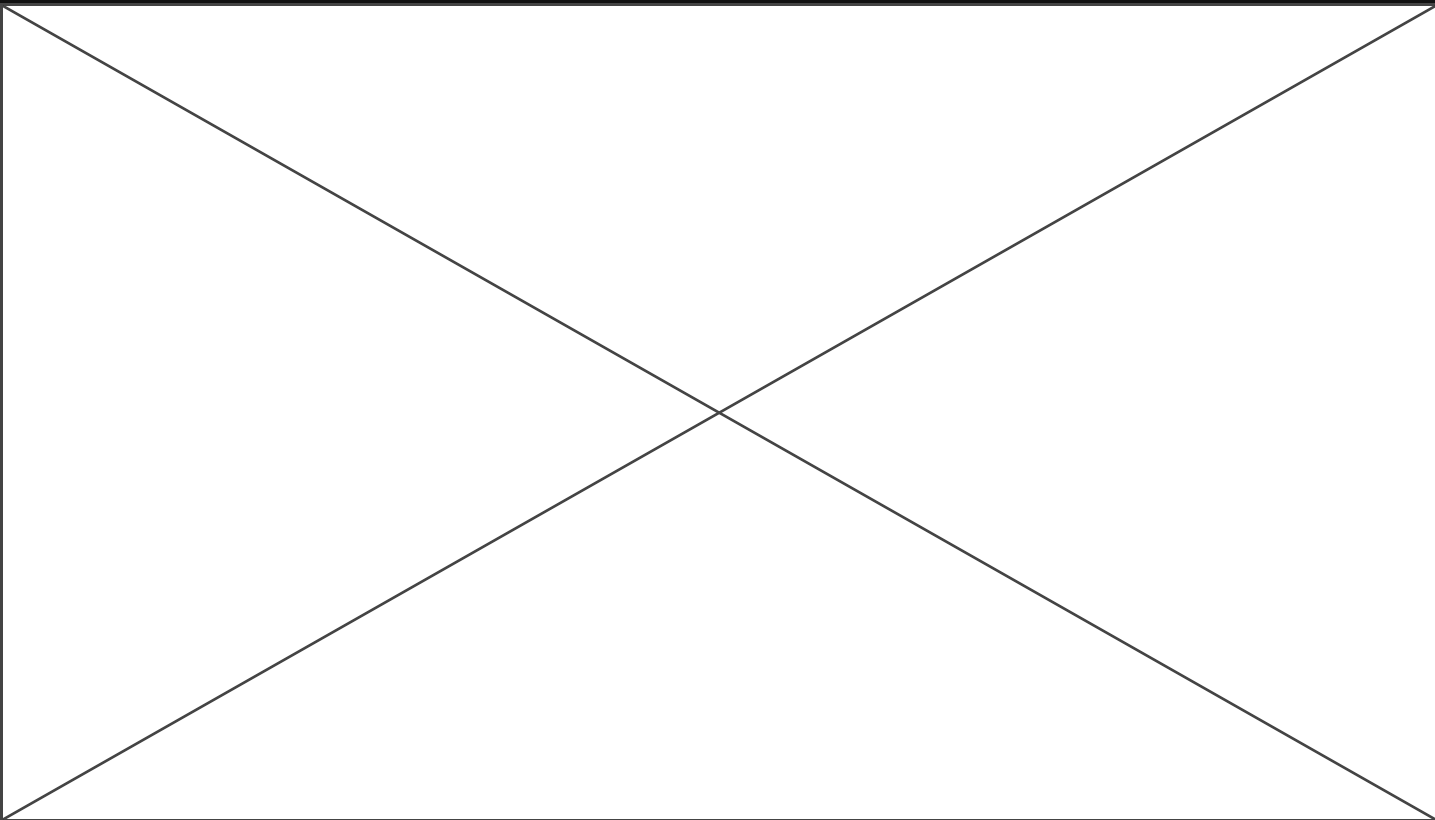I have provided technical support, as my day job, for the last 12 years. The majority of the technical support that is needed by the everyday users is basic.

The biggest obstacle to accomplishing the technical support is fear. That fear has two parts, first, the fear of looking foolish or second, fear that they will make an issue worse.

I cannot count the number of times I have worked with someone who had just 'delt' with an issue, rather then ask for help.

They fear that someone is going to make them feel foolish for not knowing how to resolve the issue themselves.

To this I say, that I cannot bake bread. Odd huh. Usually gets the person I am helping too.

The key is that we don't all have to be good at everything we do, so there is no foolishness or shame in not knowing how to solve a problem you have not faced before.
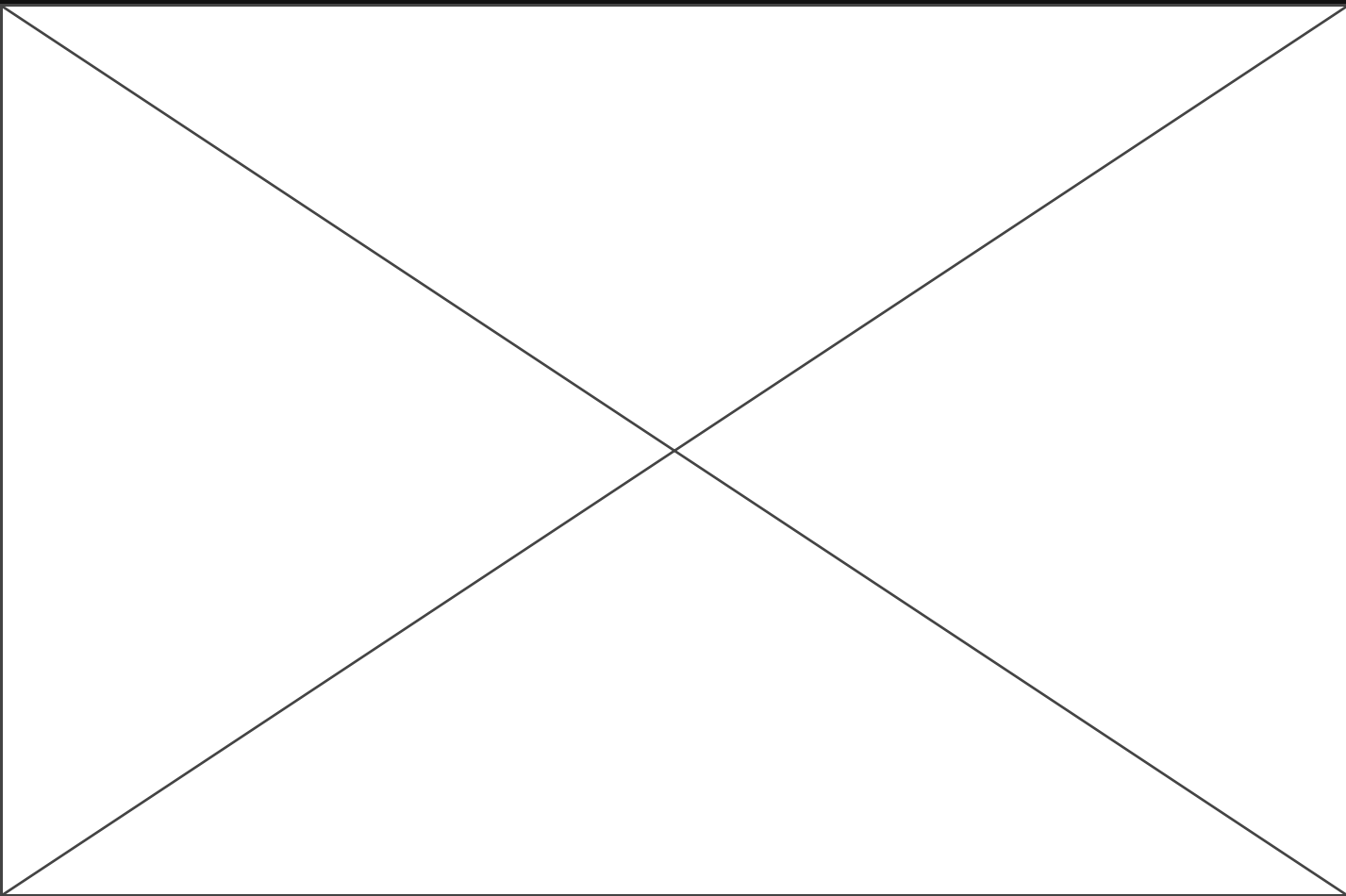


The second reason most people will not try to solve an issue is fear that they will make an issue worse.

It is true that if you try you can fail.

There are things that everyone can do both in preparation and when something has gone wrong that won't make things worse. These things will also often fix the problem or can protect you as you navigate the technical world.
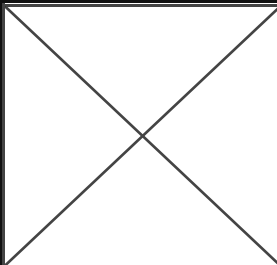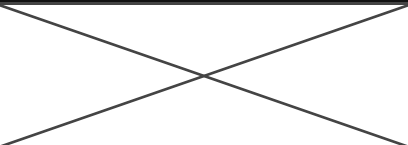
# Basic Troubleshooting

## Power Cycle

Devices are intended to work.

Almost every device has a power on process that checks for failures and in most cases can resolve them. It is the most common question asked in technical support "Have you power cycled the device?

What device – any! This applies to your computer, your phone, your TV, your modem, or router (network). Like I said, electronic devices are intended to work.
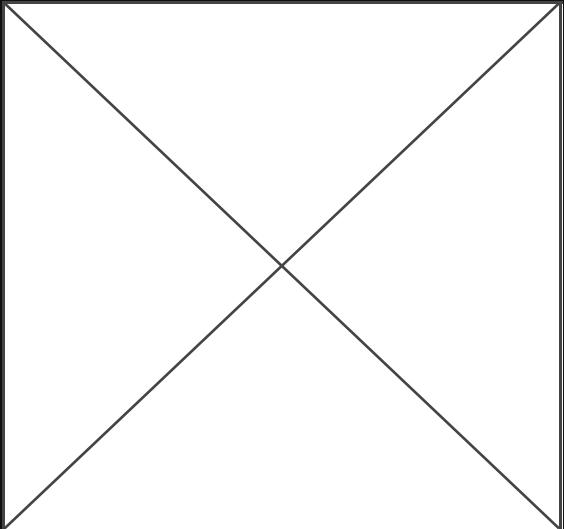
**How to properly power cycle:**
**Option 1: Each device has an intended power off cycle.**
- On a PC computer: Start Menu > Power > Shut Down
- On a Mac computer: Apple Menu > Restart
- On an iPhone: Press and hold the power and volume up button, swipe Power Off.
- On an Android: Press and hold the power button, select Power Off

**Option 2: Some devices have a Hard Shut Down Process.**
- On a PC or Mac computer: Press and hold the power button for 10-15 seconds (count slowly) until all lights and sounds stop.
- Network equipment: Unplug from power.

## Backup

You or someone you know may have lost information, or pictures, when their last computer failed. Like any machine, computers can and will fail. This information can be protected by backups.

By storing your information in more then once digital location you provide yourself data security to ensure that you don't loose precious memories. One essential is to have one source of original information and that is duplicated to the second back up location. Do not use the backup data unless the original becomes unusable.
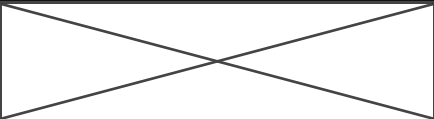
Types of Backup:
- On On a second computer device
- On a USB or remote storage device
- On a cloud storage device

Best Practices for Backup:
- Do it on a set schedule
- Check the backup to ensure that all your data is located there.
- Keep the backup in a different physical location then the original data.
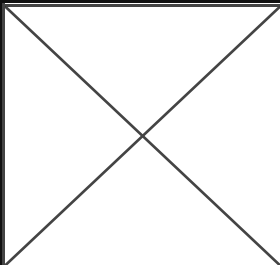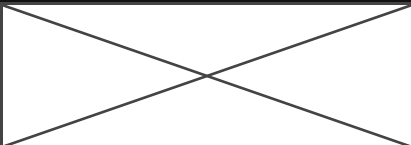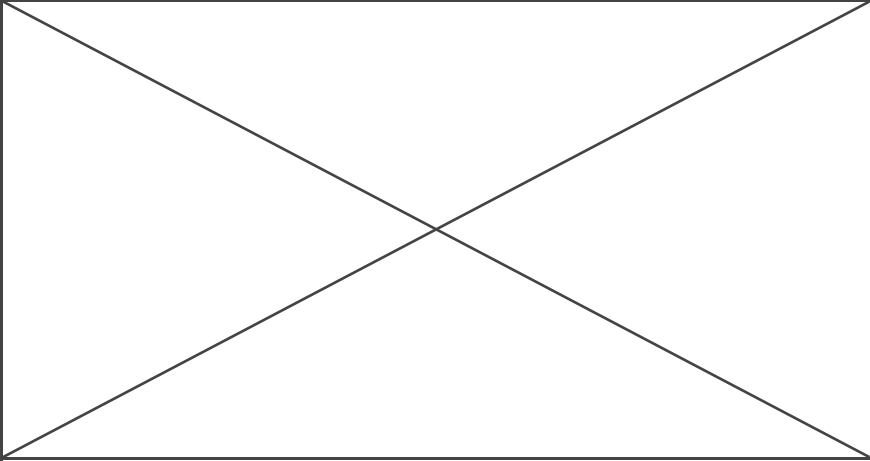
## Security - Email, Internet, Password

General Security

### If you didn't ask for it, are not expecting it, don't open it!

The key to security on the internet, with your phone, and email is to be skeptical.

The most common form of "hacking" someone's information is to get them to give you the information. They send an email and pretend (spoof) the identity of someone that you trust. They then offer you something or ask you for something very simple, but then they use that piece of information again to get more access or information.

So consider – is your bank going to text your about a banking error? Are you going to receive a refund through a link in your email? Did you expect an invoice that is asking you to enter your password? Is that really the email address that your friend has always used? How likely is it that tech support called you before you were aware of a problem? Or a pop-up number appears on your computer screen at the exact time you need it?

The key to each of the types of scams that commonly compromise accounts is they play on people not paying attention to the details. So always ask you self – Am I expecting this? Did I ask for this?
The key is that if you are unsure, follow up with the source via a different method of communication. If someone sends you an email, call and confirm it was them. If someone texts you, email them, or call them on a different number.
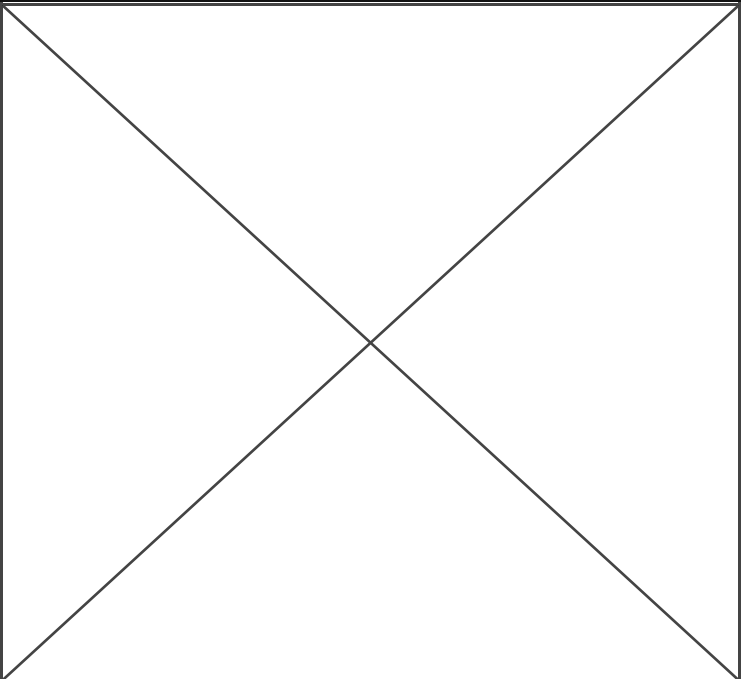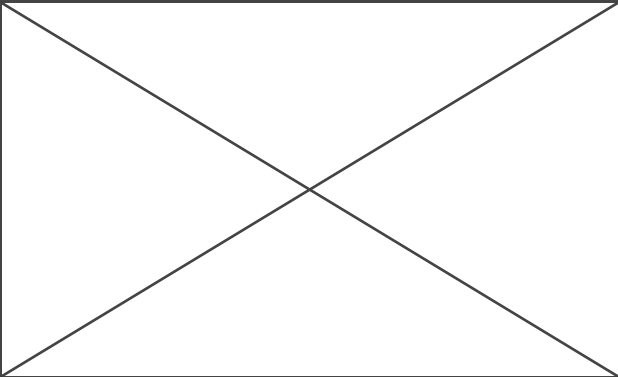


Password

How many passwords do we have…. dozens and dozens. Each system has a different requirement for passwords, so we create new ones. Sometimes we use the same password in multiple places. We keep note pads or documents with these passwords lists and then when we change passwords our documents get out of date.

The key to password security is that we need to ensure we have a method of remembering our passwords, but also ensuring that that option is secure from other user's access.

I have three recommendations for those that find they are always losing track of their passwords:
- Write your essential passwords in once place and ensure that it is secure.
- Have a different password for any banking or financial information. Different (significantly) from any of your other passwords.
- Utilize a password manager. For iPhone users – There is a password manager in settings. For Android users – There Chrome to remember your passwords. For PC users – You can also use Chrome browser signed into your Google account For Mac Users – There is the Mac key chain. There are also a number of types of software that provide the same feature. The reason a password manager is recommended is because now you can use passwords that are more complex. Passwords that have no common word but are strings of letters, numbers.



The final advise I have regarding passwords is that you should only use them or enter them or share them when you fully trust the situation. If you plan to go to a website, if you are choosing to sign in to your email, or if you are opening your banking intentionally. If something pops up asking for your password, and you were not intending to use that service, just close it. Don't use your password if you don't intend to, pop ups or redirects are not your friend.