Change The Way You Think

Learn to say "NO". Learn to not answer the phone or email. Learn how to not engage. You are under no obligation in these modern times to respond to calls, emails or texts from strangers — especially given that so many of them are fraudulent. If a scammer gets through. Get tough: "I don't do business over the phone. Goodbye." Then hang up.

Trust Your Instincts. If something doesn't sound right, run it by someone you trust and take extra time to think about it.

Resist the Urge. Many times when the phone rings, we feel compelled to answer it, regardless if we know the person calling or not. Please understand that you ***do not*** have to answer your phone, regardless of who is calling. Resist the urge to answer, unless you know for certain who is calling you. If it's urgent, they will leave a message or call you back repeatedly. If it isn't urgent or important then you have quite possibly saved yourself a lot of aggravation and annoyance and, more importantly, you reduce the chance of losing your hard-earned money via a scam.

There is not enough room in a 3-fold brochure to list *all* the ways to stay safe from scammers. Stay aware, & stay informed by signing up to receive free email notices from the government at: **ftc.gov/scams**

Avoiding Scams

Keep personal information to yourself
Scammers are professionals at getting people to lower their defenses and divulge personal information, including (but not limited to) account numbers, date of birth, PIN numbers, and more. All are used to steal money and identities.

Call back using genuine phone numbers
If you know the person, call them from a number you have used in the past. If a credit card, use the number listed on the back. If your bank is local, visit them. Just because someone *claims* they are legitimate, doesn't mean they are truthful.

Don't click links in emails or text messages
A link in a text, email or website doesn't necessarily take you to the location the visible text claims. Sometimes it's legitimate, other times it will take you to a virus-laden location. Be aware of any unsolicited text or email urging you to click a link.

Think about requested payment method
Credit cards and banks offer some protection, but once your money leaves your account in the form of a cashier's check, it's gone for good. The IRS will ***never*** demand you get Walmart gift cards!

Avoid paying any money upfront
Some legitimate businesses and individuals might have valid reasons for requesting deposits or "up front" money, but be aware of unsolicited phone calls requesting payment for products or services that you haven't requested.

Conduct online searches
There are thousands of listings of various scams available with a simple search. Most likely the urgent email, or text, or phone call you received demanding you "act now!" have a scam history.

Tug the Plug at the ATM/Gas Pump
Scammers use skimmers to steal your credit/debit card information. It's placed over legitimate credit card readers & copies your card information. Tug on it to see it's easily removed.

Mentalist Doug Anderson presents…

Avoid Scams Knowledge (ASK)

"Scams are rampant, with criminals stealing a reported $8.8 billion from Americans in 2022. There are ways to protect yourself, including staying up on the latest schemes."

"Knowledge is Power"

Stop at the Mailbox

Informed Delivery (free service from the USPS) emails photos of letter-size mail expected to be delivered to you that day or shortly after. It's a great way to be sure that nothing is stolen from your mailbox. Pick up mail as quickly as possible after it's delivered, and always take your outgoing mail directly to the post office. A hot fraud now is scammers stealing checks from mailboxes, erasing the ink and using them to steal from bank accounts. Thieves have now acquired Master Keys to the blue USPS mailboxes so a safer idea is to take your outgoing mail inside your local post office. Consider the many benefits of using a Post Office Box.

Stop Scammers at Your Front Door

Install a video camera; they are increasingly less expensive, and they're easy to install. If you don't recognize a visitor, don't answer. If you find yourself being pressured to buy or donate, have a refusal script ready (consider taping it near the door) that says, "I do not do business at my door. Please leave me something to review. If I'm interested, I'll call you." Be wary of people posing as utility workers who show up unannounced. Don't allow anyone into your house without an appointment.

Stop Garbage Theft

Shred any papers that contain private information (financial statements, bills, shipping receipts) before putting them out for pickup to avoid identity theft. The prices of a good cross-cut shredder have dropped, but if you don't want to get one (or can't afford it), many communities have shredding events or permanent drop-off sites. Get in the habit of dropping off your accumulated documents often.

Stop Credit Card Skimming

In card skimming, criminals put a credit card reader over a legitimate card reader at a store or gas station. When you are paying at a gas station or other point-of-sale location, inspect the device for loose or broken or scratched machinery to make sure someone hasn't tampered with it. If you are unsure, notify the cashier and pay using an alternative method. Tug the Plug.

Monitor Your Credit Report

Routinely check yours (many credit card companies provide for free; if not, visit AnnualCreditReport.com or call the toll-free number 877-322-8228). Watch for unusual activity; if you see any, report it immediately to the appropriate financial institution. Then freeze your credit report. This prevents scammers from opening new credit cards or making big purchases in your name. You can "unfreeze" it as needed for legitimate transactions. You can also visit IdentityTheft.gov for more information.

Monitor & Protect Your Financial Accounts

Create online accounts with each of your financial institutions. Come up with a unique password for each. Then get in the habit of reviewing the transaction lists on a weekly or biweekly basis. Be sure you can account for every listed transaction. Spot something odd or incorrect? Immediately report it.

Safeguard Your Wallet

Remove cards and information you don't need to carry (such as your Social Security or Medicare card). Make copies of the remaining cards (front and back) and store in a safe place. Audit your wallet and purse frequently. Take out any unnecessary items that collect and could compromise your personal information if lost or that would be a hassle to replace.

Safeguard Your Smartphone

If you have a newer model, turn on biometric identification. This will help prevent a thief from logging in to your phone. Send calls from unknown numbers to voicemail (you can enable this in the phone's settings). Make sure your voicemail is set up and not full, so you can receive legitimate messages. Scammers are sending bogus texts, posing as companies you routinely deal with, so never respond to an unsolicited text; if you think it's valid, call the organization or go online.

Safeguard Your Computer

Turn on two-factor authentication for all secure websites you frequent, such as financial institutions or utility companies (find out how via each site's online security center). Then only someone logged in to your phone can receive the code to access those accounts. Consider subscribing to an antivirus software service. Some security experts say browsers and device manufacturers have more built-in malware protection than years ago, such as Microsoft Defender, which comes installed on Windows 10 and 11 machines. Some paid subscriptions also include ad tracker blocking, cloud backups of your machines and identity theft monitoring.

Safeguard Your Email Accounts

Actively designate unsolicited and unwanted email that shows up in your inbox as spam, so future emails from that site get blocked. Do not open file attachments in emails from businesses or people you don't trust completely. Malware is often planted via email attachments. Set your profile so that only your friends can see your Facebook page. To do that, click the downward arrow button in the upper-right corner of your Facebook page, then click on Settings & Privacy and Privacy Checkup. This easy-to-use wizard will guide you through the settings. And never accept friend requests from people you don't know or respond to random messages from strangers. But also note that imposter scams, where someone pretends to be your friend, are rampant on social media.

Verify Online Stores

To avoid shopping scams, when typing in a URL, double- and triple-check the spelling to ensure you are on the correct page. Scammers often create a URL with one letter off from the authentic one in hopes you won't catch it. Remove your credit card number and information from restaurant delivery and retail store sites. Pay using an e-payment service that keeps credit card info on a highly secure site.