GET CYBER AWARE

How to Stay Safe Online

Simple steps to spot scams, slow down, and get help

Get Cyber Aware | Arthur Press

HANDOUT

Today’s deck and handout – Getcyber.org

- Presentation is at: getcyber.org/local-residents
- Video of a similar seminar is at: getcyber.org
- Keep the handout somewhere easy to find

Scan me

WHY THIS MATTERS

Scams are big business

$16.6 BILLION

Estimated amount stolen by scammers in 2025

- That money is all profit for the criminals
- That is roughly Whirlpool’s annual revenue
- It is not “one guy in a basement.” It is an industry.

THE SCALE

The scam economy runs all day

$19,372

Avg amount stolen

$83,000

Avg amount stolen from seniors!

$5 billion

Total amount stolen from Seniors!

Scammers scale like a business. They use scripts, quotas, workers, tools, and pressure.

GROWTH

Scam revenue is growing fast. Revenue Growth in last 5 years!

Scam growth is not a side issue. It is a fast-growing criminal market.

Arthur Press

- 25 Years in I.T.
- 15 in I.T. Security

Why do I do this:

- Seen too many good people lose their life savings to criminals.

Why online safety matters

Because scammers are organized, patient, and very good at making people panic.

This is a blame-free zone.

If something happened to you, the shame belongs to the criminal, not you.

The 3 Golden Rules

These three rules beat almost every scam pattern.

RECAP

The 3 Golden Rules

1

Be wary of the Urgent

Slow down! Scammers thrive on pressure

2

Be suspicious

Do not give them access to your computer

Do not log into online banking

Be wary of strange payment methods

3

Talk to someone

Have a trusted friend you can call. Scammers want you isolated

Golden Rule #1

Be wary of urgency

Common urgency tricks

Your account closes in 45 minutes

Countdown timers

Pay now to avoid a late fee

Police will be dispatched

You have 15 minutes for a refund

RULE 1

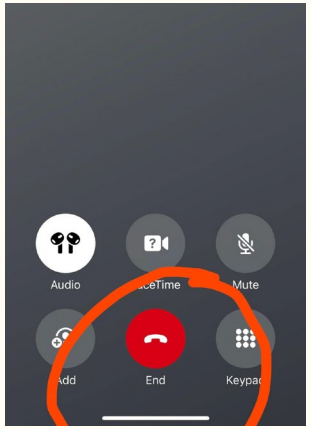
Urgency is the scammer's engine

- Be wary of the urgent
- Take a breath
- Hang up or close the message
- Verify another way. Phone # from official website, # on back of your credit card

RULE 1

Use these sentences

- “I do not make money decisions over the phone.”
- “I will call the company using the number on their website.”
- “Goodbye.” Then hang up.



Most effective tool: hang up.

Golden Rule #2

Be suspicious

RULE 2

Top red flag asks

- Remote access to your computer
- Log in to your online banking
- Send money by wire, gift cards, crypto, or transfer

RULE 2

No legitimate company asks

- Microsoft, Amazon, IRS, banks, and police do NOT demand gift cards
- Do not let strangers control your computer
- Police will not be dispatched to collect money

Solution: hang up and call a trusted number.

Golden Rule #3

Talk to someone

RULE 3

Isolation is part of the scam

- Call a friend, family member, bank, senior center, AARP, or police
- If the caller says “do not tell anyone,” tell someone immediately
- Use a family code word for urgent family calls.

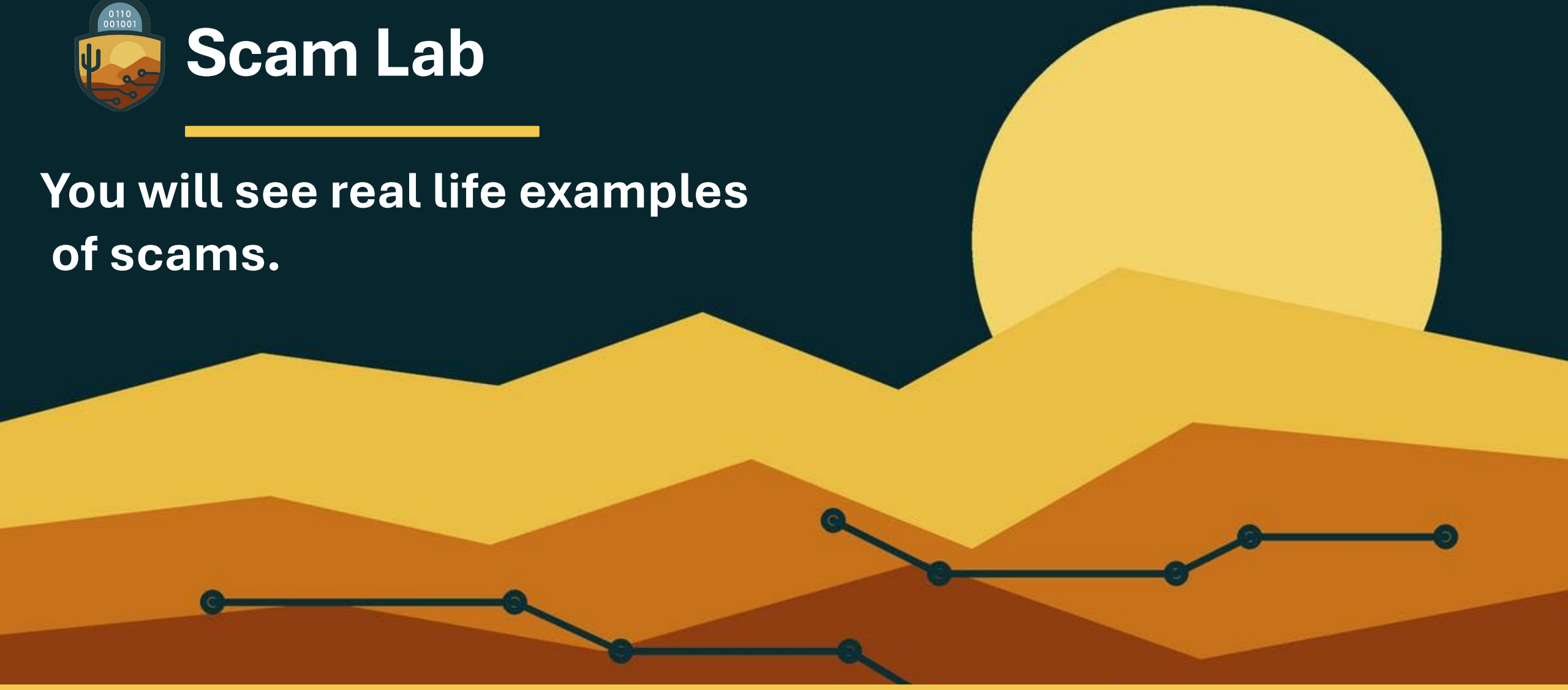
RULE 3

What to say to your bank

- “I think I am a victim of a scam.”
- Keep all evidence. Do not delete emails
- Place fraud alerts on all of your accounts

Scam Lab

You will see real life examples of scams.



PRACTICE

What is a Scam Lab?

- Look at real-world scam examples
- Teach you to spot urgency, red flags, and isolation
- Practice so you can teach someone else

DO NOT MEMORIZE NAMES

Avalanche of scam types

- There are too many scam names to memorize
- The names change constantly
- The pattern underneath is what matters

Avalanche of scams types

No need to read or memorize this list! Memorize the pattern

- 💘 **Romance & Emotional Manipulation Scams**
- Romance Scam
- Pig Butchering (crypto love trap)
- Catfishing Scam
- Fake Military Dating Scam
- Widow/Widower Companion Scam
- Online Dating Verification Fee
- Celebrity Impersonation Scam
- Inheritance Romance Scam
- Friendship-to-Investment Scam
- "Lonely Heart" Subscription Scam

- 💻 **Tech & Computer Scams**
- **Tech Support Scam**
- Remote Access Fraud (Call Center Scam)
- Fake Microsoft/Apple Alert
- Browser Locker Pop-Up
- Fake Antivirus Renewal
- Phishing Email Attack
- Smishing (Text Phish)
- Vishing (Voice Phish)
- Fake Software Update
- Ransomware Extortion

- 💰 **Investment & Financial Frauds**
- Ponzi Scheme
- Pyramid Scheme
- Fake Crypto Exchange
- NFT Investment Scam
- Forex Trading Fraud
- Pump-and-Dump Crypto Group
- Binary Options Scam
- High-Yield Investment Program (HYIP)
- "Insider Stock Tip" Scam
- Fake Wealth Coach or Mentorship
- Fake ACH Scam

- 🏠 **Real Estate & Housing Scams**
- Fake Rental Listing
- Airbnb/VRBO Vacation Scam
- Foreclosure Rescue Fraud
- Home Improvement Deposit Scam
- Title Deed Theft
- Fake Landlord Impersonation
- Moving Company Ransom Scam
- Utility Shut-Off Threat
- Timeshare Resale Fraud
- Property Management Impersonation

- 👮 **Government & Authority Impersonation Scams**
- **IRS/Tax Refund Scam**
- Social Security Suspension Call
- Jury Duty Warrant Scam
- Medicare Card Replacement Scam
- Police Charity Donation Scam
- DMV License Renewal Phish
- Student Loan Forgiveness Scam
- Fake Census or Voter Registration
- Unemployment Benefits

- 🛒 **Shopping & Consumer Frauds (51–60)**
- Facebook Marketplace Scam
- eBay Overpayment Scam
- Counterfeit Product Scam
- Fake Shipping Text (UPS/FedEx)
- Refund or Chargeback Scam
- Mystery Shopper Check Scam
- "Free Trial" Credit Card Trap
- Subscription Renewal Phish

- 📱 **Social Media & Digital Account Scams (61–70)**
- Instagram Investment DM Scam
- Account Verification Phish
- Friend "Help Me PayPal Me" Scam
- Fake Influencer Partnership
- Crypto Giveaway Fraud
- Deepfake Voice Impersonation
- QR Code Payment Trap

- ❤️ **Health & Charity Frauds (71–80)**
- Disaster Relief Charity Scam
- Medical Equipment Fraud
- Prescription Discount Trap
- Fake Insurance Enrollment
- Funeral Assistance Fraud
- Senior Care Plan Scam
- Weight Loss Pill Scam
- Medical Data Breach Phish
- Blood Donation Phish

- 🧓 **Senior & Elder Targeted Scams (81–90)**
- **Grandparent Scam**
- Utility Bill Collection Scam
- Medicare Part B Enrollment Scam
- "Arrest Warrant" Phone Threat
- Home Repair Contractor Fraud
- Fake Charity Donation Drive
- Reverse Mortgage Fraud
- Computer

The 3 major red flags

1

Want remote access to your computer

Gives them full access to your computer at any time

2

Want you to log onto online banking

Want your online banking password

Gives them full access to transfer your money

3

Want your money

Gift cards, wire, crypto, or cash are hard to reverse.

Example #1

Refund scam

Refund scam: the pitch

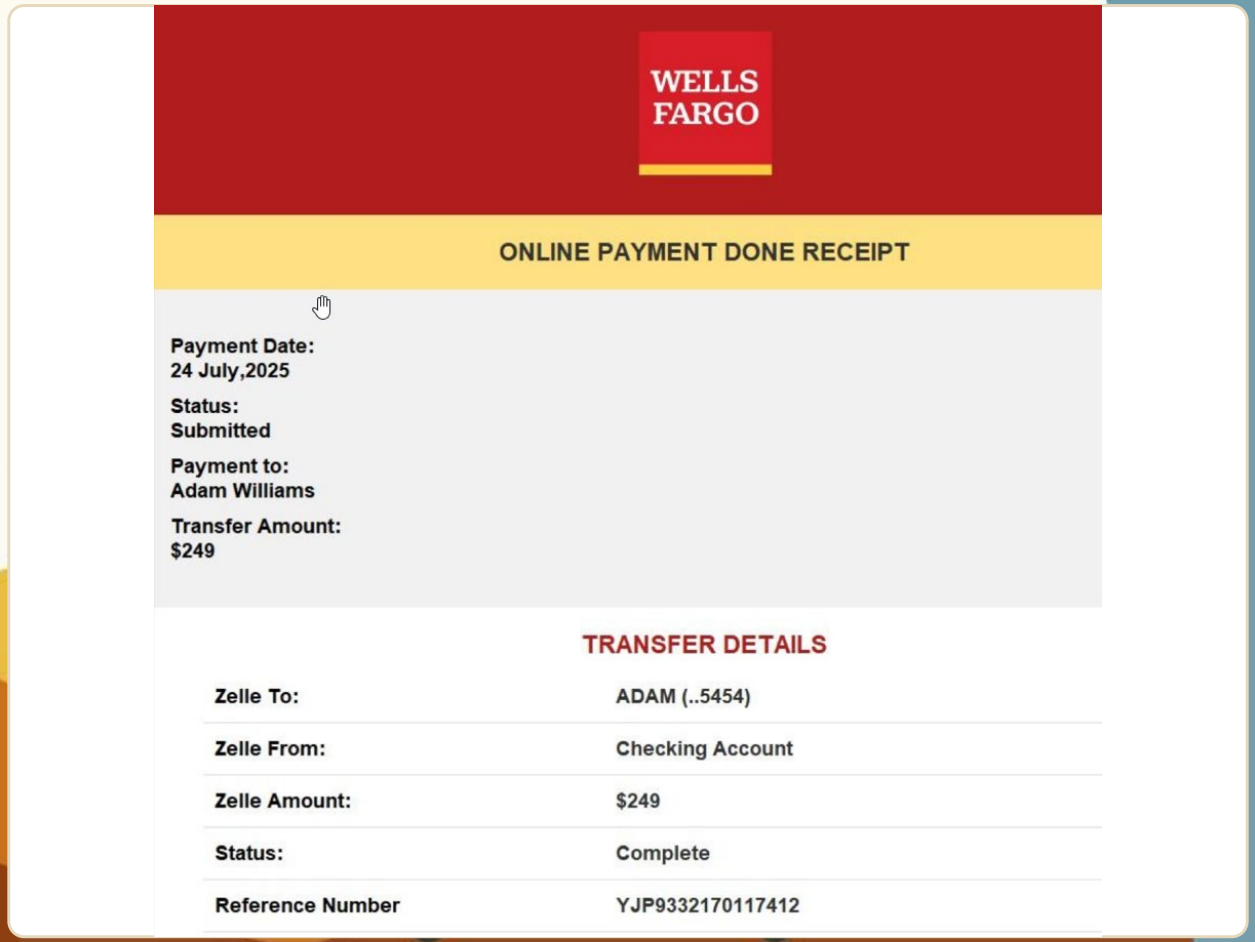
WHAT THEY ASK OF YOU

“We owe you a refund.”

“You were charged by mistake.”

WHAT TO DO

- Never allow remote access for a surprise refund
- Hang up
- Call the company using a number you find on google or back of your credit card



WELLS FARGO

ONLINE PAYMENT DONE RECEIPT

Payment Date:
24 July,2025

Status:
Submitted

Payment to:
Adam Williams

Transfer Amount:
$249

TRANSFER DETAILS

Zelle To:	ADAM (..5454)
Zelle From:	Checking Account
Zelle Amount:	$249
Status:	Complete
Reference Number	YJP9332170117412

HOW IT WORKS

How refund scams work – pretty technical.

1	Trigger	Fake invoice or surprise charge
2	Remote access	They ask you to install remote control software
3	The glitch	They make it look like they overpaid you
4	Extraction	You send the “extra” money back

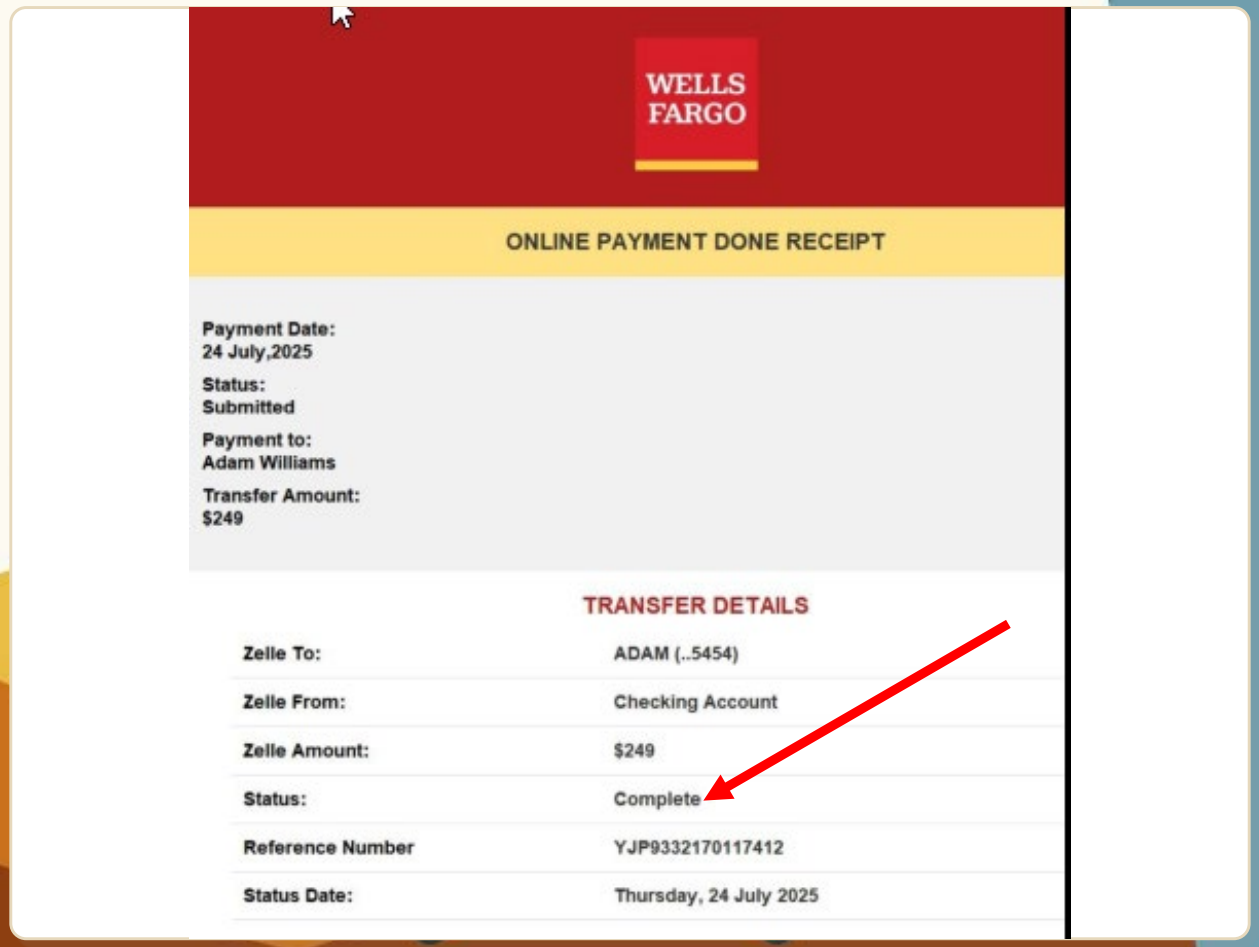
Example #1: Be wary of the Urgency

WHAT THEY ASK OF YOU

They claim a payment is “processing,” “same day,” or “complete.”

WHAT TO DO

- That language creates panic
- They want you to act without thinking
- Slow down and verify



WELLS FARGO

ONLINE PAYMENT DONE RECEIPT

Payment Date:
24 July,2025

Status:
Submitted

Payment to:
Adam Williams

Transfer Amount:
$249

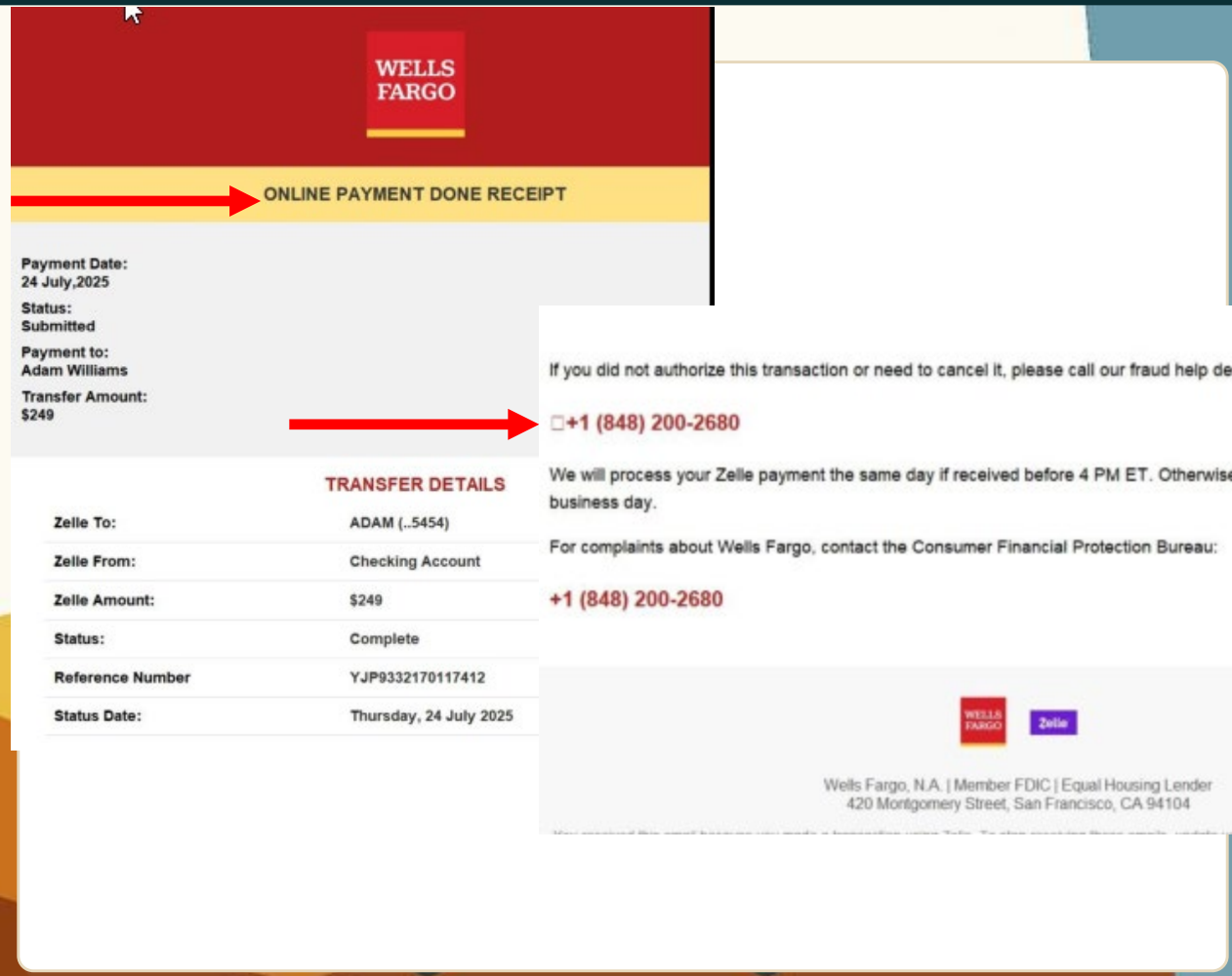
TRANSFER DETAILS

Zelle To:	ADAM (..5454)
Zelle From:	Checking Account
Zelle Amount:	$249
Status:	Complete
Reference Number	YJP9332170117412
Status Date:	Thursday, 24 July 2025

Example #1: Be Suspicious

SUSPICIOUS ITEMS

Unknown names, odd departments, fake help desk numbers, and details that do not match your bank.



WELLS FARGO

ONLINE PAYMENT DONE RECEIPT

Payment Date:
24 July,2025

Status:
Submitted

Payment to:
Adam Williams

Transfer Amount:
$249

TRANSFER DETAILS

Zelle To:	ADAM (..5454)
Zelle From:	Checking Account
Zelle Amount:	$249
Status:	Complete
Reference Number	YJP9332170117412
Status Date:	Thursday, 24 July 2025

If you did not authorize this transaction or need to cancel it, please call our fraud help desk immediately:

+1 (848) 200-2680

We will process your Zelle payment the same day if received before 4 PM ET. Otherwise, it will be proces
business day.

For complaints about Wells Fargo, contact the Consumer Financial Protection Bureau:

+1 (848) 200-2680

Wells Fargo, N.A. | Member FDIC | Equal Housing Lender
420 Montgomery Street, San Francisco, CA 94104

WHAT TO DO

- Do not call the number in the message
- Look up the bank phone number
- Use your bank app or card number

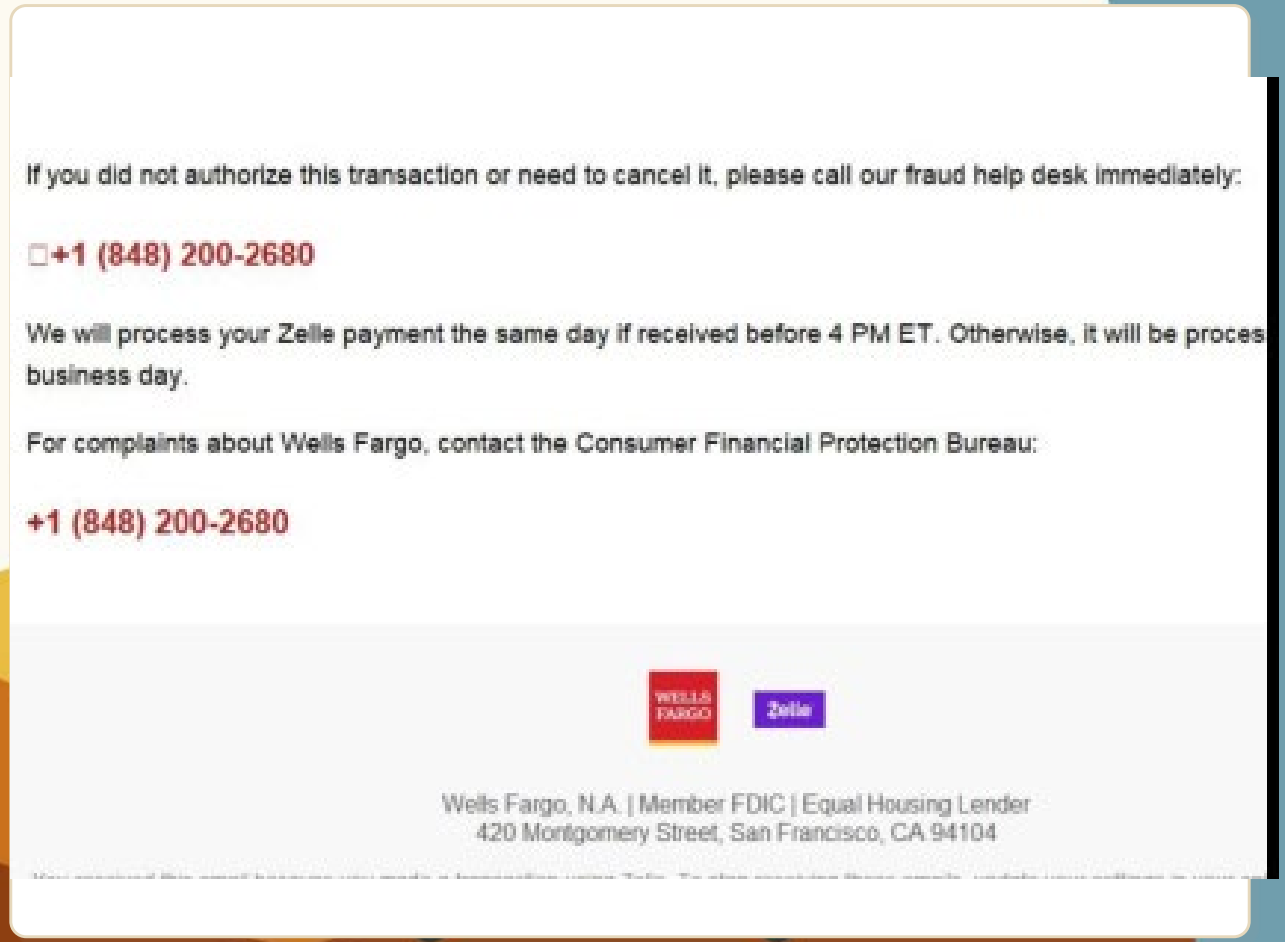
Example #1: Isolation

WHAT THEY SHOW YOU

A fake phone number keeps you inside the scammer's world.

WHAT TO DO

- End the call
- Call # on back of your CC



WHAT WE LEARNED

What did we learn from Example #1?

Urgency	Fake refund pressure and fake status
Suspicious	Odd names, fake numbers, misspellings
Isolation	Victim is pushed to call only the scammer

Example #2

Imposter scam: IRS or authority

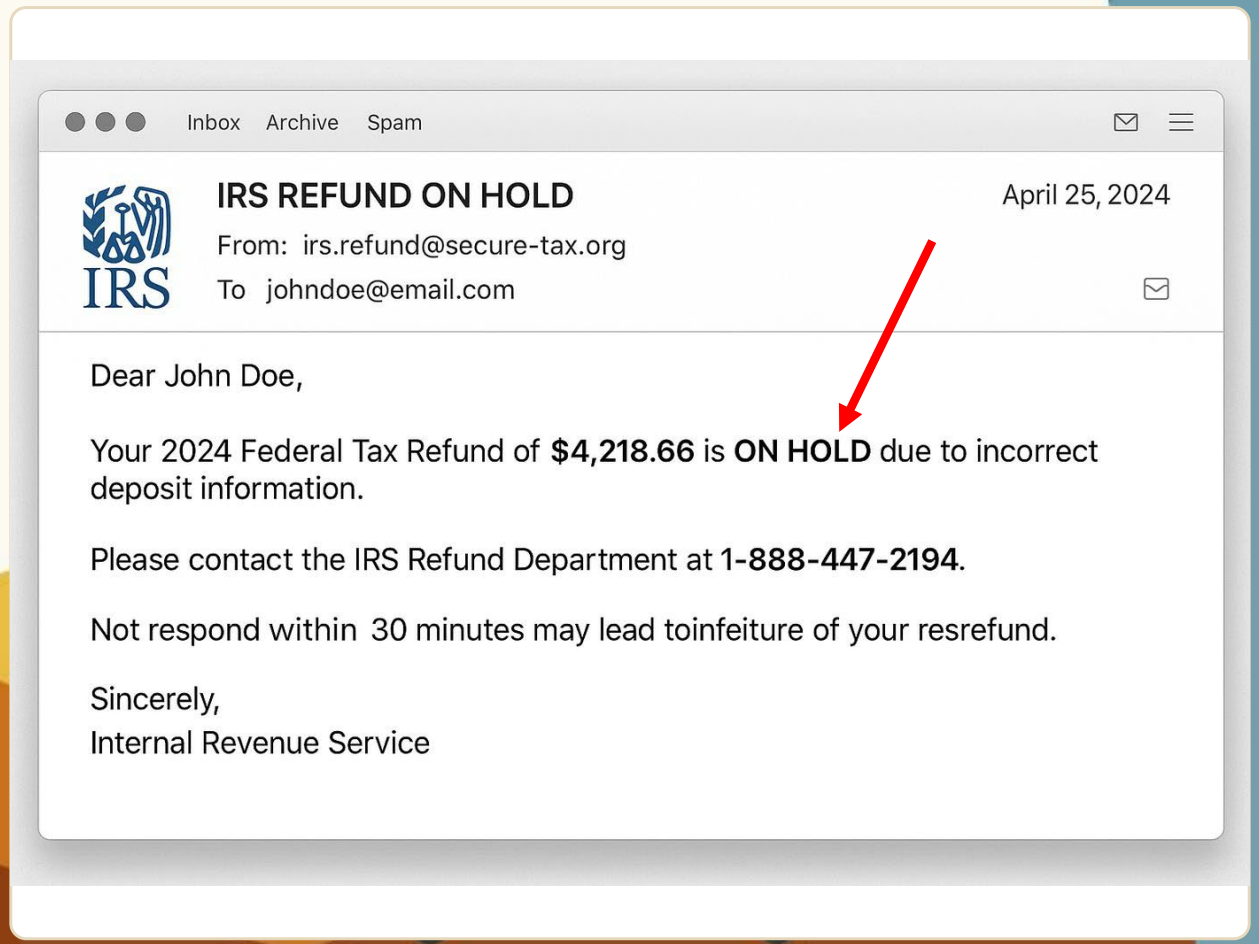
Example #2: Be wary of the urgency

WHAT THEY SHOW YOU

The message says your refund is “on hold” and demands quick action.

WHAT TO DO

- A real agency will not demand panic action by text or email
- Do not use the phone number in the message
- Go to the official website yourself



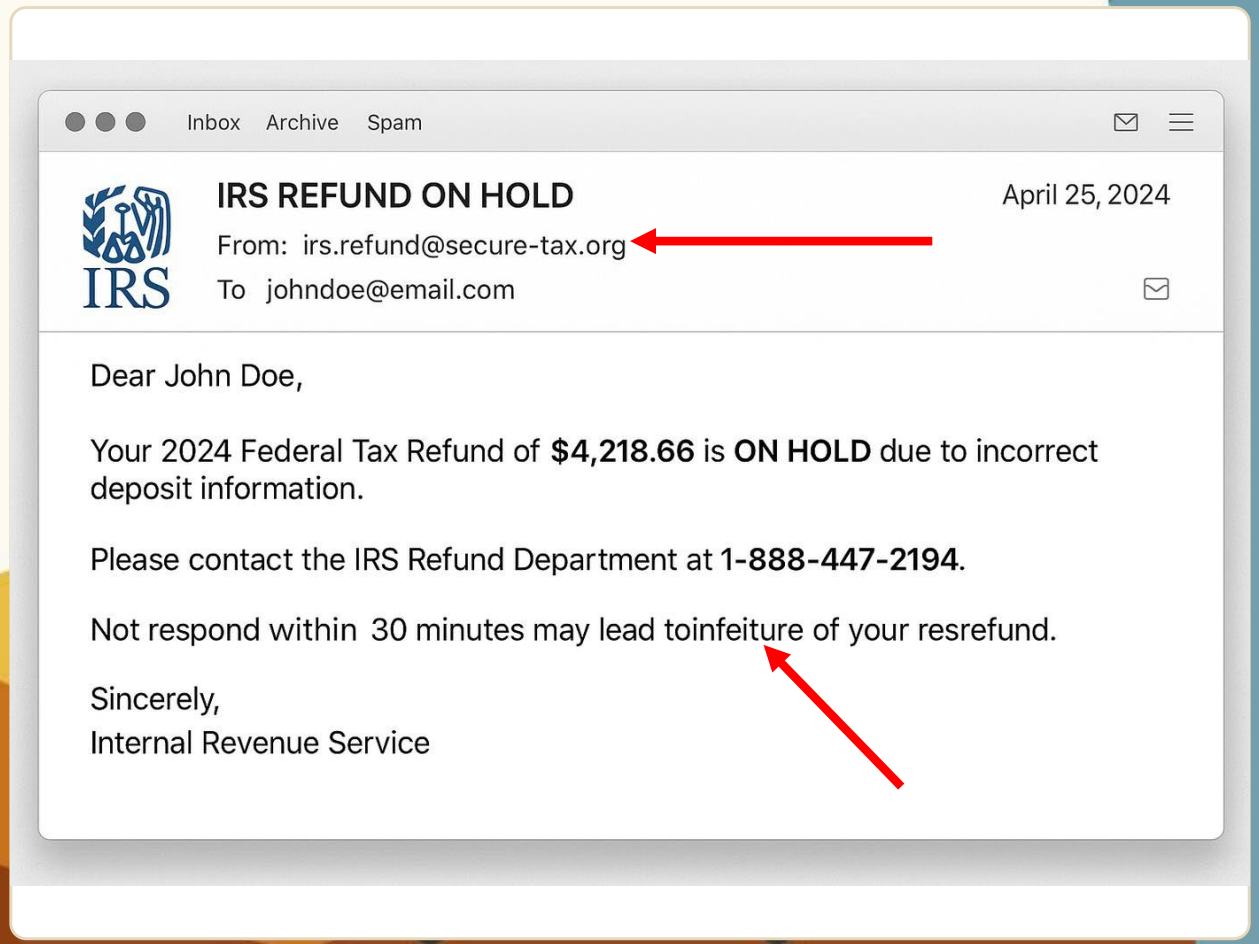
Example #2: Be Suspicious : Red flags

WHAT THEY SHOW YOU

The email address is not official. The message has misspellings. The phone number is fake.

WHAT TO DO

- Look for official .gov domains
- Do not trust logos alone
- Ask your accountant or use your IRS account



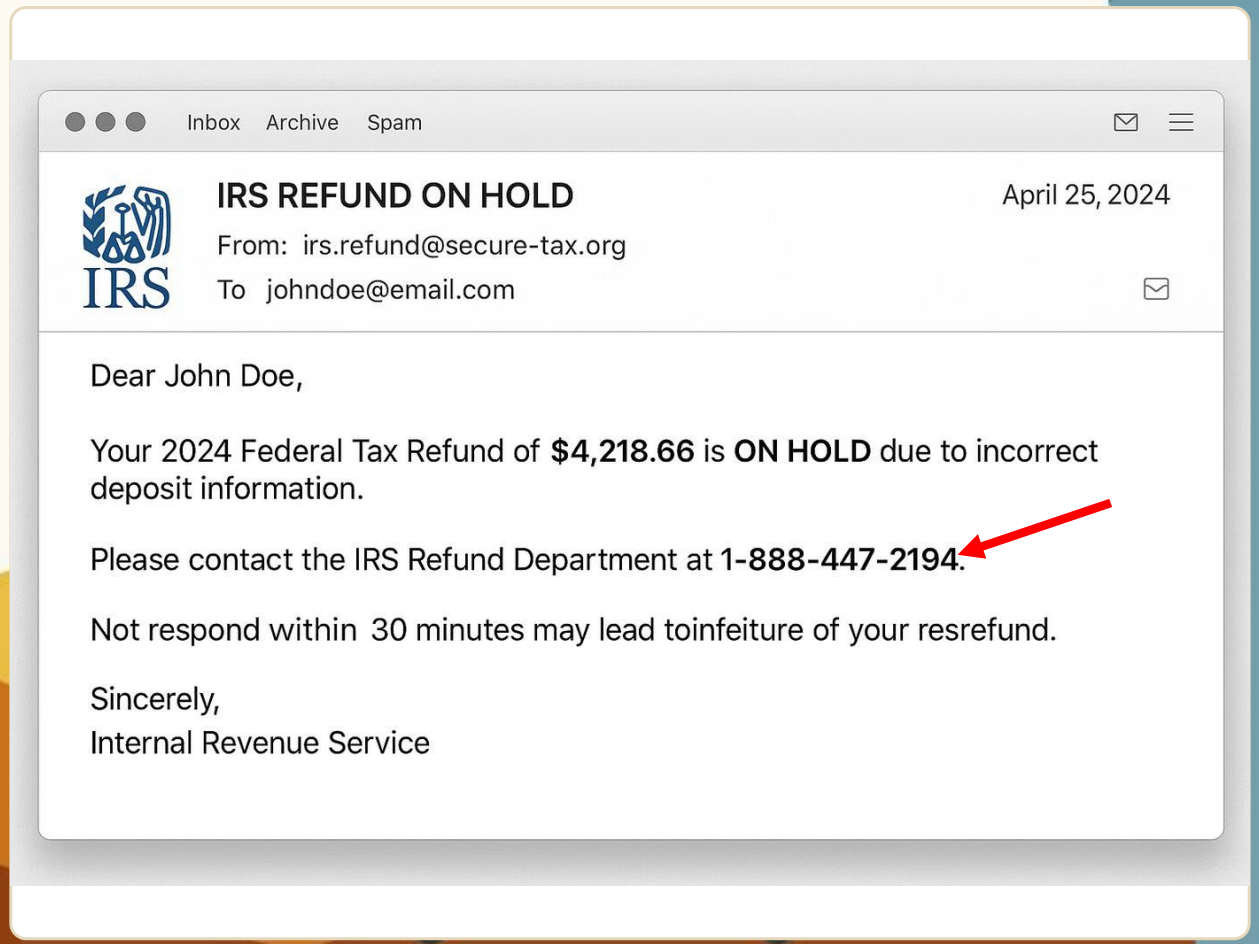
Example #2: Isolation

WHAT THEY SHOW YOU

They tell you to call only their number.

WHAT TO DO

- That keeps you trapped in the scam
- Verify independently
- Call a trusted person before acting



WHAT WE LEARNED

What did we learn from Example #2?

Urgency	“Respond in 30 minutes” pressure
Suspicious	Not a real IRS email or phone number
Isolation	You are steered to the scammer’s number

Example #3

Tech support scam

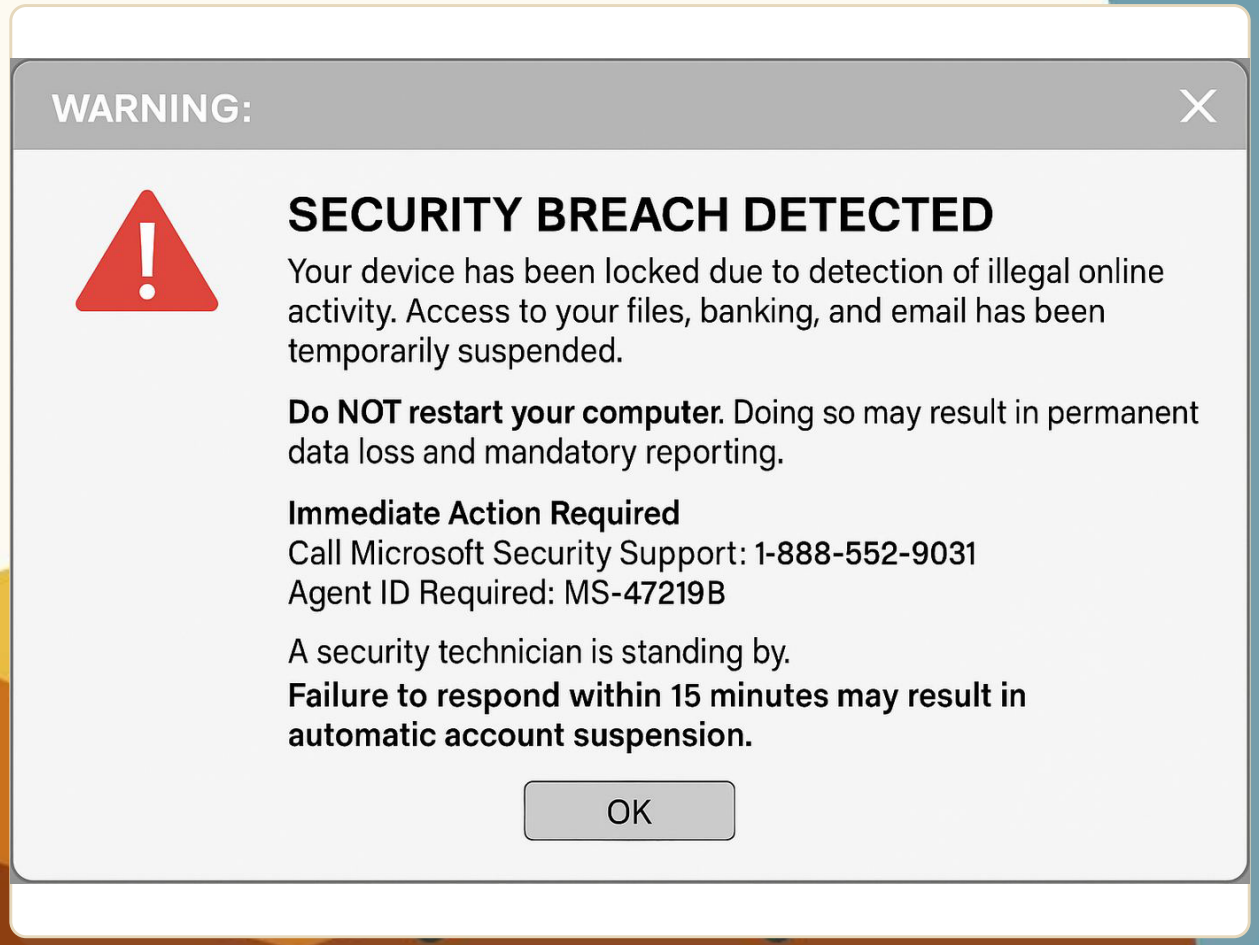
Tech support scams

WHAT THEY SHOW YOU

They pretend something is wrong with your device or accounts, then offer to "fix" the problem they invented.

WHAT TO DO

- Unsolicited tech support is a red flag
- Do not allow remote access
- Close the pop-up or hang up



SCAM LAB

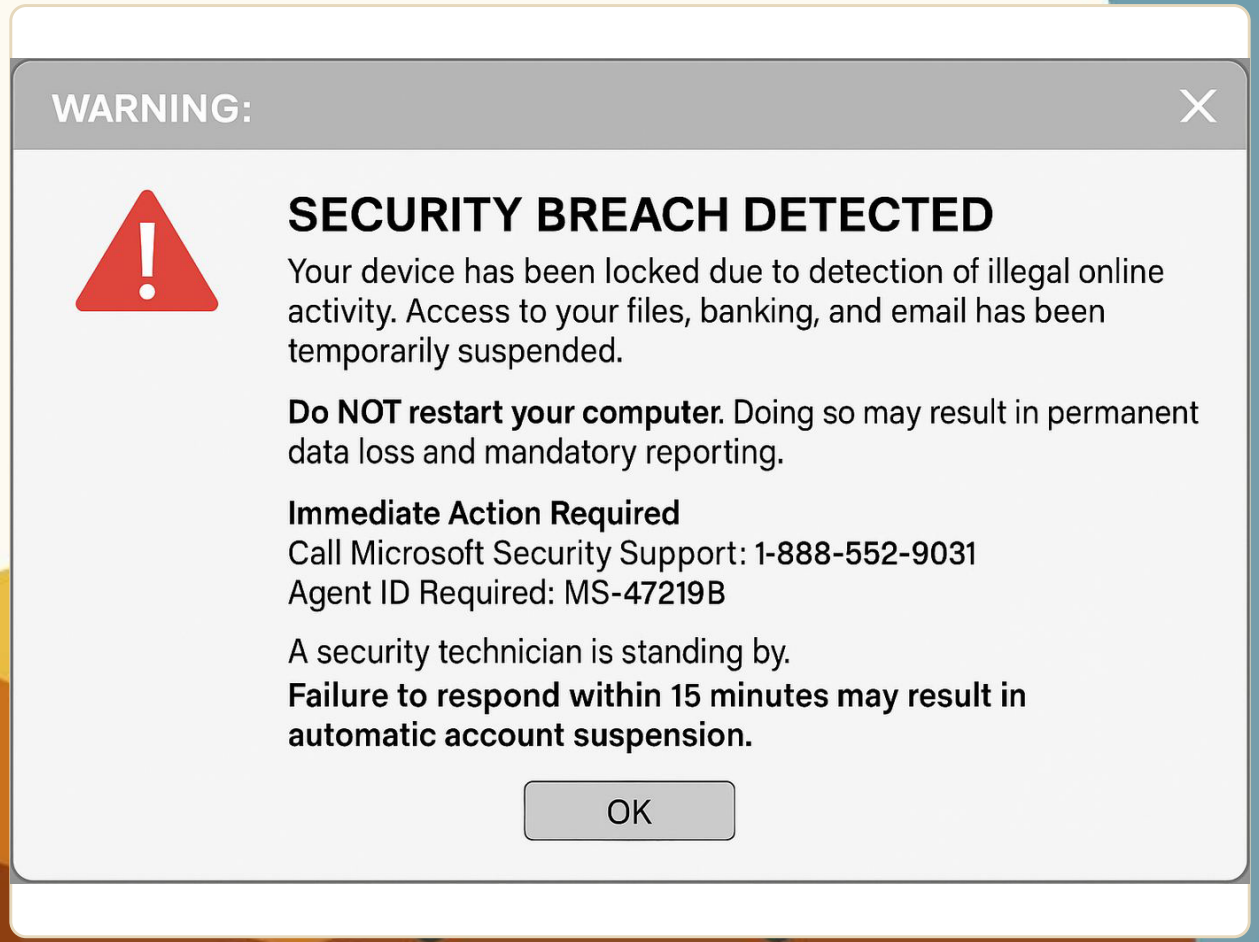
Group participation

Tell me

What is the urgency?
What is suspicious?
Where is the isolation?

WHAT TO LOOK OUT FOR

- Urgency
- Red flags
- Isolation



WHAT WE LEARNED

What did we learn from Example #3?

Urgency	Short deadline to respond
Suspicious	Threats of data loss or mandatory reporting
Isolation	Call their number or stay in their process

Grandson scam

AI voice cloning makes this one scarier, but the defense is simple.

FAMILY SCAM

The caller sounds like family

- A short clip may be enough to clone a voice
- The story is urgent and secret
- They ask for bail, hospital money, gift cards, crypto, or cash

How to stop a family emergency scam

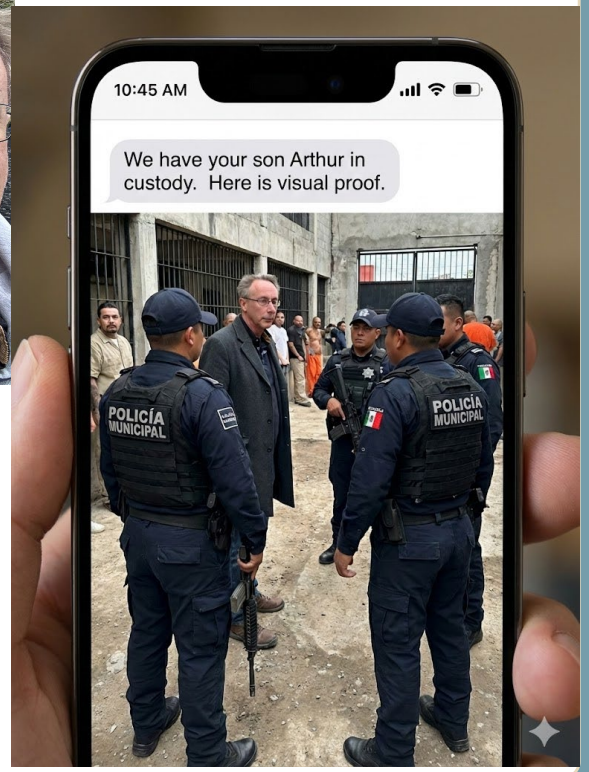
- Hang up and call your loved one on a known number
- Call another relative
- Use a family code word
- Ask a question only your real family would know

If they say “do not tell mom,” that means tell someone.

NEW TWIST

AI can fake voices and photos

- Do not trust a voice just because it sounds right
- Do not trust a photo just because it looks real
- Verify with a known number or family code word



Red flag recap

When you see these,
stop the transaction and break contact.

RECAP

Never do these for a stranger

1

Remote access

Do not let them control your computer.

2

Want your online banking info

Access your banking without you knowing

3

Weird payment

No gift cards, wire transfers, crypto, or cash.

What to do if you have been scammed

The faster you act, the better your chance of limiting the damage.

You are not to blame.

Preserve evidence.
You are a witness, evidence helps your bank and law enforcement.

Top do not’s

- Do not argue
- Do not explain
- Do not stay on the line
- Do not try to bait the scammer.
- Do not ask the scammer to return the money

Hang up means hang up.

FIRST CALL

Step 1: Call your bank

- Call the number on the back of your card or go into a branch
- Say: “I think I have been a victim of a scam”
- Ask them to stop wires, transfers, or charges immediately
- Ask for a case number and new card or account number

Time is key.

Step 2) Preserve evidence

- Do not Delete anything! Save emails, texts, screenshots, bank statements, and receipts
- Write a timeline of what happened and when money moved
- Keep phone numbers, email addresses, remote access codes, and crypto wallet addresses

Do not delete anything.

RESOURCES

Step 1a) Reach out for help

Your bank	Call all relevant banks and cards
Palm Springs Police	(760) 323-8116
FBI IC3	ic3.gov
National Elder Fraud Hotline	(833) 372-8311
Riverside County Elder Abuse	(800) 491-7123

Step 3) Contacting law enforcement

- Contact Palm Springs Police non-emergency: (760) 323-8116
- Keep all evidence
- Make a report. Get a case #
- Use who, what, where, when, why, and how
- Use who, what, where, when, why, and how

REPORT

Talking to law enforcement: who and what

Who: names they used, who they claimed to represent, phone numbers, email addresses

What: what happened, what they asked for, what they promised, what you sent

Where: phone, email, Facebook, website, bank, wire service, crypto wallet

Start with the short version first.

REPORT

Talking to law enforcement: when, why, and how

When: build a simple timeline

Why: why it seemed legitimate at the time

How: how they reached you, how you paid, and how much you lost

Recovery is not guaranteed, but the report still matters.

Protect yourself going forward

Small habits make you much harder to scam.

RECAP

Top 3

Update everything

Windows and apps need patches.

My favorite : PatchMyPC

Use a password manager

Every site gets a different password.

My favorite : Keepass Lastpass

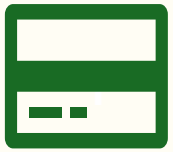
Backups

Two is one. One is none.

My favorite : Backblaze Lastpass, External drive

RECAP

Financial protection



Freeze your credit

Blocks new accounts in your name.

Turn on MFA

Text is good. Authenticator apps are better.

Use VPN

Never connect to Wifi. Use cell phone hotspot.

My favorite : Private Internet Access

Thank you for your time

Presentation and local resources:

https://getcyber.org/local-residents