STAYING ONE STEP AHEAD OF BUSINESS IDENTITY THEFT AND CYBERINTRUSION

The future of fraud for businesses, the government, and examiners alike to watch for entails the increased incidence of identity theft. Delve into ways identity theft can be effected both internally and externally to businesses and government entities, the identity information you project as an examiner, information others project that can be useful during an investigation, and how to mitigate the risk and recover from identity fraud. This session is designed for both private and public entities and individual CFEs.

LISELI PENNINGS, CFE
Training Director
Association of Certified Fraud Examiners

Liseli Pennings is the Training Director for the ACFE. She was a Special Agent with the U.S. Treasury Inspector General’s Office for Tax Administration and was previously a career special agent with the State Department’s Diplomatic Security Service. She is a subject matter expert in international investigations and physical security, and was a law enforcement attaché in both Europe and Latin America.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, republished, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
STAYING ONE STEP AHEAD OF BUSINESS IDENTITY THEFT AND CYBERINTRUSION

Identity theft is touted as the fastest growing crime that yields a new victim every two seconds\(^1\) and costs businesses millions of dollars a year. The impact of business identity theft is seen and felt by companies and governments alike, and continues to grow as information is increasingly harnessed for legitimate marketing purposes and illicit purposes as well. Business identity theft is perpetrated by employees that engage in practices that place the company at risk and or through various methods of cyberintrusion, aimed at seizing on a company’s vulnerability, the victim of which is oftentimes an unknowing employee.

**Business Identity Theft: What Is It?**
Business identity theft is a type of identity theft whereby fraudsters use varying tactics to obtain sensitive business information and or take over aspects of a business. Business identity theft and cyberintrusion are interconnected as the methodology employed by identity thieves to gain access to a business’ information is through a cyberintrusion vector.

**Internal Threats That Impact Businesses and Agencies**
Identity thieves often target employees with decision-making and signing power to obtain business information. Schemes are tailored to target employees that can mistakenly provide access to data and information coveted by an identity thief. Businesses often fall victim to business identity theft and cyberintrusion through both weak internal policies and the actions of employees.

How an employee handles information security, how strong their passphrases are, how they connect to devices and Wi-Fi, and how well they are trained to detect and respond to

---

social engineering prods, can determine whether a business falls victim to cyberintrusion or to business identity theft. Knowing the way individuals are targeted is essential for businesses to proactively protect themselves against business identity theft and cyberintrusion.

Companies are impacted by the compromise and loss of sensitive consumer information through various methods deemed internal threats to the company. One of the most basic yet most impacting threats is the way passwords are used, stored, and disclosed. This, along with the improper handling of consumer and/or employee information is the most common way that sensitive information is compromised internally. When information is not compartmentalized and/or employees do not have restricted access to varying parts of information for which they have a need to know, information is quickly compromised.

Post-incident reviews of the corporations that fell victim to cyberintrusion in the past two years revealed that several corporations lacked segregation of information access. Hence, the compromise of a low-end user account could result in access to the most sensitive files and corporate passwords since the separation of files and information was non-existent or significantly lacking.

In addition, the role that employees play in clicking on advertising and pop-ups, and downloading executable files, highlights the role individuals can innocently play in the introduction of malicious code and information compromise.

Additional vulnerabilities that rely heavily on internal employees is the risk of lost or stolen company devices as well as the use of public, unsecured, equipment such as the use of public printers for printing sensitive business data.
The information trail left behind on the hard drives of printers, copiers, and scanners, leave a permanent record of all documents that were scanned and or printed. These documents can include a company’s intellectual property and other such sensitive information, which can be downloaded using special software that is available free or for purchase. The documents and data that were copied or printed can be reproduced and memorialized for fraudsters to use, and can have a significant impact on the employer, be it a company or government agency.

**External Threats That Impact Businesses and Agencies**

Externally, business are impacted by fraudsters that utilize various forms of cyberintrusion techniques such as social engineering, introduction of malware, free Wi-Fi and digital device charging stations. The way company employees conduct themselves in the digital world whether in or out of the office, can affect the effect of an attempted cyberintrusion on a company.

Highly sophisticated attempts to infiltrate a company’s system are closely linked to both external and internal threats posed by the actions of employees. Lost or stolen company devices can render a company vulnerable to cyberintrusion if a fraudster is able to access the device. The use of unsecure Wi-Fi by employees utilizing company devices outside of the office makes electronic devices easily accessible by hackers, who establish free Wi-Fi as a means trough which to view the actions of individuals online.

This is another tactic through which external players attempt to gain access to sensitive business information.
What You Project On the Internet
In order for a business identity thief or a cyber-intruder to engage in social engineering, they must know about their prospective victims, or target company’s employees. What a better way to learn about an individual than to find out about their interests, areas of expertise, and what fuels them, than by looking online through social media.

Knowing the information that both your employees and your business project online is essential in determining what the public can access as well as the ease with which that information might be acquirable. The list below is comprised of websites and tools utilized to see what the public can see about your organization or business through various social media platforms and other sites that compile publicly available information.

**Social Media User Search**
- [http://websta.me/search](http://websta.me/search)—Searches for Instagram users, hashtags
- [https://tagboard.com](https://tagboard.com)—Uses hashtags to search for and collect public social

**Social Media Content Search**
- [www.IceRocket.com](http://www.IceRocket.com)—Searches Twitter, FB, blogs, and images
- [www.Bing.com/social](http://www.Bing.com/social)—Searches FB and Twitter feeds
- [www.WhosTalkin.com](http://www.WhosTalkin.com)—Searches 60 social media gateways
- [www.SocialMention.com](http://www.SocialMention.com)—Real-time analysis of what’s discussed on web
- [www.Addict-o-matic.com](http://www.Addict-o-matic.com)—Latest information and trends on topics
- [www.Spokeo.com](http://www.Spokeo.com)—Search by email address, number, username
Business Identity Theft Schemes

It is easy to search for businesses online using numerous online company registries that disclose public information on businesses worldwide. Online registries provide information such as the name of a company, names of the owner and registered agent, the company’s electronic address and mailing address, names of directors, the type of business and the products and service in which the company deals. Other information is available publicly and online such as where the company is located, their company logo, and even organizational charts and contractors with whom companies do business. This information can be very valuable for fraudsters.

There are many business identity theft schemes, one of the most common of which involves the manipulation of the business’ registration information and or manipulation of the business’ filing process. Fraudsters can either hack into an online account and re-register a company to a different owner or address or they can file physical documents changing important aspects of the business’ registration information such as the name of the owner, registered agent, or the business’ address. This is the most common modus operandi in business identity theft. Some online business registries allow for online submission of changes of information, making this fraud scheme even easier to commit for identity thieves.
Some company registration sites do not verify document validity when business information such as names of directors or owners are changed. In addition, some business registries do not notify business owners if business registration information for their business has been changed, making this type of fraud harder to detect.

One business identity fraud scheme involves identity thieves ordering merchandise on company credit and having items delivered to an address unrelated to the target business. Good are delivered to the address operated by the fraudster and the target company is left owing money for goods it did not order and did not receive, oftentimes ruining the company’s credit. The vendor company is also impacted as it is left with a loss of both revenue and inventory.

The fraudster can also initiate the fraudulent sale of the company and or the company’s assets and profit from the sale. Through registration manipulation, the company’s information is fraudulently utilized by the business identity thief in order to obtain loans in the business’ name, benefitting the fraudster.

Another business identity theft scheme entails leasing an office space in a multi-unit building that houses the target company. Called physical address mirroring, this type of business identity theft entails the thieves applying for credit and purchasing products in the target company’s name, which are delivered to a similar physical address in the same building that varies by a letter or number. ²

Reinstating a dissolved or closed business and making purchases on behalf of the closed company is yet another business identity theft scheme called business reinstatement fraud. After a company is dissolved, previous owners rarely monitor the business’ registration records. Owners of the dissolved company typically do not realize this is happening until they receive notices from creditors that they owe money for items purchased on behalf of the dissolved company.

Another scheme used by business identity thieves involves creating a business with a name that is similar to the target company. The tactic utilized by identity thieves in this scheme, relies on vendors to not notice or verify the slight discrepancies in the company’s name and associated information.

Utilizing stolen credit card information to order merchandise from a company is another scheme that is a form of identity theft impacting businesses worldwide. One way fraudsters conduct this type of scheme entails going through a business’ trash and recycling bins for account numbers and other sensitive data. This scheme highlights the importance of companies exercising proper information security, namely the disposal of sensitive information.

Social Engineering is one of the most common schemes utilized to trick employees of a target business into believing there is a threat or that the social engineer is trying to “help” the target employee. Through use of psychological tactics that instill a sense of trust in the company’s employee, an identity thief can gain access to accounts, information, and other sensitive information.
The Role of Social Engineering in Business Identity Theft

Criminals employ various media to establish rapport with the victim, gain their trust, and or frighten them. The most common type of social engineering tactic is termed “phishing”, which is when a criminal seeks to obtain personal and sensitive information by stressing a sense of urgency and playing on the victim’s fear.

Fraudsters typically target employees within the target business that have decision-making and signing authority. Knowing how a business functions and where an employee falls within the business’ organizational chart, helps the perpetrators tailor a scheme that looks and sounds legitimate to the target employee.

Criminals sometimes utilize e-mails, when perpetrating social engineering scams. This type of scam directs the victim to a website that appears legitimate. The prospective victim is then instructed to enter their log-on and password and other such sensitive business account information. Sometimes the sites provided are loaded with malware, so the victim is not only tricked into supplying sensitive information but in addition, malware infiltrates their computer and also steals other sensitive business information.

Another common form of social engineering is called “pretexting” which entails a fabricated scenario/pretext that the criminal uses to “confirm the victim’s identity”. This tactic relies on the criminal instilling a false sense of trust as the scenario frequently involves the criminal pretending to “help” the victim. One example of this is a thief purporting to be calling from a bank to inform the victim that their bank account has been hacked. The thief wants to help the victim and asks for the business’ bank account information.
number and pin via phone to freeze the account to prevent further fraud.

“Baiting” is another form of social engineering that entices a victim with a prize or free goods either by offering free media or downloads that contains hidden malware, located on a clickable link. The victim employee is instructed to click on the link provided to obtain the free prize and the link is riddles with viruses. Another version of baiting involves a websites requiring business identification information to be input such as a password or business account numbers before the user is able to proceed.

Being vigilant as an individual and a company requires staying current on evolving fraud scams and patterns. Company employees should be informed to never place any identifying information on emails or texts, be it an account number, password, date of birth, or other sensitive information. Some common fraud schemes have preyed on employees through use of counterfeit emails that appear legitimate and claim to have been sent by the business’ financial institution asking for verification following a fraud alert. Employees are then asked to enter passwords and business bank account information on an e-mail or via text. This type of information should never be provided on any mode of online communication. The best practice is to directly contact the company’s financial institution at the number the company possess or that is listed on the company’s credit card, not a number provided by the caller or e-mail sender. Business policy should include corroboration by employees when financial institutions or other companies contact the business to request sensitive information. These types of scams, called phishing scams, attempt to acquire information from users via misleading and fraudulent email or phone communications. Scams
perpetrated via telephone that entail voice interaction with the victim are termed “vishing.”

One current common scam, termed the “CEO email scam,” entails market research conducted by fraudsters on companies to determine vendors that engage with business with certain companies. The fraudster also conducts research to obtain an organizational chart on the business which includes names and e-mails of employees in certain departments such as the accounting department and other decision-makers such as the CEO. Much of this information is posted online by companies and government agencies or can be inferred through professional social media platforms such as LinkedIn. The fraudster spoofs an email address that appears to hail from a high-level person within the company. By finding the email address of company employees, an identity thief can spoof or create a similar email address that fits the business’ email address pattern. The e-mail address usually contains one extra letter or number. The fraudster then emails an employee from the accounting department or another targeted department and instructs the employee to wire-transfer a certain amount of money owed to a vendor for services or a product. According to the Federal Bureau of Investigation (FBI), this type of scam has impacted over 7,000 companies with financial losses estimated to be over $2.3 billion and victim businesses spanning over 79 countries.

**Staying One Step Ahead of Business Identity Theft and Cyberintrusion**

*Emphasize Information Security*

The most important step in protecting the compromise of information is to train employees how to protect information and to have policies in effect that establish protocols on how information is handled.
Compartmentalization

Information and data should be separated and classified, or compartmentalized, based on its sensitivity, use and function. Social Identification Numbers and other biodata only needs to be accessed by individuals that need that information for the conduction of business. By utilizing a classification system to determine varying levels of sensitivity for information such as “sensitive”, “confidential”, and “secret”, is the first step in streamlining what information needs to be accessed and by whom, thus limiting the breachability of sensitive business information.

Authenticating that employees have the correct password and or clearance to obtain varying levels of information is imperative to restricting access to information. This can be done through various forms of authentication such as passwords, restricted access to servers, encryption codes, and other biometric print devices that confirm identity to filter access.

Fragmentation of Data Storage

Separating and storing data in varying locations whether on servers or on cloud storage platforms, can protect data by adding layers of protection and separation in the event of a breach. Qubing and sandboxing, forms of storage fragmentation, can make it harder for hackers to obtain all of a company’s information in one fail swoop by having information stored in different locations. The separation of information storage can help prevent a hacker from obtaining all of a business’s information by having to follow different paths in order to obtain information.

Physical information that contains sensitive biodata should be stored in locked containers or locked rooms.
with various layers of authentication for access. Information should only be access if there is a legitimate work need for each person and authentication features for access such as a room code or combination and ideally various layers of authentication should be employed to protect client and consumer information.

Use of secure cloud storage to protect customer information is essential to protect client information. There are several companies that offer a variance of secure and encrypted cloud storage options as well as fragmented storage or options for peer to peer access. Similar to the concept of utilizing The Onion Router (TOR) to add layers of security and anonymity to information on the deep web, some cloud storage service companies offer layers of security, which provide added hurdles for hackers to overcome in order to penetrate information storage locations.

Some cloud storage companies that offer various levels of cloud storage are:
- Dropbox—unsecure, not encrypted
- Spider Oak—encrypted
- Made Safe—encrypted, fragmented, peer-to-peer option, in design

Disposal of Data and Scrubbing Software and Hard Drives
Accessing and storing data and information safely is equally as important as how information is disposed of. Shredding documents that contain sensitive business information should be a routine practice. This prevents the possibility that the easy and cost-free tactic of obtaining identity information from trash, called “dumpster diving” will yield anything for identity thieves.
Use of public copy machines and public printers are a risk that many people do not realize exist. Coping and printing documents that contain personal information on public devices is a risk that renders the information easily accessible. When you copy and or print documents, such machines store all of the information that was ever copied or printed on said machine and the data can be accessed from the machine’s hard drive. Accessing this hard drive can allow a fraudster access to all documents that were ever copied or printed on the machine.

The best practice is to avoid printing and copying personal documents at work and at all public locations and instead print and copy work-sensitive documents at the office and personal documents at home.

The risk of utilizing public equipment is not the only practice that renders company vulnerable to identity theft breaches, not scrubbing or clearing data from company equipment that will be disposed of presents an even bigger risk. Many companies and government agencies auction, sell, or donate used machines or swap them out with the vendor for a newer model, not knowing that the data stored on the devices is invaluable. Personally-Identifiable Information (PII), intellectual property information, identity information, IP address of and sometimes even sensitive information such as secure log-ons and passwords can be accessed and comprised on machines that are not disposed of properly or that are not properly wiped prior to being sold, donated, swapped out under a lease, auctioned for sale, or thrown away.

Some copy machine and printer vendors provide scrubbing or wiping services that clear the contents of
the hard drives on the devices. This should be a requisite that is checked with vendor and supplier procedures before engaging in contracts with equipment suppliers. There are also companies and software that can scrub machines and other devices such as computers, tablets, and phones. Most tablets and phones will publish instructions on how to wipe a device, which can be conducted whether the device is in your possession or if it is lost or stolen. Knowledge of these capabilities are essential to include in company policies aimed at protecting information.

One tool that provides information on data wiping is [www.dataerasure.com](http://www.dataerasure.com).

Some downloadable applications and programs geared towards wiping hard drives across various mediums are as follows:

- [www.whitecanyon.com](http://www.whitecanyon.com)
- Parted Magic—can recover and erase data, free that use but charges for the download.
- HDDerase.exe—more complex to use for laymen.
- Western Digital Data Lifeguard
- Hitachi Drive Fitness Test
- Samsung Magician
- Seagate SeaTools
- Media Tools Wipe 1.2
- Eraser 6

A big vulnerability exists when an employee’s company device such as a laptop, tablet, or phone is lost or stolen. In order to avoiding compromises of identity information on said device, the device should be set up prior to use with the option to remotely wipe. Tablet and phone manufacturers varying from Android to IPhone and IPad have instructions on their respective
websites on settings that need to be selected for this option to be usable. The key is to be proactive and set this feature up prior to the device being stolen.

There are also numerous applications and software that also wipe devices remotely or that can installed to wipe computer drives, some of which are free.

A list of a few free applications include:
- HDD Erase
- HDShredder
- KillDisk

### The Role of Multilayer Authentication

Fingerprint scans, retina scans, PINS, voice prints, or an icon associated with your name are ways to implement added layers of biometric authentication for online information and account access. This layering of access and verification is termed multilayer authentication. The most common form of multilayer authentication is two-factor authentication that sends a user a text or e-mail with a passcode that the user must enter to log-on or proceed with an online transaction.

This serves as a second layer of identity verification and requires an identity thief to possess the device and request a change in password. A request to re-set a password if usually sent to the lost or stolen device. When companies experience issues with devices left unsecured or devices are lost or stolen, the two layers might not be enough, especially when the thief possesses the stolen or lost device.

Another form of commonly used online two-factor authentication a security questions, typically asked in threes. The most commonly asked security authentication
questions are: What is your mother’s maiden name? What is the name of your pet? Where did you attend high school? What is the name of your best friend? This information is commonly available online through seemingly innocuous posts by individual employees that are of prime value for identity thieves. Pieces of information can be pieced together by identity thieves to steal identity information and gain access to online accounts. Some online sites allow users to change their passwords online, provided they answer the security questions, which can lead to an easy account takeover opportunity for identity thieves.

Other methods of establishing procedural multilayer authentication can entail company policies requiring employees to take steps to verify companies or vendors with which they do business by logging onto company sites and opening records and electronic files. When receiving a call requesting payment or action, one method of authentication can entail calling the inquiring company, financial institution, or Revenue Agency back on the number provided on your contract, policy card, health insurance card, bank card or official website online as opposed to the number provided by the caller to ensure a request is legitimate before proceeding.

Verifying the email and telephonic communication as well as verifying that a website is secure is a pivotal aspect to deterring identity theft. Several social media platforms offer varying levels of multilayer authentication for businesses by authenticating a company or brand. This is done by social media sites by employing a verification mark such as a badge or a check mark, to authenticate business’ accounts. Verification on social media aims to protect intellectual property, brand credibility, and business identity. Some social media sites require submission of information directly to the company to engage in a
verification process as an attempt to inform the user of the account’s validity to ensure a website or social media post is not a fraudulent site or post created by an identity thief.

It is recommended that companies authenticate and verify company websites, brands, links, and social media platforms, to protect the customer base and the company from fraud and identity theft. One way to ensure that links of sites are corroborated is to ensure that all platforms are linked directly to each other. As an example, you should be able to link a company’s website directly to their social media accounts and any other related third-party sites. This allows less chance for a customer or employee to access a fraudulent site created to defraud users.

**Staying Current on Fraud Scams**

Being vigilant requires companies to stay current on evolving fraud scams and patterns. The following sites are resources that businesses can use to stay proactive of identity theft scams and patterns:

- [www.concierge.comparecards.com](http://www.concierge.comparecards.com)
- [www.antifraudcentre-centreantifraude.ca/index-eng.htm](http://www.antifraudcentre-centreantifraude.ca/index-eng.htm)

**The Importance of Passphrases**

Although the idea seems elementary in principal, the use of strong passwords and routinely changing passwords is instrumental in lowering the risk of being an identity theft victim. In actuality, users should not use passwords but rather longer passphrases to ensure they have a lessened risk for password compromise. Several studies of companies whose information was hacked in 2014 and 2015 revealed that the lack of strong passwords by their company’s employees and the use of generic passwords

---

3 Social Media Law Bulletin, Authentication on Social Media Platforms, [www.socialmedialawbulletin.com](http://www.socialmedialawbulletin.com).
such a Password1234 or Acbd1234, allowed hackers easy access to files and restricted computer information. Employees should not use any identifying information within their password such as their name, place where they reside, birthday, a pet’s name, children’s names, and the like, as this information is made readily available on social media.

### The Importance of Wi-Fi Usage and Virtual Private Networks

The use of unsecured sites and unsecured Wi-Fi can be detrimental to businesses as hackers sometimes create free Wi-Fi sites with the sole purpose of hacking onto computers of those that use the free service. Whatever a user opens and views, the hacker can see, opening the door for identity theft. This cyberintrusion tactic is usually employed at high-traffic, public locations such as airports, hotels, and conference centers. Companies should instill a Wi-Fi policy that stated that employees should not make use of free Wi-Fi with business devices or with personal devices used for work if the business employs a Bring Your Own Device (BYOD) policy. Secure, public Wi-Fi sites should require a password to logon and the user should employ an encryption system in conjunction with public Wi-Fi use such as a Virtual Private Network (VPN), which provides added security.

In addition, various methods exist for encoding data so that only computers with the right decoders can read messages and information. Encryption exists to provide varying templates of security for different uses. Symmetric-key encryption allows all users within a pre-designated group or company to use the same key to encrypt and decrypt a message. Another form of encryption called public-key

---

encryption allows each separate user to encrypt a message and the recipient uses the public key that corresponds to the message to decrypt the message.

Maintaining and installing the most recently available security patches and updates on both company and personal device, be it a computer or personal tablet or phone, also helps protect business information from vulnerabilities that the updates and patches address. Firewall and anti-virus protection should also be utilized to further protect against cyberintrusion.

**Digital Device Charging Stations**
Businesses can be unknowingly targeted via cyberintrusion through the use of charging stations. Commonly found in airports, train stations, conference centers, and other travel and tourist hubs, charging stations offer travelers an easy way to charge their electronic devices by having a kiosk with charging cables or power strips for individuals to use. Hackers can install hidden USB cables at charging stations, which allows for a mirror image of the device’s screen to be projected on to another screen⁵. This can allow hackers to record everything the user does on their device, from opening sensitive business documents, to looking at a business’ financial statements. This threat can be remedied by having strict company policy on charging devices and training employees to charge their devices with personal charging packs.

**Malware**
Malicious code can sometimes be introduced via advertising sites and pop-ups. Establishing a policy on

---
accessing advertising sites can be a way to be proactive against cyberintrusion. Using software that blocks ads, called “adblock software” can protect businesses and from identity theft.

The Digital Advertising Alliance allows consumers to opt out of advertising applications by allowing users to conveniently opt out from participating companies that collect Web viewing data across unaffiliated sites for IBA and other applicable uses. The website for this option is www.aboutads.info.

There are several sites that offer free adblock software to block advertisement and associated malware.

- [www.adblockplus.org](http://www.adblockplus.org)
- [www.adfender.com](http://www.adfender.com)
- [www.getadblock.com](http://www.getadblock.com)
- [http://emma-ad-blocker.findmysoft.com](http://emma-ad-blocker.findmysoft.com)
- [http://ticno-bancut.software.informer.com](http://ticno-bancut.software.informer.com)

### The Importance of Privacy Policies

Most privacy policies come in at over 2,500 words which takes the average person about 10 minutes to read. A summary of interesting points of Facebook’s privacy policy includes aspects of “using your phone’s location for features like checking-in … allowing advertisers to target ads based on users’ locations … know about your device to understand battery signal strength to make sure apps work well … gather connection information such as the name of your Internet Service Provider as well as browser type and language and time zone … collect information about the purchase you make on games such as your credit card number and other account and authentication information.

---

6 University of Texas at Austin Center for Identity, Facebook’s New Privacy Policy, [https://identity.utexas.edu](https://identity.utexas.edu).
as well as billing, shipping and contact details.”

Other social media sites monitor and aggregate information similarly. Knowing what companies do with your personal information is very important.

An excellent tool created by the University of Texas at Austin Center for Identity is an application called PrivacyCheck. This free application is available on Google’s search engine. You select the application and click “start” when navigating to a privacy policy on a website. PrivacyCheck will read that website’s privacy policy and review how your personal data is handled by the company to include your email address, credit cards information, and other identifying information and to whom that information is made available and its dissemination. PrivacyCheck then provides the user with a summary and a privacy rating indicating the level of risk associated with using that website from an identity protection perspective.

In summary, in order for businesses to be proactive against identity theft, they must first understand the vulnerabilities internal and external to their company, which usually involves their employees being targeted on some front. Understanding how individuals, their employees, can be targeted is essential to combatting identity theft.

**How to Be Proactive Against Business Identity Theft and Cyberintrusion**

- Enact strict companies policies and training on:
  - Information security Social media use
  - Identity theft

---

7 Facebook, Privacy Policy, [www.Facebook.com](http://www.Facebook.com).
8 University of Texas at Austin Center for Identity, Privacy Check With Google Chrome, [https://identity.utexas.edu](https://identity.utexas.edu).
| Train employees to recognize social engineering methodology |
| Ensure employees corroborate requests for information (both internal and external) |
| Fragment data storage |
| Compartmentalize information |
| Train employees on proper passphrase use |
| Train employees on the dangers of free Wi-Fi use and charging station use (should be part of social media policy as well). |
| Train employees on information security to include wiping devices and shredding data (should be part of information security policy as well) |
| Utilize multilayer authentication for information access |
| Stay current on fraud trends |
| Utilize ad blockers to prevent introduction of malicious code |
| Ensure employees understand and check the privacy policies of websites they frequent |

**NOTES**

**Helpful Websites for Business Identity Theft Investigations**

*International Search Engines*
- [www.searchenginecolossus.com](http://www.searchenginecolossus.com)

*Internet Domain and Registration Information*
- [www.Domaintools.com](http://www.Domaintools.com)
- [www.whoisdomaintools.com](http://www.whoisdomaintools.com)
- [www.internetfrog.com](http://www.internetfrog.com)
- [www.arin.net](http://www.arin.net)
- [www.whois.net](http://www.whois.net)

*Tracing IP Addresses*
- [www.whatismyipaddress.com](http://www.whatismyipaddress.com)
- [www.whoismyip.com](http://www.whoismyip.com)
<table>
<thead>
<tr>
<th>Financial Information, Asses, and Public Records Resources</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.traceroute.org">www.traceroute.org</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate Records</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.Kompass.com">www.Kompass.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.SkyMinder.com%E2%80%94Shareholders">www.SkyMinder.com—Shareholders</a>, owners, business structure, banking relationships</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.Bvdinfo.com%E2%80%94Merger">www.Bvdinfo.com—Merger</a> and acquisition data, boards members, financials, ownership</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.dnb.com%E2%80%94Names">www.dnb.com—Names</a> of principals</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.corporateinformation.com">www.corporateinformation.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.opencorporates.com">www.opencorporates.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>