

Don't Panic

A Senior's Guide to

Computer Alerts

*When a scary message pops up on your screen,
this guide tells you exactly what to do.*

Read it now, while your computer is calm.

Prepared for the residents of Evergreen Village

The Golden Rule

If a message scares you, you do not have to fix it right now.

STOP. BREATHE. DO NOT CLICK.

Scary messages are designed to make you act fast. Real computer companies, banks, and the government will **never** demand money, gift cards, or remote access to your computer through a pop-up.

Three things to remember, always:

- **You are in control.** Nothing on a screen can hurt you or your computer if you simply do not click.
- **There is no rush.** A real warning can wait while you call a trusted person. Scams only work if you panic.
- **It is okay to turn it off.** If a message will not go away, hold the power button down to shut the computer off. You will not break it.

The Three-Color System

Every alert in this guide is sorted by color. Look for the colored bar and the symbol.

GREEN = SAFE

What it means: This is a normal message. Your computer is doing its job.

What to do: Read it, then close it or follow the simple step.

YELLOW = PAUSE

What it means: This might be fine, but it needs a second look.

What to do: Do not click yet. Write down what it says, then call a helper.

RED = DANGER

What it means: This is almost certainly a scam. Act to protect yourself.

What to do: Do not click anything. Do not call any number on the screen. Turn off the computer if needed.

The Do-Not-Click Protocol

Follow these steps in order whenever a message frightens you.

- 1. STOP your hands.** Take your hands off the mouse and keyboard. Do not touch anything yet.
- 2. Take a breath.** Count to ten slowly. The message is made to scare you. You have time.
- 3. Read it - but do not click.** Look at the words. Is it asking for money, gift cards, passwords, or to call a phone number? Those are scam signs.
- 4. Never call the number on the screen.** Real companies do not put phone numbers in pop-ups. The number goes to a scammer.
- 5. Never give anyone remote access.** If someone asks to take over your computer, say no and hang up. This is how money is stolen.
- 6. Never pay with gift cards or wire transfers.** No real business or government agency accepts gift cards. Anyone who asks for one is a scammer.
- 7. Close the message if you can.** Click the small X in the corner. If the browser asks if you want to leave the page, choose 'Leave Page' or 'Close Tab.' If the choices are confusing, do not click anything - hold the power button to shut the computer off.

8. If it will not close, shut the computer off. Press and hold the power button for 5-10 seconds until it goes dark. This is safe and will not damage anything.

9. Call a trusted person. Use the contact list at the back of this guide. Tell them exactly what the message said.

REMEMBER



No message on your screen can reach into your wallet, your bank, or your mail on its own. The only way scammers get in is if you click, call, or pay. **If you do nothing, they get nothing.**

The Alert Library

What each scary message looks like, and what to do.

1. The 'Virus Detected - Call Now' Pop-Up

WHAT IT LOOKS LIKE

A large red or blue box fills the screen. It may say 'Your computer is infected!' or 'Virus detected!' It shows a phone number and tells you to call 'Microsoft' or 'Apple Support.' Sometimes a loud beeping sound plays. The page will not let you close it easily.

DANGER - STOP & GET HELP

DO THIS

- Close the window or browser tab if you can.
- If it will not close, hold the power button to shut the computer off.
- Turn it back on and run your real antivirus program (like Windows Defender).

DO NOT

- Do not call the number on the screen.
- Do not let anyone take over your computer.
- Do not pay anything or give a credit card.

Who to call: A trusted volunteer from the list at the back of this guide.

2. The 'Scanning Your Computer' Page

WHAT IT LOOKS LIKE

A web page shows a progress bar that looks like it is scanning your files. Bars turn red, a count of 'threats found' climbs fast, and a button says 'Remove threats' or 'Clean now.' This is a picture, not a real scan.

DANGER - STOP & GET HELP

DO THIS

- Close the browser tab. If stuck, shut the computer off with the power button.
- Run a real scan using your built-in antivirus afterward.

DO NOT

- Do not click 'Remove' or 'Clean'.
- Do not download any 'antivirus' it offers - it is the virus.

Who to call: A volunteer, if you are unsure how to run a real scan.

3. 'Update Available' or 'Restart to Update'

WHAT IT LOOKS LIKE

A small, plain message from your computer (Windows or Mac) says updates are ready, or asks 'Restart now or tonight?' It is calm, has no threats, and does not ask for money or a phone call.

SAFE - NO NEED TO PANIC

DO THIS

- Save your work, then choose 'Restart now' or 'Update tonight.'
- Let it finish updating before you use it again. This is normal and keeps you safe.

DO NOT

- Do not click 'Remind me later' forever - updates protect you.
- Do not pay - real updates are always free.
- Do not trust 'update' messages inside a web page or that ask for a phone call - those are scams.

Who to call: No one - this is routine. Ask a volunteer only if it looks different.

4. 'Allow Notifications / Camera / Location?'

WHAT IT LOOKS LIKE

A small box appears asking if a website may show notifications, use your camera, or know your location. The choices are usually 'Allow' or 'Block.'

PAUSE - ASK FIRST

DO THIS

- If you did not expect it, choose 'Block.'
- On a site you trust (like a video call), 'Allow' may be fine - but ask if unsure.

DO NOT

- Do not click 'Allow' just to make the box go away.
- Do not allow camera or location on strange sites.

Who to call: A volunteer, if the box keeps coming back.

5. Email with an Attachment or 'Click This Link'

WHAT IT LOOKS LIKE

An email (maybe from a name you sort of recognize) has an attachment or a link, and says something urgent: 'Your account,' 'Invoice,' or 'You won a prize.' It may have spelling mistakes.

PAUSE - ASK FIRST

DO THIS

- Leave the email alone. Do not open the attachment or click the link.
- If it claims to be your bank, call the bank using the number on your card - not any number in the email.

DO NOT

- Do not open attachments you did not expect.
- Do not enter passwords after clicking an email link.

Who to call: A volunteer to help you check if the email is real.

6. 'Your Password Was Changed' or a Login Code

WHAT IT LOOKS LIKE

You get a text or email with a one-time code you did not ask for, or a message saying your password was changed. This can mean someone is trying to get into your account.

DANGER - STOP & GET HELP

DO THIS

- Do not share that code with anyone - not even someone who calls you.
- Change your password yourself, using a site you open by hand (not an email link).
- Turn on two-step sign-in if you can.

DO NOT

- Do not give the code to a 'support' caller.
- Do not click links in the alert email.

Who to call: A volunteer, and your bank if the account is financial.

7. 'Your Account Is Locked' - Bank or Payment

WHAT IT LOOKS LIKE

A message, email, or text says your bank, PayPal, or card account is locked or suspended. It wants you to click a link or call to 'verify' yourself. It feels urgent and scary.

DANGER - STOP & GET HELP

DO THIS

- Do not click the link. Do not call the number in the message.
- Call your bank using the number printed on the back of your card or on your statement.
- Check your account by typing the bank's web address yourself.

DO NOT

- Do not give your password, PIN, or one-time code.
- Do not sign in through a link in a message.

Who to call: Your bank's fraud line, then a family member.

8. 'Let Me Fix It For You' - Remote Access

WHAT IT LOOKS LIKE

Someone calls, or a pop-up says a technician will take over your computer to 'remove a virus.' They ask you to install a program or read them a code so they can see your screen.

DANGER - STOP & GET HELP

DO THIS

- Hang up the phone. Say nothing and end the call.
- Shut the computer off if they already connected.
- If they saw your bank or email, call your bank right away.

DO NOT

- Never install a remote-access program at a stranger's request.
- Never read a code to someone who called you.

Who to call: Your bank first, then family and the police non-emergency line.

9. 'Pay With Gift Cards' or Wire Transfer

WHAT IT LOOKS LIKE

A caller (claiming to be IRS, a grandchild in trouble, tech support, or a 'sweepstakes') says you must pay using gift cards, a wire transfer, or crypto. They keep you on the phone and tell you not to tell anyone.

DANGER - STOP & GET HELP

DO THIS

- Hang up. Do not buy any cards. Do not send money.
- If you already paid, call your bank immediately.
- Tell a trusted family member what happened.

DO NOT

- Never buy gift cards to pay any 'debt' or 'fee.'
- Never keep it a secret - secrecy is the scammer's weapon.

Who to call: Your bank, then family, then police non-emergency line.

If Something Already Went Wrong

It is not your fault. Act quickly and you can limit the harm.

Did you do one of these? Act now:

- Gave remote access to your computer
- Shared a password, PIN, or one-time code
- Sent money, bought gift cards, or gave a card number
- Entered your bank sign-in on a link from an email

DO THESE IN ORDER

1. Call your bank. Use the number on the back of your card. Tell them you may have been scammed. Ask them to freeze or watch your accounts.



2. Change passwords. On a safe computer, change your email and bank passwords. Use a different password for each.

3. Tell a trusted person. A family member, friend, or volunteer. You are not in trouble, and shame is the scammer's friend.

4. Report it. Report scams to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) or 1-877-382-4357. For a grandparent or 'in-trouble' call, contact your local police non-emergency line.

*You are not alone, and you did not 'fall for it' - these crimes are built to fool everyone. Reporting helps **protect your neighbors, too.***

My Tech-Help Contact List

Fill this in with people you trust. Keep it by the phone and the computer.

Trusted people who can help me think it through:

Family Member	
Trusted Neighbor	
Bank Fraud Number	
Local Volunteer Help	

**State Police Non-Emergency Contact Information
For Mount Bethel, PA 18343**

Station: PSP Troop M - Belfast

- Phone: 610-759-6106
- Address: 654 Bangor Road, Nazareth, PA 18064

Volunteer Sign-Up Sheet

For volunteers willing to help a neighbor with technology questions. Please print your name and a phone number where seniors may reach you. Post this sheet in a common area so everyone can use it.

Only list a phone number you are comfortable sharing with residents.

Name	Phone	Best Hours	Can Help With

Tip for the 'Can Help With' column: write things like scams & pop-ups, email, passwords, printer, phone, or 'a calm second opinion.'

Cut-Out Pocket Card

Cut along the lines and keep this card in your wallet or purse.

WHEN A MESSAGE SCARES YOU:

1. Hands off. Do not click.
2. Breathe. You have time.
3. Never call the number on the screen.
4. Never give remote access to anyone.
5. Never pay with gift cards.
6. If stuck, hold the power button to shut it off.
7. Call a trusted person.

Numbers to Remember

Your bank's fraud line	Use the number on the back of your card
FTC Fraud Report	1-877-382-4357 - ReportFraud.ftc.gov
Police non-emergency	Call 911 only for danger to a person
AARP Fraud Helpline	1-877-908-3360 (Mon-Fri, 8am-8pm ET)

This guide is general information, not legal or professional advice. When in doubt, call a trusted person before you click. Sources: [U.S. Federal Trade Commission \(ReportFraud.ftc.gov\)](#); [AARP Fraud Watch Network \(aarp.org/fraudwatchnetwork\)](#).