

**Handbook
On
Fraud
Prevention**

**For Use in
Protecting Your
Identity and Money**

Assembled and Edited

**by
Peter Eckhoff
NC NARFE
Website Editor**

Copyrighted 2021 by Peter Eckhoff

If this helps some potential victim, feel free to use it without compensation. A reference citing this publication would be appreciated.

Acknowledgement

I want to thank Dwight Weaver for the basic outline of this Handbook. Both he and Henry Brattlie provided many examples of various types of scam and phishing emails used here within. Dwight also contributed with discussions on various topics and content. Charles Talley provided an important News Release. On the other end, I want to thank Dave Phillips and Vilma Geisert for their recommended edits; especially Vilma who demonstrated how much I had forgotten about English grammar and punctuation. I also want to acknowledge the moral support of Robert Allen and Tom Jennings. Thank you all!!

Disclaimer

Please read this disclaimer carefully before reading and acting upon any content of this handbook. NARFE¹, NCNARFE², and any affiliates are not responsible for its content.

All information herein is for educational and informational purposes only. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this handbook and its links, you do so at your own risk.

While the information in this handbook has been verified, to the best of our abilities, we cannot guarantee there are no mistakes, errors, misinterpretations, omissions, or changes to referenced material or websites, etc.

We reserve the right to edit this handbook at any given time. It is up to the user to obtain the latest edition.

Disclosure

This Handbook was assembled and edited by reputable people who are not professional with regard to security issues, but have an intrinsic interest in keeping you and your self-interests safe, as they would themselves, family, friends, and valued acquaintances. This information was gleaned from various sources that are considered reputable. It is in all our interests to find good information, digest it, and apply it to our interactions. We are striving to present this information in a form that should be readily usable. We hope this helps in any searches that you do to verify this information and act upon it.

¹ NARFE is the National Active and Retired Federal Employees Association.

² NCNARFE is the North Carolina Federation of NARFE.

Introduction

Unsolicited phone calls and online fraud whether it be annoying ads, solicitations, or down right fraudulent scams and intrusions are becoming all too common and attempts are proliferating. If we are not careful or we do not know what to look out for and to listen for signs of potential wrongdoing, we can easily become victims. We want you and your finances to be safe whether it is answering your telephone or whenever you are online.

Just to reiterate, this is not an end all to end all handbooks on keeping you and your finances safe. It is a handbook that can assist you in getting started in learning how to recognize and to protect yourself and self-interests from some of the more common frauds. It is up to you to educate yourself and to become cognizant of possible perils. As my teachers used to say: "Do your homework!!"

The basic format of this handbook explains how some scams operate, what to look or listen for, and then what to do to keep you and your self-interests safe.

Table of Contents

Acknowledgement	2
Disclaimer	2
Disclosure	2
Introduction	3
Acronyms & Terms	4
General Actions to Take	6
Robocalls	8
Email based Scams and Phishing	10
Fraudulent Text Messages	13
Wire Transfers/Cash Shipments	15
2 Factor Authentication	17
On Social Media	18
Credit Reports & Freezes (Credit Locks)	20
Credit Cards & Bank Accounts	22
Credit Cards	22
Banking	23
When Using Your Computer	25
Epilogue	29
Appendix	30
A-1 Reporting Robocalls Does Work	30
A-2 Examples of Email Scams and Phishing Attempts	33
Notes	Second to Last Pages
NARFE Application	Last Pages

Acronyms & Terms

2FA – stands for 2 Factor Authentication; a method of verifying it is you, with a code sent to your phone or email address. The sent code you receive is entered on the web site in order for you to continue on.

Credit Freeze a method used to deny access to your credit reports, thus diminishing the chances of a fraudster generating credit unbeknownst to you, using your personal data for which you may become responsible.

Gift cards (Pre-loaded Debit Cards) look like credit cards and work in a similar fashion. They have a credit card like account numbers on the back next to a plastic medium (protective sticker) concealing a “PIN number”.

Identity Theft – where someone pretends to be you and tries to obtain cash, a loan, line of credit, etc. They likely have illegally obtained documents bearing your name.

Malware – a term that covers various forms of harmful software installed or attempted to be installed on a person’s computer.

NARFE - an acronym that stands for the National Active and Retired Federal Employees Association

NCNARFE - an acronym that stands for the North Carolina Federation of NARFE.

Phishing (Pronounced: fishing – like the sport) - A phishing attack occurs when someone tries to trick you into sharing personal information online or to send access codes guarding money such as gift card numbers using a ruse.

Robocalls – automated telephone calls

Wire Transfer - If you see these two words: “wire transfer” in any email, highly suspect a fraudster wanting you to transfer your money from your bank to the fraudster’s bank.

General Actions to Take:

1. Be suspicious of any email or telephone call that asks you for money or says you have won something; especially when the sender asks for personal information.
 - a. Verify that the name of the email sender is the same as the actual email address. Most scammers will use the name of someone you know but will **not** have the correct **reply** email address.
 - b. Block the telephone number and email address of a scammer.
 - c. Pay close attention to grammar in any email you receive that was supposedly from a legitimate company. Legitimate companies will use proper grammar and complete sentences.
2. Enable two-factor authentication on any online account that you have, especially your retirement accounts, Facebook, credit card(s), and bank accounts.
3. Set transaction dollar thresholds that give you automatic notice if a banking transaction or credit charge exceeds the threshold amount you selected.
 - a. A rule of thumb: Ask your bank to notify you by email of any check that clears.
 - b. Use online banking if you are comfortable with your computer skills.
4. Do not sign the back of your credit cards. Endorse them with "Ask for Photo ID".
5. The IRS, Social Security Administration, state agencies, banks, and credit card companies will not call you on the telephone about a problem. they will send you a letter. So,
 - a. Do not panic if someone tells you on the phone that the IRS is going to have you arrested.
 - b. Do not try to outsmart the caller; get off the phone as quickly as possible.
 - c. Verify with the authenticity of an unusual request with the company or agency that supposedly sent it.
 - d. If you receive a suspicious looking letter, look up a customer service telephone number online and use that number to verify the letter is legitimate. Do not use the number provided in the letter.
6. Guard your Social Security Number, retirement account information, credit card numbers and codes, and bank account information.

7. Purchase a credit reporting service account and lock your credit files. You can unlock them when you need to do so, but you will receive notice if someone else tries to run a credit report on you that you were not aware of in advance. Some of these can be subscribed to through your bank or credit card at a reduced rate.
8. Buy and install a robust computer security system that provides Virus Checking, File Scanning, a Virtual Private Network, and ???.
 - a. Avast, Norton, McAfee are all reputable.
 - b. Malwarebytes has a freebie version that is helpful for detecting various types of Malware.

Robocalls

What are they?

Robocalls are those annoying telephone calls asking you if you want to sell your home, apply for medical insurance, answer a survey or poll, scare you into panicking, thinking the call is from the IRS or Social Security with them wanting to ding you, arrest you, etc. or claiming that they are from Microsoft and that you have a computer virus or problem and they need to get into your system to fix it, etc. - for a fee. This is ****NOT**** how these legitimate organizations operate. These calls can be highly automated and even emulate human responses.

How to react?

1.) If you have a cell phone, don't answer your cell phone if an unrecognizable number appears. Let it go to voice mail. If you do answer and it is a fraudulent call, it tells the fraudster that it's an operable number and a person answers the call to hear a message. Expect more calls.

2.) If you do answer the phone and it is a Robocall, do ****not**** say "YES" to any question. The word "YES" can be recorded by the robocaller, manipulated electronically, and used to say you authorized the fraudulent charges appearing on one of your accounts. Here is some more information on this subject:

<https://www.ag.state.mn.us/Consumer/Publications/CanYouHearMe.asp>

3.) Do not press any buttons to "remove your phone number from their list". (Note: I hear this every time and I'm on the DoNotCall list. They are not supposed to call me PERIOD!!) Ask yourself, if you are on the DoNotCall list, why are they calling you in the first place?

Before the next Robocaller calls and you are not on the DoNotCall list, add your telephone number to the Federal Governments DoNotCall list:

<https://www.donotcall.gov/register.html>

While this may seem "useless", it does work and can strengthen any complaint you lodge against the caller. See Appendix 1 news release.

What To Do?

Hang up and report the call to:

Federal: <https://www.donotcall.gov/report.html>

NC State: <https://ncdoj.gov/report-robocalls/>

OR use the

NC State Robocall Hotline: (844)-8-NO-ROBO -> (844) 866-7626

The O's above are not Zeros

These complaints do work, although slowly (See Appendix 1).

Learn More About Telemarketing Scams & Do Not Call Registry:

NC State: (and contains a LOT of Information on various scams)

<https://ncdoj.gov/protecting-consumers/telephones-telemarketing/telemarketing-do-not-call/>

Email Based Scams and Phishing

What to look for:

The simplest answer is a question:

- 1.) Are they hitting me up to spend or give away my money? In other words,
- 2.) Will this lead to me spending my money or divulging personal information?

If the answer is “yes” to either one, expect a scam or a phishing attempt.

Note: NO ONE from NARFE will ask you to buy gift cards or ask you to transfer your money for any task!!! The email from a NARFE officer asking you to do so is fake.

Here is an example of the beginning of a phishing attempt:

Request

1 message

Carolyn C. Example <ccexample@att.net>

Mon, Mar 26, 2018 at 12:24 PM

Reply-To: "Carolyn C. Example" <presidentoffice2018@gmail.com>

To: Peter@anyisp.com

Peter,

Are you in the office? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

Thanks,
Carolyn C. Example

Tip offs to a scam email:

- 1.) In the example above, note the correct From address: ccexample@att.net does not agree with the Reply-To address: presidentoffice1234@gmail.com

This is a dead giveaway that this is a scam email.

- 2.) The word “Wire Transfer” is in the body of this request is a major RED FLAG. It could have been “Gift Cards”, “Personal Check”, “Credit or Debit

Card”, or other means of transferring money from a personal account to a fraudsters. This is a “Phishing Attempt” and needs to be reported.

3.) Carol C. ****knows**** I am retired and have not been in an office setting close to 8 years. - Another tip off.

4.) Never, ever reply with threats, etc. The fraudster will know they got your goat and will have a good laugh. Why? You don’t know their street address and they maybe halfway around the world (or just down the block). Leave it to the professionals to fight this battle. Report the email!! You’ll feel better.

What to do:

If in doubt about the authenticity of an email, contact the legitimate sender but not through the suspicious email. There is no rush. Take your time to verify. Fraudsters want you to “rush” and if they can cause you to “panic”, they’ve won.

If you have received a scam or phishing email or text message, report it. The information you give will help fight these fraudsters.

Step 1. If you receive a phishing email (most scam emails lead to phishing), forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.

Step 2. Report the phishing attack to the FTC at ftc.gov/complaint.

And to the North Carolina at 1-877-5-NO-SCAM or (919) 716-6000 or <https://ncdoj.gov/internet-safety/phishing/>

Step 3. Some email services such as Gmail have buttons and links to where you can automatically report the scam or phishing email to them. Some services may even detect that an email **might be** dangerous and warn you. Find out if your intended email service has such warning and reporting systems implemented. You can search on, and using Gmail as an example,

Search: Gmail report phishing email:

<https://support.google.com/mail/answer/8253?hl=en>

With such flagging, Gmail can look for other such messages and stop them.

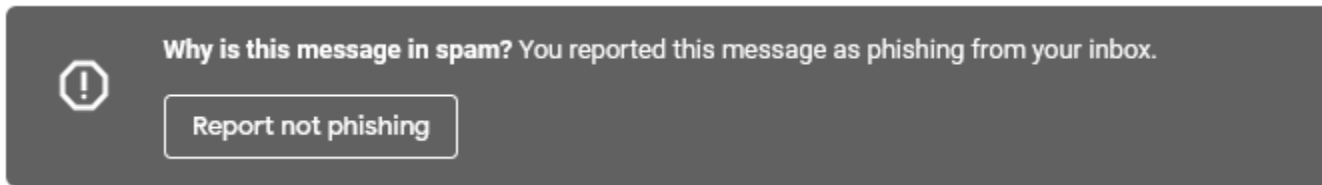
Here are some examples of Gmail warning messages:



This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

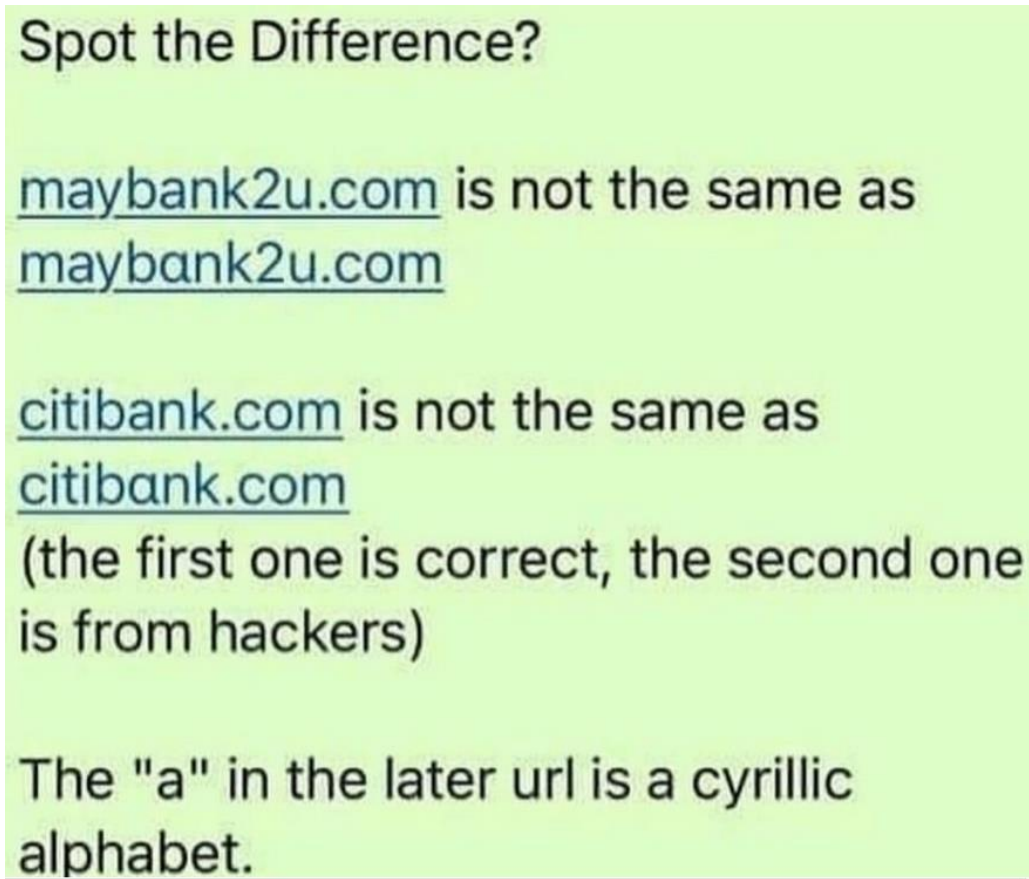
Looks safe ?



Why is this message in spam? You reported this message as phishing from your inbox.

Report not phishing

Be wary of emails from “your bank”.



Spot the Difference?

maybank2u.com is not the same as maybank2u.com

citibank.com is not the same as citibank.com
(the first one is correct, the second one is from hackers)

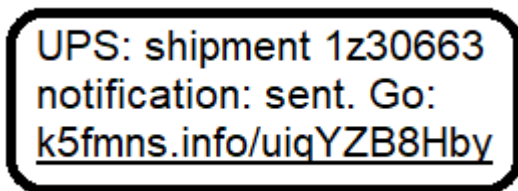
The "a" in the later url is a cyrillic alphabet.

Fraudulent Text Messages:

What are they?

These are messages sent to a person's smartphone that has text messaging (SMS/MMS) activated. The message appears to come from a legitimate source such as UPS in the example below and contains a link. **DO NOT CLICK ON THE LINK** before determining if it is from a legitimate source.

Here's an example:



1.) The UPS, United Parcel Service, looks legitimate but the underlined link is not. It does not have a UPS link address. **DO NOT CLICK ON THE LINK.** It puts you in contact with the fraudster. The service identifier inserted by the fraudster could have the name "Amazon", "USPS", "DHL", or any one of a myriads of companies that are of themselves legitimate but they did not send the message.

2.) Also, where you expecting a package? If not, this is another giveaway that it may be a scam, most likely a phishing attempt.

What to do?

This needs to be forwarded to SPAM (7726) but how do you do forwarding of text messages such as this? Each Smartphone operating system has its own methods. These methods can be found by doing an online search by entering a search engine with the operating system name such as ios, android, blackberry, etc. followed by the words "text forwarding". Links to instructions will appear at the top of your search results list.

For ios (the Apple Computer Smartphone operating system), this produces a link to: <https://support.apple.com/en-us/HT208386> which explains how to set up and forward your (SMS/MMS) text messages. The instructions are straight forward and easy.

For an Android Smartphone operating systems, substitute “Android” for “ios” and conduct a search for steps on how to forward a text message. This is one result that may work for you:

<https://www.androidauthority.com/how-to-forward-a-text-message-870759/>

Wire Transfers/Cash Shipments

What are they:

Wire Transfers are the electronic version of shipping cash. This is where you have your bank send money electronically from your personal account to another account at another bank and that bank can be anywhere in the world.

The most important thing for consumers to remember is this:

!!! Never wire money to someone you haven't known for a long time !!!

Fraudsters love wire transfers and/or cash shipments!!! This is one of the hallmarks of a scam.

Here is a link to more information:

<https://www.atg.wa.gov/wire-transfer-scams>

<https://ncdoj.gov/download/16/general-information/15645/scams-booklet-2-10-2017>

What to do?

If you did ship cash, call the shipping company right away to see if they can stop the shipment. Having a tracking number is helpful. Time is of the essence.

If you have wired money to a scam artist, call the money transfer company immediately to report the fraud and file a complaint. For MoneyGram, call **(800-926-9400)** or for Western Union, call **(800-448-1492)**. Ask for the money transfer to be reversed. Western Union has stated: “. If the *funds* haven't been picked up by the receiver, you'll get a full refund, including the transaction fee.” Then file a complaint with the FTC: [ftc.gov/complaint](https://www.ftc.gov/complaint)

MoneyGram link to instructions for reporting fraud and possibly stopping the transfer and then types of frauds:

<https://www.moneygram.com/mgo/us/en/help/contact>

Clicking on the Report Fraud button brings up the (800-926-9400) telephone number shown above.

Descriptions of common scams involving money can be found here:

<https://www.moneygram.com/mgo/us/en/help/fraud-aware/common-consumer-scams>

Western Union has a link to instructions for reporting fraud and possibly stopping the transfer. They too describe types of frauds:

<https://www.westernunion.com/us/en/fraudawareness/fraud-report-fraud.html>

For bank-to-bank wire transfers:

This is general advice I have found on the internet:

1.) Contact your bank immediately. You may have to initiate a “SWIFT recall“ on the wire transfer that may have left your account. Some banks schedule sending the transfers later in the evening. You may have time to stop the transfer if you act quickly. Know how to contact the bank involved and also how to contact them after normal banking hours. It may not be for you but for an unawares family member or friend.

2.) Contact all banks that may have also received your funds.

There are other steps that can help and your bank should be able to help you through all this. There are some additional details in this link:

<https://certifid.com/how-to-recover-from-wire-fraud/>

2 Factor Authentication (2FA)

What is it?

When we log into a web site with a User ID and Password, there is a possibility that our log in credentials have been compromised. Because such compromises have taken place, our banks, financial institutions, medical providers and other institutions that have a fiduciary and/or legal responsibility to protect our accounts and data, they have instituted a secondary verification system called 2 Factor Authentication (2FA).

This is where, after entering your User ID and password, that institution will send a code to you via a text message to your smartphone or an email to your email address or both. You then receive that code and enter it into a window that appears after your log in. Once confirmed, that institution allows you to continue into your account or data. More detailed information can be found here:

<https://authy.com/what-is-2fa/>

What to do?

Most financial based institutions will prompt you to activate 2FA . It is rather easy to do and the instructions are not difficult. They will ask you where you want your 2FA code to be sent. Often the selection is an email account or a cell phone number with texting (SMS/MMS) enabled. If you will be away from access to your email account, sending a code to your cell phone may be best.

You can do an internet search on how to enable texting (SMS/MMS). Here's an example for an Apple iPhone:

Search on: iPhone enable texting

This was the first result:

<https://support.apple.com/guide/iphone/set-up-messages-iph3d039b67/ios>

On Social Media

What is it?

Social Media is a term that categorizes the services of various companies such as Facebook, Twitter, Instagram, Dropbox, etc. These companies allow users to create accounts for areas the account holder “controls”. These companies set their own rules and the account holder operates under those rules. An account holder can post content to their area and invite friends and acquaintances to the same. The content of an area can contain personal data, schedules, ideas, jokes, pictures, recipes, and just about anything that comes to mind. In other words, the account holder can be social with their friends and acquaintances and can restrict access to all others.

Whatever you post on a Social Media site is often available to the world to look at and read. It is a way of being social with groups of people like friends and families but it also a source of information that fraudsters, thieves, and other nefarious people can use your information against you.

What to do?

- 1.) Realize that the world can possibly see everything you are posting. So, do not post anything you don't want the world to see.
- 2.) As an account holder and if the social media company implements it, enable 2 Factor Authentication. Use of just user ids and passwords is not as safe
- 3) Monitor logins to your account. You want to know where and when someone logged on to your account as well as what was posted.
- 4) To deny fraudsters access to potentially damaging information about you and your friends and acquaintances, limit the ability to view your data to only those who you allow into your area.
- 5) Learn how to perform routine security checks.
- 6.) Report all who pretend to be someone else (i.e., a Facebook Friend Request from someone who is already a Friend.)
- 7.) Do not open videos from a friend who has never sent you a video before.

Here are some further references:

<https://www.facebook.com/help/122006714548814>

<https://help.twitter.com/en/safety-and-security>

search on: “Company name” safety security

where “Company name” is the name of the social media company such as Facebook, Twitter, Dropbox, Instagram, etc.

Credit Reports and Freezes (Credit Locks)

What are Credit Reports?

From: <https://www.transunion.com/credit-reporting-agencies>

“Credit reporting agencies (also known as credit bureaus or consumer reporting agencies) that collect information relevant to your credit and financial history. There are three credit agencies: TransUnion, Equifax, and Experian. When you apply for a loan, request an increase on your credit limit or even apply for a new job, your credit report will likely come into play. The three credit agencies collect and house the information that helps potential lenders or employers rate your reliability. “

Here is an additional sources that can help you understand Credit Reports:

<https://www.equifax.com/personal/understanding-credit/>

What is a Credit Freeze or Security Freeze?

All three credit reporting agencies use similar terms to describe the process where you can deny access to your credit report. This is particularly useful in stopping Identity Theft where someone other than you, tries to obtain credit or money pretending to be you.

From Equifax:

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

From Experian:

<https://www.experian.com/freeze/center.html>

From Transunion:

<https://www.transunion.com/credit-freeze>

Also, not all vendors report to all three credit agencies. This means that the information on your credit report can vary from agency to agency, resulting in

different scores. It is wise to periodically review your credit reports from ****all**** three reporting agencies at least once a year.

Credit Cards and Banking

Credit Cards

What are they?

Banks and lending institutions can create a line of credit for a worthy (or not so worthy) applicant and when the application is approved, a credit card is issued and sent to the applicant most often with a set limit and an interest rate dependent upon the credit worthiness of the applicant.

The card itself will have a 16 digit account code, the applicant's name, and a month/year expiration date on the front. On the back will be an area for your signature (**but don't sign it**), a 3 or 4 digit Card Verification Code (CVC), and generally additional information for contacting Customer Service. Most are now issued with a "chip" that can be read when inserted into a credit card reader.

What to do?

- 1.) When you receive your card, sign the back signature block area with "Ask for Photo ID" and then activate your card. If your card is stolen, it will make it harder for a thief to use it.
- 2.) If your card is stolen, you will need to contact the issuing bank or lending institution immediately. The telephone number to their Customer Service is on the back of the card. It would be wise to have that number on a separate piece of paper. Also, the sooner the notification, the sooner a new card can be sent.
- 3.) Advise your credit card company when you are traveling. This will help prevent denial of purchases when abroad and the credit card company thinks you are at home.
- 4.) Understand cosigning before initiating a cosigning agreement.
- 5.) Find out about fraud protection calls
- 6.) Debt settlement companies pay a lot of money to advertise services that "the creditors don't want you to know about." These commercials often make it seem like they have a secret, quick-fix solution that can have you out of debt

today. But they aren't exactly up front about the effects of debt settlement and the process you go through to settle.

7.) Ask for an email or text to be sent when a charge exceeds your threshold amount and for all credit card charges where the card is not present.

8.) The Card Verification Code (CVC) number is a way for the seller to know that you have the card in your possession. Be careful of who you give it out to.

Here is a link to credit card do's and don'ts:

<https://www.consolidatedcredit.org/how-to-use-a-credit-card/dos-and-donts/>

Banking

What is it?

It is a method of storing your money for savings and transactions. A bank is set up to facilitate these methods. With the internet, you can open up a savings and/or a checking account without ever meeting with a banker or bank representative face to face. In such cases, all transactions and movement of money is done over the internet. Deposits can be done by taking a picture of the check to be deposited with a smartphone and emailing that picture to the bank's email address for such types of activities. Needless to say, you want your activities to be secure.

What to do?

- 1.) When opening up an account or applying for a loan, you will need to unlock your credit files. Once approved, relock those files.
- 2.) In addition to creating a User ID and setting a password, enable 2 Factor Authentication. Make sure your passwords is "strong" and not easily guessed.
- 3.) Set transaction dollar thresholds for your account(s).
- 4.) Ask for an email or text when a charge exceeds your threshold amount(s).

- 5.) Set up email and/or text notices for all deposits, check clearings, and notifications.
- 6.) Learn as much as you can about securing your accounts and while you are at it, today's smartphones need to be passcode protected; especially where you can start your car from one, do banking, and have a lot of personal information stored on them.
- 7.) Learn from the bank how you can protect your accounts.
- 8.) Stay away from using public WiFi. Not all WiFi's are secure.
- 9.) When connecting to a bank, make sure the URL starts with https (http with an added "s") and not http (http without an "s") before sending your user ID and password or any information that needs to be secure. The "s" stands for "secure" and your data transmission is encrypted.
- 10.) Learn what secure practices your bank recommends.

Additional information and details:

<https://www.discover.com/online-banking/banking-topics/10-ways-to-protect-your-checking-account/>

<https://www.forbes.com/advisor/banking/how-to-protect-your-online-banking-information/>

When Using Your Computer

What is a Computer?

In the very simplest term, it is an electronic device used to process data and commands. Externally, it contains a keyboard, mouse, monitor, and a case that internally contains a motherboard, RAM memory, hard drive, and Central Processing Unit (CPU - sometimes with a fan and/or heat sink). A speaker set and microphone can be attached to the case.

What to do?

This is not an easy section to write. Many of you reading this have different skill levels and it is hard to write to everyone's level.

There are a myriad of things you can do to keep your computer from being hacked and many things you can and many things you should not do when on the internet (online). We've covered some of these items already.

From here, I am going to assume that you have your system up and running, have your computer connected to a computer modem or router, you have read up on how all your components work, are using user ids with strong passwords, and you can bring up a browser such as Edge, Firefox, Chrome, Safari, etc. and can perform a search.

Online, there is a place called Wikipedia which is akin to an online encyclopedia. If you do a search for computer terms, I would start off with the word: "wiki". Here is a link and a good place to start:

<https://en.wikipedia.org/wiki/Computer> You can extend your knowledge using a web browser and search using string of words such as:

wiki what is a computer

wiki what is a computer hard drive

wiki what is a computer modem

You can search on such topics as:

wiki how to secure a modem

wiki how to secure a router

While wiki has its critics, there is a lot of good material and references there.

Once you feel comfortable enough with your system and how it operates, it's time to really look into protecting it from natural and online hazards.

1.) All systems should be on an electric surge protected power strip to protect your system from the surge of say lightning strikes or an Uninterruptable Power Supply (UPS) that can keep your system up and running on a battery while you save important work before shutting down due to loss of electricity.

<https://www.cdw.com/content/cdw/en/articles/datacenter/2018/11/30/ups-vs-surge-protector.html>

2.) Purchase good antivirus software. There are a number of known publishers that have good track records. There are also several reviews online from which to gauge their effectiveness. Just don't go with one review from one site. Read several reviews. Here is an example of one review:

<https://www.safetydetectives.com/blog/windows-defender-vs-antiviruses-is-defender-enough-for-you/>

3.) Hard drives die - eventually. When they do, there goes easy access to your programs and data. There are services out there that can hopefully retrieve your data, but they are not 100% and I know from experience that they are not cheap!! I have seen quotes of \$1500. So, what to do?

Backup, backup, and backup your hard drive. It takes time. It's an imposition and you have to read how to do it. When faced with a potential bill for \$1500 vs buying a \$140 or less backup system, it becomes a no brainer.

I backup in two ways. One I use a USB memory stick and copy important files to the stick. Easy peasy. USB memory sticks are cheap. I've seen name brand named sticks going for around \$8 for a 32 GB stick to \$30 for a 128GB stick. These are very cheap backups. The number and cost of USB sticks will depend on how much data you want to copy over.

The second way is that I use Acronis True Image hard drive cloning software in conjunction with a docking station and hard drive. A one-year Acronis subscription is listed at \$60 but I have seen offers for around \$30 from Amazon. Docking stations can be purchased for around \$30. A 2TB mechanical hard drive can be found for around \$68. Some docking stations are also duplicators where you can extract your hard drive from your computer and duplicate it.

Here is a picture with specs for a docking station plus duplicator

ENC-DOCKU3X2

This Two-in-One SATA III HDD docking station & duplicator lets you duplicate/clone an existing hard drive without connecting to a PC. It supports two SATA HDD (2.5" & 3.5") at same time and includes One Touch Backup (OTB) software.



- Interface: USB 3.0 (USB 2.0 & USB1.1 Compatible)
- HDD Interface: SATA 1.5/3/6 Gbps
- Upright, Convenient and Trendy Design
- Easy Hard Drive Ejection and Insertion
- 2 Hard Drives can be accessed at the same time
- Built-in Duplication Function
- Supports all 2.5"/3.5" SATA Hard Drives of any size capacity
- On/Off Power Button
- System Requirements:
 - Windows XP / VISTA / 7 / 8 / 8.1 / 10
- Plug and Play; Hot-Swappable
- AC/DC Power Supply included
- USB 3.0 cable included

I rely on Acronis and a docking station similar to the one above to clone my computer's hard drive. This way I do not have to remove my computer's hard drive from its case.

4.) Use only known or reputable companies or individuals to work on your computer systems. Often, the big-name computer companies (e.g., Dell, HP Acer, Asus, Lenovo, etc.) will have service centers available but you may have to ship your computer off to them. You can also do a search online using the words: "Computer repair service" followed by your town and state (e.g., computer repair service Durham, NC) and up will pop listings often with ratings and reviews that you can use to judge competency and trustworthiness of the various repair services.

5.) Limit your browsing to known/trusted sites. If you don't know the exact address of the site you want to go to. **DON'T GUESS!!!**. **Use a search engine** to try to find the correct URL address. A lot of bad sites exist on purpose with an address that is a very slight variation of the site you want to go to. You don't

want to end up on the wrong site. When doing a search, often the best sites are at the top of any listing of results.

6.) Learn the warning signs of attempted fraud when on-line. If a pop-up message says your computer is infected, click here for help, **DON'T CLICK!!!**

<https://www.bleepingcomputer.com/virus-removal/remove-your-windows-is-infected-popup-scam>

7.) Malware. Is a generic term for all sorts of nasty programs that the bad guys try to infect your computer with. Malware can be keyloggers, Trojan apps, etc. Malwarebytes is a program that you can install to look for malware and remove it from your computer. There is a free version but I like to pay for their service. It's like NARFE, cheap insurance for people who are trying to help us.

<https://malwaretips.com/blogs/remove-attention-your-computer-has-been-infected/>

<https://www.malwarebytes.com/>

We (I) could go on, but this should be enough to help you get started to help you know your computer and to keep it up and running without interference from external factors natural and fraudster-made.

Above all: **Do your homework!!**

Epilogue

“Do your homework” I cannot reiterate that enough. Try to understand what the fraudsters are trying to do to you emotionally. They may say they have an “orphanage of starving kids” but the writer of that email may be a fat slob sitting on a bar stool in New Jersey connected to a Wi-Fi. They want to tug at some emotion we may have whether it be for kids in trouble, vets who may need help, or an appeal to our greed with a relative we never knew we had and likely never did. All they want is our money.

If you feel the urge to contribute, please satisfy that emotion by looking for local charities, instead, that will do just what the fraudster say they are going to do but will not. Local charities are often in need of your help both financially and with actual physical help. Helping the locals may not seem as exotic as helping some concept of a destitute person in some far off part of the world, at least it won't be going to some fat slob on a bar stool. **Please consider the need to help locally first.**

As for the rest, it is your money. Do your homework in the ways to safeguard it. We have started to help you. It is up to you to continue to educate yourself, to understand these various situations, and to defend your assets.

Good luck!!! And “Do your homework.”

Appendix

Appendix 1: Reporting Robocalls Does Work

For Immediate Release:

Tuesday, February 2, 2021

Contact:

Laura Brewer (919) 716-6484

(RALEIGH) Attorney General Josh Stein and Indiana Attorney General Todd Rokita today took action to ensure state attorneys general can continue to fight against robocalls. Attorneys General Stein and Rokita led a bipartisan coalition of 35 attorneys general in filing an amicus brief in *Lindenbaum v. Realgy*. In their brief, the states argue that the Telephone Consumer Protection Act's robocall ban was enforceable from 2015 to 2020. Fighting robocalls is one of Attorney General Stein's top priorities.

"Beyond being a constant irritation, robocalls cause real financial harm to people," said Attorney General Josh Stein. "We cannot let robocallers off the hook – we need these federal protections to hold them accountable for breaking the law and scamming North Carolinians. I'm proud to lead my colleagues in filing this brief and will do everything in my power to protect North Carolinians from these nuisance calls."

In 2015, the president signed into law a government debt exception to the TCPA. The exception allows for calls and texts to collect on debts owed or guaranteed to the federal government. In 2020, the U.S. Supreme Court invalidated that exception and severed it from rest of the TCPA. Later, a district court ruled in *Lindenbaum v. Realgy* that because part of the law was struck down, the TCPA is invalid and cannot be used to hold robocallers accountable for their actions between 2015 and 2020.

The brief, filed in the U.S. Court of Appeals for the Sixth Circuit, asks the court to reverse the lower court's ruling. The brief argues that the Supreme Court's 2020 decision made clear that the invalid government debt exception did not affect the TCPA's primary robocall ban. It further argues that the district court's decision was inconsistent with basic principles on severability.

State attorneys general are at the forefront of the fight against robocalls, which are immensely frustrating and can cause real financial harm to people. In January 2020, people received more than [4.7 billion robocalls](#) nationwide. The attorneys general have several ongoing enforcement actions under the Telephone Consumer Protection Act (TCPA), and invalidating the law on a technicality would let robocallers off the hook. The bipartisan coalition argues that aside from the government debt exception, the rest of the TCPA can and must be upheld so it can be enforced.

In 2020, North Carolinians reported nearly 10,000 robocalls and unwanted telemarketing calls to the North Carolina Department of Justice—the number one consumer complaint filed with the office. Attorney General Stein is leading efforts nationwide to confront these incessant calls. In December, he won a \$14 million penalty against Dish Network for engaging in illegal telemarketing and violating do-not-call laws, the largest-ever state penalty for do-not-call violations. He also launched the Robocall Report Task Force so North Carolinians can report robocalls online (www.ncdoj.gov/norobo) and through a dedicated robo-report hotline (1-844-8-NO-ROBO). He also led 51 attorneys general and 12 phone companies to launch the [Anti-Robocall Principles](#) to combat robocalls.

Attorneys General Stein and Rokita are joined in filing this brief by the Attorneys General of Alaska, Arizona, Arkansas, California, Connecticut, Delaware, Hawaii, Illinois, Iowa, Kansas, Maine, Maryland, Massachusetts, Michigan, Minnesota, Nebraska, Nevada, New Jersey, New Mexico, New York, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Utah, Vermont, Virginia, and Washington, and the District of Columbia.

More on Attorney General Stein’s work to confront robocalls:

- [Attorney General Josh Stein Reaches \\$210 Million Settlement with Dish Network Over Illegal Telemarketing Calls](#)
- [Attorney General Josh Stein Leads Bipartisan Coalition of 38 Attorneys General Urging U.S. Supreme Court to Block Robocall Loopholes](#)
- [Attorney General Josh Stein Leads States’ Efforts to Expose Illegal Robocallers](#)
- [Attorney General Josh Stein Takes Texas Robocallers to Court](#)
- [Attorney General Josh Stein Leads Bipartisan Coalition to Urge U.S. Supreme Court to Protect Ban on Robocalls](#)

Submitted by Charles Talley, Executive VP, NC NARFE

Reference:

<https://ncdoj.gov/attorney-general-josh-stein-leads-bipartisan-coalition-fighting-to-defend-robocall-protections/>

Appendix 2: Examples of Email Scams and Phishing Attempts

Example 1: **Wire Transfer** request. Big RED Flag word pair. Don't reply. Report this as phishing. Give Carolyn a heads up call. She's not to blame.

Request

1 message

Carolyn C. Example <ccexample@att.net>

Mon, Mar 26, 2018 at 12:24 PM

Reply-To: "Carolyn C. Example" <presidentoffice2018@gmail.com>

To: Peter@anyisp.com

Peter,

Are you in the office? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

Thanks,
Carolyn C. Example

Example 2: Playing to your greed and gullibility

BARRISTER MICHAEL ARTHUR SAN. <dikeefe17@gmail.com>

Mar 5, 2021, 2:10 PM

to bcc: me

Good Day Friend ,

It is obvious that this proposal will come to you as a surprise; this is because we have not met before but I am inspired to sending you this email following the huge fund transfer opportunity that will be of mutual benefit to both of us. However, I am Barrister MICHAEL ARTHUR, SAN, Attorney to the Late Engineer Ronald Johnson national of Northern American, who used to work with Shell Petroleum Development Company (SPDC) in Nigeria On the 3th of November. My client, his wife and their three children were involved in a car accident along Sagamu/Lagos Express Road.

Unfortunately they all lost their lives in the event of the accident, since then I have made several inquiries to several Embassies to

locate any of my clients extended relatives, this has also proved unsuccessful. After these several unsuccessful attempts, I decided to trace his relatives over the Internet to locate any member of his family but of no avail, hence I contacted you.

I contacted you to assist in repatriating the money and property left behind by my client; I can easily convince the bank with my legal practice that you are the only surviving relation of my client. Otherwise the Estate he left behind will be confiscated or declared not serviceable by the bank where these huge deposits were lodged. Particularly, the Bank where the deceased had an account valued at about \$15 million U.S dollars (Fifteen million U.S. America dollars). Consequently, The bank issued me a notice to provide the next of kin or have the account confiscated within the next ten official working days. Since I have been unsuccessful in locating the relatives for over several years now. I seek your consent to present you as the next of kin to the deceased, so that the proceeds of this account valued at \$15million U.S dollars can be paid to your account and then you and I can share the money, 50% to me and 50% to you.

All I require is your honest cooperation to enable us see this deal through and also forward the following to me:

- 1, Your Full Name:.....
- 2, Your House Address:.....
- 3, Your Country:.....
- 4, Your Contact Telephone
- 5, Your Age and Gender:.....
- 6, Your Occupation:

I guarantee that this will be executed under a legitimate arrangement that will protect you from any breach of the law.

Please get in touch with me VIA this my confidential email (dikeefe17@gmail.com)

Yours Faithfully,
BARRISTER MICHAEL ARTHUR SAN.

This is a classic example of a phishing email format.

Example 3 and a variation on Example 2: Another example of an email phishing format.

Central Bank <cbnngbank@gmail.com> Mon, Mar 8, 12:00 PM

FROM THE DESK OF JOHN UZO,
REGIONAL MANAGER
CENTRAL BANK.

Hello [ed. Person's full name],

My name is Mr. John Uzo, I am the regional manager of the Central Bank I got your information during my search through the internet.

I am 48 years of age It may interest you to hear that I am a man of PEACE and don't want problem, but i don't know how you will feel about this because you might feel that its scam yes there are many spammers.

but am telling you that this is real and you are not going to regret after doing this transaction with me.

I only hope we can assist each other. But If you don't want this business offer kindly forget it as I will not contact you again.

I have packaged a financial transaction that will benefit both of us, as the regional manager of the Central Bank. it is my duty to send in a financial report to my head office in the capital city Abuja at the end of each year. On the course of the last year 2020 end of year report, I discovered that my branch in which I am the manager made (\$US18,5 Million United State dollar) which my head office are not aware of and will never be aware of.

I have since place this fund on what we call SUSPENSE ACCOUNT without any beneficiary.

As an officer of the bank I can not be directly connected to this money, so this informed my contacting you for us to work so that you can assist receive this money into your bank account for us to SHARE.

While you will have 50% of the total fund .Note there are practically no risk involved, it will be bank to bank transfer,all I need from you is to stand claim as the original depositor of this fund who made the deposit with our branch so that my Head office can order the transfer to your designated bank account.

If you accept this offer to work with me, I will appreciate it very much.As soon as I receive your response I will details you on how we can achieve it successfully.Please your cell phone number is very important important so that we can talk one on one phone

Best Regards
Mr. John Uzo,

Example 4: It seems extremely sincere but it is not. It's a very very common scam preying on very good people with a heart. It's designed to tug at your heart strings. If you give this person your bank details, they will likely obtain enough personal data to possibly bankrupt you. You are too good to lose your money to these fraudsters.

You can find these types of dire situations locally where you know your heart felt charity donations will be used by real people with real needs.

Greetings My dear,

Mrs. Marina Amandine. <sisterangela2004@gmail.com> Mar 14, 2021, 5:30 PM
to bcc: me

Greetings My dear,

I bring peace and love to you. It is by the grace of god, I had no choice than to do what is lawful and right in the sight of God for eternal life and in the sight of man for witness of Gods mercy and glory upon my life. My dear, I sent this mail praying it will found you in a good condition of health, since I myself are in a very critical health condition in which I sleep every night without knowing if I may be alive to see the next day. I am Mrs. Marina Amandine, a widow suffering from long time illness. I have some funds I inherited from my late husband, the sum of (Two million dollars) my Doctor told

me recently that I have serious sickness which is cancer problem. What disturbs me most is my stroke sickness. Having known my condition, I decided to donate this fund to a good person that will utilize it the way i am going to instruct herein. I need a very honest and God fearing person who can claim this money and use it for Charity works, for orphanages and gives justice and help to the poor, needy and widows says The Lord." Jeremiah 22:15-16." and also build schools for less privilege that will be named after my late husband if possible and to promote the word of God and the effort that the house of God is maintained.

I do not want a situation where this money will be used in an ungodly manner. That's why I'm taking this decision. I'm not afraid of death, so I know where I'm going. I accept this decision because I do not have any child who will inherit this money after I die. Please I want your sincerely and urgent answer to know if you will be able to execute this project, and I will give you more information on how the fund will be transferred to your bank account. May the grace, peace, love and the truth in the Word of God be with you and all those that you love and care for. In the name of Yeshua Ha Mashiach, (Jesus the Christ) Hallelujah!

I am waiting for your reply.

May God Bless you,
Mrs. Marina Amandine.

Example 5: It looks legitimate but it is not. **Don't click the "Verify Now" button!!** In fact, don't click on anything in a message like this. **Notice how this message is trying to panic the user with:** "permanent delete of your account from our data-base in the next few hours". No legitimate company tries to panic a customer. The "To:" and "From:" are not right.

From: M S N Service <example@outlook.com>

Date: March 26, 2021 at 11:13:34 AM EDT

To: member@service.com

Subject:  **FINAL Checking!**



The screenshot shows an email from Microsoft. At the top is the Microsoft logo. The body of the email starts with "Dear Microsoft User". The main text reads: "This is the last time we notified you that we will stop processing incoming emails in your account reasons are you failed to verify your Microsoft account which may lead to permanent delete of your account from our data-base in the next few hours." Below this is a call to action: "Kindly take a minute to complete our email verification below" followed by a large blue button that says "Verify Now". At the bottom, there is a red warning: "Important Notice- Account disconnection will take place today 12:00 Midnight if issue not resolved." and a link to Microsoft's privacy policy. The footer contains the address: "Microsoft Corporation, One Microsoft Way, Redmond, WA 98052".



Dear Microsoft User

This is the last time we notified you that we will stop processing incoming emails in your account reasons are you failed to verify your Microsoft account which may lead to permanent delete of your account from our data-base in the next few hours.

Kindly take a minute to complete our email verification below

Verify Now

Important Notice- Account disconnection will take place today 12:00 Midnight if issue not resolved.

Microsoft respects your privacy. Read our privacy policy for more information.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Example 6: An attempt to make contact and illicit funds for a hard luck story. Don't respond. Report it as phishing.

Is about Mrs. Stella.

Mr. Pepe Edem <mr.pmomo@gmail.com> Tue, Mar 16, 9:34 AM

to Recipients

Please can I talk to you about Mrs. Stella? is urgent.

Example 7: Very questionable. FDA approved? Talk with your doctor first!!!

The Miracle gummies For pain depression, and anxiety

Miracle Gummies <health@lobgummies.com>

Fri, Mar 26,
2:00 PM

to email addr

Example 8: Don't click on anything. This is designed to panic you into doing something quickly and hopefully, without thinking and questioning. In this case, Amazon does ****NOT**** use Gmail. It's a dead giveaway that will lead to a phishing attempt. Report it as phishing

FW: Order Confirmation

From: Amazon <ava3546gre@gmail.com>

Date: March 22, 2021 at 12:40:07 PM EDT

To:

Subject: Order Confirmation



[Your Orders](#) | [Your Account](#)

Shipping Confirmation

Order # 369-627587-583658

Hello **Henri Brattle**, ,

Thank you for shopping with us. We'll send a confirmation once your item will be shipped. Your orders detail is indicated below. If the order was not made by you then please call us on **1-877-483-0236** to report this to our fraud protection team .

Arriving:

Friday, April 02

[Track Your Package](#)

Your package was sent to:

**378 Robinson Lane, Wilmington,
Delaware, 19805.**

Your package is being shipped by ATS and the tracking number is 7647553466521.
Please note that a signature may be required for the delivery of the package.

Example 9: Fraudsters will tug at your religious and patriotic devotions as well as wanting to help kids. It's all an attempt to try to separate you from your money. This is a patriotic version.

references@mancunscm.com Apr 16, 2021, 6:16 PM

to [aVeteran@some ISP.COM](mailto:aVeteran@someISP.COM)

Hello CHARLIE ← **Note: Charlie is not at the email address originally used above.**

Are you available to assist? I am out of town now, and I have hope in you to take care of this for me. I would have called your phone but I presently do not have access to my mobile phone.

NARFE - North Carolina Federation needs some gift cards for donation to Veterans at Hospice and Palliative care units for preventive items against Corona Disease (COVID-19). I have decided to make it a personal duty. I will be responsible for the reimbursement. Need more info?

Henry Brattlie

President

NARFE - North Carolina Federation

www.narfe.org

Just for the heck of it, see if you can spot and list all the warning flags this and the other examples contain.

Notes

Notes



Active and Retired Federal Employees ... Join NARFE Today!

The only organization dedicated solely to protecting and preserving the benefits of all federal workers and retirees, NARFE informs you of any developments and proposals that affect your compensation, retirement and health benefits, AND provides clear answers to your questions.

Who Should Join NARFE?

If your future security is tied to federal retirement benefits—federal retirees, current employees, spouses and individual survivors—you should join NARFE.

★

NARFE MEMBER BENEFITS

- Access the NARFE Federal Benefits Institute for powerful resources to help you fully understand and manage your benefits.
- Visit the Legislative Action Center to contact your representatives about bills affecting federal benefits.
- Get *NARFE Magazine* with news and insights for the federal community.
- Save time, hassle and money with NARFE Perks.
- The opportunity to get involved at the local level by joining a chapter in your area.

NARFE MEMBERSHIP APPLICATION

YES. I want to join NARFE for the low annual dues of \$48.

Mr. Mrs. Miss Ms.

Full Name _____

Street Address _____

Apt./Unit _____

City _____ State _____ ZIP _____

Phone _____

Email _____

I am a (check all that apply)

- Active Federal Employee Active Federal Employee Spouse
 Annuitant Annuitant Spouse Survivor Annuitant

Please enroll my spouse

Spouse's Full Name _____

Spouse's Email _____

PAYMENT OPTIONS

- Check, Money Order or Bill Pay (Payable to NARFE)
 Bill me (*NARFE membership will start when payment is received.*)
 Charge my:
 MasterCard VISA Discover AMEX

Card No. _____

Expiration Date ____ / ____
mm yyyy

Name on Card _____

Signature _____

Date _____

TOTAL DUES

\$48 Annual Dues X _____ = _____
Per Person # Enrolling Total Dues

Dues payments are not deductible as charitable contributions for federal income tax purposes.

LOOKING TO MEET OTHERS in the federal community and participate in NARFE at a local level? Call 800-456-8410 to learn about a NARFE chapter in your area.

Would you like to receive a FREE one-year chapter membership? Choose one:

Chapter closest to home OR Chapter # _____

THREE EASY WAYS TO JOIN

1. **Complete this application** and mail with your payment to NARFE Member Services / 606 N Washington St / Alexandria, VA 22314-1914.
2. Join online at www.NARFE.org.
3. **Call 800-456-8410**, Monday through Friday, 8 a.m. to 5 p.m. ET.

MAY WE THANK SOMEONE? Did someone introduce you to NARFE? Please provide their Name and Member ID.

Recruiter's Name _____

Recruiter's Membership ID _____

NARFE respects the privacy of our members. Personal information is used to provide content and relevant communications to our members, and will not be sold or rented to third parties.

106

(01/21)



Active and Retired Federal Employees ... Join NARFE Today!

The only organization dedicated solely to protecting and preserving the benefits of all federal workers and retirees, NARFE informs you of any developments and proposals that affect your compensation, retirement and health benefits, AND provides clear answers to your questions.

Who Should Join NARFE?

If your future security is tied to federal retirement benefits—federal retirees, current employees, spouses and individual survivors—you should join NARFE.

★

NARFE MEMBER BENEFITS

- Access the NARFE Federal Benefits Institute for powerful resources to help you fully understand and manage your benefits.
- Visit the Legislative Action Center to contact your representatives about bills affecting federal benefits.
- Get *NARFE Magazine* with news and insights for the federal community.
- Save time, hassle and money with NARFE Perks.
- The opportunity to get involved at the local level by joining a chapter in your area.

NARFE MEMBERSHIP APPLICATION

YES. I want to join NARFE for the low annual dues of \$48.

Mr. Mrs. Miss Ms.

Full Name _____

Street Address _____

Apt./Unit _____

City _____ State _____ ZIP _____

Phone _____

Email _____

I am a (check all that apply)

- Active Federal Employee Active Federal Employee Spouse
 Annuitant Annuitant Spouse Survivor Annuitant

Please enroll my spouse

Spouse's Full Name _____

Spouse's Email _____

PAYMENT OPTIONS

- Check, Money Order or Bill Pay (Payable to NARFE)
 Bill me (*NARFE membership will start when payment is received.*)
 Charge my:
 MasterCard VISA Discover AMEX

Card No. _____

Expiration Date ____ / ____
mm yyyy

Name on Card _____

Signature _____

Date _____

TOTAL DUES

\$48 Annual Dues X _____ = _____
Per Person # Enrolling Total Dues

Dues payments are not deductible as charitable contributions for federal income tax purposes.

LOOKING TO MEET OTHERS in the federal community and participate in NARFE at a local level? Call 800-456-8410 to learn about a NARFE chapter in your area.

Would you like to receive a FREE one-year chapter membership? Choose one:

Chapter closest to home OR Chapter # _____

THREE EASY WAYS TO JOIN

1. **Complete this application** and mail with your payment to NARFE Member Services / 606 N Washington St / Alexandria, VA 22314-1914.
2. Join online at www.NARFE.org.
3. **Call 800-456-8410**, Monday through Friday, 8 a.m. to 5 p.m. ET.

MAY WE THANK SOMEONE? Did someone introduce you to NARFE? Please provide their Name and Member ID.

Recruiter's Name _____

Recruiter's Membership ID _____

NARFE respects the privacy of our members. Personal information is used to provide content and relevant communications to our members, and will not be sold or rented to third parties.

106

(01/21)

