Juice Jacking

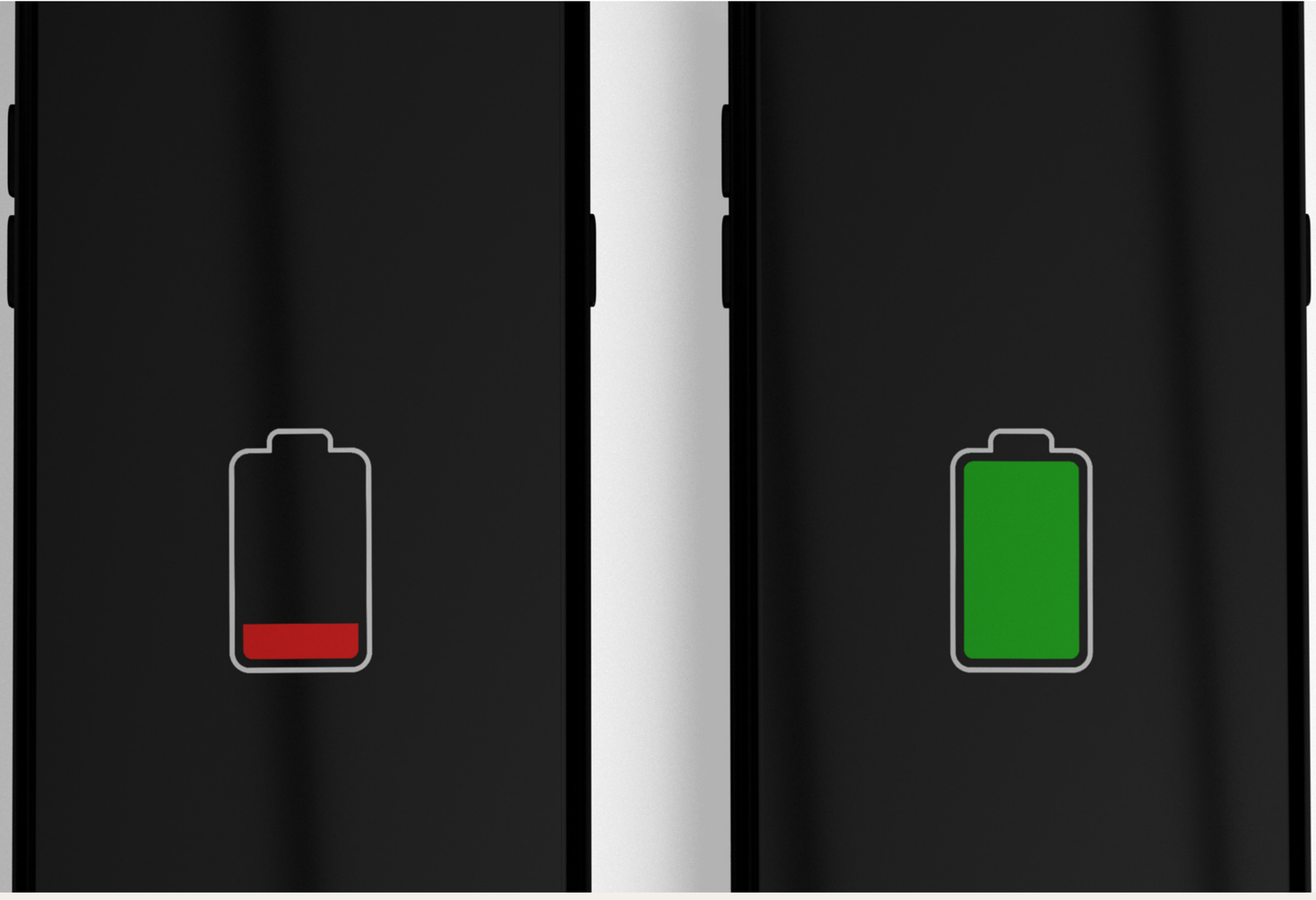
have you heard of this??

Security

At our Photo Managers conference in Orlando a couple weeks ago, we had a privacy and security expert lead a talk in keeping our electronic data (and our clients' data) safe.

I attended this session thinking I would learn about dangers surrounding Cloud Storage sites. It turns out Cloud Storage sites are not where the danger lies.

Most Cloud Services offer end-to-end encryption, keeping your photos/videos/information safe in transit.



So, what is Juice Jacking?

Juice Jacking is a cyber attack where hackers place malware on public USB ports or USB cables...at stations where you plug your phone in to charge. What this malware does is allow a transfer of data from your phone/device to their device. They then have access to all the data stored on your phone.

Where could this occur?

- airplanes
- airports
- rental cars
- malls
- hotels/hostels
- charging stations
- coffee shops
- restaurants
- train stations

What can you do?

If you are travelling, or out and about, and need to charge your phone...

- Use your own cord and AC adapter and plug into a regular outlet.

- Charge an external power block at home and carry it with you. When you're on the go, you can simply plug into the power pack in your bag.

- Purchase a Charge-Only Cable. No data will transfer through this cable but your device will still charge.

- Purchase a USB Defender. These are adapters you can use to plug your cord into if you NEED to use a public charging station. They block any transfer of data while allowing your phone to charge.

Examples of these on Amazon

I hope this helps...

There is so much to know about the constant changes in technology, our online presence and keeping ourselves, our clients, and our families safe.

We want to help you protect not only your family memories (photos/videos) but all your other personal information.