The Grumpy Sysadmin

Scam Warning Signs Quick-Start Checklist

Spot fake warnings, fake support calls, phishing emails, and account takeover tricks before they wreck your day.

Before you trust a warning, call, email, or login page, slow down.

Scammers don't always hack their way in. A lot of the time, they scare you into opening the door. This quick-start checklist helps you spot the obvious red flags before you click a link, install remote access software, approve a login, read out a code, or move money.

> ***Grumpy Rule: Scams work because they create panic. Your job is to slow the situation down before your mouse, phone, or wallet does something stupid on your behalf.***

1. Watch for Fake Computer Warnings

Fake computer warnings usually try to scare you into calling a phone number, installing software, or paying for a problem that may not exist.

Fake Warning Check	Done
A browser page says your computer is infected and tells you to call a number	☐
A loud alarm, voice, or flashing screen is trying to panic you	☐
The warning claims to be Microsoft, Windows, Apple, Google, or your antivirus company	☐
The page says not to shut down or close the browser	☐
The warning appeared inside a web browser instead of the real security app	☐
The message says files, banking, or identity are at risk unless you act now	☐

> ***Grumpy Rule: Real security software doesn't need a browser page screaming at you like a haunted slot machine.***

2. Stop Fake Support Calls Before They Start

A real support person shouldn't need to scare you, control your computer, keep you on the phone, or walk you into your bank account.

Support Call Check	Done
Caller says they are from Microsoft, Amazon, your bank, antivirus company, or internet provider	☐
Caller asks you to install AnyDesk, TeamViewer, UltraViewer, Zoho Assist, RustDesk, or similar software	☐
Caller asks you to read out a login, verification, or MFA code	☐
Caller tells you to open banking, email, shopping, or password manager accounts	☐
Caller says to keep the call secret from family, your bank, or police	☐
Caller tells you to stay on the phone while they fix, refund, or secure something	☐

> ***Grumpy Rule: Anyone telling you to keep a financial emergency secret is probably the emergency.***

3. Treat Urgent Emails and Texts Like Suspicious Packages

Phishing messages usually try to create panic, curiosity, or urgency so you click before you think.

Message Check	Done
Message says your account will be closed, charged, locked, or suspended today	☐
Message claims you bought something expensive that you don't recognize	☐
Message includes an invoice, receipt, refund, shipping notice, or attachment you were not expecting	☐
Sender address looks almost right but not quite	☐
Message asks you to click a link to verify, cancel, refund, or secure an account	☐
The safer move is to open the official app or website yourself instead of clicking the link	☐

Grumpy Rule: A fake email doesn't need to be perfect. It only needs you to be rushed.

---

4. Check Login Pages Before Typing Passwords

Fake login pages can look professional. The logo may be real, the page may look familiar, and the trap may still be waiting.

Login Page Check	Done
You arrived from an email, text, ad, pop-up, or shortened link	☐
The web address looks misspelled, strange, shortened, or unrelated to the real company	☐
The page asks you to sign in again for no clear reason	☐
The page asks for more information than usual	☐
The page asks for a one-time code immediately after your password	☐
You closed the page and went to the official site yourself when something felt wrong	☐

Grumpy Rule: Scammers discovered logos. Truly groundbreaking. Check the address before you hand them the keys.

---

5. Never Share MFA or Verification Codes

One-time codes aren't customer-service trivia. They're often the key that lets someone into your account.

Code / MFA Check	Done
You never approve MFA prompts unless you personally started the login	☐
You never read one-time codes to someone on the phone, in chat, or by email	☐
You treat random MFA prompts as suspicious, not annoying background noise	☐
You know real support should not need your login code to cancel a charge or process a refund	☐
Family members understand not to share codes either	☐
You deny unexpected prompts and change passwords if suspicious activity continues	☐

Grumpy Rule: The code is the key. Stop handing the key to the person currently trying to rob the house.

---

6. Be Careful With Remote Access Software

Remote access tools can be legitimate, but they also give another person control of your computer. Treat that like a big deal, because it is.

Remote Access Check	Done
You contacted the company yourself using a trusted number or official website	☐
You know exactly who is connecting and why	☐
They are not asking you to open banking, email, password manager, or shopping accounts	☐
They are not asking you to disable security software	☐
They are not rushing you or telling you not to talk to anyone else	☐
Remote access software you do not use has been removed	☐

Grumpy Rule: If a stranger on the phone wants remote access to your PC, the correct technical response is absolutely not.

7. Money Requests Are the Giant Red Flag

Scammers love payment methods that are fast, hard to reverse, or embarrassing enough that people hesitate to ask for help.

Money Scam Check	Done
Someone asks for gift cards, cryptocurrency, wire transfers, or instant payments	☐
Someone says to move money to a safe account	☐
Someone asks for a test transaction or refund verification payment	☐
Someone wants payment to fix a warning that appeared on your screen	☐
Someone tells you to lie to the bank about why you are moving money	☐
Someone insists you must act immediately before asking anyone else	☐

Grumpy Rule: Microsoft doesn't want Apple gift cards. Your bank doesn't need Bitcoin. And the IRS isn't calling because they misplaced their Steam wallet.

Final "Do Not Ignore This" Check

Final Scam Check	Done
You do not call phone numbers shown in scary browser warnings	☐
You do not install remote access software because a stranger told you to	☐
You do not share passwords, MFA codes, verification codes, or recovery codes	☐
You do not approve MFA prompts you did not personally request	☐
You verify suspicious emails through the official website or app, not the message link	☐
You stop when someone rushes, scares, or tells you to keep secrets	☐
You ask a trusted person before moving money during a suspicious call or warning	☐
You know how to disconnect and get help if you already interacted with a scammer	☐

If several boxes are unchecked, stop pretending you can "just tell" when something is fake. Scammers count on confidence, panic, and nobody wanting to look foolish.

Grumpy Rule: The pause is the security control. Close the page. Hang up. Verify from somewhere you trust.

After a Scam Scare: Verify Before You Relax

If you clicked, called, typed credentials, approved a prompt, or allowed remote access, don't assume everything is fine just because the warning went away.

After-Scare Check	Done
End the call or chat and stop following the scammer's instructions	☐
Disconnect from the internet if remote access was involved	☐
Change affected passwords from a different trusted device	☐
Review email forwarding rules, recovery settings, and signed-in devices	☐
Check banking, credit card, shopping, and cloud account activity	☐
Remove unknown remote access software	☐
Run a security scan and ask for help before assuming the computer is clean	☐

Grumpy Rule: The browser tab closing doesn't mean the problem is over. That isn't a cleanup plan. That's a disappearance trick.

Want the Full Scam & Phishing Defense Guide?

This free quick-start checklist helps you recognize the obvious warning signs. The full guide goes deeper and walks through the scam patterns, safe response steps, recovery checks, and family rules that are easiest to miss when panic takes over.

Full Guide Will Include	Covered
Fake browser warning and tech-support scam walkthrough	☐
Phishing email, text message, and fake invoice examples	☐
Fake login page and suspicious link review checklist	☐
MFA prompt, verification code, and "read me the code" scam guidance	☐
Remote access software risk and removal checklist	☐
Bank, gift card, crypto, wire transfer, and refund scam warning signs	☐
Emergency response plan after clicking, calling, or allowing access	☐
Family scam-defense conversation guide	☐
Monthly scam-awareness review checklist	☐

Grumpy Rule: The free checklist is enough to make you stop and think. The full guide is for knowing what to do next when something already smells wrong.

Get the full Scam & Phishing Defense Guide
or the future Home Cybersecurity Survival System
https://thegrumpysysadmin.com

Final Word

You don't need to become a cybersecurity expert to avoid most scams. You do need to slow down when something tries to scare you, rush you, isolate you, or make you share codes, install remote access tools, or move money.

Close the page. Hang up the phone. Open the official app or website yourself. Ask someone trusted before continuing.

Scams work fast. Your best defense is refusing to move at scammer speed.

Stay grumpy.