DOWNLOAD PDF IDENTITY THEFT 32

Chapter 1 : 4 Ways to Prevent Identity Theft - wikiHow

Identity theft is one of the most common outcomes from data breaches. % of breach victims in later experienced identity fraud, compared to just % of individuals not notified of a data breach in , according to Javelin.

Our electronic and physical identities are becoming increasingly intertwined. We lack adequate control over the data that is shared on our behalf in order to access services. The most obvious example of these trends United States is the electronic storage of large numbers of Social Security numbers and banking access codes that attract criminal attacks from any country with a computer science school. For any service that is regulated by the government, like healthcare, banking, and enterprise payroll systems, the SSN is the unique key that the service provider uses to identify each customer and employee. The end user is given no authority on how the SSN is protected and shared. Indeed, data loss happens all the time: We rarely hear about it. The opportunity for the IT industry is to ensure that loss and theft of electronic storage media, such as smart phones and laptops, does not imply data compromise. We can do this by ensuring that the data are always encrypted and that decryption always require strong authentication. The Importance of Disclosure Government regulation plays an important role in consumer disclosure. When Social Security numbers or credit card numbers are exposed, the citizen has a right to be notified. But government regulation moves too slowly to stay current with the latest threats. For example, regulation tends to focus on data encryption requirements without wading into the complex interaction between authentication, authorization, and access to electronic data storage. This approach leads to "check box security" which is easy for compliance checking, but ineffective at improving the real security of users on the internet. Humans are Bad at Passwords What is needed is a user identifier and credential that is of no value to an attacker. With current systems, users share sensitive personal information and passwords across a broad swath of online services. This is done for two reasons: Second, regulated markets, lacking competitive pressure, are only accountable for user privacy to the extent that the government says they must be. Nevertheless, there are two positive trends. First, while human brains are bad at creating computer passwords, computers excel at it. And a critical mass of consumers now carries a computer in their pocket everywhere they go. Second, while online privacy controls continue to lag, there is a shared desire among firms to avoid fines, lawsuits, and bad PR. In other words; these firms have an interest in protecting privacy so long as the cost in lost sales does not overwhelm their profits. What are Derived Credentials? Derived credentials are a solution proposed by the National Institute of Standards and Technology for use in government agencies. The smart chip on the CAC stores a strong cryptographic credential. To be useful, the card just needs a nice user interface, an Internet connection, and a widely supported app model. All of those needs are met by the great user experience available with any modern smart phone. As shipped the smart phone app model does not have the capability of storing secrets securely, nor does it easily allow the CAC to be read by the smart phone. Yet the hardware that powers the smart phone does have the capability to store secrets securely and act in every way just like the CAC. The solution is to use the primary credential protected on the CAC as a means to bootstrap a secondary credential derived from that onto the smart phone. New hires and recruits are issued a CAC only after nationality and tax identity have been verified. That has been a common pattern for employer and bank issued identities for many years. Birth certificates and national identities are verified, usually in person, and then a credential on a CAC is issued to signify employment or some other organization-specific identity. In fact, employer and bank credentials frequently come in two parts, a physical identity ATM card plus an online logon account. Find the Weakest Link The pattern, or chain, of identity credentials is therefore typically: But now we need to address the long certificate chain form the government to the employer to the smart phone that is owned by the user. That weak link is where innovative solution must be found so that the use of the derived credential can be trusted to maintain the security of the credential by the employer, and, in some cases, by the government itself. Phone Based Authentication Generally, since typing a complex password into a mobile phone keyboard is painful, phone-based authentication systems achieve an acceptable balance of security and usability by storing a portion of the user credential in a browser cookie or password vault. Then, each time the cell number must be verified; an

automated system calls the user and prompts for a short PIN. It is more convenient to type in the PIN than to reenter the complex password, and the average user is vastly more vigilant about not losing their phone than about picking and remembering strong passwords. Phone-based authentication systems are good from the perspective of helping to mitigate the threat of online password guessing attacks, but there are vulnerabilities in the registration process. As stated previously, phone-based authentication is a bit of a special case, since even though the original account password is only rarely manually typed by the user, the password is still being presented automatically on behalf of the user by the web browser or similar client software. The phone number is therefore additive. In order to get your employer badge in the first place, you only had to present your government ID once. In the case of phone-based authentication for online accounts, the net result is better protection against password guessing and account hijacking. However, in the case of other identity theft scenarios, a forged government ID, or even just a convincing liar, is enough to obtain a derived or replacement credential that is very difficult for its rightful owner to discover and undo. Proper care must be taken to assess the security of the issuance procedure for the derived credential. The integrity of the identity conferred by a derived credential is based on assumptions made about two separate vetting processes. If the original identity is bogus due to weak vetting, then a successfully obtained derived identity has essentially laundered it. Future newsletters will focus on these challenges. Most likely, the user account was originally created after the new employee signed some papers and submitted a W9. In many industries, no government ID is required for employment; you just have to show up and do the work. Thereafter, the user might reuse the same password in five different online accounts, tell it to his girlfriend, and save it in a file named passwords. User identity vetting procedures present the usual challenges and trade-offs one expects when the real world intersects the electronic one. On one hand, in-person verification is important when deriving a credential from a government photo ID. On the other hand, such manual steps are vulnerable to social engineering. Likewise, electronic identities can be attacked anonymously by hackers on the other side of the world. But, unlike a desk clerk, strong digital credentials cannot be tricked or bribed. This again is the type of conundrum that entities such as the DOD face in attempting to derive a relatively more convenient mobile credential from a relatively more secure physical one. In fact, these days, smart phones are capable of hosting strong credentials including cryptographic keys and biometrics. Physical to Digital Technical solutions do exist for crossing the chasm from a smart card badge to a new digital credential on a smart phone. For example, since phone compatible smart card readers are not widely used, one approach is to introduce an intermediate hop. That is, use the badge to derive a credential on a PC, where USB smart card readers are relatively inexpensive and convenient to use. Then use the PC credential, together with some second factor of authentication, to derive the digital credential on the phone. This is another example of a chain of credentials that can be linked to enable the user to strongly authenticate from the personal device that is carried everywhere. We do this using the Trusted Platform Module TPM security chip or secure firmware that is installed on every modern computer. Please explore some of the related information below from JW Secure and other sources. Read More about Protecting Identity and Credentials.

Chapter 2 : () / - Identity Theft Reports.2 Comment(s)

Identity theft poses risks to consumers and the safe and sound operation of financial institutions. The FDIC has well-defined expectations of how institutions should detect and prevent ID theft and mitigate its effects.

Does not include premiums from companies that cannot report premiums for identity theft coverage provided as part of package policies. View Archived Tables Cybercrime Interest in cyber insurance and cyberrisk continues to grow as a result of high-profile data breaches and awareness of the almost endless range of exposure businesses face. In through November, million records were exposed in June from Exactis, a marketing firm; million records exposed at Under Armor; 92 million at MyHeritage, a genealogy firm; and 87 million records at Facebook. In , the largest U. It was among the worst breaches on record because of the amount of sensitive information stolen. The number of records exposed totaled The business category continues to be the most affected sector, with breaches, or 46 percent of all breaches detected. The business sector breaches affected The IRTC noted that in September alone, hacking was the primary type of breach incident, accounting for 46 percent of all breaches in September. Unauthorized access was identified as the second most common type of attack, accounting for 30 percent of September breaches. According to the IRTC phishing was the most common form of hacking for September, representing 50 percent of the total breaches caused by hacking. The costs of cybercrime are growing. Researchers polled organizations to determine what costs they incurred after a data breach, including systems to help victims with losses and expenses, notification costs and lost business costs such as those associated with business disruption, revenue losses and reputation costs. The study also found that the average cost for each lost record rose 4. Cyber insurance evolved as a product in the United States in the mid- to lates as insurers have had to expand coverage for a risk that is rapidly shifting in scope and nature. Small business and cyber insurance, insurers foresee substantial growth coming from the small business segment, as these companies become aware of the possibilities of liability, especially due to a breach and the resulting response costs arising out of the possession of private data. According to the Insurance Information Institute I. Only about one-third of firms surveyed had cyber insurance, nearly 60 percent of respondents said their company is very concerned about cyber incidentsâ€”and 70 percent think that the risk of being victimized by a cyberattack is growing at an alarming rate. Insurers can reach these potential small business customers through education, training and risk assessment services regarding cybersecurity. Identity Theft Resource Center. In the IC3 received and processed , complaints. One out of five victims People between the ages of 30 and 39 ranked second at The most common complaints received in involved nonpayment or nondelivery of goods or services, which affected about 84, victims. There were about 31, victims affected by personal data breaches. Internet Crime Complaint Center.

Chapter 3 : Identity Theft Victim Spends 32 Days in Jail

Your identity is one of the most valuable things you own. Learn how to keep it safe and secure with our Identity Theft Resources. Recommended Actions.

B tangible or intangible personal property including anything severed from land; or C a document, including money, that represents or embodies anything of value. A labor and professional service; B telecommunication, public utility, and transportation service; C lodging, restaurant service, and entertainment; and D the supply of a motor vehicle or other property for use. Acts , 63rd Leg. Amended by Acts , 73rd Leg. Acts , 84th Leg. When amounts are obtained in violation of this chapter pursuant to one scheme or continuing course of conduct, whether from the same or several sources, the conduct may be considered as one offense and the amounts aggregated in determining the grade of offense. A to alter, make, complete, execute, or authenticate any writing so that it purports: A printing or any other method of recording information; B money, coins, tokens, stamps, seals, credit cards, badges, and trademarks; and C symbols of value, right, privilege, or identification. Amended by Acts , 72nd Leg. May 21, ; Acts , 78th Leg. Acts , 81st Leg. Acts , 85th Leg. A registered with the secretary of state; B registered on the principal register of the United States Patent and Trademark Office; C registered under the laws of another state; or D protected by Section Section et seq. Added by Acts , 75th Leg. Acts , 82nd Leg. Added by Acts , 76th Leg. The term includes the number or description of the device if the device itself is not produced at the time of ordering or obtaining the property or service. The term includes the number or description of the device if the device itself is not produced at the time of ordering or obtaining the benefit. For purposes of this subdivision, a card is incomplete if part of the matter that an issuer requires to appear on the card before it can be used, other than the signature of the cardholder, has not yet been stamped, embossed, imprinted, or written on it; 10 being authorized by an issuer to furnish goods or services on presentation of a credit card or debit card, he, with intent to defraud the issuer or the cardholder, furnishes goods or services on presentation of a credit card or debit card obtained or retained in violation of this section or a credit card or debit card that is forged, expired, or revoked; or 11 being authorized by an issuer to furnish goods or services on presentation of a credit card or debit card, he, with intent to defraud the issuer or a cardholder, fails to furnish goods or services that he represents in writing to the issuer that he has furnished. For purposes of this section, notice may be either notice given orally in person or by telephone, or in writing by mail or by telegram. If written notice was sent by registered or certified mail with return receipt requested, or by telegram with report of delivery requested, addressed to the cardholder at the last address shown by the records of the issuer, it is presumed that the notice was received by the cardholder no later than five days after sent. Acts , 79th Leg. Acts , 80th Leg. A person is presumed to have intended to appropriate proceeds if the person does not deliver the proceeds to the secured party or account to the secured party for the proceeds before the 11th day after the day that the secured party makes a lawful demand for the proceeds or account. An offense under this subsection is: Amended by Acts , 66th Leg. Added by Acts , 71st Leg. Renumbered from Penal Code, Sec. It includes the number or description on the device if the device itself is not produced at the time of ordering or obtaining the property or service. Added by Acts , 72nd Leg. Renumbered from Penal Code Sec. Amended by Acts , 75th Leg. A the check or order; B the records of the bank or other drawee; or C the records of the person to whom the check or order has been issued or passed; and 3 contains the following statement: If you fail to make payment in full within 10 days after the date of receipt of this notice, the failure to pay creates a presumption for committing an offense, and this matter may be referred for criminal prosecution. In other cases restitution may be, with the approval of the court in which the offense is filed: If the check or similar sight order that was issued or passed was for a child support payment the obligation for which is established under a court order, the offense is a Class B misdemeanor. Amended by Acts , 68th Leg. June 18, ; Acts , 71st Leg. June 16, ; Acts , 73rd Leg. Acts , 83rd Leg. A sales contest is not deceptive if the total value of prizes to each retail outlet is in a uniform ratio to the number of game pieces distributed to that outlet. A not to sell it as advertised, or B not to supply reasonably expectable public demand, unless the advertising adequately discloses a time or quantity limit; 9 representing

the price of property or service falsely or in a way tending to mislead; 10 making a materially false or misleading statement of fact concerning the reason for, existence of, or amount of a price or price reduction; 11 conducting a deceptive sales contest; or 12 making a materially false or misleading statement: A in an advertisement for the purchase or sale of property or service; or B otherwise in connection with the purchase or sale of property or service. Amended by Acts , 64th Leg. A an agent or employee; B a trustee, guardian, custodian, administrator, executor, conservator, receiver, or similar fiduciary; C a lawyer, physician, accountant, appraiser, or other professional advisor; or D an officer, director, partner, manager, or other participant in the direction of the affairs of a corporation or association. This subsection does not affect the application of Section A a participant in the contest to induce him not to use his best efforts; or B an official or other person associated with the contest; or 2 he tampers with a person, animal, or thing in a manner contrary to the rules of the contest. A a trustee, guardian, administrator, executor, conservator, and receiver; B an attorney in fact or agent appointed under a durable power of attorney as provided by Subtitle P, Title 2, Estates Code; C any other person acting in a fiduciary capacity, but not a commercial bailee unless the commercial bailee is a party in a motor fuel sales agreement with a distributor or supplier, as those terms are defined by Section A an agreement under which the fiduciary holds the property; or B a law prescribing the custody or disposition of the property. A a purported court that is not expressly created or established under the constitution or the laws of this state or of the United States; B a purported judicial entity that is not expressly created or established under the constitution or laws of this state or of the United States; or C a purported judicial officer of a purported court or purported judicial entity described by Paragraph A or B. A submit to the putative authority of the document; or B take any action or refrain from taking any action in response to the document, in compliance with the document, or on the basis of the document. A the obligor or debtor; or B any person who owns any interest in the real or personal property described in the document or instrument that is the basis for the lien or claim. A obtain money, goods, services, or other thing of value; or B initiate a transfer of funds other than a transfer originated solely by paper instrument. Amended by Acts , 78th Leg. A is a fraudulent or substandard degree; B is fictitious or has otherwise not been granted to the person; or C has been revoked; and 2 uses or claims to hold that degree: A in a written or oral advertisement or other promotion of a business; or B with the intent to: Added by Acts , 79th Leg. If a criminal episode is prosecuted under both this section and another section of this code and sentences are assessed for convictions under both sections, the sentences shall run concurrently. Added by Acts , 82nd Leg. A is fraudulent; B is fictitious or has otherwise not been granted or assigned to the person; or C has been revoked; and 2 uses or claims to hold that military record:

Chapter 4 : Identity Theft | Consumer Information

A Georgia man says he spent 32 days in a Missouri jail for crimes a former roommate committed. It was a case of identity theft, James Molden told a local news reporter, saying the ex-roommate used.

Sources such as the non-profit Identity Theft Resource Center [11] sub-divide identity theft into five categories: Identity theft may be used to facilitate or fund other crimes including illegal immigration , terrorism , phishing and espionage. There are cases of identity cloning to attack payment systems , including online credit card processing and medical insurance. Examples are illegal immigrants hiding their illegal status, people hiding from creditors or other individuals, and those who simply want to become " anonymous " for personal reasons. Posers mostly create believable stories involving friends of the real person they are imitating. Unlike identity theft used to obtain credit which usually comes to light when the debts mount, concealment may continue indefinitely without being detected, particularly if the identity thief is able to obtain false credentials in order to pass various authentication tests in everyday life. Criminal identity theft[edit] When a criminal fraudulently identifies themselves to police as another individual at the point of arrest, it is sometimes referred to as "Criminal Identity Theft. Victims might only learn of such incidents by chance, for example by receiving court summons, discovering their drivers licenses are suspended when stopped for minor traffic violations, or through background checks performed for employment purposes. It can be difficult for the victim of a criminal identity theft to clear their record. The victim might need to locate the original arresting officers and prove their own identity by some reliable means such as fingerprinting or DNA testing, and may need to go to a court hearing to be cleared of the charges. Obtaining an expungement of court records may also be required. One problem that victims of criminal identity theft may encounter is that various data aggregators might still have the incorrect criminal records in their databases even after court and police records are corrected. Thus it is possible that a future background check will return the incorrect criminal records. Synthetic identity theft[edit] A variation of identity theft which has recently become more common is synthetic identity theft, in which identities are completely or partially fabricated. Synthetic identity theft primarily harms the creditors who unwittingly grant the fraudsters credit. Individual victims can be affected if their names become confused with the synthetic identities, or if negative information in their subfiles impacts their credit ratings. In the report, she defined the crime for the first time and made the plight of victims public. Insurance theft is also very common, if a thief has your insurance information and or your insurance card, they can seek medical attention posing as yourself. After the publication of the report, which contained a recommendation that consumers receive notifications of medical data breach incidents, California passed a law requiring this, and then finally HIPAA was expanded to also require medical breach notification when breaches affect or more people. The impostor can be a family member, a friend, or even a stranger who targets children. The Social Security numbers of children are valued because they do not have any information associated with them. This fraud can go undetected for years, as most children do not discover the problem until years later. Child identity theft is fairly common, and studies have shown that the problem is growing. The largest study on child identity theft, as reported by Richard Power of the Carnegie Mellon Cylab with data supplied by AllClear ID , found that of 40, children, This includes getting credits, loans, goods and services, claiming to be someone else. Rummaging through rubbish for personal information dumpster diving Retrieving personal data from redundant IT equipment and storage media including PCs, servers, PDAs, mobile phones, USB memory sticks and hard drives that have been disposed of carelessly at public dump sites, given away or sold on without having been properly sanitized Using public records about individual citizens, published in official registers such as electoral rolls [21] Stealing bank or credit cards, identification cards, passports, authentication tokens This is particularly done in crowded places because it is relatively easy to observe someone as they fill out forms, enter PIN numbers on ATMs or even type passwords on smartphones. Befriending strangers on social networks and taking advantage of their trust until private information is given. Indicators that you may be a victim of identity theft[edit] The majority of identity theft victims do not realize that they are a victim until it has negatively impacted their lives. Many people do not

find out that their identities have been stolen until they are contacted by financial institutions or discover suspicious activities on their bank accounts. The following are ten indicators that someone else might be using your identity. Credit or debit card charges for goods or services you are not aware of, including unauthorized withdrawals from your account [24] Receiving calls from credit or debit card fraud control department warning of possible suspicious activity on your credit card account [25] Receiving credit cards that you did not apply for [25] Receiving information that a credit scoring investigation was done. They are often done when a loan or phone subscription was applied for. Checks bouncing for lack of enough money in your account to cover the amount. This might be as a result of unauthorized withdrawals from your account [25] Identity theft criminals may commit crimes with your personal information. You may not realize this until you see the police on your door arresting you for crimes that you did not commit [25] Sudden changes to your credit score may indicate that someone else is using your credit cards [26] Bills for services like gas, water, electricity not arriving in time. This can be an indication that your mail was stolen or redirected [26] Being not approved for loans because your credit report indicates that you are not credit worthy [26] Receiving notification from your post office informing you that your mails are being forwarded to another unknown address [27] Your yearly tax returns indicating that you have earned more than you have actually earned. This might indicate that someone is using your national identification number e. SSN to report their earnings to the tax authorities [27] Individual identity protection[edit] The acquisition of personal identifiers is made possible through serious breaches of privacy. For consumers, this is usually a result of them naively providing their personal information or login credentials to the identity thieves as a result of being duped but identity-related documents such as credit cards, bank statements, utility bills, checkbooks etc. Guardianship of personal identifiers by consumers is the most common intervention strategy recommended by the US Federal Trade Commission , Canadian Phone Busters and most sites that address identity theft. Such organizations offer recommendations on how individuals can prevent their information falling into the wrong hands. Identity theft can be partially mitigated by not identifying oneself unnecessarily a form of information security control known as risk avoidance. This implies that organizations, IT systems and procedures should not demand excessive amounts of personal information or credentials for identification and authentication. Committing personal identifiers to memory is a sound practice that can reduce the risks of a would-be identity thief from obtaining these records. To help in remembering numbers such as social security numbers and credit card numbers, it is helpful to consider using mnemonic techniques or memory aids such as the mnemonic Major System. These services purport to help protect the individual from identity theft or help detect that identity theft has occurred in exchange for a monthly or annual membership fee or premium. In a study, it was reported that 60 million Americans identities were wrongfully acquired [31]. The number of people this has happened to has revealed there is a wrongful epidemic in our country with how easily our identity is not truly protected among every account that we have, even our birth certificates. With this continuing problem, some new bills have been implemented to provide more security for people such as electronic signatures and social security verification for more authentication to further prove it is the true person [31]. There are several types of identity theft that are used to gather information, one of the most common types occurs when consumers make online purchases. A study was conducted with people to determine the relationship between the constructs of fear of financial losses and reputational damages [32]. The conclusions of this study revealed that identity theft was a positive correlation with reputable damages. The relationship between perceived risk and online purchase intention were negative. The significance of this findings reveal that online companies are more aware of the potential harm that can be done to their consumers, therefore they are searching for ways to reduce the perceived risk of consumers and not lose out on business. Although the idea of identity theft can be frightening to some, the aftermath of how people move forward is a pretty intense process. Some may face a year or consecutive years to prove to the legal system that they are the true person. Identity protection by organizations[edit] In their May testimony before the United States Senate, the Federal Trade Commission FTC discussed the sale of Social Security numbers and other personal identifiers by credit-raters and data miners. Credit reporting agencies gather and disclose personal and credit information to a wide business client base. Poor stewardship of personal data by organizations, resulting in unauthorized access to sensitive data,

can expose individuals to the risk of identity theft. The Privacy Rights Clearinghouse has documented over individual data breaches by US companies and government agencies since January , which together have involved over million total records containing sensitive personal information, many containing social security numbers. The use of strong encryption on these devices can reduce the chance of data being misused should a criminal obtain them. This potentially allows criminals access to personal information through credit rating and data mining services. The failure of corporate or government organizations to protect consumer privacy , client confidentiality and political privacy has been criticized for facilitating the acquisition of personal identifiers by criminals. Market[edit] There is an active market for buying and selling stolen personal information, which occurs mostly in darknet markets but also in other black markets. Noble told a forum in Abu Dhabi the previous month this was the case. The result is a major gap in our global security apparatus that is left vulnerable to exploitation by criminals and terrorists," Noble is quoted as saying. Other states and territories are in states of development in respect of regulatory frameworks relating to identity theft such as Western Australia in respect of Criminal Code Amendment Identity Crime Bill The total cost reported by the Attorney General Department was:

Chapter 5 : PENAL CODE CHAPTER FRAUD

Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss.

Chapter 6 : Identity Theft Protection | theinnatdunvilla.com

Identity Theft. Identity (ID) theft is a crime where a thief steals your personal information, such as your full name or Social Security number, to commit fraud. The.

Chapter 7 : Identity Thief Full () - Watch32

The scope of identity theft. According to Identity Fraud: Fraud Enters a New Era of Complexity from Javelin Strategy & Research, in , there were million victims of identity fraud, a record high that followed a previous record the year before.

Chapter 8 : FTC Releases Annual Summary of Consumer Complaints | Federal Trade Commission

(E) social security number or other government-issued identification number. (2) "Telecommunication access device" means a card, plate, code, account number, personal identification number, electronic serial number, mobile identification number, or other telecommunications service, equipment.

Chapter 9 : Facts + Statistics: Identity theft and cybercrime | III

PENAL CODE. TITLE 7. OFFENSES AGAINST PROPERTY. CHAPTER FRAUD. SUBCHAPTER A. GENERAL PROVISIONS. Sec. DEFINITIONS. In this chapter: (1) "Financial institution" means a bank, trust company, insurance company, credit union, building and loan association, savings and loan association, investment trust, investment company, or any other organization held out to the public as a place for.