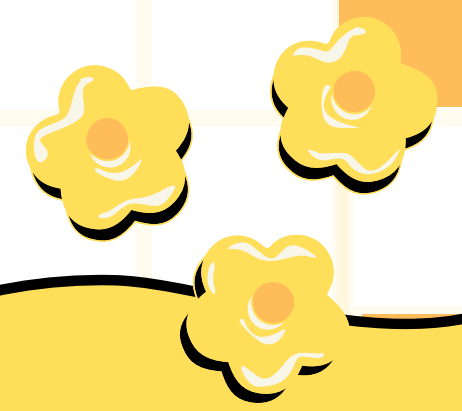
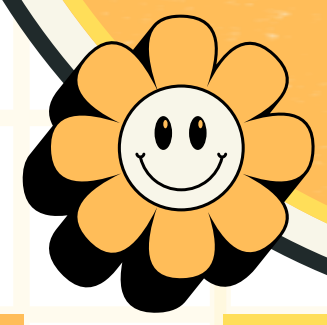
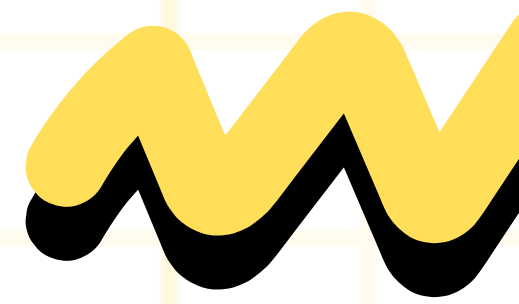
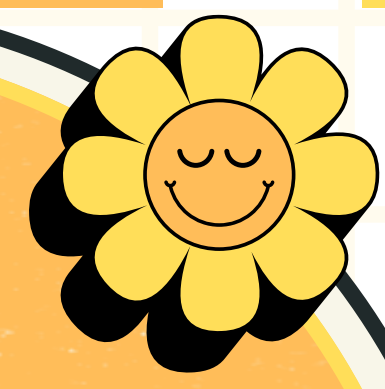
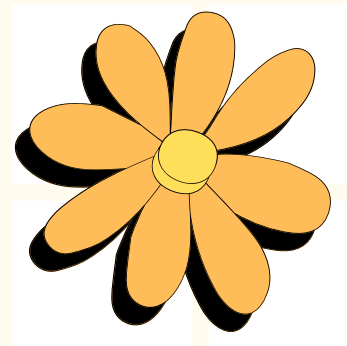


# SCAMS



# Nekoosa Help Desk Lesson #6

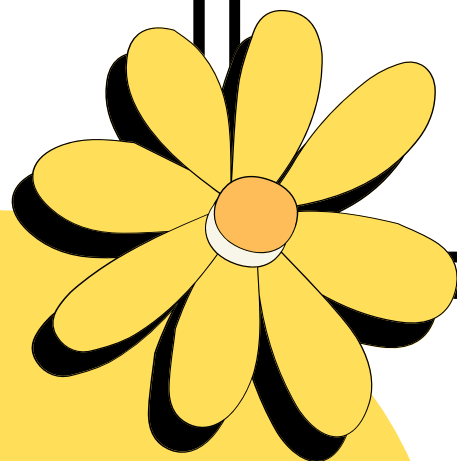
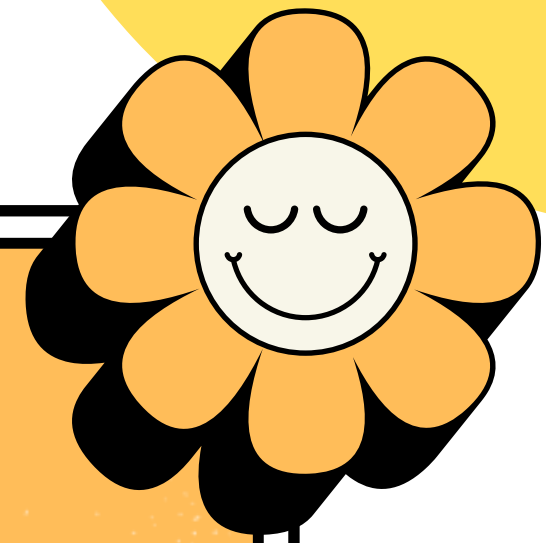
## Avoiding Scams

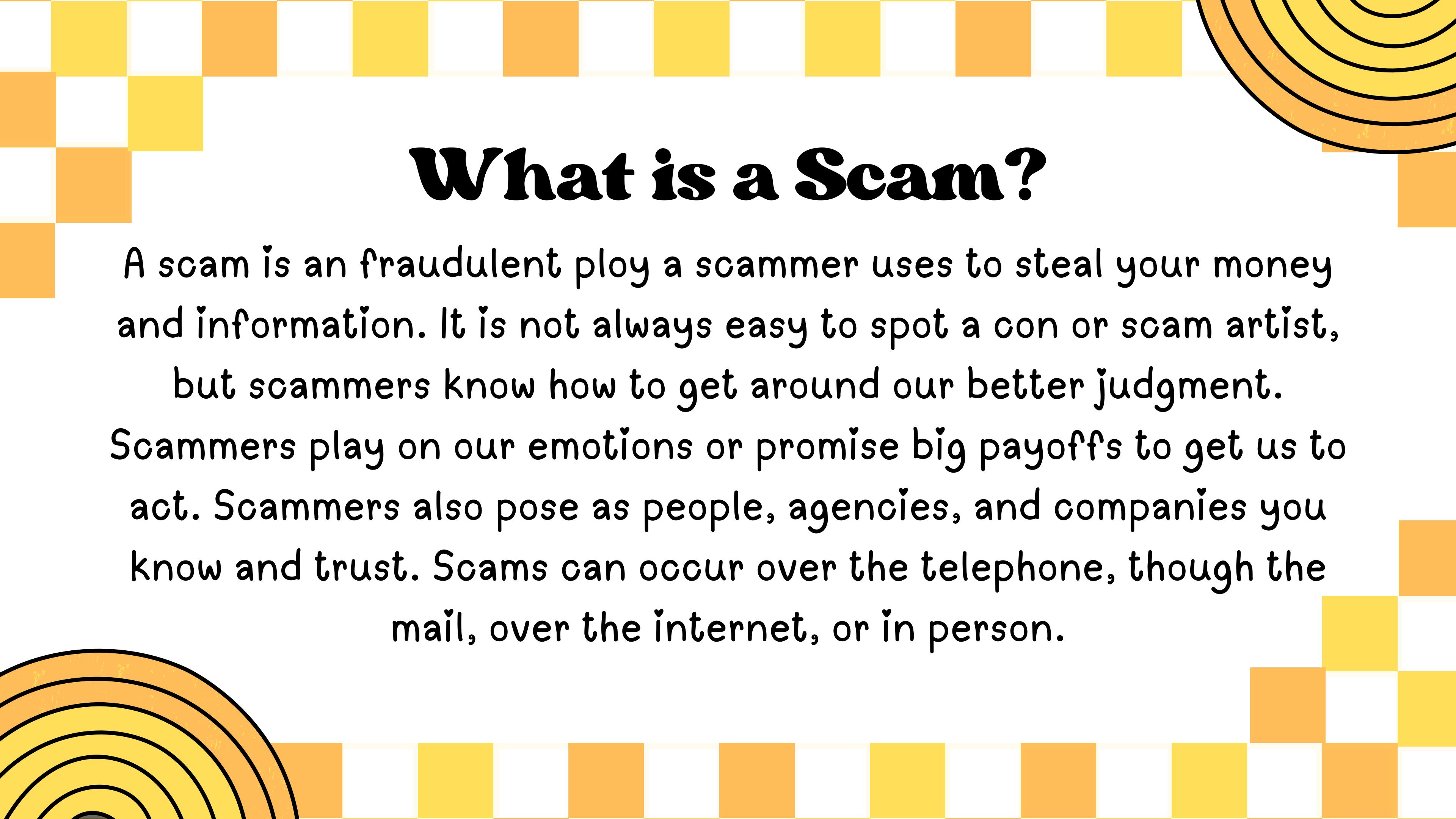
Today we will be covering...

- What are Scams?
- Types of Scams
- What to do if Scammed



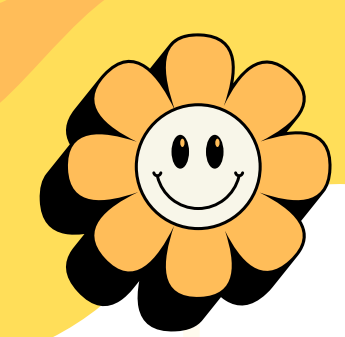
# What are Scams?



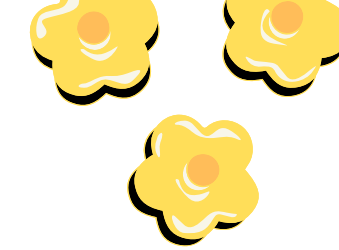


# What is a Scam?

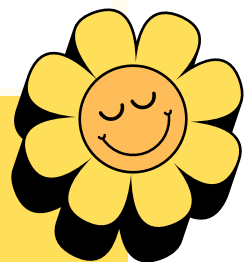
A scam is an fraudulent ploy a scammer uses to steal your money and information. It is not always easy to spot a con or scam artist, but scammers know how to get around our better judgment. Scammers play on our emotions or promise big payoffs to get us to act. Scammers also pose as people, agencies, and companies you know and trust. Scams can occur over the telephone, though the mail, over the internet, or in person.



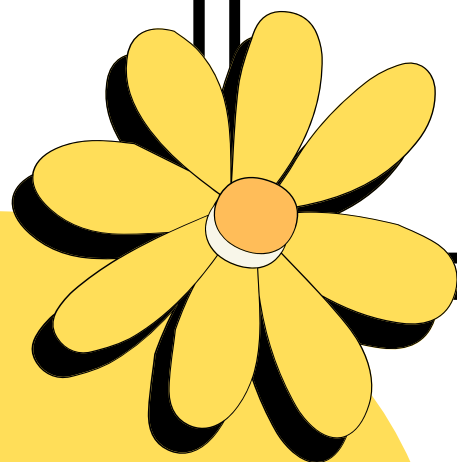
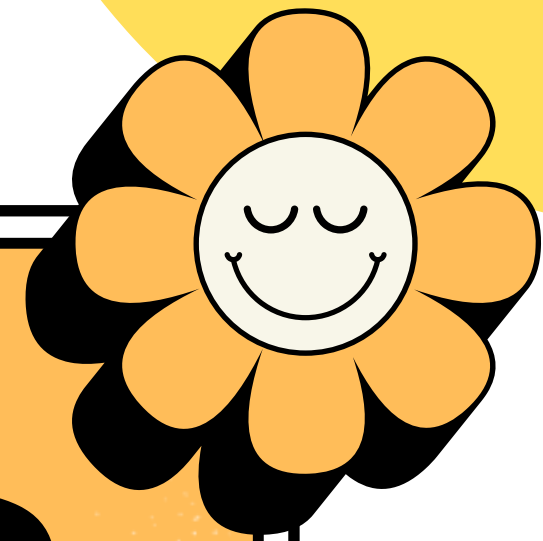
# Scams Continued



Scams are designed to trick vulnerable groups, such as older people with limited technical knowledge. With the rise of AI, a lot of scams have become very personal, and can be very scary. In this presentation, we aim to educate you on how to spot scams. The best thing you can do to combat scams is to stay calm. Scammers often try to make things loud, scary, and angry. If something seems wrong, hang up, delete the email, etc., and double check information to see if it is accurate.



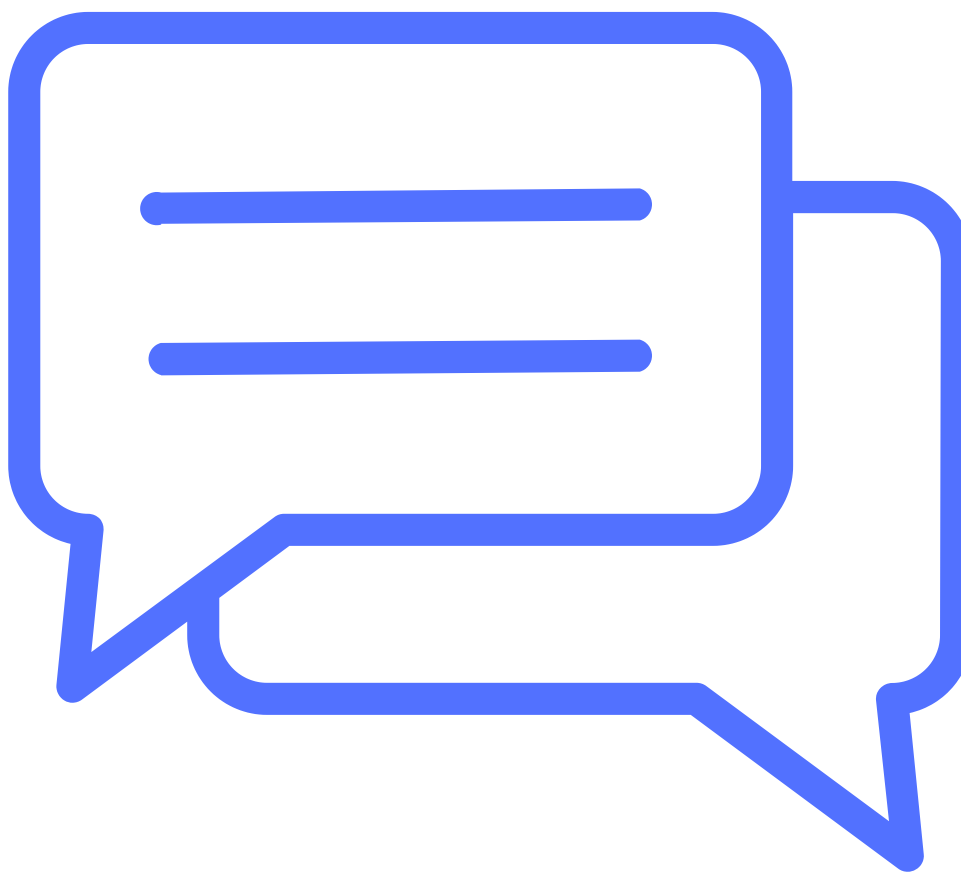
# Types of Scams



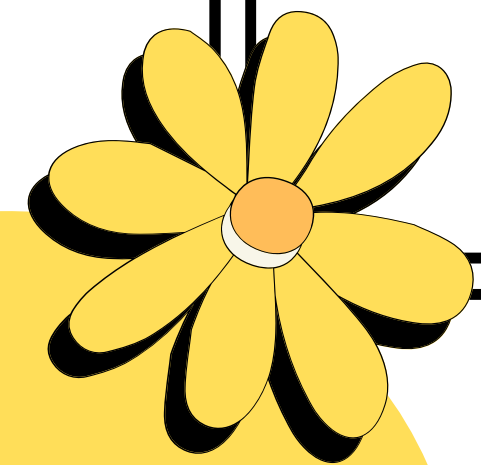
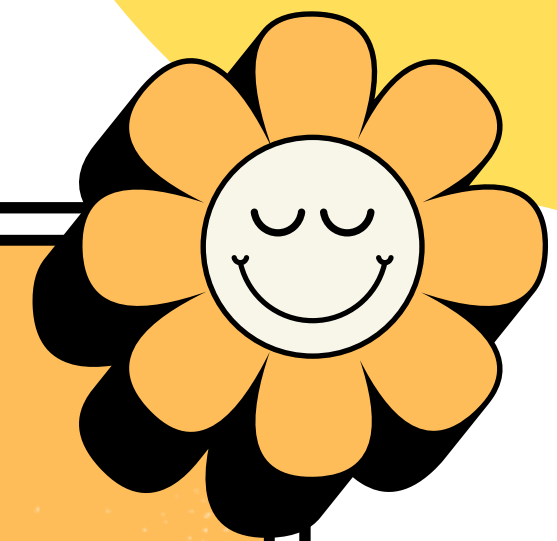


# Scam Types

There are many different types of scams, but the main ones are **Email**, **Phone Call**, **Text**, and **Ads Scams**. Lets walk through examples of each and how to avoid them.



# Phone Scams








# **How to recognize a phone scam**

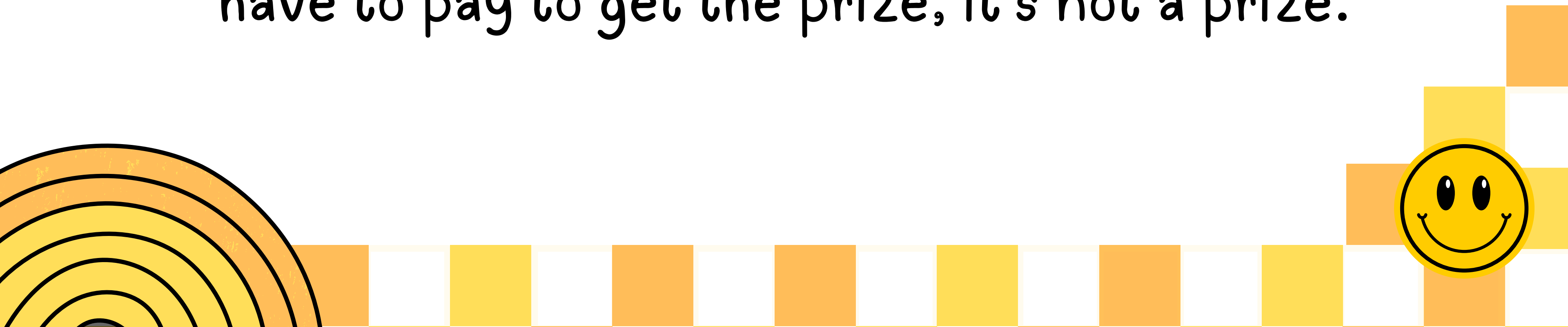
Phone scams come in many forms, but they tend to make similar promises and threats, or ask you to pay certain ways. Here's what to know:





# **There is no Prize**

The caller might say you were “selected” for an offer or that you’ve won a lottery. But if you have to pay to get the prize, it's not a prize.



# **You Won't be Arrested**

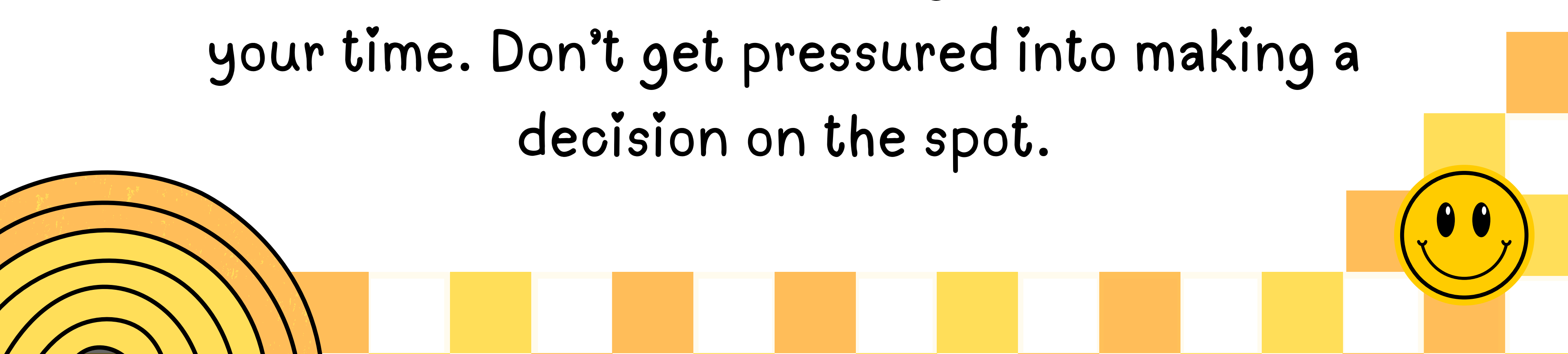
Scammers might pretend to be law enforcement or a federal agency. They might say you'll be arrested, fined, or deported if you don't pay taxes or some other debt right away. The goal is to scare you into paying. But real law enforcement and federal agencies won't call and threaten you.

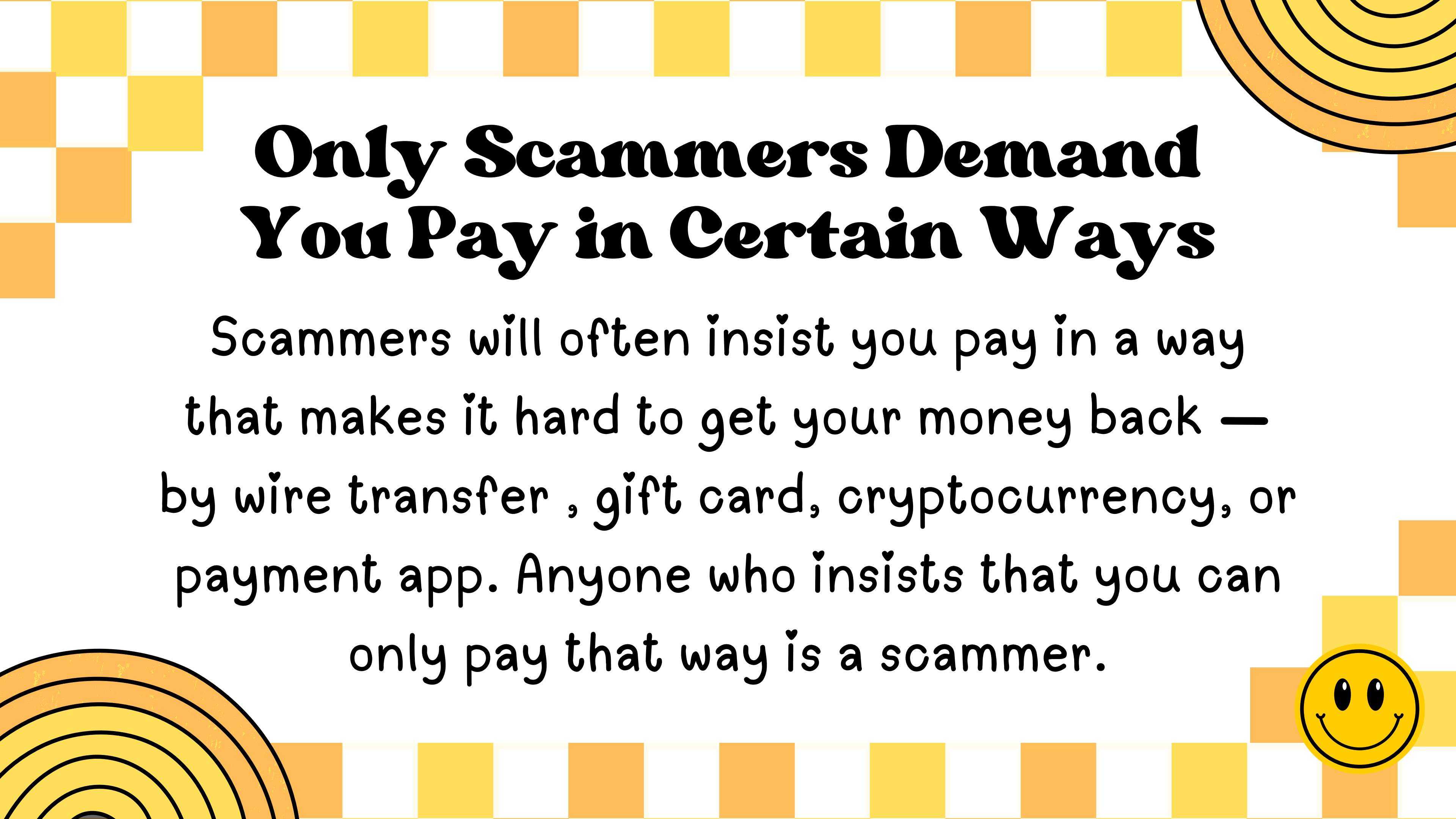




# **You Don't Need to Decide Now**

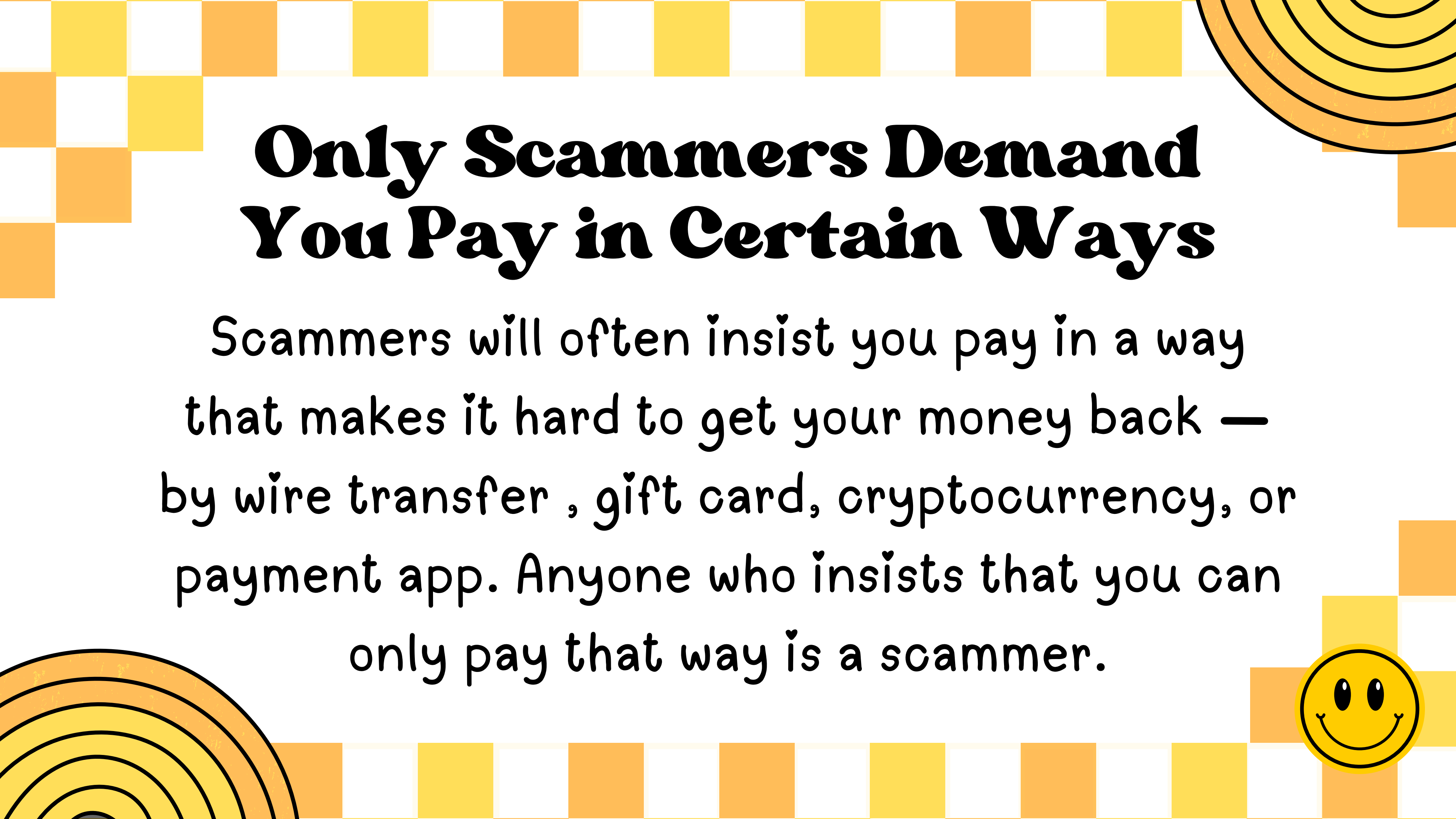
Most honest businesses will give you time to think their offer over and get written information about it before you commit. Take your time. Don't get pressured into making a decision on the spot.





# **Only Scammers Demand You Pay in Certain Ways**


Scammers will often insist you pay in a way that makes it hard to get your money back — by wire transfer , gift card, cryptocurrency, or payment app. Anyone who insists that you can only pay that way is a scammer.





# **Government Agencies Won't Call to Confirm Your Sensitive Information**

No government agency is going to call you out of the blue and ask for sensitive information like your Social Security number. They're lying if they say they're with a government agency you know, like the Social Security Administration or IRS.



# **You Shouldn't be Getting all those Calls**

If a company is selling something, it needs your written permission to call you with a robocall. And if you're on the National Do Not Call Registry, you shouldn't get live sales calls from companies you haven't done business with before. Those calls are illegal. If someone is already breaking the law calling you, what they're calling about is probably a scam.



# Example Phone Scams



Any scam can happen over the phone.  
But here are some common angles  
phone scammers like to use:





# Impersonator Scams

A scammer pretends to be someone you trust — a government agency like the FBI, the sheriff's office, a court official, a family member, a love interest, or a business you recognize. The scammer can even have a fake name, a fake AI voice, and number show up on your caller ID to convince you they're real.



# Debt Relief & Credit Repair



Scammers will offer to lower your credit card interest rates, fix your credit, or get your student loans forgiven if you pay their company a fee first. Don't believe them. You could end up losing your money and ruining your credit.



# Business & Investment

Callers might promise to help you start your own business and give you business coaching, or guarantee big profits from an investment — maybe investing in cryptocurrency. Don't believe it. Check out investment opportunities with your state securities regulator.



# Charity Scams

Scammers like to pose as real charities and might ask for donations for disaster relief efforts, support for local law enforcement or veterans, or money for kids and families dealing with cancer. Always ask how much of each dollar you donate will go directly to the charity's mission and always check out a charity before you give. Never feel pressured to give immediately over the phone.



# Extended Car Warranties

Scammers find out what kind of car you drive and when you bought it (or pretend to know) so they can urge you to buy overpriced — or worthless — service contracts or so-called extended warranties. Never buy a contract or warranty on the spot, and always research the company and contract or warranty before you pay anything so you know if it makes sense for you.



# “Free” Trials

A caller might promise a free trial but then sign you up for products — sometimes lots of products — that you’re billed for every month until you cancel. Never sign up without knowing what happens after the “free trial” ends, and always read your billing statements to look for unexpected charges.



# Loan Scams

Loan scams include advance fee loan scams, where scammers guarantee you loans or credit cards for an upfront fee. Don't buy it. Honest lenders don't make guarantees like that.



# Prize & Lottery Scams

In a typical prize scam, the caller will say you've won a prize, but then say you need to pay taxes, registration fees, or shipping charges to get it. Hang up. After you pay, you find out there is no prize.





# Travel & Timeshare Scams

Scammers promise free or low-cost vacations, but once you respond, you find out you have to pay some fees and taxes first. Or once you pay, you find out there is no vacation. In timeshare resale scams, scammers lie and tell you they'll sell your timeshare — and may even have a buyer lined up — if you pay them first.



# Spooftng

Scammers can make any name or number show up on your caller ID. That's called spoofing. So even if it looks like it's a government agency like the Social Security Administration calling, or like the call is from a local number, it could be a scammer calling from anywhere in the world. The best thing to do if you get a call you aren't expecting is to let it go to voicemail, and call back if it is a legitimate message.





# **How to Stop Calls from Scammers**

There are steps you can take to block and avoid unwanted phone calls.



# Don't Trust Caller ID

Scammers can make any name or number show up on your caller ID. That's called spoofing. So even if it looks like it's a government agency like the Social Security Administration calling, or like the call is from a local number, it could be a scammer calling from anywhere in the world. If you don't recognize who is calling, **don't answer and let the call go to voicemail**. If it is important, whoever is calling will leave you a message.



# National Do Not Call Registry

While this won't block all scam calls, law abiding companies that advertise via phone will no longer text and call you if you are registered [here](#). This should cut back on the amount of calls you get. If they do still call and text, they are violating federal law and should be reported to the FTC or FCC.



# Hang Up

Even if it's not a scammer calling, when a company is calling you illegally, it's not a company you want to do business with. When you get a robocall, don't press any numbers to let you speak to a live operator or remove you from their call list. Pressing buttons might lead to more robocalls.



# Consider Call Blocking

Scammers don't care if you're on the National Do Not Call Registry. That's why call blocking is your best defense against unwanted calls. Which type of call-blocking or call-labeling technology you use will depend on the phone — whether it's a cell phone, a traditional landline, or a home phone that makes calls over the internet (VoIP). See what services your phone carrier offers and look online for expert reviews. For cell phones, also check out the reviews for different call-blocking apps in your app store.



# Reporting a Phone Scam

If you've lost money to a phone scam or have information about the company or scammer who called you, tell the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/identitytheft/identity-theft-reporting).

If you didn't lose money and just want to report a call, use the streamlined reporting form at [DoNotCall.gov](https://www.donotcall.gov).





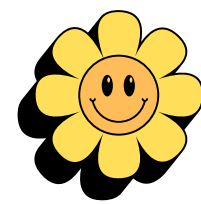
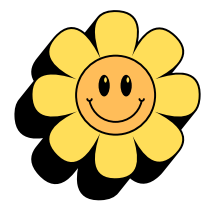
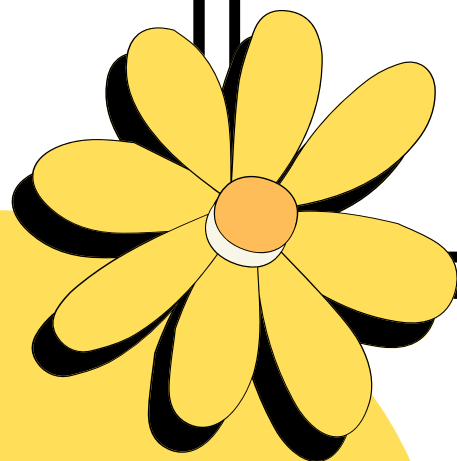
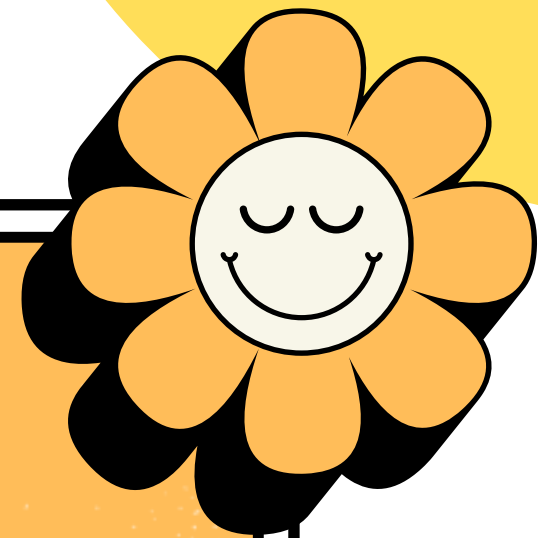
# Reporting is Important

Any information you provide will help stop the scammers. Report the number that received the call, the number on your caller ID, and any number they told you to call back. Also report the exact date and time of the call, if you know it. Knowing all this information helps the FTC and its law enforcement partners track down the scammers behind the call.

The FTC also takes the phone numbers you report and releases them to the public each business day. This helps phone carriers and other partners that are working on call-blocking and call-labeling solutions.



# Text Scams






# Recognizing Text Scams

Text scams are a lot like phone call scams.

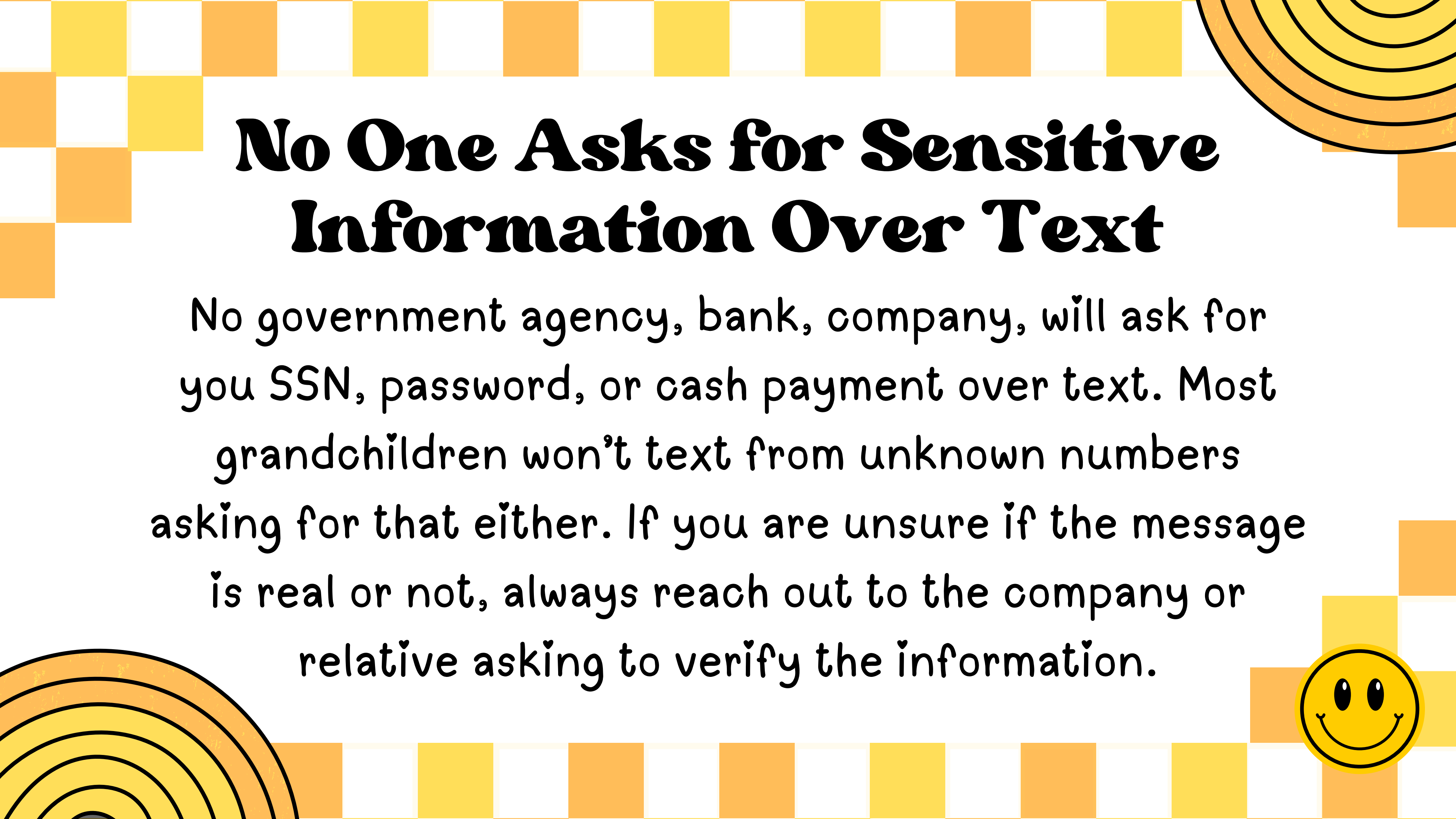
Here is what you need to know:





# **No One Asks for Sensitive Information Over Text**

No government agency, bank, company, will ask for you SSN, password, or cash payment over text. Most grandchildren won't text from unknown numbers asking for that either. If you are unsure if the message is real or not, always reach out to the company or relative asking to verify the information.



# Unknown Links

Scammers often try to get you to click on links in text messages by promising you something. Scammers might...

- Promise free prizes, gift cards, or coupons, but they're not real
- Offer you a low or no interest credit card, but there's no deal and probably no card
- Promise to help you pay off your student loans, but they won't

# Unknown Links, Again

Some links might take you to a spoofed website that looks real but isn't. If you log in, the scammers then might steal your username and password.

Other messages might install harmful malware on your phone that steals your personal or financial information without you realizing it.

To summarize: Don't Click on Text Links



# Fake Account Activity

Scammers also send fake messages saying they have information about your account or a transaction. Scammers might...

- Say they've noticed some suspicious activity on your account, but they haven't
- Claim there's a problem with your payment information, but there isn't
- Send you a fake invoice and tell you to contact them if you didn't authorize the purchase, but it's a scam
- Send you a package delivery notification, but it's fake



# Lost Package Message

This scam is super common right now. **DO NOT** click the link! USPS, UPS, and FedEx will never text you. Just delete the text and block the number.





# What To Do

Text scams are super common right now, but there are a few things you can do to protect yourself from them.



# Delete & Block

When you receive a scam text, the best thing to do is block the number & delete the text. It's as simple as that!



# Prevention

Your phone may have an option to filter and block spam or messages from unknown senders.

Here's how to filter and block messages on an iPhone.

and how to block a phone number on an Android phone.



# CTIA.ORG

Your wireless provider might have a tool or service that lets you block calls and text messages. Check out [ctia.org](https://www.ctia.org), a website from the wireless industry, to learn about options from different providers.



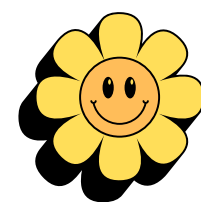
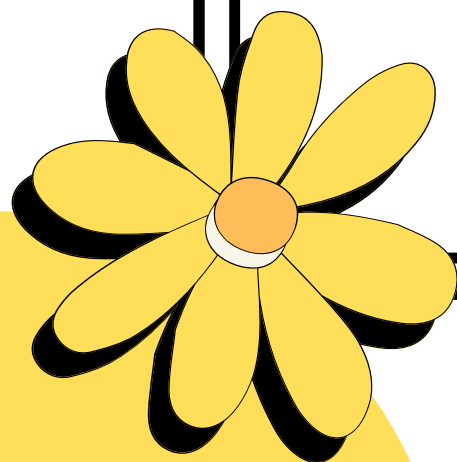
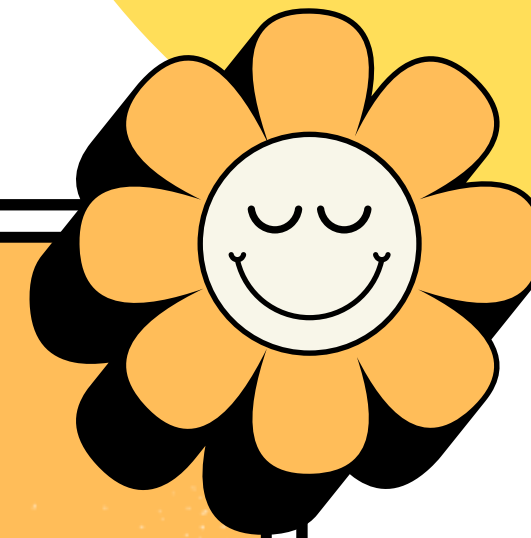
# Reporting a Text Scam

If you get an unwanted text message, there are three ways to report it:

- Copy the message and forward it to 7726 (SPAM). This helps your wireless provider spot and block similar messages in the future.
- Report it on the messaging app you use. Look for the option to report junk or spam. Use the links below for help:
  - [How to report spam or junk in the Messages app](#)
  - [How to report spam on an Android phone](#)
- Report it to the FTC at [ReportFraud.ftc.gov](#).



# Email Scams



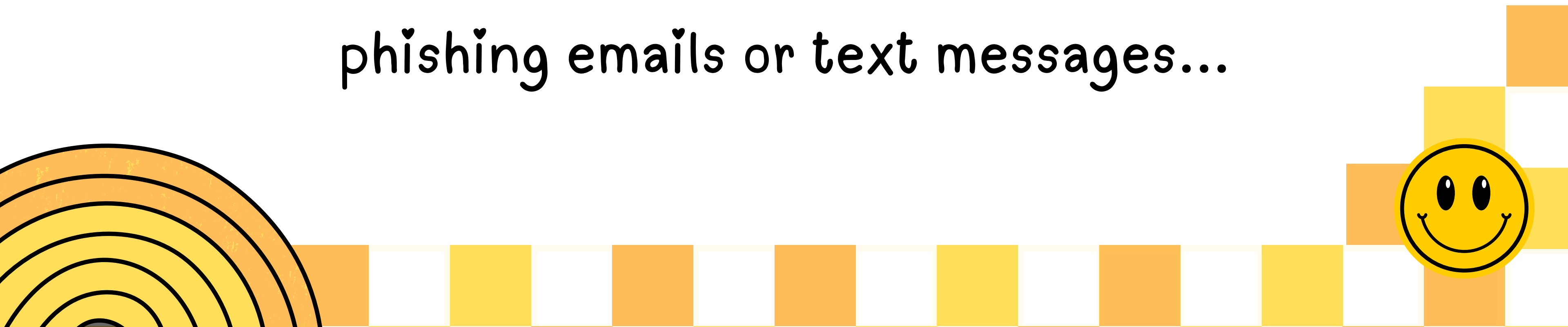
# What is Phishing?

A **phishing** scam is an email (& text) scam where a scammer tries to get your personal information via a link by pretending to be a legitimate company.




# **How to Spot Phishing**

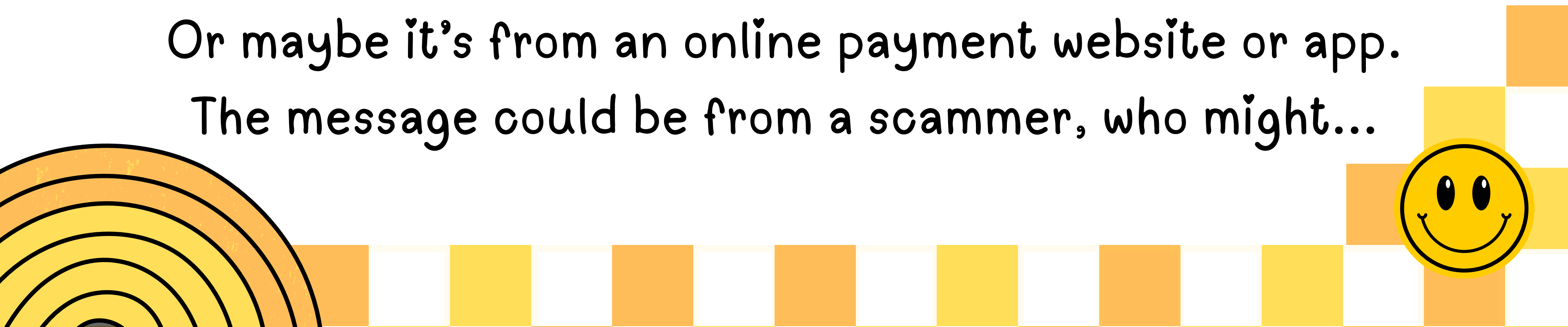
Scammers often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages...







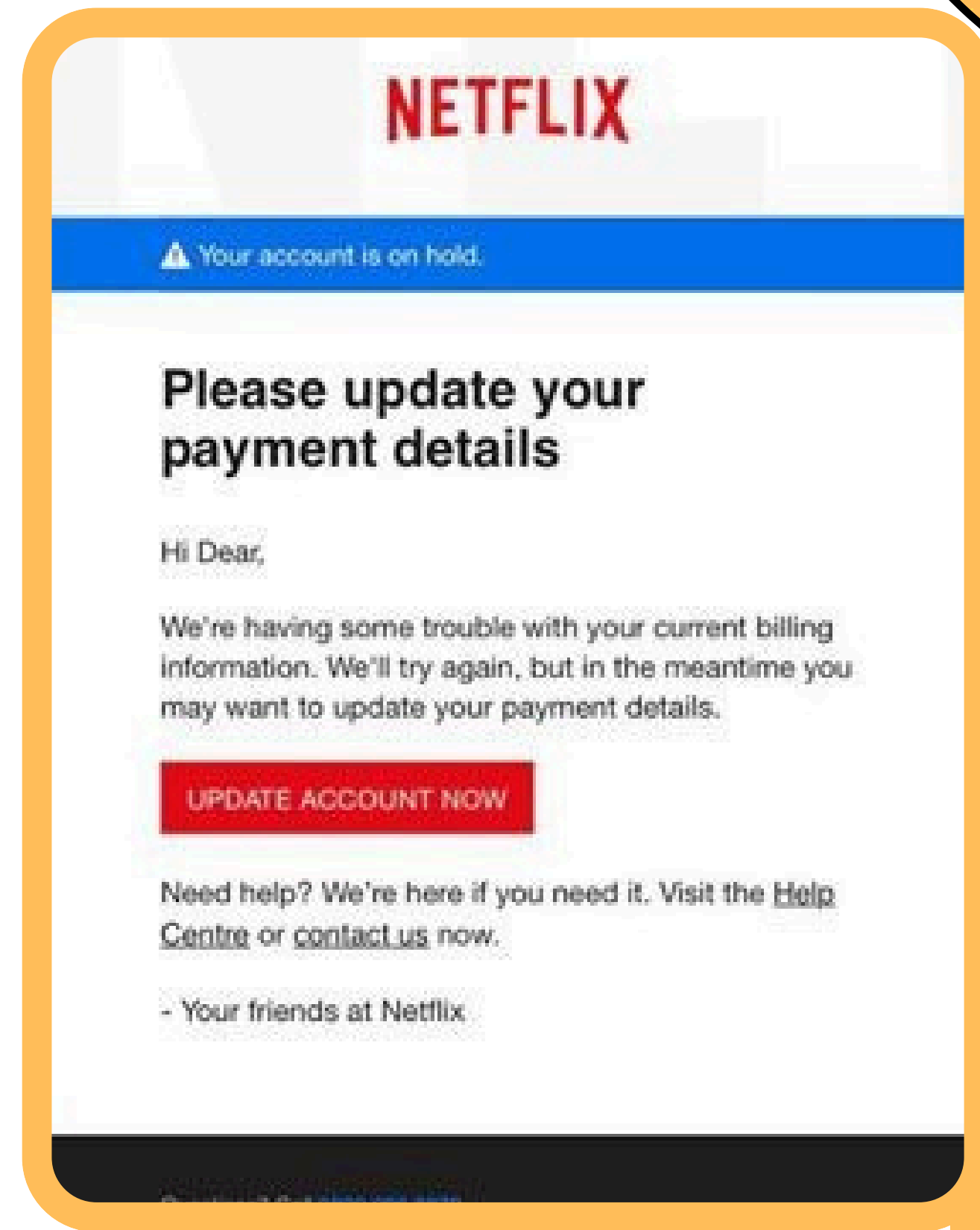


Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company. Or maybe it's from an online payment website or app. The message could be from a scammer, who might...



- 
- Say they've noticed some suspicious activity or log-in attempts
  - Claim there's a problem with your account or your payment information
    - Say you need to confirm some personal or financial information
      - Include an invoice you don't recognize
      - Want you to click on a link to make a payment
  - Say you're eligible to register for a government refund offer a coupon for free stuff
- 

All of these things are fake. Clicking on links from phishing emails could lead to fake websites where they steal your information, or they could install malware on your computer. Here is an example of an email that looks legit, but is actually fake.

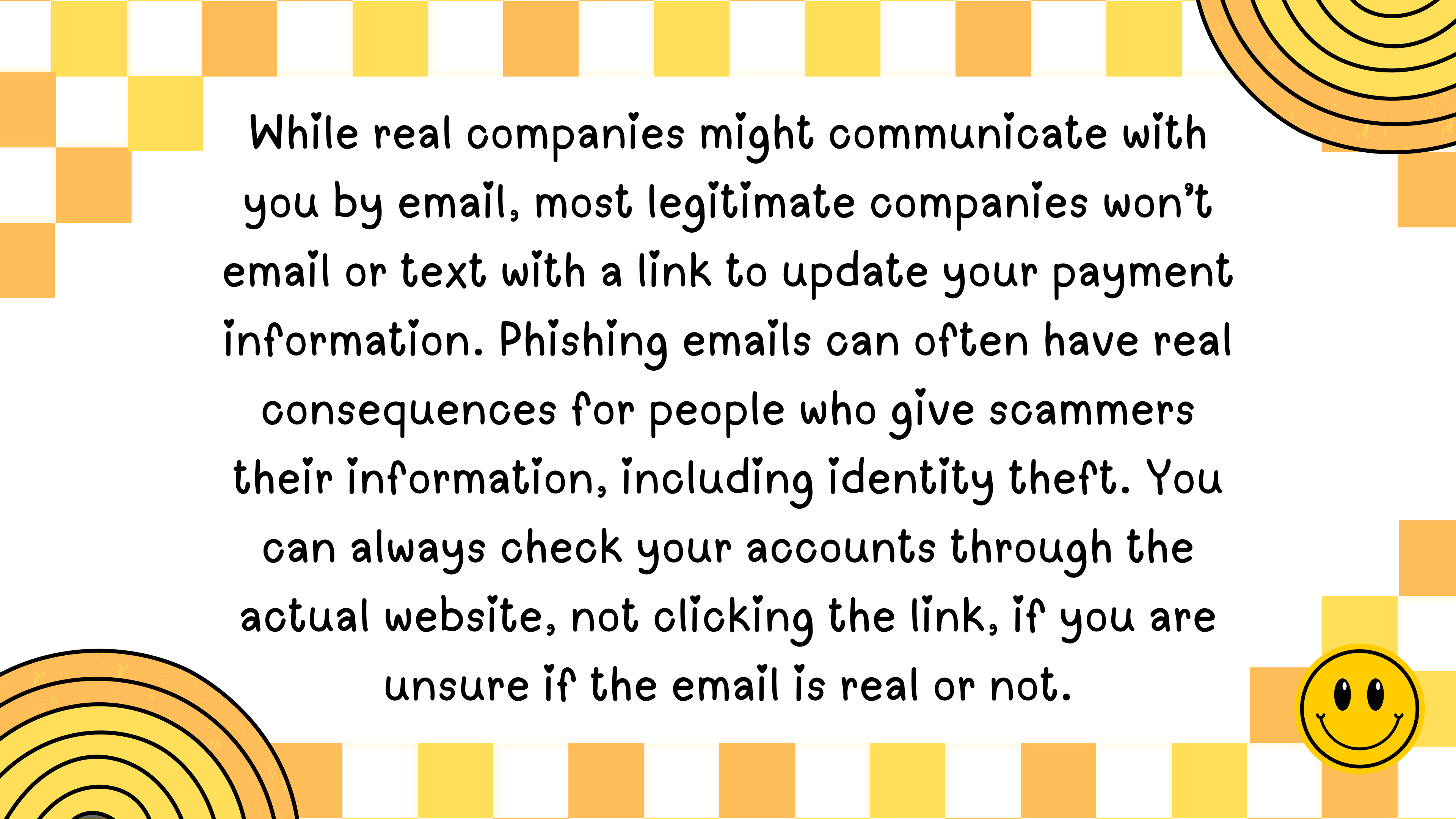


# Phishing Signs


Here are signs that this email is a scam, even though it looks like it comes from a company you know, and even uses the company's logo in the header:

- The email has a generic greeting.
- The email says your account is on hold because of a billing problem.
- The email invites you to click on a link to update your payment details.
- The email address that sent the email is jumbled and doesn't look real.

(example: an email from "Netflix" with the address "neftlix@network.net")



While real companies might communicate with you by email, most legitimate companies won't email or text with a link to update your payment information. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. You can always check your accounts through the actual website, not clicking the link, if you are unsure if the email is real or not.



# Fishy Phishing

If you suspect you have received a phishing email, first:

Do I have an account with the company or know the person who contacted me?

If the answer is “No,” it could be a phishing scam. Go back and review the previous slides and look for signs of a phishing scam. If you see them, report the message and then delete it.

If the answer is “Yes,” contact the company using a phone number or website you know is real, not the information in the email.

Attachments and links might install harmful malware.



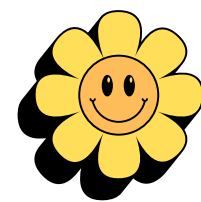
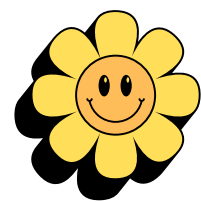
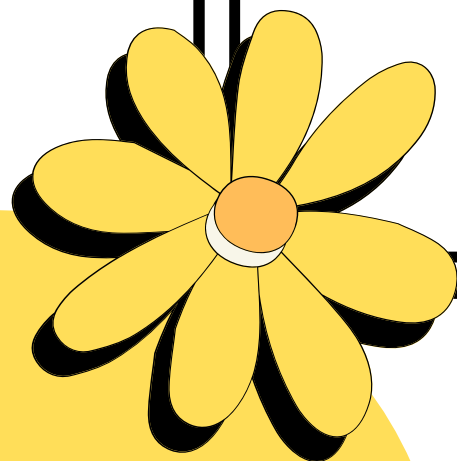
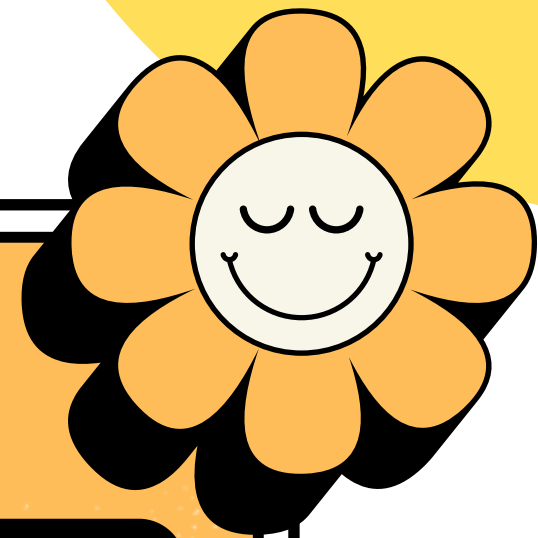
# Reporting Phishing

If you got a phishing email, report it. The information you give helps fight scammers.

- If you got a phishing email, forward it to the Anti-Phishing Working Group at [reportphishing@apwg.org](mailto:reportphishing@apwg.org)
- Report the phishing attempt to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/secure/ftc/ReportFraud.ftc.gov).
- Delete the email and report it as junk!



# Ad Scams





# Ad Scamming

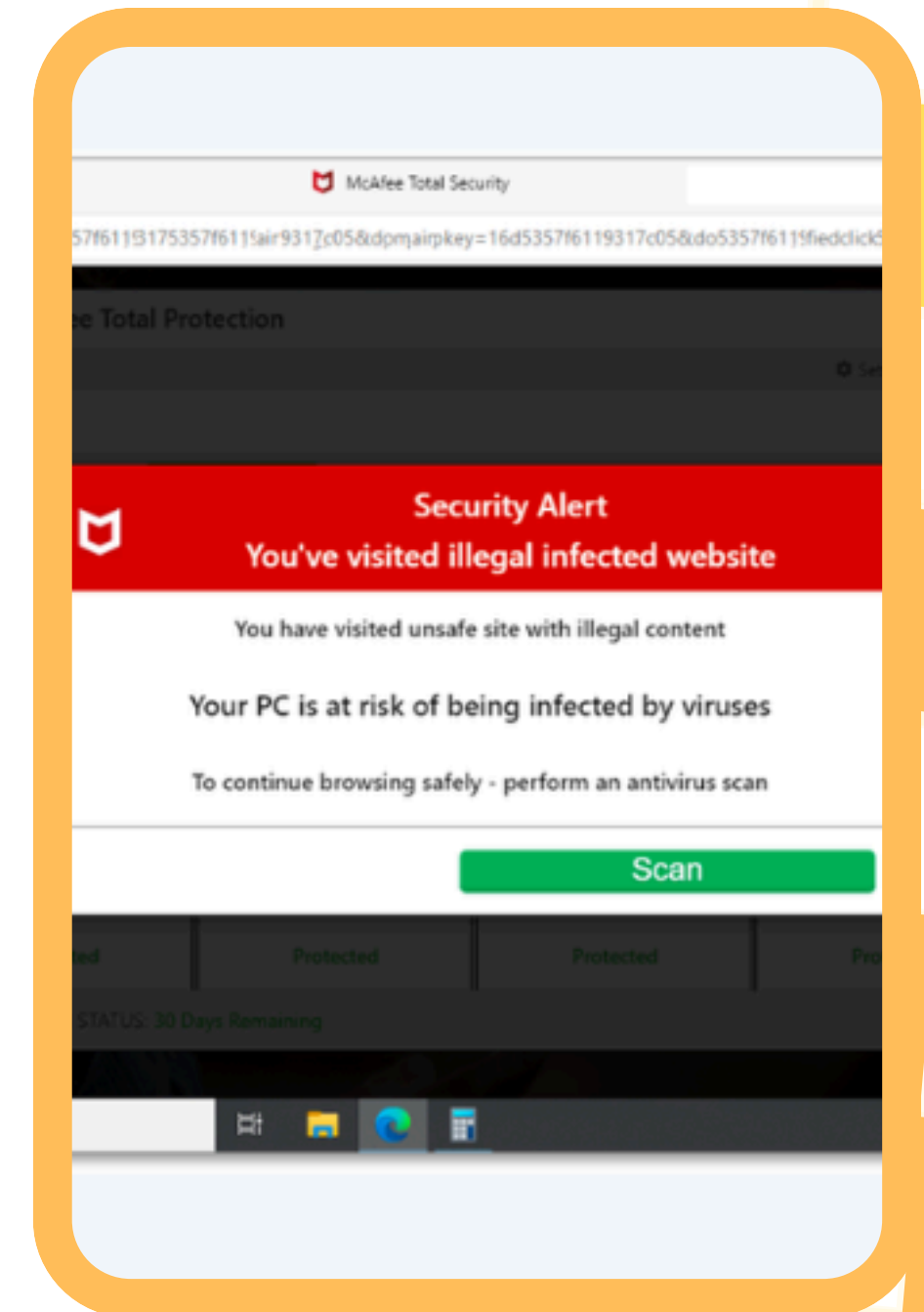
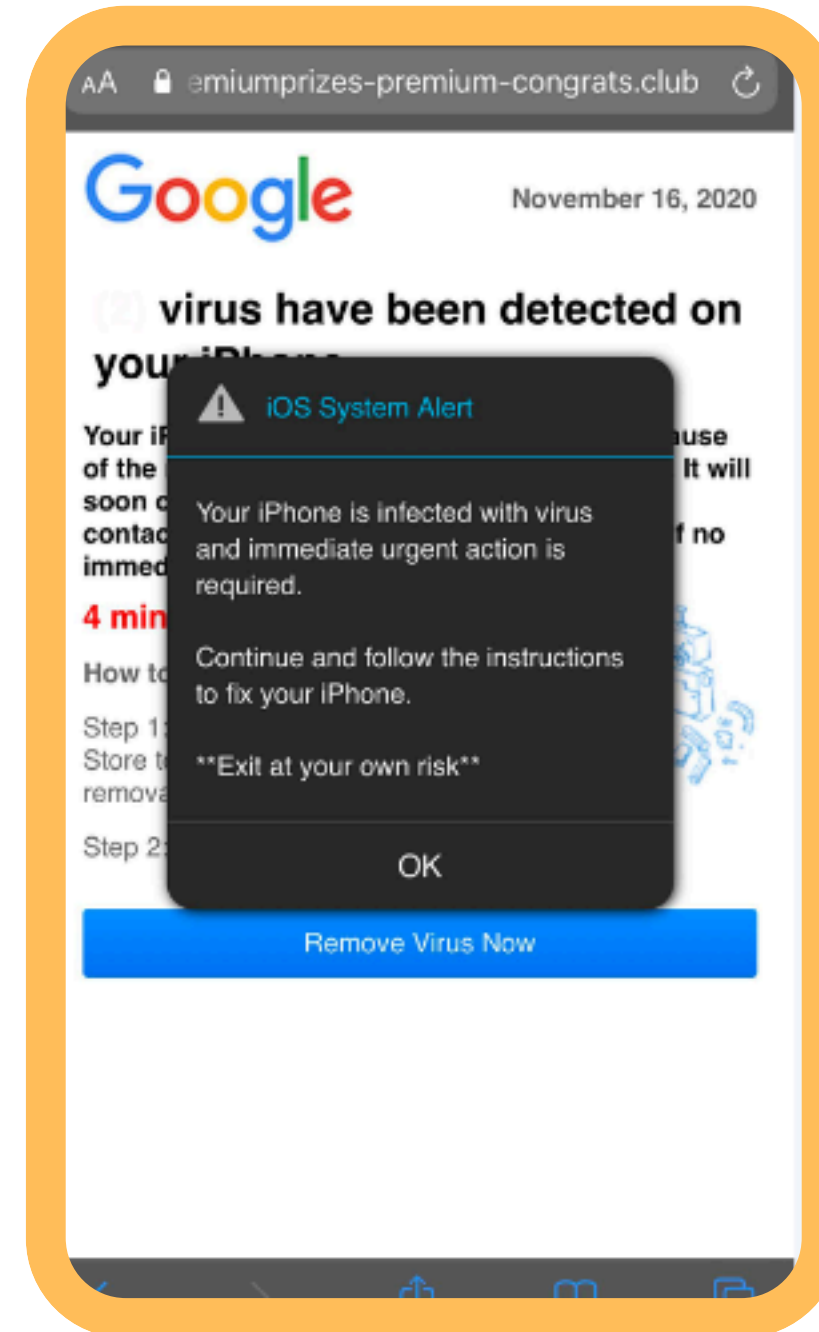
There are a LOT of ads online. Whether it be on a website you are browsing, on social media, or on TV, you are going to see them everywhere. While a lot of ads are harmless, most aim to be misleading, and some are scams. As a general rule, just ignore ads and close pop ups online. Our online safety presentation goes over what ads can look like and how to spot fake ones.



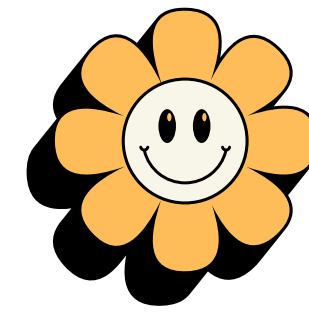
# Scary Pop Ups



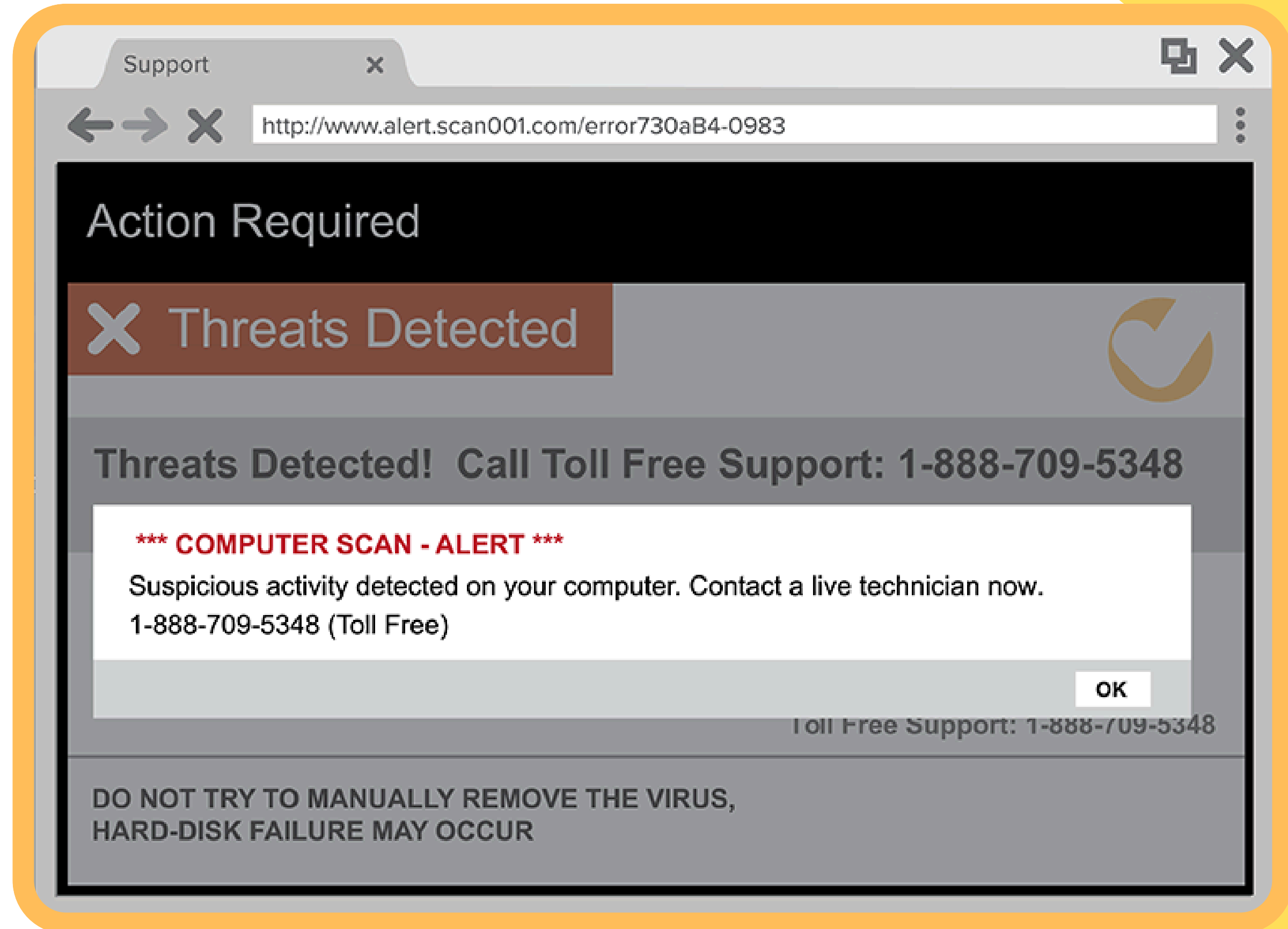
Some ads are pop ups designed to scare you. These are SCAMS and should be closed.



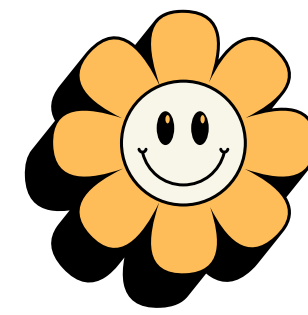
# Tech Support Scams



Sometimes these scary ads will tell you to call a phone number because there is a virus in your computer. These are fake. Don't call the phone number.



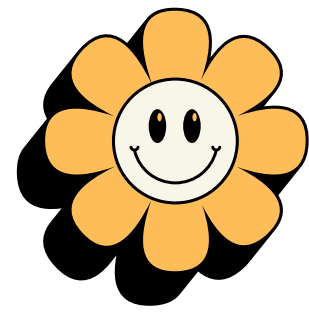
# Remote Access Scams



The tech support scams (that can be phone calls, pop ups, or ads listed on websites) often try to gain remote access to your computer to steal passwords and download viruses on your computer. If someone asks you to remotely access your computer, or install software remotely, don't let them. Hang up the phone, or close the ad.

If you are in the mood for an (adult) action movie, the plot of [The Beekeeper](#) movie (available in the library) centers around tech and remote access scams. While it is a fast paced, explosions and guns type movie, it does highlight what scammers do to steal your money. Check it out today!

# Still anxious?



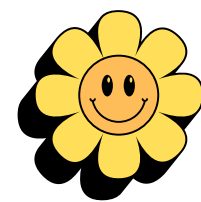
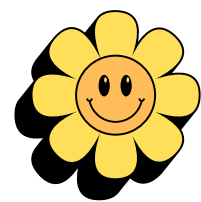
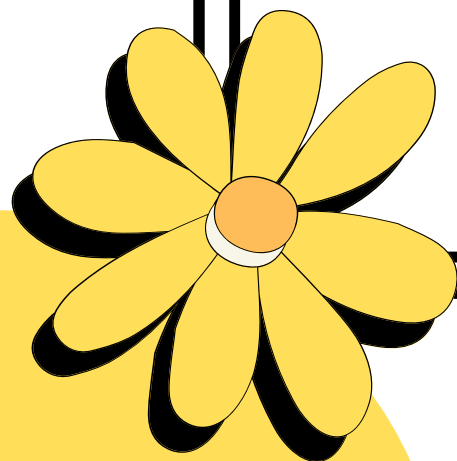
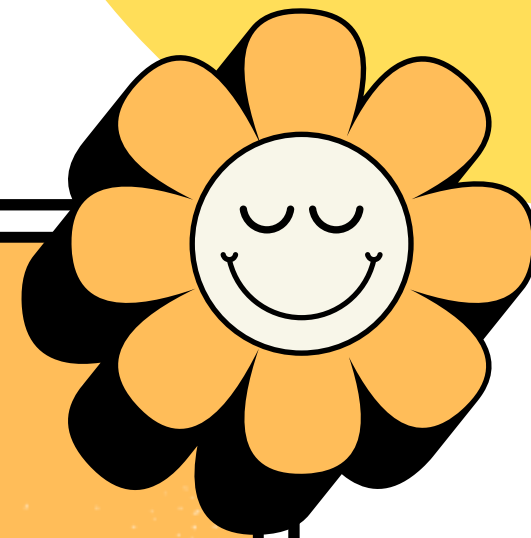
Sometimes scary ads can leave you anxious, and that is ok! As long as you close out of the ad, you should be fine. If you are still worried, you can go to your anti virus software on your computer or google steps to take to secure your phone or tablet. You can always ask a trusted adult (or tech savvy young person) to help you with this.

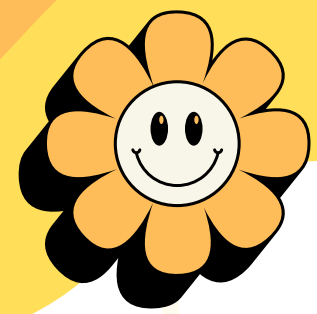
# Reporting Fake Sites

If you find a fake website, report it. The information you give helps fight scammers. You can report websites trying to steal your information at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov).



**To Sum  
It Up**





# General Notes

There are a lot of scams out there, and we just covered a LOT of information. Just remember the most important things are a few **Don'ts**...

**Don't** - Answer the phone if you don't recognize the caller.

**Don't** - Give strangers your personal information over the phone or online.

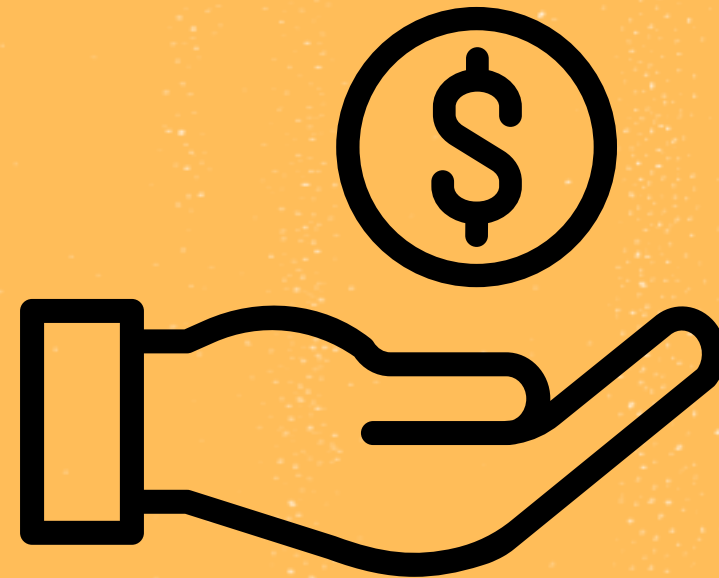
**Don't** - Click on links sent to you.

**Don't** - Click on suspicious ads or pop ups

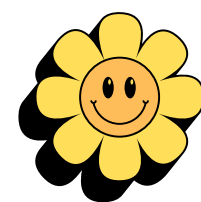
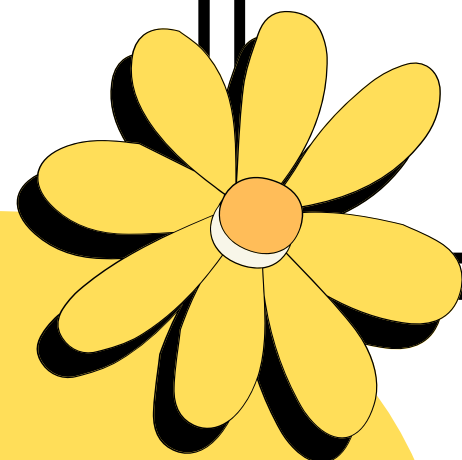
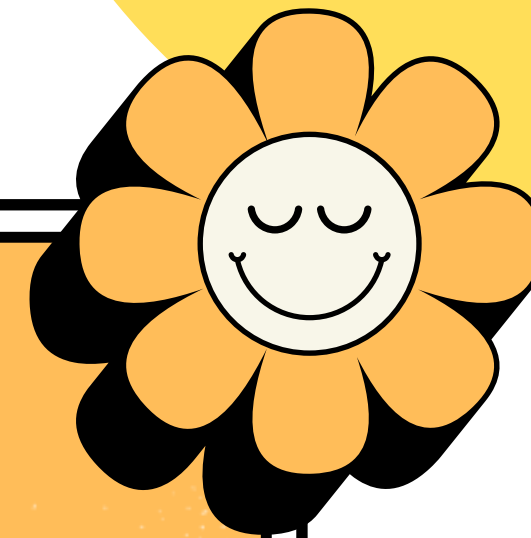




**Got**



**Scammed?**



# So You've Been Scammed..

Don't panic. There are steps you can take to try and get your money back and protect your information.

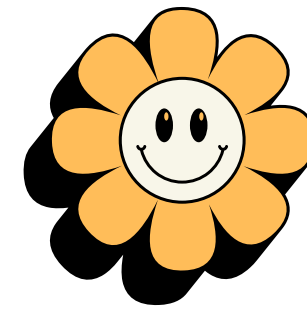
But first things first...

Don't be embarrassed about being scammed,  
and don't try to hide it.

Scams are designed to trick people, and are crimes. You wouldn't be embarrassed if you were mugged and robbed. This is not your fault! Reach out to your loved ones for help and support.



# I Paid a Scammer...



So you wanted to donate to your local police, but instead paid a criminal who should be arrested by your local police...

Here are some steps you can take to get your money back.

Did you pay with a credit card or debit card?

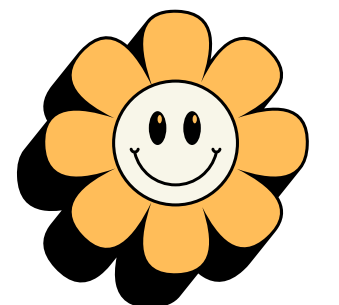
Contact the company or bank that issued the credit card or debit card.

Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back. Depending on the information you gave them, you may need to freeze your account and get a new card. Call your bank and ask for the fraud department. They should be able to help.

# For Unauthorized Bank Transfers...

Did a someone make an unauthorized transfer from your bank account?

Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back. You may need to freeze your account and get a new card. Call your bank and ask for the fraud department. They should be able to help.



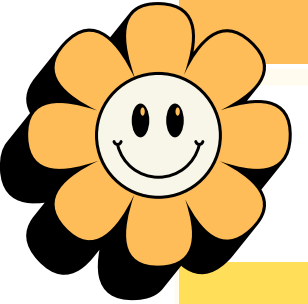
# For Gift Cards...

Did you buy a gift card and give someone the numbers off the back of the card?

Contact the company that issued the gift card.

Use this list of contacts. Tell them the card was used in a scam and ask for your money back.

Keep a copy of the gift card and the store receipt.

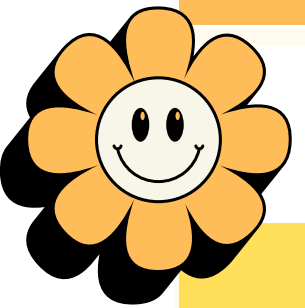


# For Wire Transfers...

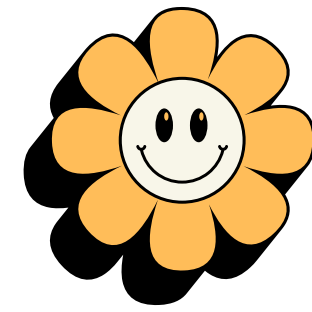
Did you send a wire transfer through a company like Western Union or MoneyGram?

Contact the wire transfer company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

- MoneyGram at 1-800-926-9400
- Western Union at 1-800-448-1492
- Ria (non-Walmart transfers) at 1-877-443-1399
- Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144



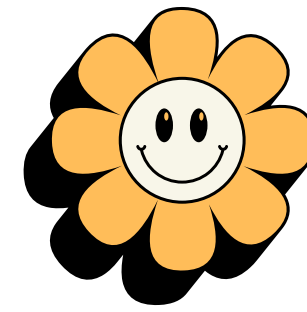
# For Bank Transfers



Did you send a wire transfer through your bank?

Contact your bank and report the fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

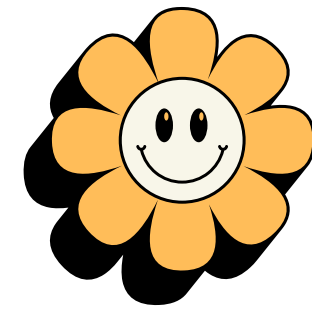
# For Payment Apps...



Did you send money through a payment app? Report the fraudulent transaction to the company behind the payment app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.

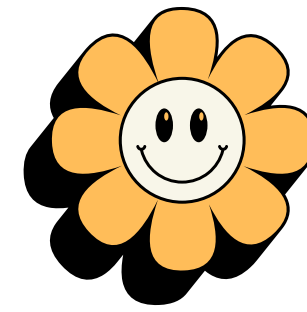


# For Crypto...



Did you pay with cryptocurrency?  
Contact the company you used to  
send the money and tell them it was a  
fraudulent transaction. Ask them to  
reverse the transaction.

# For Cash...



Did you send cash?

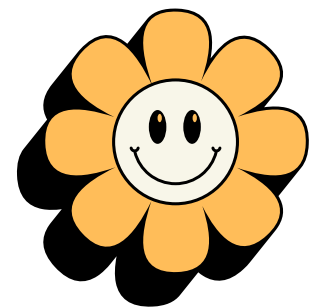
If you sent cash by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package. To learn more about this process, visit [USPS Package Intercept: The Basics](#).

If you used another delivery service, contact them as soon as possible.

# For Personal Information...

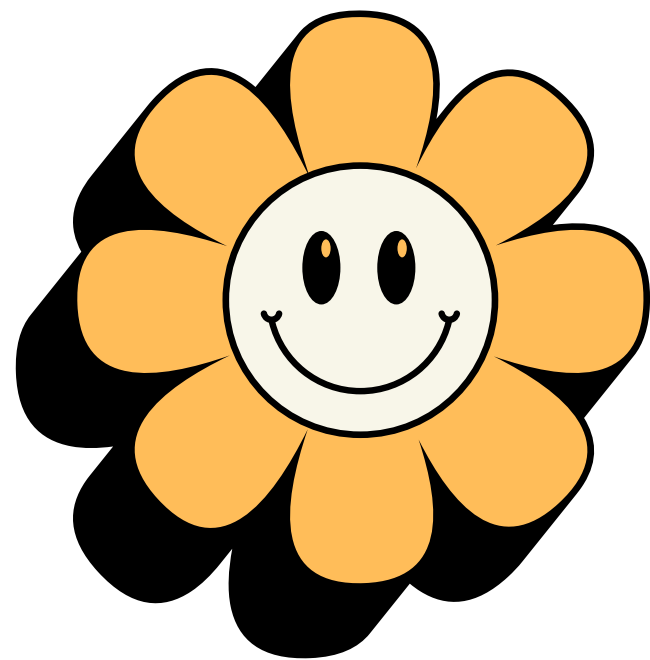
Did you give a scammer your Social Security number?  
Go to [IdentityTheft.gov](https://www.identitytheft.gov) to see what steps to take,  
including how to monitor your credit.

Did you give a scammer your username and password?  
Create a new, strong password. If you use the same  
password anywhere else, change it there, too.



# Scams on Scam Recovery?

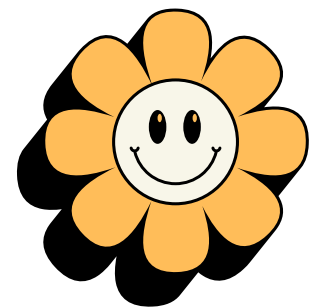
If someone calls and offers to “help” you recover money you have already lost, don’t give them money or personal information. You’re probably dealing with a fake refund scam.



# Computer Access

Does a scammer have remote access to your computer?

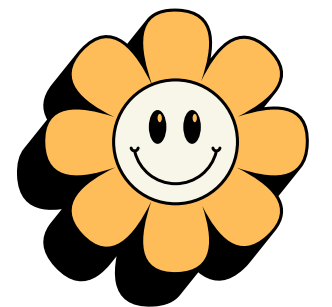
Update your computer's security software, run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information, such as changing important passwords, and updating security questions.



# Phone Number

Did a scammer take control of your cell phone number and account?

Contact your service provider to take back control of your phone number. Once you do, change your account password. Also check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution. Then go to [IdentityTheft.gov](https://www.identitytheft.gov) to see what steps you should take.

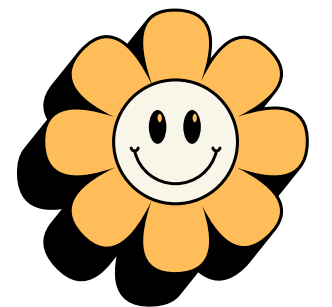


# One Last Note

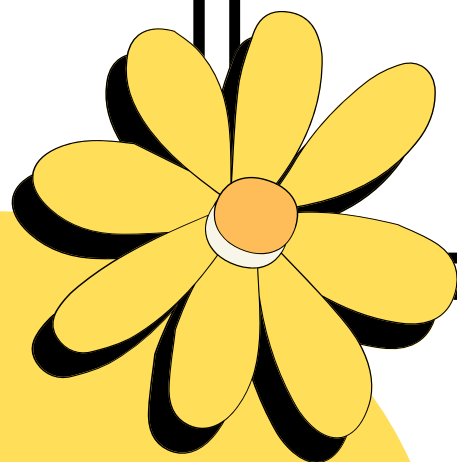
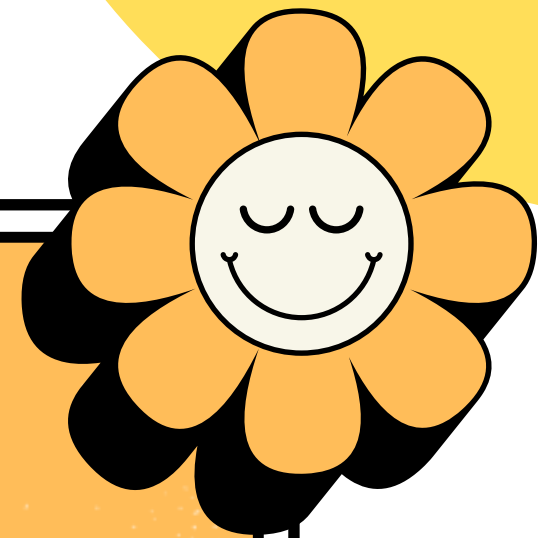
Remember, for all scams and frauds, there are ways to report them and recover from them. Start with:

<https://reportfraud.ftc.gov/> and <https://www.identitytheft.gov/>

It's important to remember to breathe. The recovery process is long, and things may not go how you want them to. There are people around you that can help you, so reach out to loved ones if you are feeling overwhelmed.



# Federal Trade Commission







# The FTC

Most of the information for this presentation was pulled directly from the Federal Trade Commission's pages. They offer tons of free information on their websites. Check the sources page at the very end of the presentation to find more detailed information and helpful links!

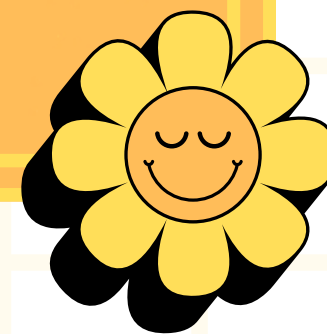
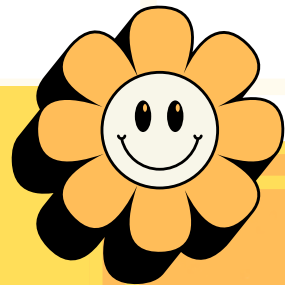


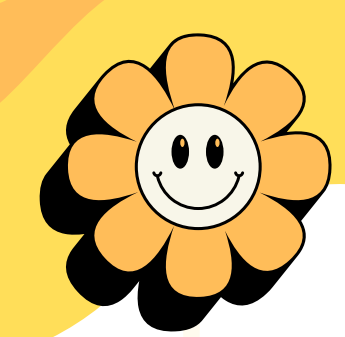
# **Tech Help Page!**

Thank you for checking out our  
scams presentation. This  
presentation can be found on our  
website along with all of our other  
Nekoosa Help Desk resources.



**THANK  
YOU**





# Sources

<https://www.bremertonwa.gov/DocumentCenter/View/1148/How-to-Avoid-Becoming-the-Victim-of-a-Scam-PDF>

<https://consumer.ftc.gov/articles/phone-scams>

<https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages>

<https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

<https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams>

<https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>

