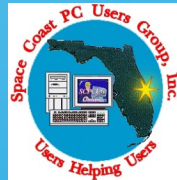


Scammers – The Worst!

Dan Douglas
June 3, 2023



What is Scamming

***Scamming* is to deceive and take money or something of value from someone by a dishonest or fraudulent scheme.** The person who does scamming is a scammer, trickster, or swindler.

Types of Scams

- phone voicemail
- romance online
- email safety
- password managers
- housing
- police
- cryptocurrency
- public records
- international
- Medicare
- travel
- you won \$\$\$
- how to report a scam to the better business bureau & US government

Types of Scams – AARP List

Apartment Rental Scams
Business Email Compromise
Car Warranty Scams
Caregiver Fraud
Celebrity Impostor Scams
Charity Scams
Coronavirus Scams
Credit Card Interest Rate Scam
Credit Repair Scams
Cruise Scams
Cryptocurrency Fraud
Customer Service Scams
Debt Collection Scams
Debt Relief Scams
Dietary Supplement Scams
Disaster Scams
DMV Scams
Email Extortion Scams
Fake Check Scams
Free Trial Scams
Funeral Scams
Gift Card Scams
Government Grant Scams
Grandparent Scam
Greeting Card Scams
Health Fraud
Health Insurance Scams
Holiday Scams
Home Improvement Scams
Identity Theft
Impostor Scams
Investment Fraud
IRS Impostor Scam
Jury Duty Scams

Medical Equipment Scams
Medical Identity Theft
Medicare Card Scams
Medicare Flex Card Scams
Medicare Fraud
Money Mule Scams
Mortgage Relief Scams
Moving Scams
Nigerian Scams
Obituary Scams
Online Banking Scams
Online Pharmacy Scams
Online Shopping Scams
Package Scams
Pet Scams
Phishing
Phone Scams
Political Scams
Political Scams
Ponzi and Pyramid Schemes
Psychic Scams
Public Wi-Fi Scams
QR Code Scams
Ransomware
Reverse Mortgage Scams
Robocalls
Romance Scams
Secret Shopper Scams
Small Business Scams
Smishing
Social Media Scams
Social Security Scams
Spear-Phishing
Student Loan Scams

Survey Scams
Sweepstakes and Lottery Scams
Tax ID Theft
Tax Preparation Scams
Tech Support Scams
Time-Share Resale Scam
Travel Scams
'Update Account' Scams
Utility Scams
Vacation Scams
VA Pension Poaching
Veterans Charity Scam
Veterans Scams
Weight-Loss Scams
Who's Who Scams
Work-From-Home Scams

Actual Scamming Attempts

The screenshot shows an email client interface. On the left is an inbox with several emails, including one from 'DriveSavers Reseller Referral Partner Progr...', 'Generac Product Activation - Action Requi...', 'Vanity Fair', 'PACKAGE NOTIFICATION.', 'Client ID:47148-1514.', 'Memberships@corvettemuseum.org', 'Brevard, Florida Today', 'L&E Research', 'BJ's Wholesale Club', 'Outback Steakhouse', 'Dan Douglas', and 'Costco Wholesale'. The main area shows an open email titled 'We missed you - schedule your next delivery date.' from 'PACKAGE NOTIFICATION. <SBMU.IDf.qZouG@bloixiog.org.uk>'. The email content includes a 'TRACK AND TRACE' header, a message 'Hi, You have (1) package waiting for delivery.', a tracking number '#29194772', and a 'Schedule Delivery' button. Below the button, it states '*if we do not receive a response within 5 working days, your package will be returned to the sender.' and a progress indicator showing a failed step. At the bottom, it says 'SCHEDULE DELIVERY MISSED. Delivery attempted: Signature required Tracking number: #29194772'. A footer note reads: 'The advertiser does not manage your subscription. If you prefer not to receive further communication please unsubscribe [here](#). Or write to: 6101 Long Prairie Rd. Ste 744 #511, Flower Mound, TX, 75028'.



Scam Detection Clues

mised you - schedule your next delivery date.

PACKAGE NOTIFICATION. <SBMU.IDf.qZOuG@bloixiog.org.uk> **1**

To: You
Cc: You

[View this email in your browser](#)

TRACK AND TRACE

Hi, You have (1) package waiting for delivery.

Tracking number: [#29194772](#)

Schedule your delivery now*:

Schedule Delivery

*if we do not receive a response within 5 working days, your package will be returned to the sender.

✓ — ✓ — ✗ — ○

SCHEDULE DELIVERY MISSED.
Delivery attempted: Signature required
Tracking number: [#29194772](#)

The advertiser does not manage your subscription.
If you prefer not to receive further communication please unsubscribe [here](#)
Or write to: 6101 Long Prairie Rd, Ste 744 #511, Flower Mound, TX, 75028

2

Actual Scamming Attempts

Inbox ☆ Filter

- VO** DriveSavers Reseller Referral Partner Progr...
- N** Generac Product Activation - Action Requi...
- Today
- VF** Vanity Fair
The V Files: The Shocking Legacy of a... 10:14 AM
Here are the stories you might have missed this ...
- PN** PACKAGE NOTIFICATION.
We missed you - schedule your next ... 10:12 AM
No preview is available.
- CI** Client ID:47148-1514.
Your package notification. 10:00 AM
No preview is available.
- M** Memberships@corvettemuseum.org
New Digital Cards: National Corvette ... 8:33 AM
Thank you for supporting the National Corvette ...
- BT** Brevard, Florida Today
Daily Briefing: SpaceX kicks off Memor... 5:32 AM
A SpaceX Falcon 9 rocket flew through clouds o...
- Yesterday
- LR** L&E Research
Small Business Owners. We Want Yo... Fri 2:01 PM
Hi Dan! L&E Research Has an Upcoming Paid M...
- BC** Bf's Wholesale Club
Here's a coupon for \$10 off. One ... Fri 11:55 AM
Memorial Day savings are here!
- OS** Outback Steakhouse
Your MEMBER-EXCLUSIVE PER... Fri 11:52 AM
Hurry—don't miss your Dine Rewards member-...
- DD** Dan Douglas
> powerpoint Fri 11:42 AM
No preview is available.
- CW** Costco Wholesale
Why Buy At Costco? Fri 11:39 AM
Memorial Day Deals and More View in browser. ...
- This month
- GV** Gene Luke Vlahovic
> James O. Born Thu 1:11 PM
The sign on the white side would be more attra...
- F** Florida Department of Revenue
FL Dept. of Revenue Sales and Us... Thu 12:48 PM
The Florida Department of Revenue has issued t...

Your package notification.

CI Client ID:47148-1514 . <info@asolo.org>
To: You
Cc: You

PackageDelivery

Delivery of The Suspended Package

You have (1) Package waiting for you in our warehouse. Ready for delivery. use your order number to Track and recieve your package !

Scheduled At **PackageDelivery** Center

Tracking number

25987463145

Confirm Now

Your Tracking-Code:

25987463145

Track Your Package

Best Regards: Shipping Customer Service

If you wish to unsubscribe, please click [here](#)!

The advertiser does not manage your subscription.
If you prefer not to receive further communication please unsubscribe [here](#)
Or write to: 6101 Long Prairie Rd, Ste 744 #511, Flower Mound, TX, 75028

Scam Detection Clues

Your package notification.

Client ID:47148-1514 . <info@asolo.org>
To: You
Cc: You

1

PackageDelivery

Delivery of The Suspended Package

You have (1) Package waiting for you in our warehouse. Ready for delivery. use your order number to Track and recieve your package !

Scheduled At **PackageDelivery** Center

Tracking number

25987463145

Confirm Now

Your Tracking-Code:

25987463145

Track Your Package

Best Regards: Shipping Customer Service

3

If you wish to unsubscribe, please click [here](#)!

The advertiser does not manage your subscription.
If you prefer not to receive further communication please unsubscribe [here](#)
Or write to: 6101 Long Prairie Rd.Ste 744 #511, Flower Mound, TX, 75028

2

Actual Scamming Attempts

The screenshot shows the Microsoft Outlook interface. The top navigation bar includes 'Outlook', a search box, and 'Meet Now'. The main area is divided into three sections: a left sidebar with 'Favorites' and 'Folders', a central list of junk emails, and a right pane showing the details of a selected email.

Left Sidebar:

- Favorites: Deleted I... 122, Sent Items, Drafts, All Mail, Your family, **Junk Em... 958**, Peter A. Doug..., Add favorite
- Folders: **Inbox 4**, 2017 Escape, 2022 Trips, 2023 cruise, 235 florida, C5 store, c5.c6 joins, DataDa... 26, east coast...
- Upgrade to Microsoft 365 with premium Outlook features

Junk Email List:

- Items in Junk Email will be deleted after 10 days
- LM Limited Time Offer: Score Memori... 9:16 AM
Today through Monday shop and get 25% off si...
- SO SilverSingles Offer**
Rediscover Romance in Your Life with ... 8:16 AM
- JC Just Care
Want medical advice? A.I. offers sma... 8:00 AM
Subscribe to the JustCare Newsletter Want som...
- L Laser Lipo by SonoBello
Find Out Which Procedure is Right f... 7:44 AM
No preview is available.
- D Disney Dining Daily Update
This Beloved Magic Kingdom Ride C... 7:09 AM
This Beloved Magic Kingdom Ride Could Chang...
- YP Your package .
Delivery update: your delivery is pen... 6:51 AM
No preview is available.
- BA BlueApron.com Affiliate
Discover the Joy of Cooking with Blu... 6:09 AM
No preview is available.
- BM Blue Dolphin Magazines
TIME Subscription Renewal (Order #6... 5:59 AM
Hi Dan, This is just a friendly reminder that your...
- TA Talc powder-ovariancancer Affiliate
8.9 Billion Ovarian Cancer - Talc Pow... 2:57 AM
No preview is available.
- BD Black Forest Decor
ABSOLUTELY FINAL Clearance Sale - ... 2:05 AM

Selected Email:

Rediscover Romance in Your Life with The Help of SilverSinglesStart Meeting Like-minded Singes this Month.

This message was identified as junk. We'll delete it after 10 days. It's not junk | Show blocked content

SO SilverSingles Offer <info@uniqurapid.com>
To: You
Sat 5/27/2023 8:16 AM



Scam Detection Clues

The screenshot shows the Outlook interface with a search bar at the top. The left sidebar contains navigation options like Favorites, Deleted Items, Sent Items, Drafts, All Mail, Your family, and Folders. The main pane displays a list of emails in the Junk Email folder, with a red '1' next to the 'Junk Email' header. The selected email is from SilverSingles, with a red '2' next to the subject line. The right pane shows the email content, with a red '3' next to the sender information.

1 Junk Email

Items in Junk Email will be deleted after 10 days

Limited Time Offer: Score Memori... 9:16 AM
Today through Monday shop and get 25% off si...

SilverSingles Offer
Rediscover Romance in Your Life with ... 8:16 AM

2 Rediscover Romance in Your Life with The Help of SilverSinglesStart Meeting Like-minded Singes this Month.

This message was identified as junk. We'll delete it after 10 days. It's not junk | Show blocked content

SilverSingles Offer <info@uniqrapid.com> **3**
To: You

Sat 5/27/2023 8:16 AM

Actual Scamming Attempts

Junk Email Filter

Items in Junk Email will be deleted after 10 days

- ChristianMatches.com Ad**
Meet Your Match Made in Heaven... Fri 4:36 PM
Virus-free.www.avast.com
- Disney Dining**
Disney-Inspired Recipes for Memo... Fri 4:31 PM
The perfect bites and sips for your Memorial Da...
- Medical Injury Claim**
Camp Lejeune Information: Poten... Fri 4:26 PM
The Time is NOW to File Your Camp Lejeune Inj...
- Capt. Jones Williams**
REPLY IMMEDIATELY Fri 4:08 PM
Dear Beloved Friend, I am Capt. Jones Williams ...
- Annuities.net Ad**
Get Your FREE Annuity Compariso... Fri 3:59 PM
No preview is available.
- SEC Network**
SEC Baseball Tournament F... Fri 3:51 PM
Watch the remaining teams battle in the Fourth ...
- Suzan DelBene**
What the GOP default plan means... Fri 3:23 PM
Americans can't afford this Hi Dan, The latest M...
- NationalDebtRelief.com Info**
A Trusted Alternative to Paying Of... Fri 3:07 PM
No preview is available.
- Amo-Latinas Ad Partner**
We understand the importance of... Fri 3:02 PM
No preview is available.

REPLY IMMEDIATELY

This message was identified as junk. We'll delete it after 10 days. It's not junk

CW Capt. Jones Williams <info@biobiz.jp>
To: You
Fri 5/26/2023 4:08 PM

Dear Beloved Friend,

I am Capt. Jones Williams of the US Army. I am currently in SYRIA as an Advisory to the SYRIA Military on the fight against ISIL/ISIS Terrorist and also helping in stabilizing the country against security challenges.

During the fight with the terrorist, we discovered the sum of FORTY FIVE MILLION UNITED STATES DOLLARS Only, (\$45,000,000.00), stocked in a boxes, which, I have moved to a Red Cross location here. I would like to move this money, as quickly as possible, to you for business purposes. If I can trust you, I am a uniformed person and I cannot be parading such an amount, so, I need to present someone, to stand, as the recipient. I am an American and an intelligence officer and for that, I have a 100% authentic means of transferring the money through Diplomatic or RED CROWN COURIER SERVICE, I just need your acceptance and all is done.

I am willing to settle you with 40% of the total sum while 60% goes to me on my arrival. You will advise me on the business to invest in, since I am not business oriented. I want to move this money to your destination for your safe keep, until, I am out of SYRIA. I believe, I can trust you. Presently, we can only communicate through our military communication facilities which are secured so nobody can monitor our emails, I will only reach you through email, because our calls might be monitored, I just have to be sure who I am dealing with.

I wait for your response so we can proceed immediately because in less than 5 days the money should be in your safe custody. I wait for your contact details so we can go on. I hope I am fair on this deal, Get back to me with information below.

Your Full Name:.....
Your Full Address:.....
Your Direct Telephone no:.....
Occupation:.....

Please get back to me so that we can discuss the way forward.

Best Regards,

Capt. Jones Williams
Us Army
Syria



Scam Detection Clues

1 Junk Email ★ Filter

Items in Junk Email will be deleted after 10 days

CA ChristianMatches.com Ad
Meet Your Match Made in Heaven... Fri 4:36 PM
Virus-free.www.avast.com

DD Disney Dining
Disney-Inspired Recipes for Memo... Fri 4:31 PM
The perfect bites and sips for your Memorial Da...

MC Medical Injury Claim
Camp Lejeune Information: Poten... Fri 4:26 PM
The Time is NOW to File Your Camp Lejeune Inj...

REPLY IMMEDIATELY **2**

3 Capt. Jones Williams <info@biobiz.jp>
To: You
Fri 5/26/2023 4:08 PM

Dear Beloved Friend,

I am Capt. Jones Williams of the US Army. I am currently in SYRIA as an Advisory to the SYRIA Military on the fight against ISIL/ISIS Terrorist and also helping in stabilizing the country against security challenges.

4 During the fight with the terrorist, we discovered the sum of FORTY FIVE MILLION UNITED STATES DOLLARS Only, (\$45,000,000.00), stocked in a boxes,which, I have moved to a Red Cross location here. I would like to move this money, as quickly as possible, to you for business purposes. If I can trust you, I am a uniformed person and I cannot be parading such an amount, so, I need to present someone, to stand, as the recipient. I am an American and an intelligence officer and for that, I have a 100% authentic means of transferring the money through Diplomatic or RED CROWN COURIER SERVICE, I just need your acceptance and all is done.

I am willing to settle you with 40% of the total sum while 60% goes to me on my arrival. You will advise me on the business to invest in, since I am not business oriented.I want to move this money to your destination for your safe keep, until, I am out of SYRIA.I believe, I can trust you. Presently, we can only communicate through our military communication facilities which are secured so nobody can monitor our emails, I will only reach you through email, because our calls might be monitored, I just have to be sure who I am dealing with.

I wait for your response so we can proceed immediately because in less than 5 days the money should be in your safe custody. I wait for your contact details so we can go on. I hope I am fair on this deal, Get back to me with information below.

Your Full Name:.....
Your Full Address:.....
Your Direct Telephone no:.....
Occupation:.....

Please get back to me so that we can discuss the way forward.

Best Regards,

Capt. Jones Williams
Us Army
Syria

AA Annuities.net Ad
Get Your FREE Annuity Compariso... Fri 3:59 PM
No preview is available.

SN SEC Network
SEC Baseball Tournament F... Fri 3:51 PM
Watch the remaining teams battle in the Fourth ...

SD Suzan DelBene
What the GOP default plan means... Fri 3:23 PM
Americans can't afford this Hi Dan, The latest M...

NI NationalDebtRelief.com Info
A Trusted Alternative to Paying Of... Fri 3:07 PM
No preview is available.

AP Amo-Latinas Ad Partner
We understand the importance of... Fri 3:02 PM
No preview is available.



Actual Scamming Attempts

NBC NEWS: 'Trump Bucks' promise wealth for MAGA loyalty. Some lose thousands.

'Trump Bucks' promise wealth for MAGA loyalty. Some lose thousands.

The products are advertised online as a kind of golden ticket that will help propel Trump's 2024 bid and make the "real patriots" who support him rich when cashed in.

Read in NBC News: <https://apple.news/A6M-oHzPkSpiJVqtU3Tgyjg>

Shared from AppleNews May 27, 2023

Actual Scamming Attempts

UPS store owner stops \$25,000 scam, warns against common scams - MSN 5/27/2023

UPS store owner stops \$25,000 scam, warns against common scams (msn.com)

Protect yourself

- In the U.S., UPS will only send texts from MYUPS (69877).
- Check the tracking number at UPS.com to see if it's legitimate.
- If there's any question, call the UPS store.

Resources

Cover Story

P. 7 TODAY'S TOP FRAUDS
P. 10 PROTECT YOURSELF!

P. 13 THEY GOT CAUGHT
P. 14 AARP RESOURCES



YOUR 2023 FRAUD SURVIVAL GUIDE

PROTECT YOURSELF AND YOUR MONEY FROM SCAM CALLS, TEXTS AND EMAILS (AND LEARN HOW THE PROS ARE FIGHTING)

PHOTO ILLUSTRATION BY MATT CHASE

—PART I—

BE PREPARED FOR TODAY'S FRAUDS

Like any smart entrepreneurs, scammers quickly adapt to the news and moods of the moment. These are the scams playing out right now **BY SARI HARRAR**

📞 'Oops, Wrong Number!' Texts
Seemingly misdirected messages are increasingly the start of a scammer's ploy.

THE CON: A text message addressed to someone else pops up on your phone. It seems urgent—a rescheduled business meeting, an illness, sometimes even a romantic get-together. (A version circulating in Florida concerned meeting up for a "spicy night," the state's attorney general warned.) Since you're a helpful person, you text back, "Sorry, wrong number!" The scammer—or often an automated chatbot that sends out computer-

CONTINUED ON PAGE 8

APRIL 2023 AARP.ORG/BULLETIN 7

Resources

Cover Story

CONTINUED FROM PAGE 7

generated messages—keeps up the friendly texts. They may eventually invite you to join

“Scammers are primarily aiming to find phone numbers where people are willing to engage.... They might then use that to try to get personal information... as a target for another scam.”

PROTECT YOURSELF: Don't respond to texts from numbers you don't recognize. Simply delete them. Don't click on links in them or respond with “STOP” if the messages say you can do this to avoid future messages. Instead, block the phone numbers they come from.



Fake Barcodes on Gift Cards
That gift card tucked into a birthday card or thank-you note could be worth zero dollars if scammers siphoned off the value first.

THE CON: Law enforcement agencies warn that nimble-fingered crooks affix fake barcode stickers over the real ones on the back of gift cards in stores. When you purchase the card, the cashier scans the fake barcode at checkout—directing your money into the scammer's gift card account.

PROTECT YOURSELF: With some gift cards, you can make sure the number of the barcode matches the number on the packaging. Or feel or gently scratch the barcode on a gift card before buying. Don't purchase if the barcode is on a sticker, or if the package is ripped, wrinkled, bent or looks tampered with, the Better Business Bureau recommends.



Crypto Refund Swindles
Beware if you've lost money in a cryptocurrency scam: Phony “refund and recovery” companies might come at you next.

THE CON: Criminals set up fake “get your crypto cash back” websites, including one that looks like it's from the U.S. Department of State. After luring targets, they contact

those who respond by phone, email or social media and ask for personal ID information, including account numbers and passwords, plus an advance fee for their services payable by gift card, cryptocurrency or wire transfer. You get nothing, warns the Federal Trade Commission (FTC).

PROTECT YOURSELF: Crypto investments aren't insured by the government the way bank accounts are. For the most part, funds lost to crypto scammers are gone. Don't trust anyone who contacts you saying they can get your money back, says Frank McKenna, chief fraud specialist for the fraud detection company Point Predictive.



Testimonial Videos

Crooks on social media promise to make you whole, but only if you make a video for them.

THE CON: After stealing your money in an investment or sweepstakes scheme or taking over your social media account, criminals take the scheme to a whole new level by promising they'll return your cash or give you back control of your account if you make a testimonial video saying that you've made money in the fraud and that it's real and trustworthy, warns Eva Velasquez, president and CEO of the Identity Theft Resource Center. Crooks post the video on your account that they have taken over to scam others, and you get nothing that was promised.

PROTECT YOURSELF: Refuse demands to make a video, Velasquez recommends. “We tell everyone, ‘You won't get your account or your money back,’” she says. “And it could just further the scam with your friends.”



Fake High School Sports Streaming Sites

They claim they'll show the big game, but instead they steal your money and info.

THE CON: Popularized during the pandemic, streaming services for high school sports let you watch your niece's or grandson's latest match from anywhere—often for free via a legit outlet aligned with the school. But scam streaming apps flood social media before events, posting messages about streaming the game; often they mention specifics (such as the names of key student athletes) to build credibility. “Sometimes the athletes resend the messages, not realizing they're scams,” says Mark Koski, vice president of the NFHS

Network, a paid service that streams games from high schools. At game time, you click on the link, enter your credit card number ... and never see the action. But now scammers have your money and your personal ID info. Some even put extra charges on your credit card.

PROTECT YOURSELF: Contact the high school before a game and ask how you can stream it, says the Better Business Bureau.



Bank Impersonator Racket

Criminals are finding a low-tech way around two-factor authentication.

THE CON: Let's say you've set up your bank or credit card online accounts so you can access them only with a live code sent from the institution. Then let's say a criminal has your bank or credit card username and password login and wants to steal from you. What would he or she do? In this increasingly common fraud, they call you, claiming to be from your bank and warning about a problem with your account. The caller tells you they're emailing or texting you a “onetime passcode” for logging in and asks you to read it back to them for verification. In reality, the scammer's login attempt triggered your bank to send you the passcode. Handing it over gives fraudsters full access to your account.

PROTECT YOURSELF: Scammers are so good at impersonating helpful bank or credit card company employees that you can't tell it's a con, warns Kathy Stokes, AARP's director of fraud prevention programs. Never give your onetime passcode to anyone who calls you. Hang up, find your institution's phone number on a bank statement or on your credit card, and call. Ask if there really is a problem and report the con to the bank's fraud department, McKenna recommends.



LinkedIn Relationship Fakes

Move over, romance scams. AARP is receiving a growing number of complaints about business relationship scams.

THE CON: You get a message on LinkedIn, the popular workplace social media site, from someone who claims to be just starting out in the same industry you're in, seeking advice from a more experienced colleague. It's flattering and fun to be a mentor, and your guard is down because you're in a legitimate professional environment, says Amy Nofziger,

CONTINUED ON PAGE 10

FARE BULLETIN APRIL 2023

Cover Story

CONTINUED FROM PAGE 8

AARP's director of fraud victim support. You get to know each other, and eventually they ask to move your conversation onto a personal device, then lure you into a scam.

PROTECT YOURSELF: A request to continue your chat on a more private channel is a warning. So is talking up crypto. LinkedIn may flag requests to go off-platform as it tries to remove fake accounts. But you should end the conversation and block the scammer.



'I've Got Your Package, Where's Your House?' Hoax
Is that text, email, phone call or note on your door from a real

delivery driver?

THE CON: New package delivery scams include texts and phone calls purportedly from a professional-sounding delivery driver who can't find your house. Didn't order anything? They may try to convince you someone's sent a gift. Or you may receive an email about rescheduling a drop-off or a fake "package delivery attempt" sticker on your front door. Their goal? To get you to provide personal information or simply click on a link they provide. That link then downloads malware that will harvest passwords and account info from your computer or dial a phone number with high per-minute fees.

PROTECT YOURSELF: Contact the seller or delivery service using a verified phone number, the FCC recommends. Don't use numbers or links provided by potential scammers.



Out-of-Stock Item Scam
The email says the company is out of stock for the product you ordered. Where's your refund?

THE CON: Scammers often place fake ads on social media sites for products at too-good-to-be-true prices, take your order and payment info, then tell you the item's not available right now. Your refund is on the way, they promise, but it never arrives. And you can't reach anyone at the company about it.

PROTECT YOURSELF: Research businesses online before you buy, and only shop on secure websites with a lock symbol in the browser bar and an internet address that begins with "https." And pay by credit card, the FTC recommends. That way, you can withhold payment pending an investigation.

Sari Harrar is a contributing writer to AARP The Magazine and writes frequently for the Bulletin and others on fraud, health and consumer affairs.

to AARP BULLETIN APRIL 2023

—PART 2—

PROTECT YOURSELF

DO THESE THINGS TODAY TO REDUCE THE CHANCES OF LOSING MONEY (OR SLEEP) TO SCAMS BY AMY NOFZIGER AND MARK FETTERHOFF



MAILBOX

► Informed Delivery is a free service from the U.S. Postal Service. The agency emails photos of letter-size mail expected to be delivered to you that day or shortly after. This is a great way to be sure that nothing is stolen from your mailbox by ID thieves. Sign up at informed.delivery.usps.com.

► Pick up mail as quickly as possible after it's delivered, and always take your outgoing mail directly to the post office. A hot fraud now is scammers stealing checks from mailboxes, erasing the ink and using them to steal from bank accounts.

FRONT DOOR



► Consider installing a video camera; they are increasingly less expensive, and they're easy to install. If you don't recognize a visitor, don't answer.

► If you find yourself being pressured to buy or donate, have a refusal script ready (consider taping it near the door) that says, "I do not do business at my door, please leave me something to review. If I'm interested, I'll call you."

► Be wary of people posing as utility workers who show up unannounced. Don't allow anyone in your house without an appointment.

GARBAGE



► Shred any papers that contain private information (financial statements, bills, shipping receipts) before putting them out for pickup. Don't want to invest in a good cross-cut shredder? Many communities have shredding events or permanent drop-off sites. Get in the habit of dropping off your accumulated documents once every few months.

CREDIT CARDS

► Card skimming, in which the criminal affixes a credit card reader on top of a legitimate card reader at a store or gas station, is estimated to cause up to \$1 billion in losses annually. When you are paying at a gas station or other point-of-sale location, inspect the device for loose/broken/scratched machinery to make sure someone hasn't tampered with it. If you are unsure, notify the cashier and pay using an alternative method.



CREDIT REPORT

► Routinely check yours (many credit card companies provide it for free; if not, go to AnnualCreditReport.com or 1-877-322-8228). Watch for unusual activity; if you see any, report it immediately to the appropriate financial institution.

► Then freeze your credit report. This prevents scammers from opening new credit cards or making big purchases in your name. You can "unfreeze" it as needed for legitimate transactions. Visit IdentityTheft.gov for more information.

PHOTO ILLUSTRATIONS BY MATEL CHASE

Resources

WALLET

► Remove cards and information you don't need to carry (such as your Social Security or Medicare card). Make copies of the remaining cards (front and back) and store in a safe place.

► Audit your wallet and purse frequently. Take out any unnecessary items that collect and could compromise your personal information if lost or that would be a hassle to replace.



FINANCIAL ACCOUNTS

► Create online accounts with each of your financial institutions. Come up with a unique password for each.

► Then get in the habit of reviewing the transaction lists on a weekly or biweekly basis. Be sure you can account for every listed transaction. Spot something odd or incorrect? Immediately report it.



SMARTPHONE

► If you have a newer model, turn on biometric identification (fingerprint or facial recognition); this will help prevent a thief from logging in to your phone.

► Send calls from unknown numbers to voicemail (you can enable this in the phone's settings). Make sure your voicemail is set up and not full, so you can receive legitimate messages.

► Scammers are sending far more bogus texts, often posing as companies you routinely deal with. Never respond to an unsolicited business text; if you think it might be valid, call the organization or go online.

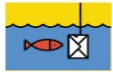
COMPUTER



► Turn on two-factor authentication for all secure websites you frequent, such as financial institutions or utility companies (find out how via its online security center). Then only someone logged in to your phone can receive the code to access those accounts.

► Yes, still consider subscribing to an antivirus software service. This remains the best protection against new attack methods.

EMAIL ACCOUNTS



► Actively designate unsolicited and unwanted email that shows up in your inbox as spam, so future emails from that site get blocked.

► Do not open file attachments in emails from businesses or people you don't trust completely. Malware is often planted via email attachments.

For discounts on device protection plans, visit aarp.org/mort-identity-theft.

SOCIAL MEDIA



► Set your profile so only your friends can see your Facebook page. To do that, click the downward arrow button in the upper-right corner of your Facebook page, then click on Settings & Privacy and Privacy Checkup. This easy-to-use wizard will guide you through the settings. And never accept friend requests from people you don't know or respond to random messages from strangers.

ONLINE STORES



► When typing in a URL, double- and triple-check the spelling to ensure you are on the correct page. Scammers often create a URL with one letter off from the authentic one in hopes you don't catch it.

► Remove your credit card number and information from restaurant delivery and retail store sites. Pay using an e-payment service that keeps credit card info on a highly secure site.



YOUR BRAIN

► Learn how to not engage. You are under no obligation in these modern times to respond to calls, emails or texts from strangers—especially given that so many of them are fraudulent.

► Learn to say no. Sometimes a caller will get through. Get tough: Say, "I do not do business over the phone. Goodbye." Then hang up without remorse.

► Trust your instincts. If something doesn't sound right, run it by someone you trust and take extra time to think about it.

Amy Nofziger is the director of fraud victim support with AARP.

Mark Fetterhoff is an AARP senior adviser who manages much of the AARP Fraud Watch Helpline and fraud-related grants.

ICONS BY ELIAS STEIN

AARP.ORG/BULLETIN

Resources

- Scams and fraud |USAGov - <https://www.usa.gov/scams-and-fraud>
- Scam, Fraud Alerts - Protect Your Digital Identity (aarp.org) - <https://www.aarp.org/fraud>
- AARP Fraud Watch Network Helpline – (877) 908-3360
-