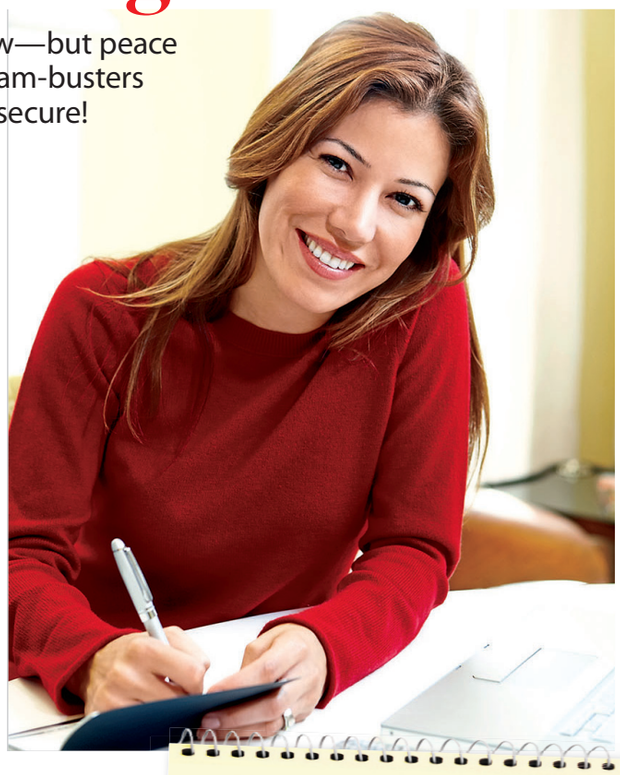
"Help! I'm afraid of being scammed!"

The good news is that your chances of getting scammed are low—but peace of mind is priceless. Which is why we asked the country's top scam-busters to share their easiest, best tips for keeping you and your family secure!



1 Protect yourself offline!

Sidestep scams!

One of the biggest scams to guard against this year is the so-called "grandparents" scam, our experts agree. The scammer will call grandparents pretending to be their grandchild in the hospital or in jail asking for money. "They'll often say, 'Don't tell Mom and Dad'," notes security expert Rob Douglas. "And if the grandparent says, 'This doesn't sound like Johnny,' the scammer will claim it's a bad connection: 'I'm calling from Mexico.' " The simple way to be sure it's a loved one? Ask for their number so you can call them back, then verify that number with a quick Internet search—999 times out of 1,000, once you say you'll call them back, they'll hang up." Another common scam? "The IRS scam—in which a caller claims you have an overdue payment—is doing a lot of damage right now," Douglas says. "The IRS will never threaten you, and they won't call or e-mail you. The bottom line: Be skeptical. Ask for *their* number, then verify the information when you hang up."

Tip! Don't rely on caller ID. "Caller ID can be 'spoofed,' which means scammers can plug in whatever number they want," says identity theft expert Robert Siciliano. "So, if, say, your bank calls asking you for information, just look up their main number, and call back yourself."

Watch for red flags!

Two tools every scammer employs are timeliness and pushiness, says Douglas. "For example, if someone shows up on your doorstep trying to convince you that, say, you need a new roof or your driveway needs paving *immediately*, or they're very pushy about being paid *right* away, those are all red flags."

2 Be safe online!

Use a pass *phrase!*

Remembering a bunch of passwords is hard, if not impossible. The solution? An easy-to-recall yet hack-proof pass *phrase* that you simply alter slightly for each account, says scam expert Steven Weisman. "Simply pick a core phrase, say, 'IDon'tLike Passwords', using both capital and lowercase letters," he advises. "Then change the phrase slightly for each account. For example, for your Amazon account, you might tack on a couple of exclamation points and the letters 'ama' to help you remember it's for Amazon, so it becomes 'IDon'tLikePasswords!!ama'. An easily customizable core pass phrase is very secure."

Fudge security answers!

To help keep your information safe, lots of online accounts will ask you to provide answers to personal security questions, such as your mother's maiden name or the name of your first pet. The easiest way to keep that info extra safe is simply to fib, reveals Douglas. "Though it's unlikely, a scammer could go on to, say, Facebook or another social media site and find the answers to questions like 'What is the name of your favorite band?' " he explains, "So, to be on the safe side, don't be completely honest when answering."

Blind prying eyes!

Avoid using public Wi-Fi to access sensitive accounts, urges Douglas. "Like the online version of looking over your shoulder, scammers can use Wi-Fi to spy on people's accounts at places like coffeehouses and hotels," he says. "Airports are particularly vulnerable, so just wait until you get home to shop online or, say, open an e-mail with your credit card statement in it."

Go ad-free!

"I would say 99% of people don't know this, but simply not clicking ads is an easy way to keep your information secure online," notes Douglas. That's because the bad guys can "inject" the *legitimate* ads you see on your favorite sites with software capable of uploading a virus to your computer!

—Kristina Mastrocola

More ways to stay safe!

Ditch debit! Use your credit card instead of your debit card for retail purchases because laws protecting credit cards are strong.

Don't click! "Never click links you're e-mailed," says Weisman. "I was recently e-mailed a bill for an astronomical amount, and it said 'click if you have a question.' I didn't click, and sure enough it was a scam. Right there on the real company's website, it read: 'We did not send that invoice!' "

Our expert panel

Rob Douglas is a nationally recognized identity theft expert and information security consultant. He specializes in the investigation and prevention of identity theft. Learn more at IdentityTheft.info.

Identity theft and personal security expert **Robert Siciliano** is the author of *99 Things You Wish You Knew Before Your Identity Was Stolen*. Learn more at BestIDTheftCompanys.com.

Steve Weisman—author of *The Truth About Avoiding Scams*—is a professor at Bentley University and one of the country's leading experts on scams and identity theft. Find out more at Scamicide.com.

Photos: shutterstock.com; Mark Leibowitz/Masterfile; iStockvectors/Getty Images; Vetta/Getty Images; Roger Good.