



RGE Tech Tips from the Field – Client Edition

Topic: Chip's Weekly Cheat Sheet: 3 Signs an Email is a Scam

Chip's Weekly Cheat Sheet: January 12 3 Signs an Email is a Scam

1. The "Panic" Play

The Sign: The email uses urgent, scary language like "Your account will be deleted in 2 hours!" or "Suspicious activity detected—ACT NOW!" **Why it's a scam:** Scammers want you to stop thinking and start clicking. Legitimate companies (like your bank or Amazon) will almost never give you a "ticking clock" ultimatum.

Chip's Tip: *Take a breath. If it feels like an emergency, it's probably a trap.*

2. The "Almost Right" Address

The Sign: The name on the email says "Netflix Support," but the actual email address is something messy like netflix-help@gmail.com or support@123-service.net. **Why it's a scam:** Large companies have their own professional domains (like @netflix.com). If the part after the "@" symbol looks like gibberish or a personal Gmail account, hit delete.

Chip's Tip: *Hover your mouse over the sender's name to reveal the real address beneath!*

3. The "Mystery Link" Request

The Sign: The email asks you to click a button or link to "Verify your info" or "Claim a prize," but you weren't expecting to hear from them. **Why it's a scam:** These links often lead to fake websites designed to steal your password.

Chip's Tip: *Don't click! Instead, go to the company's official website manually in your browser (e.g., typing www.amazon.com) to check your account status.*