# Powering and Protecting Battery-Powered Devices in Quasi-Troubled Times

*From paying bills to fixing the kitchen sink, computers and other battery-powered devices have become indispensable. As our society continues to move towards a cashless system, it will become increasingly impossible to purchase everyday needs and pay bills without using electronic devices.*

At the same time, multiple threats within and outside of our country can render these and other devices useless. No matter whether a power plant becomes inoperable, fuel costs are too high, a cyber attack wipes out key systems, or a nuclear EMP strike occurs, the end result is your devices will not work unless you take steps now to protect them.



## Types of Devices that Need Coverage

Aside from your phone or tablet, there are other battery-powered devices that you will want to keep operational for as long as possible during a crisis. These include:

- Building and repair tools such as screwdrivers/drills, saws, and other battery-powered appliances.
- Medical devices such as hearing aids, mobile assistance, and diagnostics
- Battery-powered mobile assistance devices
- Mobile hotspots, or other connectivity devices used for

tethering
- Flashlights, clocks, and RV/battery-powered camping gear for cooking, heating, and cooling.
- Laptops, wireless keyboards, and mice.
- Battery chargers for AA, AAA, D, C, and 9v batteries.
- Emergency radios and other communications devices not based on the internet

# Powering Devices

Phones and tablets today require far less power than laptops and other devices that you might use to access communications points. Most can be charged with anything from a solar-powered crank radio to a power bank that is, in turn, charged by a small solar panel kit. Other items require more power. This can range from 12 to 24 volts. For example, many power tools use a 20v power pack, while a battery-powered wheelchair may require 24v.

Choosing a small-scale power-generating system can be complicated. You will need to have a good idea of your routine device usage as well as how long it takes to charge each device. Before a major grid failure occurs, you should be fully able to charge all your devices without relying on a wall outlet. Depending on your interests, you can integrate this into daily life, or only practice from time to time.

Here are two types that I recommend:

- First, a small-scale system that you can use to charge up devices that rely on USB power. These systems can fit easily into a backpack and can be put in areas where larger panels might not fit.
  These days, you can find them in several configurations including ones that are bundled with crank-powered radios. Alternatively, you might want a system with a

battery you can swap out as well as larger panels.

- Second, a larger battery pack and solar panel combination capable of providing 110 volts. You can use these to charge up larger batteries for power tools and other devices. They can also be used to charge up smaller battery banks that you can use for phones, hotspots, and other devices. When choosing a system, make sure that you can easily swap out the battery so that you can have one charging while you use the other one.

## Faraday Cage Options

It’s hard to say how distant or near we are as a society from experiencing a nuclear detonation. Nevertheless, hostile agents may look to use an EMP first as opposed to something that will cause immediate high infrastructure and civilian casualties. The only way to protect your electronic devices and power chargers from EMP events (both natural and manmade) is to use a Faraday cage.

As with powering your devices, there are different kinds of Faraday cages to consider. For larger items, I recommend making your own Faraday cage from a metal trash can lined with a suitable material designed to stop RF and EMP interference.

Not so long ago, mesh liners were sufficient for creating a Faraday cage that would block all signals in and out of the cage. Today, phones and other devices can send signals that are in a frequency range that can get out of the cage.

You will need to do some very careful research on the frequencies sent and received by your devices to determine what kind of materials and construction elements to look for in a pre-fabricated cage. In some cases, you may either need to purchase older devices that don’t send or receive certain frequencies, or build your own Faraday cage to accommodate

newer technologies.

It is also very important to protect the devices you use most often such as your phone, charging devices, and payment cards as a matter of routine. Some useful Faraday cage options include:

- a dedicated RFID-blocking wallet for your payment cards
- an EMP/RFID blocking envelope for your phone, hotspot, and charger
- a second EMP/RFID blocking envelope for your library device, charger, and supporting drives or chips.

Even though pre-fabricated Faraday cages may not prevent signals from getting out, they may be enough to block incoming to a sufficient level.

# Protecting Your Information and Devices from Malicious Threats

There are four ways malicious actors can get access to your devices:

- through the SIM card
- WIFI access
- NFC (Near Field Communications)
- when your device is attached or tethered to another device that has communications access. There are many devices in this category including hotspots, phones used as tethers, laptops, and desktop computers connected to a network. Today, there are also power chargers that have connectivity ports.

Some people mistakenly believe that if they don’t have access to some kind of connectivity service, they don’t have to

worry. Bear in mind, however, that things like the 911 network don’t require having a subscription to a mobile phone plan. This alone indicates that your devices can always be reached, even if it is via a system that isn’t readily available to consumers.

Similarly, if a major network provider is hacked, it’s possible malicious actors can use that hardware to reach any device even if there isn’t a paid subscription plan. Considering the resources available on 5G networks combined with NFC, the threat may be much larger than anyone realizes.

A Faraday cage can only go so far when it comes to protecting your device from these kinds of threats. As different frequencies are developed, there is a chance they will be able to breach mesh-based liners and, from there, damage the device. Nevertheless, this is the best way at the current time to protect your devices when they aren’t in use.

Insofar as when the device is connected, there is no such thing as a solution that will work 100% of the time. You can use different apps that scan for threats as well as keep up with security and other patches to the system. Beyond that, keep an eye on your device for suspicious battery drainage or other indicators that the device is using more power than usual.

When in doubt, don’t hesitate to reset the device to factory settings and re-install. As long as you have backups of all your data and know how to do the reinstall, you should be fine. You can also practice on older devices or others so that you have a good idea of the process.

# Protecting Your Electronic Survival Library

It is useful to have a dedicated device for storing videos,

articles, ebooks, and other materials you might need during a crisis. This could include everything from how to splint a broken bone to starting a fire safely.



Depending on the nature of a cyber attack or other threat to electronic devices, it is possible everything can be wiped out or corrupted to a level that is of no use to you. Here are some ways to avoid those problems:

- Go back to older technology. For example, I often recommend obsolete PDA organizers that don't have a built-in modem or any other communications access. These have a good bit of storage area and can display many different kinds of content.
- Keep your data on USB flash drives and micro cards. Make sure that you have an adapter that enables you to plug the drive or card into any device that you want to use to access the information.
- If you opt for a 2G or 3G enabled device, make sure there is no SIM card in it or ability to access a WIFI network. You can also keep the battery out and only install it when you are testing the device or using it in an emergency. Never store the data chips within the device.

There is a chance that society will collapse to a point where electronic devices will no longer be available. In current times of quasi-chaos, however, it is almost impossible to do

without these devices. It is very important to know how to protect phones, power tools, and other devices in situations where you still need them, but are not yet in a situation where they are of no, or little use.