# PROTECTING YOURSELF FROM SCAMS & SWINDLES

This information is taken from *Scam Me If You Can*, by Frank W. Abagnale (AARP, 2019). As a young man, Mr. Abagnale became a self-taught scam artist who successfully worked many different swindles and cons before finally being caught and convicted (as portrayed in the movie *Catch Me If You Can*). He later became a consultant for the FBI, and is now recognized as one of the leading authorities on how to recognize and guard against various schemes, scams, and the rip-off artists who perpetrate them.

In 2017, there were 16.7 million victims of fraud in the United States, and they lost a total of $16.8 billion. Scammers are everywhere, and are constantly developing new schemes to take advantage of the gullible and unwary.

**Ten Signs You're About to Be Scammed**

1. *A request for action:* A scammer may tell you to "write down what I'm going to tell you—it's important." Once a con artist gets you to do something, he has taken control of the situation, making you more vulnerable.
2. *Demand for fees:* Any lottery, prize, or sweepstakes that requires a payment to collect your "winnings" is almost certainly a fake.
3. *Guarantees:* Promises that you'll "double your money" on an investment are bogus; no one can absolutely guarantee future results.
4. *Act now or you'll miss out:* Con artists often try to create a sense of urgency, hoping to deceive or manipulate you.
5. *Request for personal information:* If you give out information on your bank accounts, Social Security #, health background, passwords, outstanding loans, etc., scammers will find ways to use this information against you.
6. *Grammatical or spelling errors in emails:* These often indicate the sender is falsely representing himself, and is actually from another country. Beware.
7. *No address:* If a letter or email has no street address or contact information, be very suspicious—it's probably a scam.
8. *Request for untraceable payment:* Legitimate businesses don't require you to pay for products or services by Western Union, gift cards, or other untraceable means.
9. *Access to your computer required:* Never give an unsolicited caller remote access to your computer, even if he claims he wants to fix a "problem"; he probably just wants access to steal your passwords and personal information.
10. *Unsecured web addresses:* A secure site is indicated by "https," not "http." Never send personal or financial data to unsecured sites. Web browsers can help you find legitimate e-commerce sites: a small closed lock symbol at the left end of the address bar means the site is secure (while an open lock indicates the opposite).

**What to Carry in Your Wallet**

According to Mr. Abagnale, "Your wallet [or your purse] should not contain your life. Don't carry what you don't need. Here's my recommendation for what to carry:

- your driver's license
- a copy of your health insurance card
- a copy of your automobile insurance card
- a copy of your car registration
- a copy of your Medicare card with all but the last four digits blacked out
- one or two credit cards
- your identification card for work, and
- a small amount of cash for incidentals.

Beyond these essentials, what else do you really need? Blank checks in your wallet [or purse] are a really bad idea—they give the thief access to your bank account."

Also, "Leave your bank deposit slips at home. These slips contain exactly the same information as your checks and are a key that unlocks your bankbook.

"Do not carry your Social Security or Medicare or insurance card in your wallet on a regular basis. You'll need your Medicare or insurance card only the first time you visit a provider. Other than that, keep these cards at home in a secure place" (pp. 56ff).

**Seventeen Safeguards and Suggestions**

1. Always wait at least 24 hours before making any financial decision; scammers want you to accept their "offer" before you've had a chance to consider it carefully.

2. Remember that if the IRS contacts you, it will do so *by mail*, not by email or a phone call. Such bogus contacts—which may involve threats to arrest you or freeze your assets—are certain signs of a scam. Don't open emails supposedly from the IRS, and hang up on a caller who claims to be an IRS agent. (If *you* contact the IRS, however, a legitimate agent may return your phone call.)

3. Remember that banks and financial institutions never send their customers emails asking them to click on links to "verify" personal information.

4. The Social Security Administration will never contact you to verify your S.S. #; don't respond to such an email or phone call.

5. A scammer trying to sell you something will (a) emphasize its value and scarcity; (b) try to flatter you (to get your guard down); (c) create a sense of urgency; and, if all this fails, (d) use threats or aggression. Don't play along; hang up if any of these things occur.

6. Share as little personal information as possible with a caller; deflect his questions, and ask more questions than you answer.

7. Use a credit freeze (also called a security freeze); this prevents a thief from opening new credit cards in your name. (You can unfreeze your credit reports if a bank, employer, or other legitimate entity needs to check your credit, and then reinstate the freeze.)

Also, take advantage of free credit reports. You're entitled to one free report every year from each of the three nationwide credit-reporting agencies. You might ask Experian for a free report in January, TransUnion in May, and Equifax in September. To do this, go to www.annualcreditreport.com., or call the numbers or use the websites given below.

8. Don't keep papers with valuable information in your car, including your insurance and registration cards. Instead, keep copies of them in your wallet, or pictures of them on your cell phone (this is usually sufficient if you're pulled over by a police officer).

9. Be careful about using public Wi-Fi; the information you send on such a network can easily be intercepted. As an added level of security, set your devices to airplane mode (which essentially turns them off when you're away from home).

10. Never give out personal medical information in response to an unsolicited email or phone call.

11. Verify ID: if someone claims to be calling from a government agency (whether federal, state, or local), utility company, or any other organization, ask for the person's name or identification number. Then hang up and call the agency or organization he or she claims to be representing.

12. If you get an unsolicited phone call from Microsoft, Apple, or any other computer company, warning that you have a virus, it's safest to assume the call is a scam.

13. Some scammers will record your spoken words on a phone call, hoping to use them against you. If you answer "yes" to any question (even just "Can you hear me?"), that voice recording can be used to authorize fraudulent charges by telephone. Beware.

14. Block unwanted sales calls by using the Do Not Call Registry (www.donotcall.gov, or 888-382-1222); you can register up to three numbers (but charities, political groups, debt collectors, and pollsters can still call you).

15. To avoid robo-calls (which occur more often on Tuesdays and Fridays than on other days), simply don't answer phone calls if you don't recognize the number. (A legitimate caller will usually leave a voice mail.)

16. Realize that there are many charity and crowd-source scams (even including heart-warming stories reported in the media). To check on a charity's legitimacy (and also to see what percentage of your donation will actually be used for its stated purpose), go to one of these websites: www.charitynavigator.org, or www.charitywatch.org/home.

17. Restrict your use of social media to no more than thirty minutes a day. Not only will this make you less of a target for scammers; a 2018 study by the University of Pennsylvania showed that using social media more than half-an-hour a day can cause depression.

**Credit-Reporting Agencies**

*Equifax* - 800-685-1111
www.equifax.com
*Experian* - 888-397-3742
www.experian.com
*TransUnion* - 800-888-4213
www.transunion.com