Fraud Prevention Seminar

Pastor Cliff Carey
Sunrise Community Church
Sunday, January 25, 2025

Proverbs 3:21-23 (ESV)

My son, do not lose sight of these – ***keep sound wisdom and discretion***,
and they will be life for your soul and adornment for your neck.
Then you will walk on your way securely, and your foot will not stumble.

Top Ten Reported Types of Fraud

- **Imposter Scams:** Pretending to be government (IRS, Social Security), a known business, or a family member in trouble.
- **Investment Scams:** Promising quick, guaranteed returns on crypto, stocks, or AI-driven platforms.
- **Online Shopping Scams:** Fake websites, bad products, or non-delivery.
- **Business & Job Opportunity Scams:** "Task scams," work-from-home offers that require upfront payment.
- **Internet & Mobile Service Scams:** Fake tech support pop-ups or issues with service.
- **Debt & Credit Scams:** False promises of debt relief or credit repair.
- **Romance Scams:** Building relationships to get money.
- **Fake Package/Delivery Texts:** Alerts about delivery issues to get you to click links.
- **Fake Toll/Jury Duty Notices:** Texts demanding immediate payment for a supposed fee or missed obligation.
- **AI-Powered Scams:** Deepfakes, voice cloning to impersonate loved ones.

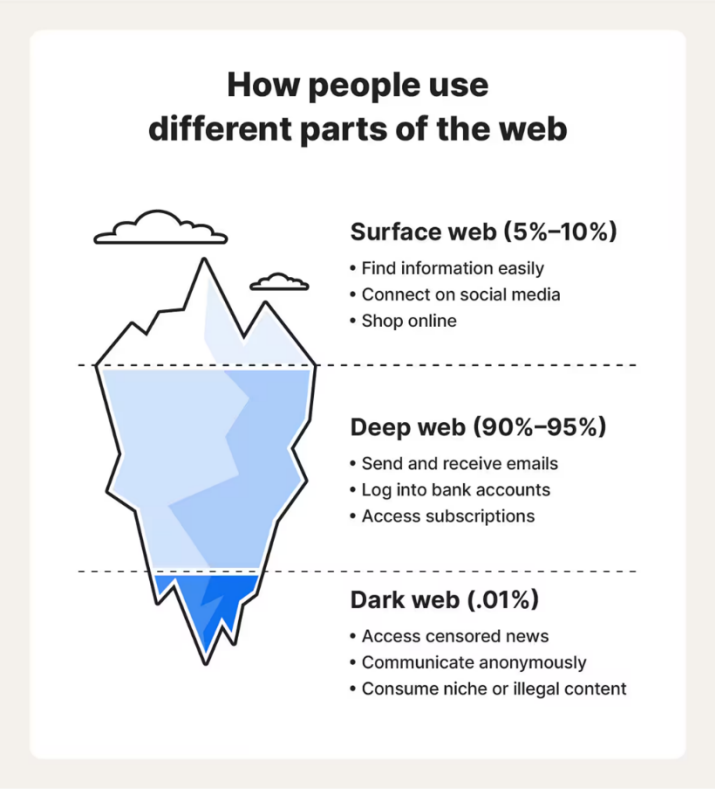
Where It Starts

CALLS EMAILS TEXTS SOCIAL MEDIA LETTERS

How do the scammers get my information?

Scammers get your information through data breaches, tricking you with phishing (fake emails/texts/calls) to reveal it, and by piecing together publicly available data from social media, public records, and even by going through your trash or mail; they also use techniques like skimmers on card readers and buy stolen data from the dark web.

The Dark Web



Quotes from Scammers

I'm with Microsoft. There is a problem with your computer.

We're rolling the trucks. Your power is going to be turned off.

Grandma? – I'm in jail

I'm calling from your doctor's office. Are you experiencing any knee pain?

Everything is okay, but your brother has been in an accident.

Spotting a Scam

Impersonation

Scammers pretend to be from an agency, organization or company you know to gain your trust.

Urgency

Scammers say there is a problem or money due – then pressure you to act immediately.

Specific Payment Method

Scammers will say that you must pay in a specific way. (Cash, Zelle, Venmo, Crypto, Gift Cards, Bank Acct #, Wire, Money Orders)

Spoofing

Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source.

Phishing

The fraudulent practice of sending emails or other messages purporting to be from reputable companies or individuals, to convince individuals to reveal personal information or make financial transactions.

When You Receive an Email… THINK Before You Click

- Does it look normal or does something not seem right?
- Is it asking you to click a link?
- Does it use odd phraseology?
- Is it written in American English?
- Look for odd formatting or bad graphics

Look at the Email Address

- Do you recognize it?
- Check the From: email address
- Is it accurate for the organization or company?
- Is it from Gmail, iCloud, Yahoo, etc.?
- Is there a mispeling in the adress or subject?

Banking

Working with Social Security

- You will always need a valid form of I.D.
- Social Security or Medicare will rarely ever call
- Does not recognize POA - Representative Payees
- You cannot change Direct Deposit information over the phone
- Create a *MySSA.gov* account through *Login.gov* or *ID.me.gov*

When You Get a Call

- **YOU DON'T HAVE TO ANSWER!!!**
- Do you recognize the number?
- What's the Caller ID?
- Listen for the Delay
- Foreign Accent?

Think About It…

- The government will RARELY call you.
    - IRS, Social Security, Medicare – They will always send letters first.
- Your utilities will NOT be turned off without written notice.
- If it seems too good to be true, it probably is.

Social Media

Types of Social Media Scams

- AI-Powered Scams
- Impersonation & Account Takeovers
- Romance Scams
- Fake Job Offers
- Fake Investments
- Online Purchase & Delivery Scams
- Sextortion

Tips for Social Media

Do a Social Media Checkup

- Is your account public or private?
- What info is visible in your profile?
- Who can see your pictures?
- Who can comment on your posts?

Examine Follow/Friend Requests

- Are you already friends?
- How many followers do they have?
- How well do you know the person?
- Friends in common?

If You Think You've Been Scammed…

- Stop & Block
- Contact Your Bank / Credit Card
- Change Passwords
- Document (time, place, etc.)
- Report the Scam (Police, FTC, FBI, A.G.)
- Freeze Your Credit (Equifax, Experian, TransUnion)

Keep Your Information Secure

WiFi

- Avoid Public WiFi
- Dangerous locations:
    - Airports
    - Hospitals
    - Restaurants/Coffee Shops
    - Hotels
    - Disneyland
- Don't make financial transactions
- Use a VPN if possible

<u>Be Secure</u>

- Two-Factor Authentication
- Strong Passwords
- Logout and Close
- For Online Transactions:
    - Separate Bank Account
    - Separate Email Address

RESOURCES

Credit Bureaus

Bureau	Website	Phone #
Equifax	equifax.com	(888) 298-0045
Transunion	transunion.com	(800) 916-8800
Experian	experian.com	(888) 397-3742

Investment Companies

Company	Website
Schwab	schwab.com/schwabsafe
Edward Jones	edwardjones.com/privacy
Fidelity	fidelity.com/security

Other Resources

Agency / Company	Website
Federal Trade Commission	identitytheft.gov ReportFraud.ftc.gov
FBI Internet Crime Complaint Center	ic3.gov
Social Security Scam Info	ssa.gov/scam
Trustpilot – Online Store Reviews	Trustpilot.com