

2.2 Scam and Social Engineering Defense

Core Concepts: Protect Yourself, Protect Your Data

Humans are the weakest link in security. Even perfect technical security fails if you're tricked into handing over credentials or sending money. The good news is most scams use the same playbook, so learn to recognize the patterns.

2.2.1 Understanding Social Engineering

Social engineering is the art of manipulating people into giving up confidential information or taking actions that compromise security. Attackers exploit human psychology, our trust, fear, curiosity, and desire to be helpful, rather than technical vulnerabilities.

Common tactics attackers use:

- Urgency: "Act now or your account will be closed!"
- Authority: Impersonating your bank, the IRS, or your boss
- Fear: "Your computer is infected!" or "You owe taxes!"
- Greed: "You've won a prize!" or "Make money fast!"
- Curiosity: "See who viewed your profile" or "This video is about you"
- Helpfulness: "Can you do me a quick favor?"

Your defense: Slow down. Verify. Be skeptical. Trust your gut; if something feels off, it probably is.

2.2.2 The Basics

- Recognize phishing emails and texts
- Check links before clicking
- Never open unexpected attachments

- Verify unexpected requests through another channel
- Watch for caller ID spoofing
- Recognize gift card and wire transfer scams
- Spotting for tech support scams
- Watch for impersonation on social media

Recognize Phishing Emails and Texts

Phishing is a fake message designed to trick you into clicking a link, opening an attachment, or sharing sensitive information. Here's how to spot them:

- Generic greetings: "Dear Customer" instead of your name
- Urgent language: "Act immediately" or "Within 24 hours"; they want you to act before you have time to think about whether or not it is a scam
- Threats: "Your account will be suspended" or "You'll be charged"
- Too good to be true: Free money, prizes you didn't enter, inheritance from unknown relatives
- Spelling and grammar errors: Professional companies proofread their communications
- Mismatched sender addresses: The display name says "PayPal" but the email is from "paypa1-secure@gmail.com"
- Suspicious attachments: Especially .exe, .zip, or files you weren't expecting
- Requests for personal information: Real companies never ask for passwords, SSN, account numbers, or any other personal information via email
- Unexpected delivery notifications "there was a problem with your package" when you didn't order anything

Check Links Before Clicking

Before clicking any link in an email or text message:

On desktop:

- Hover your mouse over the link (don't click!) and look at the URL that appears
- Does it match what you expect? If an email claims to be from Amazon, the link should go to amazon.com, not amaz0n-secure.net
- Watch for look-alike domains: paypal.com vs. paypa1.com (that's a number one), or apple.com vs. app1e.com

On mobile:

- Press and hold the link to preview where it goes
- When in doubt, don't click - go directly to the company's website through your browser or app instead

A quick note about QR codes, since those are really just links. Legitimate examples of these can be found on company advertisements, restaurant menus, business cards, etc. Scammers also sometimes use QR codes to bypass email security filters and trick you into visiting malicious sites. This is called “quishing.”

How it works:

- You receive an email with a QR code claiming to be from your bank, IT department, or a package delivery service
- You scan the code with your phone
- It takes you to a fake login page that steals your credentials

Protection:

- Be skeptical of unexpected QR codes in emails
- Before scanning, ask yourself if you were expecting this
- After scanning, check the URL before entering any information
- When possible, access services directly rather than through QR codes in emails

Never Open Unexpected Attachments

Attachments are a common way to deliver malware. Follow these rules:

- Don't open attachments from unknown senders, period
- If you get an unexpected attachment from someone you know, verify with them through a different channel (call them) before opening
- Be especially wary of: .exe, .zip, .scr, .com, .bat, .js files
- Even seemingly safe files like PDFs and Word documents can contain malware, verify before opening

Verify Unexpected Requests

If you receive an unexpected request whether by email, text, phone, or social media, pause and verify:

- Don't use contact information from the suspicious message
- Look up the organization's official phone number or website independently
- Call or message through a verified channel
- Ask: "Did you send me a message about [topic]?"

Example: Your bank sends a text saying your account is locked. Don't click the link in the text. Instead, call the number on the back of your credit or debit card.

Watch for Caller ID Spoofing

Scammers can make their phone number appear as any number they want on your caller ID, including your bank, the IRS, or even your own number.

Protection:

- Don't trust caller ID alone
- If someone claims to be from your bank or a government agency, get their name, the agency they claim to represent, and whatever topic identifier they can provide related to why you called, (ticket number, case number, incident number, etc)
- Then hang up and call back using an official number (absolutely not one they offer to provide)
- Real organizations won't mind you verifying their identity this way
- Be extra suspicious of robocalls or calls demanding immediate payment

Recognize Gift Card and Wire Transfer Scams

No legitimate organization will ever ask you to pay with gift cards or wire transfers. Gift cards are untraceable, and both gift cards and wire transfers are non-refundable. That's why scammers love them. If someone asks for payment this way, it's a scam, **no exceptions!**

Spotting Tech Support Scams

Tech support scams come in many forms. Pop-up warnings with messages like "Your computer is infected! Call this number immediately!" These are fake. Real security warnings don't give you a number to call. **Never call this number!** Close the browser tab and don't go back. If it came from a site you think is legitimate, like your bank, notify them immediately.

Cold calls are another type of scam. Someone claiming to be from Microsoft, Apple, your internet provider, or even from the FBI or local police, stating that they have detected a problem with your computer. They usually ask for remote access to "fix" the problem. What they want is access to your computer to install malware, steal files, or extort money for fake "repairs." Never give remote access to unsolicited callers. Real tech companies don't call you unsolicited about computer problems; hang up immediately. Block the number if they keep calling back.

Watch for Impersonation on Social Media

Scammers create fake profiles impersonating:

- Your friends and family members
- Company customer service accounts
- Celebrities or other influencers

Red flags:

- New account or very few posts
- Small changes in username (JohnSmith vs John_Smith or JohnSmith1)
- Requests for money or personal information
- Messages from "customer service" accounts you didn't contact

Verification: If a friend messages you with an unusual request, call or text them directly (not through the suspicious message) to verify.

Revision #1

Created 2026-07-12 21:22:36 UTC by Chris Landis

Updated 2026-07-12 21:24:21 UTC by Chris Landis