Golden Belt Bank

Identifying and Avoiding Scams

SAFE BANKING FOR SENIORS®

ABA FOUNDATION

PRESENTATION

Golden Belt Bank

What We'll Discuss

- What a scam is
- Why scams work
- Types of scams
- Warning signs of scams
- Building scam defenses

What Is a Scam?

- A scam is a trick a con artist plays on an unsuspecting victim
- The goal is to extort money
- If the scam succeeds, the victim's money is gone and so is the scammer

Profile of a Scammer

A master of persuasion with a plausible story, or the ultimate salesperson with a tempting offer.

- Easily pinpoints a victim's vulnerabilities
- Quickly gains trust
- Won't take "no" for an answer
- Insist on secrecy

Contact Methods

- Emails
- Phone Calls
- Websites
- Social Media
- Text Messaging

Solving the Scam Problem

- The scam problem has one solution: knowing how to protect yourself
- To do that, you must recognize a scam when you see it!

Type of Scams

- Investment/Cryptocurrency
- Romance/Friendship
- Sweepstakes, Lottery, and Prize
- Family Imposter
- Government Imposter
- Tech Support
- Charity
- Home Improvement
- Phishing

Investment/Cryptocurrency Scams

- Investment described as low or no risk
- Above-average return guaranteed
- High-pressure sales tactics: Immediate purchase often required
- Fees and commissions ignored or obscured

1-800-BANKERS • aba.com/Consumers
© American Bankers Association
SAFE BANKING FOR SENIORS ABA FOUNDATION

Bitcoin ATMs

Romance/Friendship Scams

- Scammers create fake profiles on dating sites, apps, or social media sites
- They work to build trust and profess love quickly
- In a hurry to get off the site
- Make excuses to postpone in-person meeting
- Hard luck stories or pitch investment opportunity

1-800-BANKERS • aba.com/Consumers
© American Bankers Association
SAFE BANKING FOR SENIORS ABA FOUNDATION

Sweepstakes, Lottery, and Prize Scams

- Letter, email or call that's "thrilled" to announce you're a winner
- Requires an immediate response
- Requests up-front payment to
  - Release winnings
  - Secure the reservation
  - Prepay taxes

Family Imposter Scams

- Urgent call from scammer posing as family member or dear friend
- Family member or friend in serious trouble
- Money required immediately to resolve problem
- Secrecy is paramount

Government Imposter Scams

- Scammers say:
  - you did not appear for jury duty
  - your Social Security or Medicare benefits have been suspended
  - you owe back taxes or there's a problem with your return and ask you to verify your information
- You can avoid prosecution, arrest, or deportation if you pay what's due within 24 hours
- Payment must be made by wire transfer, gift card, banker's check, or cryptocurrency.

Tech Support Scams

- Pop-up warning with a fake error message and a number to call
- You may receive a phone call from scammer impersonating representatives from a technology company, like Norton, Geek Squad, Microsoft, or McAfee
- Criminals try to convince victims to provide remote access to their computers to "troubleshoot" an issue

Charity Scams

- Urgent plea for humanitarian help
- Pressure to make immediate donation
- Sometimes little more than a sad story and a carefully chosen name

Home Improvement Scams

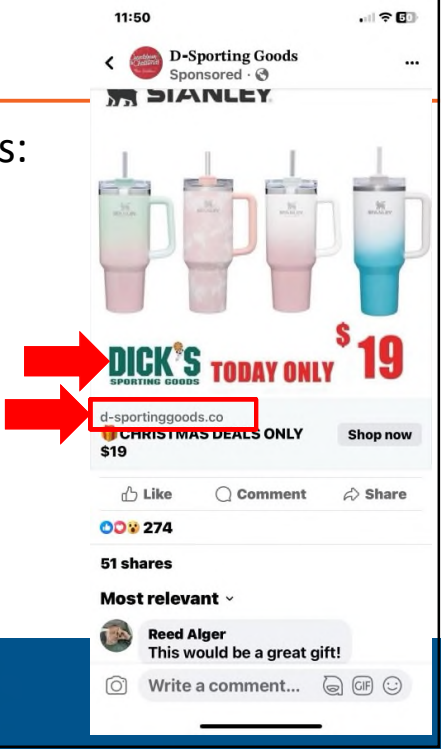
- Solicits a job by pointing out an “urgent” problem
- Asks for up-front payment in cash
- Begins the job, but claims it’s much more serious than initially thought
- Demands more money
- Disappears with the work unfinished

Phishing Scams

Typically use one of three methods to fool victims:

- Message promises a reward
- Threatens a punishment
- It appears harmless

Urges you to click a link, share information, call a phone number or download an attachment.



Spotting Scams

All scams have warning signs

- Too good to be true
- Immediate action required
- Insistence on secrecy or want to move conversation off-platform
- Money needed up front
- Hard-to-track payment methods

Block Those Scammers

- Register with National Do Not Call Registry at www.donotcall.gov to limit phone calls
- Use anti-virus software
- Be very cautious about clicking on email links
- Check privacy settings and limit personal information on social media

Build Your Scam Defenses

- Be suspicious of any situation that requires you to send money up front
- Assume that insistence on secrecy is a ploy to deceive
- Confirm all stories, offers or charities independently
- Take no action for **at least** 24 hours

If You're a Scam Victim

- Don't be embarrassed or afraid
- Tell someone you trust
- Report the scam to your bank
- Contact the police and federal agencies

Your Bank Can Help

- Monitor your account for unusual activity
- Ask why you are withdrawing large amounts of cash
- Suggest giving a person you trust access to review your account activity
- Explain why scammers prefer certain payment methods
- Provide referrals to a licensed broker or registered investment adviser

SCAM DEFENSES TO-DO LIST

Golden Belt Bank

Golden Belt Bank

SCAM DEFENSES TO-DO LIST

SPOT POTENTIAL SCAMS

Is immediate action required? ☐ Yes ☐ No

Am I being asked to keep the request for money a secret?
☐ Yes ☐ No

Is the money required upfront before any products or services are provided? ☐ Yes ☐ No

Am I being asked to pay in a hard-to-track payment method?
(ie. money orders, wire transfers, gift cards) ☐ Yes ☐ No

If you answer YES to any of the above, STOP!
Ask for help to investigate further BEFORE taking any action.

REMEMBER:

- Never send money upfront.
- Assume that if secrecy is essential, it's because there's something to hide.
- Confirm everything you're told with an independent source. Look up phone numbers, check credentials, contact your family or financial caregiver.

STAY SAFE ONLINE

- [ ] Stop. Look. Think. BEFORE clicking.
- [ ] Limit personal information shared on social media.
- [ ] Review the email phishing material in this book on pages 31-32.

PROTECT MYSELF

- [ ] Register with National Do Not Call Registry at **www.donotcall.gov** to limit phone calls.
- [ ] Register with **www.DMAchoice.org** to limit junk mail. (Minimal fee applies.)
- [ ] Have anti-virus software installed by a local professional.
- [ ] Create and rehearse a refusal script for calls that you answer from someone you don't know.
- [ ] Create a process to shred/destroy identifying information before discarding.
- [ ] Review your bank and credit card statements every month and report any transactions you don't recognize or didn't authorize to your bank immediately.
- [ ] Consider signing up for credit card and debit card text alerts.

SCAM TIP SHEETS

Golden Belt Bank

What is a Scam?

A scam is a trick a con artist plays on an unsuspecting victim to extort money. If the scam succeeds, the victim's money is gone, and the scammer will move on to the next victim.

A scammer is the ultimate salesperson with a tempting offer or a skilled liar with a plausible story

- Easily pinpoints a victim's vulnerabilities and appeals to emotions: sympathy, fear, loneliness
- Quickly gains trust
- Insist on secrecy
- Shows no mercy, e.g., doesn't take "no" for an answer

Know the Red Flags of a Scam

- Immediate action required
- Insistence on secrecy
- Money needed up front
- Hard-to-track payment methods

Build Your Scam Defenses

- Do not be rushed into any financial decision
- Assume that insistence on secrecy is a ploy to deceive you
- Be suspicious of any situation that requires you to send money up front
- Confirm all stories, offers or charities independently
- Be very cautious about clicking on email links

Block Those Scammers

- Register with National Do Not Call Registry at **www.donotcall.gov** to limit legitimate telemarketing phone calls, making phone scams easier to detect
- Register with **www.DMAchoice.org** to limit legitimate advertising mail, making mail scams easier to detect
- Limit personal information on social media and choose the strictest privacy settings on social media accounts
- Use antivirus software on your computer

What to Do If You Are Scammed

- Don't be embarrassed or afraid
- Tell someone you trust
- Report the scam to your bank immediately to limit losses
- Contact your local police and federal agencies, like the Federal Trade Commission

SAFE BANKING FOR SENIORS®
ABA FOUNDATION

For more information, visit **aba.com/Seniors**

5 Ways to Spot a Lottery Scam

Solicitation scams, commonly referred to as an "advance fee," "lottery" or "sweepstakes" scam, often begin with fraudsters telling the victim they won the lottery or a raffle. The consumer may be issued a check worth more than the amount owed and instructed to pay taxes and fees before receiving a lump sum payment. Unfortunately, the check—in addition to the raffle—is bogus.

1. **Don't be fooled by the appearance of the check.** Scam artists use sophisticated technology to create legitimate-looking counterfeit checks, money orders, and cashier's checks. The company name may be real, but someone has forged the checks without their knowledge.
2. **Never "pay to play."** If someone who is giving you money asks you to wire money back or send more than the exact amount—that's a red flag that it's a scam. If a stranger wants to pay you for something, insist on a cashier's check for the exact amount, preferably from a local bank or one with a local branch.
3. **Verify the requestor before you wire funds or issue a check.** It is important to know who you are sending money to before you make a payment. Confirm the requestor is a trusted source.
4. **Just because the check has cleared does not mean it's good.** Under federal law, banks must make deposited funds available quickly, but it can take days for the bank to learn that a check was bad.
5. **Report suspected fraud to your bank immediately.** Bank staff are trained to spot fraudulent checks. If you think someone gave you a fake check, don't deposit it—report it. Contact your local bank and report it to the Federal Trade Commission at **ReportFraud.ftc.gov**.

Don't Fall Victim to the Grandparent Scam

A grandparent scam is a type of impostor scam. Fraudsters call claiming to be a family member who needs money immediately for an emergency. They may have information about you, including your name and where you live. They'll claim to be stranded, in jail, or require help paying medical bills.

Scammers will beg you for money, ask you to keep it a secret, and urge you to act quickly. Usually, they will tell you to wire money, pay with gift cards, or send cryptocurrency. Stop! Don't pay—it's a scam! If you send money, you won't be able to get it back.

- **Confirm the caller.** Fraudsters are using social networking sites to gain the personal information of friends and relatives to carry out their crimes. Verify who's calling by contacting the person directly on a known number, or consult a trusted family member.
- **Don't be afraid to ask questions.** Fraudsters want to execute their crimes quickly. In this type of scam, they count on fear and your concern for your loved one to make you act before you think. The more questions you ask, the more inclined they will be to ditch the scam if they suspect you're on to them.
- **Never give personal information to anyone over the phone** unless you initiated the call and you trust the other party.
- **Never rush into a financial decision.** Don't be fooled—if something doesn't feel right, it may not be right. It's not rude to say no and get more information, or decline to act.
- Report it to the Federal Trade Commission at **ReportFraud.ftc.gov**.

IRS Imposter Scams

Scammers claiming to work for the Internal Revenue Service (IRS) may reach out via phone, email, or text to say you owe money to the government. Look out for any of these scenarios:

- **Taxes** – The fraudsters will say you owe taxes and demand that you pay right away. They usually require payment through a wire transfer, a prepaid debit or gift card, or funds via a mobile payment app. Often, the criminals will threaten arrest or deportation if you don't pay.
- **Information Verification** – The scammer will send you an email or text message that asks you to confirm or authenticate your personal information. The messages often include a link to click or another feature that connects you to a fraudulent form or website.

Don't Be a Victim

- Be wary of anyone claiming to be from the IRS. The IRS will always contact you via postal mail before making a call about unpaid taxes.
- The IRS won't threaten to arrest you for not paying a bill.
- If the IRS does contact you, they will offer you time to submit an appeal.
- Scammers can spoof caller ID and change the name that appears on your phone, so don't trust the caller just because it shows up as "IRS."
- If you think you owe back taxes, you can check with the IRS by calling **1-800-829-1040**.

Report the Scam

If you think you've been scammed, report the incident to the IRS at **phishing@irs.gov**.

Social Security Scams

Americans have lost millions of dollars from Social Security scams. Fraudsters reach out to unsuspecting victims to steal benefits and to obtain personal information. Victims are often exploited through two common scenarios:

Phone Call

For many, it starts with an unsolicited phone call:

An individual impersonating a government official tells the victim that their Social Security number has been suspended or linked to criminal activity.

The victim is asked to confirm the Social Security number for security purposes.

The fraudster then offers to issue a new number or reactivate the old one for a fee.

In complying, the victim shares everything that the fraudster needs to steal the victim's identity.

Office Closures

A fraudulent letter threatening to suspend or discontinue Social Security benefits due to office closures amid a crisis is sent to the victim.

The letter instructs the victim to call a number.

Once the victim makes the call, fraudsters will manipulate callers into sharing personal information and/or remitting payment via gift cards, wire transfers, cryptocurrency or cash.

Recognize the Signs

The best way to protect yourself is to recognize the signs of a scam and remember not to engage with scammers.

- If you receive an unsolicited call, email or text asking for your Social Security number, be suspicious and don't share it.
- Fraudsters try to incite fear, encourage secrecy and make you act before you can think. Don't be afraid to hang up.
- **The Social Security Administration will never:**
  - Threaten you with benefit suspension, arrest or other legal actions unless you pay a fine
  - Require payment via gift card, cash, wire transfer, cryptocurrency or prepaid debit card

If you have questions, always confirm by calling the Social Security Administration directly at **1-800-772-1213**.

Tech Support Scams

Tech support scams often begin with a phone call or a pop-up window displaying a fake error message with a number to call. Scammers often impersonate representatives from a tech company—such as Apple, Google or Microsoft—to persuade victims to provide remote access to their computers to "repair" an issue, such as malware.

If the victim provides access to the device, criminals will scan the computer to "troubleshoot the problem" and offer fake solutions. They may install dangerous computer applications or encourage the victim to pay for a phony subscription. In the process, the scammers steal the victim's money and identity.

Don't Be a Victim

- Hang up the phone if you receive an unsolicited call from someone who says there's something wrong with your computer.
- Be suspicious of pop-up warnings. Security pop-ups from real tech companies will not ask you to call a phone number.
- Do not give access to your computer or share passwords with anyone who contacts you.
- Keep your computer's security software up to date.

If Scammed

- Contact your bank to report fraud and check your statements.
- Change passwords to your computer, bank accounts and other sites.
- Scan your computer for viruses and call your security software company for help.
- Report it to the Federal Trade Commission at **ReportFraud.ftc.gov**.

How to Safely Use Mobile Payment Apps and Services

Online payment systems or apps like Zelle, Venmo, and CashApp let you quickly send and receive money. If you link the service to your bank account or debit card, it's almost like handing someone cash. Be sure you know who you're sending money to. Once you send money, it's nearly impossible to get it back.

AVOID SENDING MONEY TO A SCAMMER

Don't click on links in an unexpected email, text message, or direct message that asks you to send money. Don't give any personal or sensitive information like your username, PIN, or password.

Confirm that you know the person you're sending money to.

When sending to someone you know, **double-check their information** before you hit send.

PROTECT YOUR ACCOUNTS

Use multi-factor authentication. This means you need two or more credentials to get into your account: your password plus something else like an authentication code or fingerprint.

Never share your credentials, like a verification code you get via text or authentication app.

Set up alerts in the payment app to get transaction notifications outside of the app environment, such as via email or text.

Regularly check your payment app and bank accounts to make sure no unauthorized payments have been sent from or accepted by your account.

Paid a Scammer Through a Payment App?

- **Report it to the payment app or service and ask to reverse the transfer.**
- **Tell your financial institution.**
- **Report it to the Federal Trade Commission at ReportFraud.ftc.gov.**

Learn more at **ftc.gov/paymentapps** and **aba.com/consumers**

ABA FOUNDATION®

Money Mules Fuel Fraud

What are money mules?

Money mules are people who receive and move money obtained from victims of fraud. Some money mules know they've been recruited to assist criminal activity, but others become money mules without realizing their activity is benefiting fraudsters.

How do people become money mules?

- Responding to a job advertisement or social media post that promises easy money for little effort.
- Helping someone they've met online (possibly on a dating website) or over the phone by agreeing to receive and transfer money.

Whether it is cash, packages, gift cards, or virtual currency, assisting money movement puts money in the pockets of criminals and could lead to serious consequences for you.

By knowing the signs of money mule activity, you can protect yourself and your community, and avoid assisting fraudsters.

Think twice about agreeing to help people move money!

- Don't open a bank account or move money at someone else's direction.
- Don't give someone access to your bank account or debit card.
- Don't allow money from people you don't know to be deposited into your account.
- Don't take a job that promises easy money and involves sending or receiving money or packages.
- Don't agree to receive or forward packages.
- Don't agree to purchase gift cards or virtual currency at someone's direction.

If you've acted as a money mule, it is never too late to stop!

- Stop communicating with the person giving you direction.
- Tell your financial institution and consider changing accounts.
- Report suspicious communications or activity to law enforcement.
- Protect yourself by learning about scams and money mule activity.

Money mules help international criminal networks steal money from senior citizens, businesses, and people just like you.

#DontBeAMule

For more information, visit
www.justice.gov/civil/consumer-protection-branch/money-mule-initiat ve

Image © Europol

Money Mule Scams

If someone sends you money and asks you to send it to someone else, STOP. You could be what some people call a money mule — someone scammers use to transfer and launder stolen money.

Scammers often ask you to buy gift cards or wire money. They might recruit you through online job ads, prize offers, or dating websites.

Scammers:

Send you a check

Tell you to send some of the money to someone else

When you later find out the check was bad, you could be stuck covering the entire amount of the check, including what you sent. And that might overdraw your account.

HOW TO AVOID A MONEY MULE SCAM:

Never use your own bank account, or open one in your name, to transfer money for an employer.

Never pay to collect a prize or move any money out of your "winnings."

Never send money to an online love interest, even if he or she sends you a check first.

WHAT TO DO if you spot this scam:

Break off contact with the scammers and stop moving money for them.

Tell your bank and the wire transfer or gift card company — right away.

Report it to the Federal Trade Commission at ftc.gov/complaint.

Criminals are good at conning people into helping them move money. Don't do it. You could lose money and get in trouble with the law.

ftc.gov/ScamAlerts

ABA FOUNDATION aba.com/Consumers

CRYPTO INVESTMENT SCAMS

ABA FOUNDATION

WHAT YOU SHOULD KNOW

Crypto* investment scams, commonly referred to as "pig butchering" by scammers, cost consumers billions of dollars. Criminals befriend people to entice them to make crypto investments through phony apps and websites. The investments may start out slowly with small sums of money, but it's a scam aimed at stealing tens of thousands to millions of dollars.

**Crypto is also referred to as cryptocurrency by users*

HOW DO CRIMINALS TARGET PEOPLE & HOW DOES THE CON START

HOW DOES THE CON START?

Criminals often pose as people interested in:

- Friendship,
- Romantic relationships, or
- Business investments.

Using fake profiles, they take time and build connections with their targets. They claim to be, or to know, experts who can help investors make money. To mask their identities, they:

- Use fake phone numbers (spoofing)
- Rely on deepfake videos, voices or images
- Employ artificial intelligence

They target people through texts, dating sites, social media channels, professional networking platforms and/or other apps. After establishing trust with their victims, criminals move conversations to encrypted messaging apps and introduce crypto.

They coach victims into investing using fake platforms. Websites might look legitimate, but it's all phony and controlled by criminals. Once people begin "investing," criminals manipulate the sites/apps to show fake profitable returns. Victims might even be allowed to make initial withdrawals, but it's a ploy to encourage further investments.

HOW DOES IT END?

When victims try to withdraw larger sums of money, they are told they need to pay a fee or taxes. But there's no getting the money back, even if they pay the supposed fees or taxes. In the end, victims lose everything they invested.

PROTECT YOURSELF

- Research before you invest in anything.
- Recognize that pressure to "act fast" might be a sign of a scam.
- Do not send money to anyone you meet online or via apps, and don't make investments based on their advice.
- Do not download or use any unfamiliar apps.
- Do not pay for services that claim they can recover lost funds.
- Do not trust anyone who offers a "sure bet." All investments involve risk.
- Recognize that even video chats and online trading platforms which appear real can be fake.

WARNING SIGNS

- Unexpected contact by an unknown person.
- Requests to limit contact with financial institutions or advisors.
- New online friends sharing "can't-miss" investment opportunities.
- Sense of urgency to invest more money or pay fees.
- Misspelled web links.

IF YOU HAVE BEEN VICTIMIZED

Stop sending money to the criminals.

Contact your bank.

Keep records and communications relating to the scam.

File a report with the FBI Internet Crime Complaint Center at **IC3.gov**.

ABA Foundation is proud to work with:

Commodity Futures Trading Commission

Department of Justice Federal Bureau of Investigation

U.S. Treasury Financial Crimes Enforcement Network

FINRA

Homeland Security Investigations

IRS-CI

United States Secret Service

U.S. Securities and Exchange Commission Investor.gov

OTHER RESOURCES

Golden Belt Bank

Fraud Questionnaire

Scammers pressure people into sending money to them because it's easy and effective. Sending or wiring money or gift cards is like sending cash. ONCE IT'S GONE, you most likely can't get it back.

As part of the bank's due diligence program, we ask that you review the questions below prior to wiring funds or withdrawing large sums of cash from your account.

Have you been contacted by someone via email, text or phone who…

1. Has instructed you to place your phone in your pocket or somewhere on your person and turn speaker phone to listen to your conversation with the bank today? ☐ Yes ☐ No

2. Claims to be with law enforcement, investigation bureaus, financial institution regulatory agency (FDIC, etc) and has asked you to withdraw money to help with an investigation? ☐ Yes ☐ No

3. Claims to be with a utility company and is demanding payment for past due bills in order to avoid suspension of services? ☐ Yes ☐ No

4. Is a stranger or someone from another country and has asked you to make a withdrawal for any reason? ☐ Yes ☐ No

5. Befriended you and is asking you to invest in or purchase crypto currency, bitcoin, etc or to share cash or valuables? ☐ Yes ☐ No

6. You met online via social media or dating platform? ☐ Yes ☐ No

7. Claims to be a city inspector, employee or repairman that has found code violations or repairs that are necessary to your home or property or insists that you owe money for a service? ☐ Yes ☐ No

8. Claims to have found money that they will share with you if you give them a "good faith" payment? ☐ Yes ☐ No

9. Claims that a recently deceased spouse made a large purchase before their death and now you are obligated to pay for it? ☐ Yes ☐ No

10. Has asked you to send money in order to claim a much larger prize or larger amount of money? Ex. A lottery or drawing in which you do not recall participating? ☐ Yes ☐ No

11. Has asked you to send money for taxes or other reasons to receive an inheritance? ☐ Yes ☐ No

12. Wants you to invest or fund a new business venture domestically or internationally? ☐ Yes ☐ No

13. Claims to be a family member or friend (or acquaintance of) that has been injured, stranded, robbed or arrested and needs you to send funds? ☐ Yes ☐ No

14. You have done business with in the past but is now providing new wiring instructions such as routing and account number? ☐ Yes ☐ No

15. Are you wiring funds **recently deposited** into your account from someone **you do not know** or someone **you have not met in person?** ☐ Yes ☐ No

16. Have you allowed anyone that you do not know to remote into your PC? ☐ Yes ☐ No

IMPORTANT: If you answered YES to ANY of the previous questions and you proceed with the wire transfer request or the cash withdrawal, you acknowledge that this transaction may be a scam or other high risk transaction. The previous examples are only some of the ways customers become victims of scammers. In many cases these transactions are fraudulent and the money is NOT recoverable.

By signing below, you acknowledge that you will be held responsible for any losses and/or negative balances with your account that may occur as a result of this transaction.

I have read and understand the above statement. I request that Golden Belt Bank, FSA complete my transaction.

Account Number: _____ Transaction Amount: _____ ☐ Cash ☐ Wire Transfer

Customer Signature: _____ Date: _____

Bank Employee Signature: _____ Date: _____

Bank Officer Approval: _____ Date: _____

Bank Officer Approval is required if the customer answered YES to any of the questions.

Be On The Lookout For **Phishing!**

Phishing is when a cybercriminal uses email to trick you into giving them private information or taking a dangerous action. The consequences of falling for a phishing email can be catastrophic.

Protect yourself and your organization by learning to track down these signs of phishing emails!

Mysterious Messages

Phishing emails often appear to come from someone you know or trust. But they can also come from unknown senders.

Always check the sender's email address and make sure it matches the trusted source's email address.

Urgent Demands

Phishing messages often direct you to take action immediately, implying that something negative will happen if you don't. These messages are meant to get you to react before you think.

Always stop and think before taking an action. Does the request make sense?

Sneaky Links

One of the most common signs of phishing is the request to open an unexpected link or attachment. Malicious links or attachments can be used to steal your login info or other data.

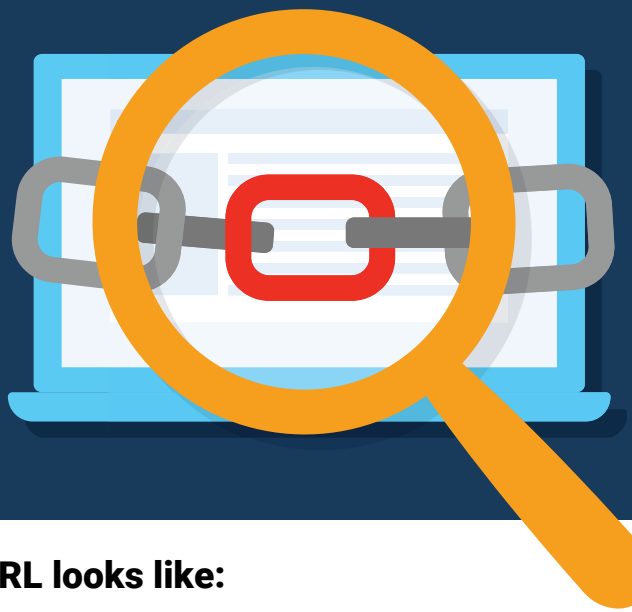
Never open links or attachments from unknown or suspicious senders. If you need to sign in to a website, go directly to the known, legitimate address.

Before taking an action, stop, look, and think!

Does it seem suspicious, out of place, or just strange?
Then report the message and delete it immediately!

KnowBe4

Learn how to spot a bad link.



This is what a URL looks like:

https://mail.google.com/gmail

Protocol | Subdomain | Domain | Top level domain | Path

Clicking on a **bad link** will take you to a completely different site.

To identify possible bad links you need to look out for:

- **Numbers** in front of the domain name, https://192.45.36.72-mybank.com
- **Hyphens** in front of domain names takes you to a completely different site https://secure-mybank.com
- **Full stops** splitting a domain name or misspelled domain name https://mybank.safetyy.com/

If you hover your mouse over a link it will show you the address it will take you to.

- **Avoid** interacting with malicious links.
- **Check** shortened links using a link expander.
- **Create** bookmarks for links you visit frequently.
- **Do not** click on links from an email.

Be careful when it comes to clicking on links.
Take a **moment** to think about your **cybersecurity**.

REFUSAL SCRIPT EXAMPLE

We know being caught in any form of communication with a fraudster can be overwhelming and hard to get out of. That's why we have found the tools to help, including the right things to say to get out of a fraudsters scam.

Below is what is called your 'Refusal Script', this will be used to provide language you or a family member might need to end a fraudulent call.

(Pick up phone call, and say)

'I'm sorry, I can't talk right now. I'm having coffee with Officer Brad'

(Proceed to hang up)

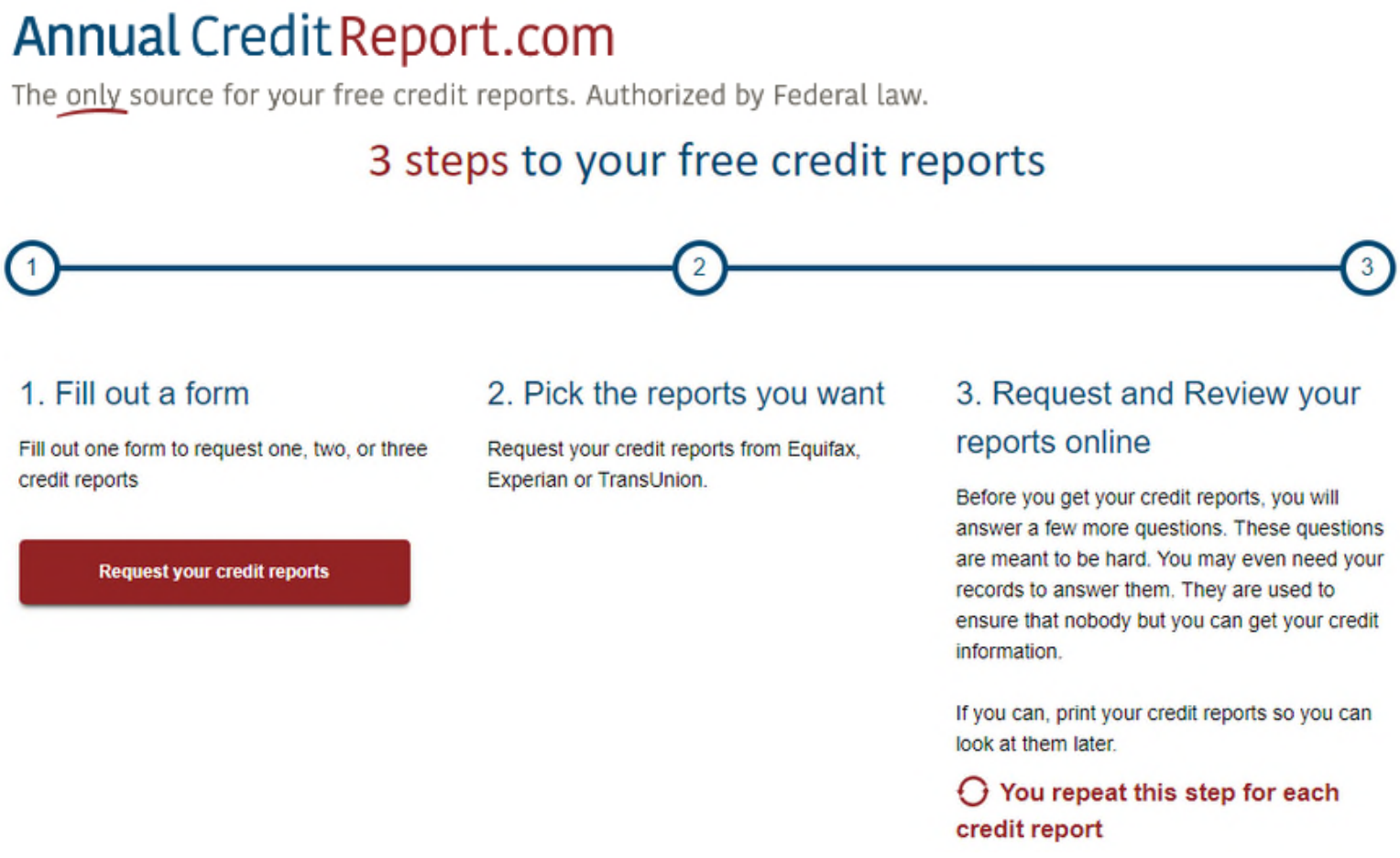
We advise that you keep the script next to your phone or door as reinforcement.

HOW TO KEEP UP ON YOUR CREDIT REPORT

Regularly checking your credit reports can help you be more aware of what lenders may see. Checking your credit reports can also help you detect any inaccurate or incomplete information.

You are entitled to a free credit report every 12 months from each of the three major consumer reporting companies (Equifax, Experian and TransUnion).

Visit www.annualcreditreport.com for your free credit report.



OptOutPrescreen.com

OptOutPrescreen.com

is the official Consumer Credit Reporting Industry website to accept and process requests from consumers to Opt-In or Opt-Out of firm offers of credit or insurance.

EQUIFAX experian. Innovis TransUnion

What is the purpose of this website?

Under the Fair Credit Reporting Act (FCRA), the Consumer Credit Reporting Companies are permitted to include your name on lists used by creditors or insurers to make firm offers of credit or insurance that are not initiated by you ("Firm Offers"). The FCRA also provides you the right to "Opt-Out", which prevents Consumer Credit Reporting Companies from providing your credit file information for Firm Offers.

Through this website, you may request to:

Opt-Out from receiving Firm Offers for Five Years - (electronically through this website).

Opt-Out from receiving Firm Offers permanently - (mail Permanent Opt-Out Election form available through this website).

Opt-In and be eligible to receive Firm Offers. This option is for consumers who have previously completed an Opt-Out request - (electronically through this website).

What are the benefits of receiving firm offers?

Equifax, Experian, Innovis, and TransUnion, (collectively the "Consumer Credit Reporting Companies"), encourage you to make an informed decision about receiving firm (preapproved / prescreened) offers of credit or insurance. There are several benefits of receiving firm offers.

Consumers are provided with product choices

Consumers learn about and have an opportunity to take advantage of offers that may not be available to the general public

Firm offers help consumers to "comparison shop", which may increase a consumer's buying power.

For more information on the benefits of receiving firm offers, click on the link below to view a PDF version of the report to Congress from the Federal Reserve on Unsolicited Offers of Credit and Insurance. See pages 32-40, "Benefits of Receiving Written Offers of Credit or Insurance"

Benefits of Receiving Written Offers of Credit or Insurance

Identifying and Reporting Fraud and Scams

Learn more about how to protect yourself or your loved ones from financial fraud and scams:

Recognize and Report Fraud and Scams

Better Business Bureau	bbb.org/scamtracker
Banks Never Ask That	banksneveraskthat.com
Federal Bureau of Investigation	fbi.gov/scams
Federal Trade Commission	consumer.ftc.gov/scams
Elder Fraud Hotline	1-833-372-8311

Accessing Credit Reports and Scores

Review your credit report at **AnnualCreditReport.com**

Contact the three credit bureaus:

Equifax	equifax.com	1-888-378-4329
Experian	experian.com	1-888-397-3742
TransUnion	transunion.com	1-800-916-8800

Get Help for ID Theft

Federal Trade Commission	identitytheft.gov	1-877-382-4357
ID Theft Resource Center	idtheftcenter.org	1-888-400-5530

SAFE BANKING FOR SENIORS®
ABA FOUNDATION