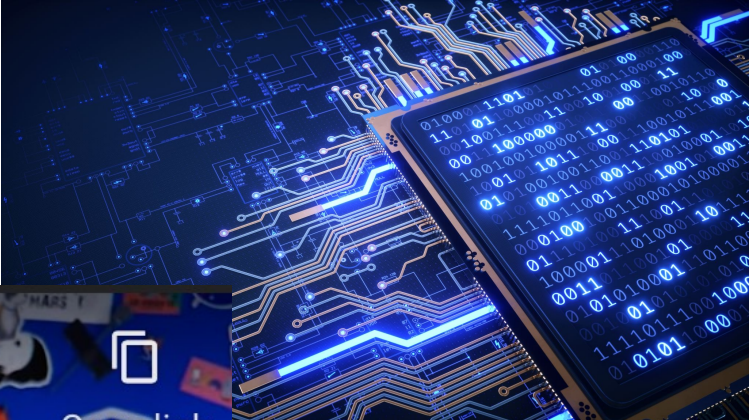
Nick-Carlson@p4cen.onmicrosoft.com

<https://grco.de/bcvKY0>

Looks like a legit address



Glitter Bomb – Mark Rober

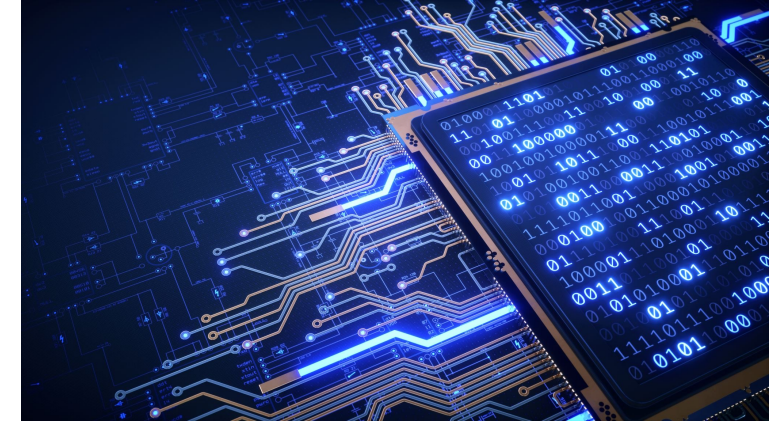


DOS Attacks

Distributive Denial of Service attacks that make a machine or network unavailable by either crashing the services flooding the target with requests in an attempt to overload the system.

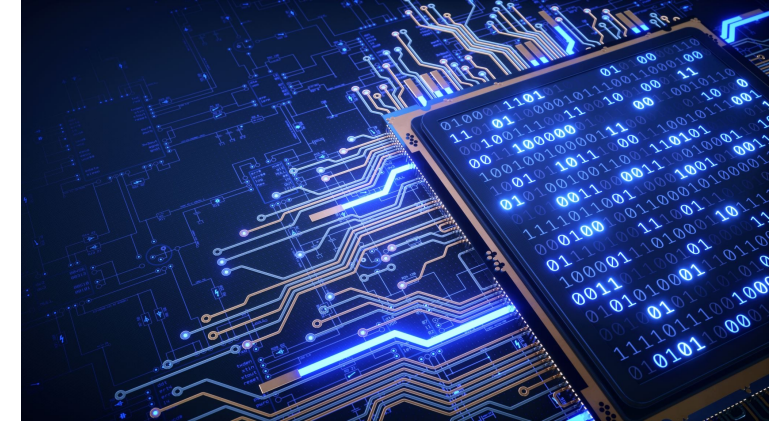
Mitigants:

- Software
- Increased bandwidth
- Good "cyber hygiene" eg. passwords, authentication practices, etc.
- Know your network traffic
- Move to the cloud



DDOS Attacks

Distributive Denial of Service (DDOS) attacks that make a machine or network unavailable by either crashing the services flooding the target with requests in an attempt to overload the system.



Case Study:

While not a true DOS / DDOS attack , we recently had a client report that their on-line application system was overwhelmed by bots submitting applications. Their IT area was able to detect it after about 1,000 applications were loaded. Know your Cyber Traffic, change passwords, watch for phishing, keep strong authentication practices (SSO, MFA, etc.)



THANK YOU – Let's Continue the Conversation !



Richard Marquez, CFE
Founder and President
Richard.Marquez@DIGroup-US.com
800-660-4202



Paul Marquez
VP, Business Development
Paul.Marquez@DIGroup-US.com
800-660-4202



Kevin C. Glasgow, ARA, FLMI, FLHC, CLU®, CFE
VP, Investigation Solutions
Kevin.Glasgow@DIGroup-US.com
(214) 316-0917



Erick Soeth, CFE
Investigations Manager
Erick.Soeth@DIGroup-US.com
800-660-4202



Lauren Loupot
VP, Operations
Lauren.Loupot@DIGroup-US.com
800-660-4202



Ashley Horton
Investigations Coordinator
Ashley.Horton@DIGroup-US.com
800-660-4202