CHAPTER 17

Elder Scams

THE ELDERLY ARE AMONG OUR MOST VULNERABLE CITIZENS, and (not surprisingly) they're among those who are most often targeted by cybercriminals. There were nearly fifty thousand complaints of fraud involving victims over the age of sixty reported to the Federal Bureau of Investigation in 2017, with adjusted losses totaling more than $342 million. The U.S. Government Accountability Office estimated in 2018 that financial fraud targeting older Americans probably cost seniors about $2.9 billion annually. Most fraud, they say, isn't reported because either the victims don't know *where* to report it, they're too ashamed to admit they've been scammed, or they *don't even know* they've been victimized.

On February 22, 2018, U.S. Attorney General Jeff Sessions announced the formation of the Elder Justice Initiative, which is designed to support and coordinate the U.S. Department of Justice's enforcement efforts to combat elder abuse, neglect, and financial frauds and scams that target senior citizens. "The Justice Department and its partners are taking unprecedented, coordinated action to protect elderly Americans from financial threats, both foreign and domestic," Sessions said at the time. "When criminals steal the hard-earned life savings of older Americans, we will respond with the tools at the Department's disposal—criminal prosecutions to punish offenders, civil injunctions to shut the schemes down, and asset forfeiture to take back ill-gotten gains."

The Elder Justice Initiative seeks to provide targeted training and resources to prosecutors, law enforcement, judges, victim specialists, first responders, and civil legal aid employees to better respond to elder abuse. The U.S. Senate Special Committee on Aging is also working hard to educate elderly citizens and their families about the dangers of telephone and computer scams. The bad guys use a variety of scams to target senior citizens, including impersonating agents of the Internal Revenue Service or telling them they've won millions of dollars in the Jamaican lottery (but need to send money to claim their prize).

Some schemes originate over the Internet, while others are conducted by telephone. I once received a call about an incident involving a man named Martin, an eighty-year-old retired attorney. One

night, Martin received a phone call and the muffled voice on the other end sounded like his grandson, Fred. "Grandpa, I'm in trouble and need your help," the man said. Martin asked Fred what was wrong and how he could help. Fred explained that he was in Florida for spring break, and his taxi driver had been arrested for having drugs in the trunk of his car. The police accused Fred of being an accomplice and arrested him too. Unless Fred paid $2,500 in bond, the police were going to keep him in jail until a trial two weeks later. Martin knew his grandson was indeed on vacation in Florida for spring break and started to worry. Fred begged his grandfather not to tell his parents, because they'd get angry if they knew he was in trouble. Fred was studying at Vanderbilt University, and he told his grandfather that he had a final exam the following week and would fail the course if he missed it.

Martin would do anything for his family—especially his grandson, whom he loved dearly. Martin asked Fred if he needed an attorney, and he replied that he only needed bail money and had already located a bail bondsman. After Martin agreed to send the money, Fred put him on the phone with a bail bondsman, who provided him with instructions on how to send the money via Western Union. The bail bondsman also told Martin that police had confiscated Fred's cell phone as evidence, so he provided him with another phone number to call once the money was wired. Later that night, Martin went to a Western Union location and wired $2,500 to the bondsman. A few hours later, he received another phone call from Fred asking for an additional $2,500 to pay a fine, and he went back to Western Union to wire more money.

Fortunately, during Martin's second visit, the Western Union clerk asked him why he was sending the money. Martin explained that his grandson was in jail and needed help. The clerk asked why Fred's parents weren't sending the money, and he explained that he was trying to cover for his grandson. At this point, the Western Union clerk was concerned that the elderly man might be a victim of a scam. Together, they called Fred's cell phone. Fred answered and said, "Hi, Grandpa. How are you?" Martin asked him if he'd been released from jail yet, and Fred sounded confused. Fred replied that he hadn't been in jail and was perfectly fine.

By the time Martin contacted me, it was too late to get his money back. It was long gone. It's extremely difficult to track money sent through the Western Union network since the recipient can pick it up at any location around the world. It didn't take long to figure out what happened either. The bad guys were able to view Fred's Facebook profile since he had set it to public (meaning anyone could view his posts). There, they identified his family and friends and saw photographs from his vacation in Florida. When they researched Martin, they discovered he was Fred's grandfather, worked as an attorney, and lived in an expensive part of town. All that information is easily accessible through county tax records and professional licensing, which are available to anyone online. Since Martin was eighty years old, the thief took a gamble by muffling his voice and pretending to be Fred. If the bad guys had asked for $10,000 or $20,000 for bail money, I'm pretty sure Martin would have paid it. He was willing to do anything to help his beloved grandson.

Grandparents are an easy target for cybercriminals. The crooks prey on the elders' love for their family and, oftentimes, their limited knowledge of Internet scams. I've seen grandparents be targeted by a bad guy who claimed that their loved ones had been involved in a car wreck and needed money for towing and medical bills. The messages are always sent with a sense of urgency, and the thieves allege that not sending the money will cause even more harm to their endangered family members. Thinking about this particular scenario doesn't just break my heart, it makes my blood boil.

I recently met a woman at a cybercrime prevention conference who explained that her daughter was traveling to South America for a mission trip. Her daughter had shared that news with the entire world on her Facebook account, and her mother wanted to know what she should do about it since it was already too late to delete the information on Facebook. I told her to expect telephone calls and emails from cybercriminals pretending to be her daughter, claiming to be in trouble, and asking for money. We can't control what the crooks are going to do, but we *can* control how we react. I told the woman to establish a predetermined code word that only she and daughter knew in case she was really in trouble. They could also come up with a series of questions that

no one else would be able to answer. I told her to make sure they didn't discuss the code word or questions and answers over text messaging and email. And, of course, I encouraged her to tell her daughter to quit sharing details of her personal life on social media. We make it so easy for the bad guys to victimize us sometimes.

One of the most rapidly growing scams involving the elderly is computer tech-support scams, in which cybercriminals pose as representatives of well-known companies—such as Apple, Microsoft, McAfee, Norton, or Dell—and advise victims that their computers have been infected with a virus. The bad guys will attempt to gain access to a victim's computer remotely so they can steal personal information and other files, or they'll inject malware into the computer that the victim would have to pay to remove. Then they'll obtain credit card or bank account and routing numbers to bill the victims for their so-called "computer services."

The cybercriminals typically call the victims on the telephone, offering to "clean" their computers or remove a virus they're about to install. They'll ask for $500 to $1,000 for subscriptions to antivirus software, and they'll even offer "senior citizen discounts" if the victim complains that the price is too high. In other cases, victims have called a telephone number that appears in a pop-up window on their computer screen. Scammers have used the pop-up windows to hack into victims' computers or lock them out and demand ransom. The Federal Trade Commission also discovered that cybercrime networks have been spending millions of dollars to advertise their fraudulent services through Google and other search engines. The search terms include words like *virus removal*, *McAfee Customer Support*, and *Norton Support*. The search-engine keywords are carefully chosen to confuse victims into believing the criminals are offering legitimate services from trusted band names. Even if they're selling you actual software, it's probably nothing you really need. Cybercriminals have also been known to call victims back weeks later to offer them refunds on their contracts. The bad guys will obtain the victims' bank account records to allegedly send them a refund—but then use their banking information to steal

money from them again. I'm telling you, cybercriminals must have a reserved room in hell.

My friend's mom was surfing the Internet one evening when a blue screen popped up on her computer with a warning that looked authentic. The message on the screen said that her computer was infected with a serious virus and she needed to act immediately because her antivirus software had expired. If she didn't act right away, the message warned her, she'd lose all of her data. When my friend spoke to his mother, she was very concerned. The message instructed her to click a link to go to a website where she could use her credit card to pay $79 for an update to her antivirus software. Thankfully, she picked up the phone and called her son before using her credit card. My friend advised her that the blue screen was a scam, and he instructed her to shut down her computer, unplug it, then plug it back in and start it up. Once the computer turned back on, the blue screen was gone. The scam is called a *fake antivirus attack*, and it has been around for about a decade. It is still going strong because unsophisticated computer users enter the market everyday. Once the victim provides his or her credit card number to the bad guys, another screen pops on the computer that says the virus has been removed, and the computer is now functioning properly. In reality, the only thing the victim has done is given the bad guys a credit card number to use unlawfully.

Computer tech-support fraud is a huge business around the world. In May 2018, the U.S. Department of Justice announced that it had arrested two Florida men who allegedly owned and operated two tech-support scam companies: Client Care Experts, LLC, based in Boynton Beach, Florida, and ABC Repair Tech, based in Costa Rica. From approximately November 12, 2013, until at least December 9, 2016, the federal government alleges, the two men and others conspired to defraud more than forty thousand people across the U.S. and other foreign countries. These criminals raked in more than $25 million, according to prosecutors, by purchasing pop-up ads that appeared without warning on consumers' computer screens and locked up their browsers. The pop-ups falsely told users that their computers were infected with malware and viruses and that they were in danger of losing their data. Just as my friend's

mother saw on her screen, the ads instructed them to call a toll-free number for help.

Computer users should be extremely careful whenever a screen pops up on a computer claiming they have a virus. The pop-ups trick the users into clicking a link, and by now you hopefully know what happens when you click on an unfamiliar link. It will usually get you into trouble, because the link is designed to install malware that either steals your password and username or encrypts all of your files so they can't be unlocked without paying a ransom. That's a horrible trap for anyone to fall into—especially our nation's seniors.

HOW TO AVOID BECOMING A VICTIM

- Do not give remote control of your computer to a salesperson or technician who calls you unannounced.
- If you receive an urgent or unscheduled call from someone who claims to be tech support, hang up the phone. Ninety-nine out of one hundred times, it's going to be a scammer.
- Do not rely on caller ID to authenticate the person on the other end of the phone. Cybercriminals spoof caller ID numbers or block their numbers before contacting victims. They can make it appear they're calling from Microsoft or Apple, but they might really be located in West Africa or Eastern Europe.
- Remember that IT professionals are never going to call you from computer and software companies like Apple, Microsoft, Norton, and McAfee. If you have a legitimate problem with your computer or software, you have to pick up the phone and call them for help.
- Keep your computer's antivirus software, firewalls, and pop-up blockers up to date.
- Never call a phone number that's included in a pop-up advertisement on your computer screen. Cybercriminals spend millions of dollars purchasing pop-up ads through Google and other search engines.
- Never call computer-repair companies that you find through Google and other search engines. I would recommend only calling well-known companies like McAfee and Norton directly for service issues. If you're close enough to an Apple Store or other computer retailer, I believe it's safer to have the repairs done in person than over the Internet.
- If you receive a call from someone offering you a refund on an antivirus software subscription, hang up the phone. How many companies do you know that actually call you to give money back? Do not, under any circumstances, provide them with a credit card number or bank account and routing numbers. It's a scam, and they're going to steal your money.
- If you're the victim of computer tech fraud, make sure you report the incident to law enforcement. It's the only way we're going to stop this type of crime.

CHAPTER 18

Keeping Kids Safe

I WITNESSED A LOT OF BAD THINGS THROUGHOUT MY LONG career, such as people losing their life savings and small businesses having to close their doors after they were victimized by cybercriminals. What could possibly be worse? That's easy: When the bad guys harm children and steal their innocence. We have the resources to hunt these terrible people down and send them to jail for a very long time, but we can never return a child's innocence.

Today, almost every young child has access to a computer, game console, tablet, or smartphone that's connected to the Internet. Being so connected has changed the way kids interact with the world. Most adults have a difficult time keeping up with their own personal cybersecurity, let alone ensuring their children are safe. That's why, over the past several years, we've seen a dramatic increase in cyber-dangers targeting children, including cyberbullying, exposure to taboo material, online predators, and revealing too much personal information and inappropriate photos on social media. Plus, they have access to the dark web, where drugs, weapons, and anything else is available for sale to anyone who gains access.

While investigating the disappearance of a juvenile in May 1993, special agents from the FBI's Baltimore Division and police detectives from Prince George's County, Maryland, identified two suspects who had sexually exploited several juveniles during a twenty-five-year period. Investigators determined that the adults were routinely using computers to transmit sexually explicit images to minors and, in some instances, luring kids into engaging in illicit sexual activity. Further investigations and discussions with experts, in both the FBI and private sector, revealed that computer telecommunications was rapidly becoming one of the most prevalent techniques used by sex offenders to not only share pornographic images of minors, but also to identify and recruit children into sexual relationships. In 1995, based on information developed during this investigation, the Innocent Images National Initiative (IINI) was created to address the illicit activities conducted by users of commercial and private online services and the Internet.

A few months after reporting to the FBI's field office in Syracuse, New York, I participated in my first IINI investigation in the fall of 1995. During

the investigation in Baltimore, investigators examined the subjects' computers and discovered they were trading images of child pornography with individuals across the country. The Baltimore investigation revealed that three hundred and fifty individuals were using the Internet to trade images and communicate, which was a shock to many people in law enforcement. One of the individuals identified during the investigation lived in the Syracuse area, and we had enough probable cause to obtain a warrant to search his residence. Our suspect was a medical professional with a wife and two teenaged children. When questioned, he denied ever looking at these types of images and communicating with other bad guys, but a forensic review of his computer told a completely different story—he had thousands of images of children stored on his computer. He later changed his story and admitted he did look at the photos, but only for a medical research project. He said he kept the project a secret from his office and wife. He eventually pleaded guilty to felony charges and helped us track down other criminals.

Not too long ago, child pornography was difficult to obtain in the U.S. because the risks were too great. The U.S. Postal Inspection Service and FBI did a tremendous job of identifying suspects and apprehending them. These well-publicized sting operations greatly reduced the abhorrent activity—until the Internet came long. The illegal activities started on online bulletin boards and then moved into chat rooms on AOL and Internet Relay Chat, where these monsters found other like-minded predators with whom to communicate and trade. When the Internet really became popular during the 1990s, we started seeing a major increase in the number of online predators. For agents working these kinds of cases, it was like shooting fish in a barrel. I worked dozens of these cases while I was assigned to Syracuse. It was dark and dirty world, and I'm not going to go into detail about the images floating around the web. They would make you sick and give you nightmares.

When I was transferred to Nashville, Tennessee, and promoted to supervisory special agent of the FBI's cybercrime squad there, I gave my first presentation about online safety to a group of inner-city kids between the ages of eight and twelve. My real estate broker's husband mentored many of the kids, and she asked if I would speak to them

about cybersecurity. It was the first time I'd talked to a group of kids in quite a while, and I don't think I realized how accessible computers were to them in 2007. When I walked into the room, I scanned the audience and thought most of them were probably too young to have access to the Internet. I figured I'd better come up with some entertaining stories about bank robberies and fugitives. But then I asked the kids how many of them had searched the Internet. About two-thirds of the audience raised its hand. Then I asked how many of them had MySpace accounts, which was the most popular social media at the time. Almost all of them raised their hands. I jokingly asked the kids how they had access to a MySpace account, because you were supposed to be thirteen or older. They laughed at me. Their answers to my next question surprised me. When I asked how many of them knew more about computers than their parents, about half of them raised their hands.

After doing dozens of cybersecurity presentations to children over the past several years, I have become convinced that most parents are happy to have their children at home on computers instead of running around on the streets. As I gave more and more presentations to the community, I noticed a trend: Most kids believe they know more about computers and the Internet than their parents. And what's even scarier is that most of their parents don't even know what they're doing on the Internet. In 2007, our advice to parents was to keep a computer in public places in the house so they could walk by and see what their kids were doing. Under no circumstances, we said, should a child be allowed to have unsupervised use of a computer in his or her bedroom. It was pretty good advice for a few years—until laptops became more affordable and game consoles and smartphones allowed kids to connect to the web from almost anywhere.

From 2007 until 2011, I supervised the Innocent Images Task Force for the FBI's Memphis Division, which included the area from Memphis to Nashville. We had three full-time FBI special agents and about a dozen full-time task-force officers assigned to the work. The task-force officers were personnel from state and local agencies who were deputized by the U.S. Marshals Service and had the same legal authority as the FBI to investigate federal cases. This program helped the FBI tremendously,

as our mission to combat online child predators was only as good as our working relationship with other federal, state, and local law enforcement agencies. During the years in which I ran the task force, we had so many cases that we were only able to investigate the worst of the worst. One year, my team did an especially outstanding job and arrested and prosecuted nearly thirty child predators. The subjects came from all walks of life, including attorneys, pilots, social workers, police officers, doctors, truck drivers, and clergymen. A lot of these bad guys were trading illicit photos and some of them were hurting kids. As effective as we were that year, though, I remember when a former FBI director acknowledged how big the problem really was. He said we couldn't have made a dent in the crisis with even eleven thousand special agents assigned to these types of crimes. But we didn't have eleven thousand agents; in fact, we didn't even have *eleven*.

After working these types of horrific cases, I made a mission of educating parents about the dangers of child exploitation on the Internet. My message wasn't always well received, however, and sometimes I was even told I was being an alarmist. But I was simply presenting the truth from where I sat as an FBI agent. At times, I became extremely frustrated. I'd talk to an elementary school principal about educating her teachers, and she'd tell me her teachers didn't have time and she couldn't force them to sit through my training. Sometimes, the principal would suggest that I contact a parent/teachers' association. I quickly learned, though, that those kinds of groups are more concerned about fundraising and supporting teachers' needs. It infuriated me that schools were teaching children how to use computers and the Internet, but they didn't think it was important to teach them about the dangers. One of my former agents made the best analogy I've heard about what it's like to let your kids have unrestricted access to the Internet. He said, "You're better off giving your kids the keys to your car, a gas card, and a case of beer, and pointing their GPS toward Bourbon Street in New Orleans."

I did make many presentations to parents, and I would provide them with actual case studies and go into painstaking detail explaining how child predators befriend children on the Internet and spend weeks, if

not months and years, grooming their victims. The bad guys build rapport with kids and often pretend to be children themselves. They'll find common interests and hobbies with children and befriend them. Eventually, the predators introduce pornographic images to the kids, which is done to trick the children into thinking these kinds of photos are normal. Then they introduce photos of adults engaged in sexual activity with children and try to persuade the children to send nude photos of themselves. The ultimate goal, of course, is to actually meet the child for sexual contact. I know it's terrifying to think about, but there's sadly no shortage of adult men who want to engage in sexual activity with underage boys and girls.

As horrifying as it sounds, I felt it was important to share this warning with parents. Our task force found these monsters in chat rooms, where our officers would pretend to be underage boys and girls. They'd spend hours online with child predators, and, once they sent us pornographic images of children, we tried to set up face-to-face meetings with them. As soon as they exchanged illicit images of kids, it was a federal crime. We wanted to get them off the streets so they wouldn't hurt any more children. The predators almost always took the bait and arranged to meet us. I recall one occasion when the bad guy we arrested had a duffel bag with him. Inside the duffel bag were a stun gun, handcuffs, lubrication, and sexual devices. Being a father of two children, it was absolutely terrifying to investigate these crimes.

During my presentations with parents, I always asked, "Is it important for your children to understand the difference between *real* friends and *virtual* friends?" Almost every parent agreed that it was a very important distinction to make. Then I asked the parents how many friends they had on Facebook. When I asked the parents if they had five hundred, nearly every hand in the room went up. It would go from five hundred to a thousand to one thousand five hundred friends. One parent jumped up and said, "I have two thousand friends!" It appears there are a lot of *adults* who can't tell the difference between real friends and Facebook friends; if a parent can't tell the difference, how are we supposed to teach our children?

Our kids have near-limitless opportunities to interact with virtual friends on platforms their parents have probably never heard of. When my own children were in kindergarten, I explained that the Internet is fun and a great tool for learning, but that there are dangerous places and people on the Internet who would like to hurt them. Whenever I said that in a presentation, though, there was always a mother in the audience who would object. She'd say, "I don't want to scare my children by telling them about all the bad things in the world." Then I would have to explain that refusing to at least make them aware of the threats put her kids at much greater risk.

Having your children understand basic threats on the Internet is a critical first step. As a parent, the day you provide your child with an Internet-connected device, whether it's a computer, tablet, or smartphone, you need to have a serious talk with them. You need to realize that, when your child gets online, he or she has access to excessive violence, hate speech, risky or illegal behaviors, and pornography. You can find any of the first three on YouTube in only a few minutes, and pornography is so readily available on the web now that your kids are going find it no matter how old they are. You can invest money in blocking software like Internet filters and pornography restrictors, but children are smart enough to find ways around it—or they'll just go to a friend's house.

Talking to your kids about the difference between right and wrong is the most important step. If your child comes across something offensive and they come to you, then you have probably succeeded as a parent. Make sure you listen attentively and try not to judge them too quickly. Tell them it's not their fault and ask questions. One day, when my son was about nine years old, he said he wanted to talk to me. Instantly, I recognized that something was wrong. He wasn't immediately forthcoming, but he eventually admitted that he'd seen something on the Internet that was inappropriate. We talked about it, and I assured him that it wasn't his fault. I was relieved he trusted me enough to talk about it, and then I explained the dangers of the Internet to him once again.

I recently gave a cybersecurity presentation to a group of parents of middle school students at an exclusive private school. There was one

mother who was shocked by what I was telling her, and she finally asked me, "So, you're saying that I'm a bad parent if I don't know who my daughter is talking to on the Internet?"

I replied, "Of course not. It's impossible to monitor our children twenty-four hours a day. However, if your daughter meets someone on the Internet, and she's never met that person before, and then they decide to meet at the mall and you don't know anything about it, *then* you're a bad parent." I explained the best course of action was to sit down with your kids and have a serious discussion about the dangers of the Internet.

I could write an entire book on Internet safety for our children, and every parent should make it a point to access the National Center for Missing and Exploited Children's website, www.netsmartz.org, which offers great resources, presentations, and games for kids to learn about online safety. Our kids must realize that there are bad guys on the Internet and they should never provide identifying information to people they don't know. They must know the difference between real friends and virtual friends, and we as parents must be aware of what our kids are doing online. Most importantly, you must provide a home environment in which your kids can come to you with questions and concerns. Listen to them without judgment. It's the only way we're going to keep our children safe.

HOW TO AVOID BECOMING A VICTIM

- Parents must understand that there are no rules on the Internet, and that your children can be exposed to pornography, inappropriate material, and hate speech. Keep this in mind when making the decision about giving them access.
- Always be aware of what your children are doing online, including what they're searching for and which websites they're visiting. Install content filters if necessary to be extra safe.
- Realize that there is no shortage of people on the Internet who are looking to harm children.
- Make sure your children understand the difference between real friends and virtual friends.
- If your children have their own social media accounts, their usernames should never be their actual first and last names. That information is too easy to find on Google and other search engines, making it easy for online predators to find them.
- Children should be educated about never providing their name, address, date of birth, or telephone numbers to anyone on the Internet.
- Children should never send photographs of themselves to strangers they meet online.
- Teach your children that anything they write and post on the Internet, including tweets, comments, photographs, and videos, is probably going to stay online forever.
- Set house rules and limit your children's time on computers and other devices. Talk about rules and the consequences of breaking them.
- Teach your children not to open email from strangers, not to respond to hurtful or disturbing messages, and not to arrange face-to-face meetings with anyone they meet online.
- Make sure your children know they can come to you about questions and concerns about material they see on the Internet.