



Protecting Your Data & Personally Identifiable Information (PII) ...*Finally* Explained in Plain English!

Presented by

Wynn J. Salisch

CHS, ETA CPP

Principal, Casablanca Ventures LLC



Casablanca Ventures

Payments Intelligence

Powered
By



MERCANTILE
PROCESSING INC.

Wynn J. Salisch

CHS, ETA CPP

- Over 50 years in hospitality, payment processing and cyber security
- Graduate – The School of Hotel Administration at Cornell University
- Boards of Directors – Association of Lodging Professionals, Hospitality Financial & Technology Professionals (Vice President, NYC Chapter)
- Partner – United States Secret Service Electronic Crimes Task Force
- Member – National Cybersecurity Alliance
- ETA CPP – Electronic Transactions Association Certified Payments Professional, the payment industry's professional certification awarded for knowledge, professionalism, integrity, and excellence in payment processing, earned by less than 1% of the entire industry.





Casablanca Ventures

Payments Intelligence

Powered by



**MERCANTILE
PROCESSING INC.**

- **Casablanca Ventures LLC** is the hospitality industry’s oldest credit card processing and data security firm that specializes in highly personal “concierge” service – and saving money – for each of our clients, which has given us one of the longest client retention rates in the payments industry.
- **Mercantile Processing Inc. (MPI)** is a full service registered national processor and the official processor of the Maryland Bankers Association. Founded in 2006 by an actual hotel industry professional, MPI understands and prioritizes exceptionally prompt and friendly service for each of their clients at some of the lowest *lodging-certified* costs in the industry because it’s an efficiently run, family-owned processor with low overhead. It is completely independent and not part of any giant global conglomerate that requires higher margins from its subsidiaries.

Core Beliefs





The West Side Tennis Club & Forest Hills Stadium: “America’s Wimbledon”







“Data Breaches Soar, Remaining on the Rise for the Third Consecutive Year”



April 13, 2022



43% of cyber attacks target small businesses.

```
    @height & count < 2) {  
      @height : data.$image.outerHeight  
      @width : data.$image.outerWidth  
      @width;  
      @height;  
    }  
  }  
  @width;  
  @height;  
  @height);  
}
```

60%
of those hacked close
their doors within
6 months.

Why Would Miscreants Want to Hack Your PC?



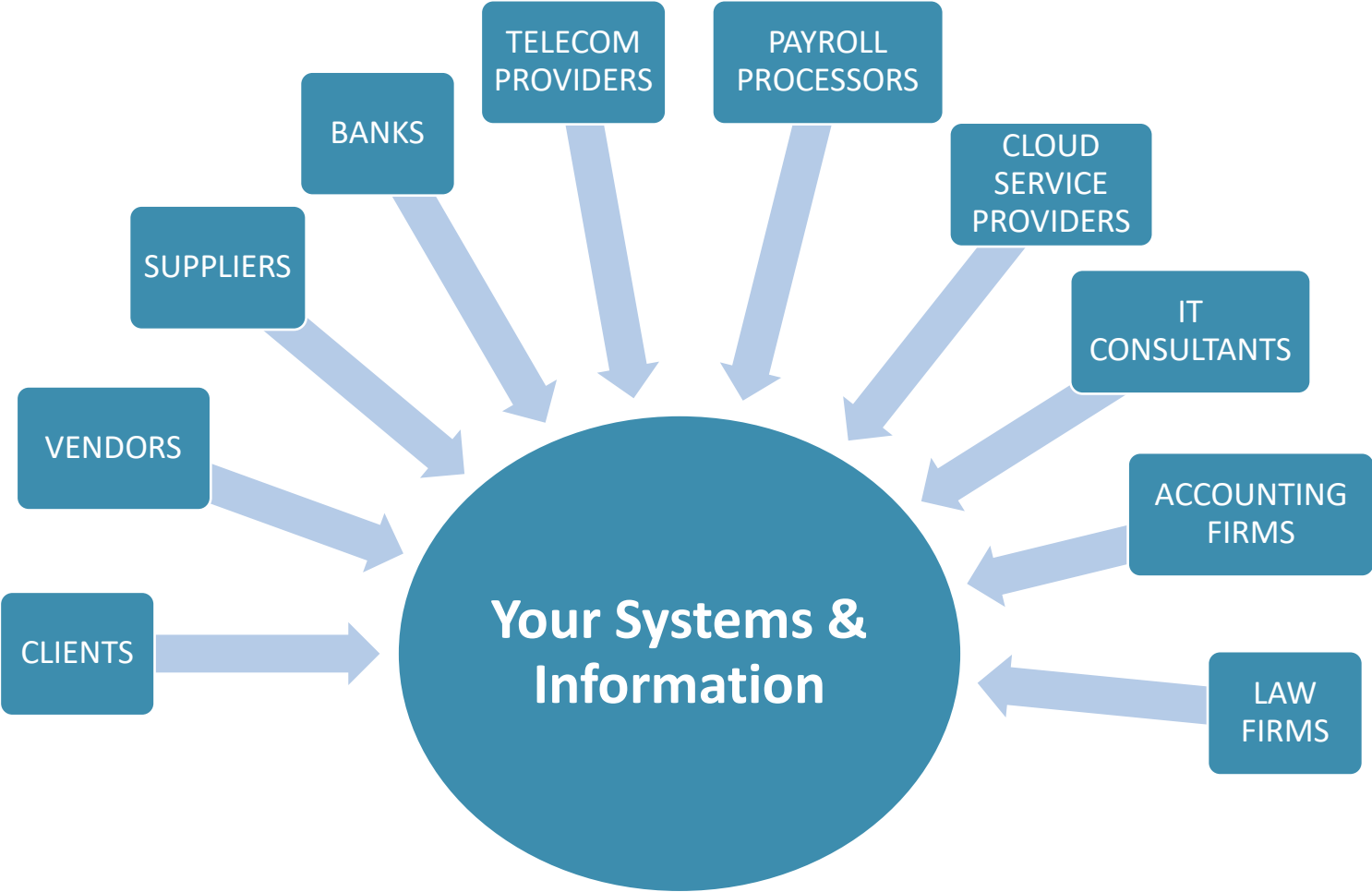
What's at Risk: *Everything!*

- Account Data – cardholder data, ACH/check info, Bitcoin private key
- Customer Data – PII, PHI, metadata, authentication info
- Corporate Data – sales, revenue, projections, employees
- Competitive Intelligence – pricing/cost, sourcing, new products, new markets
- Intellectual Property – R&D, processes, trade secrets, electronic products

10 common attack vectors



Trust Relationships



Phishing Accounts for 91% of Data Compromises



Don't Get Hooked!

Phishing

WHAT YOU NEED TO KNOW

SCAMMERS ARE AFTER YOUR



Passwords



Financial Info



Identity



Money

WHY DO WE FALL FOR THESE SCAMS?

- Urgency
- Curiosity
- Desire to please
- Complacency
- Greed
- Fear



PROBABILITY THAT A PHISHING MESSAGE SUCCEEDS
1 out of 10!



WATCH OUT FOR

- Spelling & Grammar Errors
- Sender Address
- Things That Sound Too Good to be True

BEWARE OF UNSOLICITED MESSAGES

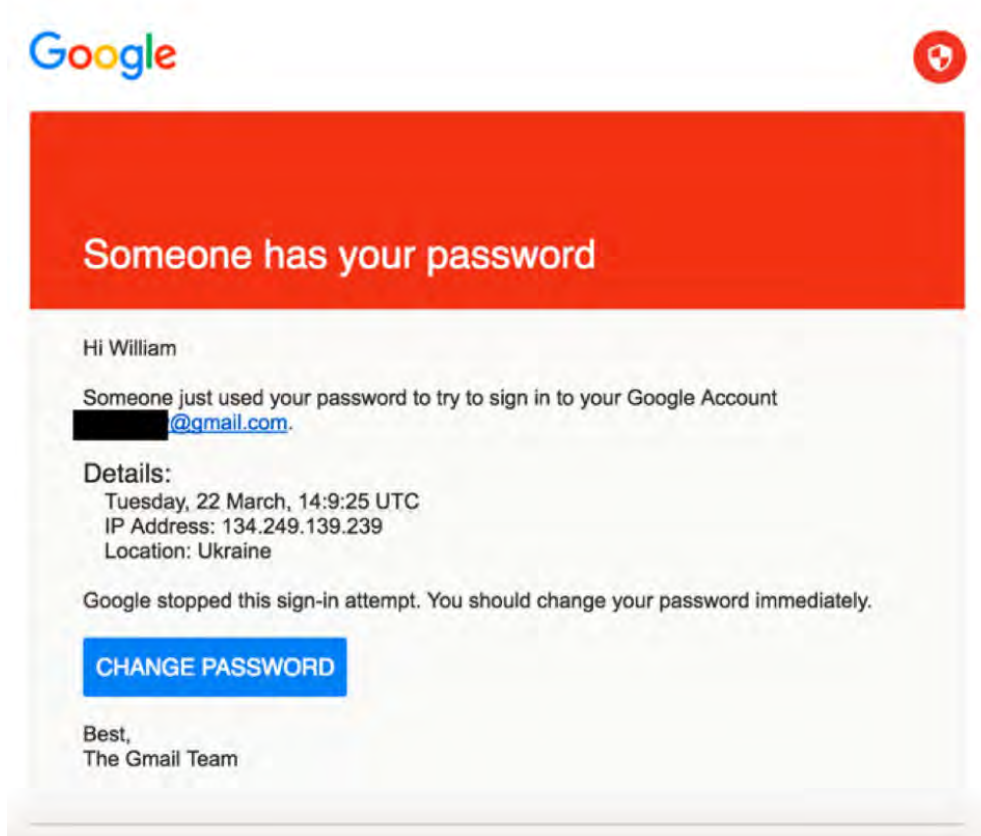
- Attachments
- Links
- Login Pages

IF YOU SEE SOMETHING, SAY SOMETHING!

Report phishing emails to spam@stanford.edu

security.stanford.edu

Don't Click on Embedded Links!



Google

Someone has your password

Hi William

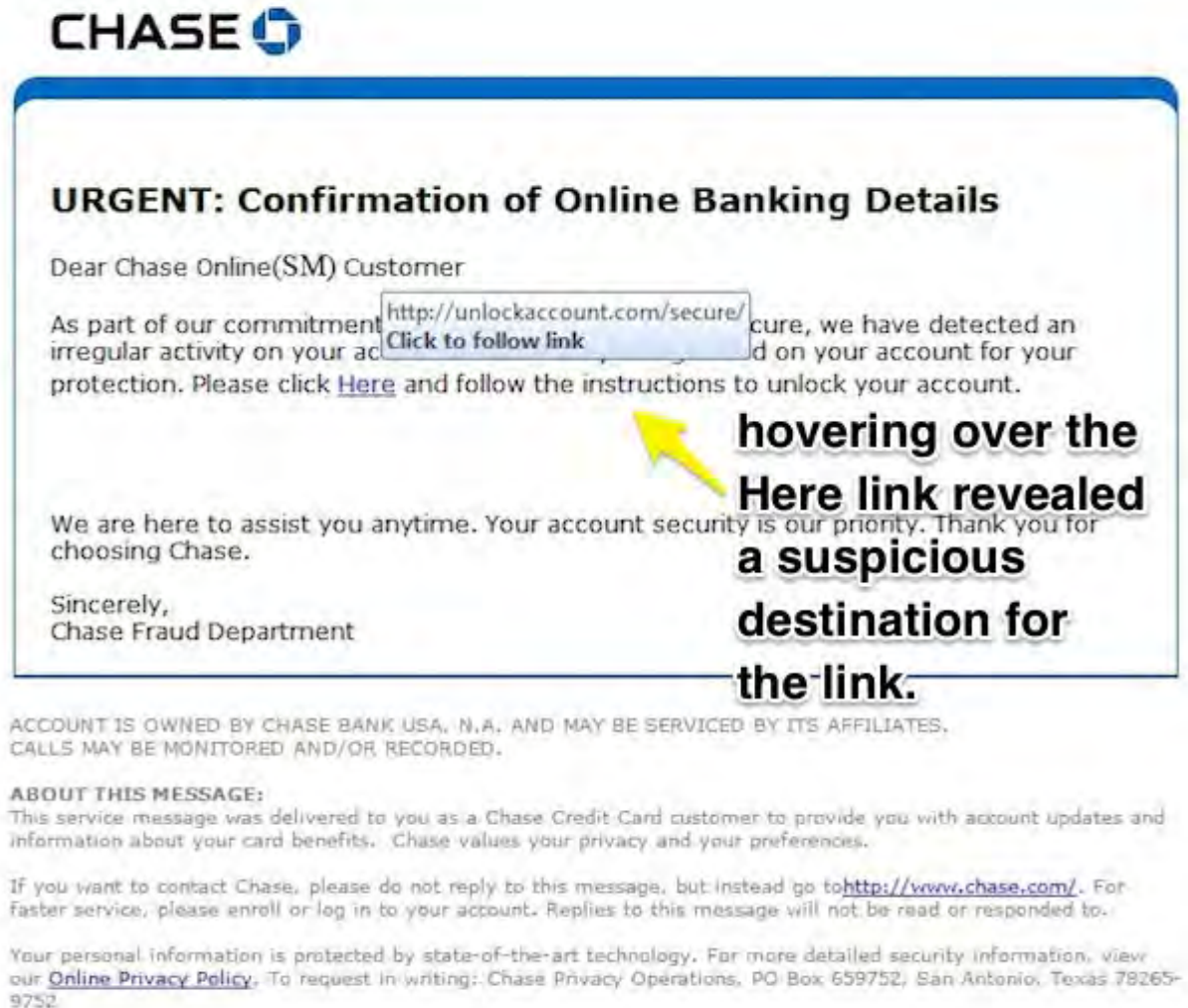
Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,
The Gmail Team



CHASE

URGENT: Confirmation of Online Banking Details

Dear Chase Online(SM) Customer

As part of our commitment to secure, we have detected an irregular activity on your account on your account for your protection. Please click [Here](#) and follow the instructions to unlock your account.

We are here to assist you anytime. Your account security is our priority. Thank you for choosing Chase.

Sincerely,
Chase Fraud Department

hovering over the Here link revealed a suspicious destination for the link.

ACCOUNT IS OWNED BY CHASE BANK USA, N.A. AND MAY BE SERVICED BY ITS AFFILIATES. CALLS MAY BE MONITORED AND/OR RECORDED.

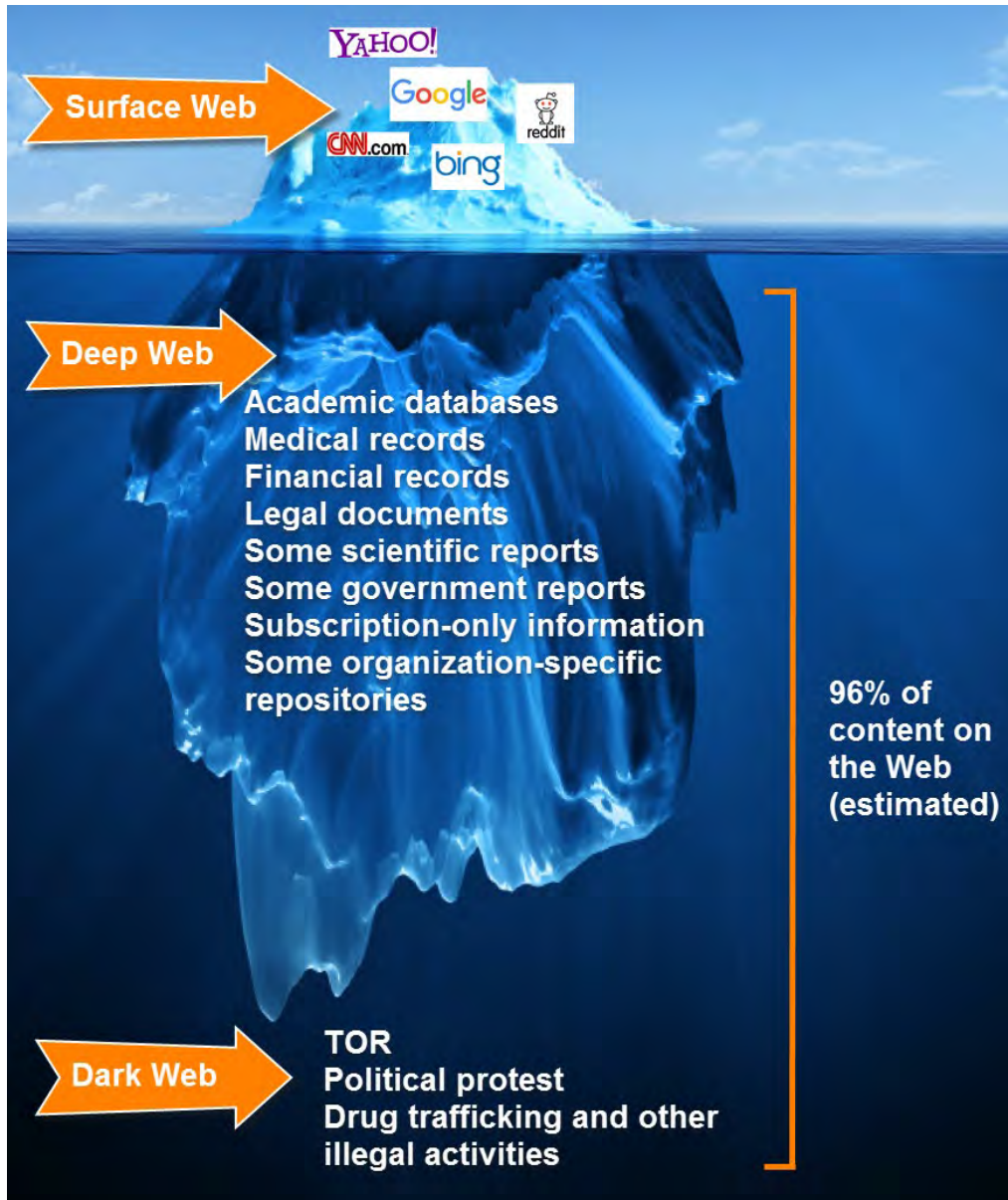
ABOUT THIS MESSAGE:
This service message was delivered to you as a Chase Credit Card customer to provide you with account updates and information about your card benefits. Chase values your privacy and your preferences.

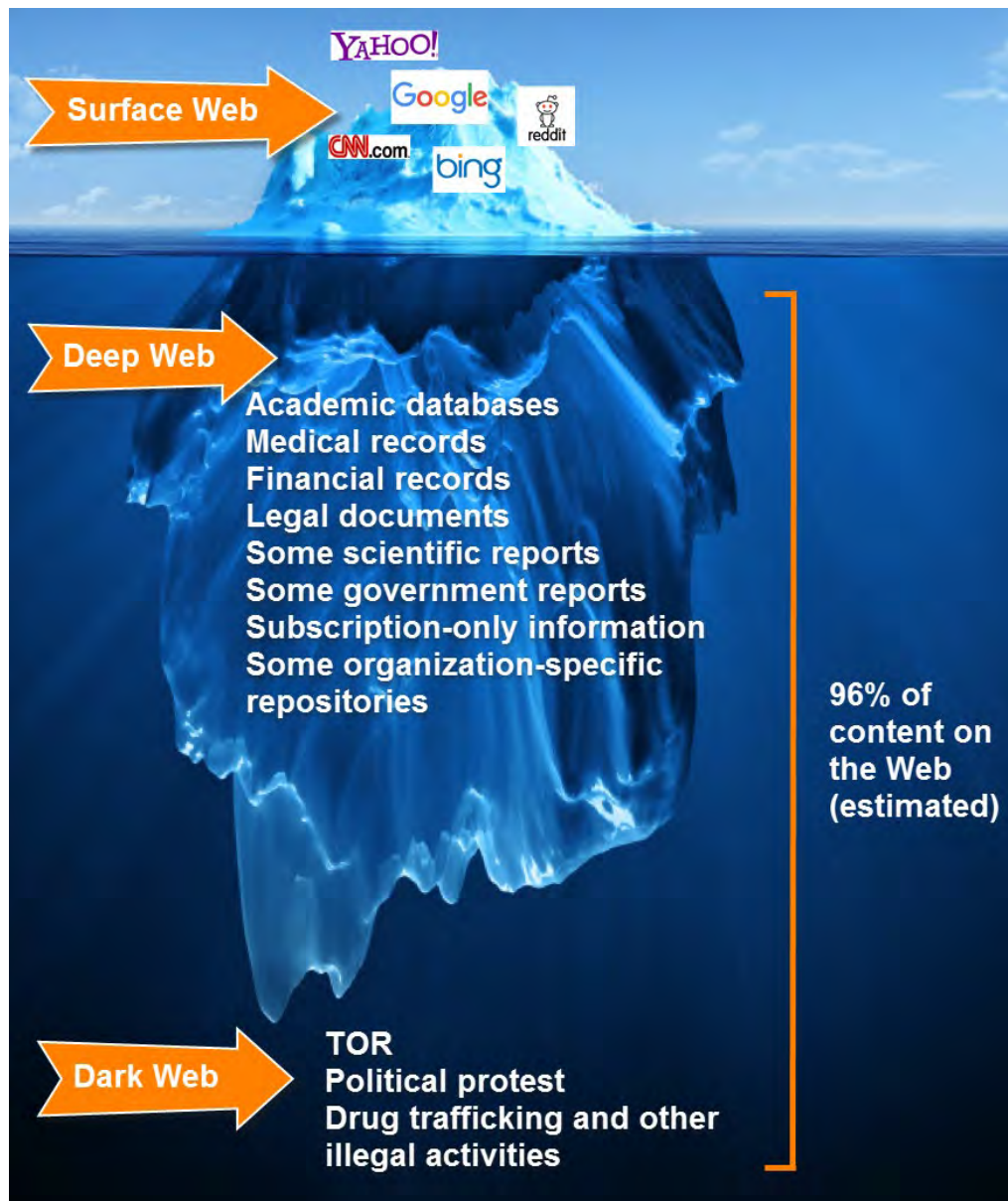
If you want to contact Chase, please do not reply to this message, but instead go to <http://www.chase.com/>. For faster service, please enroll or log in to your account. Replies to this message will not be read or responded to.

Your personal information is protected by state-of-the-art technology. For more detailed security information, view our [Online Privacy Policy](#). To request in writing: Chase Privacy Operations, PO Box 659752, San Antonio, Texas 78265-9752.

Phishing Lessons

- Don't click on links in emails or open attachments unless you recognize the source.
- Even then, be careful. A healthy dose of skepticism is advisable in our online world.
- Hackers spoof emails to look almost exactly like the page you're used to seeing.
- Watch for red flags such as urgency and grammatical, spelling, punctuation, and syntax errors.
- Be cautious and wary and inspect the email address for strange features like extra digits or characters (e.g., a lower-case L can be substituted for an upper case I to result in an entirely different URL).
- Instead, open your browser and enter the URL for the page from your records, don't use the link in the email.
- Don't re-use passwords.
- Turn on your spam filters.
- To avoid phone phishing attempts, when in doubt, hang up, look up, and call back.
- Real World Lesson: Clicking on a Change Password link is how John Podesta, the chairman of Hillary Clinton's presidential campaign, had his email account compromised. Logging in via the embedded Change Password button exposed his username and password to the hackers. What he should have done instead was to close the email, open his browser, log into his Gmail account via his known link, and change his password that way.





HOW DO YOU ACCESS THE DARK WEB?











The dark web can be accessed through specific browsers. The most popular browser is The Onion Router or simply known as TOR. Because the websites in the dark web are not indexed, the use of TOR hides the IP addresses of websites within the dark web to maintain its anonymity. The IP addresses are hidden using the .onion suffix.



For Sale: Everything & Anything

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$45,000	\$90,000	\$180,000
Missing in action	\$60,000	\$120,000	\$240,000
Death in accident	\$75,000	\$150,000	\$300,000
Cripple Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$12,000	\$24,000	\$48,000
Uglify	\$18,000	\$36,000	\$72,000
Two Hands	\$24,000	\$48,000	\$96,000
Paralyse	\$30,000	\$60,000	\$120,000
Rape	Low Rank	Medium Rank	High Rank and Political
Regular	\$7,000	\$14,000	\$28,000
Under age	\$21,000	\$42,000	\$84,000
Bombing	Low Rank	Medium Rank	High Rank and Political
Simple	\$5,000	\$10,000	\$20,000
Complex	\$10,000	\$20,000	\$40,000
Beating	Low Rank	Medium Rank	High Rank and Political
Simple	\$3,000	\$9,000	\$18,000

Dark Web Prices

 Social Security \$1	 DDOS as a service -\$7 per hour
 Medical record \$50 and up	 Credit card data \$0.25 to \$60
 Bank account info \$1,000 and up <small>depending on the account type and balance</small>	 Mobile malware \$150
 Spam \$50 for ~500,000 emails	 Exploits \$1,000-\$300,000
 Maleware development \$2,500 <small>(Commercial malware)</small>	 Facebook account \$1 for an account with 15 friends

SOURCE: RSA CNBC

Credit Card Dumps

What are the bank logins and credit cards available?

Some Of US \ UK Banks Available Now

• For United States Of America Banks

Bank Names	Balance	Price	Preview Screenshot
Bank Of America	Between 2k - 50k	400\$	Download
WellsFargo	Between 4k - 40k	300\$	Download
Chase Bank	Between 2k - 30k	250\$	Download
Citibank	Between 9k - 70k	300\$	Download
Wachovia	Between 2k - 18k	275\$	Download

• For United Kingdom Banks

Bank Names	Balance	Price	Preview Screenshot
Barclays	Any Balance	400\$	Download
HSBC	Between 30k - 312k	400\$ up to 100k=600\$	Download
Halifax	Between 20k - 180k	450\$	Download
Nationwide	Between 15k - 230k	450\$	Download
Lloyds TSB	Between 10k - 400k	600\$	Download

If You Are Not Able To Raise The Amount For Any Of The Logins, I Can Make For You Any Transfer To Any Bank Listed With Upfront 250\$ And My Share 20%

Payments With : E-gold, Western Union, Moneygram, Moneybookers.

VERIFIED HACKER GENUINE

CREDIT CARD

ICQ 664198618

ATM Dumps Cashout

DUMPS | TR1 | TR2 + PINS

*** ONLY CODE (101) * USA - CANADA - EURO - CHINA - JAPAN - KOREA ...**

*** High Balance 3.000 To 10.000 (USD/EURO) * Fresh Validity 85%-95%**

NEW DUMPS + PINS IN STOCK VALIDITY 95% OF CARD

5422937190153322-18022011769807369310? PIN: 8584
 6769925867666743-16102211963221500000? PIN: 5698
 432484527928860-18102211412699500000? PIN: 2252
 5351781510029530-18092211246702271217? PIN: 5576
 4324845271142993-17112211685124000000? PIN: 6417
 4324845257070903-18102211962031800000? PIN: 9635
 4324845271679143-19072211553797200000? PIN: 9387
 4324845259465952-17072211422311200000? PIN: 0653
 4324845259940434-17102211954331800000? PIN: 6584
 5351781510443509-19072211341706833314? PIN: 6430
 4324815590217594-17112011733550100000? PIN: 5750
 4324845258628576-19042211773996100000? PIN: 9573
 4324845270443533-19032211092741000000? PIN: 3098
 4324845271141086-16112211632130400000? PIN: 5635
 5351781510392755-18102211592103216686? PIN: 8043
 4324845257962521-19082211818395600000? PIN: 4151
 4324845270428229-19032211385672100000? PIN: 2143/3143
 4324845271288911-18022211763870300000? PIN: 0306
 4324845271007774-17082211067894090000? PIN: 1121

*** BINLIST --- ICQ 664198618 --- GOOD BUSINESS A LONG TERM

LIST PRICE DUMPS VALID 85%-95%

** Card Dumps Usa :101, 201
 - Visa Classic/Master Standard = 40\$
 - Visa/Master/Amex/Discover (Gold,Platinum) = 45\$
 - (Business,Signature,Purchase,Cooprate,Word) = 50\$

** Card Dumps CA + AD: 101 201
 - Visa/Master Standard = 55\$
 - Visa/Master/Amex/Discover (Gold,Platinum) = 60\$
 - (Business,Signature,Purchase,Cooprate,Word) = 70\$

** Card Dumps ED + ASIAN: 101 201
 - Visa/Master Card (Classic,Standard) = 60\$
 - Visa/Master/Amex/Discover (Gold,Platinum) = 70\$
 - (Business,Signature,Purchase,Cooprate,Word) = 80\$

** Other countries: 101 201
 - Visa/Master Card (Classic,Standard) = 60\$
 - Visa/Master/Amex/Discover (Gold,Platinum) = 70\$
 - (Business,Signature,Purchase,Cooprate,Word) = 80\$

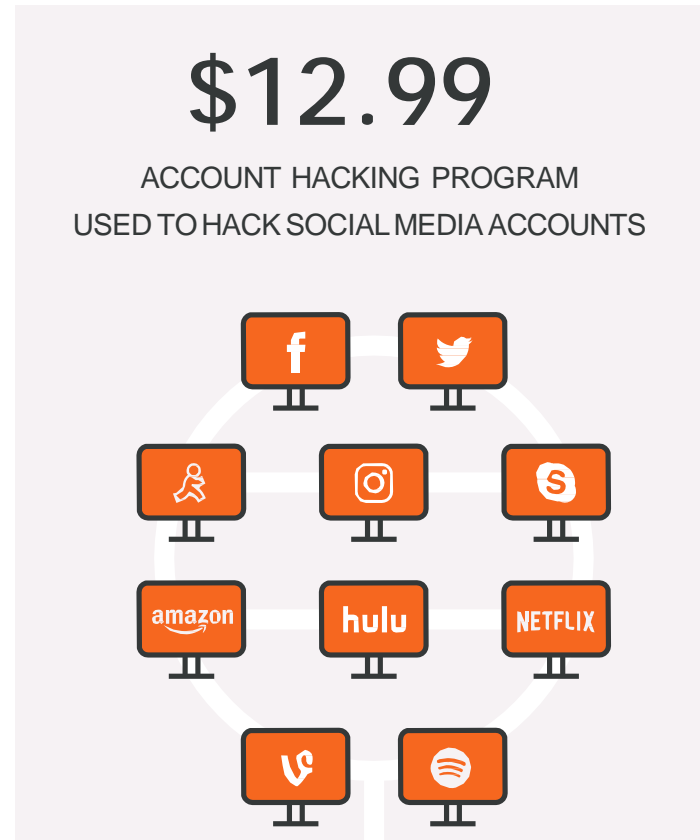
*** WITHDRAW MONEY FROM ANY ATM + SHOPPING

RULES MY BUSINESS

- + NO TEST FREE , NO SPAM
- + NO RIPPER, NO SCAMMERS
- + EXCHANGE MONEY
- + BANK LOGINS USA-UK-CA
- + CHANESL.WEBMAIL
- + METHODS PAYMENT
- + OLD ACCOUNT ELECTRONIC
- + SMTP-RDP-MAILPASS-LEADS
- + CREDIT CARD
- + DEBIT CARD
- + PULLZ INFO WITH PIN
- WE ACCEPT PAYMENT
- * BITCOIN
- * PERFECTMONEY
- * WEBMONEY
- * WESTERNUNION
- * MONEY GRAM

*** MERRY CHRISTMAS ***
 *** ALL CUSTOMERS ***
 *** BIG!!!MONEY ***

You Too Can Learn to Hack!



HACKED ACCOUNTS ARE THEN USED FOR:

Purchasing Products | Broadcasting | Verification | Cashouts and more.

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **Send \$300 worth of bitcoin to this address:**
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

THE STATE OF RANSOMWARE AMONG SMBs



In the last 12 months

22% of organizations had to cease business operations immediately because of ransomware

81% of businesses have experienced a cyberattack

66% have suffered a data breach

35% were victims of ransomware

Malwarebytes

INFECTION TO ENCRYPTION IN 3 SECONDS



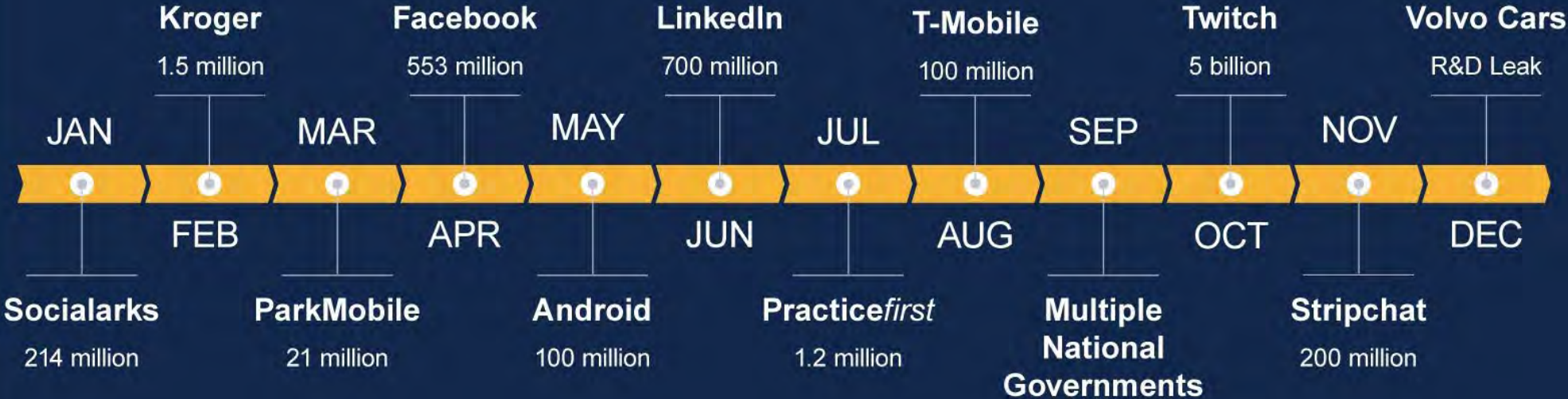
How to Prepare for a Ransomware Attack

1. **Stay educated and up to date on ransomware risks.** Keep an eye on news concerning the latest threats.
2. **Know what data you stand to lose.** If you know what data is at risk for your company and where it's all stored, you will know how to prioritize scheduling backups and investing in offsite storage.
3. **Make sure everyone you work with is focused on security.** Third parties, partners, and supply chain elements could all introduce ransomware risks that could affect your company. Talk with anyone who accesses your data about their security plans.
4. **Review and test your incident response plan.** Who will you call to get your computers back online during a ransomware attack? How much are you willing to pay to get your data back? How long can your business remain offline during a security incident? It's important to create and regularly review an incident response plan to make sure you aren't at the mercy of a ransomware group.
5. **Implement a zero-trust strategy.** Eliminate implicit trust. This means every authorization request and every session must be validated before a user can continue on the network. Validating at every stage of every digital interaction makes it harder for attackers to get in and wreak havoc.

How to Prepare for a Ransomware Attack

- 6. Identify your exposed assets.** What's on your social media feeds? What's in your inbox? Any information about yourself and your business you make public is in danger of being exposed in a data breach or used as fodder for ransom attacks. Don't get caught unawares. Protect your logins with complex, hard-to-guess passwords that you keep in a password manager's encrypted vault.
- 7. Identify and block potential threats.** Keeping exploits, malware, and command-and-control traffic at bay takes away easy targets from attackers.
- 8. Learn how to automate your protection.** Use tools such as antivirus protection that will detect ransomware threats early so you can respond and recover quickly.
- 9. Secure your cloud presence.** To launch ransomware attacks in cloud environments in the future, criminals will probably use tactics we have yet to encounter. Prepare your business by using identity and access management software (visit www.pcmag.com) to secure cloud APIs.
- 10. Reduce response time with retainers.** Keep incident response experts on speed dial. They can help you create a budget for responding to a ransomware threat and thus take faster action to get you back in business faster.

Most Impactful Data Breaches of 2021



MEDIA S(📡)NAR

The Target Breach

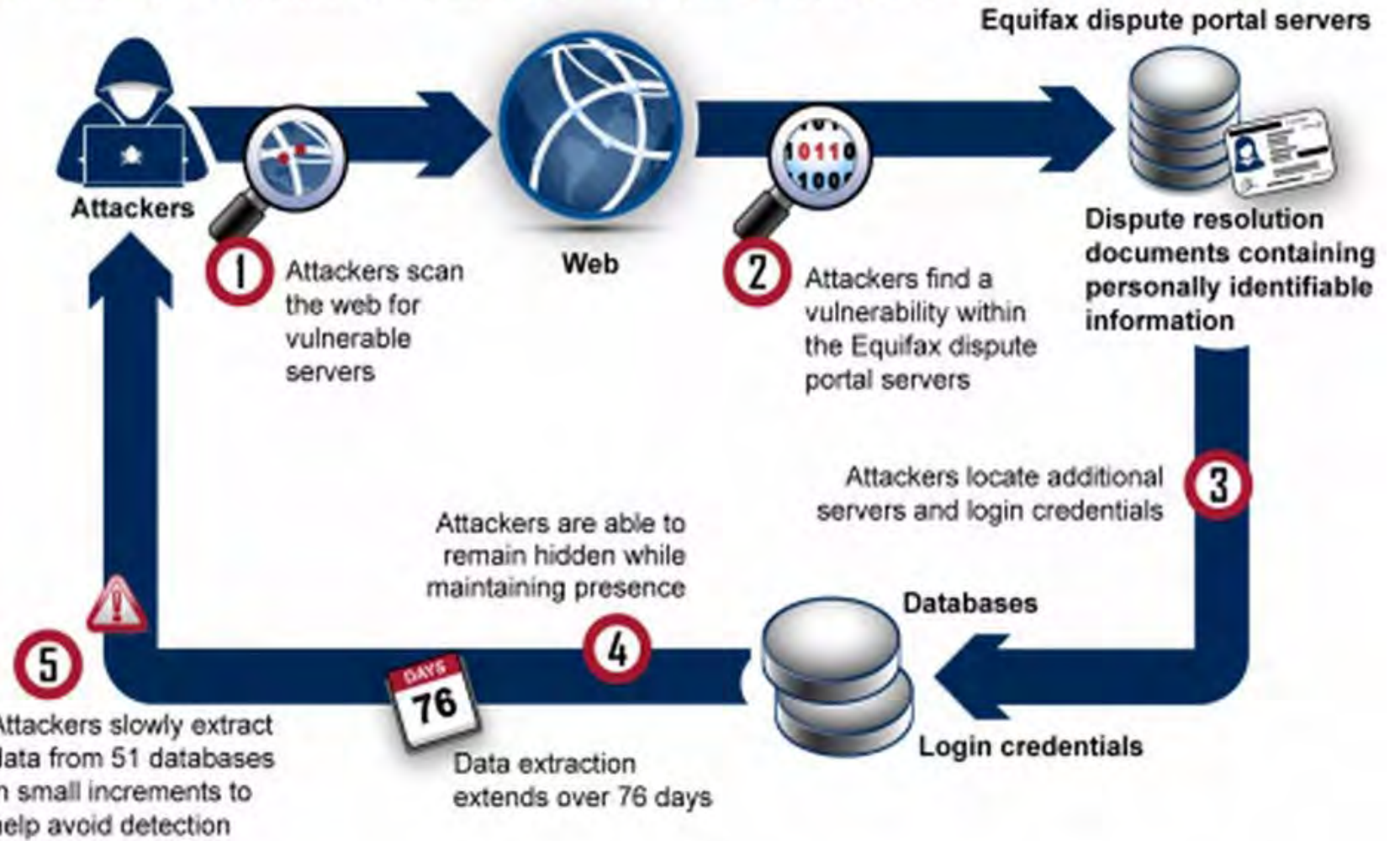


1. All Target stores used same HVAC contractor.
2. Malware delivered in an email to employees.
3. VPN (Virtual Private Network) credentials used by the contractor to remotely connect to Target's network were then stolen.
4. That foothold was then used to push malicious software down to all of the case registers at more than 1,800 stores nationwide.
5. DAMAGE:
 - 70 MILLION credit & debit card account numbers stolen.
 - \$595,000,000.00 estimated value to the hackers.
 - Total cost to Target: \$291,000,000.00 *PLUS* lost sales and profits due to reduced consumer trust.



The Equifax Breach

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information



Source: GAO, based on information provided by Equifax. | GAO-18-559

United States Government Accountability Office

A Lesson from the Marriott Breach



500 Million

guests were affected by the 2018 data breach at the Marriott Hotel chain.



\$350 Million

is the cost of 50 million records - the Marriott breach is ten times bigger.



\$3.5 Billion

is the total cost that the Marriott Hotel chain could face over the next several years.

Card Testing Attacks on the Rise

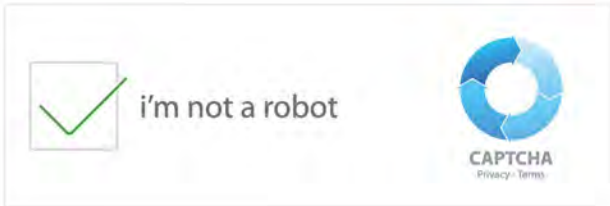
- A fraudulent card testing attack **begins with fraud actors acquiring stolen partial or full card credentials**. The fraud actor will then use various digital tools, including bots or scripts, that can rapidly submit hundreds of thousands of card-not-present (CNP) transaction authorization requests on an e-commerce site.
- **Impact of Card testing** – card testing can be detrimental to ecommerce, especially small to medium sized businesses. Due to the large scale of transactions processed as a result of card testing, unfortunate businesses targeted by card testing attacks suffer:
 - **Disputes (or Chargebacks)** – cardholders become notified upon successful payments, leading to high disputes and an increase in chargeback ratio
 - **High Decline Rates** – large number of declines may raise alerts to banks; high decline rate when associated with the BIN can also damage the reputation of issuer banks
 - **Extra Costs** – surge of testing transactions will accumulate a large sum of interchange fees charged by the authorization process. Not only will merchant pay for extra costs of interchange fees, but also the cost of disputes and dispute fees that will emerge.
 - **System and Network Performance** – consumes system capacity and network bandwidth

Card Testing Attack Remediation

1. **Set Card Limits** – add a maximum number of new cards allowed daily from a single IP address
2. **Velocity Control and Lock Out Mechanism** – limit the number of transactions submitted over a specified period and lock out customer or IP address if detected
3. **Decline Restrictions** – block IP address or customer if ‘transaction declined’ for a specified number of times
4. **Refund Fraudulent Transactions** – to avoid further financial and reputational repercussions, merchants should make effort to refund fraudulent transactions, when possible, to maintain customer satisfaction and reduce opportunities for disputes.
5. **Secure Checkout Cart and Payment Page** – employ tools to prevent bots or automated scripts from submitting transactions e.g., **CAPTCHA** (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part)

CAPTCHAs

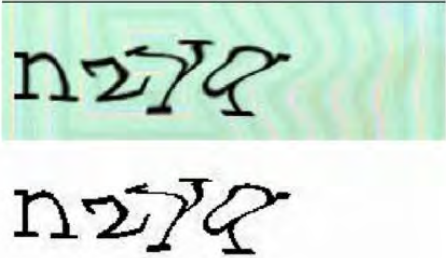
i'm a captchal



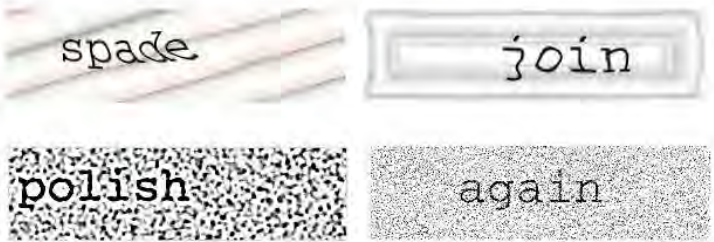
Gimpy



Gimpy-r



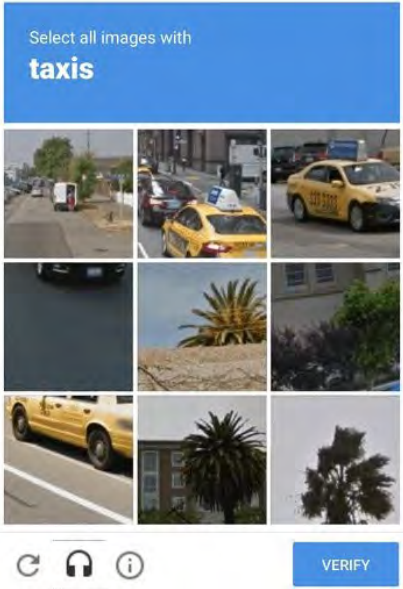
EZ-Gimpy



Simard's HIP



Image CAPTCHA



Improve Security, Enhance Guest Relations, and Save Money with EMV

- **Reduce vulnerability to hackers** within hotels' Local Area Network (LAN) — data coming out of EMV terminals is encrypted.
- **Reduce your PCI footprint** — data encrypted by EMV chip readers can only be decrypted by the processor, thus making your PCI compliance easier to achieve.
- **Reduce your chargeback risk** — as of Oct. 2015, hoteliers processing credit cards with chips the old-fashioned way (reading magnetic stripe) are now liable for fraud instead of the issuing bank. When guests see you swipe their chip card instead of dip or tap it, some engage in friendly fraud and call their issuer to claim they were never at your hotel, and because you didn't process the transaction with the chip, you'll lose the chargeback dispute.
- **Meet expectations of security-savvy guests** — hotel guests appreciate merchants that take extra steps to protect their credit cards from theft.
- **Offer guests modern payment alternatives** — most EMV-equipped terminals can accept EMV-NFC (Near Field Communications) chip mobile payments like Apple Pay, Google Wallet, and Samsung Pay.
- **Electronic guest signature** — upon check-in, guests can sign using built-in electronic signatures pads on some EMV readers, making signature retrieval easier when necessary to dispute chargebacks.
- **SAVE MONEY** — if a merchant has greater than 10% fallback transactions monthly (a “fallback” occurs when a chip card is presented in a face-to-face transaction, but the card is swiped instead of dipped or tapped), VISA now charges a Non-EMV Fallback Fee of \$0.10 per transaction, and some processors then add their own penalties of up to \$300 a month and 0.65% tacked on to the Interchange cost of each fallback transaction.

Beware: Your Digital Voice Assistant is Listening!



Protect Your DVA from Hackers

- 1. Watch what you connect** – Since your voice assistant can be a hub for your connected devices — lights, thermostat, TV — be selective about what you connect. It's smart not to connect security functions, such as a door lock or a surveillance camera. You don't want a burglar to yell "Unlock the door!" and have your voice assistant oblige. At the same time, you should disable the feature that links your calendar or address book — often rich sources of information.
- 2. Delete commands** – Smart speakers allow you to listen to your past commands and to erase some or all of them. This is a good way to wipe any sensitive information that may be stored. It's true, your device may have to "relearn" a command, but it's a quick learner.
- 3. Be careful what you share** – There's plenty of information you don't want your voice assistant to know. That includes your passwords, credit card information, and Social Security number. Remember, it's possible anyone could access your sensitive personal information just by asking for it.
- 4. Turn off the microphone** – Consider muting your device when you're not using it. That's the easiest way to get your device to stop listening. Of course, you'll have to turn it back on next time you want to check the weather. Or you could look outside.
- 5. Turn off purchasing** – Smart speakers often can be set to make purchases on command. Anyone with access to the device may be able to make a buy. That could be a problem. The solution? Set up a purchase password and keep it a secret.
- 6. Stay on top of notification emails** – What if someone happens to slip in a purchase. You'll usually receive a notification email. If it's something you didn't order — maybe it's something suspiciously suited to your 12-year-old — you can cancel it.
- 7. Turn off "personal results"** - Your voice assistant may help you to pay bills and manage other personal information. That could expose information you'd rather keep private, such as passwords or bank account numbers. One option? Turn it off.
- 8. Mind your network** – Use a WPA2 encrypted Wi-Fi network and not an open hotspot at home. Create a guest Wi-Fi network for guests and unsecured IoT devices.
- 9. Enable voice recognition** – You may be able to configure your device for voice recognition. This enables your device to tell different voices apart. This can be helpful, but it may not work all the time.
- 10. Strengthen your passwords** – Protect the service account linked to your device with a strong password. If it's available, use two-factor authentication. This can prevent anyone who has access to the account from listening in remotely.



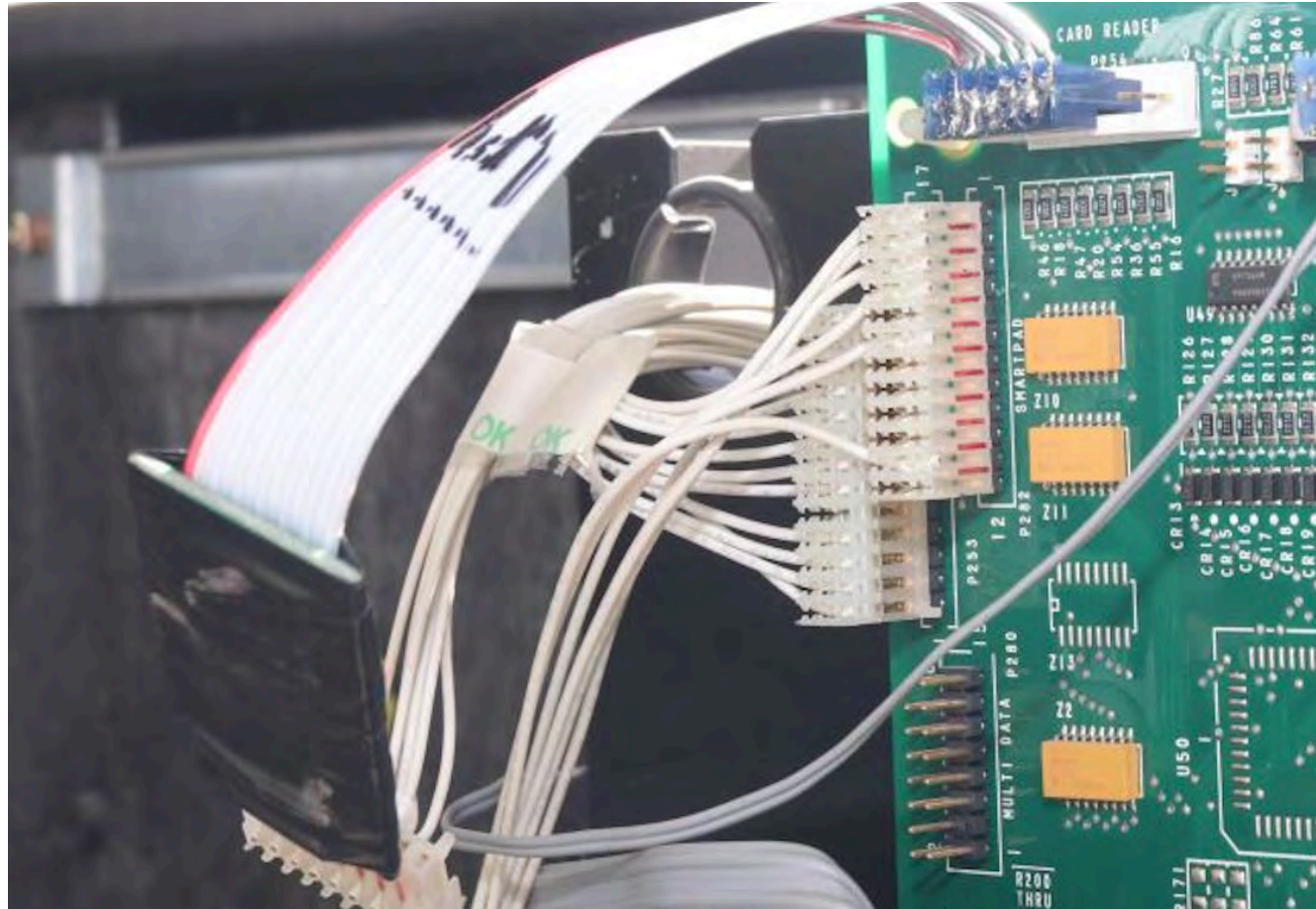
The compromised pump with the hidden camera bar still attached. Newer, more secure pumps have a horizontal card reader and a raised metallic keypad.



The fake panel (horizontal) above the “This Sale” display obscures a tiny hidden camera angled toward the gas pump’s PIN pad.



A front view of the hidden camera panel.



The unauthorized Bluetooth circuit board can be seen at bottom left attached to the pump's power and card reader.

Discovering a Breach

Average time it takes a company to detect that they've been breached:

250-300 days

Source: 2017 Nuix Black Report

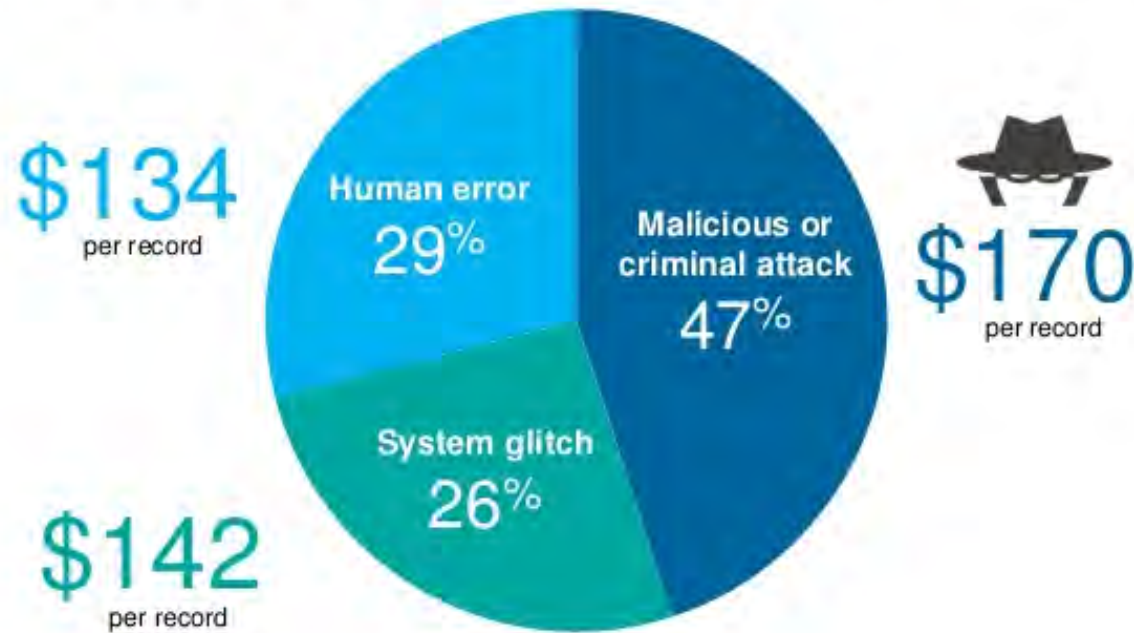
A Public Relations Nightmare



Breaches are Expensive!



Malicious or criminal attacks are the leading root cause of a data breach...and result in the highest cost per record.



Breaches are Expensive!

IBM

Malicious or criminal attacks are the leading root cause of a data breach...and result in the highest cost per record.



A Breach Can Put You Out of Business

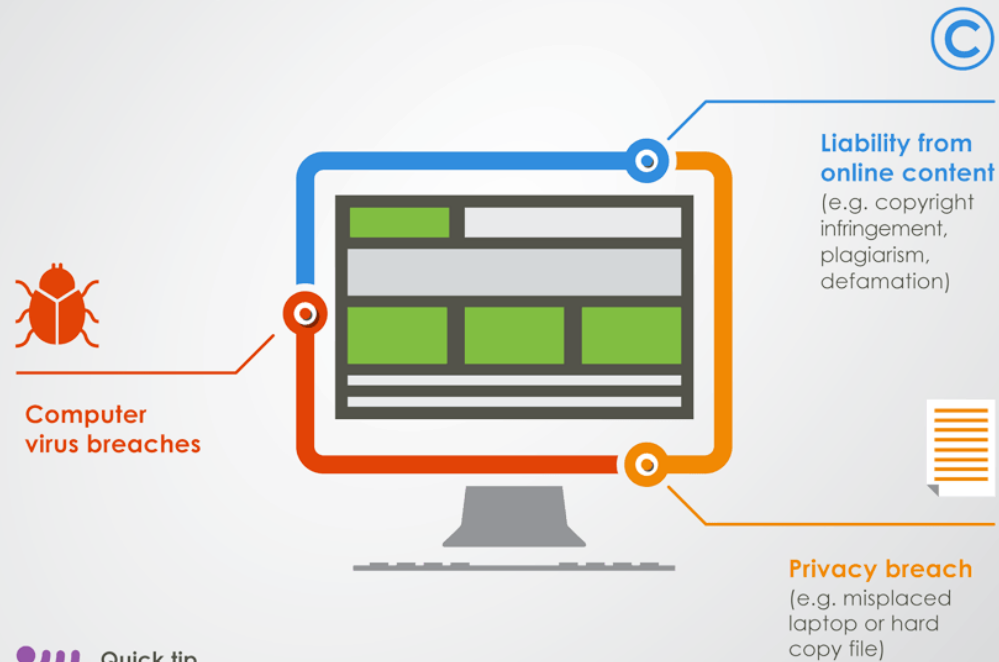
<u>Variable</u>	<u>Example 1</u>	<u>Example 2</u>
Number of rooms	10	15
÷ Average stay	2 nights	2.5 nights
x 365 days	365	365
x Years of storage compromised	3	5
x Cost per record	\$170	\$170
= Total cost of a data breach	\$930,750	\$1,861,500

Breach Remediation Item	Approximate Cost
PCI Forensic Investigator	\$50,000 to \$500,000 +
Forensic investigation	\$12,000 to \$100,000 +
Accelerated Remediation: Short-term - Stop the bleeding Controls (low-hanging fruit) & full PCI gap assessment Long-term processes and procedures, and tactical and strategic fixes	\$200,000 to \$500,000 + \$500,000 to \$1,000,000 + \$1,000,000 to \$10,000,000 +
Card brand compromise fines	\$5,000 to \$50,000 +
QSA assessments	\$20,000 to \$100,000 +
Free credit monitoring for affected cardholders	\$10 to \$30 per card
Card re-issuance penalties	\$3 to \$10 per card
Breach notifications - each affected cardholder must be notified as required by their own (not just your) state's law, usually within 30 days of when the PFI confirms the breach and notifies you; there are significant fines for violating state deadlines	\$2,000 to \$5,000 +
Technology repairs	\$2,000 to \$10,000 +
Legal fees	\$5,000 to \$100,000 +
Increased card processing fees	
Civil judgments	
Reputational costs - after a breach, many businesses have lost up to 40% of their sales from customers losing confidence in their brand	Up to 40% of sales
PR & marketing communications firm retainer	Expensive!
Insurance co-pays	

Coverage snapshot: Cyber liability insurance

All businesses – small businesses are especially vulnerable, and are top targets for cyber criminals

First- and third-party losses resulting from:



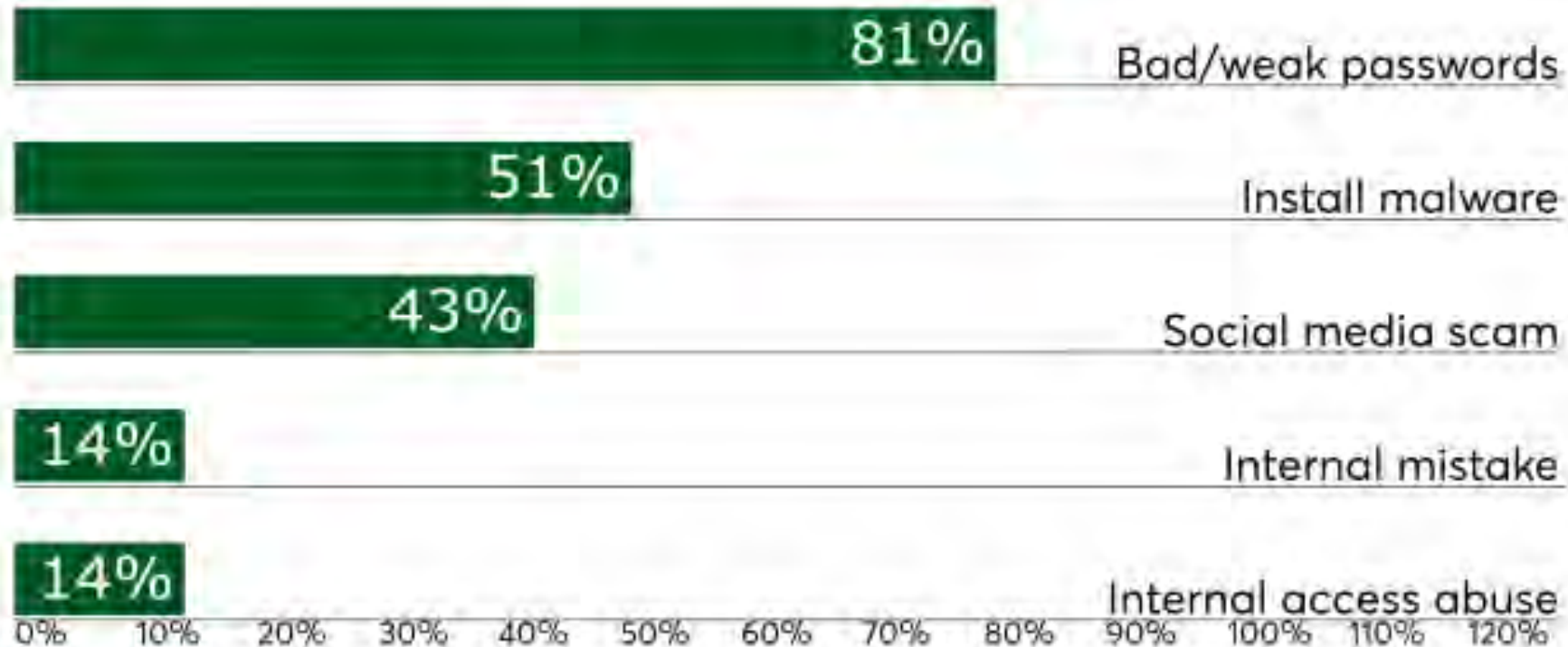
Quick tip
Cyber criminals may use your networks (which includes technology like smart thermostats) to gain access to your larger clients' data

Password Pain



The problem with passwords

Hackers have more than one way to get in, but passwords are the most common soft spot



Source: Verizon

Bad Passwords Have Consequences!

- **Financial losses** for both businesses and consumers.
- **Lack of privacy.**
- **Theft of your personal information.** After gaining access to a user's credentials, many hackers will log into their accounts to steal more of their personally identifiable information (PII) like their names, addresses, and bank account information. They will then use this information either to steal money from the user directly or to steal their identity. Identity theft can result in further financial losses or difficulty getting loans or employment.

The 50 Most Used Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 11111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

Multiple Passwords Are A MUST!

The average person regularly visits **25 password** protected sites BUT only uses **6 different** passwords.

73%

of people use the same password for multiple sites

33%

of people use the same password for EVERY site

32%

of people save passwords and other login information on a cell phone

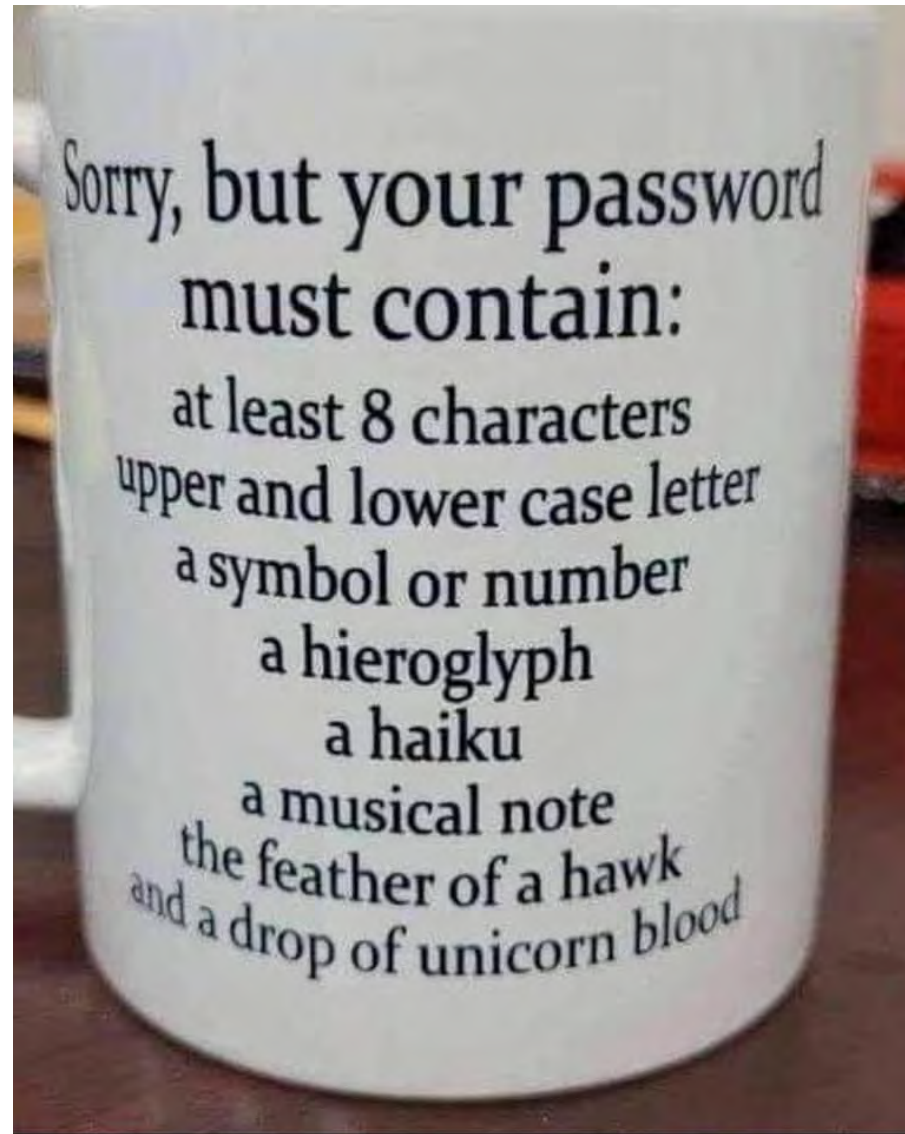
62%

of smartphone owners do NOT use a passcode to secure their phone

One Solution...



Or this...



Another Solution...



Password Entropy

Password entropy – measurement of a password’s unpredictability based on the character set used (which is expandable by using lowercase, uppercase, numbers, and symbols) and password length.

For example, at 1,000 guesses per second...

- **Tr0ub4dor&3** would take **3 days** to crack.
- **correcthorsebatterystaple** would take **550 years** to crack.
 - Don’t use this specific one because it’s already been widely publicized on the web. Come up with your own.

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Free Password Checking Tool



<https://www.security.org/how-secure-is-my-password/>

Solution: A Password Manager!



Search **password manager apps comparison** on pcmag.com, us.cybernews.com, tomsguide.com, wired.com, nytimes.com/wirecutter, or other reputable tech websites.

Password Don'ts and Do's

DON'T:

- Use the same password twice. (And no, “poodle 3” and “poodle4” don't count as different passwords.)
- Use personal information (name, birth date), keyboard patterns (qwerty), sequential numbers (1234), or repeating characters (aaaazzz).
- Make your password all numbers, uppercase letters, or lowercase letters.
- Tell your password to anyone, write your password down, or send your password by email.

DO:

- Use long word strings without spaces or randomly-generated gibberish passwords.
- Make your passwords at least 8 characters long.
- For increased security, mix upper- and lower-case letters, numbers, and symbols depending on the website's rules.
- Store passwords securely in a password manager app on your smartphone and/or desktop or laptop.
- Change passwords at least annually.
- Check if your password has been exposed in a leak at: *Have I Been Pwned?* (<https://haveibeenpwned.com/>).
- At the very minimum, use a:
 - **Basic password** for websites that don't store or require any of your personal information,
 - **Secure password** for retailer websites where you enter your credit card information, and a
 - **Very secure password** for financial, medical and other websites containing your most sensitive information.

A good password written down and stored in a secure location is much better than a bad password memorized!

MAKING MOBILE MORE SECURE



1

Keep your devices updated



2

Use biometric passwords

3

Disable Bluetooth
whenever you're not using it



4

Only go on public wi-fi with
an active VPN connection





1. Freeze (not lock) your credit for free with all four credit reporting agencies to prevent anyone from pulling your records except you and those financial institutions where you already do business:

Equifax

<https://www.equifaxsecurity2017.com/>

Experian

<https://www.experian.com/freeze/center.html>

TransUnion

<https://www.transunion.com/credit-freeze/place-credit-freeze>

2. To allow future lenders to pull your records, you'll need a PIN that each of the above credit agencies will give you when you freeze your account (keep it somewhere safe!) so you can unfreeze your records either for a few days or permanently.
3. Once your credit has been checked by the lender you've authorized, you should re-freeze the records.



Always use credit cards for purchases and debit cards ONLY for bank ATM cash withdrawals!

- Debit Card Downsides:
 - Consumer protections stronger for credit cards (e.g. issuers' zero-liability policies) than debit cards (no such policies).
 - If a debit card is compromised, your entire checking account gets drained and all your outstanding checks will bounce, and banks require a lot of red tape and take a long time to reimburse you. When fraud happens on a credit card, you just contact the issuer and they'll delete the offending transaction or issue you a new card, and you're done.
 - Using a debit card for purchases doesn't help your credit score at all.
 - If there's a cashier error on a debit card, you'll wait weeks while the bank investigates and then they may or may not reimburse you.
- Card skimming, in which an illegal reader is attached to a payment terminal, is a pervasive financial scam on ATMs.
- Avoid street corner or bodega ATMs – much more prone to being compromised with skimmers and other devices.
- Set up fraud alerts for both your credit and debit cards.
- To avoid finance charges, choose a credit card and opt in to your bank's automated payment option to pay the card's statement value each month automatically – you'll avoid finance charges while getting all of the card's miles and points.

Annual Credit Report.com

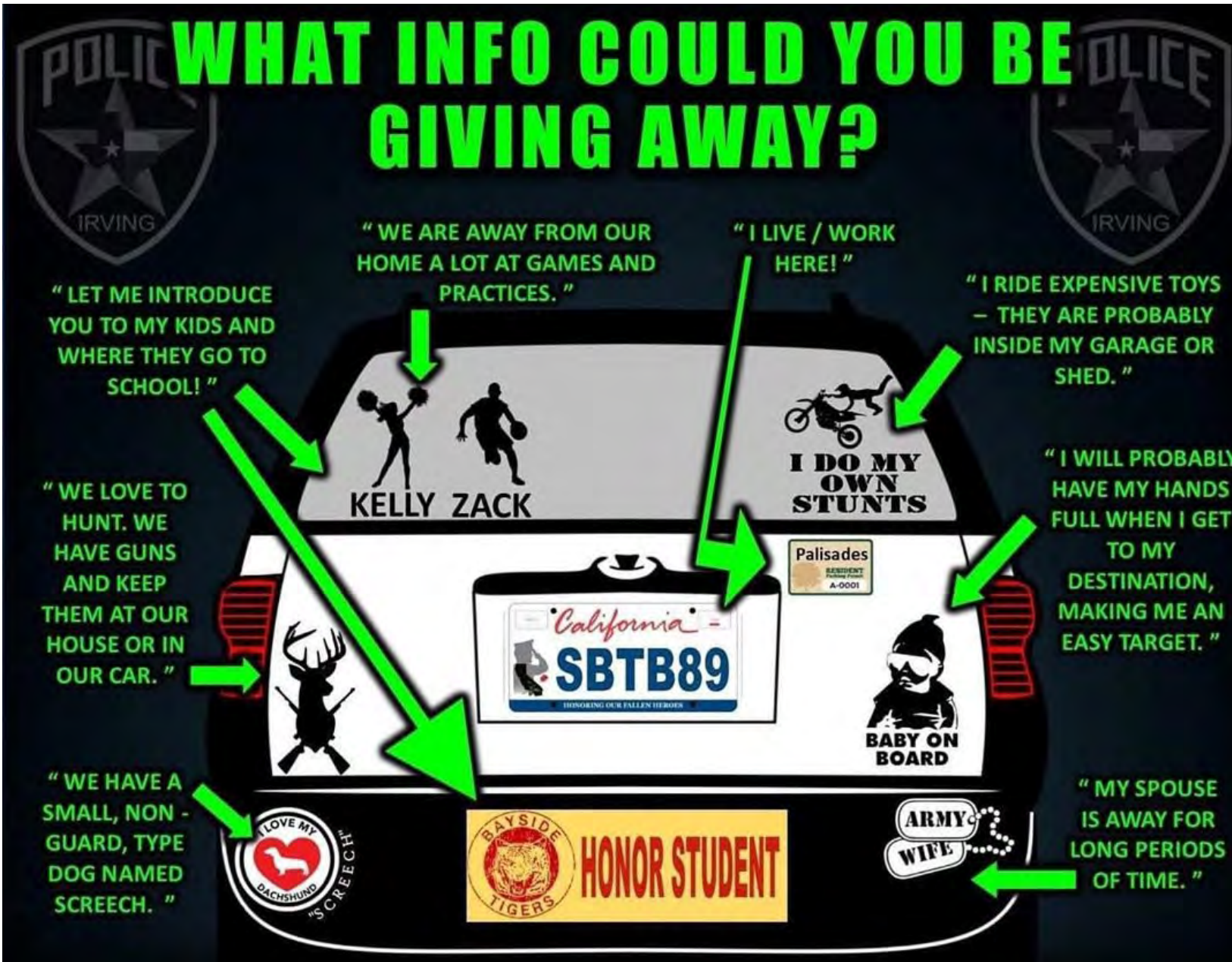
The only source for your free credit reports. Authorized by Federal law.

- Your credit reports matter.
 - Credit reports may affect your mortgage rates, credit card approvals, apartment requests, or even your job application.
 - Reviewing credit reports helps you catch signs of identity theft early.
- Federal law allows you to get a free copy of your credit report every 12 months from each credit reporting company.
- TIP: Pull a different one every four months so you cover all three over the course of a full year.
- Ensure that the information on all of your credit reports is correct and up to date.

EQUIFAX


 experian.

TransUnion 



Source: California Highway Patrol

CYBER SAFETY CHECKLIST



Back up online and offline files regularly and securely




Manage social media profiles




Strengthen your home network



Check privacy and security settings



Use strong passwords



Avoid opening and delete suspicious emails or attachments



Keep your software updated



INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

Ten Takeaways

- 1. Get cyber (breach) insurance:**
 - a. Not expensive.
 - b. Available from nearly all insurance companies.
 - c. Should cover as many of the cost elements as possible.
 - d. Some credit card processors claim to provide it...but review the coverage details!
- 2. Use layered security:** tokenization, encryption, EMV, multi-factor authentication, smart passwords, PCI.
- 3. Upgrade your passwords** and store them in an encrypted password manager app.
- 4. Segment your network** to restrict cross-contamination between your guest and administrative networks.
- 5. Secure remote access** with multiple layers of authenticating security.
- 6. Use the latest versions** of firewalls, antivirus software, programs, and operating systems.
- 7. Monitor your operating systems.**
- 8. Get lower Lodging Industry Interchange rates:**
 - a. Make sure your processor uses the Lodging Industry SIC (Standard Industry Classification) code 7011 for your account.
 - b. Use a processor that offers lodging Interchange rates and connects to your PMS via a lodging-certified gateway.
- 9. Freeze your credit...NOW!**
- 10. Use a Trusted Advisor:** No one can be an expert at everything, so use a Trusted Advisor like an accredited Certified Payments Professional with decades of hands-on experience as both a hospitality and payments professional to guide and advise you, help reduce risk, reduce your costs, and protect your business!

“...the beginning of a beautiful friendship.”



Thank You!

A copy of this presentation will be sent to you, along with additional data security guidance from the FBI and U.S. Secret Service, upon request.



Casablanca Ventures
Payments Intelligence

Powered
By



**MERCANTILE
PROCESSING INC.**

Wynn J. Salisch

CHS, ETA CPP

203-253-7259

wynn@casablanca-ventures.com