Common Internet Scams and How to Avoid Them

By Jim Broussard

The IRS Scam:

How it works - Someone will call or email you claiming to be from the IRS, and that you owe a large amount of money. They will demand you pay up now or be arrested.

What to Do: Hang Up. Seriously, you can just hang up. The IRS is not legally allowed to communicate via phone or email, only by snail mail. Anyone who calls from "The IRS" is a scammer.

The Security Scam

How it Works: You get a message on your computer saying you have a virus, or you get a person trying to sell you a security system for your house.

What to do: If you get one of these messages, delete it and run your actual antivirus. If someone comes to your door selling this stuff, ask yourself "How long have I lived here and how often has something happened?" and then think about how much they're asking you to pay a year.

"Grandma! I'm in Jail and need Bail Money!"

How it Works: You'll get a call or text from someone claiming to be a relative (usually a grandchild) and that they are in trouble. Usually this involves legal issues like needing Bail, but it can involve any situation similar.

What to Do: Call a different number that allows you to contact that person, if possible, or someone who you trust. Confirm the person is in trouble before proceeding.

The Nigerian Prince

How it Works: This is an old one, and it has many variations. What they all have in common is that they pretend to be a rich person who want to share their wealth, if you will just give them a bit to get started...

What to Do: These cons are as old as time. The best course of action is simply to be vigilant. Ask yourself "if he's so rich, why does he need money from me"?

The Foreign Girlfriend/Boyfriend

How it Works: You will find yourself contacted on Social Media by someone, usually a person with a very good looking young profile pic. They'll talk to you, maybe even befriend you, and act like they are into you. Eventually, once you're involved with them, they'll ask for money to help them out, or perhaps to come see you.

What to Do: Remember that just because they have a pretty picture doesn't mean anything. This scam is very hard to avoid because the person seems so genuine. But rest assured, their interest in you is in your pocketbook, nothing more.

The Open Warrant

How it Works: You will get a call, email, or text from someone claiming that there is a warrant out for your arrest, usually for an unpaid fine. They will ask you to confirm some information and then usually inform you that you can put a hold on the warrant by paying the fine that you owe.

What to Do: Once again, just hang up. They are lying to you about both the fine and the warrant. If you feel anxious about it, consider this: Why would the police call you to tell you there is a warrant instead of simply arresting you?

"I need your Info..."

How it Works: Someone will call or email you claiming that they need your information for something. It might be a contest you won, or there was an 'IT incident', or any number of excuses. The important part is that they need your information and need it now.

What to Do: This is called "Phishing", and it is the most common form of data breach. Do not give out your information, period. Especially not your username or password. If you're worried about it being from IT, IT doesn't need it. No one will ever legitimately need to get your info from you.

Generic Spam and Clickbait

How they Work: "OMG, Watch this Vid!", "10 Things you won't Believe!", "What happens when [X]?", "You are our Millionth Visitor!" We've all seen these a hundred times. Ads on screens, random links popping up everywhere.

What to Do: Just don't click on them. The ads are Fake. The story is nonsense. The videos aren't nearly as entertaining as one might think.

General Tips for Avoiding other Scams:

- Use a different password for each account
- Make sure you use a strong password
- There is a Password Strength Checker at the end of the Booklet
- Don't be afraid to keep a little booklet of passwords, but keep it in a safe place at home
- Never answer questions Online about your identity
- NEVER give out your Social Security Number
- If someone says they need an answer from you NOW...the answer is No
- If someone asks you to pay in Gift Cards, they're scamming you
- The same goes for if they ask you to pay in anything weird
- If you didn't enter a contest, then you didn't win one
- If it sounds too good to be true, then it isn't true
- Always ask yourself: "What is the other person trying to get from me?"
- If you get a strange email, check the sender's address. Scammers often have weird ones.
- If they're threatening you, then they're scamming you

"Trust But Verify"

General Tips for Avoiding Misinformation:

Misinformation is one of the biggest problems that plagues the Internet, where social media gives a microphone to everybody with an idea, good or bad. The below tips, however, can help you avoid some of it.

- Only watch the News once a day
- If your News source only makes you mad, find a new one. They're upsetting you for views, not informing you
- Social Media is not a reliable information source
- Wikipedia is, and is shown at the back of this book
- Find a reliable fact checker
- Beware of Biased Sources
- You can spot a biased source by watching for various logical fallacies
- Don't be afraid to Google things you don't know
- Always check the site an article is on
- If someone claims to be always right, they're lying to you
- If someone claims that their way is the only way, they're lying to you
- Always remember: It's okay to be wrong if you admit it and learn
- If a claim sounds outlandish and weird, verify it
- Finally, remember that the start of Wisdom is found in the sentence "I don't Know"

The saying across from this page is the ultimate key to avoiding scams and misinformation. Trust in your fellow man, but always verify and double-check your facts. Even if the person doesn't know it, they could very easily be wrong.

If you or a loved one gets scammed:

1. Don't Panic. This can be fixed.
2. Ask for help if you need it and can ask for it
3. Try to discern exactly what information was revealed, if you can.
4. Contact any Institutions involved via phone or in-person and inform them
5. Cancel any cards associated with the scam
6. Change any information that was revealed
7. Double check to make sure everything was fixed as best as could be
8. Review these resources again
9. Don't feel bad, everyone falls for these sometime

If you get a Data Breach Email:

1. See who it is from and verify it is real
2. Change your password for that website, if you have one
3. Call them on the phone to discuss what happened
4. While calling, ask what info was leaked
5. After that, ask about what compensation is available for this

Some Useful Websites to work with:

Wikipedia (www.wikipedia.org)
Despite its reputation in schools, Wikipedia is a very reliable source of general information and knowledge about a topic. Googling "[subject] wikipedia" will almost always be enough to give you a working knowledge of the subject in question.

haveibeenpwned (haveibeenpwned.com)
This highly useful website will allow you to enter your email address and see if it was involved in any number of data breaches. If it was, follow the steps above.

cisa (www.cisa.gov)
This website is more for businesses to work with, but they are the United States Cybersecurity branch, and they have a number of resources available for use and to help with problems.

Security Password Checker (https://www.security.org/how-secure-is-my-password/)
A highly useful tool that allows you to type in your password and see how long a computer will take to break it. If you are making a new password, try for at least 100 trillion years.

Snopes (www.snopes.com)
The original Internet Fact Checker, this is the one that I personally recommend using, though there are others out there.