Avoiding Scams in Alaska

Alaska Department of Law Consumer Protection Unit

Filing a consumer complaint:

- Complaint forms are available on the Consumer Protection Unit website at http://www.law.alaska.gov/department/civil/consumer/cp_complaint.html
- **Consumer complaints are our most important tool for identifying businesses with a pattern of bad conduct.**

Contacting the Consumer Protection Unit:

- By email at consumerprotection@alaska.gov
- By phone at **907-269-5200** or toll free outside of Anchorage at **1-888-576-2529**

What is a Scam?

- For this presentation, we're going to be talking about mass scams that contact you by phone, email, or mail.
- These scams are particularly dangerous because many of these scammers are overseas, and it is extremely difficult to recover money once it has been sent.
- AI scams are often just more sophisticated versions of common scams.

Explore Age & Fraud Loss

Source: FTC's Consumer Sentinel Network

Select Age: 20 - 29 | **30 - 39** | 40 - 49 | 50 - 59 | 60 - 69 | 70 - 79 | 80 & Over

Select Year: 2023

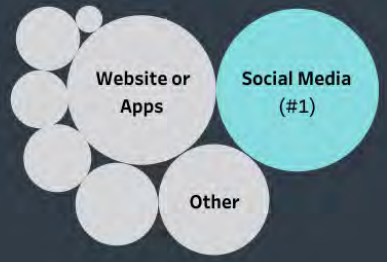
Fraud affects every generation differently.

Top Loss Reports for People Aged 30 - 39

1. Online Shopping
2. Business Imposters
3. Miscellaneous Investments & Investment Advice
4. Government Imposters
5. Job Scams & Employment Agencies

Payment Method

Contact Method



Explore Age & Fraud Loss

Source: FTC's Consumer Sentinel Network

Select Age: 20 - 29 | 30 - 39 | 40 - 49 | 50 - 59 | **60 - 69** | 70 - 79 | 80 & Over

Select Year: 2023

Fraud affects every generation differently.

Top Loss Reports for People Aged 60 - 69

1. Online Shopping
2. Business Imposters
3. Miscellaneous Investments & Investment Advice
4. Government Imposters
5. Romance Scams

Payment Method

Contact Method

Spotting a Scammer

- A scammer wants three things:
  - To get your attention.
  - To get you to act fast.
  - To get your money in a form that you can't retrieve.

Trust your gut:

If you think it might be a scam, it probably is!

Scams aren't Boring

FINAL NOTICE

- A scammer is like a advertiser: they need to get your attention.
- Scams often present you with a deal too good (or a situation too bad) to be true.
- Scams often pretend to be from legitimate government agencies or companies.

Congratulations!!!

No time to think

- A good sign of a scam is that somebody is asking you to take action right away.
- A scammer doesn't want you to take time to talk to somebody or do research.

No time to talk

- A scammer doesn't want you to talk to anybody who might tell you you're being scammed.
- They will pressure you to act fast, and they may tell you not to talk to other people.

It’s All About the Money

- The scammer wants you to send money in a way that can’t easily be retrieved.
- A scammer may ask you to transfer money through Western Union or MoneyGram.
- These days, its likely that a scammer will ask you to buy a gift card or pre-paid debit card and then provide them with the payment information.

Gift Cards are for Gifts, not Payments

- If somebody asks for payment in the form of a gift card, they are a scammer.
- Gift cards look like credit cards, but they function like cash. Whoever has the payment information from the card can use it without any verification.
- *A gift card is as good as cash to a scammer.*

Information is Money

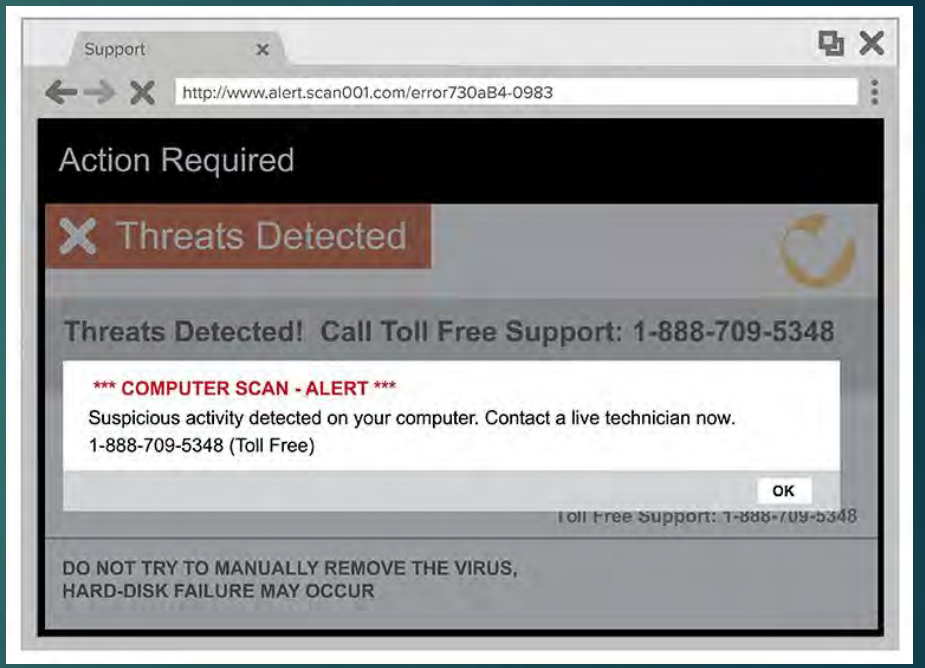
- If a scammer gets your Social Security Number, they can, among other things, open credit cards in your name, use them, and not pay the bill.
- Some scammers will attempt to get your SSN or banking information by posing as your bank or the Social Security Administration and asking for personal information to verify your identity.

Cold Call: Tech Support Scam

- Somebody calls you claiming that they work for Microsoft.
- They say that they have detected a virus or some other problem on your computer.
- They tell you that you need to take action to address the virus immediately.
- They ask you to give them remote access to your desktop so that they can run diagnostics.

Cold Call: Tech Support Scam >>How do you know it's a scam?

- Tech companies will never call you to tell you that there is a virus on your computer.
- Remember, scammers will try to confuse you, and get you to act in ways you wouldn't otherwise by creating fear.
- Tech support scammers may also call you to demand payment for a non-existent piece of software or computer security subscription.
- Tech support scammer my try to get you to call them through pop-up with the logo of large tech companies on them. Real security notices will never ask you to call a phone number.



Cold Call: Grandchild Scam

- Somebody calls you claiming to be your grandchild or other relative.
- Something has happened. They need help right away.
- They need you to wire money to an account or go to the store, buy gift cards and read them the payment information.
- They tell you “Don’t tell Mom and Dad!”

Cold Call: Grandchild Scam >>How do you know it's a scam?

- Urgency is always a good sign of a scam.
- Remember, scammers can glean personal details about your family members from social media.
- A scammer may hand off the phone to somebody pretending to be a police officer. But this is just a trick to make the scam seem credible.

Voice Mimic Scams

- Have a family password, or ask questions only your relative would know like “what did I get you for your birthday?”

Cold Call: Unpaid Debt Scam

- Somebody calls you or texts you and says they are from the IRS.
- They tell you that you have unpaid taxes and that you will be arrested unless you pay right away.
- You can pay by transferring money to a particular bank account.

Cold Call: Unpaid Debt Scam >>How do you know it's a scam?

- Its extremely unlikely that a real government agency would threaten you with arrest.
- If you're not sure if you're speaking to the actual government agency, hang up, find the number for the real agency, and call them.
- A variation of this scam is somebody claiming that you've missed jury duty and owe a fine.

Cold Call: “Verification” Scam

- Somebody calls you and says they are from your bank.
- There is a problem with your account. In order to fix it, they need to verify that you’re the owner of the account.
- To verify that you’re the owner of the account, they need you to tell them your account information.

Cold Call: “Verification” Scam >>How do you know it’s a scam?

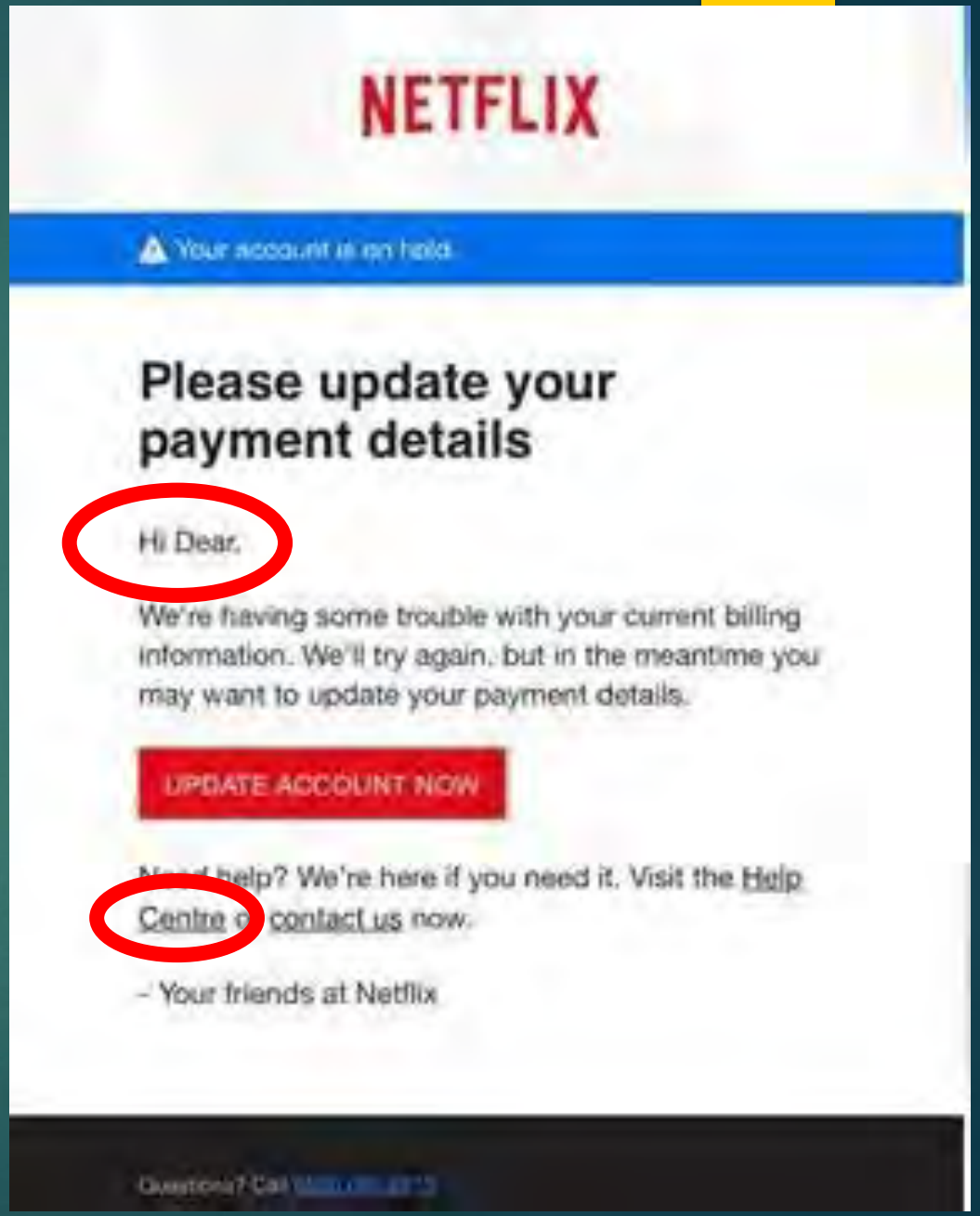
- A bank will not ask for account information to verify that you’re the account owner.
- You should hang up and call your bank directly.
- A variation of this scam is somebody calling from the SSA claiming that there is an issue with your benefits.

“Phishing” Emails

- “Phishing” is a term for a wide variety of email scams that attempt to get your personal information.
- It’s important that you don’t click on links in suspicious emails. These links can install malware on your computer. More likely, they will take you to a “spoofed” website that will ask you to enter personal information.

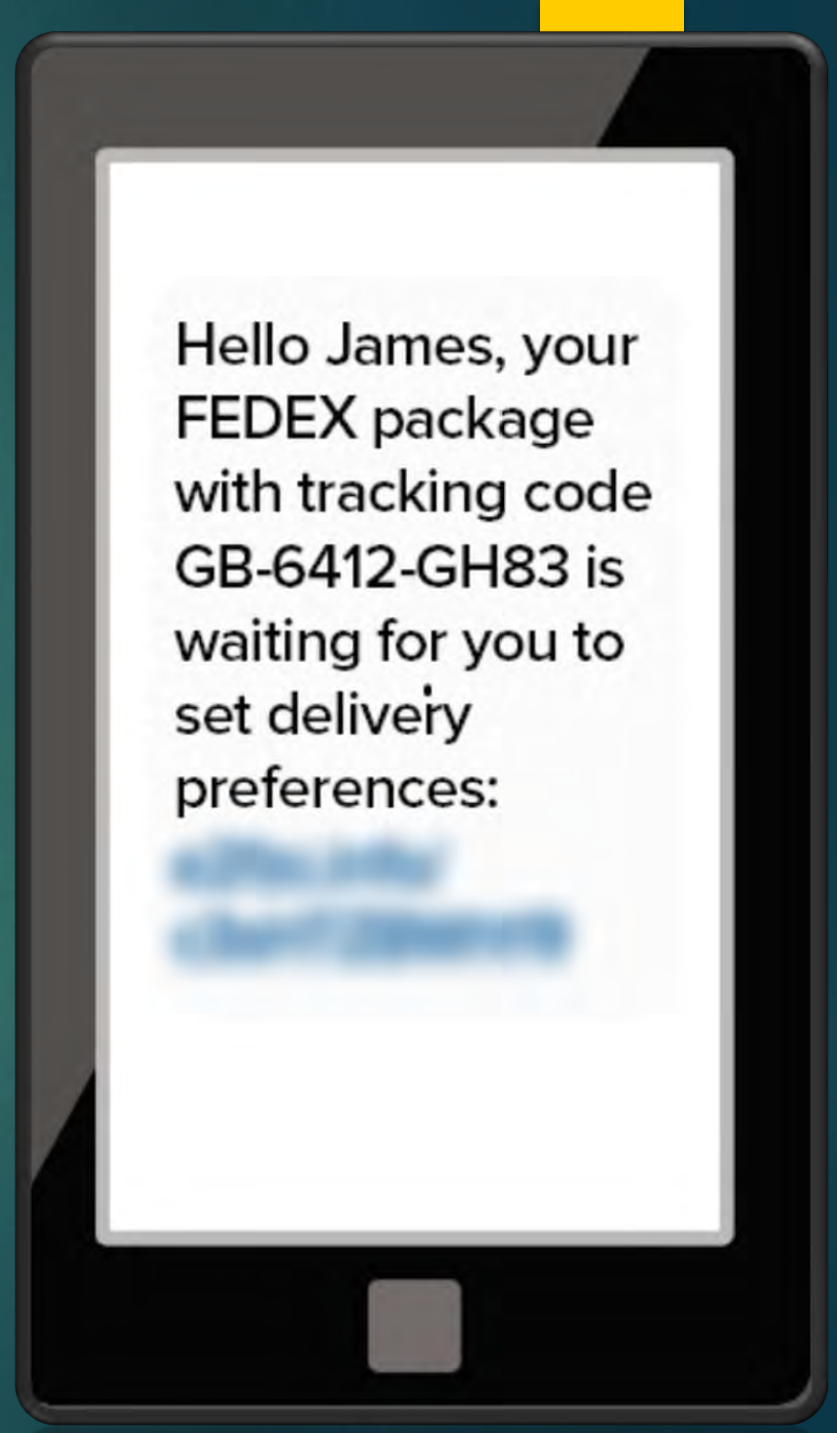
“Phishing” Emails

- Hard to spot, because scammers can use names and images from real companies.
- Look for generic greetings and misspellings.
- You should always contact the real company or agency directly.



“Phishing” Texts

- Like with emails, you should never follow links in suspicious texts.
- Again, its smart to follow the rule that you shouldn’t give personal information to somebody who contacts you.

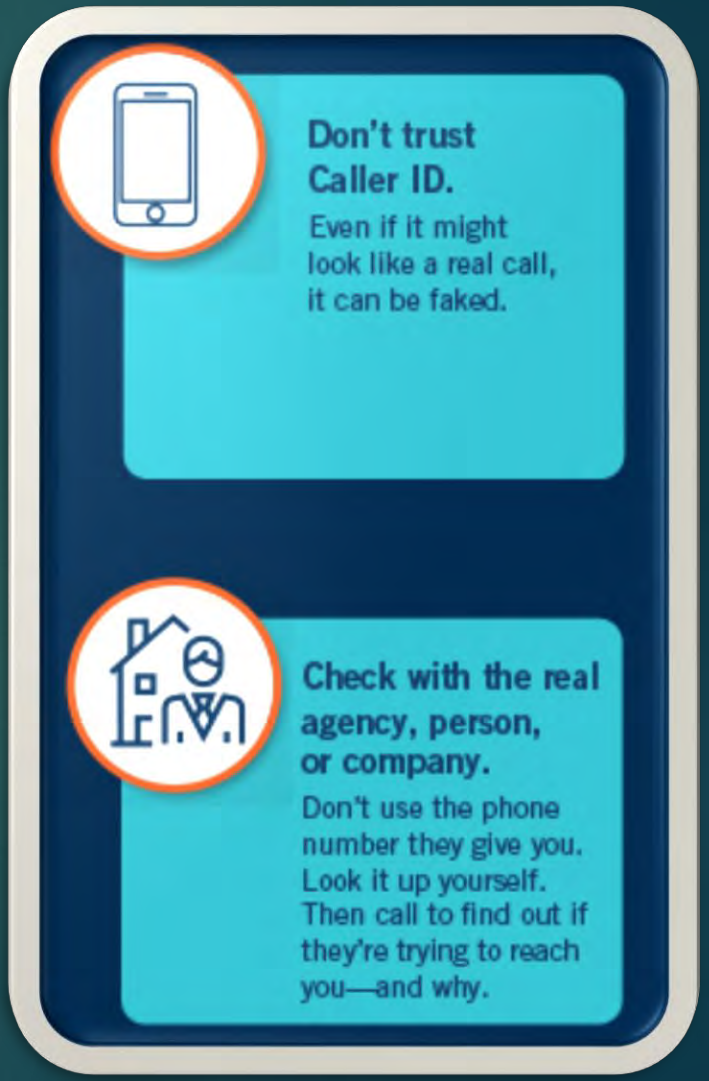


Avoiding Scammers

- The best way to avoid scammers is not to talk to them in the first place.
- Don’t answer calls from numbers you don’t know.
- Don’t open emails from people you don’t know.
- Don’t respond to texts from people you don’t know.

Verifying

- It's a good general rule to never give personal information to somebody who calls you.
- You can hang up and call a business or government agency directly so you can be sure who you are talking to.



Reducing Robo-calls

- Adjust settings on your phone
- Use 3rd party app
- Sign up on the Do-Not-Call list
- Install call-blocking device for landline

For more information go to:

https://www.fcc.gov/call-blocking

https://www.consumer.ftc.gov/articles/how-block-unwanted-calls

https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts

https://www.consumer.ftc.gov/articles/0259-robocalls

Online Shopping Tips

- Verify seller
- Check reviews
- Use credit card instead of other payment apps

Be wary of where you found the shopping link/ website

Remember: If it seems to good to be true, it probably is.

You think you've been scammed: now what?

- You must act quickly.
- Scammers know that they may still be discovered. They will move fast.
- Get help: there are free resources meant to help seniors address scams, such as the AARP Fraud Watchdog website

https://www.aarp.org/money/scams-fraud/?cmp=KNC-BRD-MC-REALPOSS-TODAY-GOOGLE-SEARCH-FRAUD&gclid=EAIaIQobChMI6pes4f2m7wIVTRmtBh3-WAPEEAAYASAAEgIbW_D_BwE&gclsrc=aw.ds

What to do if you have already given scammers a gift card

- Contact the business for whom the gift card was for immediately. They may be able to cancel the card or intercept orders paid for by the card.
- Contact the store you bought the card from.
- Report the fraud to the FTC and the Alaska AG's office.

Public Resources for Scam Victims

- File a consumer complaint with the Attorney General's Office
- File a complaint with the Better Business Bureau
- File complaint with FTC or FBI

Consumer Protection Unit at AG Office – (907) 269-5200

Federal Trade Commission – 1-877-382-4357

Better Business Bureau – (907) 644-5200

AK Div. of Banking and Securities – (907) 269-8140

Social Security Fraud Hotline – 1-800-269-0271 or www.socialsecurity.gov/fraudreport/oig/public

What to do if your personal information has been compromised

- Notify all 3 major credit bureaus and freeze your credit if necessary
- -Pull your free credit reports annually and monitor for unauthorized activity
- -monitor credit card and bank account information regularly (Also for any pay apps like Paypal, Venmo, etc.)

- The 3 Major credit bureaus are Experian, Equifax and Transunion

- A free credit report can be pulled annually on https://www.annualcreditreport.com/

- IdentityTheft.gov is a great website with resources for victims of identity theft.

What to do if your personal information has been compromised

Bank Account Number/ Debit Card Info	-Notify bank immediately. -Close out compromised cards/ accounts and get new one opened/issued. (Don't forget to update auto payments if needed) -Monitor account activity regularly for fraudulent or unauthorized charges.
Computer Information Compromised	-Change passwords/ logon information. -Do not use a password that is easily guessed. -Do not use the same password for multiple accounts.
Child's Information Compromised	-Freeze their credit with all 3 credit bureaus

Trust your gut:

If you think it might be a scam, it probably is!