CSI PROTECTION CERTIFICATION

protectnow

Robert@ProtectNowLLC.com
ProtectNowLLC.com

Defend From Hackers, Attackers, and Thieves:

Risk Management & Privacy Protection
for Service Professionals & Their Clients.

1

AGENDA - The CSI Protection Certification

CSI PROTECTION CERTIFICATION

SESSION #1	SESSION #2	SESSION #3	SESSION #4
			
Personal & Client Protection	Defending Against The Data Breach	Identity Theft Protection, Prevention & Awareness	Social Media Security & ORM

Let's get rolling!

protectnow

2

The TARGET of Organized Crime

THE GREATEST WEALTH TRANSFER in Human History

Nearly $124 trillion in assets is set to change hands through 2048, according to estimates by the consulting firm Cerulli Associates. The recipients, primarily members of Generation X (those born between 1965 and 1980), millennials (1981-1996) and Gen Z (born after 1997), are expected to inherit some $106 trillion of that amount, mainly from baby boomers, with the rest going to charity.

protectnow

3

The Human Blindspot™ Why We Are Hardwired To Fall For Scams

The **Human Blindspot™** is a biological "short circuit" where our innate need to trust overrides our analytical intelligence.

- **The Biological Mandate:** Interdependence as Infrastructure. This ancient survival infrastructure creates the **Human Blindspot™** Human beings are an interdependent species defined by a fundamental evolutionary requirement: "man needs woman and woman needs man" to ensure the survival of the next generation. This mandate for procreation requires a high-stakes psychological infrastructure: **Trust**. We are, quite literally, biologically programmed to "Default to Trust" as a core mechanism for species survival.
- **The Modern Vulnerability: Weaponizing Trust.** The Compulsion of the Blindspot. Because our DNA is hard-wired to default to trust for the sake of the species, we possess a psychological gap that obscures the truth; when lied to, we are biologically compelled to believe that lie. Today, this ancestral programming is being weaponized by AI-driven predators. They use synthetic media and voice clones to hijack this internal hardware, turning our greatest evolutionary strength (interdependence and trust) into a predictable security liability.



protectnow

4

The Anatomy of Manufactured Urgency: Tactics of Immediacy

Criminals use urgent "pretexts" to trigger our biology and force immediate action:

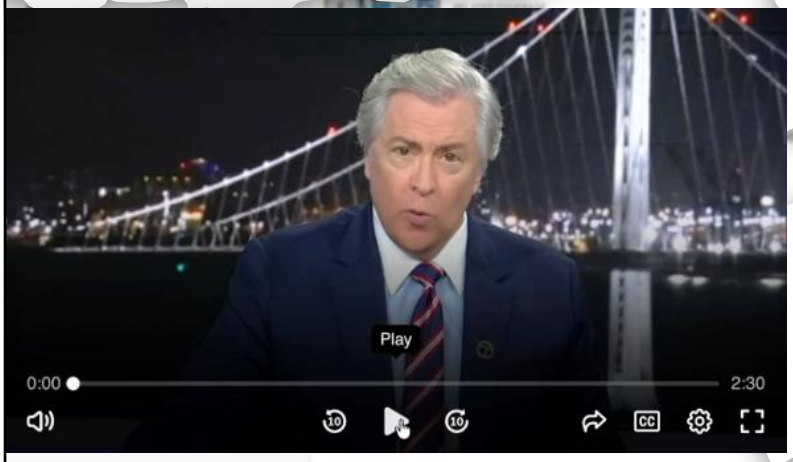
- **Fear of Loss:** Impersonating authorities to threaten severe consequences or account closures.
- **Impending Expiration:** Claiming vital deals or benefits will vanish without instant payment.
- **The "Emergency" Crisis:** Using voice cloning to fake a loved one's dire situation.
- **Manufactured Loneliness:** Exploiting the human need for connection to bypass logic.
- **Confidentiality:** Enforcing secrecy to isolate targets so others cannot intervene.



protectnow

5

Mom out thousands after scammers use AI to mimic daughter's voice in fake kidnapping

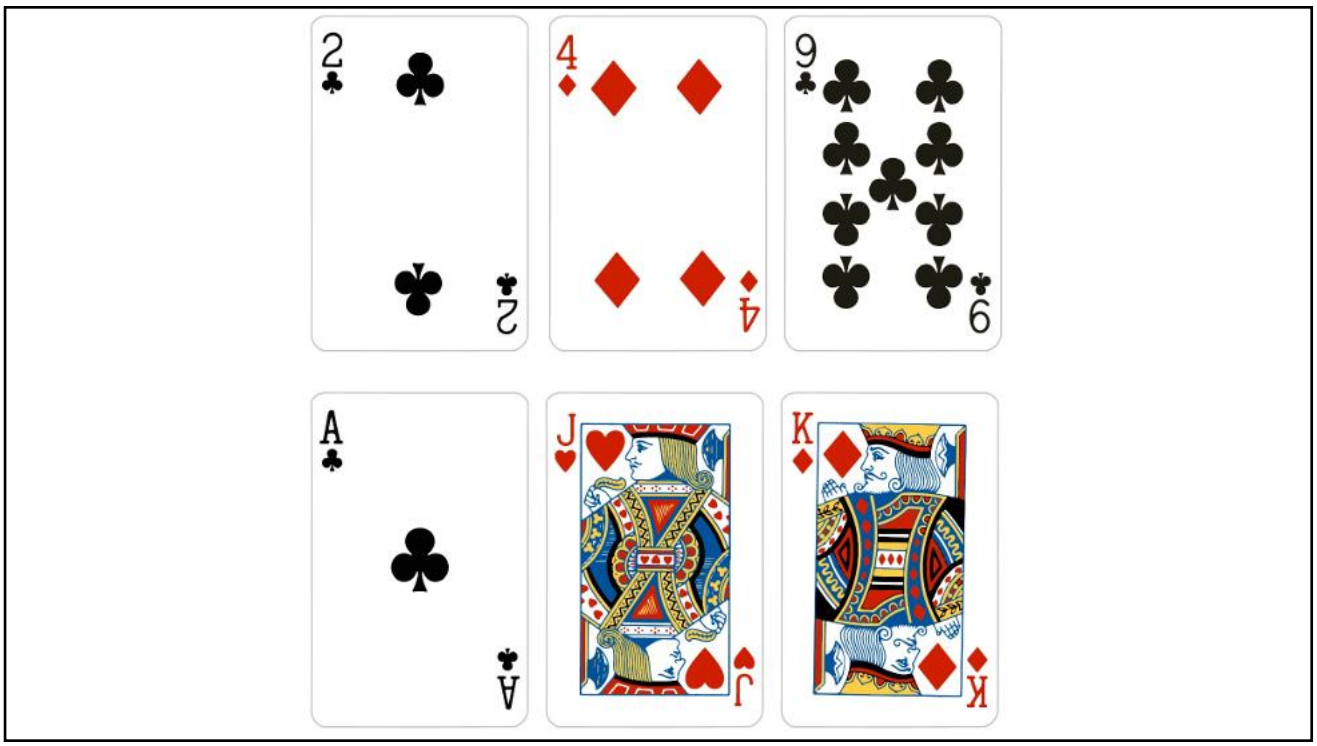


Thousands of dollars were stolen from a Bay Area woman after scammers used artificial intelligence to mimic her daughter's voice in what authorities describe as a growing type of fraud.

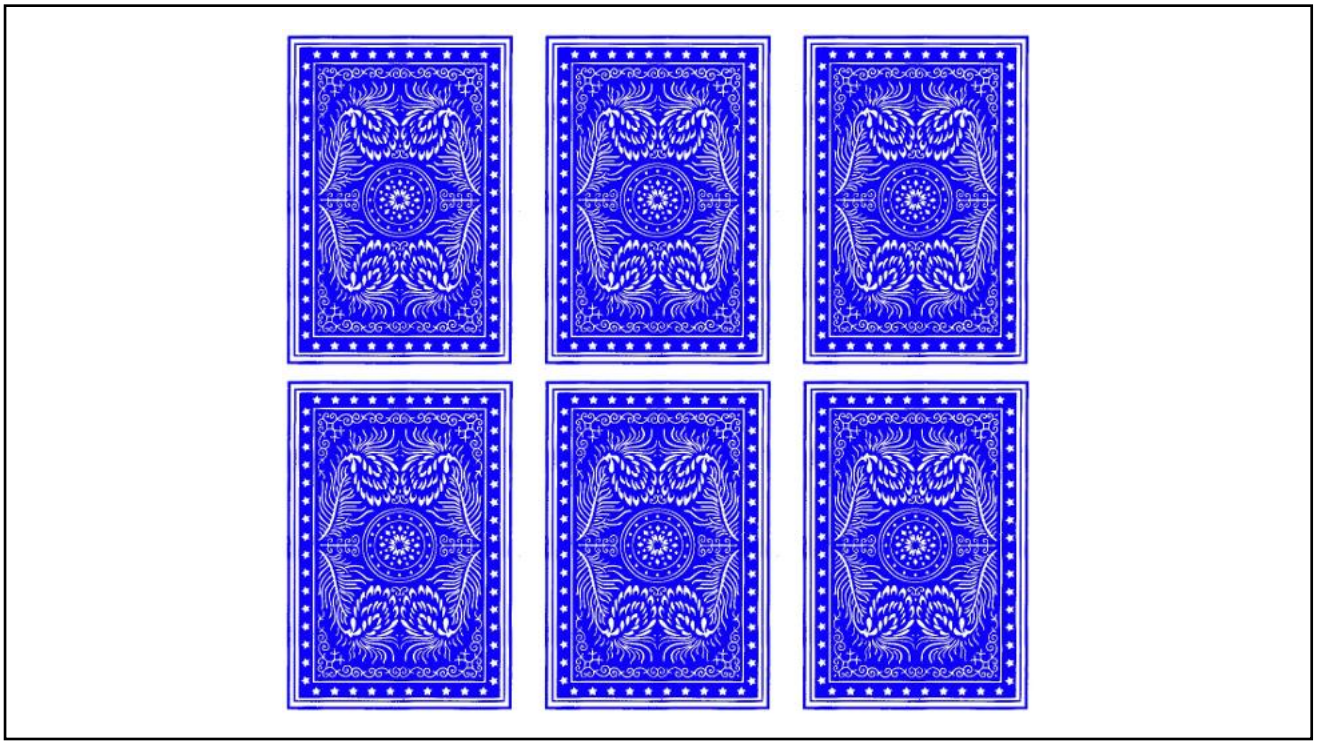
Fearing for her daughter's life, she followed the caller's instructions for five hours, as the caller issued a series of urgent commands. "Don't speak, go and get dressed and get out' 'do this now, it has to happen now'," he said. After wiring $5,400 to Mexico from she was told her daughter would be released at a grocery store. When she arrived and could not find her, she called her daughter directly, who picked up and said she was at work.

Train's arrival in Beijing raises speculation of Kim visit

6



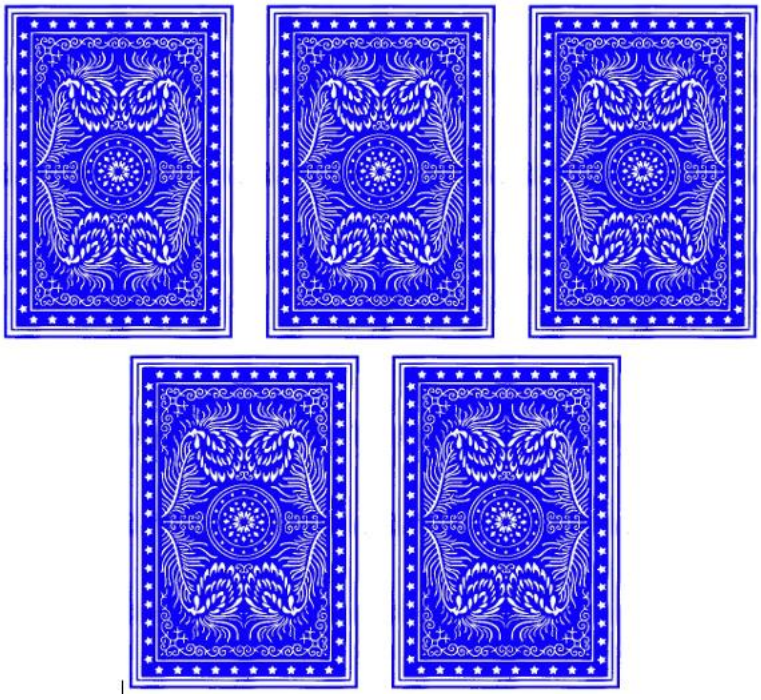
7



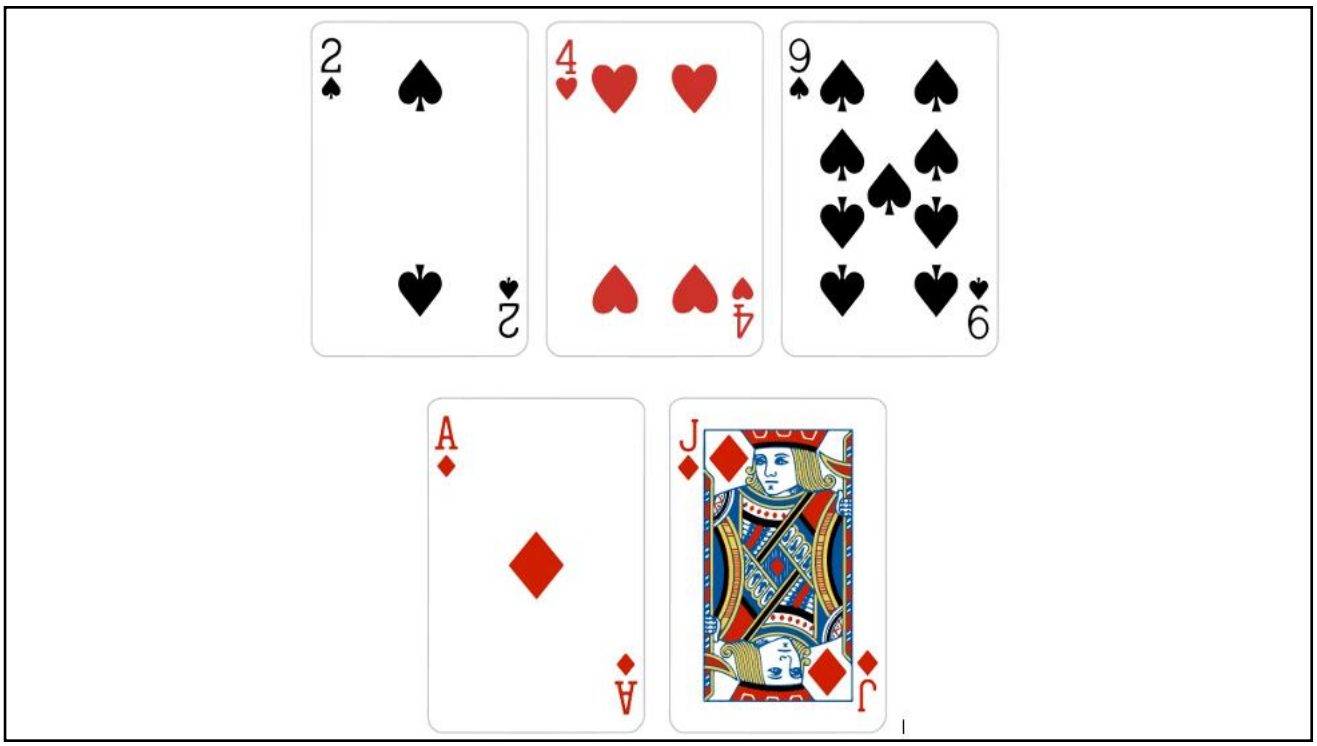
8



9



10



11

The Human Blindspot™ Trust & Selective Attention

The **Human Blindspot** isn't created by a lack of intelligence; it's created by **cognitive tunneling**. Bad actors don't hack systems; they hijack your attention. Most people operate under the *assumption* that they would see the scam 'I'm too smart, only stupid people get scammed". This demo proves that **we don't see with our eyes; we see with our attention**.



The Reveal

Only a relatively small percentage of you caught what just happened. I didn't just vanish the card you were thinking of—I changed all five cards. Every single one of them. What you just experienced wasn't a magic trick, and it wasn't sleight of hand. It was an exploit of your brain's natural architecture.

Isolating Your Attention

When I asked you to focus on one card, your brain instantly triggered **cognitive tunneling**. To give 100% of your attention to that target, your mind actively erased the surrounding perimeter. You didn't fall for this because you weren't paying attention. You fell for it **because** you were paying attention—to my request.

Predictive Anticipation

When a fraudster manufactures an urgent wire request or spoofs your CEO or a family member, they are handing you 'one card.' While your entire focus is locked on fixing that immediate emergency, they swap the entire landscape right under your nose. The moment an adversary controls where you look, they control what you miss. Protect the perimeter—don't just look at the card.

protectnow

12

The Human Blindspot™ Proof of a Neurological Vulnerability

Real world execution of *attentional capture using manufactured urgency*: Parallels between the card trick and how the AI Kidnapping extortion attack played out:



Tactic: *"Forcing your mental spotlight onto a single variable"*
The Real-World Parallel: The ultimate high-urgency variable—the sound of her adult daughter screaming and begging for help. By triggering extreme parental panic, they seized 100% of her cognitive bandwidth. Her focus was entirely consumed by saving her child's life, preventing her mind from processing any surrounding warning signs.

Tactic: *"Manipulating the world around it."*
The Real-World Parallel: While the mother's focus was hyper-fixated on the voice on the line, the reality around her remained completely unchanged—her daughter was safe at work the entire time. The scammers manipulated her perception of reality by keeping her on the phone for nearly five hours straight. This prevented her from taking a pause to execute an out-of-band verification (such as hanging up and calling her daughter directly).

Tactic: The Human Blindspot™ *"Criminals manipulate human trust..."*
The Real-World Parallel: The mother's brain relied on a baseline trust assumption: *that a distinct voice belongs exclusively to the person who owns it*. Because her brain processed the familiar voice as an undeniable truth, her natural skepticism dropped, leading her to wire over $5,400 to foreign accounts before ever checking if the foundational premise was real.

13

Telephone Scams: Caller ID Spoofing



14

The Anatomy of Manufactured Urgency: Tactics of Immediacy

Criminals use urgent "pretexts" to trigger our biology and force immediate action:

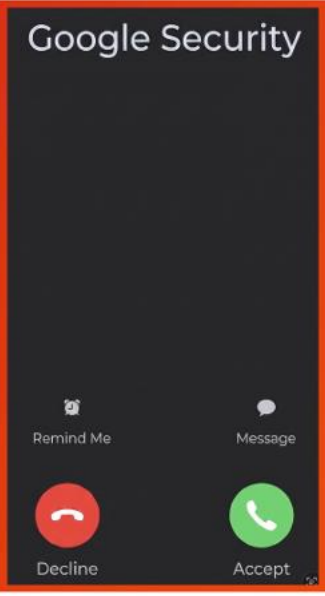
- **Fear of Loss:** Impersonating authorities to threaten severe consequences or account closures.
- **Impending Expiration:** Claiming vital deals or benefits will vanish without instant payment.
- **The "Emergency" Crisis:** Using voice cloning to fake a loved one's dire situation.
- **Manufactured Loneliness:** Exploiting the human need for connection to bypass logic.
- **Confidentiality:** Enforcing secrecy to isolate targets so others cannot intervene.



protectnow

15

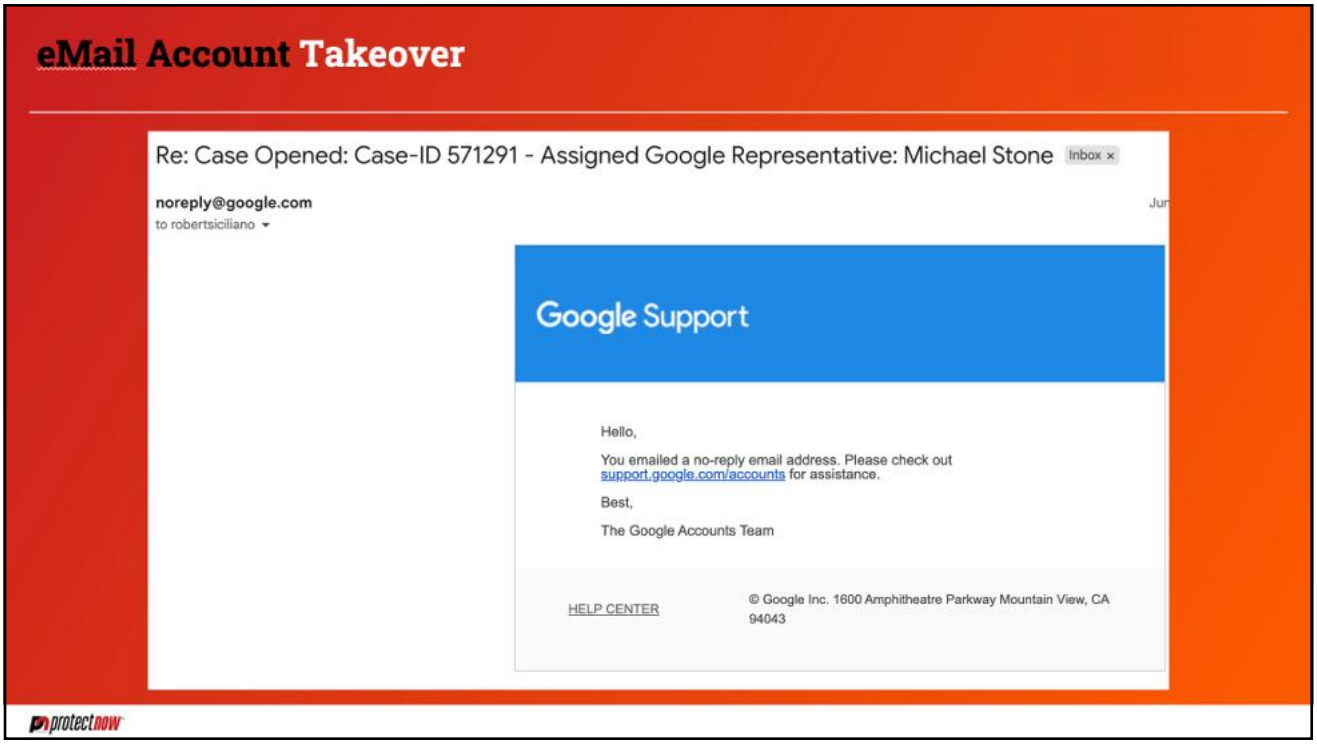
eMail Account Takeover



protectnow

16

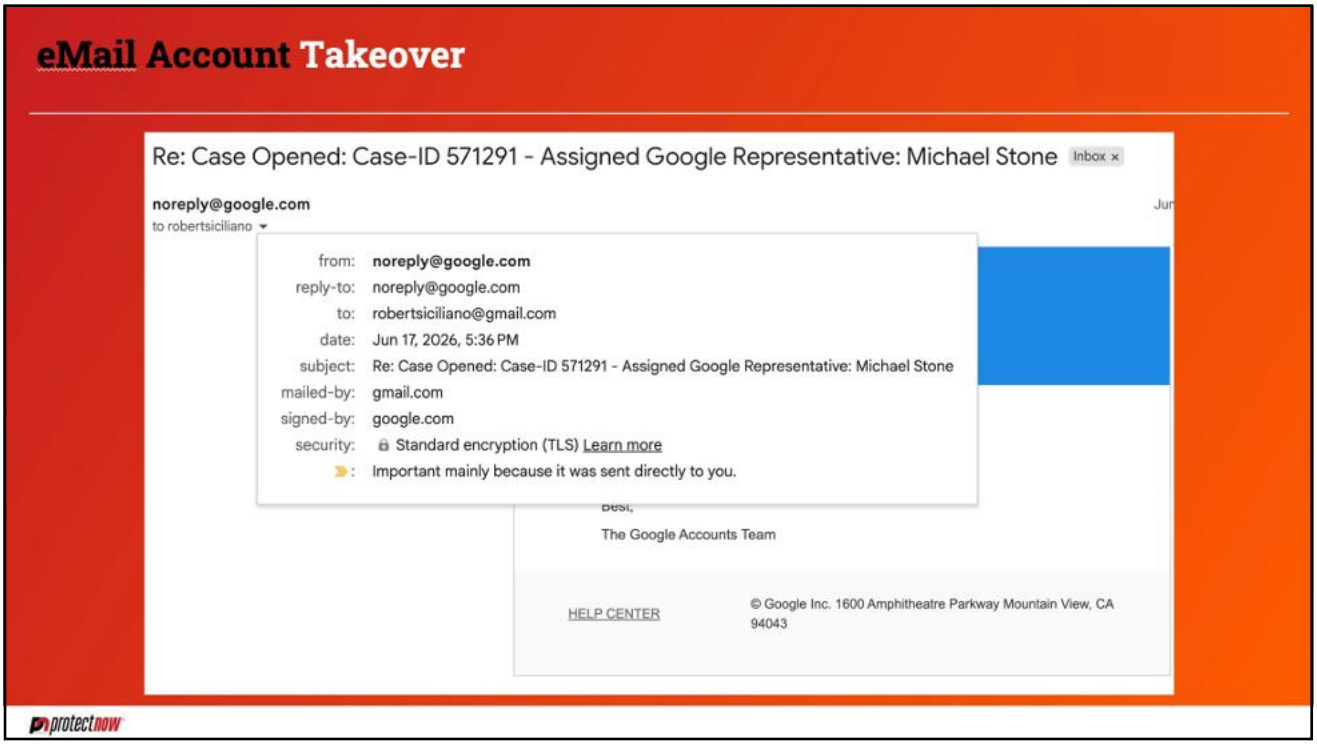
eMail Account Takeover



protectnow

17

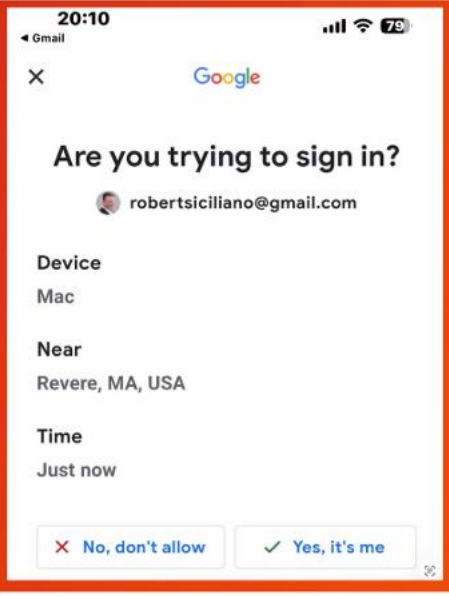
eMail Account Takeover



protectnow

18

eMail Account Takeover



protectnow

19



20

"She was just a woman that worked alone – a rich broker."

~ Arron Lewis, in response to questions about his motives for murdering a Real Estate Agent.



21

Civilized Conditioning

CSI PROTECTION CERTIFICATION

- Respond to an attacker?
- Goes against our core beliefs
- Think it can't happen to you?
- Head in the sand mentality
- You're too nice
- Become an observer of the human condition







protectnow

22

Protection Weapons

CSI PROTECTION CERTIFICATION

Non-lethal – non-aggressive

- Alarms

Non lethal - aggressive

- Pepper spray, stun gun, baton

Lethal - aggressive

- Guns, knives

Tactical Pen?









protectnow

23

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

1. Be suspect of everyone.

There isn't any benefit in being paranoid; however, being a little guarded can keep you from getting into a vulnerable situation. Don't just be wary of a man showing up unaccompanied. Expect them to show up in a nice car, well dressed, maybe with a wife and kids tagging along.

They might have a business card saying they are a doctor or a lawyer. Don't let your guard down. It might not be till the second or third meeting that they decide to make their move. They like to gain your trust so you feel comfortable carrying cash and jewelry, and then they decide it's safe to move in.



protectnow

24

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

2. ID and pre-qualify at your first meeting.

Whether you are at your office or meeting at a property, get some form of identification.

Also, it is to your benefit that a potential client buying a home is pre-qualified. Someone who is pre-qualified by a lender and meets you at the office is less likely to be a predator. Open a file with all their identification, including information such as a license plate and employer contact information. All auto dealers require ID.



protectnow

25

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

3. Stay in communication with the office.

Before showing a property, make it known to your co-workers, a spouse or a friend where you are going and when you will be back. Have them call you at a designated time to check on you. Have them set an alarm on their phone as a reminder.

A system where you call in has its advantages too.
Have a designated in-out file. Use a clip board, cork board, e mail or voicemail system that everyone has access to.
Utilize various smartphone GPS apps.



protectnow

26

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

4. Have a plan for safe open houses.

Take a friend and bring a cell phone. Spend a few minutes considering all the vulnerable points within the home and how you would escape if necessary.

When someone walks in, say, "I'd be happy to show you the benefits of this home! In a few minutes my partner Rocco will be along to assist me." When a couple shows, require them to stay together.

Often, they split up, and while one has your attention, the other raids jewelry boxes and medicine cabinets for narcotics. In high crime areas, consider hiring an off-duty police officer to watch the property during a showing. Remove knives from counters. Have a discussion.



protectnow

27

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

5. Use predetermined code words to alert your office of distress.

Utilize green, yellow, and red, a traffic light, for levels of distress. For example, say to your caller: "it's in the green folder", letting your caller know you are fine.

Or "it's in the yellow folder", alerting your caller that the situation is shaky and you might need assistance. Use an acronym for help such as Have Emily Leave the Papers at 35 Cherry Street.



protectnow

28

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

6. Conduct safe personal marketing.

To a stalker, your photo on a sign or in print is a personal ad. He determines if you have the 'look' he is seeking. Keep photos professional opposed to overly “attractive”.



protectnow

29

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

7. Separate business from personal.

Home phone numbers and addresses give a predator everything he needs to stalk his prey.

Use P.O. Boxes and voicemail systems. Keep your personal phone number unlisted.



protectnow

30

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

8. Implement a buddy system.

Whenever possible, bring along a co-worker. There is strength in numbers.

Predators thrive on isolation. By pairing up, you reduce the chances of being attacked.



protectnow

31

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

9. Dress for safety and success.

Don't wear expensive jewelry. A $3-5 thousand-dollar diamond buys a lot of drugs. Dress professionally instead of provocatively.

Scarves and loose fitting 'flowy' styles of dress can give attackers something to grab onto.
Wear shoes you can run and kick in and won't hinder fighting back.



protectnow

32

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

10. Don't take predators for a ride.

Driving your client to a showing is a great time to determine your client's needs and move along the sale. Don't allow the client to ride in your car if you don't know who they are. Properly identify them. Make sure this is a client, and not a predator.

Make sure you have taken the necessary precautions ahead of time before you are put in an isolated situation. If they make you feel uneasy, let them follow you and bring along a buddy.

If they do get in your car and make attempts to control you, determine your options.



protectnow

33

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

11. Pay attention to your intuition.

Trust your gut, and don't discount any troubling feelings you might have about your new client. If anything seems wrong, then it IS wrong. Cancel if necessary.

When the hair on the back of your neck stands on end, your sixth sense is signaling you, so pay attention. This feeling is a survival mechanism and you should use it.



protectnow

34

12 Tips for Real-Estate Agents Safety

CSI PROTECTION CERTIFICATION

12. Know how to defend yourself.

You are worth fighting for. We don't think about hurting others because we have been conditioned not to. However there might be a time when it is necessary to defend yourself.

Go for the eyes, throat, groin and the instep of the foot. Fighting from the ground is an advantage that few people realize they have. Kicking the knees and groin is very effective from the ground.

Scream, gouge, bite, and fight with whatever you have. Have pepper-spray in your hand or a coat pocket. Have a ball point pen ready to jab. In previous studies, 80 percent of women who fought back in an attack situation have gotten away.

You have more power than you think.



protectnow

35

CSI Protection Client PRO TIPS PHYSICAL

CSI PROTECTION CERTIFICATION

Before A Showing Remove

- Keys
- Garage remotes
- Jewelry
- Jewelry boxes
- Credit cards
- Blank checks
- Mail
- Kids gaming systems
- Electronics
- Art, and other valuables
- Weapons
- Knives
- Family photos
- Prescription drugs
- Pets

During A Showing

- Monitor Security cameras
- Signage Identification Required
- Signage Signing in Required
- Signage Video Surveillance in Use

After a Showing

- Check all door locks
- Check all door hinge pins
- Check all window locks/screws
- Look for anomalies
- Look for anything ajar
- Deadbolts
- Secure sliding doors with bars
- Turn on motion lights

protectnow

36



SESSION #2

Defending Against the Data Breach

37

Welcome to the Golden Age of Scams



Fraud Factory Hackers and Scammers have likely stolen more than $442 billion from victims around the world, far more than previously estimated, according to a new study. Cybercrime To Cost The World [$12.2 Trillion] Annually By 2031.

38

Making the Case To Prevent Breaches



protectnow

39

Making the Case To Prevent Breaches



protectnow

40

Making the Case To Prevent Breaches



protectnow

41

Stolen Raw Data For Sale On The Dark Web



protectnow

42

Cybercriminals Hack Realty Deals & Sneak Out w/100k or More.

CSI PROTECTION CERTIFICATION

Your Closing Funds Might be heading to a Cyber Criminal.

While no one knows the exact number of victims or extent of the problem, the National Association of Realtors® in Chicago told the Post that this scam has hit "hundreds, if not thousands," of home closings. It's become serious enough, in fact, that on March 18, the Federal Trade Commission issued a warning to home buyers. As for what's fueling this trend, some experts we spoke to point to the relatively lax security in the world of real estate compared with other financial industries.

"It was just a matter of time until scammers recognized the opportunity to target real estate agents and their clients," says **Robert Siciliano**, CEO of IDTheftSecurity.com. "Currently, most industries that have experienced large data breaches have put systems in place and have become hardened. That means the real estate industry and others become the path of least resistance. Unlike the entire financial industry who have encrypted communications, the real estate industry is a hodgepodge of free email accounts and unprotected communications."

protectnow

43

Beware of Wire Fraud

CSI PROTECTION CERTIFICATION

Young Family Loses Life Savings of $775K in Escrow Wire Scam

The victims had received an email asking them to wire their funds into escrow. They had received another email from their escrow company a few days earlier and all their personal and bank account information lined up. Everything in the second email matched their closing statement.



protectnow

44

CSI Protection PRO TIPS CYBER

CSI PROTECTION CERTIFICATION

Prevent Money Wire Scams:
Email or phone communications can be easily manipulated or "spoofed" to seem legitimate. It is extremely important that email is looked at with a cynical eye.

- **Beware:** Never wire money, or pay a bill based on an email or a phone call without first making contact with **the payee that you have on file** to confirm the legitimacy of the transaction.
- **Email:** In the process of buying or selling a home, there will be many emails to and from your real estate agent and other service professionals including your attorney, mortgage broker, title, insurance companies and home inspector. Discuss between client, real estate agent and service professional, the nature of email communications and what links might be required to click on.
- **Call Your Agent:** Under no circumstances and at no time in this process should the client or service professional engage in a money wire transfer unless the client specifically speaks to the real estate agent in person or over the phone to confirm the legitimacy of the money wire transaction..
- **Email Disclosure:** Clients should always look for language in the real estate agent's email communications stating the below or a similar facsimile.
- *Wire Fraud is Real*. Before wiring any money, call the intended recipient at a number you know is valid to confirm the instructions. **Prevent Money Wire Scams: WAVIER**

protectnow

45

Synthetic Scams: The Phantom Buyer & The Vacant Land Trap

Vacant land fraud—specifically seller impersonation fraud—has surged, with alerts from the FBI Internet Crime Complaint Center (IC3) and the National Association of Realtors (NAR) revealing that vacant land accounts for over 60% of all deed and title fraud cases.

Scammers systematically search public records for unencumbered, high-equity parcels owned by absentee, foreign, or deceased owners. Posing as legitimate owners using stolen Personally Identifiable Information (PII), fraudsters list properties remotely, execute quick sales, and vanish with buyer proceeds before the true owner or agent discovers the scheme.



protectnow

46



47

Synthetic Scams: 5 Vacant Land Scam Red Flags

Here are five signs that you could be about to fall for a Vacant Land Scam:

- **Communication Barriers & Meeting Refusals:** Initial contact occurs strictly via text or email. While sophisticated scammers might agree to a phone call, they will flatly refuse in-person meetings or video calls, often citing remote travel or personal emergencies.
- **Below-Market Pricing & "Tales of Woe":** Properties are priced significantly below market value to generate an immediate sale. Scammers frequently fabricate financial hardships or urgent personal needs to explain the discount and compel speed.
- **Prohibition of Signs, Showings, & Inspections:** Scammers refuse "For Sale" signs on the parcel and ban physical showings, inspections, or open houses—preventing activity that could alert real owners or vigilant neighbors.
- **Insistence on Their Own Notary:** Fraudsters push to use their own remote or out-of-area notary. While standard in some contexts, it allows criminals to submit forged, highly convincing phony documents.
- **Immediate All-Cash Demands:** They insist strictly on all-cash transactions with funds wired immediately upon closing, ensuring the money is drained and unrecoverable by the time the buyer discovers the fraud.



protectnow

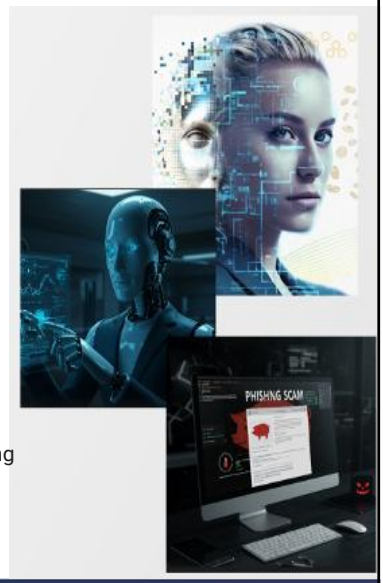
48

Vacant Land Scam: Combat Seller Impersonation

Actionable Verification Protocols for Realtors
To combat the steep rise in seller impersonation and vacant land fraud, real estate professionals, title agents, and buyers must move beyond standard paperwork checks. Implementing these top five risk-reduction strategies creates a robust defense against fraudulent transactions:

1. Independent Seller Identity Verification & Live Chat Controls
- **Live Video Verification:** Mandate a live, face-to-face video call or in-person meeting. Always generate and send the meeting link yourself to prevent scammers from using malicious video links.
- **Dynamic ID & Fraud Screening:** Utilize identity verification platforms (such as CertifID or Forewarn) that run sellers through dynamic knowledge-based questions and cross-reference contact details with public records to detect stolen or synthetic identities.

2. Direct Out-of-Band Contact via Public Tax Records
- **Independent Tax Address Lookups:** Pull county recorder and tax assessor records independently—never rely on contact details provided directly by the seller.
- **Certified Physical Mail Checks:** Send an express or certified letter to the official tax billing address on file to notify the recorded property owner of the active listing attempt and verify their authorization.



protectnow

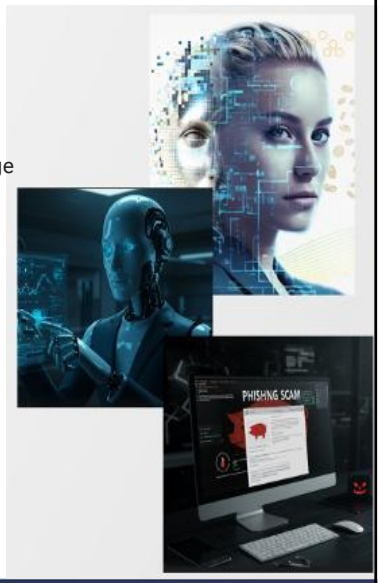
49

Vacant Land Scam: Combat Seller Impersonation

Actionable Verification Protocols for Realtors
3. Requesting Non-Public Documents & Physical "Feature Tests"
- **Private Paperwork Proof:** Require document copies that only the legitimate owner would retain, such as original title insurance policies, previous settlement statements (HUD-1/Closing Disclosure), or official survey maps.
- **Property Feature Verification:** Visit the lot in person and test the seller's actual knowledge by asking specific or intentionally deceptive questions (e.g., asking about an imaginary fence, old shed, or non-existent utility hookup) to see if they spot the falsehood.

4. Direct Control Over Notaries and Title Officers
- **Reject Unknown Remote Notaries:** Never allow a remote seller to arrange or supply their own notary public, as fraudsters frequently use forged notarizations or co-conspirators.
- **Vetted RON & Title Services:** Insist on using title-approved Remote Online Notarization (RON) platforms or verified closing attorneys that perform multi-factor identity authentication before documents are signed.

5. Automated Property Fraud Alerts & Comprehensive Title Insurance
- **County Title Monitoring:** Encourage landowners to sign up for free Property Fraud Alert services provided by their local county recorder's office, which automatically notify owners when any document or lien is recorded against their parcel.
- **Enhanced Title Policies:** Ensure buyers purchase comprehensive title insurance policies (such as an ALTA policy) that specifically offer post-policy protection against forgery, seller impersonation, and fraudulent conveyances.



protectnow

50

Vacant Land Scam: Transaction Policy email

Subject: Our Transaction Policies

Dear [Client Name],

We are thrilled to work with you to sell your property. Before we can list it, we ask you to review the policies outlined below, and reply with the statement, "I agree." We are unable to list any property unless you first agree to these terms:

1. We will be conducting an exhaustive title search to confirm the rightful ownership of the property at the cost of the seller.
2. We require a copy of the seller's property tax bill and most recent proof of payment.
3. We require an in-person meeting or video conference with all sellers.
4. A For Sale sign with our contact information must be posted on every property we list, including the name of our listing agent and a phone number where we can be reached.
5. We require all clients to use one of our approved Notaries Public. If you are located out of our immediate area, we will provide a list of approved Notaries Public for you.
6. All transactions are subject to a minimum 48-hour hold before funds will be released. If the 48-hour period ends during a holiday or weekend, funds will be released on the next business day.



protectnow

51

Home Title Fraud

Proactive Measures: You don't need to pay for a subscription to protect your title if you use the tools already provided by the state:



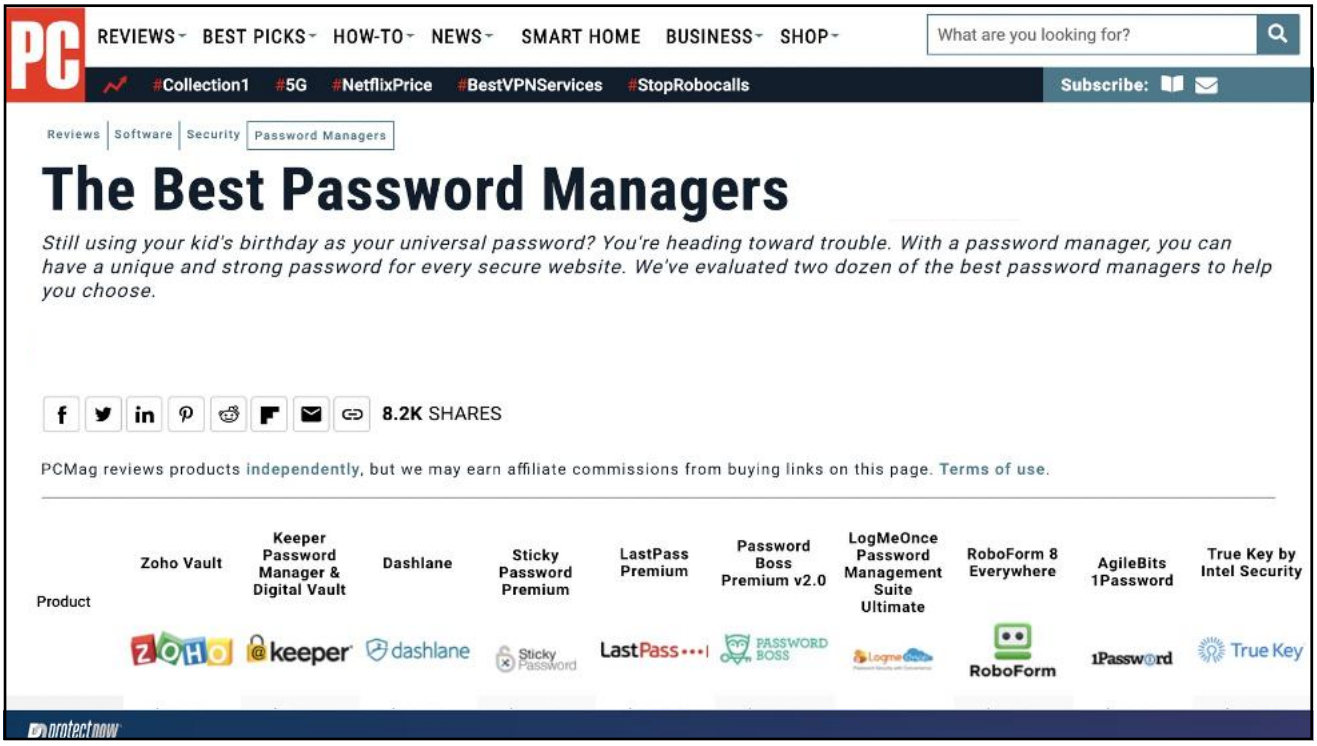
- **Property Transfer Affidavit (PTA):** Ensure the local assessor knows exactly who the owner is.
- **Property Records Alert/Notification:** Via County Clerks/Register of Deeds get a **Free Property Alert**. Sign and they email you the second *any* document is recorded against your property.
- **Open a HELOC, but don't spend it:** Banks often offer HELOCs with $0 closing and no fees. By opening the line at a $0 balance, you place a "frozen" lien on your title.
- **Freeze Your Credit:** Since title fraud often involves taking out a loan, a credit freeze at the "Big Three" bureaus is a powerful deterrent.

protectnow

52

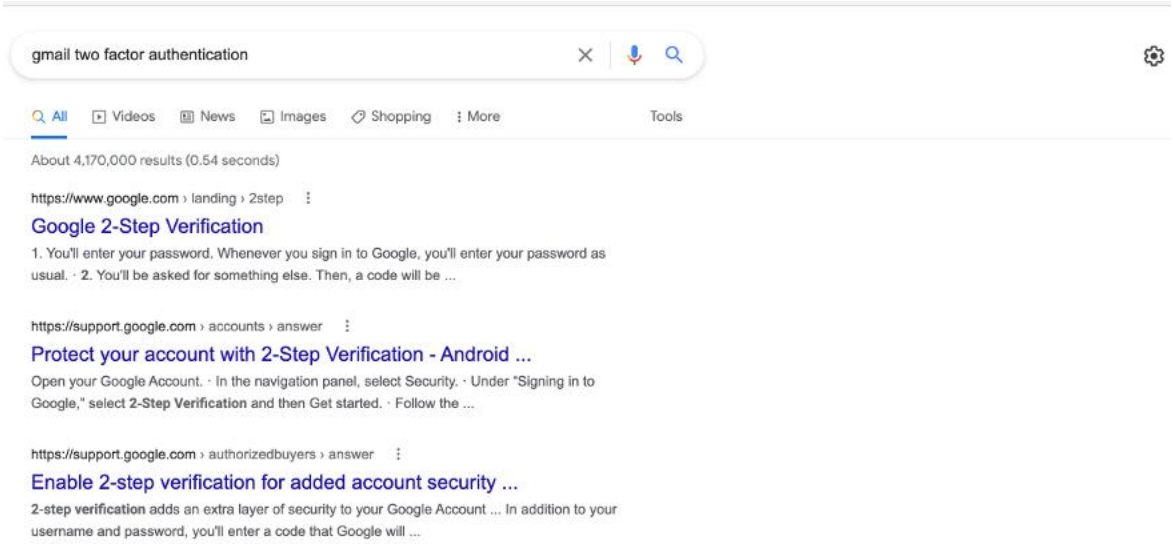

Check If Your eMail/Password Has Been Breached
Cyber Security Awareness Check
Has your personal or organizational security been breached? Get an instant answer.
Check if your email has been breached
EMAIL CHECKER
Check if your password has been breached
PASSWORD CHECKER
Protect Now does not capture, store or share ANY information you provide to these checkers.
protectnow

53


PC
REVIEWS
BEST PICKS
HOW-TO
NEWS
SMART HOME
BUSINESS
SHOP
What are you looking for?
#Collection1
#5G
#NetflixPrice
#BestVPNServices
#StopRobocalls
Subscribe:
Reviews
Software
Security
Password Managers
The Best Password Managers
Still using your kid's birthday as your universal password? You're heading toward trouble. With a password manager, you can have a unique and strong password for every secure website. We've evaluated two dozen of the best password managers to help you choose.
8.2K SHARES
PCMag reviews products independently, but we may earn affiliate commissions from buying links on this page. Terms of use.
Product
Zoho Vault
Keeper Password Manager & Digital Vault
Dashlane
Sticky Password Premium
LastPass Premium
Password Boss Premium v2.0
LogMeOnce Password Management Suite Ultimate
RoboForm 8 Everywhere
AgileBits 1Password
True Key by Intel Security
ZOHO
keeper
dashlane
Sticky Password
LastPass
PASSWORD BOSS
RoboForm
1Password
True Key
protectnow

54

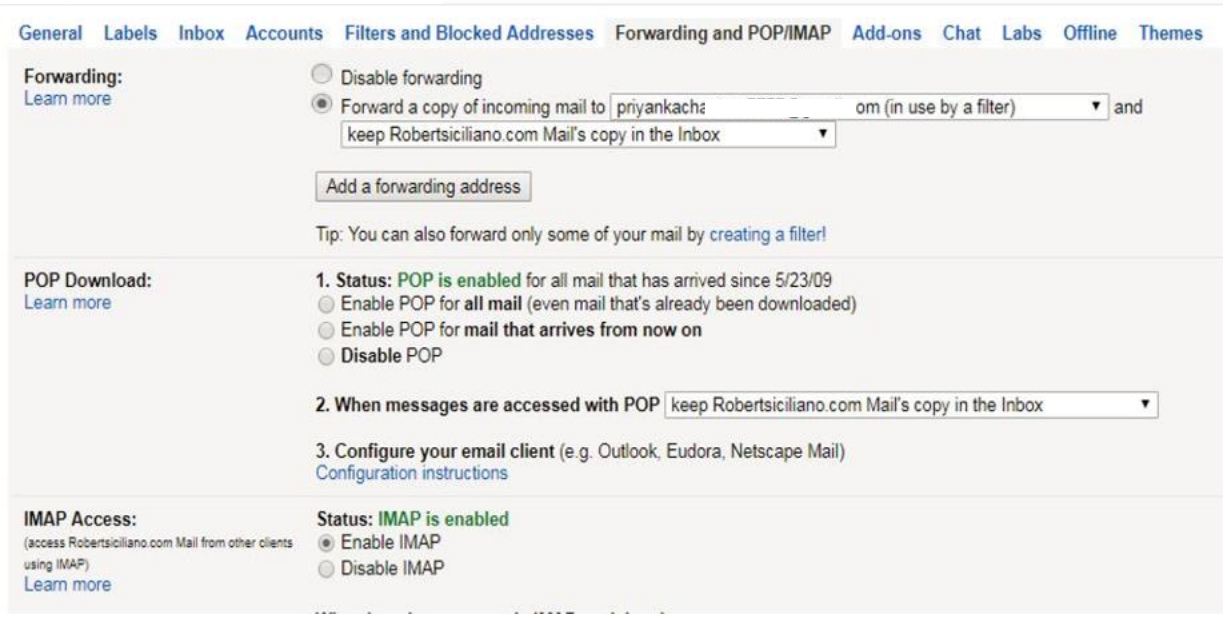
Password Management: Two Step Authentication



protectnow

55

Email Settings



protectnow

56

AI Deepfake Fraud



protectnow

57

AI Deepfake Zoom Video Scam



protectnow

58

What is a Deepfake?

- **A deepfake is;** an image, video, or audio recording that has been convincingly manipulated or entirely generated using artificial intelligence (AI), specifically a branch of machine learning called ***deep learning.*** The term combines "deep learning" and "fake."
- **The goal of a deepfake;** is to depict a person saying or doing something they never actually said or did, creating media that is difficult to distinguish from authentic content.
- **Deceiving, non-consensual synthetic media** (video, audio, or image) created to **impersonate a specific person** without their consent. The defining characteristic is the intent to deceive or simulate a reality that never happened. It mimics a *specific* real person to make it look like they are doing something they didn't do.



59

What is an Avatar or Deepfake?









60

AI Deep Fakes and Voice Clones

AI Voice Cloning Is on the Rise



An Arizona family was terrified a few months ago when what they thought was a kidnapping and ransom call turned out to be a total scam created by artificial intelligence.

A mom received an anonymous call one January afternoon while her 15-year-old daughter was out of town for a ski race. She heard her daughter answer the phone, panicking and screaming, quickly followed by a man's voice threatening to drug and kidnap her daughter unless he was sent $1 million

protectnow

61

AI Deepfakes and Voice Clones

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

Real human voice

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

0:00 / 0:15

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 generate on the human sample.

0:00 / 0:16

Source: OpenAI

An AI-enabled text-to-voice tool could help with translation, reading assistance for children or aiding people who have lost the ability to speak, the company says. But some skeptics worry it could also fuel the creation of disinformation or make it easier to perpetrate scams.

AVoice Engine can use a voice sample in one language to create a replica voice that can speak in multiple other languages.

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

protectnow

62

AI or Not?

https://www.nytimes.com/interactive/2025/06/29/business/ai-video-deepfake-google-veo-3-quiz.html

The New York Times

Artificial Intelligence › | A Personalized Internet | Romance Novels | 'A.I.-Washing' | Grok Controversy

A.I. Videos Have Never Been Better. Can You Tell What's Real?

By Stuart A. Thompson June 29, 2025



63

What is Pig Butchering

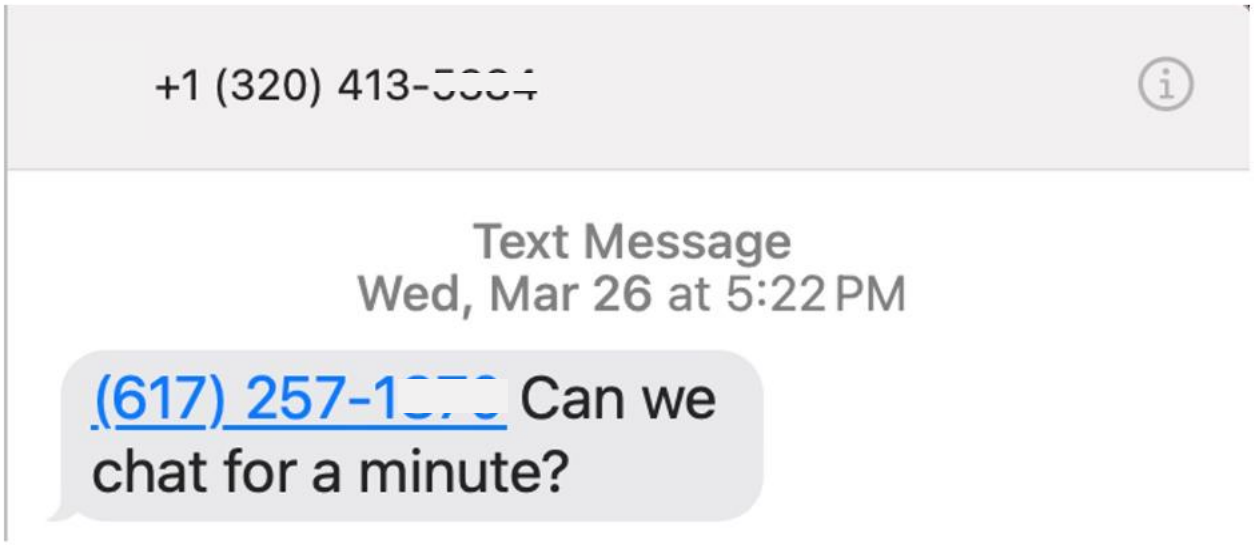
"Pig Butchering" Crypto Scam Using AI and Human Trafficking

- The name comes from the nature of how the scam happens – the scammer "fattens up" their victim before the "slaughter," in final stage of the scam. Using AI to groom their victims on messaging/dating and social media apps the scammer uses a fake profile of a gorgeous, wealthy-looking person to befriend people.
- Initial Contact starts with a seemingly accidental message or "wrong number" text, or a new connection on social media/dating apps.
- Building Trust: The scammer cultivates a romantic or friendly relationship over weeks, to create emotional dependence.
- The Pivot: Once trust is established, the scammer introduces an "amazing investment opportunity," often related to cryptocurrency, forex, or gold.
- Fake Platforms: Victims are directed to fake trading websites or apps that look highly professional, where they see artificial, growing profits to encourage larger investments.
- The "Butchering": When the victim tries to withdraw funds, they are asked to pay high taxes or fees, eventually losing all invested capital.
- Targets: EVERYONE especially BOOMERS $124 Trillion in wealth!!!



64

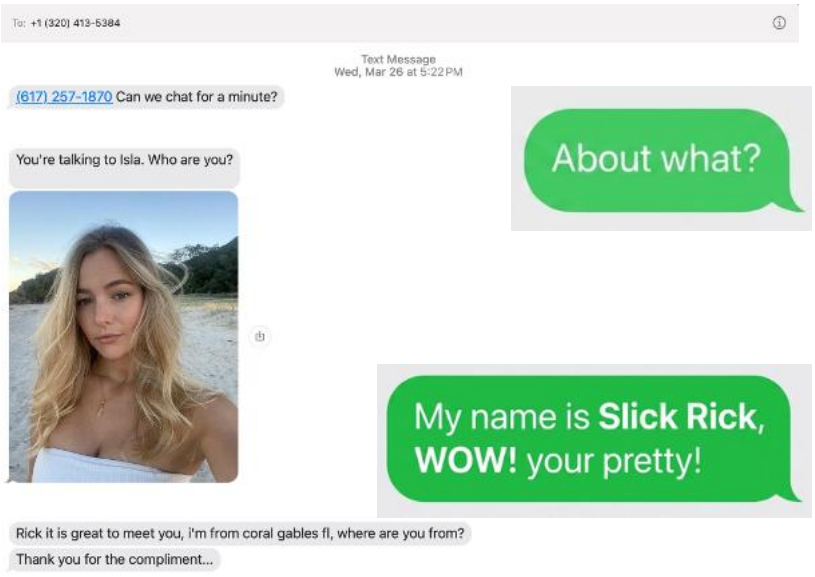
"Wrong number" Text Scams Pig Butchering



protectnow

65

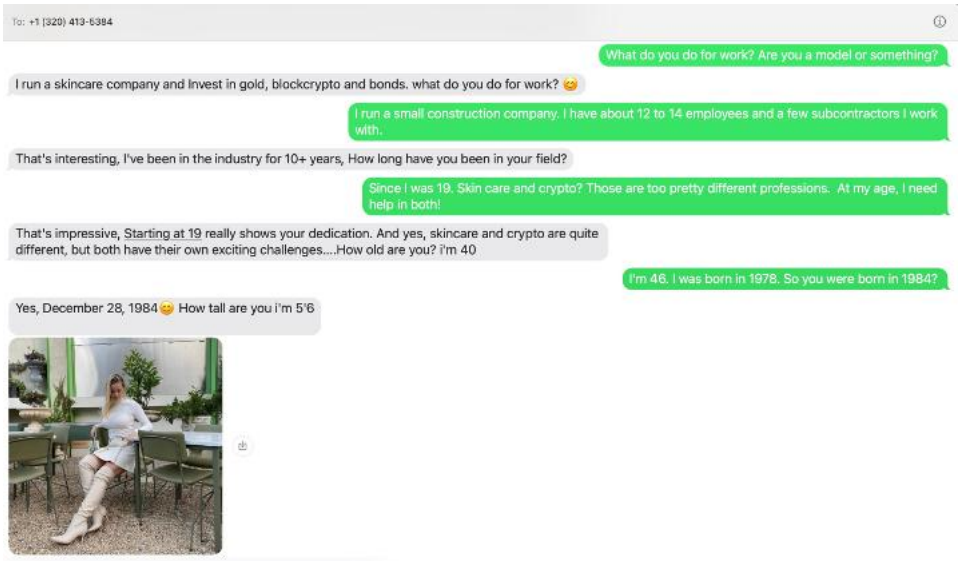
"Wrong number" Text Scams



protectnow

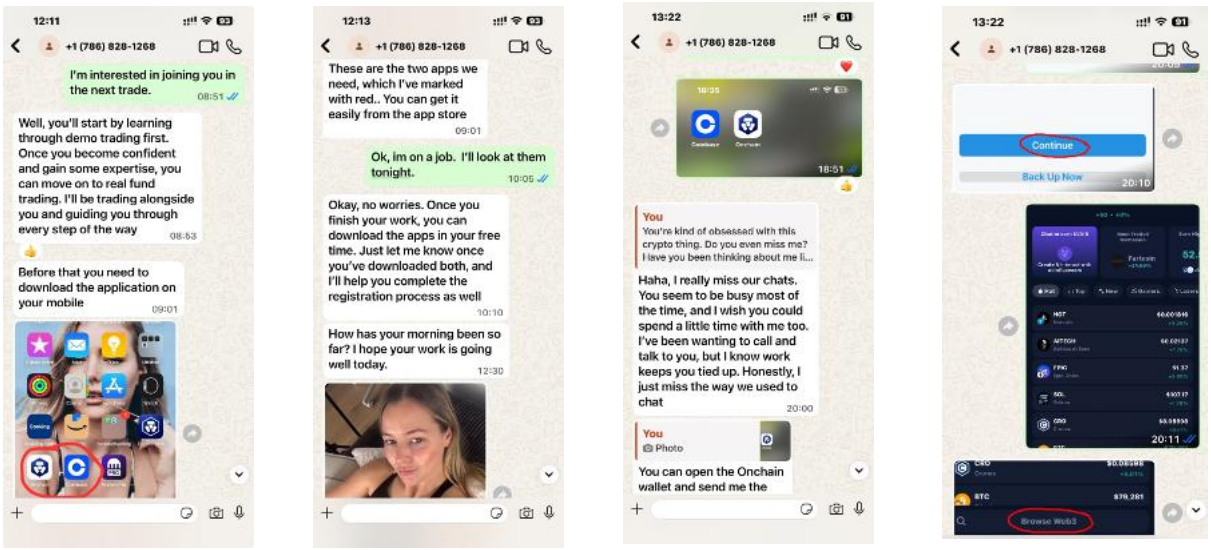
66

"Wrong number" Text Scams



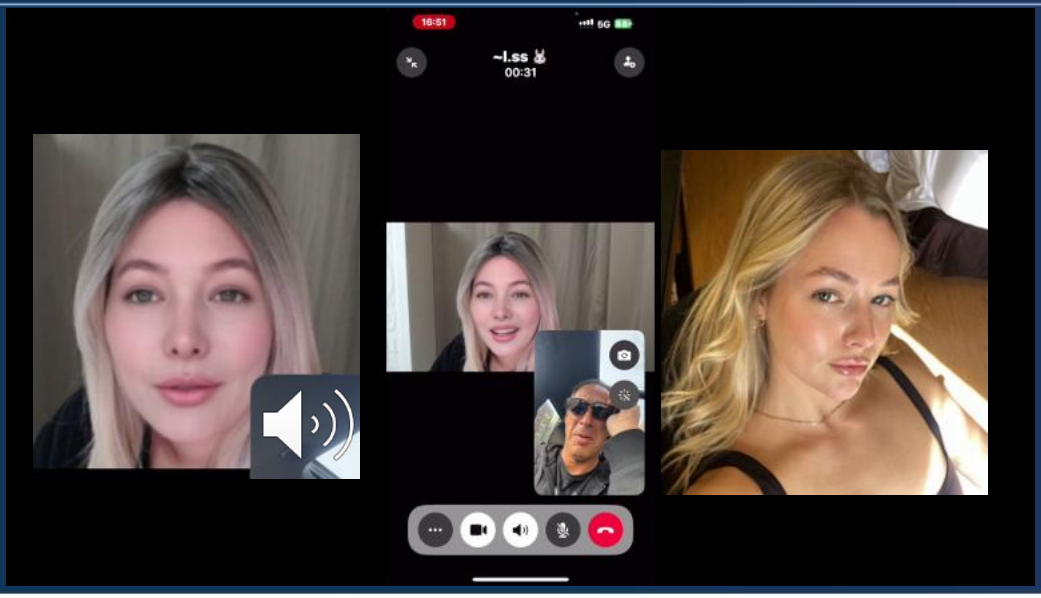
67

Pig Butchering



68

MY Pig Butcher-er Isla “ees-la”



protectnow

69



70



71

Real Time Intervention: Active Challenges

If a video call feels "off," perform these active challenges to disrupt the AI's rendering:

- **The Profile View:** Ask the participant to turn their head 90° to the side. Most real-time models are trained on frontal views and will "break" or dissolve in profile.
- **Physical Occlusion:** Ask them to wave their hand in front of their face or scratch their nose. This causes the AI "overlay" to flicker or glitch as it struggles to map the obstruction.
- **Knowledge Check:** Ask a question not findable on social media or in hacked email threads (e.g., "What was the name of the dog you had in third grade?").



protectnow

72

Operational Friction: The Only Real Defense

The most effective defense is not software; it is **Operational Friction**. The goal is to slow down the **Momentum of a Crisis**.

- **"Never Trust, Always Verify":** Implement a layered security posture. Use Multi-Factor Authentication (MFA) and require multi-party authorization for all wire transfers.
- **The Three-Step Playbook:** If a call is suspicious: **Flag** (verbally pause the call), **Isolate** (move them to a waiting room), and **Escalate** (use a secondary channel like an internal phone to verify).
- **Wet-Ink Signatures:** For high-value closings, insist on in-person verification or "wet-ink" signatures in the presence of a verified notary.
- **The Corp/Family Codeword:** Establish a secret phrase to verify identity during "emergency" or "grandparent" scams. If the person on the phone can't provide the word, it's a clone.
- **Limit Biometric Exposure:** Make social media profiles private. Stop providing the "raw materials" for your own deepfake by letting strangers scrape your voice and likeness.



protectnow

73

The Strategic Human Firewall™: Triple A Protocol

The **Strategic Human Firewall™** is a permanent governance mindset. The essential shift from **"I trust what I see" to "I verify everything"** The foundation of this firewall is the **Triple-A Protocol**.

The Triple-A Protocol: Your "Break the Fake" Playbook:

1. **Analyze: Recognize Manufactured Urgency.** The moment a request demands "secrecy" or "immediate action," stop. Your brain has moved into emotional reaction. Take a breath move back to analytical thinking.
2. **Authenticate: Identify the "Digital Mask."** Treat every digital communication as a potential breach. Look for the technical and biological "red flags" of a scam, fraud or deepfake.
3. **Act: Execute Out-of-Band (OOB) Verification.** Never use the contact information provided in the suspicious message. Hang up and call the person back on a trusted, pre-validated number. OOB techniques require verifying requests through a **secondary, independent channel** separate from the original contact method. Common techniques include placing a "voice-to-voice" phone call to a trusted number, or requiring a physical, in-person confirmation to authorize a transaction.



protectnow

74

CSI Protection Course Action Items

CSI PROTECTION CERTIFICATION

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 posses, secure.



- **TIPS:** Discuss with your client how to facilitate secure digital transactions
- **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.
- **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"

protectnow

75

CSI Protection Course Action Items

CSI PROTECTION CERTIFICATION

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 posses, secure.



- **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.

protectnow

76

SESSION #3

Identity Theft Protection, Prevention and Awareness



77

Equifax Breach Affects 146 Million Customers!

CSI PROTECTION CERTIFICATION





protectBOW

78

Making The Case To Get a Credit Freeze

- **Freezes credit reports** so lenders can't see your scores
- **Prevents new lines of credit** from being opened
- **Has no effect** on existing credit cards or credit lines
- **Requires a temporary "thaw"** prior to applying for a new line of credit
- **Set up all three credit bureaus mobile apps** on your phone and it's easy to temporarily thaw and refreeze credit.
- **Search: "Credit Freeze TransUnion" and Equifax and Experian**
- https://www.experian.com/help/credit-freeze/
- https://www.equifax.com/personal/credit-report-services/credit-freeze/
- https://www.transunion.com/credit-freeze
- https://www.innovis.com/personal/securityFreeze



79

CSI Protection Identity Course Action Items

CSI PROTECTION CERTIFICATION

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 posses, secure.



- **Credit Freeze:** Upon the consumers request, the 4 credit bureaus provide freezes on consumer credit reports preventing new account fraud. Keep good records so you can unfreeze whenever you need. And make sure to freeze your kids' credit and your parents' credit.
- **Credit Checks:** Check it at least annually and look for anomalies or accounts not authorized by you. Do the same for family members and request clients check theirs too.
- **Identity Theft Protection:** There are many services that offer identity theft protection. These services watch your credit reports, seek out your data on the dark web and provide restoration should your identity get stolen.
- **Information Security:** Make sure to print out, review and take action on the "Course Action Items" from the "Information Security: Data Theft Prevention and Protection" course to stop most forms of fraud and prevent most forms of digital identity theft.
- **Credit Cards:** Sign up for text or email alerts and notifications via your bank or card companies website. These alerts notify you in real time of charges, withdrawals, deposits on all card activity whether card present at a merchant, over the phone or not present online.

80

CSI Protection Identity Course Action Items

CSI PROTECTION CERTIFICATION

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 posses, secure.



- **Tax Identity Theft:** Head to IRS.gov, download and fill out form 14039 (Google it) the IRS Identity Theft Affidavit. If you have ever received notification your data was compromised in a breach, list it out on the form. Monitor your business credit to stay on top of potential fraud.
- **Medical Identity Theft:** Simply be cognizant of it. Monitor your insurance statements and any bills that come in. Consider not carrying your medical insurance card in your wallet unless you are going to the doctor that day.
- **Business Embezzlement:** If anyone other than you is responsible for or has access to your books and bank account then you need to have a forensics accountant come in at least biannually to make sure nothing is missing and the books are in order.
- **Mail and Sensitive Docs:** Get a locking mailbox. Shred everything disposable that can be used against you or a client.
- **ATM Skimming:** Cover up the keypad or monitor with your other hand while entering your PIN code. Pay attention to your statements.
- **Banking Online:** As long as your devices are properly secured then banking online is fine. Eliminate manual bill pay and set up EFTs via "Lifestyle" credit cards and enjoy more points and more security.

protectnow

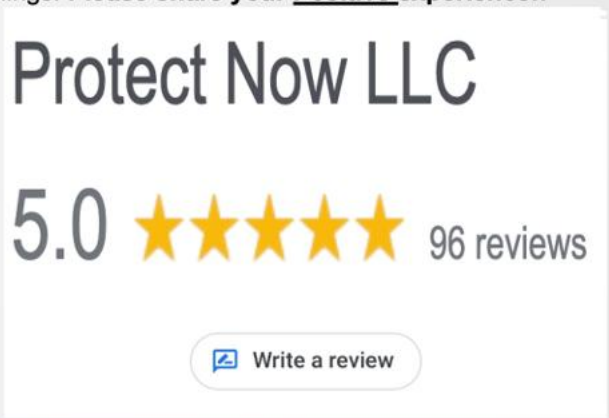
81

We Are Seeking Google Reviews!

CSI PROTECTION CERTIFICATION

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!!**



protectnow

82

Want To Learn More? Visit our Website!

CSI PROTECTION CERTIFICATION



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

ProtectNowLLC.com

protectnow

83