

# Protect Yourself From Scams

*Place this near your computer or phone*

**No matter who they claim to be, I know this is a scam if:**

- They ask me to pay in Bitcoin or buy Gift Cards.
- They ask me to withdraw cash and hand it to a delivery person.
- They want control of my computer or for me to download something.
- They tell me to “not tell anyone else about this”.
- They threaten my arrest if I don’t do something.
- They tell me to move to WhatsApp or Telegram to continue chatting.
- It’s a wrong number message but “I seem nice” and “let’s be friends”
- They ask me to tell them a code (numbers) that they’ll send me.

**Some simple truths:**

- They may know things about you that they’ve found on the internet. That does not make them real!
- Never give your personal information to someone who’s called, texted, or emailed you. You never know who they really are!
- Google or Microsoft will NEVER call you to tell you your account has been stolen or is at risk.
- The “wrong number” text is a scam. They want to steal your money.
- You’re not talking to a famous person on their secret Facebook account.
- That “invoice” for McAfee or Norton you weren’t expecting? Fake.
- The IRS, FBI, or police will NEVER call to inform you your money isn’t safe or that you can just pay for something to avoid trouble.
- Text messages about work from home jobs, packages, or unpaid tolls are fake. Assume any message from someone you don’t know is not real.

If I’m ever in doubt, hang up the phone. Call your trusted family member. Call back the number on your bank card **or on the ACTUAL COMPANY WEBSITE.**

If I’m in doubt, I will call my trusted person: \_\_\_\_\_

I can protect myself from scams from people pretending to be my family (asking for money, claiming they’ve been arrested, are in trouble, are in a foreign country and need help, etc.) by **agreeing with my family on a password.**

My family password is: \_\_\_\_\_