Don't Get Fooled

Trusted Tech at Home | Scam awareness and response support for seniors, families, and home computer users

Call or Text: 253-480-6771 | trustedtechathome.com

Your screen fills with a flashing red warning. An alarm sounds. Large text says your computer has been locked and your banking information has been compromised. A phone number tells you to call Microsoft Support immediately. The window will not close no matter what you click.

Nothing is wrong with your computer. Nothing has been stolen. But the next thirty seconds will determine whether you hand over hundreds of dollars to a criminal running a call center in another country.

That scenario is real. It happened to someone in Bonney Lake last month. Versions of it happen every day across the South Sound -- by phone, by email, by text, and by pop-up. The targets are not naive. They are careful, intelligent people who were caught off guard for thirty seconds.

Why These Scams Work

Scammers are full-time professionals. They run organized call centers, follow tested scripts, and rehearse responses to everything you might say. Their entire job is to trigger fear quickly enough that you act before you stop to think. Four things make it possible every time.

- **Urgency:** Act now or it will be too late. There is no time to call someone or look it up.
- **Fear:** Arrest, account loss, or family emergency. The threat is designed to override reason.
- **Secrecy:** Do not tell your family. Real emergencies never require silence.
- **Irreversibility:** Gift cards, wire transfers, and Zelle cannot be undone once sent.

What This Guide Covers

Seven scam types that target South Sound households every week. For each one: what it looks like in real life, the exact red flags to spot before you act, step-by-step instructions for what to do, and what to do if someone already responded.

- Fake tech support pop-ups and browser lock screens
- Government imposter calls from the IRS, Social Security, or Medicare
- Family emergency and grandparent scams, including AI voice cloning
- Phishing emails from banks, Amazon, PayPal, and the Post Office
- Romance scams and long-game emotional fraud
- Lottery, prize, and fake-check scams
- Universal red flags and what to do if someone already responded

The Strongest Rule in This Entire Guide

No legitimate company, government agency, or real emergency needs gift cards, secrecy, panic, or instant action before you have time to verify. If any of those are present, stop. Every single time.

Something Feels Off?

Call or text Barry before clicking, paying, or giving anyone access to your device. No judgment -- just a calm second opinion. 253-480-6771 | trustedtechathome.com

The Fake Microsoft or Apple Pop-Up

What happens

A terrifying message suddenly fills your screen claiming your computer has a virus, your personal information has been stolen, or Windows has been blocked for your protection. A loud alarm may sound. A phone number is displayed and the message says to call immediately. The page may seem impossible to close.

REAL-WORLD EXAMPLE

"YOUR COMPUTER HAS BEEN LOCKED. Suspicious activity detected. Your banking information is at risk. Call Microsoft Support immediately: 1-800-XXX-XXXX. Do NOT restart your computer or your files will be deleted." This message is completely fake. Microsoft never sends pop-up alerts with phone numbers.

Red flags to watch for

!	Any pop-up that shows a phone number and says to call immediately.
!	The message plays an alarm sound or claims your computer has been locked.
!	It claims to be from Microsoft, Apple, Google, or Windows Defender.
!	You are told NOT to turn off or restart your computer.
!	The pop-up cannot be closed by clicking the X button.

What to do

1	Do NOT call the number. Microsoft and Apple never display pop-ups with phone numbers to call.
2	Force-close the browser. Windows: Ctrl+Alt+Delete, open Task Manager, End Task. Mac: Command+Option+Escape, Force Quit.
3	Restart your computer. This clears almost all fake alert pages completely.
4	Run your normal antivirus scan after restarting to confirm the device is clean.
5	Never allow remote computer access to anyone you did not call yourself using a verified number.

IF YOU ALREADY RESPONDED

Turn off your computer and disconnect from Wi-Fi immediately. Call me at 253-480-6771 before using the computer again for email or banking. If you paid by credit card or gift card, call your bank and report it as fraud right away.

The IRS, Social Security, or Medicare Call

What happens

You receive a call, voicemail, text, or email claiming to be from the IRS, the Social Security Administration, or Medicare. The message says your Social Security number has been suspended, you owe back taxes and face arrest, or your benefits are being cancelled. They demand immediate payment or personal information to verify your account.

REAL-WORLD EXAMPLE

"This is a final notice from the Internal Revenue Service. A lawsuit has been filed against you for tax fraud. You must call 1-800-XXX-XXXX within 24 hours to avoid arrest and criminal prosecution." The IRS contacts you by mail only -- never by automated phone calls threatening arrest.

Red flags to watch for

!	Any government agency demanding immediate payment over the phone.
!	Threats of arrest, lawsuits, or benefit cancellation unless you pay right now.
!	Requests for payment by gift card, wire transfer, Zelle, or cryptocurrency.
!	Caller asks you to confirm your Social Security number, Medicare ID, or bank account number.
!	An automated robocall claiming to be from a government agency.

What to do

1	Hang up immediately. You do not owe an explanation or a polite goodbye.
2	The IRS contacts you by mail first -- never by phone, text, or email for a first notice.
3	Social Security will never suspend your number. Medicare will never cancel benefits by phone.
4	If concerned, call the agency directly using a number from their official .gov website.
5	Report the call at reportfraud.ftc.gov.

IF YOU ALREADY RESPONDED

If you provided your Social Security number, call the SSA fraud line: 1-800-269-0271. If you sent money by gift card or wire transfer, contact your bank immediately and file a report with local police. Keep all records.

The Grandparent or Loved One in Trouble Scam

What happens

You receive a call from someone claiming to be your grandchild, a family member, or a person representing them such as a lawyer or bail bondsman. They say there has been an accident, an arrest, or a sudden emergency and need money right away. They beg you to keep it secret from other family members. AI voice cloning technology can now convincingly copy a real family member's voice from just seconds of audio found online.

REAL-WORLD EXAMPLE

"Grandma, it's me -- I was in a car accident in another state and I need bail money today. Please don't tell Mom and Dad. My lawyer will call you right back with where to send the money." The voice sounds real. The "lawyer" calls asking for $3,000 in Google Play gift cards.

Red flags to watch for

!	The caller asks you to keep the emergency completely secret from other family members.
!	Urgent request for money by wire transfer, gift card, or cash sent by courier.
!	The story involves being out of state, in jail, in a hospital, or in legal trouble.
!	The voice sounds slightly off even if it seems familiar.
!	You are rushed -- "I need the money in the next two hours or it is too late."

What to do

1	Hang up and call your grandchild or family member directly on their known number.
2	Establish a family code word in advance -- a secret word anyone can use to confirm it is really them.
3	Never send gift cards, wire transfers, or cash to anyone you have not personally verified.
4	Tell another family member immediately -- scammers count on secrecy to succeed.
5	If the caller claims to be police or a lawyer, look up the actual agency and call to verify.

IF YOU ALREADY RESPONDED

Contact your bank or the gift card company immediately -- some transactions can be reversed quickly if you act fast. Call local police and file a report. Do not be embarrassed -- this scam has fooled careful, intelligent people.

Fake Emails From Your Bank, Amazon, or the Post Office

What happens

You receive an email that looks exactly like it came from your bank, Amazon, PayPal, the Post Office, or another trusted company. It says there is a problem with your account, a package could not be delivered, or an unauthorized charge was detected. It asks you to click a link to verify your information. The link leads to a fake website designed to steal your login, password, or credit card number.

REAL-WORLD EXAMPLE

An email arrives that looks exactly like Chase Bank -- correct logo, colors, and format. It says: "Unusual sign-in activity detected. Verify your identity within 24 hours or your account will be suspended." The actual sender email address is "chase-alert@secure-accounts-verify.net" -- not Chase at all. Clicking the link opens a fake login page that captures your username and password.

Red flags to watch for

!	The sender email address looks wrong -- check the actual address, not just the display name.
!	Urgent language: "Your account will be suspended," "Verify now," "Action required within 24 hours."
!	The link address does not match the real company website (hover over it without clicking to check).
!	You were not expecting the email -- you did not place an order or contact this company.
!	The email asks for your password, full credit card number, or Social Security number.

What to do

1	Never click links in unexpected emails. Go directly to the company website by typing the address yourself.
2	Check the real sender address by clicking the sender name. A bank email comes from @bankname.com -- not a random domain.
3	Call the company directly using a number from the back of your card or their official website.
4	Real companies will never ask for your password by email. Not ever.
5	When in doubt, delete it. If it was real and important, the company will contact you another way.

IF YOU ALREADY RESPONDED

If you clicked a link and entered your password or payment information, change your password immediately from a different device and call your bank. If you entered a credit card number, report the card stolen and request a replacement.

The Online Friend or Love Interest

What happens

Someone reaches out on Facebook, a dating site, or by text -- sometimes claiming to have the wrong number at first. They are warm, attentive, and genuinely interested in your life. Over weeks or months they build a close relationship. They often claim to be a military officer overseas, a doctor on assignment abroad, or a successful professional. They never meet in person and always have a reason they cannot video call. Eventually they ask for money for an emergency, medical bills, or a plane ticket to come visit.

REAL-WORLD EXAMPLE

A widowed woman connects on Facebook with a man claiming to be a U.S. Army engineer in Germany. They talk every day for two months. He says he loves her and will visit soon. Then his equipment is seized at customs and he needs $2,500 to recover it. She sends it. Then there is a medical emergency. She loses over $40,000 before her daughter intervenes.

Red flags to watch for

!	They are never available to meet in person or video call at a time you choose without advance notice.
!	They express deep romantic feelings very quickly, often within days or weeks.
!	Their profile has few photos and little history -- images may be stolen from a real person.
!	They ask for money for emergencies, medical bills, travel costs, or customs fees.
!	They want to move the conversation off the platform to private text or email.

What to do

1	Never send money to someone you have not met in person, no matter how well you feel you know them.
2	Do a reverse image search of their profile photo at images.google.com -- scammers regularly steal photos.
3	Ask to video call at a time you choose without advance notice. Real people can do this.
4	Tell a trusted family member or friend about the relationship before it becomes serious.
5	Report the profile to the platform and to the FTC at reportfraud.ftc.gov.

IF YOU ALREADY RESPONDED

Stop all contact immediately and do not send more money. Contact your bank if you sent funds. Report to local police. Do not be embarrassed -- these are full-time professional criminals.

You Have Won -- Just Pay the Fee First

What happens

You receive a letter, email, text, or call saying you have won a lottery, sweepstakes, or major prize -- sometimes using a familiar name like Publishers Clearing House. The prize might be cash, a car, or a vacation. But before you can collect, you must pay a fee for taxes, processing, customs, or insurance. Once you pay, more fees appear. No prize ever arrives.

REAL-WORLD EXAMPLE

A realistic-looking letter arrives by mail with a check for $4,800 and a note saying you have won $50,000. To release the full amount you must first deposit the check and wire back $1,200 to cover "government processing taxes." The check appears to clear in your account -- but bounces five days later. You are out $1,200 in real money.

Red flags to watch for

!	You must pay money upfront to receive your prize -- real lotteries never work this way.
!	You do not remember entering the contest.
!	You are sent a check and asked to send back a portion of it -- always a fake check scam.
!	Urgency: you must respond within 24 to 48 hours or forfeit the prize.
!	Contact comes from a phone, text, or email address that does not match the real company.

What to do

1	You cannot win a contest you did not enter. If you do not remember entering, you did not win.
2	Legitimate prizes never require an upfront payment for taxes, processing fees, or anything else.
3	Never deposit a check and send back money -- the check will always bounce and you will owe the bank.
4	Call the real company using a number from their official website if you are genuinely uncertain.
5	Throw away the letter, delete the email, or hang up the call.

IF YOU ALREADY RESPONDED

If you deposited a fake check, notify your bank immediately. The check will bounce and you will owe the bank the funds -- the faster you act, the better your options.

Universal red flags — keep this page nearby

If any of these are true, stop immediately and verify before doing anything else.

- URGENCY: “Act NOW or it will be too late.” Legitimate situations allow time to pause and verify.
- SECRECY: “Do not tell your family.” Real emergencies do not require secrecy.
- GIFT CARDS: No legitimate business, government agency, or real person uses gift cards as payment.
- WIRE / ZELLE / CRYPTO: These payments are difficult or impossible to reverse once sent.
- REMOTE ACCESS: Someone wants to take control of the computer to “fix” or “protect” it.
- YOUR SSN / MEDICARE / PASSWORDS: Requests to “verify identity” by phone, text, or email.
- BAD ADDRESS: Slightly wrong email addresses, phone numbers, or website URLs.
- UNEXPECTED CONTACT: A package, account problem, prize, or emergency you were not expecting.
- GUT FEELING: If something feels wrong, stop and verify independently.

> **Strongest rule in the entire guide**
>
> No legitimate company, government agency, or real emergency needs gift cards, secrecy, panic, or instant action before you have time to verify.

If you think you have been scammed — do these steps now

1	Stop immediately. If you are in the middle of a call, transaction, or sending money -- stop right now. Hang up, close the browser, or cancel the transfer before anything else.
2	Do not be embarrassed. These are full-time professional criminals. Smart, careful people get scammed every day. The shame belongs entirely to them, not to you.
3	Call your bank right away. If you gave financial information or sent money, call the fraud number on the back of your card immediately. Ask about reversing or freezing the transaction.
4	Change your passwords. If you clicked a link, entered a login, or allowed computer access -- change your email and bank passwords from a different device if possible.
5	Call Barry. He can check your computer for remote access software, help you understand what was exposed, and walk through next steps with you. No judgment, just help. 253-480-6771.
6	Report it. FTC: reportfraud.ftc.gov | FBI Internet Crime: ic3.gov | SSA Fraud Hotline: 1-800-269-0271 | Local police (for a report number your bank may need).

Need a calm second opinion?

If something feels off, call or text Barry before clicking further, sending money, or giving access to your device.

Got a suspicious call, email, or pop-up? Not sure if something is real?

Call or text Barry anytime — help without judgment.

253-480-6771

trustedtechathome.com

Serving South Hill · Puyallup · Bonney Lake · Tacoma · surrounding areas