AARP Current Scams

Tech support

This just might be the biggest consumer scam in the U.S. right now. According to Microsoft, in 2015 an estimated 3.3 million people — many of them seniors — were victimized by a tech-support con, at a total cost of $1.5 billion. That's one American duped out of an average $454 nearly every 10 seconds.
Here's how the scam typically unfolds: You get an unsolicited call from someone claiming to be with Microsoft or Windows tech support, who says viruses have been detected on your computer. In order to protect your data, you are told to immediately call up a certain website and follow its instructions. A dummy screen may appear that shows viruses being detected and eliminated, but in reality malware is being installed that allows the scammer to steal your usernames and passwords, hold your data for ransom or even use the webcam to spy on you.
Your Plan Hang up the phone. "Neither Microsoft nor our partners make unsolicited phone calls," says Courtney Gregoire, senior attorney at the Microsoft Digital Crimes Unit. Also, don't click any links in unsolicited emails from "Microsoft" or in pop-up ads promising to speed up your computer. "And if you haven't downloaded Windows 10 or the latest version of OS X, do it," says William Woodworth with Best Buy's Geek Squad. "Each update is free and has lots of new security built in." Ditto for any other software programs you're running.

Silent call

Has this been happening to you? The phone rings, you pick it up, say "hello," but there's no one on the other line. It's a new type of robocall — an automated computer system making tens of thousands of calls to "build a list of humans to target for theft," according to the Financial Fraud Research Center. It's the first step in opening you up to many of the phone-based scams discussed in this article.
Your Plan If you haven't already done so, ask your phone company to put caller ID on your landline. Then simply screen your calls, and don't pick up if the number is unfamiliar.

IRS impostor

This con is still going strong. "It's our number one reported fraud right now," says Amy Nofziger with AARP Foundation and Fraud Watch Network, "and I think it'll get more sophisticated." Here's how it works: Someone claiming to be from the IRS either phones or leaves a voice message saying you owe back taxes and threatening that, unless funds are wired immediately, legal action will be taken or you'll be arrested. (Or they may say you have a refund waiting but need to verify personal info before sending.)
"They're very convincing," says Nofziger, "and they often use aggressive language." And let's be honest, beyond the intimidation factor, who doesn't feel guilty about fudging something on a 1040 at some point? Plus, scammers are getting more devious: Sometimes "IRS" shows up on caller ID, the con artists supply their "badge numbers" and they know the last four digits of your Social Security number.
Your Plan Do not return a call from someone claiming to be with the IRS. The real IRS opens communications with a taxpayer only via the U.S. Postal Service. If you're ever in doubt about an IRS matter, call the agency directly at 800-829-1040. Sometimes for kicks Nofziger actually calls the IRS impostors back. "They usually pick up on the first ring," she says. "The IRS doesn't usually have the staffing capacity to pick up on the first ring, but the scammers do."

Cancer rip-off

Last spring, in one of the biggest busts of its kind, the Federal Trade Commission (FTC) charged four national cancer charities (the Cancer Fund of America, Cancer Support Services, the Children's Cancer Fund of America and the Breast Cancer Society) with defrauding consumers of $187 million. At the other end of the cancer-scam spectrum, last August a reigning beauty queen (Miss Pennsylvania U.S. International) was arrested after allegedly claiming she had cancer and swindling tens of thousands of dollars from sympathetic supporters. She even shaved her head and staged "Bingo for Brandi" fundraisers, authorities say.

Your Plan Before contributing to any charity, check out its rating on charitynavigator.org. Instead of giving cash to door-to-door solicitors or your credit card number to callers, ask for more information about the charity (brochures, websites) so you can investigate the cause first. Also be wary of popular online giving sites such as gofundme.com. The best thing you can do to protect yourself from this or any scam is to be skeptical, says Frank W. Abagnale, a former con artist who became a long time FBI consultant on scams and is now AARP's Fraud Watch Network Ambassador. Ask questions. Trust your gut.

Chip card

Banks and credit card companies are in the process of issuing customers new "chip" cards. "The data is protected in an integrated circuit [rather than a magnetic strip], and there's a dynamic code that resets after each use," explains Vernon Marshall, senior vice president and functional risk officer for American Express. "They're almost impossible to counterfeit."

But here's the scam. The FTC is warning that con artists are impersonating card issuers and sending emails requesting personal and financial information, or asking that you click on a malware-laced link before being issued a new card. The fraudsters are sending emails — purporting to be from companies such as American Express — that convincingly use the company's logo and color scheme, and even have footer links such as "View Our Privacy Policy" and "Contact Us."

Your Plan No credit card company will email or call you to verify personal info it already has on file before mailing a new card. (At most, you'll get a letter in the mail saying it will arrive soon.) If you're ever unsure, simply call the number on the back of your card (not the one supplied by the email) and ask the company if it's trying to contact you.

Faith-based dating

Reports are surfacing in AARP's Fraud Watch Network about a new ripple in online dating deceptions. Traditionally, these scams have involved con artists stealing the hearts of unsuspecting singles (many of them seniors) and then using various ploys to steal money. But now scammers are targeting faith-based sites like BigChurch, ChristianMingle, JDate and others."People are more likely to fall for scams on sites like these because they can't believe somebody of their own faith is a con artist," explains Jane Margesson of AARP's Maine office.

Your Plan Before getting involved with anyone online, use Google or Spokeo.com to research the person, and even view his or her address on Google Maps. Finding "no results" is a red flag. Do a Google Image search for a profile picture. Keep in mind that people who are legitimately looking for love won't ask for money (unless they're your kids).

Medical identity theft

When most people hear identity theft, they think of someone stealing their credit card info and buying a big-screen. But you can't legally be held liable for fraudulent purchases like that. It's different, however, with medical identity theft. "You can be required to cover the cost for health care services you never received," Abagnale says. These can include tests, prescription drugs and even operations.

Your Plan Never surrender Social Security, Medicare or health insurance numbers to anyone you don't know and trust. Be particularly wary of free health checks offered at shopping malls, fitness clubs and retirement

homes (so-called rolling labs). If they ask to photocopy your cards or ask you to sign a blank insurance claim form, don't do it, Nofziger says. (After all, it's supposed to be free.) It's also vital to review all statements from your insurance provider. If there are any charges you don't understand, call immediately. And when shopping online for prescription drugs or other health-related items, remember that if a price seems too good to be true, it probably is.

Counterfeit apps

In September, news broke that Apple's normally secure app store had been compromised. Some developers had evidently used a fake version of Xcode (hence dubbed Xcode Ghost) to build their apps, not knowing it contained malware designed to steal passwords and do other devious things.
Your Plan Apple says it has purged its store of these malicious apps. But that doesn't mean it couldn't happen again. Geek Squad's Woodworth recommends always reading an app's reviews before downloading and choosing proven, popular ones. Be aware, too, that you can limit an app's access to your location by adjusting your device's privacy settings, thus reducing the chance of being spied on.

Grieving widow

The key to every scammer's success is being able to put you under "emotional ether." "It's when you're not thinking cognitively, but emotionally," Nofziger says. At no time are we more vulnerable than after the loss of a loved one, and con artists know that. A man was arrested last August for allegedly bilking an 89-year-old Wisconsin widow out of nearly $4,500. Police say he scanned obituaries for prey, then pretended to be a bank official to trick them out of money. He may have been working the scam across the country for decades.
Your Plan Ask a trusted family member to temporarily handle your financial responsibilities while you are grieving. Have that person follow up on any suspicious phone calls or emails. And be aware that while you are grieving, you may be more vulnerable to fraud tactics that play on your emotions.
Gift voucher
This rip-off involves getting an unsolicited email from McDonald's, Subway or another popular restaurant or retailer offering a free gift card if you click a link to activate it. The pitch looks legit, but it's a phishing scam, meaning the perpetrator is either trying to install malware on your computer or gather personal info by having you complete an online questionnaire.
Your Plan Repeat after us: Never click a link in an unsolicited email or divulge personal info, no matter how enticing the offer. Do a Google search (such as "McDonald's gift card scam") and see if any warnings come up. In most cases, they will.

Taking Advantage of Dementia

Scam: Fake charities
Broadcast journalist Richard Lui's father, Stephen Lui, who suffers from dementia, became a victim of scam artists who bombarded him with hundreds of phone calls from fake charities and lotteries.
The 82-year-old former Presbyterian youth pastor and retired social worker for the city of San Francisco has always been outgoing and trusting. "As dementia has taken more hold, it has exposed more trust," says Richard, a news anchor with MSNBC.
Thieves made small, automatic withdrawals from Stephen's personal checking account for about a year, stealing around $2,000 in withdrawals that the bank couldn't trace.