

DISCLAIMER: This information is provided "as is". The author, publishers and marketers of this information disclaim any loss or liability, either directly or indirectly as a consequence of applying the information presented herein, or in regard to the use and application of said information. No guarantee is given, either expressed or implied, in regard to the merchantability, accuracy, or acceptability of the information.

The Dangers of Identity Theft and How to Protect Yourself!



Table of Contents

How Serious Is Identity Theft?

Are You at Risk?

How Can You Tell if YOUR Identity's Been Stolen?

What To Do if You're a Victim of Identity Theft

Who Has the Right to Access Your Information?

What is Being Done to Protect Your Privacy?

What Can You Do to Prevent Identity Theft?

Special Concern: Online Privacy

Learn How to Read a Privacy Policy

Protecting Your Children's Privacy

How Serious Is Identity Theft?

Imagine waking up one morning. You are on your way to an interview for a new job. Maybe you're looking to jump up the corporate ladder or perhaps it's for a second job to help get ahead of the bills. Whatever the case you are optimistic about the day. A friend of yours has given their personal recommendation and you are confident the job is in the bag.

The interview goes well. The interviewer seems pleased with you and you have a good feeling about the offer. While nothing is promised you are more than certain the job is yours as soon as the paperwork is approved.

You finish the interview and stop by the car showroom. It's looking like a good time to finally get that new car you've had your eye on! You've been thinking about it for months. The salesperson takes you for a spin and it's everything you've dreamed of – and more!

Stepping back into the showroom the salesperson suggests you sit down. “Grab a cup of coffee and we'll talk about driving this baby away today!” Sounds good.

Bantering over the paperwork you sit back with a sigh of contentment and put down the pen. “Let's just check your credit and you should be off in a few minutes” he says. Today is a GREAT day!

As you sit back and gaze at the gleaming cars on the showroom floor you notice the salesperson has become rather silent.

“I’m sorry but it looks like this might not work out right now” he says. You look at him and see a sudden sternness in his eyes. “Really,” you say “why’s that?”

“Well, you’ve got a few things on your credit report that are a concern. I’m afraid this car would be impossible to finance.”

“What do you mean? My credit is fine!” you start to sputter “let me see”.

“I’m not allowed to share your report with you, but maybe in a few months you can come back and look again.”

You head out the door in confusion. You KNEW you could get that car. What was he talking about?

As you open the door to your home you see the message light flashing on your phone. That was fast! The job offer – that will put you back in a good mood!

“...I’m afraid we won’t be able to offer you a position with us right now...” you don’t even hear the rest of the message. WHAT??

Ding-dong. The doorbell. Who could that be?

“Hello, I’m Officer Brown, may we have a word with you...”

What Identity Theft Can Do To You

We often take our liberties for granted. What you know life to be can suddenly change if you've been a victim of identity theft.

While you've been busy with your day-to-day life someone could have stolen your personal information and racked up debts or committed fraud – all with your name on it. What happens then can be anything from being denied employment, credit or even being arrested for a crime you didn't commit.

Identity theft is that serious.

Victims of identity theft can spend years paying back debts or fighting to restore their credit as well as their reputation. Finding out you are a victim of identity theft can be frightening and a source of anxiety even after you've resolved the issue.

According to a survey conducted by the FTC (Federal Trade and Commission) 4.6% of Americans involved in the survey responded that they had been a victim of identity theft within the past year. That means about 10 million Americans dealt with some form of identity theft – from using existing credit cards to setting up new accounts or giving false identification when arrested for a crime.

It doesn't stop there. The cost of clearing up the theft ranged from an average of \$500 to \$1200 per victim. It took them on average 30 hours to resolve the issue while also costing time and money for businesses and agencies who assist these victims.

With all the tools available to potential thieves along with our increasing reliance on paperless money transfers (credit cards, debit cards and online payments) we are

incredibly susceptible to having this nightmare come true.

How can you reduce the risk and what do you do if it happens to you or your family?

Are You at Risk?

If you think you've figured out how to keep the thieves out of your personal information you may be surprised at the methods they use to gain access to it. Finding out HOW thieves access your information is the first step in reducing the risk.

Lost or Stolen Wallet

Not surprisingly a person who has had their wallet lost or stolen is at great risk of becoming a victim of identity theft. Carrying important documents like your Social Security Number, birth certificate, driver's license and credit or debit cards in your wallet can give a thief easy access to your personal information.

Missing Mail

If you think you've missed a couple bills or know that your mail box has been broken into, your personal information may have been stolen. Credit card bills, offers for credit cards and information that contains personal information or your SSN can be used to gain access to unauthorized credit or to commit fraud in your name.

Garbage

Thinking of throwing the latest credit card offer in the garbage? Clearing out old tax forms or other personal information? Rummaging through the garbage for such

information is known as ‘dumpster diving’ and can be an easy source for identity thieves. Your personal garbage isn’t the only source – businesses that collect personal information can also be targeted.

‘Phishing’ or ‘Pretexting’

Online or over the phone there are unscrupulous individuals masquerading as legitimate businesses in an attempt to convince you to pass on personal information for illegal purposes. Any requests to ‘validate account information’ by providing personal information online or over the phone should be questioned.

Businesses or Employees

Employees or businesses that have legitimate access to your personal information may use that information for non-business activities. Identity thieves that work in institutions that contain sensitive personal data may abuse the access they have or even present themselves to you as someone that should have access, such as a landlord or employer.

‘Skimming’

Thieves have access to ‘tools of the trade’ that allow them to steal information from your card at ATM’s or during a card swipe for a purchase. These data storing devices capture your information without your realizing it.

Change of Address

By filling out a form at the post office the identity thief can have your bills and other personal mail diverted to a new address. It may take you a few days to realize what has happened and make the correction.

Spyware

A new threat on the scene is from computer viruses that 'spy' on you while you shop or do banking online. Any website that you enter personal information into can be 'spied on' putting you at risk.

Unsecured Online Transactions

Online shopping at a site that is not secured can potentially put you at risk of having your information stolen. Websites may also collect and sell some of your information without your knowledge unless their posted Privacy Policy states otherwise.

Break In

Anytime you or a business that has your information is a victim of a break in you may have had personal information stolen.

Personal Computers

Are you storing sensitive passwords on your laptop? Are you throwing out an old computer? If your laptop is stolen or accessed by a thief they may be able to find that information. Old computers may hold information on their hard drives even when you've deleted it.

How Do You KNOW if Your Identity's Been Stolen?

If you know that your personal information has been accessed or otherwise tampered with there are steps you must take to stop the thieves and try to repair the damage. It is important to stay alert to signs that your information is being used without your consent even when you don't suspect you've been a victim.

Staying alert to these signs will help you respond quickly if your identity has been stolen:

- **Unfamiliar charges or withdrawals**

Always check your bank and credit card statements and make immediate inquiries to unfamiliar charges and withdrawals.

- **Missing mail**

If your bills and other mail have gone missing a thief may have broken into your mail box or had your mail redirected to a new address.

- **Calls from Creditors**

If you are being contacted by creditors you did not do business with you need to take immediate action to find out who has.

- **New Credit Cards**

Receiving new credit cards or bills that you didn't sign for is a danger sign that your identity may have been stolen.

- **Denial of Credit**

Unexplained refusal of credit requires investigation on your part.
You need to get access to your credit report right away.

What To Do if YOU are a Victim of Identity Theft

If the worst has happened and you find out you have indeed been a victim of identity theft (or have reason to suspect it) you must take IMMEDIATE action to control the damage.

Report to the Credit Bureaus

If you are a victim of identity theft you must report it immediately to one of the three major credit bureaus. You only need to call one bureau to place the fraud alert and they will forward the information to the other two. Your SSN will be flagged for 90 days to prevent a thief from trying to obtain new credit with your identification.

If you are certain that your identity has been stolen you can request an extended fraud alert. The extended fraud alert will remain on your report for seven years and will require you to submit an identity theft police report.

Flagging your account will alert potential creditors to take steps to protect you. This will also delay the credit approval process.

The three bureaus are:

- **Equifax:** 1-800-525-6285
www.equifax.com P.O. Box 740241, Atlanta, GA 30374-0241
- **TransUnion:** 1-800-680-7289
www.transunion.com Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- **Experian:** 1-888-EXPERIAN (397-3742)

You will be asked for your SSN and other identifying information through an automated service. The alert will be passed on to the other two bureaus and all three credit bureaus will send you a letter to confirm the fraud alert is in place. You will also be given directions for obtaining your credit report for free from each of the bureaus.

The credit reports will have a telephone number listed on them if you need to contact the bureaus about fraudulent activity listed on the reports.

Get Copies of Your Credit Report

Send for your credit reports following the instructions from the credit bureaus. Review the reports carefully. Look for creditor's names that you did not request credit from. Also check your personal information; SSN, address, name, initials and employer information.

Order your credit report at least every three months for the first year of the fraud. Some areas provide a free report every 12 months. Other areas will give you several free reports for the year you report an identity theft. Some will charge for each report. Tell them you are an identity theft victim and ask for a free report.

File a Police Report

Keep records of the fraudulent activity as proof for your report. Blackout unrelated activity and give copies to the police. Give them any new evidence as it turns up and keep a copy of the report as proof for creditors and the credit bureaus.

Collect Account Information

Contact the creditors who issued accounts to the identity thief. The Police may give you a form to request the information. Send a copy of the police report and the account statements to the creditor. Pass any new information over to the police.

Close the Accounts

For NEW Accounts created by the thief: Call the creditors (including credit cards, department stores and cell phone accounts) and ask for their security or fraud department. Tell them you are an identity theft victim and ask them to close the accounts and report the closing to the credit bureau. If the account has already been used by the thief ask them not to hold you responsible for the debt.

For EXISTING Accounts used fraudulently by a thief: Close the accounts and ask the creditors to report the closing to the credit bureaus. Request that they declare the account “closed at consumer’s request”. If you open a new account don’t use personal information like your mother’s maiden name or your SSN for a password. If those are the only options request to use a different password.

Alert Government Agencies

If your driver’s license or other government ID has been stolen report it to the proper agency to cancel it and order a replacement. Ask that your information be flagged so that no one else can get copies.

Complete an Identity Theft Affidavit

In order to remove the debts created by the identity thief you will need to send an affidavit to the company or creditor holding the debt. When you contact them to close the accounts ask what forms they require. The affidavit permits them to investigate the claim – it does not ensure that the debt will be cleared.

While each business may have its own requirements you can also obtain a free affidavit form at: <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>. Ask the business if they will accept this form or need you to fill out one of theirs.

Send the copies of the affidavit and supporting documents to the businesses (a separate

form should be created for each account or institution responsible for providing the identity thief with credit). Do not send original bank or card statements. Blackout any information on the statements not related to the account.

Send a copy of each affidavit and the police report to the credit bureaus. Write a letter requesting the information you declared was a result of theft be blocked or removed from your credit report.

Report Stolen Mail

If you believe that your mail has been stolen you must contact the nearest Postal Inspector. You can look for the number in your white pages under Government Services, call 1-800-ASK-USPS or search online at <http://www.usps.com/ncsc/locators/find-is.html>.

While the information above is provided for those living in the US the steps are nearly the same in other countries. Here are some links and numbers to credit and police agencies in the UK, Canada and Australia.

Contact Numbers for the UK

If you are a victim of identity theft in the UK use the following contact information;

Credit Bureaus

- Call Credit: 44 (0) 113 244 1555
www.callcredit.co.uk/ Callcredit plc, One Park Lane, Leeds.
West Yorkshire, LS3 1EP.
- Equifax: 0870 010 2091 for the CIFAS Protective Registration Service
www.equifax.co.uk/ Credit File Advice Centre PO Box 1140,
Bradford, BD1 5US
- Experian: 0870 241 6212 (M-F 8-6, Sat 9-1)
www.experian.co.uk/ Experian Ltd, PO Box 9000, Nottingham,
NG80 7WP

Police

File a report at your local Police Station. Locate the closest station at <http://police.uk>.

Contact Numbers for Canada

If you are a victim of identity theft in Canada use the following contact information;

Credit Bureaus

- Trans Union Canada: 1-877-525-3823 (Quebec Residents: 1-877-713-3393)

www.tuc.ca

- Equifax Canada: 1-800-465-7166
www.equifax.ca Equifax Canada Inc. Consumer Relations
Department, Box 190 Jean Talon Station, Montreal, Quebec,
H1S 2Z2

Hotline

PhoneBusters National Call Centre – with a mandate to gather information and intelligence about identity theft PhoneBusters will provide advice and assistance.

Toll free at 1-888-495-8501

Contact Numbers for Australia

If you are a victim of identity theft in Australia use the following contact information;

Credit Bureaus

- Baycorp Advantage: (02) 9464 6000
www.baycorpadvantage.com Public Access Division
Credit Reference Association of Australia
PO Box 966, NORTH SYDNEY NSW 2060
- Dun and Bradstreet (Australia) Pty Ltd: 13 23 33
www.dnb.com.au Attention: Public Access Centre
PO Box 7405, St Kilda Rd VIC 3004

The Australian Crime Commission

The Australian Crime Commission operates an Identity Fraud intelligence facility that can assist victims in notifying some Australian and State government agencies that their

identity has been stolen.

Tel: (02) 6243-6666

Contact your local police for instruction if the information for your country is not listed or is incorrect.

Who Has the Right to Access Your Information?

It can be difficult to determine WHO has the right to access your information. This is especially true in situations where you are requested to divulge information such as Social Security Numbers (for employment or rentals). Who has the right to demand that information and do you have the right to refuse?

You may also be concerned with who is accessing your information within businesses or government agencies. Understanding the need for your information can help you judge whether providing it is in your best interest.

Your Social Security Number is Your Biggest Threat

While information such as your name, date of birth, mother's maiden name, address etc. are easily traced it is your SSN that is the biggest threat. If thieves know your SSN they can access your banking information, utilities and other personal information as well as establish new credit in your name.

Although originally the SSN was only to be used for Social Security programs it is now commonly used for filing purposes including bank accounts, employee, student and medical records. This makes your SSN a free pass gaining access to your personal information.

Who Should Require Your SSN?

There are some government agencies (tax, welfare, Medicare and motor vehicles) who can lawfully require your SSN. Other agencies may request your SSN in a manner that implies you must give it.

You can determine whether the agency has a right to your SSN by reading the disclosure statement that is mandatory on government forms requesting the number. The disclosure statement will tell you if the SSN is required or optional. It also states which agency is requiring the number and what it will be used for. Government agencies have strict laws about the use and storage of SSN's – private agencies or businesses do not.

You cannot be denied services from government agencies if you refuse to give your SSN unless they are legally required to obtain it or had a law in effect before January 1, 1975 requiring a SSN.

Employers must obtain your SSN to report earnings and payroll taxes. While they are required by law to have your SSN you might ask for them to protect your number if it is used for filing, listed on ID badges or otherwise made public.

Other businesses or agencies, including private medical insurance and schools, may request your SSN. If they are federally funded schools or are reporting to the IRS they may have a legal right to the information. If the reason for the request is not listed on the form you can leave the space provided for your SSN blank and ask for an explanation of why they are requesting it.

While a business may have no legal right to the information they can refuse service if you choose not to disclose it. State laws differ but businesses should not willfully display SSN's, however, carelessness or inadequate protection of SSN's may not violate these laws.

Financial information that is of interest to the IRS requires your SSN to be listed. Banking, stocks, employment and other financial statements all must include the number.

Credit card companies may request your SSN but are not legally required to have it. Since the number is used to validate who you are you may be able to provide proof with other forms of identification. Be prepared to have a difficult time finding a creditor who will provide credit if you refuse to submit your SSN.

Since potential creditors (including landlords) may wish to see your credit report you will likely be required to give them your SSN to obtain the report. You may ask if they will accept a current report without the SSN and confirm your identity with other forms of ID.

Federal records, including driver's license, divorce papers, child support and death certificates all require SSN's. Birth certificates usually require the SSN's of both of the parents unless there is good cause for not requiring it.

If you receive email that appears to be from a service provider or government agency that

requests your SSN do not reply. This information will not be requested through unsolicited emails and is being sent from a fraudulent source.

You can find out more about the legal requirements for using your SSN at:
<http://www.privacy.ca.gov/recommendations/ssnrecommendations.pdf>

What is Being Done to Protect Your Privacy?

While government agencies are submitted to legal requirements that protect your personal information, other businesses are not. This makes it vitally important to take steps protecting your information yourself and knowing who has it and what they are doing with it.

State laws do have requirements for the disposal of personal records but the manner of disposal can vary depending on the nature of the information and the resources available to the business. If you do business which requires you to keep personal information on record you must check with local law regarding the disposal of these records.

Fair Information Practice Principles

While the law is still catching up to the needs of individual privacy protection, Europe, Canada and the USA have created a guideline of processes for collecting and using personal information. This guide is called the 'Fair Information Practice Principles'. It outlines the safeguards necessary to ensure the use of personal information is fair and to protect privacy.

The core principles outlined in the Fair Information Practice Principles are:

Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress.

Here is a brief outline of these principles:

Notice/Awareness

Notice and awareness requires businesses requesting personal information to disclose their information practices before collecting information. The following principles listed would be included in the notice.

Choice/Consent

Choice and consent give the individual the ability to allow or restrict the use of personal information beyond the transaction being initiated. Opt-in or opt-out choices include how much personal information is included and what it may be used for.

Access/Participation

Access and participation requires the individual to be able to access, correct or verify their personal information on record. The means of accessing and making corrections must be timely and inexpensive.

Integrity/Security

Integrity and security refer to the business' steps to maintain accurate records, secure the information and destroy records in an appropriate manner.

Enforcement/Redress

Enforcement and redress must be established either by self-regulation or legislation.

The full report of Fair Information Practice Principles can be found at:
<http://www.ftc.gov/reports/privacy3/fairinfo.htm>.

While steps are being made to create enforcement it is up to the individual to be aware of the use and protection provided by each business and agency they provide personal information to.

What Can You Do to Prevent Identity Theft?

Are you familiar with the expression “an ounce of prevention is worth a pound of cure”? This is absolutely true in regards to protecting your identity from being stolen rather than dealing with the trauma and cost of being a victim.

It must be stated here that there are no guarantees that the steps you take will prevent your identity from being stolen. Personal information is available from sources (including government, employment and other business records) that we are not in a position to personally protect.

Taking steps to limit the use of our personal information makes it more difficult to become a target. Proper disposal of personal records and other common sense steps will also thwart any opportunistic thieves.

Here are some steps that every individual should incorporate into the management of their personal information. What you choose to implement will depend on how much time or energy you want to use in protecting your information. Making conscious decisions as to how or when our personal information is shared will give us more control and should become a lifelong habit.

Monitor Your Credit Reports

If you are entitled to one free credit report each year you can request a report every four months by requesting one from each of the three credit agencies in turn. It is wise to check your credit report at least once every year even if you must pay to receive it. If you suspect your identity has been stolen or have received notice of information that has been stolen you may be able to get free reports throughout the first year of the incident.

Don't Carry Your SSN in Your Wallet

Social Security Numbers, birth certificates, passports or any other personal identification should not be carried in your wallet. The same goes for extra credit cards and store or gas credit cards. The less you carry the less risk if your wallet is stolen or lost.

Stop Pre-Approved Credit Offers

You can stop the mailing of pre-approved credit offers by calling toll-free 888-5OPTOUT (888-567-8688). Ask to have your name removed from the list as pre-approved credit offers can be easily abused by thieves.

Shred Personal Documents

If you do throw away pre-approved credit offers or other personal information (such as old tax forms, bank statements or expired credit cards) you must shred the information before disposing it.

Pick Up the Mail EVERY Day

Don't allow mail to sit overnight in the mail box or you give thieves an easy target.

Credit card offers, bank statements and possibly information with your SSN can be used to open new credit in your name or steal from you.

Don't Respond to Email Requests

If you are contacted by a bank or service provider through email you must never submit any personal or financial information to them. These attempts to 'trick' you into believing they are a legitimate business is called *phishing*.

If an email claims that you must validate your information and provides you a link to the form DO NOT OPEN THE LINK! If you are concerned that the request may be legitimate close the email and enter the URL to the actual business in your browser window. If your account looks fine contact their customer service department to verify the email. A fraudulent email is called a 'spoof' and the company will likely want you to forward it to them.

Don't Give Information to Phone Callers

Unless you initiate a call to a business you should never give personal or financial information to a caller over the phone. Your bank or Credit Card company will not ask for your card or account number if they call you. They have that information on file.

If a caller portrays themselves to be representing a charity or offering a prize or trip you can ask for a phone number to call back. Verify the phone number and hang up. If they are with a reputable organization you will be able to check the number and call back.

Telemarketing scams that ask for credit card deposits, account information or personal information such as your mother's maiden name, your SSN or other information are common. If you wish to donate it is better to call the organization yourself.

Put Passwords on Your Credit Cards

Credit card companies like Visa offer added protection by allowing you to create a password along with the card number when making a purchase. Even if your card is stolen you can prevent thieves from using it by having it password protected.

Be Aware of Who Has Access

Don't give passwords to credit cards or other personal information to friends and family. According to a survey done by www.idtheftcener.org the victim respondents indicated that 43% of them thought they knew the imposter. About 34% were aware that the thief had a history of needing money to support a drug, drinking, gambling or shopping addiction.

Online Shopping

Only shop at merchants you are familiar with or contact the Better Business Bureau. Look for secure shopping sites with identifying marks such as https appearing in the browser window or a lock icon appearing below the webpage on your browser.

Never give PIN numbers or passwords to the merchant. Verify your bank statements immediately online or over the phone to check the transaction was made for the proper amount and no other charges were made. Be sure to have anti-virus and anti-spyware programs running and always print out the transaction record, log out and close the browser when completed.

Read more about Online Privacy in the following chapter.

Always Ask or Opt-Out

Whenever you are asked for personal information you have a right to know why it is needed and how it will be used. Online you may find that information in a Privacy Policy (read about that in the chapter 'How to Read a Privacy Policy').

Limit the use of your personal information by requesting financial institutions not to share your information with affiliates. This is called 'opting-out' and the financial institution must allow you to do so. Once you have requested to opt-out, either on the phone or in writing, they must never share your information unless you specifically request they do so.

Sign Your Cards Immediately

When you do receive a new credit or debit card sign it immediately and never carry it unsigned.

Don't Save Passwords

Don't save passwords to personal information (such as online banking) in a program that 'remembers' your information. Remove cookies from your computer and have your hard drive professionally 'wiped' before disposing it.

Use strong passwords – that means a combination of letters and numbers that can't be easily guessed. Never use information such as your mother's maiden name or birth date that can be figured out by thieves.

Protect Your Computer

Set your browser security settings to Medium or higher. Install a firewall to prevent unwanted access from hackers and install anti-virus and anti-spyware programs. Never download software when you don't know where it's from and never click on pop-ups or spam email.

How to Identify a ‘SPOOF’ Email

Along with the convenience of the internet has come a new wave of predators looking to steal from innocent victims. This often occurs through ‘spoof’ emails.

A ‘spoof’ email is an email that appears to be from a legitimate organization or business – often banks or service providers – but is really a fake email sent from a con artist.

These thieves construct emails that use the logos and styles of the bank or business and attempt to convince the recipient to reply or click on a link to a website and submit personal and financial information that can be used to commit identity fraud.

While these emails are extremely common they can be difficult to identify unless you know what to look for. Here are some signals that an email may be a fraud as well as some general warnings about dealing with ‘spoof’ emails.

Not Using Your Name

Spoof emails will likely not have your name in the message. They may be addressed ‘Dear Customer’, ‘Member’, ‘Friend’ or other ambiguous title. Real emails from institutions or business you have accounts with will use your name or a name you created for your account.

No Account Number

Companies that you have done business with will have account numbers and passwords on file. If you are ever contacted by a business that asks you to verify your account number or password do not respond. Only give information to businesses if you have initiated the contact.

Improper Grammar or Spelling Errors

A surprising amount of these ‘spoofs’ will have grammar or spelling errors. Whether this is because the con artist is not a native English speaker or it was done in a hurry is immaterial. A legitimate business email will not likely have these glaring errors.

Warnings to Close Your Account

Often the ‘spoof’ email takes the form of a warning that your account has been illegally accessed, that you have been a victim of fraud or that your account will be closed unless you respond to the email. They will ask you to click on a link in the email and verify your information. In reality you are giving the information to the thief who will use it to access your real accounts.

Always be suspicious of emails that ask for personal information. Contact the business through their official website and find out how to forward the fraudulent email to them. If you have opened any links or provided personal information you should immediately contact the business about the account and watch for unauthorized activity. Change all passwords or close the accounts and open new ones with different access codes.

‘Phishing’ Emails

‘Spoofs’ are also called ‘phishing’ emails. ‘Phishing’ refers to any email that attempts to get you to share personal or financial information that can be used to commit fraud.

While ‘spoofs’ pretend to be a known business or institution, ‘phishing’ emails also include offers to collect prizes, requests for help, charity donations or false notices that you have won a lottery or a trip. They tell you that to reserve your prize you must give them a credit card number for verification or as a deposit.

Some emails request your help by offering you a portion of a fund that will be deposited into your bank account. These are often sent as requests from rich foreign (particularly Nigerian) nobility or government officials. They are dangerous groups and should never be contacted or replied to.

Similar scams are also done over the telephone and are called 'pretexting'. Always contact the organization or business directly if you are contacted for charitable donations or account information.

Special Concern: Online Privacy

While many suggestions have already been listed to protect your identity online there are a few areas that require special attention.

Email Fraud

Email fraud was thoroughly explained in the preceding chapter about steps to take to prevent identity fraud. Treat every unsolicited email with suspicion and exercise caution when sending information that contains personal or financial details through email.

Protect Your Computer

Computer viruses and spyware can enter your computer when you click on a link in an email or by accessing a website that downloads the program without your consent.

While no person can prevent all exposure to these viruses and spyware you can protect your computer by installing a firewall as well as purchasing anti-virus and anti-spyware programs that routinely search your computer and remove these threats.

Viruses can spread through your computer, corrupting files and information as well as being passed on to other people through your email. Spyware can track your movements

on the internet as well as collect information that you enter while using the internet including passwords, banking information and personal data.

You may also download programs that appear safe but are hiding spyware or viruses. These programs are called Trojan Horses. Only download information from sites you know and trust.

Shop Securely

Online shopping is convenient but can also pose hazards for unwary buyers. While electronic exchange of funds makes buying online easier it is important to watch for signs of a secure site. Secure sites provide encryption of data so that others can't view it or intercept it. This encryption is called SSL (Secure Socket Layers).

Look for security symbols such as a closed padlock on the bottom of your browser window and URLs that start with *https* instead of *http*. Encryption that hides your sensitive information (like passwords, credit card numbers and other personal data) by displaying it as dots rather than the actual numbers or letters is another safety feature.

Check the Privacy Policy and only deal with reputable merchants. Check with the Better Business Bureau if you're unsure. You may also consider third party payment processors (such as Paypal and ClickBank) which prevent the merchant from obtaining any financial information directly. Check the security status and privacy policies of any third party processor before making a transaction.

Sharing Computers or Using Laptops

If you are sending personal information on a public or shared computer you must log out of the browser before ending your session. If you don't log out another person may be able to use the back button on the browser to obtain your information. Empty cookies so

other users will not be given your information if they access the same site.

Storing personal information on personal computers (especially laptops) can be dangerous if the computer is stolen or hacked (illegally accessed). Don't save sensitive passwords in programs that can auto-fill forms.

Online Forums and Chat Rooms

You may find that in the excitement of meeting new people and developing personal relationships in online forums and chat rooms you to forget the dangers of providing too much information.

In these social or business gatherings you may foster friendships within the group but it is important to remember that these areas are available to the public and individuals who are not making their presence known can still be 'lurking' on the forums and searching for personal pieces of information that are inadvertently expressed.

You never really know who you are talking to so it is wise to make it a habit to never reveal personal information such as your telephone number or address to these public groups.

Even if you are dealing with a private chat room you should exercise caution if you are not personally familiar with the individual(s) you are speaking too. Misrepresentation happens often enough to make it a real danger even for adults. Never send personal or financial information to individuals in a chat room or on a forum.

The anonymity of the internet can cause people to say things online that they would never say in person. It is wise to avoid getting involved in heated debates (also called "flame wars" or "flaming" when directed to a particular individual). People online are

just as real as those you meet in the flesh and saying something to incite another person can be just as dangerous online as offline.

Watch Where You're Going

Don't download anything when you don't trust the source. Even if you are emailed or given a link in a chat room or forum you should be cautious. Look at the URL. Some links will directly download programs – including viruses – without your consent.

While using anti-virus and anti-spyware programs will help avoid problems they can't catch everything. Know where you're going and who is sending you.

When You Need Help...

If you need help dealing with online security issues including harassment or fraud you can contact the Cyber Law Enforcement Organization at:

<http://www.cyberlawenforcement.org/> or check out more information at <http://www.wiredsafety.org/> or <http://www.idtheftcenter.org/vresources.shtml>.

While these organizations have connections to legal or volunteer assistance you should contact your local police if you suspect your identity has been stolen or fear for your safety.

Learn How to Read a Privacy Policy

One of the essential steps to protecting your privacy is understanding how to read a privacy policy.

Privacy policies should be made available in some form anytime you are asked to provide personal information. Financial institutions, health facilities or other businesses that collect your information can be asked to show you their privacy policy before you give them your information.

If the company does not have privacy policy consider doing business elsewhere. It is a show of respect to customers to tell them how their information will be used.

Online you will find privacy policies posted on websites. The privacy policy is an indication of the steps they will take to protect your identity or to inform you of how they will treat the information you provide. Simply having a privacy policy does not guarantee you any level of protection. To understand what is protected and what is shared you must read the policy.

Each site has its own criteria for a privacy policy. Some give full protection including encryption of passwords and not providing your information to any third party while

others tell you that your information will be shared with affiliated companies or businesses they feel you would be interested in hearing from. You must read the policy to be aware of the steps being taken to protect you.

Here are some of the items to look for on a privacy policy:

What Information is Collected and Why?

When a business is requesting personal information it is reasonable to ask what information is collected and why it is needed. If they request information that doesn't seem relevant they should state why they need it.

If there is no explanation for the request try to avoid giving the additional information or ask them why they need it. Asking for your income or the name of your spouse is the kind of information you might question providing without reasonable cause.

How is the Information Collected?

While filing out paper forms is straight forward you need to find out from websites how the information is being collected. Websites sometimes use cookies that they install on the visitor's computer to track information about what pages they click on, how long they spend there and your IP address.

This information can be tracked without your consent. Usually it is only to facilitate the company's marketing research or to assist you by using your information from previous visits. You should be able to find out what information is automatically stored by reading the privacy policy.

What Will the Information be Used for?

If the business asks for your personal or financial information you have a right to know

what it will be used for.

Is it only to complete the transaction? Will they view a purchase as permission to market to you again or to sell your information to other businesses? This information should be available in the privacy policy as well as information on how to ‘opt-out’ of these uses.

Who Will Have Access to Your Information?

Is the information sold or rented? Do they share your name, email address or purchasing habits with other businesses? These areas should be clearly outlined in the privacy policy. If they do sell or rent the names on their list you may wish to limit the information you provide.

Watch for terms like “affiliates”, “sponsors” or “partners” since you will have no idea who will be receiving the information.

How Secure is Your Information?

What steps are taken to protect your personal information? Any transaction that requires you to submit personal or financial information should have SSL (Secure Socket Layers). SSL will encrypt the information so that it can’t be read by others during transmission.

You can verify the security by looking for the *https* at the beginning of the URL and an icon with a lock (closed) in the bottom corner of your browser window. While these methods are not completely infallible and can possibly be mimicked on fraudulent sites they are a good indication that security precautions are being taken.

Can You Correct Personal Information?

You should be able to review or correct information that is collected about you. The steps should be outlined in the privacy policy and be both convenient and inexpensive.

Can You ‘Opt-Out’?

Wherever your information may be shared you should have the right to ‘opt-out’. In some cases there will be a box that you can click to opt-in or opt-out when entering your information. Watch out for small boxes that are already checked as the default since you are implying you are accepting the offer even if you don’t personally check the box.

The privacy policy should also give you directions on how to opt-out if the option isn’t given when entering your information.

While this list is not exhaustive it does highlight some of the main features that you should look for in a privacy policy. The other information that should always be listed is a contact name, address and telephone number where you can speak to someone regarding the policy.

Protecting Your Children's Privacy

Protecting your children's privacy is perhaps the most important reason in the world to be familiar with the steps necessary to prevent problems with privacy invasion.

While children are not necessarily targets of identity theft they are overwhelmingly susceptible to becoming targets of more insidious crimes which start with the perpetrator learning the identity of your child.

Understanding how chat rooms and email work can help parents teach children to behave safely online. While there are many programs and procedures you can use to track the activity of your children it is most important to educate them about the dangers of chatting online when you don't know who they are talking to or who is reading what they say.

Take similar precautions when your child has a cell phone or text messaging service.

Online Forums and Chat Rooms

Does your child understand that listing their real name, address, telephone number or information like the school they attend can be potentially dangerous if the wrong person decides to get in contact with them?

Do they realize that although the forum or chat room is SUPPOSED to be for children there are possibly adults pretending to be children in order to take advantage of them?

While you do not want to unduly frighten your children it would be more terrifying if you found out that they had been in contact with a pedophile and they did not know how to tell you about it.

Give them rules. Here are some you may want to discuss with your child(ren):

- 1) **NEVER** give out your name, address, telephone number or picture. **NEVER** agree to meet someone you met online without your parent's approval.
- 2) **REMEMBER** you are speaking in a public area – other people may read what you write.
- 3) **REFUSE** to enter a private chat room. These rooms are closed off to the public and your child may be lured in by an adult trying to seduce them.
- 4) Encourage them to **TELL** you what goes on. Just as you would monitor who they spend time with after school or what TV programs they watch – you want them to feel comfortable telling you about their online friends.
- 5) **LIMIT** the amount of time they spend online. While talking with friends about sports, fashion or other interests may be fun it is not wholly productive for children to spend hours online chatting. It is also more likely that they will investigate sites or forums that are unsuitable for children. Curiosity may lure them in over their heads.
- 6) Have the computer in a **PUBLIC** area of the home. This will protect your children more than any software program. Check on them occasionally just to see what they are doing.

- 7) **INFORM** them about Spam and other email that looks suspicious. If they are not sure tell them to ask you before opening it.

- 8) Tell them never to engage in **FLAMING**. Flaming is an attack on another person who is posting. It is both emotional and uncontrolled – often due to the power of anonymity that exists online. Children have been bullied by other children from school or elsewhere (called cyberbullying) and it can be devastating. Remind your child to show manners to others and be careful how they respond.

- 9) Check the **HISTORY** of their online surfing if you are concerned. It is good to let your child know that you will occasionally check this out as a protection for them.

- 10) Use a **POP-UP BLOCKER**. Sometimes windows open up that advertise pornography or other disturbing images. Make sure you use a pop-up blocking program to protect yourself and your family from this unwelcome exposure.

Even with the previous suggestions you can further secure your child's online experience by looking for organizations like WiredKids.org – these teams provide safe chat supervision to children and teens at WiredKidz.org and WiredTeens.org.

Not only are these areas supervised (although following the above rules is still necessary) but they teach young ones about safe communication, how to use the Internet and other methods of communications responsibly.

They also provide information on cyberbullying, cyberstalking, flaming and more. If your child has been a victim you can use their resources to find the information and support you need to fight back.

Reminder

With the age of advanced communications and technology people can learn new things, meet others and connect in ways never before imagined. It is important to respect the need for diligence to ensure these experiences are positive and worthwhile so that you and your family can enjoy these conveniences without undue risk.

Regardless of if you are protecting your financial information, personal information or your child's identity you need to understand how this information can be abused online, through text messaging and in the real world.

Educating yourself is the first step. Passing these rules onto your children will protect them and give you peace of mind.

Incorporating steps to protect yourself and your children is a way of respecting your privacy and theirs. While we cannot combat all crimes we CAN make ourselves and our children less likely targets by always showing respect for our personal information and understanding how new technologies, like the Internet, work.