NEW EDITION

FRIENDS DON'T LET FRIENDS GET SCAMMED

How to Spot Fraud and Avoid Becoming a Victim

BROUGHT TO YOU BY
THE EASY PREY PODCAST

EASYPREY

Scammers Aren't Going Away. In Fact, They're Headed Your Way.

Scammers are relentless. They roll out hundreds of different tricks and schemes to find easy prey, and those who are unlucky enough to fall into one of their traps become their victims.

The goal of this colorful and easy-to-read ebook, brought to you by the Easy Prey podcast, was designed to increase your awareness of scams…and help you avoid them.

In this new edition, we included information on reporting a scam (or a close encounter) to authorities and why that's so important. And while we made this ebook fun and enlightening, the topic is a serious one. So, I encourage you to read it now. And after you do, I want you do one more thing.

Pass it along—because friends don't let friends get scammed.

Chris Parker
Host of the Easy Prey podcast

CONTENTS

Part 1

What Does it Mean to be Easy Prey for a Scam?

Millions of people get scammed every year. It can happen to anyone: young and old, rich and poor, and those who say "it will never happen to me!" Here are 7 everyday life situations where you could become victimized.

IT DOESN'T MATTER HOW INTELLIGENT YOU THINK YOU ARE. FACT IS, UNDER THE RIGHT CIRCUMSTANCES, PRETTY MUCH ANYONE CAN BECOME EASY PREY FOR A SCAM. WORSE YET, IF THAT HAPPENS, YOU COULD LOSE PLENTY OF MONEY BEFORE YOU KNOW WHAT HAPPENED.

What does it mean to be easy prey? Let's start with definitions.

Prey: a person or animal that falls victim to another.

Easy prey: someone who is easy (or easier) to deceive or be taken advantage of.

In April of 2020, I launched the Easy Prey podcast, which covers a wide range of topics all related to scams and fraud. In my first podcast, I talked about why I decided to launch the podcast.

Still, I didn't quite explain what it meant to be easy prey for a scam.

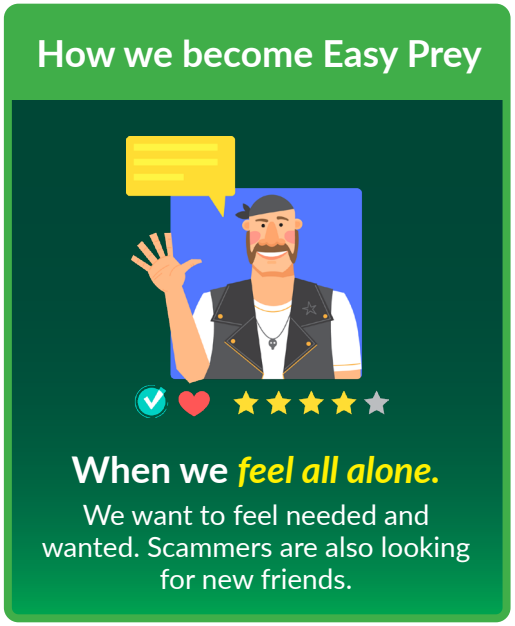
After all, the term "easy prey" is right in the title of my podcast. So, let me explain.

First off, there's one thing everyone should know when it comes to scams. Quite simply, we're all targets.

You're a scam target every day.

As you saw above, the word prey means "victim." However, being a target for a scam doesn't mean you are or will become a victim. To start with, you need to understand the following:

Everybody is a potential **target** for a scam. You, right now, will likely be contacted by a scammer in some way, several times in the next month. You're a target now.



You make yourself a bigger target if you engage in certain activities. If you use online dating sites, you are a target for romance scams. If you're looking to make money fast, you're a target for get-rich-quick schemes.

A scam involves you directly. A scam isn't like a car break-in. It involves an actual interaction between the scammer and a target—their potential victims.

We included in this ebook an article that talks about the steps involved in a successful scam. Targets who become victims chose to take certain actions. Just realize that being a target (prey) doesn't mean you'll become a victim.

Who becomes "Easy Prey for a scam?"

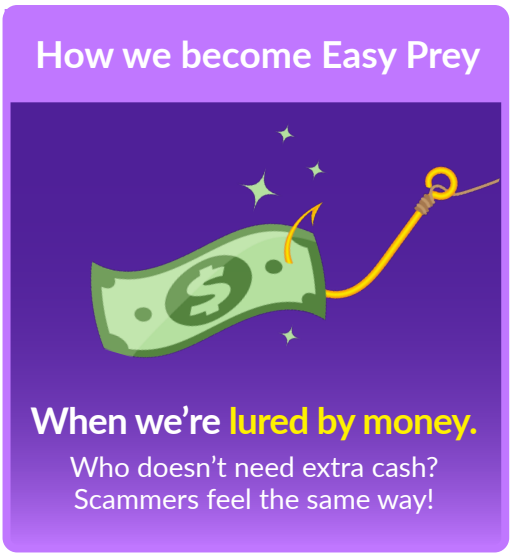
The term we all have heard, *easy prey*, can be explained rather simply. Someone who was easy prey was a person who, for whatever reasons, was more likely to be a victim.

Saying that a victim was **easy prey** isn't putting a negative label or tag on them. And it certainly doesn't imply that someone was dumb, clueless, lacked common sense or simply should have known better.

That's because being easy prey isn't always the victim's **fault**. The journey from a target to a victim can be a matter of circumstance, an unlucky day, or simply a lack of awareness.

Here are real-life examples of easy prey.

Here are a several scenarios that will help me explain that aspect of it.



- **The hungry lamb.** If a hungry lamb strays away from the herd, it is at most risk to be attacked by a pack of wolves nearby—it stands out as the most vulnerable.

- **The high school freshman.** Students just starting out in high school are easy targets for bigger (mean) kids. Although it's getting better, the weird or shy kids still get bullied by the bigger, older students.

- **Famous "wannabes."** Every year, hundreds of boys and girls, and men and women come to Hollywood hoping to be a movie star and get famous. They're preyed upon by very bad people who are looking to lure them into a bleak life.

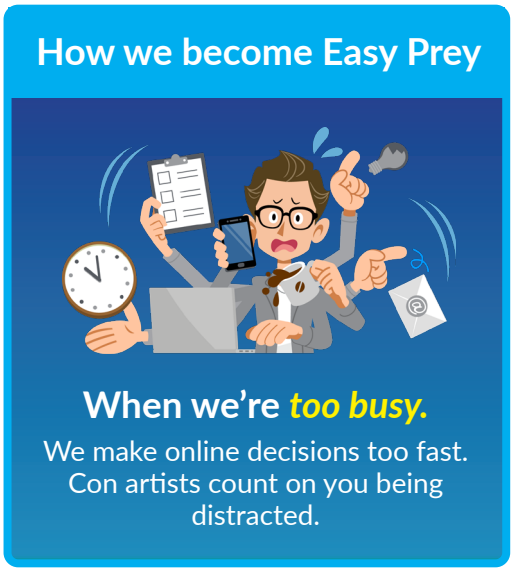
- **Homeless teens.** Homeless kids and runaways are prime victims of drug-dealers and pimps.

Could you be easy prey for a scam and not know it?

How does someone become easy prey for con artists and scammers, online and in the real world? Here are a few examples of targets who could be easy prey. As you read this, realize that you or someone you know could easily become easy prey, if the right circumstances fall into place:

- **A lonely online dater.** People who are starving for attention or affection get scammed by fraudulent girlfriends or boyfriends, who take advantage of their emotions.

- **A first-time Craigslist seller.** Someone new to Craigslist or eBay who posts something for sale could be vulnerable. They may not be aware of some of the common scams for online selling and buying. First timers often get swindled.



- **A senior on Social Security.** An isolated senior gets an email or call saying they've won $1 million in a special sweepstakes. There's a catch, of course. First, they're told, they must pay the "required" taxes and fees upfront. Sadly, the winnings never come.

- **Someone who's unemployed and needs income.** An online job that offers good pay for easy work would excite anyone. Scammers know this and rip-off people who are desperate for income.

- **A care-free, happy traveler going overseas.** Friendly con artists are eager to pounce on (and steal from) people who are new to a city, popular tourist spots and its currency.

How to avoid being easy prey for a scam.

Knowledge and awareness are your best weapons for fighting off scam attempts. Here are a few suggestions for you right now that can help you strengthen your defenses.

Learn anti-scam skills now. This ebook includes a section that teaches you eight simple things you can do to fend off scam attempts. There's even a creative infographic that goes with it. Be sure to share it with others.

Take our free Easy Prey Self-Assessment. We created our own free and easy-to-use self-assessment to help you protect yourself. It helps you discover whether you're doing a good job protecting your personal information, privacy and identity—or whether you're at risk of becoming easy prey for a scam. You can find the Easy Prey Self-Assessment here.

Listen to the Easy Prey podcast. The absolute best way to avoid becoming a victim of a scam is to be aware the risks online and in real life. One way to keep your guard up is to hear experts interviewed on the Easy Prey podcast. They will give you insights on the various scams and schemes out there. Best of all, they help you avoid being easy prey for a scam.

The more you know, the safer you are.

We are all targets, but we can avoid being a victim if we know what to look for and what to do. The good news is, you can do that by keeping your eyes open, your scam radar on, and developing good, scam-savvy habits.

Stay safe. Be wise. And remember, if it all sounds too good to be true, it very likely isn't real.

You just learned what makes us easy prey for a scam. Next, find out what the top 5 online scams are that you need to the watch out for!

Part 2

The Top Ten Online Scams That Fool People Most

Scammers use a bag of tricks and cons to fool their next victim.
This chapter shows you the online scams that are best for them, but bad for us.
If you find yourself in any of these situations, keep your eyes and ears open
and proceed with caution.

WHY DO PEOPLE STILL FALL FOR ONLINE SCAMS? MOST OF US THINK WE'RE TOO WISE TO LET FRAUDSTERS FOOL US. WE'RE NOT. ACCORDING TO A RECENT SURVEY DONE BY THE BETTER BUSINESS BUREAU AND OTHER ORGANIZATIONS, THE OUTLOOK ISN'T GOOD. IT SAYS ONE PERSON OUT OF TEN IN THE U.S. WILL BE A SCAM VICTIM IN THE UPCOMING YEAR.

So, here's a little quiz for you:

Do you know the top ten online scams that are working the best for con artists right now?

Could you even make a list of three?

It's important to know things like that—here's why.

Surveys provide a ray of hope with the scam statistics. The good news is this: if we know what the top scams are, the harder it is to trick us. In other words, the more we know, the safer we are.

So, let's look at the top ten scams that fool people the most.

#1. Online shopping scams.

Consumers are losing billions of dollars to fraud and scams every year, and online shopping scams are one of the top culprits. In the U.S., online shopping scams were the second most reported scams to the FTC and accounted for more than $350 million in losses.

Cybercrooks and con artists go where the money is, so online shoppers must be extra careful when they're looking for a bargain, a gift or simply saving time by going online. Crafty thieves have dozens of ways to direct your online shopping dollars their way.

They'll try to fool you with fake texts or emails about a delivery problem, or they might contact you with a problem with your credit card. They may try to pretend they're from your bank, saying there's been fraud reported on your account, related to a shopping purchase. In some cases thieves acquire bank account and

Social Security numbers, then use that information to commit identity crimes.

We're not only talking about eBay, Craigslist, Mercari or Poshmark scams anymore. Scams will pop up tied to Amazon, Facebook Marketplace, Walmart Marketplace and other well-known brands. In addition, fake or disreputable online shopping sites are also a problem, because it's hard to know what sites are legitimate and trustworthy and which aren't.

It's all part of the online shopping fraud epidemic. The best advice? Buyer beware!

#2. Fake tech support scams

Here's a scam that uses fear to motivate victims into forking over money. After all, nothing worries us more than having a deadly virus on our computers, such as ransomware. Tech support scams trick you into believing you have malware lurking on your computer. To fix the "problem" they've identified, you'll need to send them money to pay for the repairs—or run the risk losing all your data.

Scammers will play dirty, too. Often times, they will make you believe that Microsoft—the world's leading software developer—is reaching out to you with a pop-message, an email or phone call. In India in 2018, police raided ten illegal call centers and arrested dozens of scammers who were running a very sophisticated tech support center! Police found live chat apps and scripts for calling and fooling victims.

Microsoft is aware of the problem and, according to their own consumer research, victims of fraudulent Microsoft tech support usually pay (and lose) anywhere between $150 and $500 for worthless tech support. If you see a pop-up ad or a warning screen saying your computer has been infected, ignore it, say the experts. That's not only a scam, but it's usually the gateway to a link that might infect your computer!

#3. Employment/job scams

Job hunters beware, especially if you're a little desperate for work. Scammers masquerading as employers are eager to meet you.

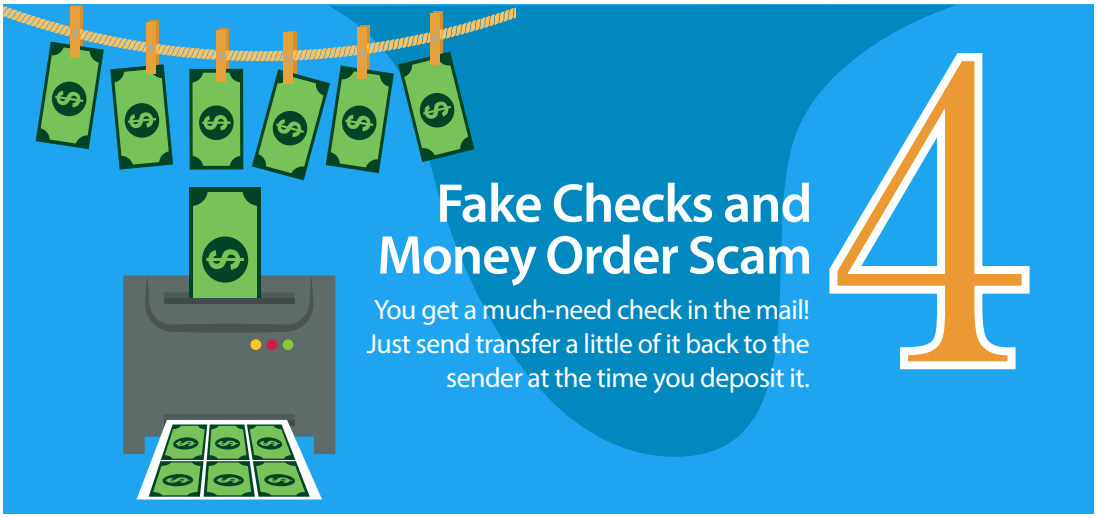
Many people who think they've just gotten a legitimate job, soon end up losing money or having their identity stolen, without ever making any money. And often, those getting scammed are the ones who need money the most! Perhaps they were even joyous that, at last, they were able to land work!

Here are just three possible clues that the job you see posted might be a scam: 1) they don't make you take and interview. 2) It promises good money for not a lot of hours or hard work 3) you can start immediately. (You can see how those features could seem to be beneficial for many job seekers and lure people into the scam.)

Here's what happens if your new job isn't real. You'll get a sizable initial check to buy supplies, for instance. But wait! They ask you to send some money to another

employee, out of your own pocket. Of course, they paid you with a worthless check. *(Read the #4 top scam for more on that.)*

And sometimes it's more than money you lose. You give the scammer all your valuable personal information on the job application. They have your Social Security number, drivers license number, home address, and more.



#4. Money order and fake-check scams

Money orders and checks are at the heart of several scam types...and a tip-off that there could be something wrong.

The situation is this: you find yourself receiving a check or a money order (maybe for selling an item online, or as part of a new job) and you're asked to deposit the check in your bank account—but before you do that, the sender tells you to wire or transfer some of the amount back to you. Or maybe you are told to send a portion of the money to someone else.

Why? You were overpaid, you're told; they sent you $300 instead of $200. Or it's your first paycheck for $500, and you need to send back $200 for supplies.

They might say, "Just deposit the check and send the money. It will all work out." So, you send the money, and deposit the check in your bank. Of course, you find out in a few days that they sent you a bad check or a fake money order.

You lose twice. For one, you owe the bank the amount they initially gave you (if any), and you lost the money you wired back to the con. To avoid this predicament, NEVER send money to anyone until you make sure they're check has cleared.

#5. Phony sweepstakes and prize scams

This scam works well for con artists once they get a target interested…and that's pretty easy for them to do. The cons reach out to people, often the most vulnerable or needy, with the news and the promise of sweepstakes winnings—sometimes in the thousands or even millions of dollars. It all sounds and looks convincing. There's a catch, of course.

To get the money, the "winners" must first pay a small upfront fee to claim their prize. That fee might be $10 or $200.

In Missouri, not long ago, the State government shut down a fake sweepstakes that tricked senior citizens into giving scammers millions of dollars. As a director of the FTC said, the older adults "paid money to collect prizes that never materialized."

This scam, as you might expect, deceives those who are in a financially insecure situation—where a "miracle" influx of cash could be a life changer.

Here's the main thing to remember: It's not possible for you to win a sweepstakes or contest that you didn't enter. If someone tells you you've won a sweepstakes you didn't enter—in a letter, email or text—don't fall for it. Report it to the authorities instead!

#6. Imposter scams

The U.S. Federal Trade Commission ranks imposter scams as the most reported con in recent years. By pretending to be the IRS, your bank, the police or other authority figures, these imposters steal money from millions of people every year.

It's not that some con artists have a special talent at pretending to be someone they're not. It's that the impersonators are very skilled at manipulating victims' emotions.

An impersonator pretending to be from the Internal Revenue Service instills fear and worry into their victims first, then uses pressure to have them pay back taxes (which don't exist). Other scammers might pretend to be a friendly banker notifying a customer of an account problem. In that case the thief is friendly, caring and helpful while stealing the victim's money.

These ruses are very effective because scammers also know how to mimic actual websites and can even spoof phone numbers of the organization's they're impersonating. The thieves also know that most ordinary people have a measure of respect for organizations they generally trust.

If you get a message or call from anyone saying they are from your bank, the IRS or any organization saying there is a problem, hang up. Check the phone number they called from or email address they used and look for inconsistencies. Then, look up the organization's contact information online and see if they called.

#7. Investment and cryptocurrency scams

People from all walks of life lose money in investment scams: old and young; experienced vs. first-time investors; the greedy and the hopeful. They all have something in common: they're hoping to find good returns, fast and easily.

The bad news (and a worthwhile reminder) is that scammers have an approach—and an investment opportunity—for everyone. It's wise to heed the advice security professionals have for everyone: if it sounds too good to be true, it probably is. And today, it's also probably a scam.

Not only did the cryptocurrency craze not work out the way investors wanted, but thousands of people also lost money to crypto investments that were pure scams from the start.

Investments are risky to begin with, and most investors are willing to take some risks to make a lot of money. If there is a promise of an incredible and quick return, many investors will be tempted to jump in—with their fingers crossed. That's why more than $1 billion of losses in cryptocurrency scams have been reported in the U.S. alone.

Sadly, many cryptocurrency scam victims were talked into the investment by someone they developed a relationship and trusted. Once the victim's money was in the hands of the scammer, the romance or relationship was over. Which leads us to number 8…

#8. Romance scams

Romance scams cause financial losses in the millions every year, and that number keeps growing. In 2022, reported losses due to romance scams reached $1.3 billion dollars, following explosive growth year by year.

These scams are especially cruel to victims because it involves both emotional and financial loss and pain. And here's what's both shocking and surprising: typically, the romance scam victim never meets their online sweetheart.

It's easy to think, "how is that even possible?" You would think people would be skeptical of anyone they meet online. And many people are. But scammers know

exactly what to say to those they target and how to win over their emotions, trust and eventually, talk them into giving them money.

More than that, for the single or lonely person, there are a lot of dating apps to choose from, for every age and profile. And remember that Facebook and other social media sites offer a way to meet new people, make new friends and possibly find that special someone.

That's why scammers are on dating apps and social media, pretending to be that person.

#9. Business Email Scams (Spear Phishing)

Better known as BEC, for Business Email Compromise, business email scams cause some of the largest losses per incident because they target the bank accounts of businesses. In 2022, victims of BEC lost a total of $2.7 billion.

Any employee that has the authority to initiate a wire transfer at a company should pay attention to this advice: Stop, relax and think before paying any vendor from a request that comes urgently and out of the blue from someone in your company. There is a very high likelihood the request is from a scammer.

BEC often starts with spear phishing—instead of using a wide net to ensnare victims, thieves first research a company executive to impersonate. They also profile and target the exact employee they'll attack and trick to wire the funds.

BEC is highly effective because companies have multiple vendors to pay, and more than one manager may have the clout to request a vendor payment to be made on demand. And most employees will think twice before refusing an executive's demand.

Through these highly coordinated attacks, usually done by criminal enterprises in faraway countries, scammers can steal money, identities, business secrets and launch ransomware...none of which are good for business.

#10. Charity scams

When a major, tragic event takes place, such as an earthquake, hurricane or devastating fire, people want to know how they can help. As our hearts go out to the victims, scammers get ready to send out texts, emails and phone calls to potential targets of a charity scam.

Scammers know we are susceptible to being generous (and fooled) when charitable donations are needed. It doesn't have to be a natural disaster either: It can also be during the holidays, the annual season of giving. Scammers know how to make it easy for you to give by creating fake charities or impersonating well-known ones, like the Red Cross.

A scammer might also contact you to support other genuine worthwhile causes, such as help for military veterans, the homeless or troubled teens. If you have a

special place in your heart for these people in need—or you feel bad for never having made a donation—you may easily become a scam victim.

You don't need to give up donating to charities, but you should decide never to donate from a solicitation that comes to you. Also, if you have donated in the past, beware of "follow-up" calls from someone claiming to be with that organization.

But making any donation do your research. There are online resources that can help you find the charities that truly need your support and will get it to the people who need it...not the scammers who want it.

It's good to know the top scams. It's also important to know how a scam works, so you don't accidentally fall into a trap.

Part 3

How Scams Work and Fool Millions of People Every Year

How does someone go from being a target of a scam, to being a victim of one? It's not an automatic or instant process. It can take few minutes, a few hours or a few days. Here's a look at how someone gets tricked by a scam

EVERY YEAR, MILLIONS OF PEOPLE LOSE BILLIONS OF DOLLARS TO FRAUD AND SCAMS. AND THE CON ARTISTS WON'T BE GOING ANYWHERE SOON. NEW SCAMS ARE CREATED EVERY DAY. FOR INSTANCE, THIS YEAR IN THE U.S. ONE IN TEN PEOPLE WILL FALL VICTIM TO A SCAM.

Know how scams works, and you can work your way out of one.

Research and surveys clearly show that knowledge and awareness regarding scams can reduce the chance of being a victim. The more we know how scams work, therefore, the less likely we are to become victims of them.

Knowledge is power. The power to stay safe.

From start to finish, here is what makes a "successful" scam work.

A successful scam by a con artist happens only when they get what they were out for—usually someone's money.
It doesn't happen by accident. They're not waiting for people to drop their wallets,

leave their purse or backpack unattended, or leave their front door unlocked. Scammers create their fraud with precision.

A scam is a plan that a con artist rolls-out hundreds of times a day. And even though the scammer knows their schemes won't work 80%-90% of the time, that doesn't matter. The payoff they get from their victims is worth it.

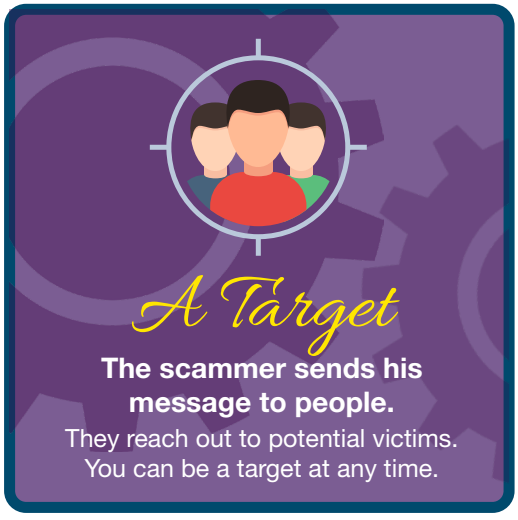
Here's a breakdown of how 5 components of a scam turn a target into a victim.

1. It starts with a devious plan.

A scammer is a liar and a thief, make no mistake about it.

The scammers "tool" is trickery, deceit, lies, and a plan (a scheme). It takes the form of a message, with the promise of something very special that people want—money, a job, riches, love. Once he or she has a scheme, they're ready to launch their fraud on the world.

Scammers are devious. They often prey on innocent, vulnerable, and desperate people, often taking advantage of their kind-hearted nature.



Scammer are liars and impersonators—you won't always see them coming.

2. Add targets (potential victims).

A scam involves two people—the scammer and a target, a potential victim. Almost anyone can be a target at any time for fraud of some kind.

Consider yourself a target for a scammer right now. One day and maybe soon, you'll likely be talking to a scammer, getting a message from one, or reading a fraudulent email or letter.

Just remember that being a target is not the same as being a victim. If you can sniff out the scam while it's unfolding, you can bring the con's plan to a quick halt.

That's why it's important to be aware of the different kinds of scams out there today. A believable yet devious scheme has the power to fool.

Consider yourself a target at any time. If you do, your eyes will be open and your radar will be up.

3. There's the sales pitch, the hook.

Fraudsters must initiate a conversation to the target, to get their scheme underway. They contact people through phone calls, emails and texts. They'll sometimes post ads on websites or on social media. To them, it's a numbers game to them. That's why they'll keep sending out messages, because they know a percentage of people will respond.

The scammer's message usually isn't personalized. They typically don't know your name or much about you. They simply have a sales pitch or an opportunity they hope will catch your attention.

Often their message—the hook—will seem reasonable or even interesting: they may pose as a buyer interested in what you're selling online, or they want to hire you for the professional services you provide, such as photography. Scams work because they're well thought out.

Scammers know some people will listen to their sales pitch, and that's all they're hoping for.

A scammer's "hook" is a lie that will sound a lot like the truth.

4. The potential victims listen—they "engage" with the scammer.

Scammers need the attention of their targets to get their deceptive story going.

They don't always get it. Research shows, for instance, that almost 50% of people who get an unwanted message don't waste a second listening. They instantly reject the message and move on. (Think of it like getting a sales call and just hanging up.)

The other 50%? They'll keep listening…at least initially. That's what scammers need: the ***ears and attention*** of their targets, so the con artist can tell their whole message and hook people.

Research shows that 85% of people who begin engaging with a scammer (even if they don't know it's a scam) terminate the contact sooner or later. Good for them.

Those who keep on listening and talking to the scammer, however, aren't so lucky.

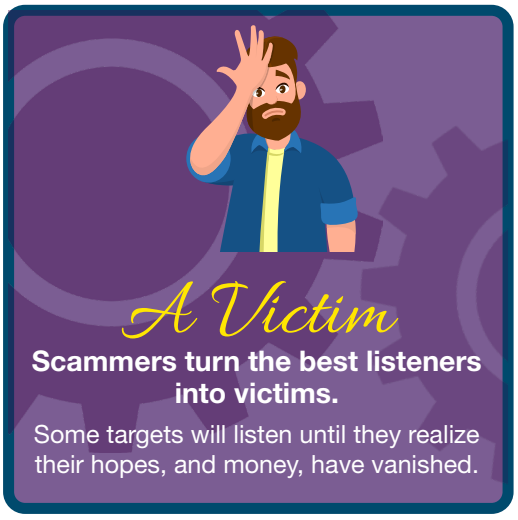
Scammers need only a small percentage of people to stay engaged in the conversation.

5. Scammers turn fully engaged listeners into victims.

The targets who eventually become victims fall into a wide variety of scams, but they all share one thing in common:

They kept listening the scammers lie, believing it and hoping for the best. They do it right up to the point when they realize their hopes—and money—have vanished, and there is nothing to show for it. For victims, it goes something like this:

- The victim got a new job and had to pay for supplies and training: they sent their money and received nothing for it.
- The victim accepted a check for a professional service and agreed to send some cash to someone else as part of the deal. The check bounced and their cash disappeared.
- They paid for merchandise online that never arrived or came damaged, and the seller disappeared with their money.



- The victim won a sweepstakes prize that never arrived—even after they paid a fee to get it.

If you willingly give a scammer your full attention, they will happily take your money.

Knowledge is your best defense. Listen to the Easy Prey podcast.

Here's what we know. The more information someone knows about scams and how they work, the less likely they are to become a victim of one. There are hundreds of scams and millions of victims every year.

The best defense isn't the police or the FBI—they get involved after people become victims of a scam—it's knowledge and awareness that can keep you out of scammers' grip.

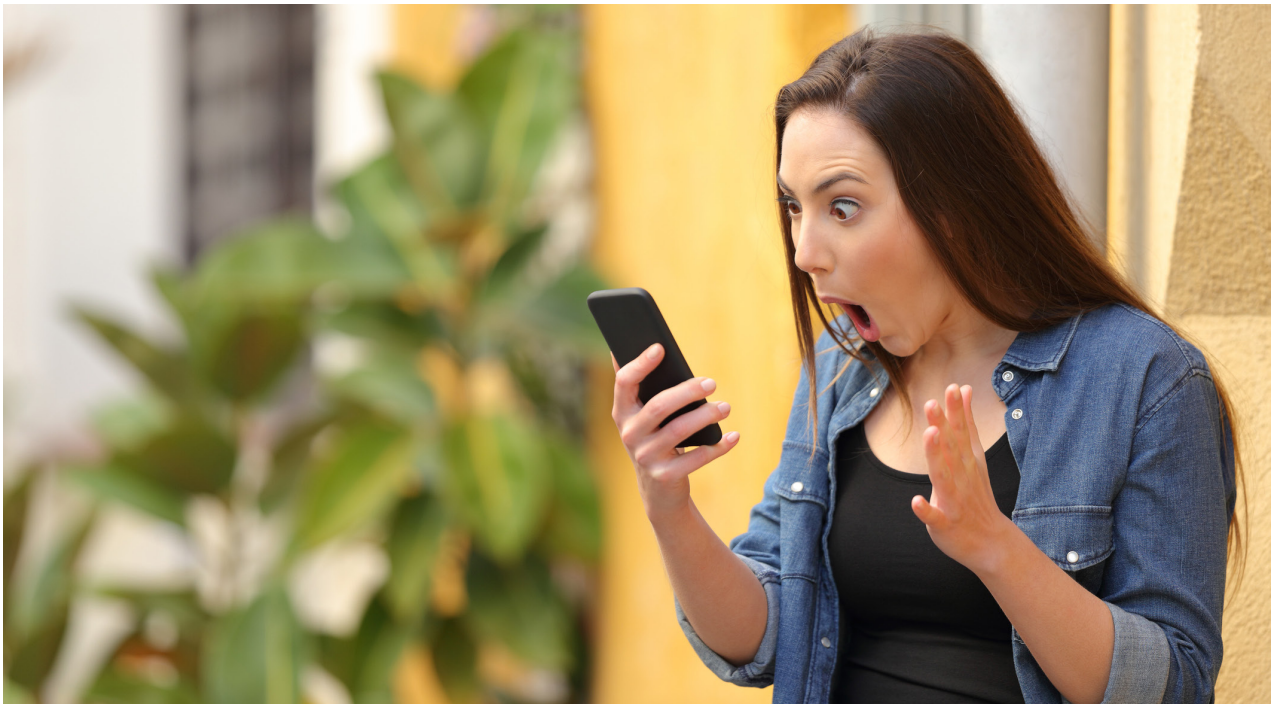
That's why you need to learn about scams, how they work, what they sound and look like—so you can avoid being a victim. For instance, in this ebook you learned that hanging up on an unwanted call is a sure-fire way to avoid a potential scammer. You need to find information resources you can trust.

Just because you're a target for a scam doesn't mean you'll end up being a victim. Next, we'll give you some simple tips to avoid a fraudster's schemes.

Part 4

8 Clever Tips on How to Avoid a Scam

People who get conned by scammers make several mistakes, the main one being they communicated with the con artist just long enough to get tricked into losing money. Could they have done anything different? You'll find out in this chapter.



YOU CAN LOWER THE CHANCE OF BEING A VICTIM OF A SCAM BY ADOPTING A FEW NEW HABITS TO KEEP SCAMMERS OFF GUARD AND OUT OF YOUR LIFE. YOU THINK YOU'RE TOO SMART TO FALL FOR A SCAM? NOT SO FAST, BECAUSE SCAMS COME IN ALL SORTS OF SHAPES AND SIZES—AND SO DO THEIR VICTIMS.

This year, one out of ten people in the United States will fall victim to fraud and become one of the thousands who lose billions of dollars every year.

In the months (or even weeks!) ahead, you might be targeted and contacted by a scammer when you least expect it and, of course, you won't be notified in advance that it's coming.

And that's what scammers count on…catching you off guard or tricking you into putting your guard down and becoming more vulnerable—for just enough time to pull the wool over your eyes and steal your money.

The wrong way to boost your scam radar.

The best way you could boost your radar for scams is also the worst way:

To get scammed.

Why is it the best way? Because, for sure, you'd likely never let yourself be fooled again! But who wants to learn the hard way? No one!

Here's a better way.

Develop some sure-fire, effective, and proven anti-scam responses. For example, the next time you get a "great deal," "super offer," "dream job," or "pay up or else!" message by phone, email or text, you'll know how to respond.

We say proven responses because recent research bears it out. The following tips, for example, come direct from their accounts of what happened to former victims.

Following simple, sound advice is good for us.

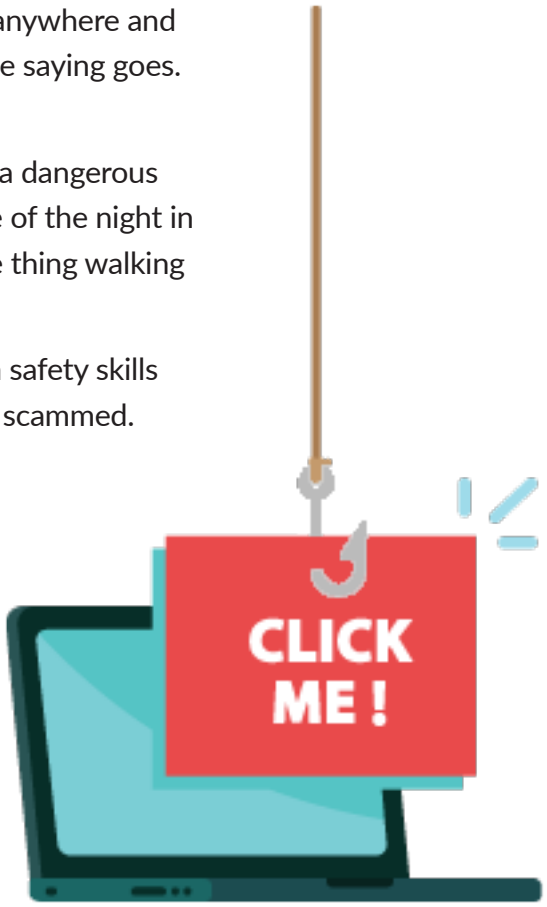
Some tips that seem too simplistic are usually spot-on and helpful.

Here's what we mean:

- You tell your children "don't talk to strangers" for reasons that can save their lives.
- People tell travelers going to foreign countries "don't drink the water," to help keep their friends from getting ill.
- And everyone advises a job seeker to "have a firm handshake" and "dress for success" to make a good first impression.

Think of these anti-scam tips below for you and your friends to be just as important. We say that for good reasons:

1. Scams are on the rise. Fraudsters aren't going anywhere and "there's a new sucker born every minute," as the saying goes. Con artists still believe that.
2. You need to see yourself as potential victim in a dangerous world. You wouldn't go for a walk in the middle of the night in a strange town—you know better. It's the same thing walking into dangerous situations digitally.
3. As mentioned before, it is much better to learn safety skills now, rather than learn the hard way by getting scammed.
4. You will get approached this year (maybe a few times) by a scammer, either directly in person or by phone, or indirectly through a message or ad.
5. These are tips you need to teach your entire family. Are you aware that there are specific types of scams for seniors, baby boomers, millennials, teens and even younger children?



Anti-scammers boot camp.

Are you ready to change your thinking and develop some new habits to keep you safe from scammers?

Let's go!

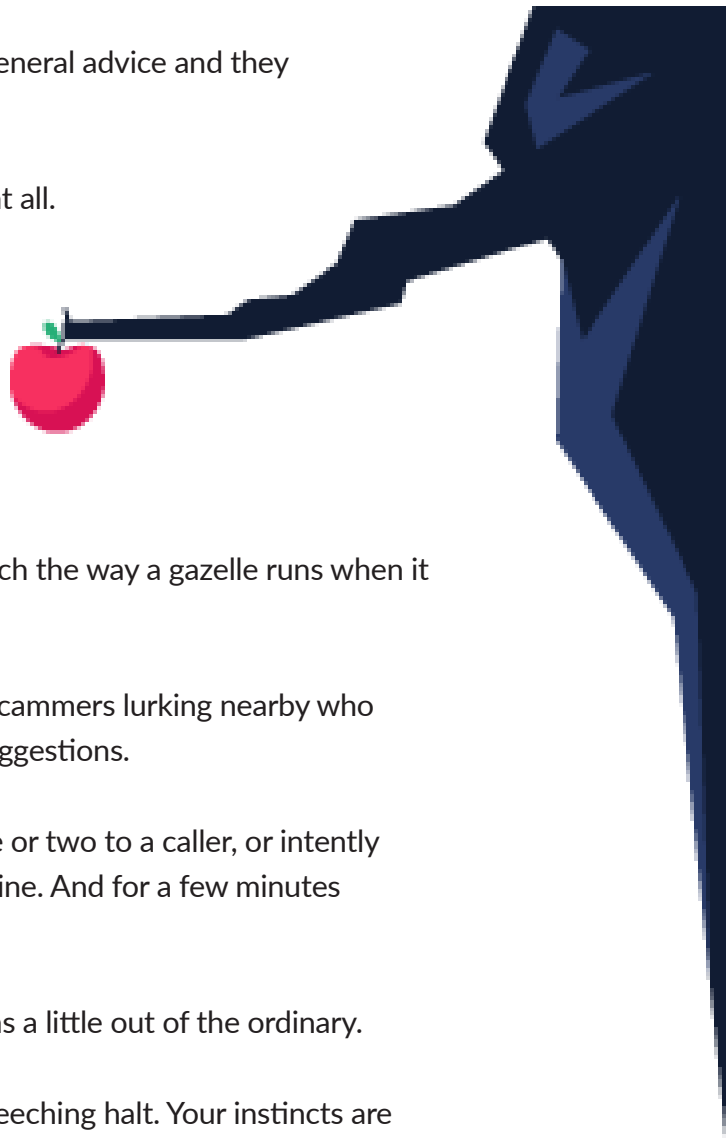
1. Hang up! Delete! Block! Don't give strangers a minute of your time.

scammers need your attention, so you might simply refuse to open strange emails and take calls from numbers you don't recognize, etc.

Does that sound harsh? Is that not like you? It's hard to imagine being so strict with rules or responses, but keep this in mind: There is nothing that says you need to engage with anyone or any message that you did not initiate.

There are thousands of people who follow this general advice and they all have this one thing in common:

They won't get scammed anytime soon…if ever at all.



2. Trust your instincts. Flee the second something just doesn't seem right.

Dave Ramsey, an expert on personal money management, advises people to "run" from every credit card offer they get, in much the way a gazelle runs when it senses a lion lurking nearby.

That's a good analogy for us, because there are scammers lurking nearby who approach us with innocent sounding words or suggestions.

You may find yourself lending an ear for a minute or two to a caller, or intently reading an email, or responding to a job offer online. And for a few minutes everything may seem perfectly normal to you.

Until…you hear or read something that just seems a little out of the ordinary.

Trust your instincts and bring everything to a screeching halt. Your instincts are trying to warn you, just like the gazelle who gets a whiff of danger. Run!

3. Be more skeptical.

Maybe you don't have it in you to hang up on people or to delete every email you don't recognize. We understand—"what if," you're wondering, "that urgent email really is from the bank, telling me that my payment is late?"

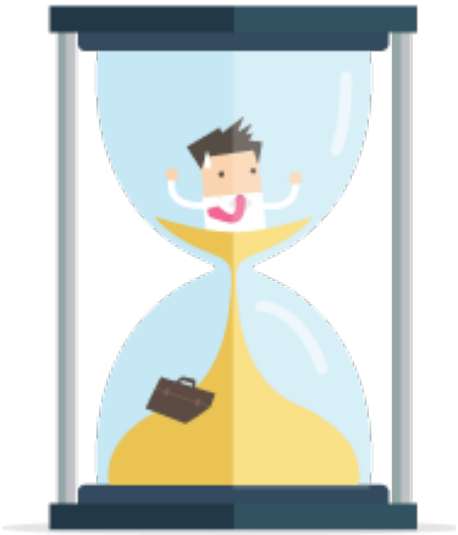
However….

Many people do get scammed because they lend an ear to callers or read emails diligently and carefully: maybe simply because they haven't been scammed before. And besides, they like to give everyone a measure of respect and the benefit of the doubt.

Although that's an admirable sentiment, you simply can't afford to be that trusting in this day and age.

For example, there's a term called social engineering that you should know about.

Social engineering involves a con artist acquiring information about you (personal or work-related) and developing a quick profile of your home life or work life. From there, they use that little (but accurate and convincing) information to trick you into some kind of fraud to steal either your (or your employer's) money.



Therefore, when someone sends you an email, claiming to be your boss or coworker, and tells you to send a Mr. Jones in New York the company credit card number, YOU NEED TO BE VERY SKEPTICAL.

Just because a stranger is polite doesn't mean they're honest. This is very important piece of advice to share with senior citizens, who are part of generation where politeness goes a long way. That's something scam artists know very well.

4. Research the person or organization.

There are times when you may be moved to donate money or resources—maybe in response to a local disaster, a devastating earthquake overseas, or the homeless

crisis. There are many legitimate organizations that will take donations; however, there are also many legitimate-sounding groups that are fraudulent.

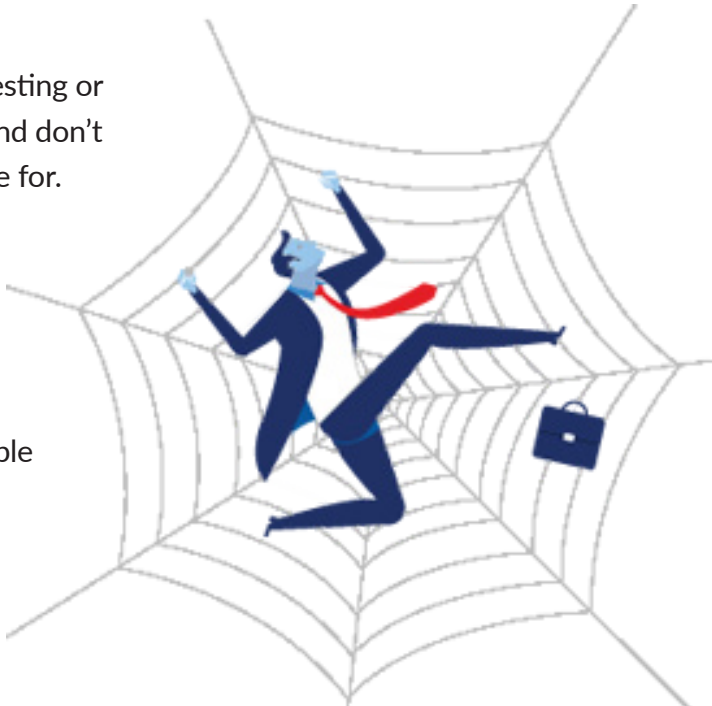
Take your time to research organizations and double verify the information you're told. Don't let yourself be fooled simply because a group has an impressive website with professional photographs and a list of testimonials. Use the entire internet to get at the truth and donate only after you're convinced your money will wind up in reliable hands.

5. Talk to a friend!

The last thing a scammer wants is for you to talk to someone before you make the decision they're pressuring you to make. In fact, news accounts of sweepstakes scams report that con artists tell victims not to talk to their friends. They insist you must act fast to get a great deal.

But by reaching out to a friend, you avoid making a rash decision. You also might simply destroy what could be a scam altogether—because friends don't let friends get scammed!

This is good advice in many areas of life, from investing or buying a used car to getting married. Be patient and don't rush an important decision. That's what friends are for.



6. Don't be bullied!

Scammers often call victims at home and impersonate authority figures. They pretend to be IRS Agents, the FBI, the police—and threaten people

to pay fees, fines, or back taxes…or else! The scammer will sometimes say the police are on their way to your location as they're speaking. Of course, they assure victims, that can all be called off if you pay what you owe immediately over the phone with a credit card.

This trick works more often than you think, especially if the scammer reaches a target who might be behind on their taxes or simply has a guilty conscience.

Take note! A bullying caller or threatening letter is a clear indication of a scam in the works. Don't let that first wave of fear trick you into responding to their demands. Hang up on any caller who uses threats and fear. Then call a friend…and the authorities.

7. Just say "no!"

If you're not the type to hang up on people, go off to do research, involve a friend, etc., then simply follow this piece of advice: Just say "no thanks" at some point during a conversation that you did not initiate or that you don't want to continue.

Just say "no," "no thanks," "not interested," or even "good luck with your efforts… good bye!" End the conversation and step away. You have every right to do so, even if a caller is NOT a scammer.

If you gave every telemarketer your time and ear, you'd waste a lot of minutes, buy services you don't need. Worse than that, you might get talked into a well-designed scam.

8. Follow the Easy Prey podcast.

Keep learning about scams! Finally, there's one more habit and routine you can adopt that could fine-tune your scam-radar and keep you from becoming a victim: simply keep up to date is to listen to the Easy Prey podcast.

The Easy Prey podcast features interesting, entertaining and insightful content. Ranging from interviews, talk and tidbits on how you can stay safe in today's world.

The more you can learn about scams—how they work; the latest types, the warning signs—the better prepared you are to kick into gear with your new-found scam-savvy skills to stay out of the clutches of fraudsters.

Get notified of the new Easy Prey podcasts.

You can sign up for Easy Prey podcast alerts. That way, you can be notified anytime a new podcast is available or when important new content is posted on the EasyPrey.com website.

You can find the **Easy Prey** podcast on iTunes, Google Play and other media player platforms.

Part 5

If You've Been Scammed, You Need to Report It. Here's How.

Sad to say, only a small percentage of people who get scammed ever tell anyone. Typically, a victim feels too embarrassed to let a friend know about the incident or report it to authorities. That needs to change. This information will help.

AGENCIES AND LAW ENFORCEMENT NEED YOUR HELP—AND SO DOES THE ENTIRE COUNTRY. WHEN YOU REPORT A SCAM, YOU'RE PROTECTING OTHERS BY HELPING POLICE AND GOVERNMENT AGENCIES. REPORTING YOUR INDIVIDUAL CASE HELPS THEM DO A BETTER JOB CATCHING CYBER CRIMINALS.

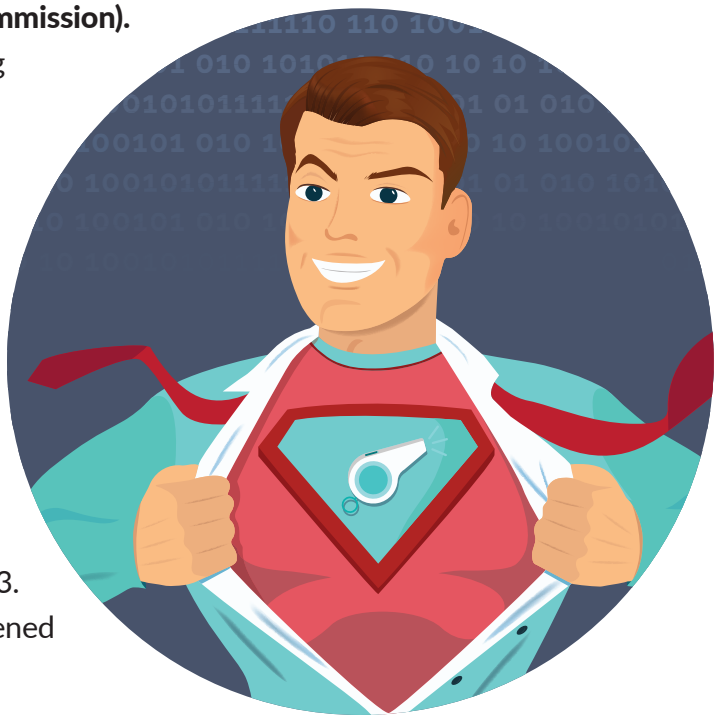
If you've been scammed, you should report it. Here's how.

If you've been scammed online in some way, you need to report it to authorities. Yes, it's embarrassing, and you want to forget about it, but it's vital that you do it.

Here's who to report it to.

Let's get right to it. On the next page, these are the places where you could report a scam and other fraudulent activity.

1. **Contact your local police department.** They may or may not have a fraud unit, but they'll want to know if people in their jurisdiction are being targeted. A little online research on your part will tell you what services or assistance they offer.
2. **Contact the scam and fraud unit in your state.** Your state has resources and a place to file a report on cybercrime, and to begin the recovery process.
3. **Contact the FTC (Federal Trade Commission).** This is a must for any scam involving fraudulent transactions pertaining to purchases and/or businesses, whether online or offline. This is also the place to report text and phone scams, which account for a majority of fraud these days.



4. **Contact the FBI and their IC3 unit.** If you've had an encounter with an online scammer, reach out the FBI and their Internet Crime Complaint Center, also known as IC3. You can report any crime that happened online to the FBI IC3 website here: https://www.ic3.gov/.
5. **Go to the U.S Government website for help.** You'll find complete information and resources regarding scams and fraud on the us.gov website: https://www.usa.gov/scams-and-fraud.

If you have any questions about reporting fraud to the FTC, you can get answers through their FAQ page at https://reportfraud.ftc.gov/#/faq.

Report near scams too!

Report a scam even if you weren't victimized. Because there's a very fine line from being targeted for a scam and becoming a victim. Your report of a close call still helps build a profile of and case against scam networks. Your report of near scams gives authorities more information to build profiles and track trends.

The majority of scams and fraud are not reported.

Government agencies around the world tasked with fighting cybercrimes and fraud need our help. The fact is, too few victims are reporting that they've fallen prey to scammers and fraudsters.

A recent guest on the Easy Prey podcast, hosted by Chris Parker (CEO of WhatIsMyIPAddress.com), shared this dismal news on cybercrime reporting by victims. In his estimation...

- For losses of less than $100, the expert guessed that perhaps 1% of the victims reported the lost to any authority.
- For losses around $1,000, he believes that only around 10% of victims report the crime.

While those losses may seem too small to matter, think of how fast these small "successful" scams add up and the money losses with them. In other words, These unreported scams quickly add up to hundreds of thousands of losses, and no record at all of how the scam worked, where it happened and who the victim was.

Also, don't assume that when someone loses $5,000 or $10,000 those losses are reported. Again, many victims are too ashamed or feel too guilty to tell anyone about their loss. Thousands of scams involving significant losses go unreported every day.

An unsuccessful scam...is still a scam.

Maybe we need to redefine what a scam is, because nearly every thinks they if they haven't lost money to a con artist or a fraudster, they haven't been scammed.

That's not the case.

Think of it like this: If there was a night burglar who was checking houses for unlocked windows and doors, wouldn't people report that? And wouldn't the police want to know if that was going on? Here's what would happen:

- Several neighbors would report the incidents they saw.
- Each report would include time, location, and a description of the suspect of vehicles.
- Investigators would use the information, from targets and victims, to try to identify and locate the intruders.

And yet, it's likely that only 10% to 15% of actual scams are reported to authorities.

And if people who get scammed don't file a report, you can imagine how few people report a close encounter with scammer.

Reporting scams is key to the fight.

Just like police detectives or FBI investigators on a case, cyber sleuths need leads to track down cyber thieves. You've seen the crime shows and movies for years. When a crime has happened, the police and detectives go looking for leads.

Think about this for a minute:

- Without any leads, the investigators can do very little. They're chasing ghosts.
- The more information, tips, insights and details they can get, the better chance of breaking the case.

That's why sharing in-depth details of your scam experience is helpful:

- It can benefit millions of others by helping take a successful scammer or a scam trend out of circulation.
- It can prevent scammers from preying on others who have a similar profile to you.

It's not only government officials who analyze the information they receive from reports of fraud. Cybersecurity experts and financial security advisors also have joined the cause to help reduce the occurrence of money scams. They need statistics and information to analyze and share with others.

Scams make headlines; however, scam networks that get busted don't often make headlines, even though that's the news we should hear and cheer.

That's why we all must report financial scams (whether we lose money or not) to government agencies that are set up to fight cybercrimes or fraud.

Winning the fight against cybercrimes.

Yet, there are two types of scam victims:

- There are those that retreat in shame and guilt, and cannot get themselves to admit to others or report it to authorities.
- Then there are those who, despite the emotional pain and hurt, take action and report it. They understand that it's important to tell authorities of the scam, in hopes of catching the criminals or recovering some of their losses.

Reporting scams and internet crimes helps authorities bring criminals to justice, with hopes of making the internet a safer place for everyone.

Increase your awareness of cybercrimes and scams!

Reporting scams is one step against the fight against scammers. Increasing your awareness—becoming scam savvy and avoiding scams—is another big step.

One way to do that is to subscribe and listen to the Easy Prey podcast, where host Chris Parker interviews experts on a wide range of important topics, all relating to staying safer online and in the real world.

Keep informed, stay safe, and join the fight against scams and fraud.

Thank You.

We hope you enjoyed our ebook on how to spot scams
and avoid becoming a victim.

For more enlightening insights on scams and advice for staying safe,
follow the **Easy Prey** podcast with host, Chris Parker.