(Approx. 1563)

President's Corner

Build a Wall?

By Greg Skalka, President, Under the Computer Hood UG, CA

February 2019 issue, Drive Light

www.uchug.org

President (at) uchug.org

Walls can keep things out. Walls can keep things in. Walls that do these well usually aren’t so good at also letting some things pass from one side to the other.

Walls are meant to separate. You can’t have separate things without some kind of boundary or barrier between them. Countries have borders that define the extent of their territories. Parcels of land have survey markers that define their boundaries. Our dwellings have their spaces defined by their walls, doors, windows, floors and roofs. Our bodies have skin and tissues that define what is within us and what is external to us.

Borders and boundaries can vary in permeability. Some need to be more porous, letting more things in or out. Others need to be more impenetrable, keeping most things out for protection or in for containment. In many cases a single barrier approach is not sufficient; a layered approach with many aspects to the boundary is more effective.

Our body’s skin and hair help protect us, but they can’t be too impenetrable, for without the ability to ingest food, expel wastes and exchange gases with the external world, we would quickly die. Our bodies must have a layered defense, with our immune systems helping to fight off infections that get past that initial outer boundary. We can also use technology to help, with clothing and sunscreen adding protection against solar radiation, for example. Our homes must follow similar border compromises, for while living behind blast doors in Cheyenne Mountain might provide great safety, we would lose easy contact with the outside world. Our home’s windows let in desirable sunlight, but we must often draw the curtains to protect our privacy. Walls, while often essential, are seldom a one size fits all solution to boundary problems.

Our modern tech communication systems have given us the ability to easily exchange information instantly and at low cost with anyone on the planet. Unfortunately, we must erect barriers in these mediums to protect ourselves from offensive information and interactions, while still allowing us to send and receive the information we want. Just as in the physical world we might like to build a wall to keep away someone that has violated our “personal space” and tries to talk to us from six inches away, we need walls in our electronic interactions to protect us.

Our oldest form of electronic communications that is still in common use is the telephone; it has been around since the late 1800’s. In the early days, the cost to use it provided a barrier to misuse. While the recent modernization of the system and its lower costs have benefited the user greatly, undesirable use has also greatly increased as a result. In addition to scam calls, legitimate businesses often overuse the system as it has become a cheap way to advertise and to solicit customers. Today most of the calls I receive on my home phone and my cell phone are unwanted. While I do receive some useful calls, such as medical appointment reminders and notifications that my prescriptions are ready to pick up, most are calls to try to sell me solar panels, get me to refinance my home mortgage or solicit donations. Some are of criminal intent, trying to impersonate the IRS or some other entity, with hopes of convincing me to send them money. I’ve had to add technology and alter my behavior to try to wall these people out of my life.

For my home phone, an answering machine is an essential barrier in the communications chain. I don’t have Caller ID, so unless I happen to be expecting an immediate call, I make it a practice never to answer when it rings. I allow all calls to go to the answering machine, which I use as a filter. Unless the calling party’s message is compelling enough, I will simply delete the message. I think most scammers and many businesses are deterred by the answering machine barrier, as most calls I receive result in no message left. This wall seems to be working well, at least so far.

I also get unwanted calls on my smart phone, but here I have more layers of tech barriers to help. It has Caller ID, but the scammers can falsify the information transmitted about their identities, reducing its usefulness. My phone carrier is T-Mobile, which sometimes helps by identifying calling numbers as “Scam Likely.”

I have done some phone programming to help me quickly identify those unknown callers trying to scale my tech walls. I have only added numbers to my phone’s contact list that I truly wish to receive calls from. For each contact added, I have changed the ringtone for that contact to something other than the default for the phone. When my phone rings and I can’t see the display (if it happens to be on the other side of the room), I can still tell that the caller is in my contact list, as it will ring with a ringtone that is different from the default. If it is the default ring, I know it is not one of my contacts and I don’t need to get up to answer, as I’ll just let it go to voice mail. Again, my border defense is multi-layered, with technology and my behavior helping to filter out the bad guys, while allowing me to easily communicate with those I like.

My smart phone also allows me to send and receive text messages, but I’ve yet to receive any unwanted texts. If I do, I’ll have to come up with some kind of tech barrier to counter those intrusions.

There was once a time when receiving a letter in the mail was a cause for excitement; now we mostly receive junk mail and bills. Of the roughly 40 years we have had email, the early years had that excitement. Unfortunately, as costs came down and connections proliferated over the globe, email communications became primarily electronic junk mail and scams. I keep trying to find ways to make email great again, but it has proved to be a daunting task. I can’t seem to find the right kinds of walls and barriers, as it is much harder to separate the desired from the undesirable in this medium.

One of the problems with barriers for email is that they are often swamped by quantity. I typically receive 50 to100 emails to my primary personal account per day. I might get a few of personal correspondence, maybe some financial alerts and notifications, a bunch of advertising that I am interested in, a bunch of legitimate ads that I’m not, some scammy stuff and a few really odd ones. Most of my email appears to be safe. I have had phishing emails from time to time - emails from banks I don’t do business with (and a few that I do) asking me to click on a link. I’ve also received a few emails with suspicious attachments - who knows what malware they may contain.

Some email users swear by spam or junk filters. Some email providers have filtering capability, and there are also external spam filters that can be used. My provider does not provide filtering, my client (Thunderbird) appears to have some junk filtering but I’ve never tried it, and I’m not desperate enough so far to try external filters. I am skeptical of the effectiveness of email filtering programs. They may be able to filter off the very bad items, but I can usually spot those fairly easily anyway. My bigger concern is for items that I only want to see periodically, or that I have to investigate to see if I want. Sometimes I want to see the Fry’s or Groupon emails, and sometimes I don’t. I’m still looking for walls that work for my email needs; right now my walls are pretty low, and I do a fair amount of manual inspecting on what comes over.

The Internet is only about 35 years old and already has over half the people in the world using it. It and the World Wide Web allow people anywhere on the planet (and even in space, on the International Space Station) to get information and communicate with any of the other users. With this borderless medium, each user requires some boundaries be placed at the interface to their network for protection. An Ethernet router is the main line of defense, a wall between your network and the rest of the Internet. Making sure your router is configured correctly for maximum security will help block malicious intrusions into your network and computers, while allowing you to get the information you need. Setting up your Wi-Fi correctly is also an essential part of keeping your network safe and preventing the misuse of your internet connection.

In our electronic, interconnected world, boundaries are essential for keeping our communications secure and our personal data private, but just putting a wall around ourselves is not the answer. The barriers we use must be appropriate and configured for maximum protection with minimum restriction for the passage of desired data. A layered and evolving defense will usually be the most practical and have the most success.