

Robert@RobertSiciliano.com
<https://Protectnowllc.com>



**Defend From Hackers,
Attackers, and Thieves:**

Protect Your Data and Identity from Predators

1

Threats, Risk and **the Problem**

Threat: Ransomware

- ❖ The rising trend of ransomware attacks has created serious issues in the IT environment.
- ❖ Ransomware threats revolve around easily compromised operating systems, create vulnerabilities with significant ramifications.
- ❖ Preventing ransomware begins with Password Management



2

Making the Case To Prevent Breaches

Clorox products in short supply after cyberattack disrupts operations 9/18/23



A cyberattack at Clorox is causing wide-scale disruption of the company's operations, hampering its ability to make its cleaning materials

The company revealed in a regulatory filing that it detected unauthorized activity in some of its information technology systems in August.

protectnow

3

Protect Yourself From Evil Cyber Scams To Prevent Fraud



4

Prevent Data Breach 101

"IT personnel, Local Police, State Police, FBI and U.S. Secret Service" by 11am with guns!

1. Consistent cyber security training in place that includes phish sim and remedial training?
2. Strictly enforced complex passwords changed every 60 days?
3. Multi factor authentication for internal, cloud and vpn access?
4. Automated systems for updating operating systems?
5. Highly restrictive website and content filtering defined by the core business function?
6. Do you utilize Endpoint Detection and Response (EDR)?
7. Are you considering Extended Detection and Response (XDR)?
8. How many are leveraging artificial intelligence looking for networking anomalies?
9. How many perform monthly random data, bare metal, and virtual machine restorations as part of BDR (back up disaster recovery) validation?
10. How many can restore any platform or data point on premises or in cloud?



5

Managed Security Service Provider

Third-party providers offer managed security services for the oversight and administration of a company's security processes. Managed security service providers (MSSPs) conduct services either in-house or remotely, typically via the cloud. MSSPs offer a wide range of security services, from setting up infrastructure through security management or incident response. Source <https://digitalguardian.com/blog/what-are-managed-security-services-why-organizations-hire-managed-security-service-providers>

Common services include

- ❖ cybersecurity monitoring and management
- ❖ managed firewall
- ❖ intrusion detection
- ❖ virtual private network
- ❖ vulnerability scanning
- ❖ anti-viral services
- ❖ spam blocking
- ❖ provide 24/7 services to security posture
- ❖ system changes, modifications and upgrades
- ❖ reduce the number of operational security personnel
- ❖ reduces hiring, training and retaining
- ❖ vCISO:



6

Cyber Security Insurance



Direct Monetary Losses From Theft

- Losses due to cyber extortion, such as DDoS blackmail or ransomware.
- Losses related to mitigating and investigating an incident, including computer forensics and consultants.
- Losses due to downtime, which includes customer revenue, worker productivity, and increased operational costs.
- Loss or damage to data or software, including costs associated with replacing, patching, recreating, or restoring things to the way they were before the incident.
- Expenses associated with remediation activities, such as new control purchases, application design enhancements, monitoring, supporting staff, etc.
- Expenses associated with customer breach notification, including public relations, legal consultation, postage fees, and telephone support.
- Expenses associated with customer compensation because of the incident, including credit monitoring, service level agreement penalties, refunds, and contractual violations.
- Expenses related to liability exposures due to the incident, such as investigator fees, legal defense costs, civil court damage costs, and third-party liability exposures

protectnow

7

Making the Case To Prevent Breaches

27 billion records exposed in the first half of 2020

The latest Data Breach Report from Risk Based Security shows 2,037 publicly reported breaches from January to June.

The number of records exposed between January 1, 2020 and June 30, 2020 reached 27 billion, exceeding the total number of records exposed during the entirety of 2019 by more than 12 billion.

protectnow

8

Making the Case To Prevent Breaches



More than 40 billion records exposed in 2021

According to the research from Tenable's Security Response Teams, they found a considerable increase in breach incidents. The research also found that healthcare and education remain the most-targeted industries worldwide.

Ransomware and attacks on vulnerabilities remained top reasons for the data breaches. With breaches at an all time high, your organization may be wondering how you can improve application security for your organization.

protectnow

9

Making the Case To Prevent Breaches



146 billion digital records will be stolen by 2023, Juniper Research predicts

The number of digital records stolen by cybercriminals is expected to increase by 175% from 12 billion in 2018 to 33 billion in 2023

protectnow

10

Making the Case: Equifax Breach 146 Million Customers!

**Equifax Breach Affects
146 Million Customers**



protectnow

11

Stolen Raw Data **For Sale On The Dark Web**

**10 billion passwords have been leaked
on a hacker site. Are you at risk?**

RockYou2024 leak is a compilation of real-world passwords used by individuals all over the world. Revealing that many passwords for threat actors substantially heightens the risk of credential stuffing attacks

Credential stuffing is when hackers take information, such as passwords, from one data leak and attempt to log onto other websites

protectnow

12

Prevent Breaches: Password Management

AN ASTONISHING 773 MILLION RECORDS EXPOSED IN MONSTER BREACH



772,904,991 unique email addresses, over 21 million unique passwords, all recently posted to a hacking forum.



13

Stolen Raw Data For Sale On The Dark Web

Index of /combos/		
../	25-Aug-2021 03:05	-
Mail Access/	25-Aug-2021 03:05	-
Worldwide/	25-Aug-2021 02:44	48824543
1.5M Combo [Email-Pass].txt	25-Aug-2021 02:43	40979306
1.25M [By Al-Caesar] HQ Combo Private Gold Prem..>	25-Aug-2021 02:43	3269660
100K EmailPass High-Quality GamingStreamingVPN.txt	25-Aug-2021 02:44	4801413
142K Fresh HQ Private Combos Good For Everythin..>	27-Aug-2021 04:54	5148639
148k hq US Domain Combos Private.txt	25-Aug-2021 02:44	3841929
180k userpass.txt	25-Aug-2021 02:43	6350147
186K private mail-pass(Vpn,Spotify,Minecraf,Net..>	25-Aug-2021 02:43	11696722
1M combo (Email_Pass).7z	25-Aug-2021 02:44	32760685
1M combo [Email-Pass].txt	25-Aug-2021 02:44	91590379
2,821,227 Combined Combos.txt	25-Aug-2021 02:44	6909956
211K High Quality Combolist.txt	25-Aug-2021 02:44	17113356
476K High Quality Combo.txt	25-Aug-2021 02:43	134646
4k valid HQ COMBO Uplay- Netflix-Sky-Fortnite-S..>	25-Aug-2021 02:44	3586151
5M - Gaming - StinkyBathWater - 1 - 4.txt	25-Aug-2021 02:44	3080465
621K+HQ+COMBOLIST+FRESH.rar	25-Aug-2021 02:44	24525111
760k combo [Email-Pass].txt	25-Aug-2021 02:44	9151421
794k Combo Email-Pass (Netflix, Spotify, Hbo, A..>	25-Aug-2021 02:43	26233442
794k Combo [Email-Pass].txt	25-Aug-2021 02:44	9151421
794k Ultra HQ Netflix Spotify Fortnite Gaming P..>	25-Aug-2021 02:43	15829601
AUS-SemiPrivate.txt	25-Aug-2021 02:44	36222204
private_zabugor.txt		



14

'Shark Tank' star Barbara Corcoran loses \$400k in email scam!

'Shark Tank' star Barbara Corcoran loses \$400,000 in email scam

The 70-year-old mogul's bookkeeper received an email about an invoice to approve a payment on a real estate renovation, which isn't at all uncommon given how many real estate deals she works with on a daily basis.

The detail that no one caught was that my assistant's email address was misspelled by one letter, making it the fake email address set up by the scammers," Corcoran explained.



15

Check If Your eMail/Password Has Been Breached

Cyber Security Awareness Check

Has your personal or organizational security been breached? Get an instant answer.

Check if your email has been breached

EMAIL CHECKER

Check if your password has been breached

PASSWORD CHECKER

Protect Now does not capture, store or share ANY information you provide to these checkers.

16

18

Password Management **Security**

- Social engineering
- Phishing
- Password re-use
- Insecure/weak pass
- Password managers
- Two step verification
- NO PASSWORDs



1:01 PM

Hi Rob,

I'm not sure if you saw what had happened on my FB Page last night, but someone stole my cell phone while I was at a concert, and posted all of my naked pictures off of my phone and posted them to my wall.

They were up there for hours. 😞

Is there anyway you could help me find out who it was?

Email Security: Forwarding Settings

Settings

General Labels Inbox Accounts Filters and Blocked Addresses Forwarding and POP/IMAP Add-ons Chat Labs Offline Themes

Forwarding:
[Learn more](#)

☒ Disable forwarding
☐ Forward a copy of incoming mail to and and

Tip: You can also forward only some of your mail by [creating a filter](#)

POP Download:
[Learn more](#)

1. Status: POP is enabled for all mail that has arrived since 5/23/09
☐ Enable POP for all mail (even mail that's already been downloaded)
☐ Enable POP for mail that arrives from now on
☐ Disable POP

2. When messages are accessed with POP

3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)
[Configuration instructions](#)

IMAP Access:
(access Robertsiciliano.com Mail from other clients using IMAP)
[Learn more](#)

Status: IMAP is enabled
☒ Enable IMAP
☐ Disable IMAP



21

Protect Yourself From Social Engineering Scams

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.

THERE IS NO PATCH FOR HUMAN GULLIBILITY

- | | |
|--|---------------------|
| Lose something | Thieves pose as You |
| Gain something | Spouse |
| Fear/greed | Bill collector |
| "Principles of Influence and Persuasion" | Bank |
| email | Utility |
| telephone | Fellow employee |
| in person | Government agency |



22

Prevent Breaches: Password Management

Alert: Uber's internal systems hacked giving bad actor 'full access'



Full access to Uber's systems

In addition, the hacker shared with cybersecurity researchers and *The New York Times* reporters the screenshots of the platform's internal systems, email dashboards, cloud storage, and Slack server, showing what seems like complete access to these systems.

According to a report by *The New York Times*, which first reported on the attack, Yuga Labs' security engineer Sam Curry, who communicated with the alleged hacker, said that:

"They pretty much have full access to Uber. (...) This is a total compromise, from what it looks like."

The report also said that the attacker claimed to have sent a text message to an Uber employee pretending to be a corporate IT person, convincing the employee to share a password that allowed the hacker to access the company's systems.

In addition, the attacker said he was 18 years old and had hacked Uber's platform because it had poor security, adding that Uber's drivers should have better salaries.

Beware of Romance Scams



An Imposter Claiming to Be an Astronaut Wooed a Japanese Woman Into Paying for a 'Return Ticket to Earth'

The space romance unfolded through Instagram, but the victim soon grew suspicious of the astronaut's monetary demands.

By **Pasant Rabe** | Monday 3:00PM | Comments (0) | Alerts



The scammer claimed he wanted to return to Earth and start a new life in Japan.
Illustration: Max Word/Stocktrek Images (AP)

A 65-year-old woman in Japan paid the equivalent of \$30,000 in a recent online scam that defied gravity. The con artist tricked the woman into believing he was a Russian astronaut who just couldn't afford a ticket back to Earth, local media in Japan reported.

The pair started corresponding through Instagram on June 28, and the scammer claimed that he was a cosmonaut on board the International Space Station (ISS). He blamed the poor cell service aboard the orbiting space station for his lack of communication at times. Things between them quickly escalated when the fake astronaut professed his love to her, claiming that he would want to marry her once back on Earth. Except there was one problem, he simply could not get off the ISS unless he had enough money for a ride back to Earth.

Beware of Romance Scams

CSI PROTECTION
CERTIFICATION



A 65-year-old woman in Japan paid the equivalent of \$AU47,932 in a recent online scam that defied gravity. The con artist tricked the woman into believing he was a Russian astronaut who just couldn't afford a ticket back to Earth, local media in Japan [reported](#).

The pair started corresponding through Instagram on June 28, and the scammer claimed that he was a cosmonaut on board the [International Space Station \(ISS\)](#). He blamed the poor cell service aboard the orbiting space station for his lack of communication at times. Things between them quickly escalated when the fake astronaut professed his love to her, claiming that he would want to marry her once back on Earth. Except there was one problem, he simply could not get off the ISS unless he had enough money for a ride back to Earth.



25

Beware Every Time An email Comes In

CSI PROTECTION
CERTIFICATION



The screenshot shows a LinkedIn search interface. At the top, the search bar contains "Mattel, inc." and navigation icons for Home, My Network (with a 12 notification badge), Jobs, and Messaging. Below the search bar are filter tabs: People (selected), Connections, Locations, Current company, and All filters. The results section shows "About 30,000 results". A "Search with Sales Navigator" banner is visible. The first result is for Ynon Kreiz, Chairman and CEO at Mattel, Inc., with a "Follow" button. The second result is for Tom Le, CISO at Mattel, Inc., also with a "Follow" button.



26



Barbie-brained Mattel exec phell for phishing, sent \$3m to China

Barbie

Hackers scoped internal structures to figure out who had authority to send funds. Toy maker Mattel has recovered some US\$3 million it shipped off to Chinese hackers who sent a well-crafted phishing email to a finance executive.

Abandoned flash drive **Bad USB!**



People Are Picking up "Bad USBs"
They Find In Parking Lots And Are Still
Plugging Them In!



Would you pick up and use someone
else's dirty toothbrush?

Key Logger

← → ↻ Secure https://www.amazon.com/Original-USB-KeyLogger-8MB-Black/dp/B078LN4W6H/ref=pd_sim_147_2?_encoding=UTF8&pd_rd_i=B078LN4W6H



DataLogger
The Original USB KeyLogger 8MB Black
★★★★☆ 46 customer reviews | 26 answered questions

Price: **\$49.95** & **FREE Shipping**. [Details](#)

Get \$50 off instantly: Pay \$0.00 upon approval for the Amazon Rewards Visa Card.

✓prime | Try Fast, Free Shipping ▾

Only 4 left in stock - order soon.
Want it Thursday, Jan. 11? Order within **16 hrs 21 mins** and choose **Two-Day Shipping** at checkout. [Details](#)
Sold by [Vengeance Gaming](#) and [Fulfilled by Amazon](#). Gift-wrap available.


- Saves Over 4000 Pages Of Text!
- 100% Undetectable
- Works Instantly! No Installation Needed!
- Works with Windows and Linux
- For Wired Keyboards

protectnow

29

AI Deep Fakes and Voice Clones

What is FraudGPT?



AI in fraud can amplify scale and sophistication, causing widespread harm by accelerating scams, identity theft, and financial losses.

FraudGPT refers to the malicious use of GPT (Generative Pre-trained Transformer) models, like ChatGPT, to deceive or manipulate individuals. This can involve generating fake content, spreading misinformation, or impersonating legitimate sources. Detecting and preventing such fraudulent activities is crucial to maintaining trust and integrity in online interactions.

RELATED COVERAGE
Stormy Daniels describes her alleged affair with Trump
Highly Cited - 100+ News - Mar 22, 2019

Train's arrival in Beijing raises speculation of Kim visit
Washington Post - 4h ago

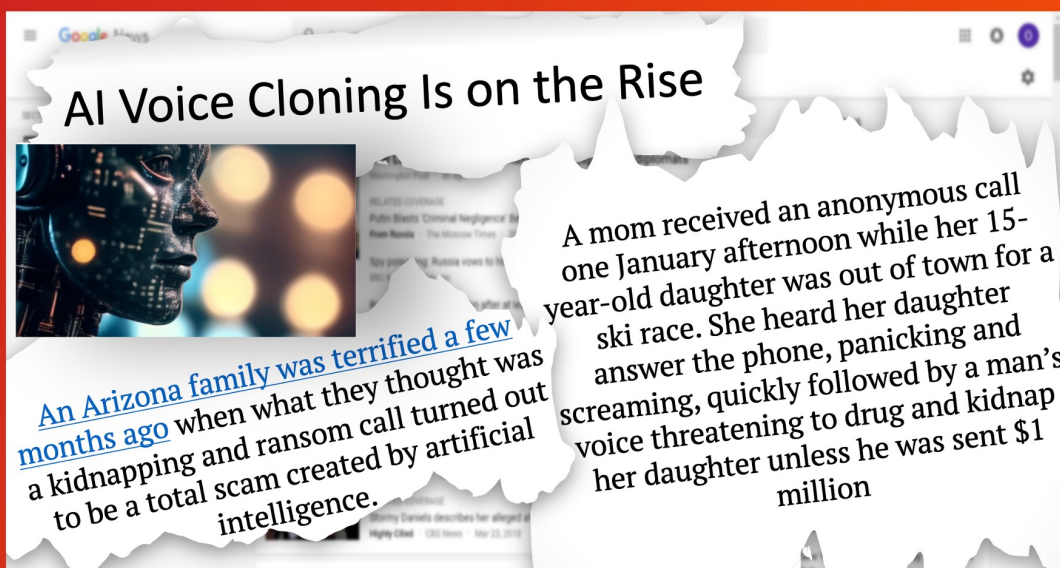
Fake news: Trump will not grower UK
Seemingly... over Data scandal
Reuters - 11h ago

New York Today: A Sunny Day at the Death Cafe
New York Times - 20h ago

protectnow

30

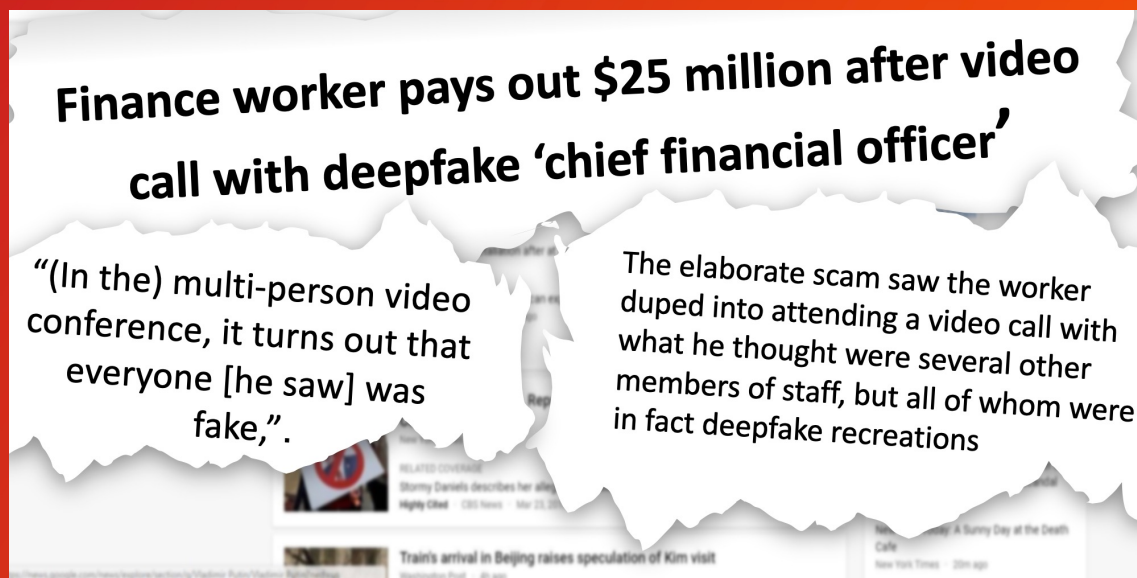
AI Deep Fakes and Voice Clones



protectnow

31

AI Deep Fakes and Voice Clones



protectnow

32

AI Deepfakes and Voice Clones

OpenAI says it's working on AI that mimics human voices

<https://www.cnn.com/2024/04/01/tech/openai-ai-voice-generator-tool-voice-engine/index.html>

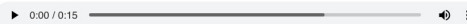


By Clare Duffy, CNN

3 minute read · Updated 4:21 PM EDT, Mon April 1, 2024

Real human voice

This is the clip of a real human voice that was input into OpenAI's Voice Engine.

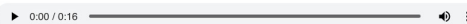


Source: OpenAI

The next audio clip is the AI-generated voice that was created by Voice Engine based on the above human speech and a written paragraph that told the machine what to say.

AI-generated voice

This is the resulting AI-generated voice clip that Voice Engine generated based on the human sample.



Source: OpenAI



33

Don't Worry: Course Action Items

This bulleted list is what you will learn from this course and these are all reminders and action items for you to keep yourself, your business and the data you possess, secure.



- **Security Awareness Training:** Whether it be hardware, software, or human hacking, there are always vulnerabilities in all systems, all around us. The only way to properly plug these various holes is through education both in person, virtually, and through phishing simulation training. This requires a little bit of time and expense and is an absolute necessity of doing business.
- **Social Engineering:** Recognize social engineering scams every time the phone rings, an email comes in or someone knocks on the door.
- **Hardware:** Make sure your devices such as PC's, laptops, mobiles, modems, routers and any peripherals are newer. Old hardware (5+ years) sometimes lacks internal resources to run current more secure software and firmware.
- **Software:** Keep all devices operating systems updated with the latest software updates and critical security patches.
- **Security Software:** Install and run a paid version of antivirus, anti-spyware, anti-phishing and a firewall.
- **Wi-Fi Security:** Set up a secure Wi-Fi connection in your home or business.



34

CSI Protection Course Action Items



- **VPN:** Ensure your laptop and mobile devices and its data are protected on open free Wi-Fi by using a VPN or "virtual private network"
- **Encryption:** Protect your data with encryption software.
- **Tracking:** Install, set up and enable tracking software for lost or stolen laptops and mobile phones
- **Backup:** Back up and sync all your information on redundant internal and external local hard drives. Back up externally to cloud based backup sites. Back up all data on iPhone and Android mobiles.
- **Passwords:** Set up and run password manager software and eliminate password re-use by having a different password for every online account.
- **Two Factor:** Set up two-factor or two step authentication for any and all critical accounts that deploy it.
- **IT Vendors:** Use your circle of influence or trusted network to make recommendations when hiring IT security contractors or MSSPs to ensure the security of your network.
- **Cyber Security Insurance:** if or when all else fails cyber security insurance is imperative.

Second Hand Devices

- ❖ Printers
- ❖ Craigslist
- ❖ 30 devices
- ❖ 30 mile radius of Boston
- ❖ Basic forensics
- ❖ Half provided data
- ❖ ATMs



ATM Security



37

ATM Security



38

ATM Security



39

ATM Security

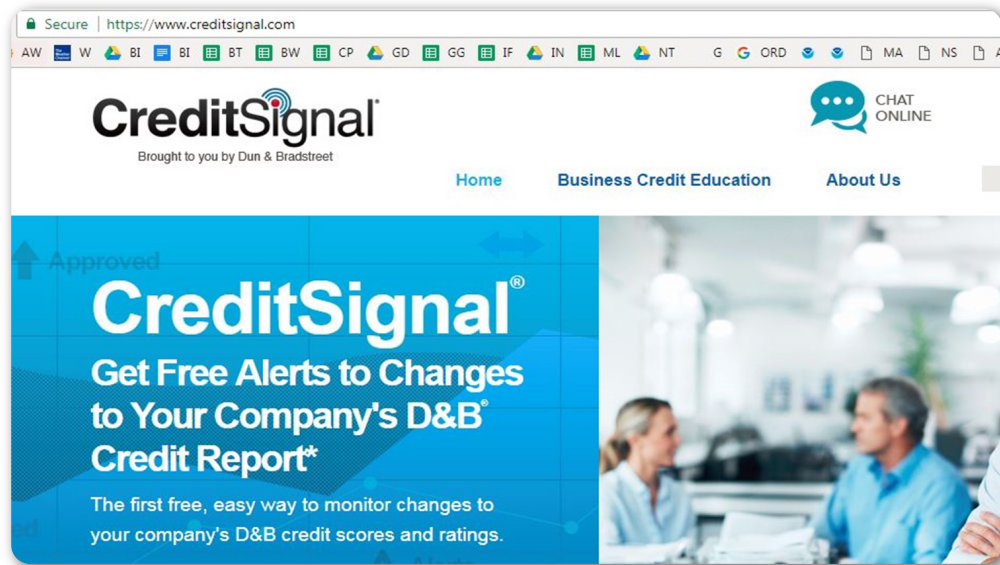
CSI PROTECTION
CERTIFICATION 



 protectnow

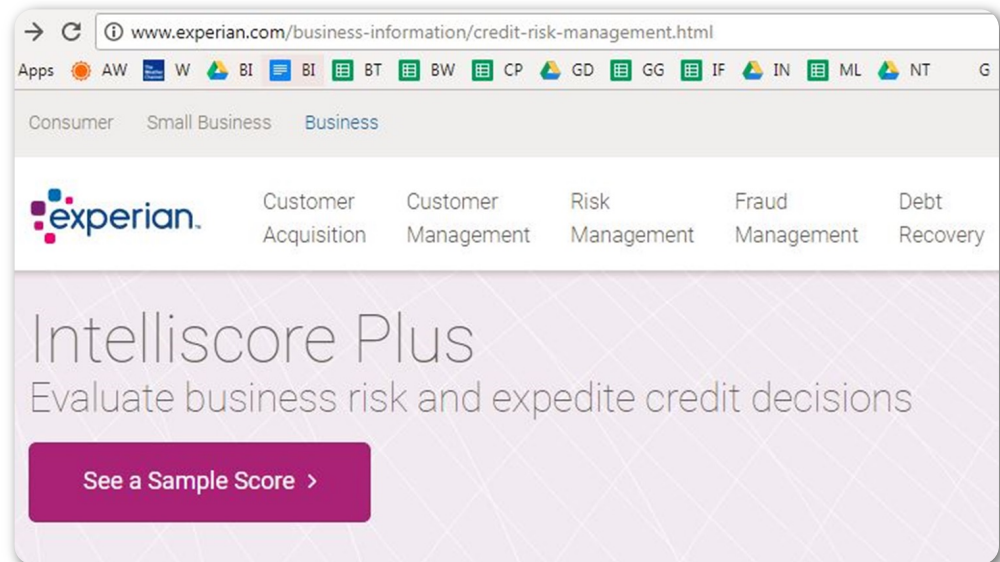
40

Credit Checks To Protect **Your Business Identity**



41

Credit Checks To Protect **Your Business Identity**



42

Credit Checks To Protect **Your Business Identity**



43

We Are Seeking **Google Reviews!**



bit.ly/robreview

...on how Robert's presentation can help you personally and professionally. If you have "critical feedback" that would help us improve **PLEASE**, email us Robert@ProtectNowLLC.com so we can incorporate those important requests into future trainings. **Please share your Positive experience!!**

Protect Now LLC

5.0 ★★★★★ 96 reviews

[Write a review](#)



44

Want To **Learn More? Visit our Website!**



Personal, cyber, social and identity theft protection for you, your family and your business.

ProtectNowLLC.com