



PERSONAL CYBER SAFETY

PROTECTING YOURSELF IN EVERYDAY DIGITAL LIFE

EMAIL • TEXTS • PHONE CALLS • ONLINE ACCOUNTS

Presented By



**Caldera
Cybersecurity**

Comply • Defend • Protect

ALLIANCE LEAGUE

FEB 13, 2026

Before we start...

WELCOME & GROUND RULES

This is about *you* as an individual

No one will be called on

No trick questions

No technical knowledge required

This is a conversation, not a test.



WHY DO SCAMMERS TARGET PEOPLE LIKE US?

Helpful, trusting people

People who want to do the right thing

People who respond quickly

Scams succeed because of emotions, not technology.

CYBERSECURITY HORROR STORIES

TOP 5 CYBER CRIMES IN 2025



Impostor Scams



- Posing as IRS, Social Security, or big companies
- High Losses for 60+ Victims
- Demands for \$\$\$ or Personal Info

Tech Support Scams



- “Your Computer Has a Virus!”
- Remote Access to Your Device
 - Payments in Gift Cards or Crypto

Romance & Family Scams



- Fake Emergencies & Love Cons
- Emotional Manipulation
- Millions Lost by Seniors

Investment & Crypto Frauds



- “Get Rich Quick” Schemes
- Too-Good-to-Be-True Offers
- Billions in Losses Reported

Online Purchase Scams



- Fake Listings & Shops
- Paying Upfront, Nothing Delivered
- Unsafe Payments (eg. Bank Transfer)

MEET YOUR TWO BRAINS!

Reptilian Brain



- Emotional Responses
- Fear & Impulses
- Fight or Flight



Primal Reaction

Logical Brain



- Critical Thinking
- Reason & Analysis
- Rational Decisions



Thoughtful Response



THE EMOTIONAL **RED** FLAGS



Urgency

“Act now” • “Last warning”



Fear or Authority

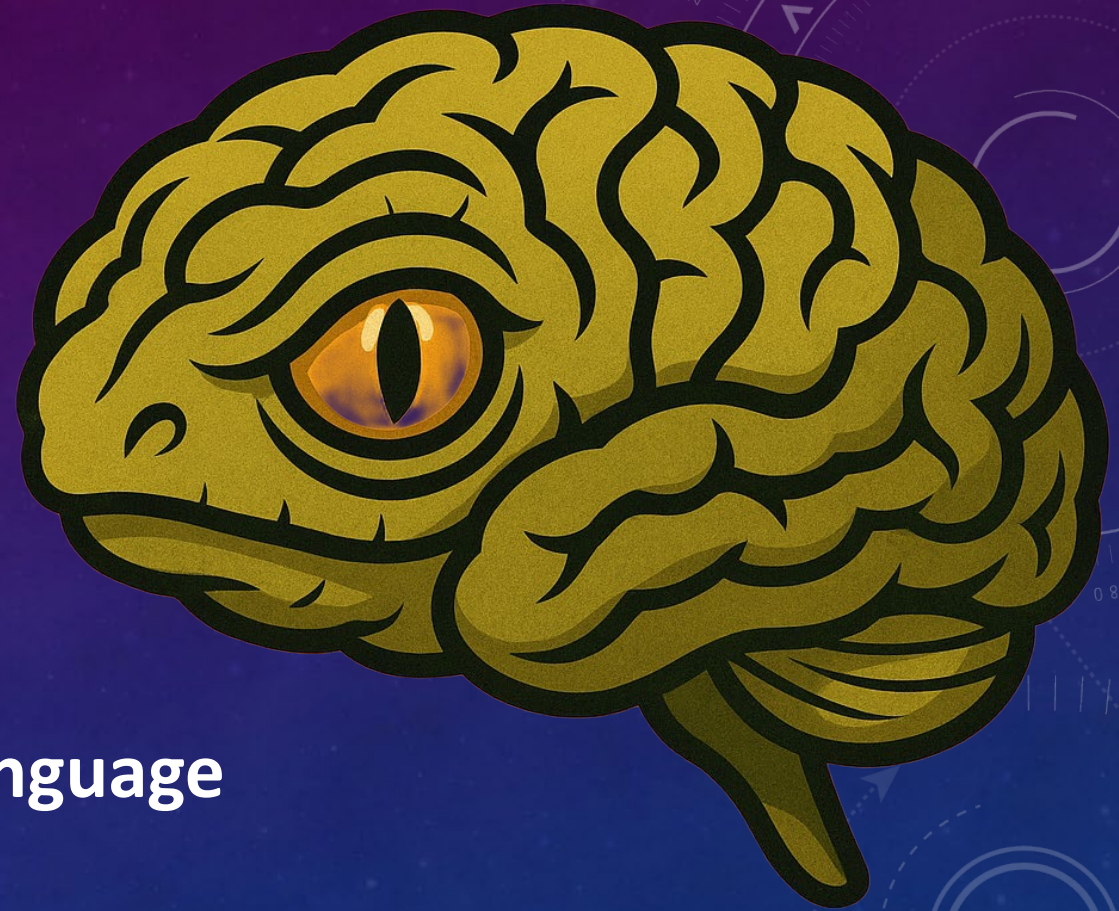
Banks • Government • Tech support



Pressure or Secrecy

“Don’t tell anyone” • “This is confidential”

PHISHING RED FLAGS



- Spoofed Email Addresses
- Generic Greeting
- Sense of Urgency or Threatening Language
- Suspicious Links or Attachments
- Poor Grammer – Not so much now
- Requests for Personal or Financial Info



Collaborate easily in Microsoft Teams

Collaborate easily in Microsoft Teams

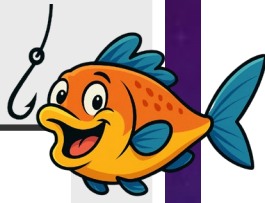
Use Teams to connect and collaborate in one place through meetings, chat, or file sharing. Plus, get work done faster by using Microsoft 365 apps in Teams—keeping everything streamlined.

Open Teams



Phishing Examples

Phishing Examples



LinkedIn

Jeremy Benson has sent you an Inmail message on LinkedIn.



Jeremy Benson
Recruiter at All Hands on Deck Inc.

Hello rmyers@convene-tech.com,

Nice to meet you. I'm Jeremy and I work at All Hands on Deck, a recruiting firm for Fortune 500 companies. I'm reaching out because your qualifications are exactly what we have been looking for with a new role at

Nice to meet you. I'm Jeremy and I work at All Hands on Deck, a recruiting firm for Fortune 500 companies. I'm reaching out because your qualifications are exactly what we have been looking for with a new role at the largest-value media company in the United States. The role includes unlimited PTO, paid healthcare, a \$150,000-\$250,000 range base salary based on experience, and...

[View More](#)



Reply to Message

Jeremy Benson has sent you a new message via LinkedIn

JobOffer.pdf



LinkedIn <noreply@linkedin-requests.com> via convene-tech.com

To: Rick Myers



Thu 2025-05-01 1:55 PM



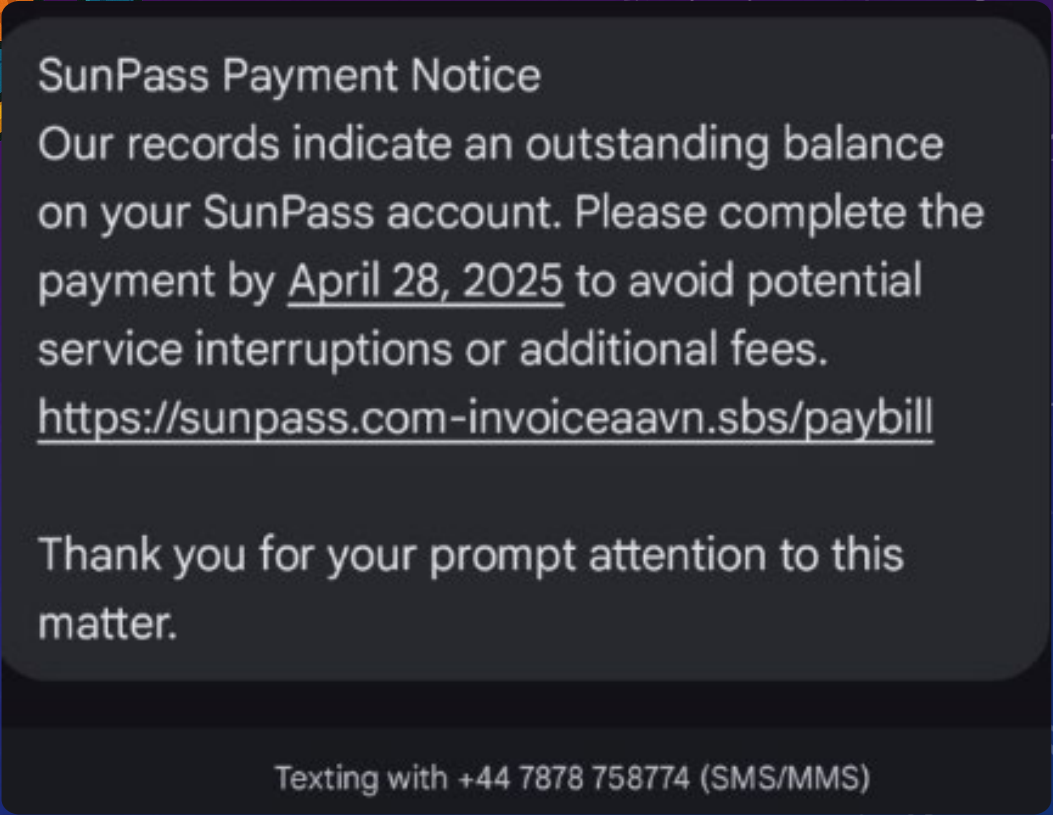
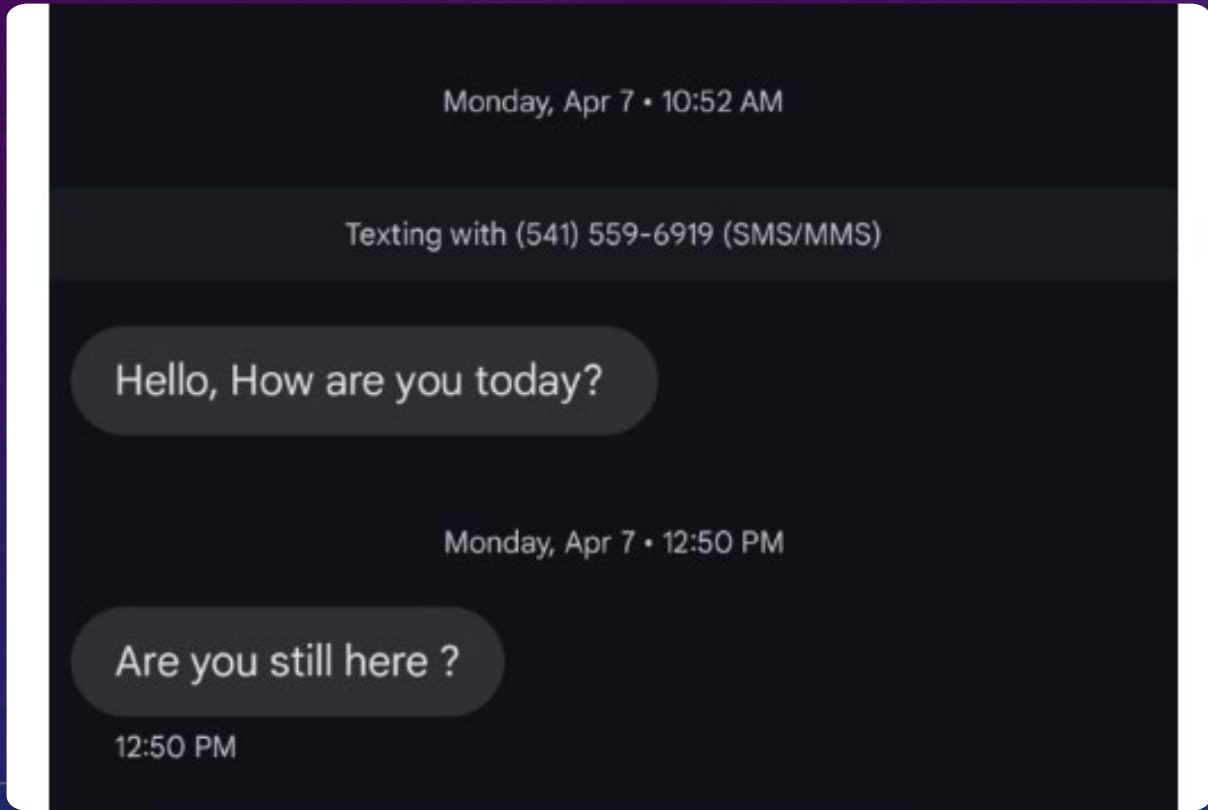
We can't verify that this email came from the sender so it might not be safe to respond to it. [Learn more](#)

Delete email

JobOffer.pdf
107 KB



CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.





SMISHING EXAMPLES

WHAT TO DO IF YOU ENCOUNTER A SCAM CALL



! If You Get a Suspicious Call

 **SLOW DOWN, HANG UP**
Scammers create urgency. **Take a breath**, hang up, and think.

 **DON'T SHARE INFO**
Scammers often ask for: **SSN, Medicare** or bank info, Computer access.
• Real agencies never demand these **urgently**.

 **CALL BACK**
Use a **trusted** number from your card or their **website**.

 **NEVER PAY IN ODD WAYS**
Gov't & big companies **NEVER** ask for **gift cards**, **crypto**, or **wire transfers**.

! If You Get Scammed

1. CALL YOUR BANK ASAP
 Freeze accounts, report fraud.
Bank accounts. **vic**

2. REPORT THE SCAM
 **FTC: 877-382-4357**
Local police

4. TELL A TRUSTED FAMILY MEMBER
 Don't be embarrassed to bring it up.

REMEMBER THIS: 
If they pressure you to act fast, keep it secret, or pay in odd ways
IT'S A SCAM.

- ✓ You **won't** get in trouble for **hanging up**.
- ✓ You **won't** get in trouble for **saying no**.
- ✓ You **won't** get in trouble for **double-checking**.



WHAT NOT TO DO IF YOU'RE SCAMMED OR SOMETHING FEELS SUSPICIOUS

✗ DON'T STAY ON THE PHONE

If something feels off, **HANG UP IMMEDIATELY**. Scammers keep you talking & emotional.

✗ DON'T SEND MORE MONEY

Common trick:

"We can recover your money for a fee."

STOP – that's likely a second scam trying to get more from you.



✗ DON'T CLICK ON LINKS

Suspicious text, pop-up, or email?

DON'T CLICK. Go to the official website using a trusted number.



✗ DON'T TRY TO OUTSMART

Don't argue, **THREATEN**, or try to play along.

They trick you. **JUST HANG UP.**



✗ DON'T TRY TO OUTSMART

Don't argue, **THREATEN**, or try to play along. They trick you.



✗ DON'T FEEL EMBARRASSED

Silence protects the scammer. **TELL** a trusted family member, your bank, authorities.



If it feels urgent, secret, or **unusual**—**pause**.

✓ They don't stay on the phone ✓ They don't send more money ✓ They don't feel embarrassed to share

7 Seconds to Security!

Start the clock and see if the email...

Take a moment to check for **these red flags** before you click on anything suspicious.



- ✔ Contains threatening language designed to create a sense of urgency
- ✔ Contains a request for you to act.
- ✔ Contains a generic greeting.
- ✔ Was unexpected.
- ✔ Contains spelling, grammar, or diction errors.
- ✔ Contains suspicious attachments or links.

When you get an email, the clock is ticking so **take 7 Seconds to be Secure!**

ONE
SIMPLE
HABIT
THAT
WORKS

More Resources



WHERE TO REPORT SCAMS & GET HELP

Extra resources if you need to report scams, fraud, or cybercrime.



REPORT SCAMS & FRAUD

- **Federal Trade Commission (FTC)**
ReportFraud.ftc.gov Report scams, identity theft, and fraud.
Also offers prevention education.



- **FBI Internet Crime Complaint Center (IC3)**
IC3.gov Report online scams, phishing, wire fraud, and cybercrime.



- **USA.gov Scam Reporting Guide**
USA.gov/scams-and-fraud Helps people find the right agency to report specific scams.



- **SUPPORT FOR OLDER ADULTS**
- **National Elder Fraud Hotline (U.S. DOJ)**
1-833-FRAUD-11 (1-833-372-8311) Live assistance for adults 60+.



- **AARP Fraud Watch Network** Education, scam alerts, and a fraud
aarp.org/fraudwatchnetwork



ABOUT MONEY OR ACCOUNTS

- **Your Bank or Credit Union**
Call the number on the back of your card immediately.
- **IdentityTheft.gov (FTC)**
Step-by-step recovery plan if personal information was stolen.
- **Equifax / Experian / TransUnion**
Request a free credit freeze or fraud alert.



IF YOU FEEL in IMMEDIATE DANGER

Call 911 or your local law enforcement.

Reporting helps protect others. You are not alone — and you are not to blame.



Phish-Proof Founders Mission Statement

At Phish-Proof Founders, we believe cybersecurity knowledge should be accessible to all. Small businesses struggle with the high costs of cybersecurity tools and consulting.

Our mission is to empower local business owners and nonprofit leaders with practical cybersecurity insights and resources.

Together, we create a resilient community, equipped to protect what matters most. No jargon, no pressure—just real-world security solutions for everyone.

Continue learning :




<https://www.meetup.com/phish-proof-founders-abq>

A Quick Summary



THANK YOU!

For taking the time to make yourself more secure.

-  You are taking important steps to stay safe.
-  You know how to slow down and spot a scam.
-  You're protecting yourself, your family, and your community from online threats.

Keep asking questions, stay alert, and remember—
pause, and trust your instincts.



Tech *for* Humans Newsletter

Rick Myers, CISSP

Email: rmyers@calderacyber.com

Website: calderacyber.com



**Caldera
Cybersecurity**

Comply • Defend • Protect



Sign up for our FREE newsletter with helpful news and tips to stay safe and secure. **No Sales and No Jargon!**