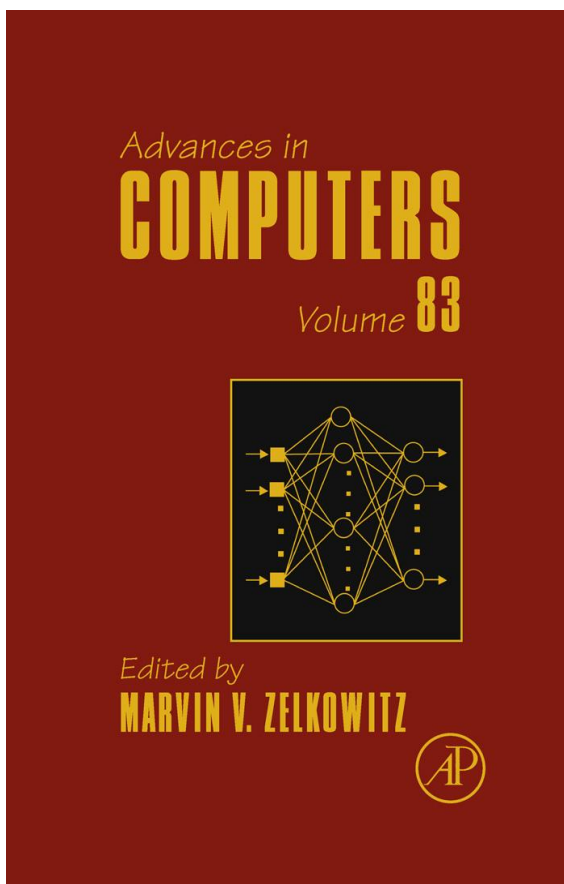


This chapter was originally published in the book *Advances in Computers*, Vol. 83, published by Elsevier, and the attached copy is provided by Elsevier for the author's benefit and for the benefit of the author's institution, for non-commercial research and educational use including without limitation use in instruction at your institution, sending it to specific colleagues who know you, and providing a copy to your institution's administrator.



All other uses, reproduction and distribution, including without limitation commercial reprints, selling or licensing copies or access, or posting on open internet sites, your personal or institution's website or repository, are prohibited. For exceptions, permission may be sought for such use through Elsevier's permissions site at:

<http://www.elsevier.com/locate/permissionusematerial>

From: Amit Grover, Hal Berghel and Dennis Cobb, The State of the Art in Identity Theft. In Marvin V. Zelkowitz, editor: *Advances in Computers*, Vol. 83, Burlington: Academic Press, 2011, pp. 1-50.

ISBN: 978-0-12-385510-7

© Copyright 2011 Elsevier Inc.  
Academic Press.

# The State of the Art in Identity Theft

AMIT GROVER

*Identity Theft and Financial Fraud Research and Operations Center, UNLV School of Informatics, University of Nevada Las Vegas, Las Vegas, Nevada, USA*

HAL BERGHEL

*Identity Theft and Financial Fraud Research and Operations Center, UNLV School of Informatics, University of Nevada Las Vegas, Las Vegas, Nevada, USA*

DENNIS COBB

*Identity Theft and Financial Fraud Research and Operations Center*

## Abstract

This chapter examines in detail the various aspects of identity theft—the nation's fastest-growing crime—and its impact in today's world. The introduction section defines several meanings of “identity theft” as it is commonly used, while [Section 2](#) explores the unique characteristics of identity theft as a crime. [Sections 3](#) covers detailed analyses of statistical data for identity theft and associated crimes. [Sections 4 through 9](#) discuss the core issues involved including the genesis of the problem, the misuse of Social Security Numbers, the ubiquitous use of fungible credentials, the role of phishing and strategies to minimize its effect, the problem of inadequate credential management procedures and its solution, and the impact of technological advances in the

unprecedented rise of identity theft incidents. [Section 10](#) discusses the strategy of prevention as well as cure in the context of identity theft.

1. Introduction . . . . .	2
2. What Sets Identity Theft Apart from Other Crimes . . . . .	3
3. Statistical Data for Identity Theft and Associated Crimes . . . . .	6
4. The Genesis of the Problem . . . . .	11
5. How SSN Became the <i>De Facto</i> Primary Key for Most Databases . . . . .	12
6. The Ubiquitous Use of Fungible Credentials . . . . .	13
7. Phishing . . . . .	14
7.1. Phenomenal Growth in the Number and Sophistication of Phishing Attacks . . . . .	14
7.2. The Importance of Secure Online Transactions . . . . .	15
8. Modus Operandi . . . . .	26
9. Inadequate Credential Management Procedures . . . . .	31
9.1. CardSleuth . . . . .	31
10. Strategies for Defeating Identity Thieves . . . . .	32
10.1. Precautions to Prevent ID Theft . . . . .	33
10.2. Remediation . . . . .	47
11. Conclusion . . . . .	47
References . . . . .	47

## 1. Introduction

Technically, the term “identity theft” refers to two distinct, but interrelated, crimes: the act of stealing another’s identity and the use of that stolen identity in committing a fraudulent act. In the first case, identity theft is similar in function to “pretexting”—or the attempt to take on the persona of another individual for social engineering purposes. In the second case, identity theft falls into the category of digital crime, along with copyright infringement, espionage, phishing, financial crimes, money laundering, and so forth. In many if not most cases, the first type of identity theft is used as a means to the commission of the second type of identity theft. In the fullest sense, identity theft is a strong candidate for the major crime of the new millennium. Identity theft usually begins with a fraudulent document such as that shown in [Fig. 1](#).



FIG. 1. Example of Identity Theft. Source: The Identity Theft and Financial Fraud Research and Operations Center. [www.itffroc.org](http://www.itffroc.org).

## 2. What Sets Identity Theft Apart from Other Crimes

As per the U.S. Internal Revenue Service, “Most scams impersonating the IRS are identity theft schemes” [1]. The inherent dangers associated with Identity Theft as a crime-facilitator ensure that its potential for causing disasters can hardly be over-emphasized. The calamitous effect of identity fraud is perhaps best illustrated by the

fact that the 9/11 hijackers successfully opened 35 U.S. bank accounts using fictitious Social Security numbers that the banks never bothered to countercheck. These accounts were used for international money—laundering and financing terrorist activities. As per a Department of Homeland Security report titled, “Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security” [2], “The 9/11 hijackers engaged in a travel operation that included fraudulently obtaining 17 driver’s licenses (one in Arizona, two in California, and 14—four of which were duplicates—in Florida) and 13 state-issued identifications (five from Florida, one from Maryland, and seven from Virginia). All seven in Virginia were obtained fraudulently, and three of the hijackers presented those same identification cards on the morning of 9/11 at Dulles International Airport ticket counters.”

Further, during a hearing on “Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves” as part of a testimony to the U.S. House of Representatives [3], Chris Jay Hoofnagle stated that “a terrorist suspect reportedly connected to the Al Qaeda network was recently charged with selling the SSNs of 21 people who were members of the Bally’s Health Club in Cambridge, Massachusetts. The SSNs were sold in order to create false passports and credit lines for bank accounts.”

The New York Times Square incident involving Faisal Shahzad in May 2010 which is the most recent terrorism attempt on U.S. soil was financed by international money laundering operations (known as “hawala”) originating in Pakistan and made possible in part by identity theft [4]. The use of identity theft in facilitating cross-border crimes ranging from international espionage to illegal trafficking of weapons as well as narcotics is also well documented. The U.S. Treasury’s Terrorist Financing Tracking Program (TFTP) focuses among other things to investigate identity theft involved in funding international terrorist activities [5].

Identity theft is unique in its spread across all demographics and apart from ordinary citizens, victims of identity theft or people whose personal information has been compromised in some way include high-profile individuals such as Warren Buffett, Bill Gates, Tom Cruise, Steven Spielberg, Oprah Winfrey, Danny DeVito, David Letterman, Jay Leno, Federal Reserve Chairman Ben Bernanke, Tiger Woods, Martha Stewart, Ted Turner, George Lucas, Ross Perot, Senator Norm Coleman of Minnesota, Will Smith, Steven Segal, Mel Gibson, Michael Ovitz, Sydney Pollack, Leonard Nimoy, Lawrence Tisch, Arsenio Hall, Lew Wasserman, Alan Ladd, former Vice President Al Gore’s daughter, CEOs, senior corporate executives, high-ranking military officials, and top politicians along with thousands of Clinton administration staff members and White House visitors [6–8].

Identity theft is probably one of the only crimes that can ruin within days the sound financial health, good credit history as well as an impeccable reputation that a

victim might have painstaking built over a lifetime. There have been cases where innocent identity theft victims have been arrested for crimes committed by others. Many identity theft victims have reported that apart from the financial loss, they had to endure a lot of stress and emotional challenges in their battle to get back their life. An identity theft often results in having a debilitating effect on the victim's potential for getting a new job or buying a new house.

The Social Security Administration has identified identity theft as one of the fastest-growing crimes in the nation [9] and the 2010 Identity Fraud Survey Report by Javelin Strategy & Research [10] states that while there were approximately 10 million victims of identity fraud in 2008, the number rose to *more than 11 million victims for 2009* with the associated *annual costs as high as \$54 billion*. As per the Federal Trade Commission's 2006 Identity Theft Survey Report [11], the number of identity theft victims in 2005 was around 8.3 million. This steady increase in the number of victims of identity fraud over the years is charted in Fig. 2.

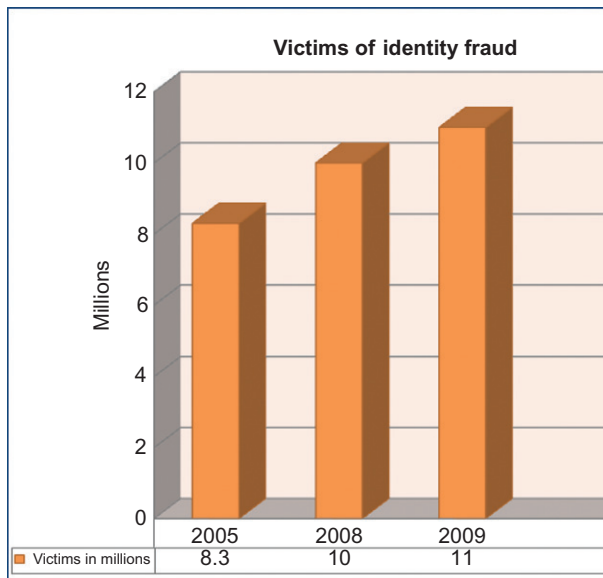


FIG. 2. Steady increase in the number of victims of identity fraud over the years.

### 3. Statistical Data for Identity Theft and Associated Crimes

Identity Theft and Financial Fraud Research and Operations Center (ITFF/ROC, [www.itffroc.org](http://www.itffroc.org)) is a collaborative effort between the University of Nevada Las Vegas and law enforcement agencies such as the Las Vegas Metropolitan Police Department dedicated to effectively fight the problem of identity theft and associated crimes through a synergy between high-tech research and current law enforcement procedures. Established in 2004, the ITTFROC has worked with the Department of Justice on a number of projects using cutting-edge technology to fight digital crime.

For increasing social awareness, ITTFROC also highlights the most important data breaches relevant to identity theft and financial fraud on a weekly basis and archives the data for future reference in its “Reading Room” [section \[12\]](#). The detailed statistics presented in this section are derived from 61 specific incidents representing all major data breaches from January 24, 2009 till June 24, 2010. It is important to note that the data represent the total number of compromised records and not the total number of verified identity theft victims. The data collection, analysis, and interpretation highlighted the following salient points:

- The combined data suggest that during the period under consideration, *more than 260 million (260,247,580) records* were compromised with almost 50% of the records attributed to a single incident—the largest U.S. Identity Theft case involving *130 million stolen credit and debit card numbers* from credit-card processor Heartland Payment Systems and retail chains including 7-Eleven Inc. and Hannaford Brothers Co.
- [Figure 3](#) depicts a chart (derived from data from [Table I](#)) indicating the number of compromised records based on the type of incident responsible for information exposure and shows that apart from the Heartland Payment Systems incident, the maximum number of compromised records can be attributed to *failure in sanitizing hard disk drives before disposal*.
- [Figure 4](#) represents a graphical distribution of the number of compromised records per incident which was spread over a very wide range from the humongous 130 million to the paltry 50.
- [Figures 5 and 6](#) represent, respectively, a breakdown of the number of incidents and the number of compromised records based on the type of organization (derived from data from [Table II](#) and [Table III](#) respectively).

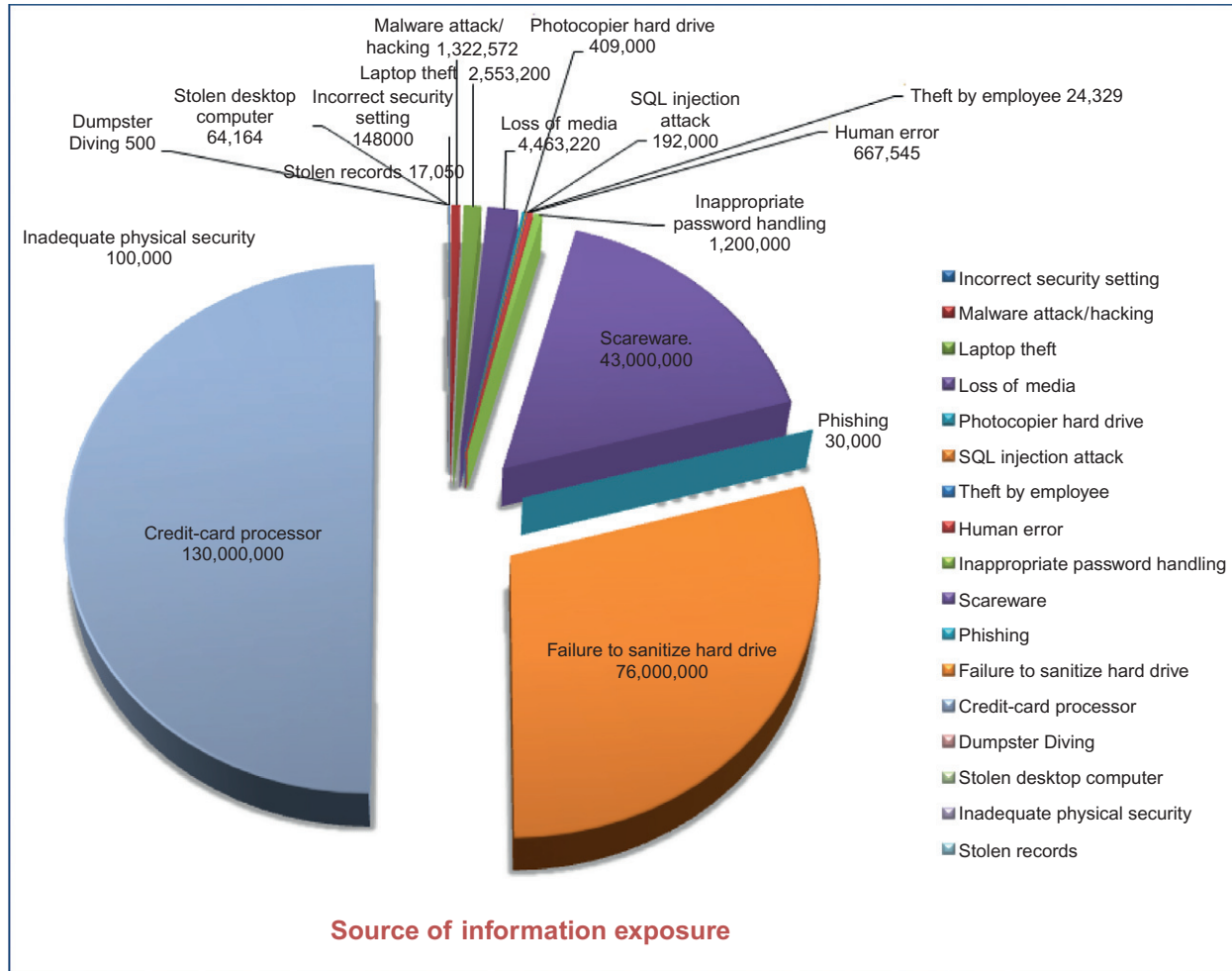


FIG. 3. Compromised records based on source of information exposure (data in Table I).



TABLE I  
COMPROMISED RECORDS BASED ON SOURCE OF INFORMATION EXPOSURE

Incorrect security setting	148,000
Malware attack/hacking	1,322,572
Laptop theft	2,553,200
Loss of media	4,463,220
Photocopier hard drive	409,000
SQL injection attack	192,000
Theft by employee	24,329
Human error	667,545
Inappropriate password handling	1,200,000
Scareware	43,000,000
Phishing	30,000
Failure to sanitize hard drive	76,000,000
Credit-card processor	130,000,000
Dumpster diving	500
Stolen desktop computer	64,164
Inadequate physical security	100,000
Stolen records	17,050

- While all individuals whose data have been compromised are at a high risk of becoming victims of identity theft, the actual number of victims would be substantially less.
- Since the data are derived from a large number of incidents spread over a 17-month period, it is very likely that data of some individuals have been compromised in more than one incident, thus reducing the actual number of distinct individuals affected.
- Even in a single incident such as the Heartland Payment Systems breach, the number of distinct people affected might be less than the number of records compromised as it is common for people to use a number of different credit/debit cards.
- There are instances when the identity theft victims do not file reports with law enforcement for various reasons, and hence the actual number of victims is more than what is reflected by the law enforcement records.

As per Privacy Rights Clearinghouse, a nonprofit consumer organization, the consolidated number of records breached based on 1728 data breaches made public since 2005 till September 20, 2010 is a staggering 510,547,119 [13].

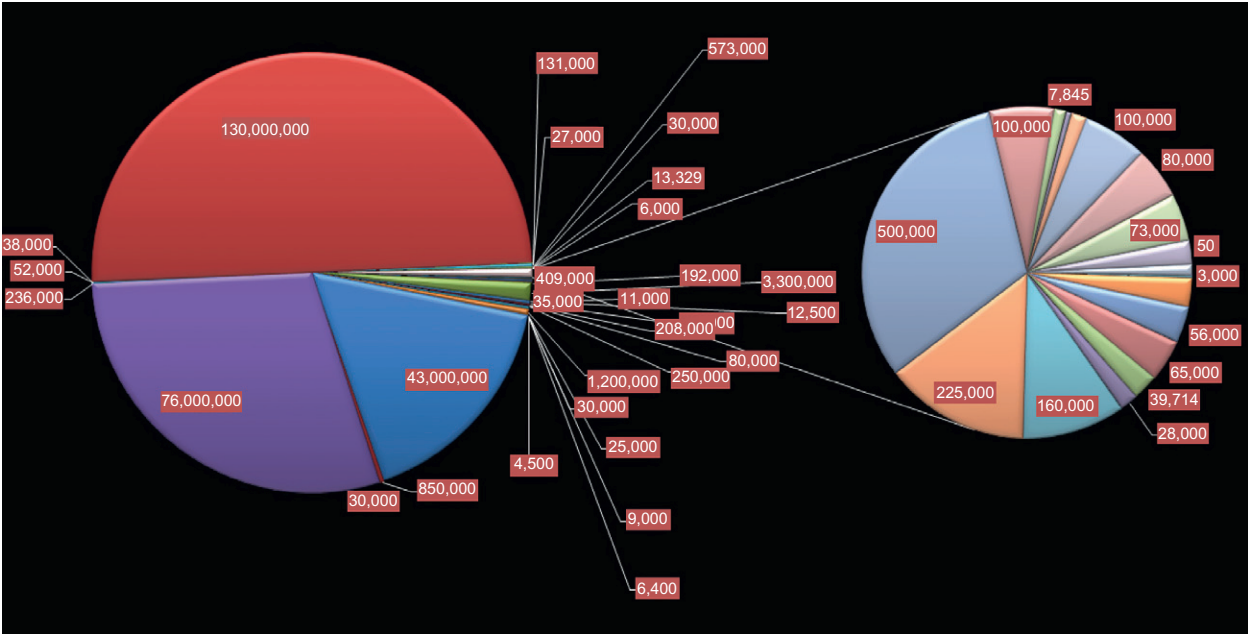


FIG. 4. Number of compromised records per incident.

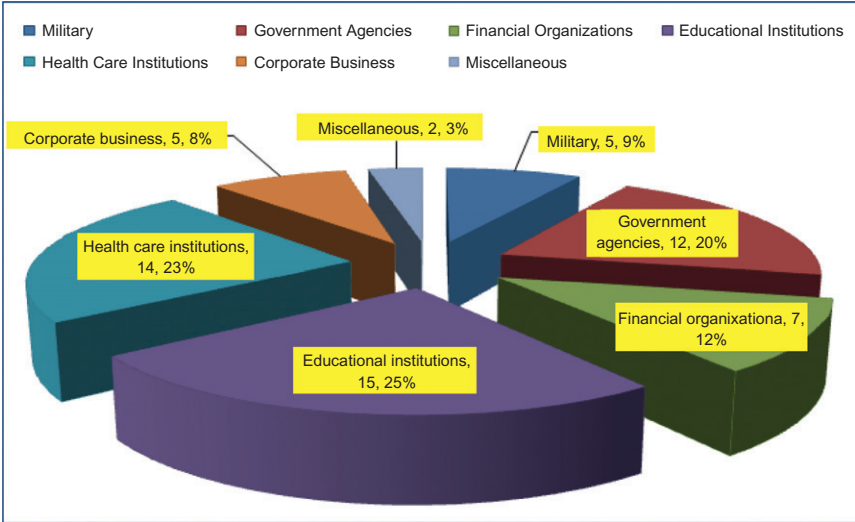


FIG. 5. Number of incidents based on type of organization (data in Table II).

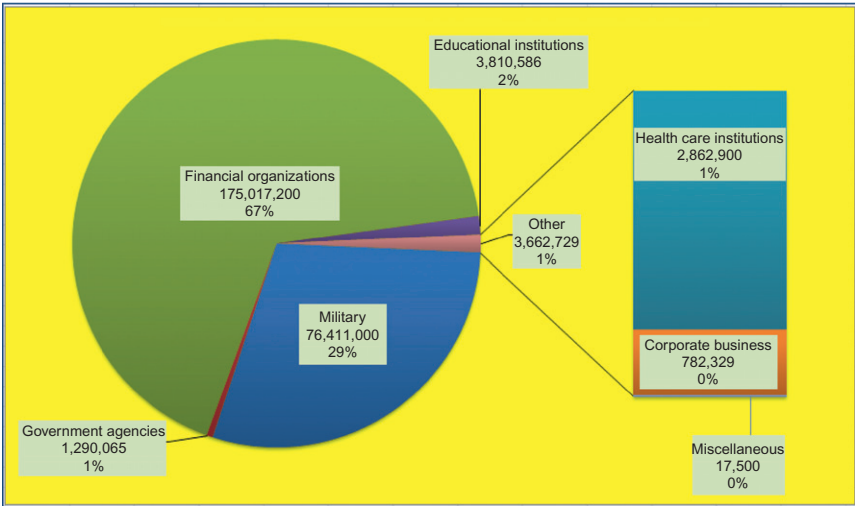


FIG. 6. Compromised records based on type of organization (data in Table III).

TABLE II  
NUMBER OF INCIDENTS BASED ON TYPE OF ORGANIZATION

Organization type	Number of incidents
Military	5
Government agencies	12
Financial organizations	7
Educational institutions	15
Healthcare institutions	14
Corporate business	5
Miscellaneous	2

TABLE III  
COMPROMISED RECORDS BASED ON TYPE OF ORGANIZATION

Organization type	Number of compromised records
Military	76,411,000
Government agencies	1,290,065
Financial organizations	175,017,200
Educational institutions	3,810,586
Healthcare institutions	2,862,900
Corporate business	782,329
Miscellaneous	17,500

## 4. The Genesis of the Problem

The primary components for a successful identity theft are name, Social Security Number, date of birth, address, and any other personally identifiable information such as driver's license information, passport details, account information, or online login credentials that can be used to generate counterfeit IDs or allow an identity thief to open a line of credit in the victim's name without the victim's knowledge [14] (Fig. 7). Once this information is compromised and is out in the public domain, it is very difficult to control the damage. The underground market for exploiting personally identifiable information is so efficient that stolen credit/debit card information has been used in many cases to perform fraudulent financial transactions in a matter of minutes rather than days from the time information was compromised [15].

The primary reasons that make identity theft the fastest-growing crime in the USA can be identified as:

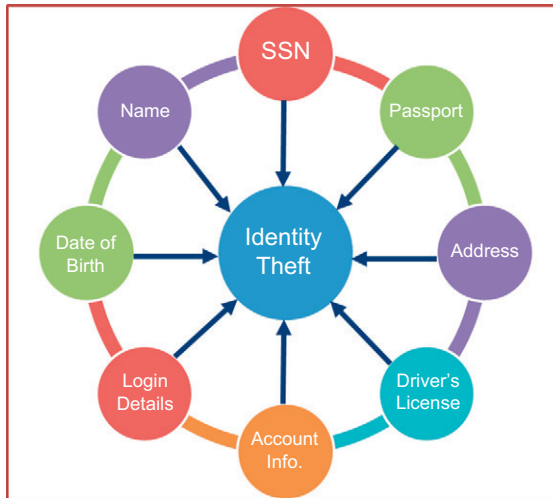


FIG. 7. Primary components of identity theft.

- (a) The unprecedented and unregulated use of Social Security Number as a primary identifier for an entire range of transactions.
- (b) The ubiquitous use of fungible credentials.
- (c) Phenomenal growth in the number and sophistication of phishing attacks.
- (d) Ease of making counterfeit IDs facilitated by an exponential growth in the technological prowess available to the masses.
- (e) The inadequate and far-from-secure credential management procedures.

Each of these aspects is examined in detail in the following sections.

## 5. How SSN Became the *De Facto* Primary Key for Most Databases

The use of the Social Security Number was a by-product of the Social Security Act of 1935. This was extended to federal agencies other than the Social Security Administration by Executive Order 9397 in 1943. These restrictions were further relaxed in the Federal Privacy Act of 1974 to include state and local agencies. This resulted in the unprecedented and unregulated use of Social Security Number as a

primary identifier for an entire range of transactions even when there was no logical/legal requirement for using the SSN [16]. Now state governments are attempting to do damage control with what are known as “Security Breach Notification Laws.” Generally, these laws require companies, and in some cases state agencies, to report to consumers if their computers have experienced a security breach resulting in important personal information being released to unauthorized parties. As per the National Conference of State Legislatures Web site, 46 states, District of Columbia, Puerto Rico, and the Virgin Islands had enacted such legislation as of April 12, 2010 [17]. Although the laws differ somewhat, they generally replicate California’s breach protection law passed in 2003. At least two states, Michigan and Massachusetts, require businesses that collect SSNs to have an “information security program that specifically addresses SSN protection.” The only states presently without such a law are Alabama, Kentucky, New Mexico, and South Dakota.

The good news is that the Federal and various state governments are now taking the issue of identity theft very seriously [18]. Of the 31 recommendations made in the President’s Identity Theft Task Force Report [19], the top two recommendations are to decrease the unnecessary use of SSNs in the public sector including the establishment of a Clearinghouse for Agency Practices that Minimize Use of SSNs, and develop a comprehensive record of SSN use in the private sector. Other recommendations included increased prosecution of identity theft and the establishment of a National Identity Theft Law Enforcement Center to deal more effectively with various aspects of the crime.

## **6. The Ubiquitous Use of Fungible Credentials**

The operative meaning of “fungible” in this context is “interchangeable” [20]. As we use the term, fungible documents include counterfeits (e.g., currency), forgeries (contracts, negotiable instruments, signatures), as well as a third category that we will call “quasi-verifiable” or “legitimized.” Most fungible documents are created for criminal purposes, usually with the intent to defraud. “Legitimized” documents are those that are produced by legitimate issuing authorities based upon false information. One example is a driver’s license that has been issued to an individual under a fictitious name. That is where the quasi-verifiable characteristic comes in. The driver’s license corresponds to a Department of Motor Vehicle (DMV) database record—in that sense it is legitimate. However, the data fields do not correspond to the holder—both the credential and the credentialed are real; they just do not correspond to each other.

Fungible credentials are useful precisely because they simultaneously obscure the criminal’s real identity and facilitate any authentication that may be required. The starting point of a legitimized credential remains the counterfeit document. However, the counterfeit is only the means to the end of obtaining a legitimized document.

A typical scenario might be to begin by ordering a counterfeit passport from people who linger about the dark side of swap meets. It is not uncommon nowadays for criminals to special order the passports by country, name, visas, and endorsements. The counterfeit passport is then used in the “credential amplification” phase to produce the tokens that will be actually used to defraud—e.g., a driver’s license issued by DMV. The typical DMV has no means to validate passports, so the amplification is relatively straightforward. The driver’s license may in turn be used to obtain a Social Security Number, county health card, etc. until the wallet is filled. It goes without saying that the variations on this theme seem endless.

## 7. Phishing

According to Microsoft [21], “Phishing (pronounced ‘fishing’) is a type of online identity theft. It uses e-mail and fraudulent Web sites that are designed to steal your personal data or information such as credit-card numbers, passwords, account data, or other information. Con artists might send millions of fraudulent e-mail messages with links to fraudulent Web sites that appear to come from Web sites you trust, like your bank or credit-card company, and request that you provide personal information. Criminals can use this information for many different types of fraud, such as to steal money from your account, to open new accounts in your name, or to obtain official documents using your identity.”

Phishing attacks carried out using Short Messaging Service (SMS) or text messages on cell phones are referred to as *SMiShing*, while those that depend on voice communications especially using the Voice-over-Internet Protocol (VOIP) are termed as *Vishing*. A related term, “Pharming” refers to Web site redirection with an aim to carry out phishing attacks.

### 7.1 Phenomenal Growth in the Number and Sophistication of Phishing Attacks

A phenomenal growth in the number and sophistication of phishing attack is a major contributor to the exponential growth of identity theft and related crimes. As per the Anti-Phishing Working Group (APWG)—a global consortium of law enforcement agencies and private sector entities with a stake in secure online transactions that strives to eliminate identity theft and related fraud resulting from phishing, pharming, and e-mail spoofing—more brands are under attack today than ever before [22,23]. As per the Phishing Activity Trends Report, 4th Quarter/2009 [24], the number of hijacked brands rose to a record 356 in October 2009 up nearly 4.4% from the

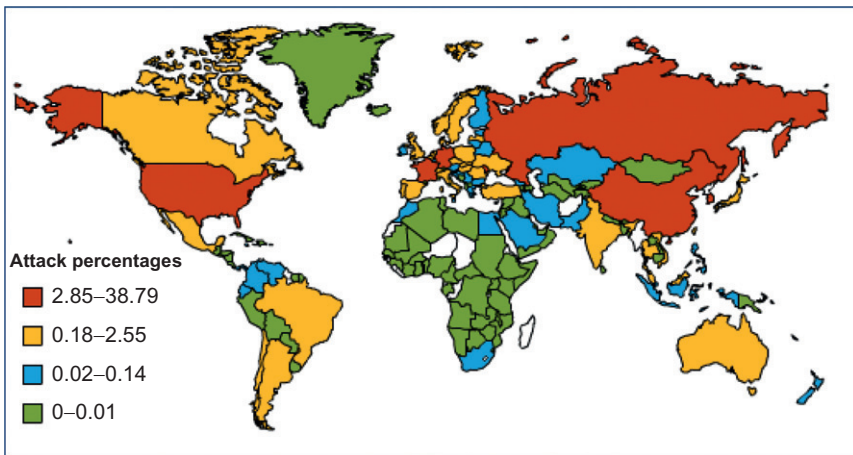


FIG. 8. Global phishing and crimeware map. Source: Anti-Phishing Working Group Web site, generated by Websense Security Labs.

previous record of 341 in August 2009. The report also states that “the United States continued its position as the top country hosting phishing sites in Q4, 2009.”

Figure 8 shows a global distribution of Phishing and Crimeware (a term coined by Peter Cassidy, Secretary General of the APWG to refer to malware specifically designed to perpetrate cybercrime) attacks for a 12-month period from June 2009 to June 2010 [25].

## 7.2 The Importance of Secure Online Transactions

To effectively deal with phishing and other online threats, the best defense against identity theft is undoubtedly practicing a proactive policy of an “abundance of caution” based on awareness and a thorough understanding of the various threats and their countermeasures. Some of the salient points to remember before entering any sensitive personal or financial information on a Web site are discussed below.

### 7.2.1 *Use of Hypertext Transfer Protocol Secure Instead of Hyper Text Transfer Protocol*

The Hyper Text Transfer Protocol (HTTP), the backbone of the World Wide Web, is inherently insecure for sensitive transactions. To ensure secure transmission of data, HTTP is used in conjunction with Secure Socket Layer (SSL) or its successor



Transport Layer Security (TLS) in what is known as Hypertext Transfer Protocol Secure (HTTPS). SSL/TLS provide encryption of the data between endpoints as well as a mechanism to certify the authenticity of a web server. From an end-user's point of view, it is necessary to confirm that the protocol mentioned in the URL in the address bar of the browser should be "https" and not "http" when dealing with sensitive information.

### 7.2.2 *Is the "Lock" Really Your "Key" to a "Safe and Secure" Transaction?*

A prominent visual indicator of SSL has been the "lock" icon displayed on the right-hand side in most browsers' status bar as shown in Fig. 9. Many malicious sites have successfully fooled victims into believing that a Web site offers secure transactions just because it displays an image of a "lock" icon somewhere on its page even though the protocol in the address bar clearly states "HTTP" thereby signifying an inherently insecure connection. Similar to the real-estate industry, the location of the "lock" icon is of paramount importance to determine the reliability.

### 7.2.3 *Encryption Versus Trust*

Most online users wrongly interpret the lock icon in the status bar as an indication of a guarantee of a safe transaction. All that the lock icon denotes is that the connection between the web browser and the server uses encryption. It does not imply that the web server is a trusted source. Rouge Web sites set up with malicious intent will also display the lock icon as long as they use SSL, and the connection is

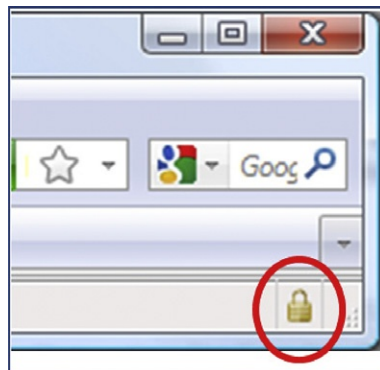


FIG. 9. SSL "lock" icon displayed in browser's status bar.

encrypted. The authentication of a Web site as a trusted site is handled by the associated digital certificate. An expired, invalid, or revoked certificate is as bad as (if not worse than) the absence of a certificate but many users tend to skip the browser warnings and assume that as long as there is a certificate (even though invalid), the transaction is secure. The certificate contains the web server's identity information which needs to be authenticated and verified by an independent third party (known as Certification Authority) for a site to be considered as "trusted."

Figure 10 shows a comparison of a valid/authenticated digital certificate with an invalid certificate both issued to the same entity. The certificate on the left-hand side is invalid as it has not been authenticated by an independent trusted Root Certification Authority. The person it is issued to as well as the person it is issued by is one and the same (Amit Grover). The certificate on the right-hand side is valid as it has been authenticated by an independent trusted Root Certification Authority, and the certification path is clearly evident and verifiable.

It is interesting to note, however, that both certificates represent a public key in the PKI cryptography system and generated a corresponding private key for the user which can be used for encryption/decryption. Hence, the "Details" tab will not indicate anything unusual even with the invalid certificate as shown in Fig. 11.

Another important precaution is to ensure never to trust a site whose certificate has been revoked. RFC 5280 specifies 10 different reasons for certificate revocation including private key compromise and fraudulent or erroneous issuance of the digital certificate [26]. A high-profile example was when VeriSign revoked two digital certificates issued to Microsoft after discovering that an individual had obtained them fraudulently by falsely claiming to be Microsoft's representative. As per the VeriSign advisory [27], "The certificates were VeriSign Class 3 Software Publisher certificates and could be used to sign executable content under the name 'Microsoft Corporation.' The risk associated with these certificates is that the fraudulent party could produce digitally signed code and appear to be Microsoft Corporation. In this scenario, it is possible that the fraudulent party could create a destructive program or ActiveX control, then sign it using either certificate and host it on a Web site or distribute it to other Web sites." Figure 12 shows the revoked certificates.

#### 7.2.4 Visual Indicators

The foregoing discussion underlines the critical importance of correctly analyzing and interpreting the visual indicators during an online session. Thus, ensuring a secure connection requires verifying the validity of the digital certificate as well as the location of the "lock" icon. The lock icon in the status bar was used to signify a level of trust in the Web site for a number of years till it was successfully

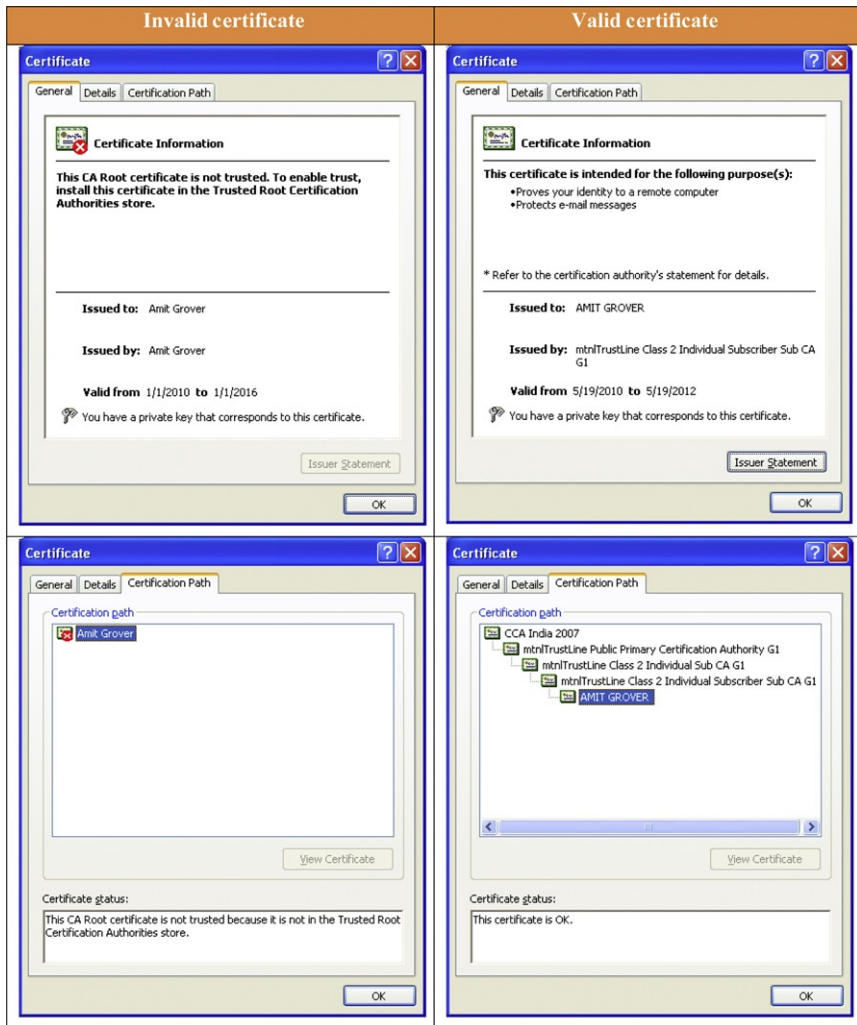


FIG. 10. Comparison of valid and invalid digital certificates.

demonstrated that the status bar in a browser can be faked and JavaScript can be used to manipulate the fake status bar in real time to falsely display the lock icon even when the connection was not encrypted [28]. This prompted many browsers to move the location of the “lock” icon to the Navigation/Address bar and depict the presence

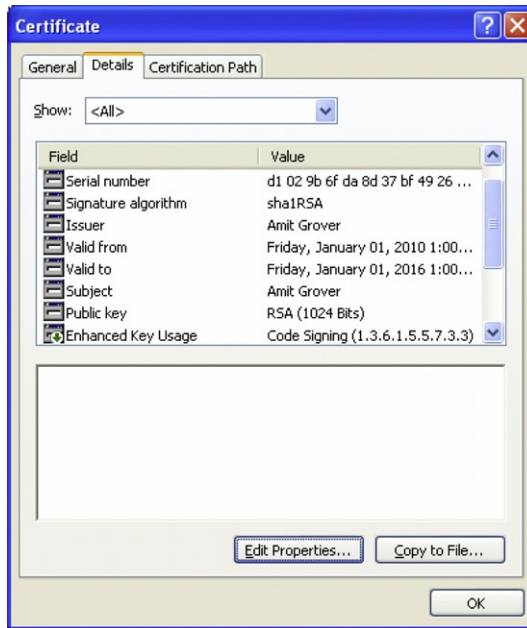


FIG. 11. “Details” tab of an invalid digital certificate.

of SSL/TLS with a different color of either the text or the background of the Navigation/Address bar. This is considered extremely difficult to spoof, and there are no reported claims to break this security feature as yet.

**7.2.4.1 Trusted Sites with a Secure and Authenticated Connection.** Figures 13–16 show the different visual indicators for a trusted HTTPS connection with an authenticated certificate in four popular browsers, viz., Mozilla Firefox v 3.6.3, Apple Safari v 5, Microsoft Internet Explorer v 8, and Google Chrome v 5, respectively.

**7.2.4.2 Sites with Invalid Certificate Warning.** Figures 17–20 show the different visual indicators for an untrusted HTTPS connection with an invalid/unauthenticated certificate in four popular browsers, viz., Mozilla Firefox v 3.6.3, Apple Safari v 5, Microsoft Internet Explorer v 8, and

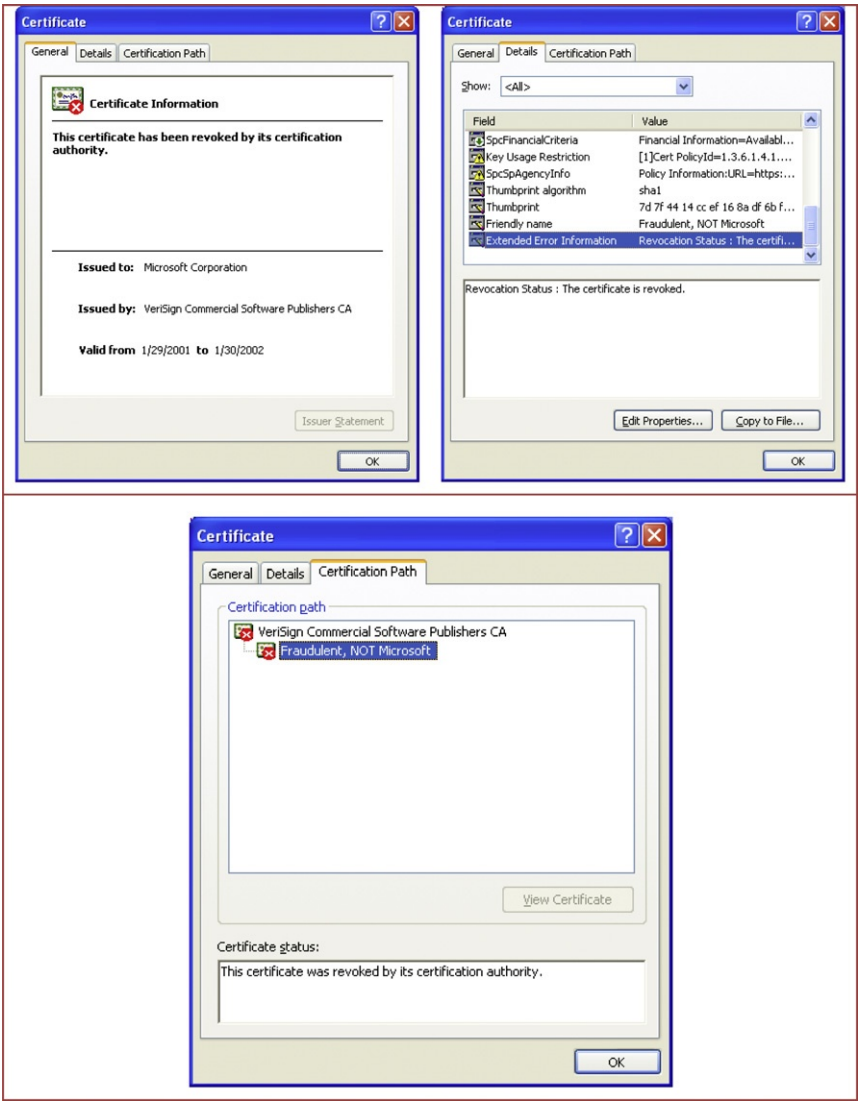


FIG. 12. Details of a revoked digital certificate.



FIG. 13. Visual indicators for a trusted HTTPS connection in Firefox v 3.6.3.

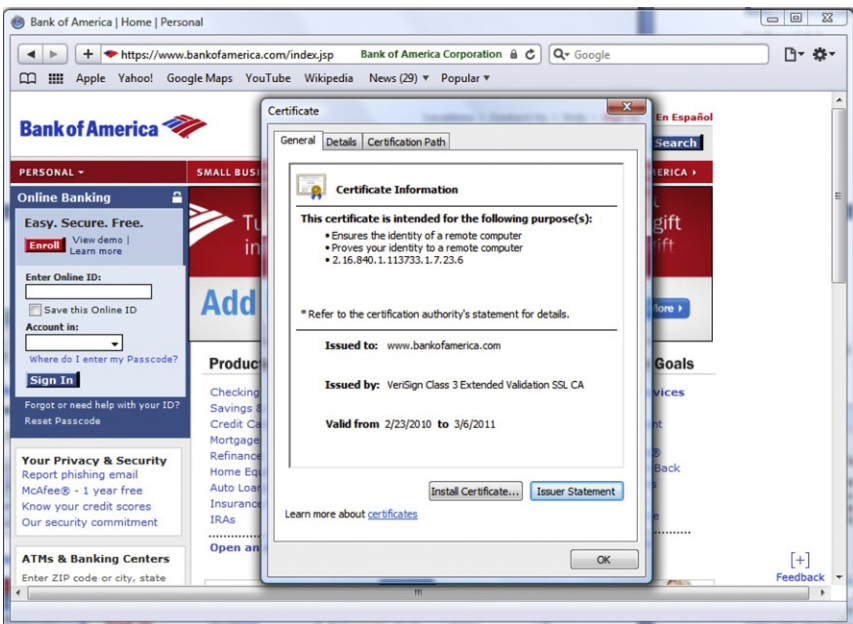


FIG. 14. Visual indicators for a trusted HTTPS connection in Safari v 5.

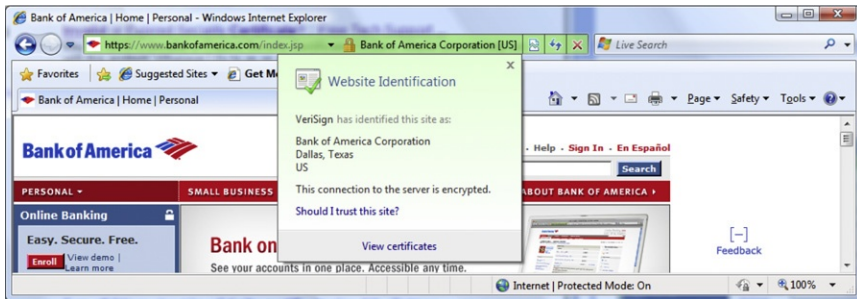


FIG. 15. Visual indicators for a trusted HTTPS connection in Microsoft Internet Explorer v 8.

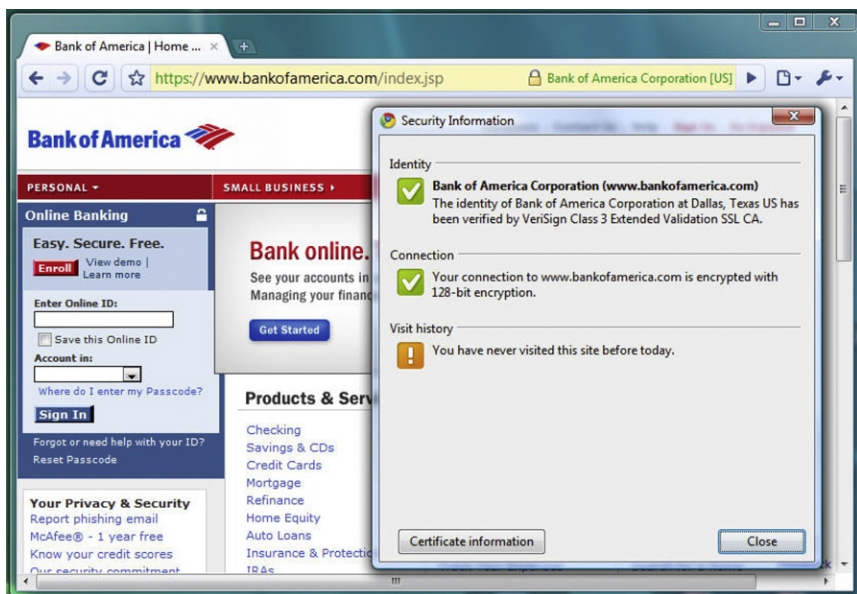


FIG. 16. Visual indicators for a trusted HTTPS connection in Google Chrome v 5.



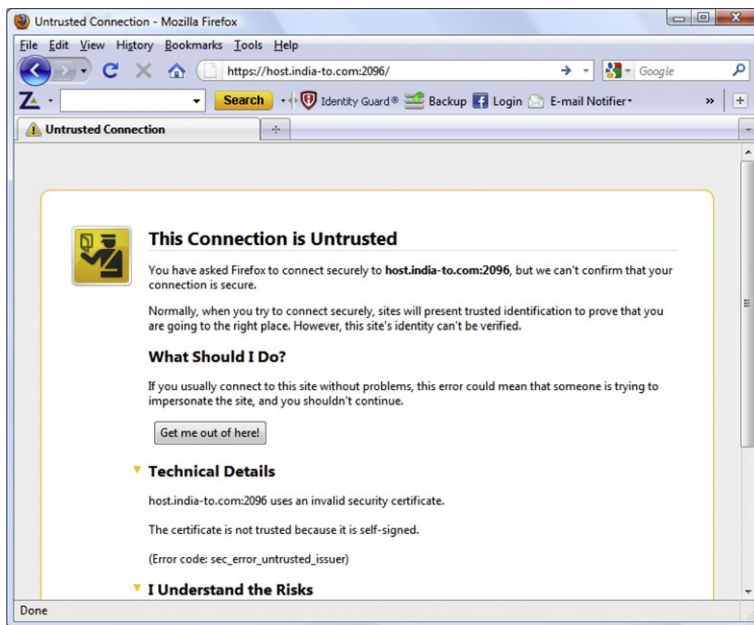


Fig. 17. Visual indicators for an untrusted HTTPS connection in Firefox v 3.6.3.

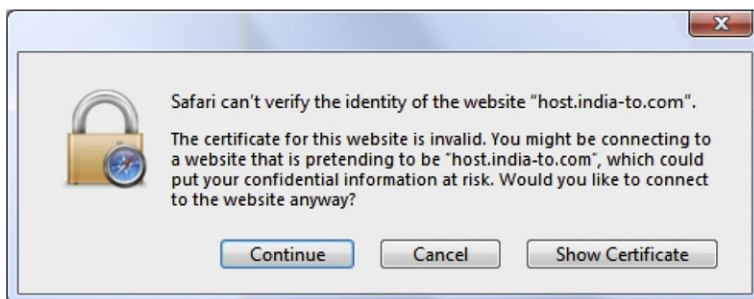


Fig. 18. Visual indicators for an untrusted HTTPS connection in Safari v 5.



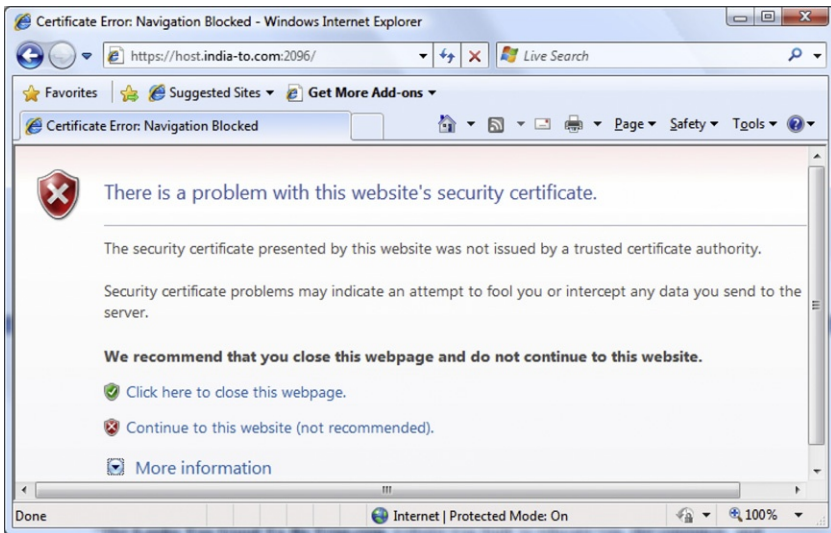


FIG. 19. Visual indicators for an untrusted HTTPS connection in Microsoft Internet Explorer v 8.

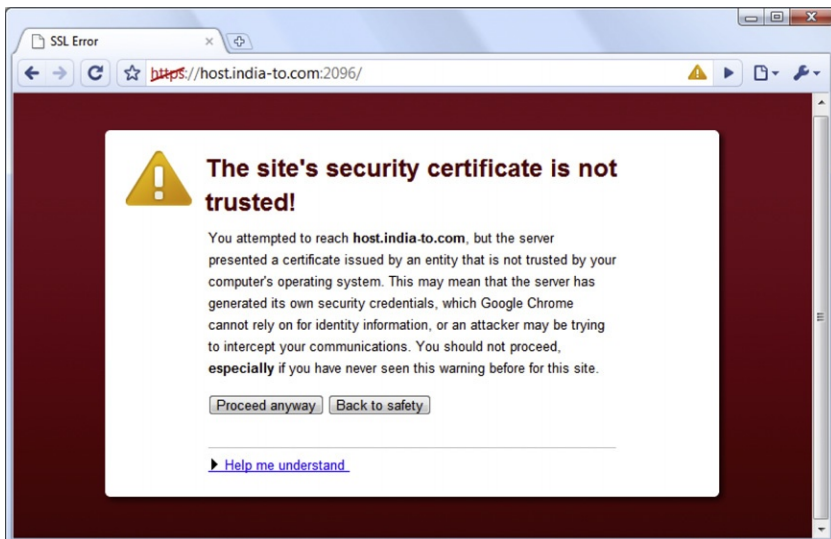


FIG. 20. Visual indicators for an untrusted HTTPS connection in Google Chrome v 5.

Google Chrome v 5, respectively. In this specific example, the certificate has not been verified by a trusted root Certificate Authority.

### ***7.2.5 Favicon Spoof to Undermine the “Lock” Icon Visual Indicator***

With many popular browsers moving the location of the SSL “lock” icon to the Navigation/Address bar and specifically to the right side of the URL, an exploit emerged that puts the “lock” icon in the Navigation/Address bar but on the left side of the URL as opposed to the right side. This is done by replacing the Favicon—short for “favorites” icon that generally displays the logo of the Web site—with a “lock” symbol. This exploit banks on creating sufficient confusion in the mind of the unsuspecting victim as a vast majority of the online users are not savvy enough to appreciate the difference between a favicon placed by a malicious user and an SSL lock icon placed by the browser. [Figure 21](#) shows numerous examples of sites—all displaying a “lock” icon (of various styles) in the Navigation/Address bar—and none of them actually using SSL as is evident from the “HTTP” in the URL. It is also noteworthy that the lock icon in the status bar is missing (as highlighted in [Fig. 22](#)) even though the browser used is Mozilla Firefox v 3.6.3 which uses the status bar to display the visual indicator for an SSL/TLS connection.

### ***7.2.6 Domain Validation Versus Extended Validation Certificates***

To make things more complicated, all valid digital certificates do not offer the same level of trustworthiness. Entry level certificates known as Domain Validation Certificates are issued after minimal verification, and request are honored as long as the person requesting the certificate is the registered owner of the domain name. However, Extended Validation (EV) Certificates are issued after thorough vetting of credentials of the applicant by the Certificate Authority and thus offer the highest industry standard for authentication and trustworthiness. The examples shown in figures through are for EV Certificates. When viewed in Firefox, a Domain Validation Certificate will use blue color as the visual indicator as opposed to green that is used for representing EV certificates as shown in [Fig. 23](#).

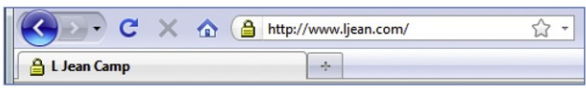


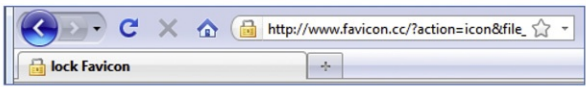
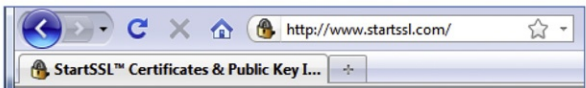
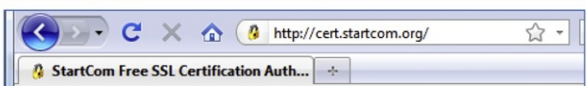


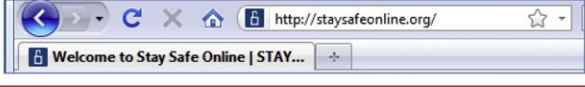
Browser screenshots indicating favicon spoof	Domain
	ljean.com
	iang.org
	pgp.com
	favicon.cc
	startssl.com
	startcom.org
	iconix.com
	sslshopper.com
	staysafeonline.org

Fig. 21. Favicon spoof undermines the “lock” icon visual indicator.

## 8. Modus Operandi

One of the primary factors that have fueled the unprecedented rise in identity theft incidents is the easy and relatively cheap availability of computing resources including the necessary hardware and software required for counterfeiting fungible credentials. An entire set of high-quality counterfeit driver's licenses can be made at home with just



FIG. 22. Favicon spoof with the missing “lock” icon visual indicator in the status bar.

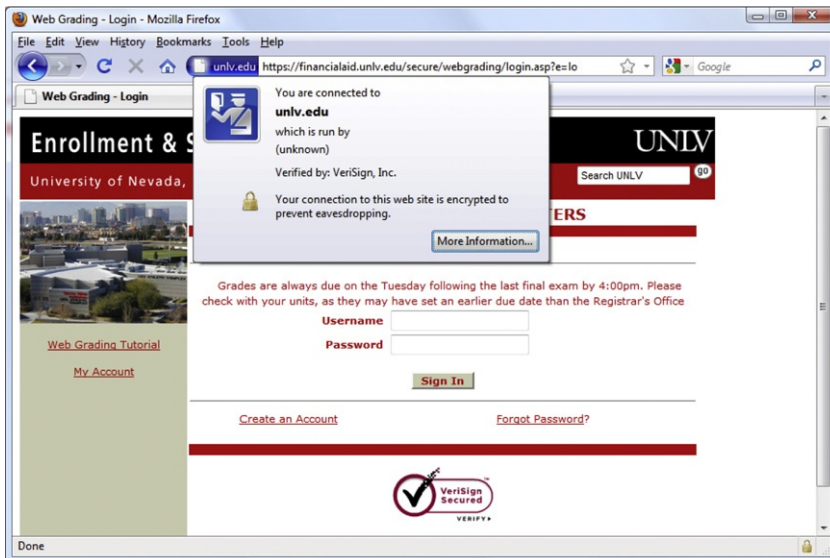


FIG. 23. Visual indicators for a trusted HTTPS connection with a DV certificate in Firefox v 3.6.3.

a regular computer, card printer, credential management software, magnetic stripe writer, and card stock/lamination supplies that are easily available at a cost that is minimal as compared to the potential return on investment (ROI) that such an operation promises. It is therefore understandable as to why obtaining multiple counterfeit IDs with fictitious or stolen identities such as those shown in Fig. 24 is so easy.

Easy accessibility to the Internet compounds the problem by facilitating the identity thief to carry out the crime while being located in a geographical location outside the jurisdiction of the victim's country, thereby dramatically reducing the risk of facing any legal consequences. Identity thieves use the Internet to “safely and efficiently” sell the stolen personally identifiable information of victims through



FIG. 24. Near-perfect counterfeit IDs with different fictitious or stolen identities being used by a single individual. Source: The Identity Theft and Financial Fraud Research and Operations Center, [www.itffroc.org](http://www.itffroc.org).

organized crime broker sites which are commonly known as “dumpsites.” The name comes from the word “dump” which in the credit-card industry parlance refers to an electronic copy of the magnetic stripe data of a credit/debit card [29]. What is shocking is that this underground black market for stolen card information is highly organized and thrives openly on the Internet from Web sites hosted in countries with a poor track record of law enforcement.

On a professionally run dumpsite based in Russia, called Golden Dump (registered to a certain Alexey A Potapov from Moskow), the prices of stolen dumps ranged from \$23 to \$200 as shown in the screenshot taken on June 25, 2010 (Fig. 25) [30]. The prices depend on how detailed the stolen information is and





FIG. 25. A professionally run Russia-based dumpsite selling dumps ranging from \$23 to \$200.

the extent of financial gain a Fin-Av stands to make by purchasing a particular dump. The communication is generally done using the anonymous instant messaging service; ICQ or e-mail and the preferred route for money transfer are services such as Western Union, Moscow-based WebMoney Transfer, or the Caribbean Island-based e-Gold Ltd. As per a report in the New York Times [31], “A user by the nickname Sirota is peddling account information so detailed, and so formatted, that it clearly came from a credit report. He is asking \$200 per dump on accounts with available balances above \$10,000, with a minimum order of five if the buyer wants accounts associated with a particular bank. ‘Also, I can provide dumps with online access,’ he wrote. ‘The price of such dumps is 5% of available credit.’”

To make matters worse, trends indicate that the underground prices of dumps are only decreasing and as per the RSA Online Fraud Report for August 2010 on “Prices of Goods and Services offered in the Cybercriminal Underground,” Fin-Avs can buy CVV2 data sets for as low as \$1.50, “Fulls” data sets for as low as \$5, and Track 2 data

dumps for as low as \$15. A DDoS Attack Service for 24 h can be purchased for just \$50 and bulletproof hosting services (to allow criminals evade law enforcement) can be purchased for as low as \$87 per month [32].

Figure 26 shows a screenshot of a Malaysia-based dumpsite forum with all the necessary details to produce counterfeit credit/debit cards or use the data for online financial transactions as the 3-digit Card Verification Value also known as the CVV code (required for completing Card-Not-Present or CNP transactions) is also displayed [33].

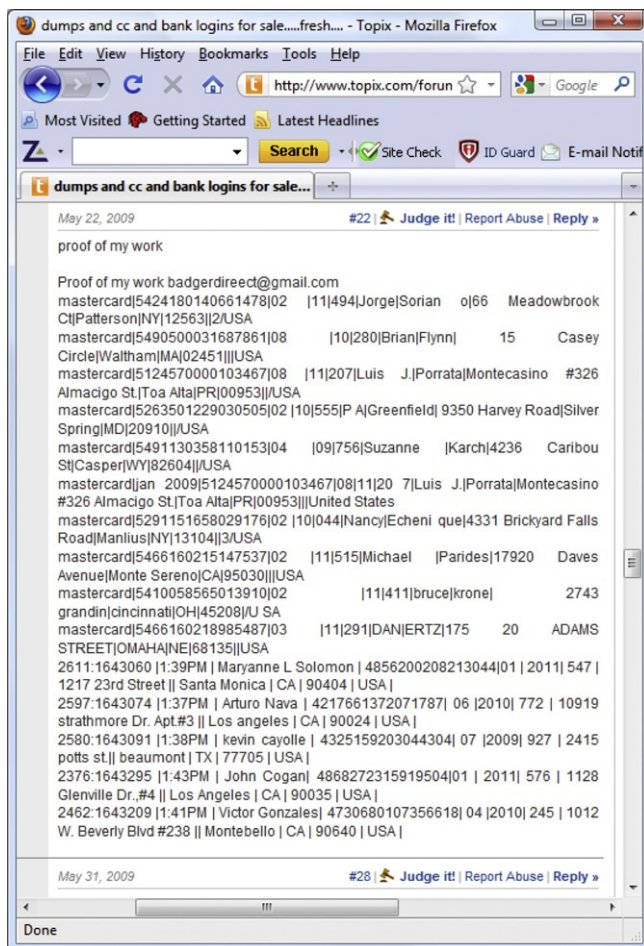


FIG. 26. A screenshot of a Malaysia-based dumpsite with stolen credit-card details.

## 9. Inadequate Credential Management Procedures

Another important factor responsible for the exponential rise in identity theft incidents is the inadequate and far-from-secure credential management procedures used during all the typical phases of credential management including creation, validation, authentication, and storage.

A recent news report on CNN revealed that two different women sharing the same birthday and the same name—Alyssa Green—with one living in Albany, New York (SSN issued in Florida) and the other in Minneapolis (SSN issued in Illinois) have been allotted the same Social Security Number by the Social Security Administration making life difficult for both of them [34]. As mentioned in Section 5, the inadequate credential validation procedures allow quasi-verifiable IDs to be used for “credential amplification,” thereby legitimizing counterfeit credentials. The over-reliance on “look and feel” authentication despite the fact that typical credentials such as the driver’s license are inherently fungible indirectly gives a boost to the business of producing counterfeit credentials. The far-from-secure storage procedures were highlighted by a 2005 incident where identity thieves stole around 1700 blank driver’s licenses along with laminated covers and the entire license-making equipment including a digital license camera, a camera computer, and a license printer from a Nevada Department of Motor Vehicles office in North Las Vegas [35]. The operation was conducted in a very professional manner, and the thieves were out of the DMV office with all the necessary equipment in less than 20 min. Given this background, it is hardly surprising to come across news headlines such as, “Teens can get fake IDs in a few keystrokes on Web” [36]. CardSleuth is a unique solution that provides the next generation of credential management and control.

### 9.1 CardSleuth

CardSleuth is a secure, ephemeral, self-referential mobile credential system developed at ITFF/ROC to solve the abovementioned problems in a traditional credential management system. It is FIPS compliant and supports a layered-security approach toward managing credentials. As shown in Fig. 27, it is ideal for various types of credentials including employee ID, Hotel room key, driver’s license, event ID, and financial transactions card. CardSleuth offers encrypted ID information as well as photo encoded in standard 2D barcode symbologies such as PDF 417 and the QR Code. Additional security is provided by means of detailed access and validation logs. It is compatible with standard encoding technologies including magnetic stripes, common 2D barcode symbologies, RFIDs, and smart cards.





Fig. 27. CardSleuth: The next generation of credential management and control.

A typical ID scan as shown in Fig. 28 indicates complete badge holder information including normal and photographs, visual indication of the scan result, the encrypted data stream, multilevel security with two separate barcode symbologies being used simultaneously and support for biometrics or future enhancements.

## 10. Strategies for Defeating Identity Thieves

This section discusses in detail the finer points of the two-pronged strategy of prevention and cure. The first part deals with the precautions that can effectively prevent a person from becoming a victim of identity fraud, while the other part focuses on the measures to be taken if a person's identity has already been compromised. While prevention is always better than cure, the key to surviving an identity theft is taking effective steps to minimize the damage by carrying out specific actions in a timely manner. The importance of keeping one's presence of mind



FIG. 28. CardSleuth features at a glance.

and acting swiftly to effectively defeat one's identity thief is perhaps best demonstrated by Seattle-based 23-year-old Michelle McCambridge who helped authorities not only to catch her identity thief but also to bust an active ring of Identity thieves who had stolen at least 39 identities [37].

## 10.1 Precautions to Prevent ID Theft

The precautions that should be taken to prevent being a victim of identity theft can broadly be classified into two categories based on the type of transaction: offline transactions and online transactions, both of which are described in detail in the following sections.

### 10.1.1 Precautions for Offline Transactions

#### 10.1.1.1 Document and Information Handling.

- Be vigilant whenever dealing with sensitive personal or financial information.
- Shred all unnecessary documents that contain personally identifiable or financial information before disposing them off as dumpster diving is a very big source of identity theft.

- Do not carry your Social Security card in your wallet unless required for a specific purpose.
- Be extremely cautious about providing your SSN to non-governmental agencies and do so only if it is absolutely necessary.
- Do not leave checks in your car and avoid carrying your check book with you unless required for a specific reason. The Fed Chairman, Ben Bernanke became a victim of identity theft when his wife left her purse carrying personalized checks in a restaurant [38,39].
- Do not carry all your credit cards and debit cards in your wallet—if your wallet is lost or stolen, you stand to lose all your cards.
- Prefer using credit cards over debit cards as a fraudulent use of a stolen debit card number would result in immediate withdrawal of funds from your checking account as opposed to a financial transaction on the credit card that can be disputed more easily with the banks.

#### **10.1.1.2 Monitoring Financial Accounts and Records.**

- Monitor your credit reports thoroughly and regularly.
- Federal law allows one free credit report from each of the three nationwide consumer credit reporting companies: Equifax, Experian, and TransUnion every year by going to [www.annualcreditreport.com](http://www.annualcreditreport.com). It's a good practice to stagger the reports from the three different agencies thereby allowing a free credit report every 4 months.
- One can also utilize free services at [www.Quizzle.com](http://www.Quizzle.com) that offer free credit reports as well as free credit score twice a year to monitor the credit reports more effectively. Call the three major credit reporting bureaus—Equifax, Experian, and TransUnion and ask them verbally as well as in writing to correct any discrepancies in your credit report with immediate effect.
- Track the possible misuse of your identity at the free service My ID Score, [www.myidscore.com](http://www.myidscore.com).
- Be wary of tall claims by companies offering services to repair bad credit history or guaranteeing protection from identity theft. Just a few months back, identity theft prevention service LifeLock was fined \$12 million for making inaccurate identity theft prevention claims and in fact failing to secure its own customer data adequately [40].
- Scrutinize credit card and bank account statements closely. Even small amounts that look suspicious should be followed up and reconciled. The need for this is

highlighted by the recent incident where FTC revealed that fraudsters have stolen millions of dollars in a highly sophisticated scheme that fraudulently charged 1.35 million credit cards and ran successfully for about 4 years [41]. The scammers escaped detection for such a long time by charging very small amounts per transaction (usually between \$0.25 and \$9.00 per card).

### 10.1.1.3 ATM Transactions.

- While using ATM machines, make sure that the machine does not look suspicious as many identity thieves install card skimmers to capture the information from the magnetic stripes and hidden cameras to capture the PIN.
- If an ATM appears to be altered, there is a high possibility that it has been equipped with a skimming device.
- Cover the keypad while entering the PIN on an ATM.
- Be aware that stand alone ATMs in convenience stores may be more susceptible to fraud than bank-based ATMs.

## 10.1.2 Precautions for Online Transactions

**10.1.2.1 Defense in Depth.** It is important to use a multilayered approach to security so that a single failure does not translate into a complete breakdown of security. This involves using tools like antivirus, antimalware (to detect keyloggers, crimeware, etc), firewalls, and security plug-ins in addition to ensuring that system updates and security patches are always up-to-date. A free personal firewall, ZoneAlarm, is a very effective tool that gives real-time online protection from malicious attackers. Figure 29 shows the yellow colored visual warning produced by ZoneAlarm when a user tries to access a site with suspicious activity.

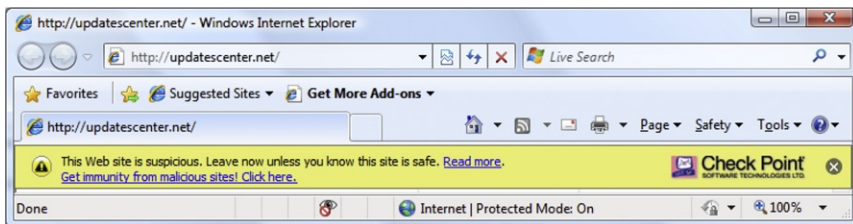


FIG. 29. Visual warning produced by ZoneAlarm.

Most browsers support a wide range of browser plug-ins and add-ons, and at the time of writing, there were almost 700 different add-ons available covering an entire gamut of privacy and security issues for Firefox as shown in Fig. 30. It is a good idea to use verified add-ons to make one's online experience more secure.



FIG. 30. Privacy and security add-ons for Firefox.

**10.1.2.2 Anti-Phishing Measures.** Most popular web browsers use phishing filters to warn users about known phishing sites based on global blacklists. Thus, for example, when a user tries to access a known phishing site such as <http://www.kinova.net/PayPal.com/index.php>, which hosts a perfectly spoofed PayPal site as shown in Fig. 31, most browsers display adequate visual warnings.

Figures 32–36 show the different visual indicators when an attempt is made to access a known dangerous Web site in Phishing and other malicious activities in four popular browsers, viz., Mozilla Firefox v 3.6.3, Apple Safari v 5, Microsoft Internet Explorer v 8, and Google Chrome v 5, respectively.

In case the browser does not support phishing filters, the defense-in-depth strategy would pay off as ZoneAlarm would step in and issue a warning as indicated in Fig. 37.

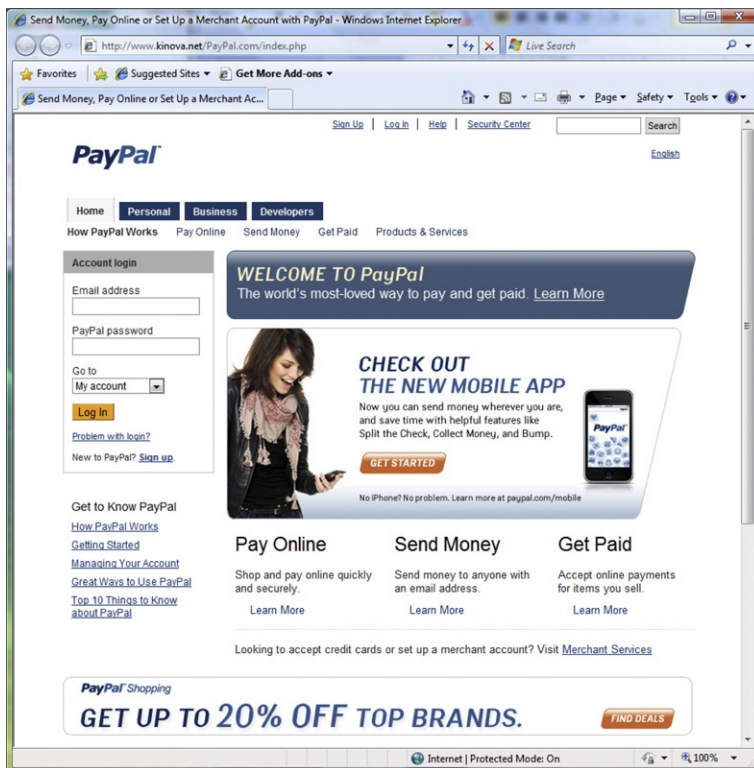


FIG. 31. Perfectly spoofed PayPal site on [www.kinova.net](http://www.kinova.net).



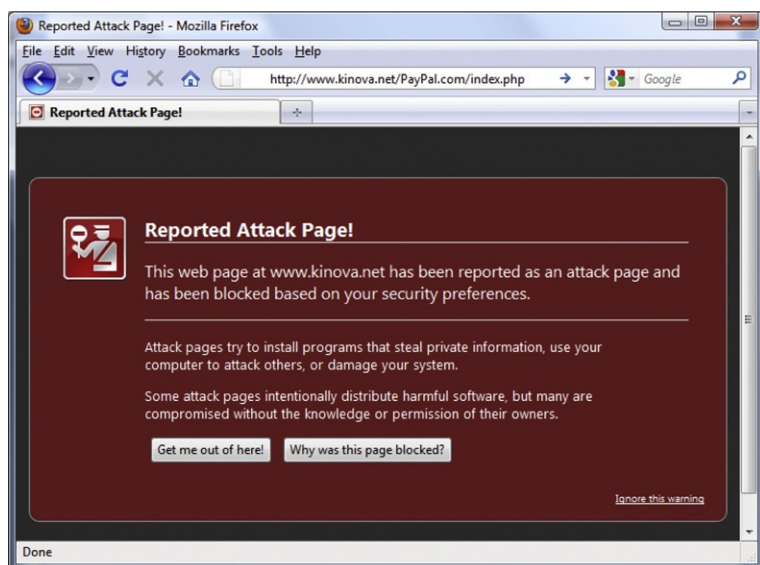


FIG. 32. Visual indicators while accessing a known dangerous Web site in Firefox v 3.6.3.

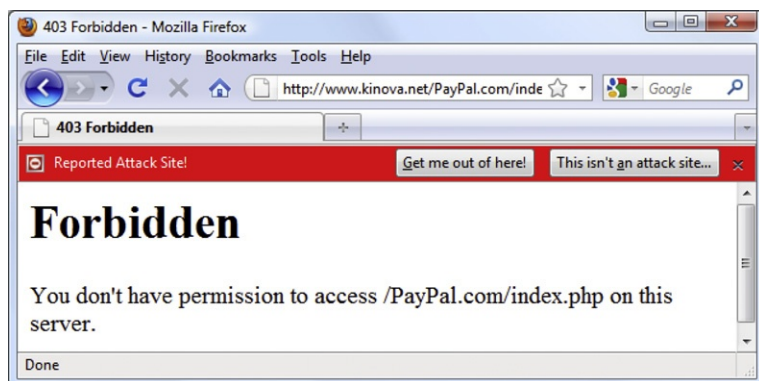


FIG. 33. Visual indicators while accessing a known dangerous Web site in Firefox v 3.6.3.



FIG. 34. Visual indicators while accessing a known dangerous Web site in Apple Safari v 5.



FIG. 35. Visual indicators while accessing a known dangerous Web site in Internet Explorer v 8.



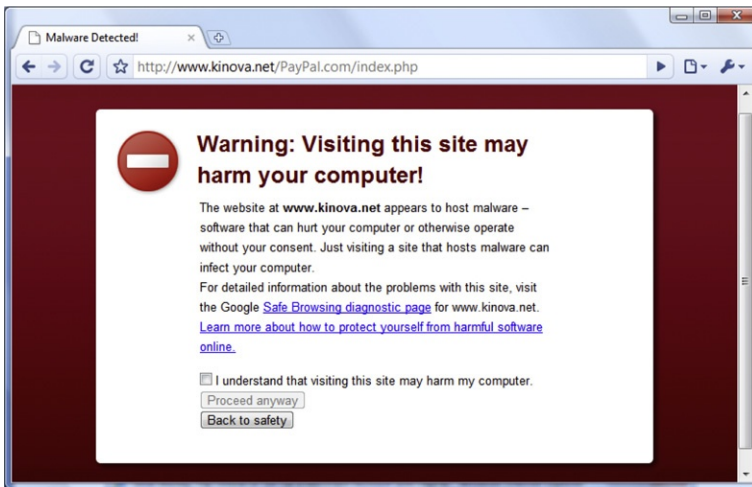


FIG. 36. Visual indicators while accessing a known dangerous Web site in Google Chrome v 5.

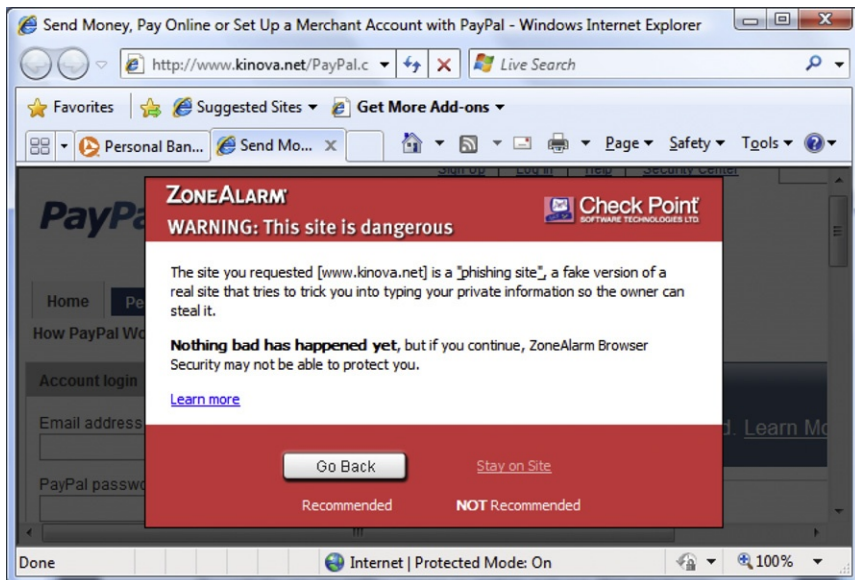


FIG. 37. Visual warning issued by ZoneAlarm while accessing a known dangerous Web site.

Since these warning are based on global blacklists and whitelists and new threats keep emerging every day, it is possible that a particular filter may not detect all known bad sites. In case one requires specific information about a suspected site, one can manually check the details by entering the corresponding URL. A good example is *PhishTank* <[www.phishtank.com](http://www.phishtank.com)>—a collaborative clearinghouse for information about phishing that provides a free service for verifying suspected phishing sites as shown in Fig. 38. As per statistics as of September 19, 2010, PhishTank had verified 591,862 phishes as valid out of a total of 1,021,375 submissions received [42].

**10.1.2.3 Anti-Spoofing Measures.** *SpoofStick* is another free browser extension that works well with Internet Explorer and prominently displays the most relevant part of the domain name, thus making the process of manually detecting a spoofed Web site easy. The example in Fig. 39 shows a fabricated URL deliberately made lengthy to obfuscate the real domain name [http://www.customer\\_service.trusted.secure.server.bestandmostsecureonlinebankinamerica.myfavoritebank.com.berghel.com/home.php](http://www.customer_service.trusted.secure.server.bestandmostsecureonlinebankinamerica.myfavoritebank.com.berghel.com/home.php) and using a number of words that

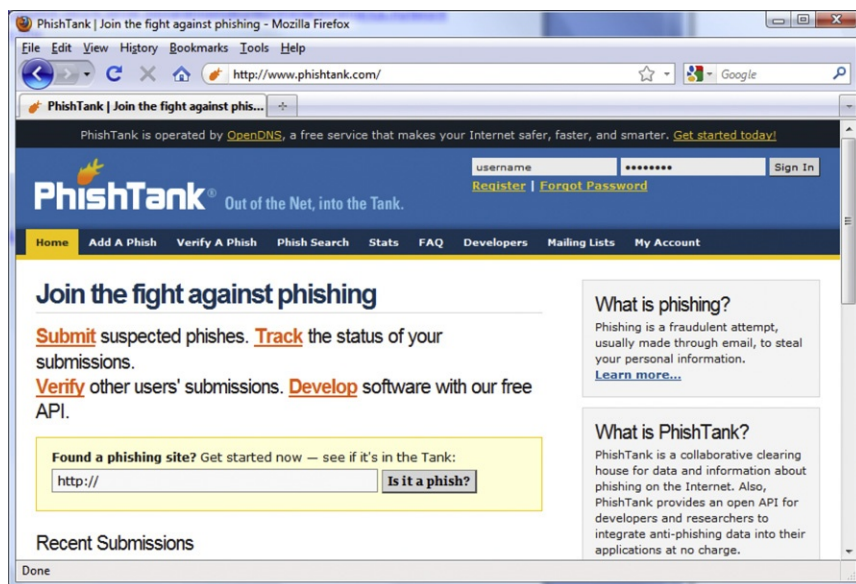


FIG. 38. A free service for verifying suspected phishing sites.

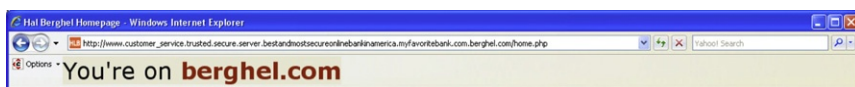


FIG. 39. SpoofStick in action.

make it look like a genuine, trusted and secure customer service site of a standard bank to an unsuspecting Internet user. However, the SpoofStick add-on gives a very prominent visual indication of the actual domain [www.berghel.com](http://www.berghel.com) which is certainly not that of a bank.

*Iconix* [www.iconix.com](http://www.iconix.com) offers a professional service that visually identifies messages from over 1500 senders—one can instantly recognize who the message is from and whether it is been verified as coming from the claimed sender or not [43]. They support most major web-based e-mail providers such as Gmail, Yahoo, Hotmail, AOL, etc., as well as POP3 e-mail clients like MS Outlook. Figure 40 shows a screenshot where verified messages are identified by an Iconix Truemark icon.

**10.1.2.4 Trust indicators.** As mentioned earlier, trust is different from encryption, and a malicious Web site can legitimately display the SSL lock icon if it uses encryption. A very popular add-on for indicating the trustworthiness of Web sites is the WOT (Web of Trust) add-on that relies on community feedback to rate Web sites on aspects such as trustworthiness, vendor reliability, privacy, and child safety. The rating scale has five grades: very poor, poor, unsatisfactory, good, and excellent, and these are available as visual indicators with five distinct colors ranging from red (very poor) to green (excellent) as shown in Fig. 41. Figure 42 shows a screenshot displaying WOT in action.

*URLVoid* [www.Urlvoid.com](http://www.Urlvoid.com), started in May 2010, offers a free service to facilitate detection of malicious Web sites by giving users the ability to scan any URL with multiple scanning engines such as Google Diagnostic, McAfee SiteAdvisor, Norton SafeWeb, and MyWOT simultaneously.

In-built trust indicators in browsers should act as the first line of defense. Table IV gives a summary of the visual indicators used by Firefox for Web site identification along with their interpretation.

The vast majority of the Web sites will display the “no identity information” icon (Fig. 43) as most Web sites do not deal with sensitive information exchange and hence do not require the additional safety offered by HTTPS. It is perfectly safe to visit these sites as long as you are not entering any sensitive information.

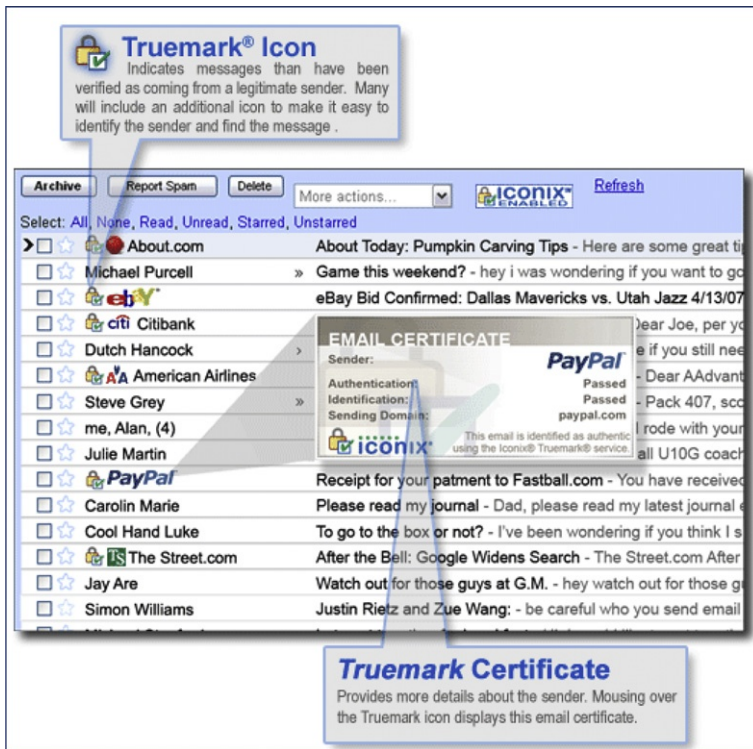


FIG. 40. Iconix in action. Source: <http://www.iconix.com/index.php>.

#### 10.1.2.5 Financial Transactions.

- Use virtual credit cards that are generated online for one-time use to limit the extent of damage even if the card details are compromised.
- Keep one credit card exclusively for online use with a small credit limit and monitor that account vigorously.
- Use virtual keyboards if possible to enter passwords for sensitive Web sites such as online trading and brokerage accounts as this is a good defense against keyloggers.
- Remember that while SSL is reasonably safe, nothing is foolproof as Man-In-The-Middle (MITM) attacks have been demonstrated to compromise even SSL connections [44–47].

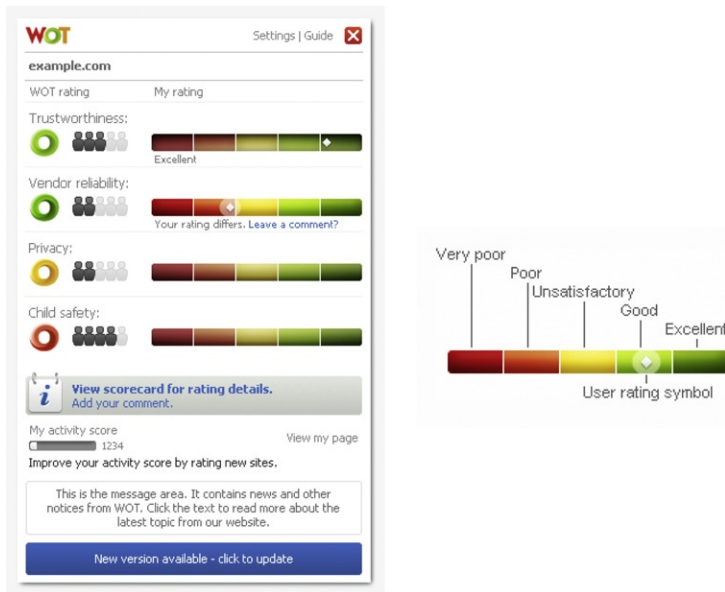


FIG. 41. Visual indicators used in WOT. Source: <http://www.mywot.com>.

#### 10.1.2.6 General Precautions.

- Phishing e-mails generally evoke either a sense of urgency or a certain amount of fear of consequence to elicit people to submit their sensitive information. These scams can also take the form of IRS scams, fake traffic ticket scams, fake Jury summons, 4-1-9 Nigerian scams, or lottery scams involving trans-national money transfer.
- When you get e-mails asking you to go to some site for entering information, do not click on the link, type the URL instead.
- Follow safe password formulation guidelines.
- Do not reuse passwords.
- Copy machines store images of all documents—be careful of using public machines for making copies of highly sensitive data.
- Wipe hard disks before disposing off old computers.
- Remember that FTP and telnet sessions are inherently insecure and transmit passwords in clear-text.
- Be careful about the information you provide on online social networking sites such as Facebook, LinkedIn, MySpace, and Twitter.

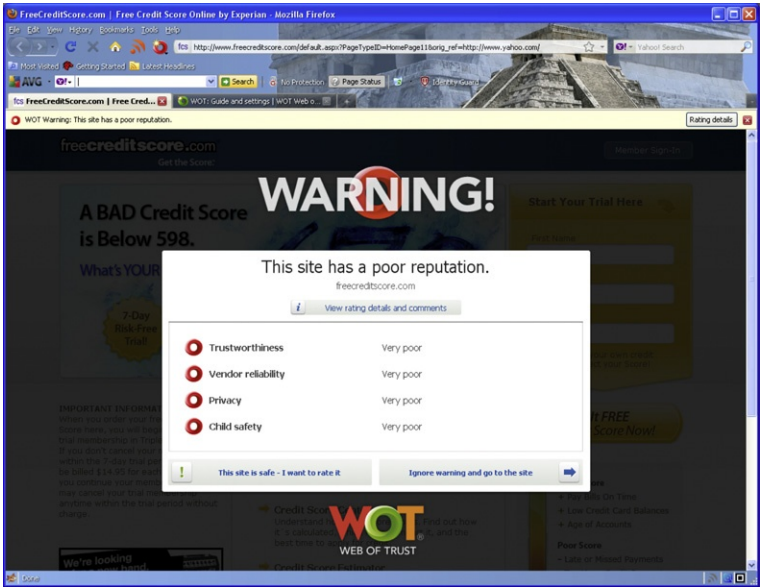


FIG. 42. A screenshot displaying WOT in action.

TABLE IV  
VISUAL INDICATORS USED BY FIREFOX FOR SITE IDENTIFICATION

Icon Used					
Significance	Reported attack site	Invalid or self-signed Certificate	No Identity information	Domain Validation Certificate	Extended Validation Certificate
Interpretation	Dangerous	Be Cautious	Neutral – without SSL	Safe – with SSL support	Highest level of safety
Example	Figure 32	Figure 17	Figure 43	Figure 22	Figure 13
Safety Level					

- Use virtualization—Using the freely available VMware Player along with the VMware Browser Appliance will add an additional layer of security and even if malware attacks compromise the OS of the Browser Appliance, the native operating system will remain insulated. Figure 44 shows a VMware Browser Appliance running on Ubuntu as the virtual operating system and Windows XP as the native operating system.





FIG. 43. Visual indicators while accessing a neutral Web site over HTTP in Firefox v 3.6.3.

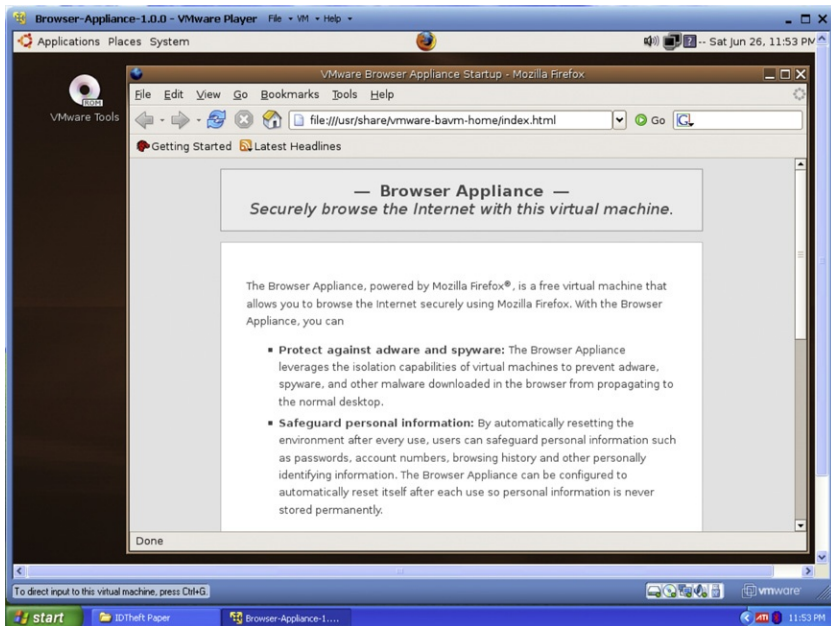


FIG. 44. VMware Browser Appliance with Windows XP as the native operating system.

## 10.2 Remediation

- The FACT (Fair and Accurate Credit transactions) Act of 2003 which amended the Fair Credit Reporting Act allows individuals to put a fraud alert on their credit reports—Call any of the three major credit reporting bureaus—Equifax, Experian, and TransUnion and ask them to place a fraud alert on your file so that no new credit line is opened in your name without an explicit confirmation from you [48].
- Lodge a complaint with the FTC and use the ID Theft affidavit available on their Web site [49].
- File a police report as that will help expedite the reconciliation of any discrepancies in your credit reports.
- Close all the tainted accounts with immediate effect.
- Make full use of state-sponsored programs to support victims of identity theft such as Ohio's *Identity Theft Verification Passport Program* [50].
- If the identity theft was a result of a cybercrime [9], then also file an online complaint with the Internet Crime Complaint Center (IC3)—a partnership between the FBI and other agencies—at [www.ic3.gov](http://www.ic3.gov).

## 11. Conclusion

The fight against identity theft is an ongoing battle wherein the key to victory lies in inculcating a professional attitude with an enduring persistence to guard your sensitive information from being compromised. In the unfortunate eventuality where actions beyond your control have resulted in an information breach, it is imperative to proactively pursue all legal remedies as outlined in the preceding sections and limit the damage to yourself and claim back your life. Further, the inherently dynamic nature of the Internet results in generation of new exploits almost on a daily basis and the only way to fully protect oneself is by aggressively monitoring emerging threats and taking timely countermeasures. The need to have a defense-in-depth approach toward online security and make optimum use of the strategies and tools mentioned in this chapter to stay one step ahead of the bad guys can thus hardly be overemphasized.

## REFERENCES

- [1] <http://www.irs.gov/newsroom/article/0,,id=217794,00.html> (accessed 28.11.2010).
- [2] Department of Homeland Security report titled, 'Identity and Security: Moving Beyond the 9/11 Staff Report on Identity Document Security'. <http://www.homelandsecurity.org/journal/Default.aspx?oid=153&ocat=1> (accessed 28.11.2010).



- [3] Testimony of Chris Jay Hoofnagle during the Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves at the U.S. House of Representatives. <http://epic.org/privacy/ssn/ssntestimony9.19.02.html> (accessed 28.11.2010).
- [4] Three held in Times Square probe face immigration charges. <http://www.cnn.com/2010/CRIME/05/14/times.square.investigation/index.html?iref=allsearch> (accessed 28.11.2010).
- [5] Security Brief: To track terrorists follow the money—if you can. <http://news.blogs.cnn.com/2010/05/14/security-brief-to-track-terrorists-follow-the-money-if-you-can/> (accessed 28.11.2010).
- [6] ID thief to the stars tells all. <http://www.msnbc.msn.com/id/5763781/> (accessed 28.11.2010).
- [7] 250,000 White House Staffers, Visitors Affected by National Archives Data Breach. <http://www.wired.com/threatlevel/2010/01/national-archives-data-breach/> (accessed 28.11.2010).
- [8] Apple's Worst Security Breach: 114, 000 iPad Owners Exposed. <http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed> (accessed 28.11.2010).
- [9] Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, August 2009, ICN 463270. <http://www.ssa.gov/pubs/10064.html> (accessed 28.11.2010).
- [10] 2010 Identity Fraud Survey Report: Consumer Version, Javelin Strategy & Research.
- [11] Federal Trade Commission's 2006 Identity Theft Survey Report.
- [12] [www.itffroc.org](http://www.itffroc.org) (accessed 28.11.2010).
- [13] <http://www.privacyrights.org/data-breach#CP> (accessed 28.11.2010).
- [14] Hal Berghel, Ph.D., Identity Theft and Financial Fraud for the New Millennium.
- [15] [http://cardcops.com/press/nbc\\_dateline\\_20070327.htm](http://cardcops.com/press/nbc_dateline_20070327.htm) (accessed 28.11.2010).
- [16] Hal Berghel and Bob Aalberts, Identity Theft FAQs. <http://www.itffroc.org/faqs/index.php> (accessed 28.11.2010).
- [17] <http://www.ncsl.org/default.aspx?tabid=13489> (accessed 28.11.2010).
- [18] <http://www.idtheft.gov/> (accessed 28.11.2010).
- [19] The President's Identity Theft Task Force Report, September 2008.
- [20] Hal Berghel, Ph.D., Fungible Credentials and 'Next Generation Fraud'.
- [21] <http://www.microsoft.com/protect/yourself/phishing/faq.mspx> (accessed 28.11.2010).
- [22] <http://www.antiphishing.org/> (accessed 28.11.2010).
- [23] Global Phishing Survey: Trends and Domain Name Use 2H2009, APWG, May 2010.
- [24] Phishing Activity Trends Report, 4th Quarter/2009, APWG, p. 2.
- [25] <http://www.antiphishing.org/crimeware.html> (accessed 28.11.2010).
- [26] <http://www.ietf.org/rfc/rfc5280.txt> (accessed 28.11.2010).
- [27] <http://www.verisign.com/support/advisories/authenticocodefraud.html> (accessed 28.11.2010).
- [28] Eileen Zishuang Ye, Yougu Yuan, Sean Smith, Web Spoofing Revisited: SSL and Beyond, p. 7, Section 4.6.
- [29] <http://www.creditcards.com/glossary/term-dump.php> (accessed 28.11.2010).
- [30] <http://www.goldendump.com/> (accessed 28.11.2010).
- [31] Black Market in Stolen Credit Card Data Thrives on Internet. [http://www.nytimes.com/2005/06/21/technology/21data.html?#59;partner=rssuserland&38=&\\_r=1&en=c06809a02406a9f8&ex=1277006400;ei=5090;emc=rss&pagewanted=print](http://www.nytimes.com/2005/06/21/technology/21data.html?#59;partner=rssuserland&38=&_r=1&en=c06809a02406a9f8&ex=1277006400;ei=5090;emc=rss&pagewanted=print) (accessed 28.11.2010).
- [32] RSA Online Fraud Report, Prices of Goods and Services offered in the Cybercriminal Underground, August 2010, p. 3.
- [33] <http://www.topix.com/forum/my/kuala-lumpur/TGVDR9ASS6C8BNDNT> (accessed 28.11.2010).
- [34] Women share same SSN. <http://www.cnn.com/video/#/video/us/2010/06/24/dnt.women.same.ss.number.KARE.WNYT?hpt=T2> (accessed 25.06.2010).
- [35] Identity Theft: Blank licenses stolen from DMV. [http://www.reviewjournal.com/lvrj\\_home/2005/Mar-08-Tue-2005/news/26018927.html](http://www.reviewjournal.com/lvrj_home/2005/Mar-08-Tue-2005/news/26018927.html) (accessed 28.11.2010).

- [36] Teens can get fake IDs in a few keystrokes on Web. <http://www.csmonitor.com/2001/0829/p1s4-ussc.html/%28page%29/2> (accessed 28.11.2010).
- [37] Identity-theft victim meets her identity thief. [http://seattletimes.nwsourc.com/html/business/technology/2009818847\\_idtheft07m.html](http://seattletimes.nwsourc.com/html/business/technology/2009818847_idtheft07m.html) (accessed 28.11.2010).
- [38] Bernanke Victimized by Identity Fraud Ring, Newsweek. <http://www.newsweek.com/2009/08/24/bernanke-victimized-by-identity-fraud-ring.html> (accessed 28.11.2010).
- [39] Federal Reserve Chairman Hit by High-Tech Pickpocket Ring, Wired.com. <http://www.wired.com/threatlevel/2009/08/cannon-to-the-wiz/> (accessed 28.11.2010).
- [40] LifeLock fined \$12 million over lack of life-locking ability. <http://arstechnica.com/tech-policy/news/2010/03/lifelock-cant-guarantee-id-theft-prevention-after-all-settles-with-ftc.ars> (accessed 28.11.2010).
- [41] FTC Says Scammers Stole Millions, Using Virtual Companies. [http://news.yahoo.com/s/pcworld/20100628/tc\\_pcworld/ftcsaysscammersstolemillionsusingvirtualcompanies](http://news.yahoo.com/s/pcworld/20100628/tc_pcworld/ftcsaysscammersstolemillionsusingvirtualcompanies) (accessed 28.11.2010).
- [42] <http://www.phishtank.com/stats.php> (accessed 28.11.2010).
- [43] <http://www.iconix.com/index.php> (accessed 28.11.2010).
- [44] New Tricks For Defeating SSL In Practice, Moxie Marlinspike. <http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf> (accessed 28.11.2010).
- [45] Researcher Hacks Twittter Using SSL Vulnerability, Brian Prince. <http://www.eweek.com/c/a/Security/Researcher-Demonstrates-SSL-Vulnerability-on-Twitter-291904/> (accessed 28.11.2010).
- [46] Renegotiating TLS, Marsh Ray, Steve Dispensa, PhoneFactor, Inc. [http://extendedsubset.com/Renegotiating\\_TLS.pdf](http://extendedsubset.com/Renegotiating_TLS.pdf) (accessed 28.11.2010).
- [47] Hackers Forge SSL Certificate, Anastasia Tubanos. [http://www.thewhir.com/web-hosting-news/123008\\_Hackers\\_Forge\\_SSL\\_Certificate](http://www.thewhir.com/web-hosting-news/123008_Hackers_Forge_SSL_Certificate) (accessed 28.11.2010).
- [48] <http://www.onguardonline.gov/topics/identity-theft.aspx> (accessed 28.11.2010).
- [49] Filing a complaint with the FTC. <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html> (accessed 28.11.2010).
- [50] <http://www.ohioattorneygeneral.gov/About/FAQ/Identity-Theft-Passport-FAQs> (accessed 28.11.2010).

#### ABOUT THE AUTHOR

**Hal Berghel** is currently professor and director of the School of Informatics and associate dean of the Howard R. Hughes College of Engineering, and professor and past director of the School of Computer Science, all at the University of Nevada, Las Vegas. He is also founding director of the Center for Cybersecurity Research, and the founding co-director of the Identity Theft and Financial Fraud Research and Operations Center ([www.itffroc.org](http://www.itffroc.org) (accessed 28.11.2010)). Berghel has held a variety of research and administrative positions in industry and academia during his 30-year career in computing. His current research focuses on computing and network security, digital forensics, and digital crime. Berghel is a fellow of both the Institute for Electrical and Electronics Engineers and the association for Computing Machinery, and serves as an ACM Distinguished Lecturer and an IEEE Distinguished Visitor. He holds a Ph.D. from the University of Nebraska–Lincoln.

**Dennis Cobb** is retired from the Las Vegas Metropolitan Police Department Deputy Chief and now president of DCC Group, Inc. assisting public and private organizations with critical communications technology, processes, and capabilities. Dennis is a founding co-director in the UNLV/LVMPD Identity Theft and Financial Fraud Research and Operations Center. Dennis served as Nevada's Interoperable Communications Coordinator and chaired Nevada's Communications Steering Committee, and as a

member of USDHS SAFECOM Emergency Response Council. He assisted in developing the U.S. National Emergency Communications Plan and assists with radio interoperability issues in National Institute of Justice Technology Working Groups. Dennis Cobb holds a BA in political science and MS in crisis and emergency management from the University of Nevada, Las Vegas. He is a graduate of the FBI National Academy, a 1992 Fulbright Fellow, and 1994 White House Fellow.

**Amit Grover** has 14 years of experience in information technology and has played an instrumental role in the development, implementation and commissioning of a wide variety of defense-related IT applications. He has had the opportunity of designing and implementing INFOSEC policies in military units and has worked on interfacing information systems on board warships, submarines and UAVs (Unmanned Aerial Vehicles). Amit holds a Master of Science degree in Computer and Information Science from East Tennessee State University and a Bachelor's degree in Mechanical Engineering. Presently, he is the Project Manager of the Identity Theft and Financial Fraud Research and Operations Center at Las Vegas where he contributes to the development of comprehensive secure credentialing systems.