What is RF Shielding and Why do Survivalists Need It?

Radio frequency shielding is used to protect privacy, prevent auto theft, the theft of credit card information and sensitive data, to prevent tracking, and to protect microelectronics from damage by powerful RF signals and HEMP.

RF Shielding Products

You probably already use RF shielded products every day. Here are a few products people use and why they use them:

- **Wallet** – To prevent theft from bank and credit card accounts and identity theft by skimming. You can also put the card you use to pay travel tolls in an unshielded pocket and your other cards inside, preventing any confusion about which method you wish to use to pay travel tolls as you roll past the machines.
- **Key Pouch** – To prevent auto theft.
- **Passport Cover** – To prevent identity theft.
- **Neck Wallet** – To prevent identity theft during travel.
- **Pocket Liner** – I like the EM shielded pocket liner by SCOTTeVEST. I don't think they make them anymore, but other companies do. Just use your search engine to find one and drop your phone, keys, wallet, and whatever else you need to protect inside.
- **Faraday Bag or Cage** – To protect vulnerable microelectronics from hacking or HEMP.
- **IT Forensics Pouch** – Prevents devices collected as evidence from connecting to cell towers or Wi-Fi, making it possible for a user to initiate a remote wipe, overwrite evidence or make the device harder for authorities to gain access to.

Even electronics such as cellphones, computers, and two-way radios feature shielding. If radios weren't well shielded, circuits would blow when they transmit. For this reason, two-way radios are perhaps less vulnerable to events such as HEMP than people worry. Although I store some of my radios in a Faraday cage just in case. Commercial amateur radios have reportedly survived some HEMP simulations pretty well, but none of the tests I have seen in the public domain have simulated HEMP form a SuperEMP weapon.

Is Card Skimming Still a Threat?

That depends on the device, the card, and the criminal. Some academics believe that it's not a threat because it's cheaper for criminals to buy credit card info off the dark web than to be expensive card skimming gear and they point out that there is no data to support the fact that it's a threat. They say that most of the evidence to support the fact that it is a threat is provided by security testers and additional security measures have patched some of the weaknesses that they exploited.

I think that's kind of like arguing that government spying wasn't a threat until after Snowden leaked proof that it was happening. If you are articles by writers like me on sites like Survivopedia, there is a good chance that you knew the government was spying on you long before the Snowden leak. Plenty of us wrote about it years before we could prove that was, in fact happening. The only thing the Snowden leak changed was that the leaked documents proved that our government was spying on us… a fact that was not exactly a revelation. In fact, very little changed afterward precisely

because it wasn't new information. It simply moved from "conspiracy theory" column, to "fact" on Wikipedia, well, that *and* it was proven in Federal Court that the federal agencies broke the law as they spied on Americans by the millions. (Kalmbacher, 2020)

At the moment, skimming might not be a threat to devices that use NFC (Near Field Communication), which is specific type of RFID that has extra security, but the beauty of using shielding is that it's an old school solution to a high-tech problem. If you use shielding, you no longer have to stay up on the latest development of RFID technology and which version is in your passport vs your bank card, credit cards, cellphone or key fob and what the vulnerabilities are at any moment in time in the never-ending arms race between hackers and IT security.

Do the academics who argue criminals aren't skimming because it's too expensive think that it's too expensive for governments, too? Because it's obviously not. Passengers who pass through customs will notice that they are now herded through ever narrowing apertures. This is because they have no 4th amendment rights at customs checkpoints. Every imaginable scanning technology is used to pull every shred of data it can off travelers. Stingray like cellphone tower cloning is used to man-in-the-middle attacks against cellphones, facial recognition software scans your face, ANPR systems scan your license plate if you are driving.

But they must not be skimming your bank cards because they haven't been caught, right? Attacks on phones have been proven by court documents and the cat was let out of the bag on license plate and facial recognition when loads of data collected at entry points was stolen. (Barrett, 2019) If proof of the rest hasn't been found yet, in my opinion, it's simply a matter of time until it will be proven that the government has been skimming that data along with all the other kinds of

data it has have been stealing.

But the beauty of shielding is that you can simply stop it all from working until you want it to. You are invulnerable to skimming attack, phone hacks, the government or companies tracking your cellphone location… all of it. You can turn it all off by putting it in a shielded pocket liner and then take it when you want it to work. Old school protection when you want it without having to limit yourself to a flip phone.

I don’t like to leave a detailed bread crumb trail of every place I go, not because I’m a criminal, but because I don’t think that every detail of my pattern of life is anybody’s business. If you leave enough data out there for authorities to sift through, they will have plenty of data to cherry pick and misinterpret. Everybody has all the makings of a murder kit in their home… duct tape, dish gloves, shower curtain, hammer, zip ties, and so on. The difference between the average American and a serial killer is context. He has these items in a duffel bag in his car. You have them scattered throughout your home. The problem with cherry picking data is the lack of context.

I don’t think that’s a good idea in the litigious age we live in, especially given that the average American professional commits three Felonies a day, on average. They aren’t criminals, there are just a whole lot of ridiculous laws on the books. If overzealous law enforcement has it in you because somebody doesn’t like your politics, religion, or, well, pretty much anything about you … they can weaponize the system against you and the more data you give them, the easier you make it for them.

What Does EM Shielding Do?

Many people think that RF shielding acts like ballistic shield and blocks or reflects RF signals like a mirror. It’s a little more complex than that. When an electric field is applied to

the surface of the conductor the shielding is comprised of, this induces a current in the conductor, displacing the charge inside it and cancels the field inside the shielded envelope. When this happens, the current stops. This effect can be demonstrated with a Faraday cage. (Wikipedia, 2024)

Low frequency magnetic fields are not completely attenuated by EM shielding. Without getting too technical, you can think of it as decreasing the volume of the signal as it passes through the shielded envelope.

How is the Efficacy of EM Shielding Measured?

The efficacy of EM shielding is measured in decibels. If I turn on a radio receiver and then place it inside a Faraday bag, the volume of the signal is reduced. So, instead of hearing the signal loud and clear, I might hear the signal as more of a whisper. The signal isn’t blocked, it is just attenuated or reduced in intensity, as if the volume was turned down so much that you couldn’t understand the voice talking on the radio.

In the case of a shielded wallet, the object is to attenuate the RF signal from the credit card skimmer to the point that it cannot be detected by the RFID to the point where it cannot be detected by the RFID chip’s transceiver or to reduce the RF signal from the RFID’s transceiver to the point that it is not detectable by the credit card skimmer.

HEMP & Faraday Cages

HEMP is High Altitude Electromagnetic Pulse, and it is caused when a nuclear weapon is detonated high enough in the atmosphere that they leverage an effect called Compton Scattering which can cause a thousand-fold increase in the electromagnetic field strength of a HEMP.

A Faraday cage is simply an envelope of magnetic shielding. For it to be effective in the frequency range that endangers electronics, the free flow of electrons throughout the shielded layer is necessary. The shielded layer must conduct electricity. Please see my previous articles for additional information on HEMP and Faraday cages.

How much RF Shielding Do I Need?

That depends on what you are trying to do. If you are concerned with HEMP, 74dB is enough to protect against the HEMP caused by a normal nuclear weapon incapable of producing an EM field strength of 50Kvm. (Don White, 2013) It is thought that this is the maximum field strength that a conventional nuclear weapon could generate over the USA because information in the public domain claims that field strength is limited by saturation effects in upper atmosphere.

It should be noted however that Soviet military literature discussed the employment of “SuperEMP” weapons capable of generating field strengths in excess of 200Kvm. (Emanuelson, 2024)

References

Barrett, B. (2019, June 10). *Hackers Stole a Border Agency Database of Traveler Photos*. Retrieved from wired.com: https://www.wired.com/story/hackers-stole-traveler-photos-border-agency-database

/
Don White, J. E. (2013). 3.4 EMP Protection Requirements (for technical readers). In J. E. Don White, *EMP Protect Family, Homes and Community* (pp. 60, 61). Lake Suzy, Florida: Renewable Energy Creations, LLC.
Emanuelson, J. (2024, September 4). *Super-EMP*. Retrieved from futurescience.com: https://www.futurescience.com/emp/super-EMP.html
Kalmbacher, C. (2020, September 2). *Federal Court Rules Government Broke the Law By Spying On Millions of Americans, Credits Edward Snowden*. Retrieved from lawandcrime.com: https://lawandcrime.com/high-profile/federal-court-rules-government-broke-the-law-by-spying-on-millions-of-americans-credits-edward-snowden/
Wikipedia. (2024, July 17). *Electromagnetic shielding*. Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Electromagnetic_shielding