❄ FROSTWATCH

The Senior Scam Protection Packet

Scammers are getting bolder — but one simple habit stops almost every one of them. This free packet teaches you that habit, in plain English, in about ten minutes.

100% FREE — yours to keep & share

Inside this packet:

- ✔ The 60-Second Rule that defeats nearly every scam
- ✔ The 7 scams aimed at seniors most — and what to do
- ✔ How to safely close a fake "virus" pop-up
- ✔ What to do in the first hour if you already paid
- ✔ A one-page cheat sheet for your fridge

Free from The FrostWatch Team. Print it. Share it. Give a copy to a friend or neighbor — staying safe is something we do together.

Questions? Email us any time: **frizzlelogger@gmail.com**

THE ONE HABIT THAT PROTECTS YOU

The 60-Second Rule

Every scam — every single one — needs you to **hurry**. The scary pop-up, the urgent phone call, the "act now" text: they all want you to act before you think.

So here is the rule — the heart of this whole packet:

STOP. BREATHE. VERIFY.

When anything online or on the phone frightens you or rushes you, **stop everything for 60 seconds**. Take a slow breath. Then verify — using a number or address *you* already trust.

How "verify" works

- A message says your bank account is frozen? **Hang up.** Call the number printed on the back of your bank card — not the number in the message.
- A pop-up says your computer is infected? **Do not call the number on the screen** — it belongs to the scammer. (Page 5 shows the safe way to close it.)
- A caller says a grandchild is in trouble? **Hang up and call your grandchild** — or their parents — on the number you already have.

Remember: Real banks, police, and computer companies will *never* be angry that you hung up and called back on a trusted number. Only a scammer will argue — and that argument is your proof. You are not being rude. You are being safe.

KNOW THEM AND THEY LOSE THEIR POWER

The 7 Scams Seniors Face Most (1 of 2)

1. The Fake Virus Pop-Up

What it looks like: Your screen fills with warnings — "VIRUS DETECTED! Call this number now!" — often with a loud alarm voice.

What to do: Never call the number or click anything in it — close it the safe way on page 5.

2. The Tech-Support Call

What it looks like: A caller claims to be from "Microsoft," "Apple," or your internet company, says they found a problem, asks to connect to your computer, or be paid in gift cards.

What to do: Hang up. Real companies never call out of the blue, and repairs are never paid for with gift cards.

3. The Grandparent Scam

What it looks like: "Grandma? It's me — I'm in trouble. Send money and don't tell Mom." Computers can copy voices now — it may sound exactly like them.

What to do: Hang up and call your grandchild on their real number. A family code word (page 6) stops this cold.

4. Medicare & Social Security Impostors

What it looks like: A call or letter saying your benefits will stop unless you "confirm" your Medicare or Social Security number.

What to do: Hang up — those agencies never threaten benefits by phone, new Medicare cards are free, and never share your numbers with someone who contacted *you*.

KNOW THEM AND THEY LOSE THEIR POWER

The 7 Scams Seniors Face Most (2 of 2)

5. The Fake Bank Fraud Alert

What it looks like: A text or email: "Suspicious charge of $499 — click here to dispute it," or a caller asking you to move money to a "safe account."

What to do: Never click the link or move money because a caller told you to. Call the number on the back of your card instead.

6. Romance & Investment Scams

What it looks like: A friendly stranger online slowly becomes a sweetheart — or pushes a "sure thing" investment, often in cryptocurrency, that always needs a little more money.

What to do: Never send money to someone you have not met in person — and remember, real investments let you take money *out* as easily as putting it in.

7. Package-Delivery Texts

What it looks like: A text: "Your package could not be delivered. Tap here to reschedule" — with a small "fee" or a request to sign in.

What to do: Do not tap the link. If you're expecting a package, go to the company's real website yourself, the way you normally would.

The pattern to remember: every scam pushes you to *hurry* and *keep it secret*. Honest people do neither. Urgency + secrecy = scam.

HANDS-ON HELP

The Safe Close: Escaping a Fake Virus Pop-Up

That full-screen "virus" warning is just a web page pretending to be an alarm. It cannot hurt you by itself — it only wins if you call the number.

Step 1 — Close the browser completely

1. Try the normal way first: click the **X** at the very top-right corner of the window.
2. If it will not close, hold down **Alt** and press **F4** — that closes the window.
3. If the screen seems frozen or the pop-up keeps coming back, hold down **Ctrl + Alt + Delete**, choose **Task Manager**, click your browser (Chrome, Edge, or Firefox), then click **End task**.

Step 2 — Say no to "restore pages"

If your browser later asks to bring back the pages you had open, choose **"Don't restore"** — restoring brings the scary page right back.

Step 3 — Clean up the noisy notifications

These pop-ups often return because a website was once allowed to send "notifications." Turn them off:

- **Chrome:** Menu (⋮) → Settings → Privacy and security → Site settings → Notifications. Remove any site you don't recognize.
- **Edge:** Menu (...) → Settings → Cookies and site permissions → Notifications. Remove anything unfamiliar.

That's it. No harm done, no number called. If warnings keep appearing after this cleanup, FrostWatch's Browser Guard and Scam Shield help block exactly this — see the last page.

SMALL STEPS, BIG PROTECTION

Passwords & the Family Code Word

Passwords that protect you — and that you can actually remember

- **Use a passphrase, not a password.** Three or four plain words strung together — like *SunnyPorchCoffee7* — are long, strong, and easy to remember.
- **Never reuse the same password in two places.** If one company is hacked, a reused password unlocks everything else.
- **Your email password matters most.** Whoever gets into your email can reset almost every other account — make it extra strong.
- **Turn on two-step verification** for email and banking wherever offered. Even if someone learns your password, they can't get in without your phone.
- **Writing passwords down is okay — done right.** A notebook kept at home, away from the computer, beats reusing "Fluffy123" everywhere. Better still: a password vault (FrostWatch includes one — last page) locks them behind one master PIN.

The family code word — two minutes, total protection

Pick one secret word with your children or grandchildren — something only your family would know, like a childhood pet's silly nickname:

"If you ever call me asking for help or money, I will ask for the code word. No code word, no money — I hang up and call you back."

A computer can copy a voice in seconds — it cannot guess your family's secret word.

IT HAPPENS TO SMART PEOPLE — ACT FAST

"I Already Called the Number / Paid" — Your First-Hour Checklist

First: **do not blame yourself.** This happens to careful, intelligent people every day — these are professional criminals. Act quickly:

1. **Hang up and stop all contact.** If they call back, do not answer. Write down the number, what they said, and what you paid.
2. **Call your bank — now.** Use the number on the back of your card, explain what happened, and ask them to stop or reverse the payment — banks can often help if you call fast.
3. **If you paid with gift cards,** call the number on the back of the card and report it right away — keep the cards and receipt.
4. **If you let them connect to your computer,** stop banking on it until a trusted person checks it. Change important passwords from a *different*, clean device.
5. **Change passwords and turn on two-step verification** — email and bank first, then the rest.
6. **Report it** to your local police non-emergency line and at reportfraud.ftc.gov — it protects your neighbors too. Then tell your family: no shame, and your warning may save someone you love.

Safe Internet Basics

- **Let updates happen.** When Windows or your browser offers an update, say yes — updates close the doors scammers use. Restart weekly so they finish.
- **Back up what matters.** Once a month, copy photos and documents to a USB drive — then *unplug it* and store it in a drawer.
- **Check the address before you sign in, and treat email links like strangers at the door** — scammers use look-alikes like "amaz0n." When in doubt, type the real address yourself.

✂ CUT THIS PAGE OUT — PUT IT ON YOUR FRIDGE

MY SCAM CHEAT SHEET

STOP. BREATHE. VERIFY.

- **A warning with a phone number IS the scam.** Never call it.
- **Hang up. Call back** on a number YOU trust — the one on your bank card.
- **No real company** takes payment in gift cards. Ever.
- **Urgency + secrecy = scam.** Honest people never rush you.
- **Ask for the family code word.** No code word → hang up.
- **Already paid?** Call your bank right away.

About FrostWatch — the folks who made this packet

Full disclosure: we make FrostWatch — a Windows safety program designed senior-first, in big, clear, plain English:

Browser Guard warns before scam pages · **Scam Shield** spots scam sites and pop-ups · **Password Vault** keeps passwords behind one PIN · plus 9 more protections.

Works **alongside Windows Defender**, already built into your computer. Simple pricing, **30-day money-back guarantee**:

1 Device	**$19.99/month**
3 Devices — household	**$29.99/month**
Lifetime — pay once	**$159 once**

Get FrostWatch at antivirus.passtrue.xyz or our new store **virusguardpros.com** · **Free lessons:** antivirus.passtrue.xyz/learn.html · **Questions?** frizzlelogger@gmail.com
Stay curious, stay connected — take your 60 seconds. — The FrostWatch Team