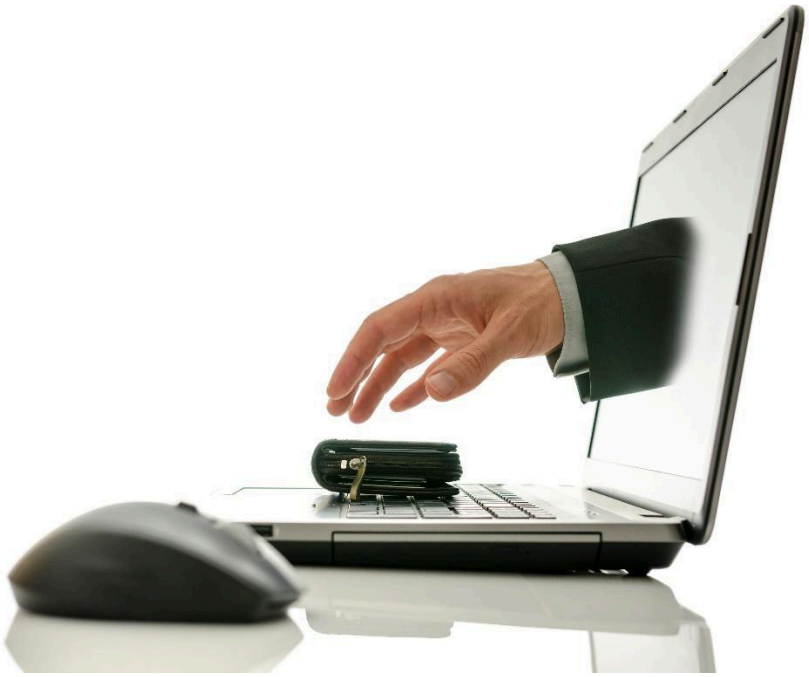
Retirement
Identity Theft & Scams
Never be a Victim

eBook Format Only: FREE



The Police, FBI, Mounties And Crime Stoppers

Eleanor Rose TEAM
FantasticRetirement.com: eBook FREE
 40 pages

Our Gift to You
value $8.95

Published by: Chelsea Lane Publishing

Library of Congress Cataloguing in Publication Data

Rose, Eleanor
Retirement : Identity Theft & Scams

Bibliography
identity theft, scams, retirement, credit card companies, FBI, Canadian Mounted Police, Phone Busters, phone scams, fraud, fraudulent, AARP, CARP, Stolen, credit payments, internet fraud, old age, experiencing loneliness,

I.S.B.N. 0-9692967-1-1

DISCLAIMER

The information presented in this ebook is solely sourced from contributing retirees. It is intended for educational and entertainment purposes only. It is not meant to replace a professional, such as a doctor, travel agent, travel professional, or any other type of professional.

Because each person and each situation is unique, the compilers and web master, Eleanor Rose, Chelsea Lane Publishing and the team at www.FantasticRetirement.com accept no responsibility for any travel, health or non-health related ideas or procedure outline by contributing retirees in this ebook, which a reader adopts

Eleanor Rose and/or her team at www.FantasticRetirement.com are not responsible for any action, opportunity or idea a reader may take in response to reading the ebook Retirement: Identity Theft & Scams.

A reader is totally responsible for their own safety, finances, and recognition of identity theft or scams. etc..
No liability, legal or otherwise will be assumed or credited to Eleanor Rose and/or her team regarding any consequences a person takes regarding reading, Retirement: Identity Theft & Scams.

Always seek the advice of a professional if you plan to implement anything read, here.

Eleanor Redding and/or the team at, www.FantasticRetirement.com is/are not responsible for any adverse effects or consequences, from the use of, information presented in the ebook Retirement: Identity Theft & Scams.

The information presented in this ebook is for entertainment purposes only.

Privacy

Confidentiality and privacy are maintained. No, submitted address, e-mail address, specific location, nor full name, will be exhibited in this ebook. If you wish to contact a contributor, we will not put you in touch with them.

Copying This eBook

Since this book is copyrighted, it is illegal to copy the whole book or segments of the book. A Data tracker is placed on each ebook. You would be wise not to copy.

Introduction

Seniors 'Up For the Count'

As you know, on, FantasticRetirement.com, the information comes from research and retirees who email their experiences to:

FantasticRetirement@gamil.com

They shared their stories or information pertinent to seniors. This book,

Retirement
Identity Theft and Scams

follows the same premise. Information submitted by seniors in North America, England, Ireland, Scotland, Australia and one well-informed guy in Panama, supplement facts from Phone Busters, the FBI, the Canadian Mounted Police, local police, AARP, and CARP, (Canada).

Some of our senior emailers, have been victims. All are crusaders to keep retirees and their families safe from identity fraud and any other type of fraud. Many people are familiar with how devastating and invasive one feels when your house is broken into. Suffering identity theft carries the same emotions and for many, huge financial losses.

If you have further information to share on identity theft, please email it to us: FantasticRetirement@gmail.com.

What follows is a compilation of information these wonderful seniors have sent, which further exemplifies what the police forces, Phone Busters, AARP and CARP, do to fight Identity Theft and scams against seniors.

The Extent of the Problem

There is a worldwide massive black-market industry in identity theft, with yearly revenue of $55 billion. Stolen personal information is procured through credit cards, loans, telemarketing, stolen purses and wallets, bank account info., theft, etc.

Case #1

Karen emailed, "I didn't realize that anything was amiss until I read my credit card statement at the end of the month. I was shocked to find that a laptop computer, tires, clothing and food were listed on my bill. I was angry that these stores didn't believe me. I called my credit card company quickly. Along with feeling angry I felt tainted and bewildered. How could this have happened to me? I contacted the police to find out that there was an ongoing investigation, particularly regarding computer black market purchases. I also called "Phone Busters".

Karen M. Connecticut

www.FAntasticRetirement.com also, contacted Phone Busters and the police to confirm some of the stories and information emailed. The stories were all true happenings.

The Definition

Who really wants a definition, but here it is:

Identity Theft is described as obtaining or using someone's personal information without his or her consent or in a fraudulent manner for economic gain or other purposes. Credit card and debit card fraud are the most common but the danger is much broader including long distance calling, opening bank accounts in your name, mortgage fraud, and much more

ARP, in the U.S. and CARP in Canada, both seniors' organizations, fight identity fraud as part of their mandates. From the police, to the credit card companies, to organizations and banks, they all say that education is the key to avoid becoming a victim.

As one police officer said, "You are dealing with sociopaths. They have no conscience. As he interviewed a suspect who was about to be charged with fraud he asked, "Don't you find this hard on your conscience, stealing from old ladies?" The answer:

"Next question?". As the policeman shared with me, they have no conscience. They will rip off the same person time and again.

Typical Frauds

Sheila in England emailed. "I found out that many of my friends received the same letter from Nigeria. Some got them from other points in West Africa or Mexico. It goes like this,

I am a person of wealth. I have 60 million dollars which I would like to, 'get out of the country', because of political unrest. If I could transfer this money to your bank account it would be safe from our politicians. In return I will share the money with you, giving you _____X_____ million which would leave me with _____X_____ million. We would both benefit. etc., etc."

I'm glad Sheila was wise to this scam but I investigated, to find out that many were sucked in. My, 'found', statistics, showed that 10,000 people in the U.S.A, lost 41 million with this scam and 5,000 folks in Canada, lost 12 million.

The Stolen Wallet Story

This one came from Walter in the U.S. south. He read it in a newspaper. Apparently, several women were out for dinner in a rather posh restaurant. They chatted and ate all evening. One of the women had parked her purse, by its strap, slung around the back of her chair. Again, she didn't find out till her credit card bills started to come in, that she was, 'out', 42 thousand dollars.

What Happened

While she was enjoying herself her wallet was taken from her purse. By phone, several large purchases were made and then her wallet was replaced. No one at the table knew this had happened.
It took months for the police to trace her contacts and for her to remember everywhere she had been. Eventually they nabbed a waiter and the barman. It’s rare that anyone is caught.

Credit Card Company Response

Credit Card companies make billions of legitimate dollars on interest rates from people who don't pay off their debt at the end of each month. That's why people use cards, so they can run up their debt, 'over into the next month'. That service costs the consumer.

Off the topic: By the way, if you have huge credit card debt, did you know that you can call the credit card company and tell them you can't pay and would they lower your interest rate and chances are you will be shocked by how much they will lower it.

Back to the credit card companies being very responsible. I don't know how they do it, but they get suspicious of purchases that seem to be out of the ordinary and call you. Here are 2 stories.

Ethel K. Baton Rouge U.S.A.

"My son wasn't home 5 minutes when the credit card company called. They wanted to know if he really got gas for 14 dollars and 5 minutes later got another 5 dollars worth of gas. That's exactly what he had done. Was he impressed with Visa? You bet. Obviously, Visa thought that someone might have double swiped his card for the 5 dollars. Wasn't that quick?"

I don't know if they have computer robots or real people watching, but it is amazing.

Double Swiping

About this double swiping: It is wise to insist that you see the clerk swipe your card. That means at a gas station, you get out of your vehicle and follow the attendant into the booth and watch the swiping. It also means, particularly, in clothing stores, that you do not let the clerk, turn his or her back to you and swipe your card on the back counter. Make him or her stand sideways so you can see the swipe.

Double swiping means the clerk runs your card through the legitimate machine and then through a smaller, nearly inconspicuous machine for a second swipe. That machine records your numbers.

Another easy place for 'swipe theft' is a gas station. Thieves, within 1 minute, can replace the component, at the gas pump, where people slide in their card, to pay for their gas. Folks like this feature because they can pay quickly without going into the kiosk.

Thieves leave their component in the 'gas pump', for a few hours, then pull up and get gas again. Within 1 minute they have slipped out their component and replaced the original one back into the gas pump. Again, they have your credit card numbers.

The Vacation Fraud

Archie H., in Western Canada, told me about this one. He got it and took it to the police. He also reported it to PhoneBusters. This can happen by phone or mail.

Archie got a letter with a whole lot of enclosures. It looked like the real thing: vacation pamphlet, opening letter, day trips, included, certificates, the whole works.

He had 'won' a trip to the Caribbean. All that was required was that he sent $235.00 to cover the paper work and air port taxes. Of course, all this was to be done in 1 day. The quicker the better is the scammer's motto. They would forward the tickets as soon as they got the $235. Archie was smart to follow it up as a scam.

The Lady in the Old Age Home

You would wonder how a lady in an old age home, could have 2 new vacuum cleaners and accessories, under her bed. This was a lonely lady with basically, little family visiting. The old age home staff never noticed. That's hard to believe. It seems, 2 different companies had been to her room, without detection, to deliver their machines and collect money from a lonely old lady.

A niece came by and found the vacuums. One had been purchased within the month and with the 30-day cancellation policy, she got that vacuum cleaner returned and the money back. But the old lady was, 'out' the cost of 1 of the machines. This isn't Identity Theft, it’s taking advantage.

Loneliness

It seems that older women, more so than older men, are alone and lonely. Scammers call them and call them. They learn about the grandchildren, perhaps a deceased spouse, and all kinds of stuff. They call, "to chat". The lonely are sucked in.

As they enjoy the phone calls and trust the caller, they are talked into buying, donating, or helping that person out, and it always involves cash.

A lot of these ladies go to fairs and bazaars. That's were you fill out an entry to win a quilt, a sewing kit, jewelry, etc. Scammers find this easy pick'ins. Who would think you'd get ripped off at a bazaar? Just think, churches host some events and yet scammers can infiltrate there as well.

Don't fill out those forms.

Returns

I just returned some faulty make-up to the pharmacy. To get my money back I had to fill in a form with my name and address. I told the clerk, "I've just been to an **Identity Theft** seminar. I don't want to give you my name and address." She settled for my name. I was told that without something on the form, she couldn't refund my money.

The Internet

Phishing:

Lots of thieves pose. That is they pose as your, **bank,** as **eBay,** as your **credit card company,** as a **store** you shop at. They are phishing for your personal information. They send very, very official forms via email requesting your personal information.

For example, "Our computer system has, "gone down". Please fill in the following so that we can re-establish you in the system".

Always phone the real company and ask if they have sent, via email, a request for your information. Chances are, they have not.

Legitimate companies never use email to ask for personal or financial information. If you receive such a message, by phone, letter or email, call the institution using a phone number you already have. Thieves can install spyware software on your computer plus use popups to convince you that they are legitimate.

Check at : http://www.fbi.gov/yberinvest/escams.htm

Downloading Free Software

Do this only from sites you trust

Virus Protection, Firewalls, Anti Spyware

Install protection on your computer and update it regularly. Use a secure browser when shopping online. Look for an unbroken-key or closed-padlock symbol, usually at the bottom of your screen which insures a protected site.

Spyware keeps a log of your every keystroke and can capture passwords, PINS and other personal info. Anti Spyware alone is not safe enough. Use a firewall as well and make sure it's turned on.

Install a pop-up blocker, antispyware, a fire wall and anti Spam programs

SAMPLES

Internet Security Barrier Family Edition by Intego
MailWasherPro by Firetrust Limited
eTrust Antivirus by Computer Associates Internetaional
Norton Antivirus by Symantec
Sphos Anti-Virus by Sophos
McKaffee
Kids GoGoGo by Maki

Password Protect Your Computer

Password-protect your computer from strangers or careless roommates, for college kids. You use a password and lock it by pressing the Windows logo key +L.

Fingerprint readers for less than 50 dollars work well if you can't remember passwords.

The Grandkids

All the kids are on email and instant messaging. Doing this invites 'worms' to their computers, which ride along on messages they receive. Under these circumstances, those computers need all the protection they can get.

That Cafe, Coffee Shop, or Library

Never, never, access your personal info there. Someone, at a library, could access your info, if they are next in line to use the machine.

Wireless

Schools, campuses, etc., have wireless. These networks are convenient but they come with a security risk. It is a known fact that another remote computer, perhaps someone, sitting nearby, in an internet cafe, can 'pick up' your information.

Also, with wireless, make sure there isn't a car parked out front of your house that you don't recognize. It could be a scammer hacking into your links via wireless. In an apartment, wireless is just about hopeless, in keeping your personal info. safe.

Computer Heaven

When you are ditching your computer, buy a "wipe" utility program to overwrite your entire hard drive before you dispose of an old computer. Many people take a hammer to the old drive.

READERS PLEASE NOTE

If you find something that should be included in this tome, please email it to

FantasticRetirement@gmail.com

with the following on the subject line

For Your Identity Theft eBook

Your Shredder

Preferably it should be:

1. handy
2. a cross cutter that shreds vertically and horizontally

Charity

I'm sorry to say, but I do not, 'give' over the phone or 'to', anything that comes by snail mail or email. I no longer give to the police or firemen

who phone and say they are putting something on, like a circus, for kids. Those charities I wish to give to, I go right to them and donate.

Also, I no longer leave used clothing, in a bag, at the curb, for a charity. I take the bag there.

The Telemarketer's Cut

Did you know that many telemarketing companies, asking for charity donations, are reputable? BUT, did you know that most of these telemarketing companies get 50 to 90 % of the cash that is donated.

Organ Donation

"Imagine identity thieves using organ donation to scam my personal information",
Sharon, in Ireland, thought it had to be a hoax.

She,"let the caller talk on and on," and then Sharon said, "Give me your name and phone number so I can call you back"." CLICK
End of conversation.

The Tsunami , 911, and Katrina

Within hours, after those tragedies, with the donation information on television, thieves had web sites up and running that looked like the donation sites, felt like the donation sites BUT had 1 letter different than the true donation sites.

People make typing mistakes. Internet thieves made lots of money this way.

Speaking of the Internet

Banks, credit card companies, eBay and reputable companies, have their sites, encrypted. That means that 99.999% of thieves could never break in to your information.

It also means, that, our FantaticRetirement.com website, is 'safe'. When you buy a book from our web site, your personal information, your credit card number, goes through Amazon, not to us. Amazon is an incredibly, heavily encrypted site. We at, FantasticRetirement.com never see your personal information.

Yes we have your email address in order for you to receive your free ebooks. Our reputation is based on the fact that :

WE NEVER SELL OR SHARE YOUR NAME OR EMAIL ADDRESS.

hint: Have a separate credit card that you use only for the internet which has low limit. My credit card for the net has a limit of 500 dollars.

hint: Have a different email address for downloads you buy or get fr*ee on the internet. eg, a hotmail address

hint: An incoming email attachment can install spyware on your computer, allowing the sender to watch your every keystroke, (including those used to log onto your bank's Web site).
Never open attachments from unfamiliar senders.

The Lothario Not Exactly Identity Theft

Katie, in Australia emailed. "Here's a story from our local gazette I thought you would want to share. A man, aged 71 had married 4 times during his lifetime, all to older women,

He scammed them of their life savings and then divorced them. One lady died of a heart attack. The police got involved when wife # 4 contacted them with her son and daughter-in-law in tow. The thief was interviewed on the telie, No remorse. He thought they were dumb women."

eBay Fraud

eBay is a fantastic company, moving thousands and thousands of dollars worth of goods, daily. All legitimate. But there are scammers on eBay. You find a product you like, win the auction, send your money and don't get the item.

Of course, you report it to eBay, but chances are you have lost out.

Lottery Fraud

"**Is this** Mark_____ on _____ Elm Street in _____? Well Hello Mark! Are you sitting down?

You've just won $750,000, half of the Florida State, (or wherever), lottery. It's my pleasure to tell you that you and I have won the, eg. Florida State jackpot."

"By this time, they could wipe me off the floor", emailed Mark, in Ontario Canada. "I had been to Florida. I wasn't thinking straight, with all the hype about their lottery, I didn't even think about the fact that I hadn't bought a ticket.

I was told if I send money to cover the taxes and customs fee, they would happily send me a certified check. I didn't do it.

The very next week, I got another call, telling me that the other winner had not been quick enough to respond so I was to get his $750,000, too. All I had to do was send the amount to cover the taxes on his share and the customs fee and I would receive $150,000.00".

Can you beat that scam! "

Also watch out for the L'Gordo , the Spanish Lottery and the lotteries in the Netherlands and Australia.

NEVER: pay money to win something

Your Lottery Ticket

Sign it before you hand it to a clerk who puts it into a machine to see if you won. Ask for you ticket back whether you won or not. Check to see that you got back your ticket because it has your signature on the back. This prevents the retailer from substituting another ticket and claiming your ticket for themselves. A disproportionate number of retailers have been lottery winners.

Better yet check your 'numbers' against those published on the lottery's official website.

900 and 809 Phone Number Scams

Here's how this one works to an ad, to a flyer, to an email, something... that has a 900 or 809 phone number. Now, people that indulge in porn recognize how this works because it's how they get their,'porn fix', on a sex line.

When you dial the number, for porn, the clock starts ticking and the money starts being taken off your credit card. The longer you talk to the, 'porn star, the more it's going to cost you.

So, an innocent person maybe gets a call, about winning a prize. "Just call this number or worse still, just press ____, to get the information about how to collect your MONEY, FREE GIFT, etc.

You dial the number, or press the asked for number key, and next you are put on hold.

Translation: Their clock starts ticking up the money as you sit there on 'hold'.

At the end of the month, on your phone bill, you are charged 7 dollars per minute, equaling 35 dollars for a 5-minute call. Slick!

Social Security Number (U.S.A.) SIN Number (Canada)

Except to get a job, don't give this number to anyone. Don't carry this card. Leave it in a safe place at home or in a safety deposit box in a bank.

Your Wallet

Limit the number of credit cards you carry. Make copies of everything in your wallet and keep the copies in a safe place at home or in the bank. This applies to your Passport as well.

Traveling

Use a money belt that fits down inside your slacks or skirt. Keep your money, credit cards, airline tickets and passport in it. If you need them, just turn your back on the clerk and 'fish' out what you need. Also keep them in a plastic bag in the money belt to prevent them from going haywire, should you sweat.

Signing A Credit Card

NEVER NEVER NEVER NEVER Sign the back of your credit card.

On that line, write, 'Photo I.D. Necessary'.

If a thief gets your credit card there's not much he can do to show a photo I.D.

We are told that soon credit and debit cards will require a pin number for every use. Good idea.

Pin Numbers

Did you know that 61% of kids in college have given their pin number to someone else?

eg. : "Hey get me a beer". Giving their pin.

Never use the year you were born as your pin number, or 1-2-3, or the words, 'PinNumber'. Use a sequence of numbers and letters which is a nuisance, but hard to 'crack'. Change pin numbers, often

Pin Numbers

If anything feels, 'off', when you are standing at an ATM, leave immediately and go to another place to get money from a machine.

No matter where, use your hand to cover the machine where you are keying in your pin number, even at a grocery store. Just as the component where you slide in your card, can be removed at a gas station, this can happen, as well, at an ATM machine.

Maybe I'm crazy but I use them only when traveling.

Your Checks

Checks are getting rather passé now but sometimes you have to write a check.

Make sure that when you order new checks, see about putting only your initials or an initial and last name... **no address**. Checks float around in snail mail.

Your Credit Card Statements

Make sure to be aware when your statement should arrive in your mail box. If it doesn't arrive, call the company.

Check Online

I know several people that have a look at their credit card statements and their bank accounts daily. As Bob in Britain said, 'It just takes a quick glance. I keep them on my desktop to make it even faster. Anyone using my computer information would need a password to get to them."

Buying Theatre Tickets

Often the person on the phone asks for the 3 digits that are on the **back** of your credit card. Do your darndest not to give this.

Hotel "Keys"
Those thin plastic keys, that look like a credit card, that you stick in the lock to open the hotel room door: Keep it after you check out of the hotel. Lots of time it has all your info on it till it is rekeyed again.

Test Driving A Vehicle

Jack in Idaho emailed, "Did you know that it's common practice, at a car dealership, that they make a copy of your license before you can take a car for a test drive.

I refused and took the salesman for that drive without letting them copy my driver's license".

Dumpster Diving

Your trash can hold a treasure of information. Shred it all.

Your Outdoor Mailbox: Especially Rural Ones

Put a lock on it or use a box at the post office.

Photocopiers

Most digital copiers have a disk drive, the same kind of data-storage mechanism found in computers-to reproduce documents. Often, they are set up to retain the information scanned.

If the data on the copier's disk isn't protected with encryption or an overwrite mechanism and if someone with malicious motives gets access to the machine, industry experts say sensitive information from the original document falls into the wrong hands.

Many of these less stringent copiers are what you find in pharmacies, etc.

"It's a valid concern and most people don't know about it."

Garbaging in old copier means that often, the information is still, "in there". "Small businesses and everyday consumers are less likely to know about the risk."

And don't we all, dutifully, make copies of all our credit cards, driver's license, passport, travel documents, insurance, etc, to be stored for safe keeping, especially before taking a trip.

Mortgages and Selling Your House

The latest horror of I.D theft is: the thief takes a mortgage against your house or even sells your house, especially a rental property you might own. Several cases have happened in Toronto, Calgary and Vancouver. After the thief gets enough of your I.D. they remortgage or sell your house. Not only, you are "out", but so are the folks that bought your place.

The Canadian government, right now, is passing laws to stop this, but many people are now in limbo, not having ownership of their homes, or being the person or couple who bought your house, but the question, legally, is, "Who really owns this house?".

It's a nightmare. The law, as it has been, in Ontario, was:

"if the transaction went through the Land Registry office, (even though it wasn't legal), it was a 'done deal'."

Your Credit Card & Bank Statements

Keep them for several years. You may have to prove that you didn't "buy that".

Pre-Approved Dangers

Have you ever received ready made checks from a credit card company or bank, which you do not deal with? These checks have your information on them.

1. shred these checks
2. call the company 25 times, if necessary, to get them to stop doing that.

(**Off Topic:** on the phone, when you are trying to get someone to talk to, I constantly click, 'O', when the message is telling me to "press this, press that". I have had luck getting a,'human being' on the end of the line by constantly punching '0'.)

Mind Blowing Danger

A thief can take over your financial accounts, open new bank accounts, transfer bank balances, and apply for loans, credit cards, and mortgages. They can purchase a vehicle or take a luxury vacation all paid for by you through your bank or your credit card company.

Phone Busters received 11,231 identity theft complaints from consumers in one year, with financial losses of $8.6 million. Trans Union and Equifax receive between 1400 to 1800 complaints per month in Canada alone.

PHONEBUSTERS

What follows is the information given by Phone Busters to educate people. They want to help to prevent I.D. theft and also, help those that have suffered I.D. theft. This is a fantastic organization.

Read on

"Gary Lumsden, of Phone Busters, made it his business to find out about fraud in my small town", reported, Garth S. in Ontario Canada. "He unearthed 42 cases in our sleepy little town in the past year. Information provided by the police."

Just because what I am emailing is Canadian information with lower financial figures doesn't mean that the U.S., Europe, Australia, etc. are not suffering the same losses. With the U.S., being 10 times the population of Canada, just take the figures I heard and multiply them by 10 to get an idea of the theft occurring in the U.S.

The following is my summary of what he said.

The laws are there but individual protection lies in education. "Awareness is the key". These are bad people. They are sociopaths and they don't care about anybody.

I don't want to make people paranoid. But you need to be aware. Fraud by telephone, Internet and mail is a serious international problem.

Phone Busters receives 1200 calls per week, which are passed on, to authorities for investigation.

It's hard to talk to people who have lost their life savings. Gary encourages people to call ahead, when they need information or advice. You don't have to be a victim to call.

Scam artists are well organized and use the latest trends and marketing materials. Gary said that $8 million was skimmed from Canadians alone during the Nigerian scam last year.

A major ongoing deceit is still a lottery scam, which bilked $41 million from unsuspecting victims and cost Canadians $12 million last year. Also be careful of phone solicitations for local charities. They may be legal but only give a small portion of funds to the intended charity. Lumsden said residents should write a check and send it directly to the charity.

Skilled identity thieves use a variety of methods to gain access to an individual's personal identity information. They steal wallets and purses, your mail, go through your trash, or they buy personal information from inside sources. Don't carry your social insurance number. ("For Americans, it's their Social Security Number)".

Be wary of revealing any information on the phone or in person. The thief can open credit card accounts, get phone service or access to bank accounts, all without your knowledge.

Gary said to read your credit card statement and change the PIN number often.

If you do suspect your personal information has been hijacked, take action immediately.

First contact the fraud departments of each of the two major credit card bureaus.

Equifax: 1-877-323-2598
Trans Union: 1-877-525-3823 "

More Places To Contact
www.identityguard.com
www.IdentityTheftShield.com
(services you pay for which checks your credit report daily. There are more.)

Canadian Royal Mounted Police : (RCMP) rcmp-gra.ca

Canadians : www.tuscores.ca to launch an investigation or Trans Union Canada, Consumer Relations Centre, PO Box 338, LCD 1, Hamilton, On, L8L 7W2 905-525-0262

Americans : It's safe and free, to give your social security number by checking your credit once a year at : annualcreditreport.com

Watch Out

I think the next scam could be, getting a call, email or letter, from a source pretending to be any of these bureaus, claiming they need your information. It's you job to ditch the caller and phone Equifax and Trans Union yourself to check it out.

Contact the creditors for any accounts that have been tampered with or opened fraudulently. **CLOSE THOSE ACCOUNTS IMMEDIATELY.**

Carry , the Equifax and Trans Union phone numbers, in your wallet or purse so that if you are away from home you can make the call right on the spot.

Call the police and report it.

To reach Phone Busters call 1-888-495-8501".

Hope this helps

Garth S., Ontario, Canada "

Keep A Written Record

Another good idea came from Cynthia T. in New Mexico.

"I was a victim of identity theft regarding my credit card. My husband and I wrote down everything that happened with the date on all our experiences, all our phone calls and the names of everyone we spoke to. We worked to solve the identity theft we experienced. This really helped with having the credit card company erase the losses and our records helped the police, once they caught the woman."

Thanks for 'listening' "

Cynthia T.

Phone Busters
The National Call Center Combating Telemarketing Fraud
P.O. Box 686 **1-888-495-8501**
www.phonebusters.com

Key Words

A con artist is difficult to detect by looks or voice alone. But you can often spot him or her by their words or expressions, including

- Cash Upfront on the promise they will send or deliver your winnings/prize

- "Secret plans"- Why are you being asked not to tell anyone?

- "Get rich quick" - Any scheme should be carefully investigated.

- "Something for nothing" - A "retired" swindler once said that any time you are promised something for nothing, you usually get nothing

- "Contests" -Make sure they aren't a 'come-on', to draw you into a money-losing scheme

- "Haste" - Be wary of any pressure to act immediately or lose out.

- Friday only" -If something is worthwhile today, it's likely available to-morrow

- "To good to be true" - such a scheme is probably neither good nor true

- "Last chance" - Is it a chance worth taking. Why is it offered on such short notice?

REMEMBER if you have won a prize, it doesn't cost a dime.

With new technology scammers used to call and claim to be your grandson/granddaughter, in trouble, perhaps at a police station or at an accident, asking you to send money quickly, so they can get home.

Older people get 'sucked in', even though the voice sounds different. BUT, today, with new technology, scammers can replicate your young relative's voice. Many seniors heartily believe it's their grandson or granddaughter. They will not believe it's a scammer. It takes a lot to get them to understand that somehow the scammers have duplicated the voice.

Have a password between you and the 'child' and ask for it. Or ask a question only your young relative would know the answer to; such as, where was grandma born?

How To Avoid the Latest Scams Making Headlines in 2023 from Aura.com

READERS : Please Note: We thank Aura for the use of their research. They are a protection company you pay monthly for. The following is what you need to know to-day.

"Kelly Reynolds was relaxing at home when she received a text from her bank asking if she had tried to send money via Zelle. Alarmed, Kelly responded "no" — within seconds, her phone rang, and the caller ID showed "Wells Fargo Fraud Protection."

The agent instructed Kelly to transfer her savings to a new, secure account — but Kelly was skeptical. She quickly did an online search to verify the agent's name and phone number. When everything checked out, Kelly hit "send" for her transfer — and lost her life savings to a scam.

LOSSES

Victims lost nearly $4 billion to cybercriminals in the first half of 2023 alone. But what's even more surprising is that Gen Xers, Millennials, and Gen Zs were more likely than seniors to report losing money to fraud.

Suffering financial loss from fraud, scams, and identity theft is devastating. The ugly truth is that fraudsters are always looking for new ways to scam you. To stay safe, you need to keep up to date with the latest scams going around — and learn how to avoid them.

1**. The "pig butchering" scam** (fake crypto investments)

This year, cybercriminals started playing the long game. In "pig butchering" scams, what begins as a chance online encounter or wrong number text slowly turns into a romance scam.

The fraudster, "fattens the pig," by building trust over time, eventually luring the target into a financial trap — the "butchering" phase, during which the victim loses everything.

An example of a "random" text that starts the pig butchering scam.
Source: Aura
Pig butchering scams are often connected to cryptocurrency, though scammers can use any investment scheme.

How the scam works:

- Scammers reach out via text, social media, or dating websites and start to build a relationship (whether friendly or romantic).
- Eventually, the scammer starts talking about how much money they've earned on their "secret" or "exclusive" cryptocurrency investments.
- They convince their target to try a small investment on their "special" app or platform (which is really just a bogus website that steals the victim's money).
- The scammer makes it look like the investment was successful, and encourages the target to keep investing and earning.

Here's how to stay safe:

Be suspicious of any stranger on the internet who initiates a close personal relationship with you out of the blue. Cut off all contact if someone starts pressuring you into making risky investments, such as via cryptocurrency — especially if they promise "guaranteed" returns.

2. Student loan forgiveness scams

Whenever a government relief program hits the headlines, scammers get to work. One of the most highly-publicized relief initiatives in the past year, to which scammers have flocked, has been President Biden's student loan forgiveness program.

How the scam works:

- Scammers communicate via phone calls or emails. They use generic business names that sound trustworthy, or they pose as federal loan servicers and set up a phony website that looks official.
- They might offer various services, from loan consolidation help to loan forgiveness. They claim they can speed up the loan repayment process or lower monthly payments (for a fee). One recent victim lost $600 to a scam like this one.
- If a target falls for the fraudulent offer, they unwittingly disclose sensitive information to a criminal — including details like their Social Security number (SSN), IDs, financial information, or whatever else the scammer requests on the fake application form.

Here's how to stay safe:

Avoid speaking with anyone who contacts you claiming to be your loan servicer. Instead, hang up the phone and contact your loan servicer directly, using the contact information from your billing statement, the provider's official website, or your own address book.

3. Damaged used cars selling for sky-high prices

Used car prices hit historic highs in 2021 and 2022 — offering huge opportunities for scammers. If you're shopping for a used car, it can be difficult to determine whether it's actually in good condition. Dishonest sellers tamper with the vehicle's identification number (VIN) or car title, or they hide serious issues like water damage that affect the value of the car.

How the scam works:

- In one type of car scam, sellers charge high prices for cars that have endured extensive water damage. Scammers can clean up a flood-damaged car and lie to the buyer about its history.
- Title fraud is another common way that scammers fool unsuspecting buyers. They'll sell a salvage title vehicle for the price of one with a

pristine record by forging or altering the car title document in a way that the buyer doesn't detect.

Here's how to stay safe

Thoroughly inspect the vehicle title, and compare it to a legitimate one to check for signs of forgery.

Beware of cars being sold from out of state or with a recently-issued title. It's also ideal to pick the Department of Motor Vehicles (DMV) as your meet-up location. That way, you can double-check the validity of the vehicle documentation and history, as well as the seller's driver's license information.

4. **Google Voice verification**

One of the most common scams targeting Americans in the past year involves fraudsters trying to gain access to private Google Voice verification codes. If they're successful, they can use your Google Voice number to run scams, break into your other online accounts, or even harvest more information to steal your identity.

How the scam works:

- Fraudsters use social media or online marketplaces to pose as an interested buyer or someone who's found a lost pet. The scammer uses your phone number listed in the ad to start setting up a Google Voice account.

- Next, the scammer tells the target that they're about to send them a verification code for "security reasons." This is a classic double-scam ploy in which the scammer acts as if you're the one who they should be worried about.
- Google automatically sends a private authentication code to the victim's phone number as part of the Google Voice account setup process. When the target shares it, the scammer can begin using a new phone number that isn't connected to their identity.

Here's how to stay safe:

Thankfully, the solution to avoiding this scam is pretty simple: Don't ever share a Google Voice verification code with anyone. It's meant for you and only you, and there's no good reason for anyone else to have it.

5. **Zelle, Venmo, and Cash App scams**

Unlike purchases made directly through your bank account using your credit card or debit card, payment app transactions are usually irreversible. If you accidentally pay a scammer via Zelle, Venmo, or Cash App, it's the same as handing them cash.

Here are some of the most common payment app scams:

- Accidental overpayments. Fraudsters target online sellers by posing as a buyer and "accidentally" overpaying the seller on a payment app by using a stolen credit card. They then request a refund paid directly to their own bank account. But when the actual card owner reports the fraud, the money comes out of your account.
- Fake fraud alerts. Scammers send spoofed text messages that look like your bank's fraud alerts. But when you call the number in the text, you'll be connected to scammers who pressure you to share personal information or transfer your money to a "secure" account (that they control).
- Phishing emails or texts. Hackers create phishing emails or texts that look like they're from Zelle, CashApp, or Venmo. These messages prompt you to click on a link to sign in to your account. But in reality, the link takes you to a fake website that steals your login credentials and gives scammers control of your online accounts.

Here's how to stay safe:

Treat all online transactions like cash, and don't use payment apps for online transactions with strangers. When you get a message that looks like it's coming directly from a payment app company, verify it by first logging in to your account using the official app or website.

6. **Robocalls attempting to steal 2FA codes**

This scam preys on people who hold cryptocurrency in an exchange like Coinbase**.** It offers the promise of helping safeguard the victim's assets — but in reality, it does just the opposite.

How the scam works:

- You get a robocall claiming to be from the fraud prevention department of your cryptocurrency exchange. It claims there's an unauthorized charge on your account.

- The automated call asks you to "verify" your identity by entering a two-factor authentication (2FA) code that's been sent to your phone.
- Behind the scenes, a scammer has hacked into your account and needs only this code to gain complete access to your assets. If you share the code, the scammer will take over your account and drain it.

Don't get scammed! Here's how to stay safe:

Never share two-factor authentication codes with anyone for any reason, even if the situation seems legitimate. No cryptocurrency exchange will ever call and ask for your password or 2FA code.

7. **Job scams** (work-from-home scams)

A common COVID-19 scam involves fake job postings for lucrative work-from-home jobs. In these schemes, fraudsters pose as recruiters and fool victims into providing personal information or sending money to pay for "supplies and training."

According to the Federal Trade Commission (FTC), Americans lost a collective $68 million to employment scams during the first quarter of 2022

How the scam works:

- Fraudsters create fake job listings that offer attention-grabbing perks. Scammers impersonate recruiters or employers, and reach out directly to users on job websites like LinkedIn.
- When someone accepts the job, scammers collect sensitive information like the victim's credit card numbers or account information, Social Security numbers (SSNs), and other sensitive documents that can be used to commit identity theft.

- Victims of job scams are often prompted to make payments for expenses like job training or supplies — requests that a legitimate company would never make.

Here's how to stay safe:

- Do your research before getting too far into the interview process with a potential employer. Search for the name of the business or recruiting company on the Better Business Bureau (BBB), as well as on job rating and review websites like Glassdoor.

Finally, never give a recruiter your personal or financial information via email, text message, or phone call.

8. **Amazon impostor emails, calls, texts, and more**

Of all the well-known businesses out there, Amazon inspires the largest number of impostor scams. Since it's a powerhouse online retailer with a vast customer base, most people won't think twice when they receive a communication that looks like it's from Amazon.

Amazon is the most impersonated brand by scammers. Source: FTC

How the scam works:

- Fraudsters create phishing emails or texts that impersonate Amazon customer service agents or include security alerts. They fool targets into responding or clicking on malicious links that infect their devices with invasive malware.
- Amazon phone scams convince victims to share personally identifiable information (PII) over the phone or make payments to resolve a fake issue or bogus security concern.
- Some internet criminals create Amazon lookalike websites (that trick people into entering their payment information) or bait their targets by sending fake Amazon invoice emails for items that they didn't purchase.

Here's how to stay safe:

Ignore unsolicited emails or text messages from Amazon, and never use the links or phone numbers they include. If you have any concerns about your account or order history, navigate directly to your Amazon app or the official Amazon website, and call the customer service phone number to get answers.

9**. Crypto "recovery" scams** (and other refund scams)

This popular scam targets people who have already lost money in a cryptocurrency scam. Fake crypto recovery services promise a quick fix to the devastating loss — but the only result is more money lost in a scam tailored to prey on previous victims.

How the scam works:

- After falling victim to a cryptocurrency scam, you share your story online to warn others or look for solutions.

- Someone reaches out over social media or in the comments section of your post and claims to be able to recover stolen cryptocurrency. To process your "refund," they'll ask you to pay an upfront fee (then disappear with your money) or request sensitive information that gives them access to your crypto wallet.

Here's how to stay safe:

If you've lost cryptocurrency in a scam, it's essentially impossible to get it back. Ignore messages from anyone who claims to be able to get a refund. They will only scam you out of more money.

10. Tech support scams that gain remote access to your computer

Scammers know that most people are afraid of getting hacked or having their computer or phone infected with viruses. In this scam, they trick you into thinking your device has been compromised and then pressure you into downloading software that gives them remote access to your computer.

How the scam works:

- Scammers send an alarming phishing email, text message, or even pop-up ad declaring that your device has been hacked or infected.
- The tech support phone number provided in the alert is a direct line to the scammer. Once they get you on the phone, they request remote access to your device in order to "fix" the nonexistent problem.
- When they gain access, they install invasive malware, spyware, or even ransomware onto your device. They can also use hacking techniques to steal sensitive data from your hard drive — such as personal and financial information, usernames, and passwords.

Here's how to stay safe:

If you get a troubling message from a tech support team, don't click on links or respond via any contact information listed in the message. Contact Apple, Microsoft, or your antivirus provider by using their official websites or phone numbers.

11. **Rental apartment and home scams**

With more Americans moving because of the pandemic, fraudsters have created new ways to scam renters. Scammers create fake listings and duplicate ads, and then steal money for deposits or "fees."

In one example, a family from North Carolina replied to a rental listing and paid their first month's rent — only to arrive at the location and discover that the home was never actually for rent.

How the scam works:

- Scammers create fraudulent home or apartment listings depicting photos of a rental unit that doesn't belong to them. They keep the listing prices below market rates to attract attention from potential renters.
- When apartment hunters show interest, the scammer tries to get them to make a payment before meeting up or seeing the unit in person.
- The scammer disappears once the payment goes through, leaving the victim to discover that they don't have a new place to live after all.

Here's how to stay safe:

Avoid listings that look too good to be true. Always insist on an in-person meetup and tour of the unit, and don't make any payments beforehand (or before signing a lease agreement). Finally, never agree to use nontraditional payment methods like wire transfers or payment apps.

12. **Fraudsters using your friends' online accounts to scam you**

If any of your personal contacts fall victim to account takeover fraud or a data breach, you might get a strange request from someone you think you know. In reality, it's a hacker impersonating your friends or family members by using their personal accounts or spoofing their social media profiles.

One woman from California recently lost hundreds of dollars after a "friend" on Facebook convinced her to sign up for a special program with amazing benefits.

How the scam works:

- Fraudsters hack into or copy your friend's social media account, email address, phone number, or even payment app platform.
- They reach out via social media, email, text message, or direct message, pretending to be the account owner. They ask you to send them money or gift cards to help them out of a tight situation.

- **Here's how to stay safe:**
- If someone you know is acting pushy or asking for money out of the blue, never take it at face value. Don't click on links or continue the conversation — instead, try either calling them directly or contacting them on a different platform.

- **How To Spot a Scammer in 2023**
- Although online scams are getting more sophisticated every year, most online con artists recycle the same social engineering strategies repeatedly. With enough information and vigilance, you'll be able to recognize new scams that you've never seen before.

Here are the most common red flags to look out for:

- A strong sense of urgency. Scammers fabricate high-pressure situations like time-sensitive security alerts, urgent messages, or a limited-time offer for an amazing sweepstakes prize. These scams are designed to make you feel rushed and stressed out. The moment you feel that pressure, take a step back and reevaluate.
- Threats or scare tactics. Scammers often use fear to get you to act. They may call pretending to be law enforcement and threaten arrest, deportation, cancellation of your Social Security number, or some other dramatic consequence. Legitimate government agencies don't do this.
- government agencies don't do this.
- Sob stories and excuses. Whether you're buying and selling online, trying to find an apartment to rent, or looking for companionship on a dating platform, beware of anyone who uses a sob story or excuse to ask for money, avoid meeting in person, or request nontraditional payment methods for a purchase. They're probably trying to win your sympathy so they can swindle you.

- Calls or messages from authoritative or trustworthy organizations. The sooner scammers can establish trust or claim authority, the faster they can steal from you. They impersonate representatives from your credit card company, a well-known organization like Google or Microsoft, or a government agency like the IRS or Medicare.

- Don't give away any information or click on links before verifying the source elsewhere. Asking for sensitive information. It's not common practice for a legitimate agency or business to contact you out of the

blue and request sensitive personal details or have you "confirm" payment information — but this is the bread and butter for all kinds of phishing scams.

-
- Insisting on nontraditional payment methods. Using payment apps, gift cards, or wire transfers as payment for an online transaction with a stranger is extremely risky. Scammers prefer these payment methods because they're immediate, irreversible, and lack the security of transactions made via credit and debit card.

Don't Become a Victim: Here's How To Protect Yourself From Scammers

There are few worse feelings than realizing you've been the victim of a scam. But fraudsters in 2023 know that your personal information can be even more valuable than money.

Don't wait for scammers to pounce. You can significantly reduce your chances of being victimized by a scam — but you have to think proactively. Here's what to do:

- Freeze your credit with all three credit bureaus (Experian, Equifax, and TransUnion). A proactive credit freeze is an easy way to prevent fraudsters from opening up new lines of credit or accounts in your name.
- Update your passwords, and enable two-factor authentication (2FA) whenever possible. Visit the settings menu in all of your accounts and apps, and choose the most secure options. Use a password manager to generate and store secure passwords.

- Learn to recognize the signs of a phishing email, text message, or phone call.
- Don't refund overpayments. "Accidental" overpayments indicate a scam. Instead of issuing a refund, cut off contact and wait for the fraudulent payment to disappear (since the scammer never really sent you money in the first place).
- Register your phone number on the FTC's Do Not Call registry (donotcall.gov). This could lower the amount of spam and robocalls you receive.

For peace of mind, consider signing up for identity theft protection.

Even the best efforts get thwarted sometimes. Aura's comprehensive plan extends beyond identity theft protection and provides overall fraud prevention, digital security, and financial and credit monitoring.

Plus, if the worst should happen, every adult member on an Aura plan is covered for up to $1,000,000 in insurance for eligible losses due to identity theft.

We do not promote AURA. You need to investigate any protection agency for yourself to see if they are a 'fit' for you. Aura provided good information.

You are the best person to look after you.

Fabulous Retired Baby Boomers, Junior Seniors and Senior Seniors

Ya'owsers! "We", that is the team here at Fantastic Retirement and tons of contributing retirees, worldwide, together, have produced:
The website : www.FantasticRetirement.com
The YouTube Channel : Eleanor Rose
A Blog
7 books

Please keep your identity theft and scam experiences coming. Send them to

FantasticRetirement@gmail.com

When you share your story with us you are agreeing to the use of your words in any of our following formats: ebook, book, website, blog, Newsletter, YouTube Channel or article for sale or for free. You know, as fellow retirees, we will treat your story as our own, with dignity and appreciation.

Also remember that we never share full names or addresses. An example:

Susan D. Texas

If you agree with our premise: sharing Fabulous Retirement with the world and educating people about how fulfilling retirement can be;

Another Retirement Request

Notice below, all the books we have at

www.FantasticRetirement.com.

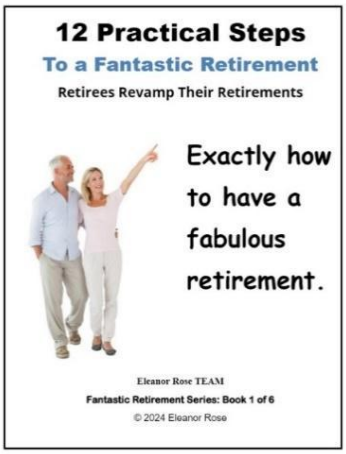
- If you are not sure how to upgrade your retirement or
- you simply want to read how other retirees are spending their time
- buy one of the following books.

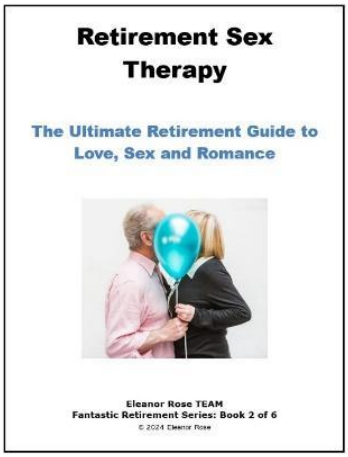
They are full of great things to do in retirement. They range from funny, to endearing to enlightening. You'll love them. Retirees have nothing, 'to lose'. **They tell the truth.**

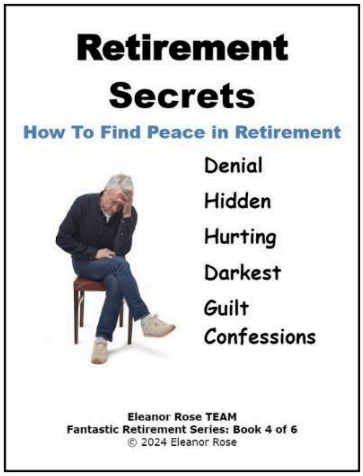
Or, Grab one of the other free book, Live a Lot Longer which is also filled with retirees sharing their health successes.

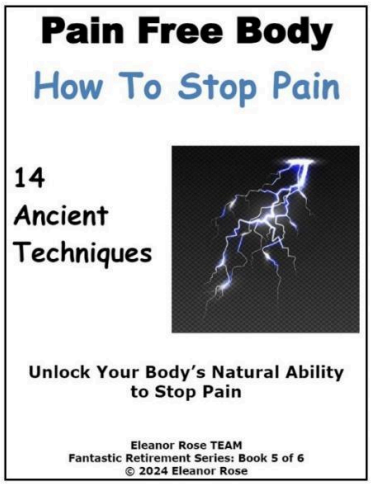
The Eleanor Rose TEAM

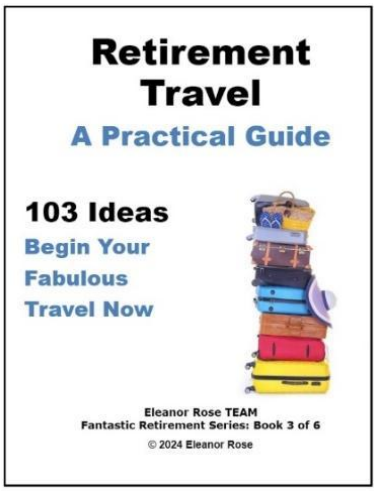
FREE






Retirement Secrets
How To Find Peace in Retirement
Denial
Hidden
Hurting
Darkest
Guilt
Confessions
Eleanor Rose TEAM
Fantastic Retirement Series: Book 4 of 6
© 2024 Eleanor Rose


Pain Free Body
How To Stop Pain
14
Ancient
Techniques
Unlock Your Body's Natural Ability to Stop Pain
Eleanor Rose TEAM
Fantastic Retirement Series: Book 5 of 6
© 2024 Eleanor Rose


Retirement Travel
A Practical Guide
103 Ideas
Begin Your
Fabulous
Travel Now
Eleanor Rose TEAM
Fantastic Retirement Series: Book 3 of 6
© 2024 Eleanor Rose