# HCHC Lego Hospital

## How To Use

Note: All web pages are built with a 60-second auto-refresh.

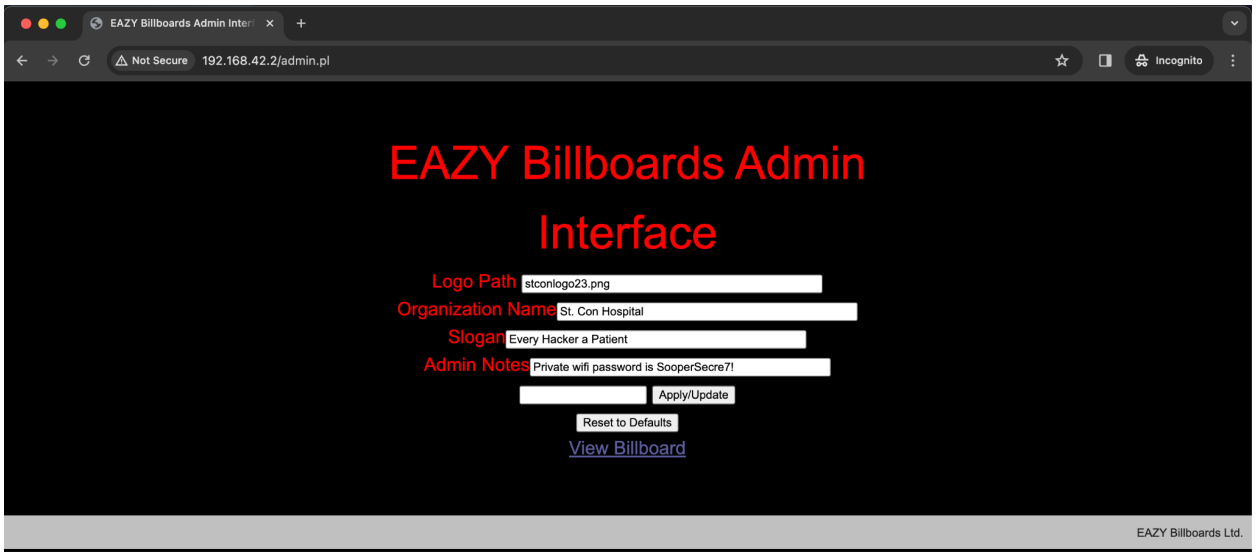
The Hospital Billboard is the entry point to hacking the hospital. The billboard is a Kindle Fire tablet enclosed in a Lego frame, so the con attendee can only see:


The attendee must find the Admin console for the billboard in order to proceed. There are two ways to accomplish this:

1. Hack the Billboard Wi-Fi:
    a. Attach to the open (no password) wifi network for the billboard:
        i. EAZYBillboardsLtd
        ii. EAZYBillboardsLtd_5G
        iii. EAZYBillboardsLtd_5G-2
    b. Find the web server on the network: http://192.168.42.2
        i. Note: For Mobile phone users, the “Fing” app is a great app to introduce to them. It’s essentially *nmap* for mobile 🙂. https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=en_US&gl=US or https://apps.apple.com/bw/app/fing-network-scanner/id430921107
    c. Find the “Admin” link in the lower left corner of the main page
2. Touch and scroll down on the billboard itself to find the “Admin” link in the lower left corner of the main page

Here is the full page as seen in a web browser:


Once on the Admin page itself, the attendee will see:




This is a real working page, if you know the password in order to make changes. This may be used in future expansions to the Lego Hospital.

For now, the critical information is the “Admin Notes” field, which contains the Wi-Fi password for the private network of the hospital itself!

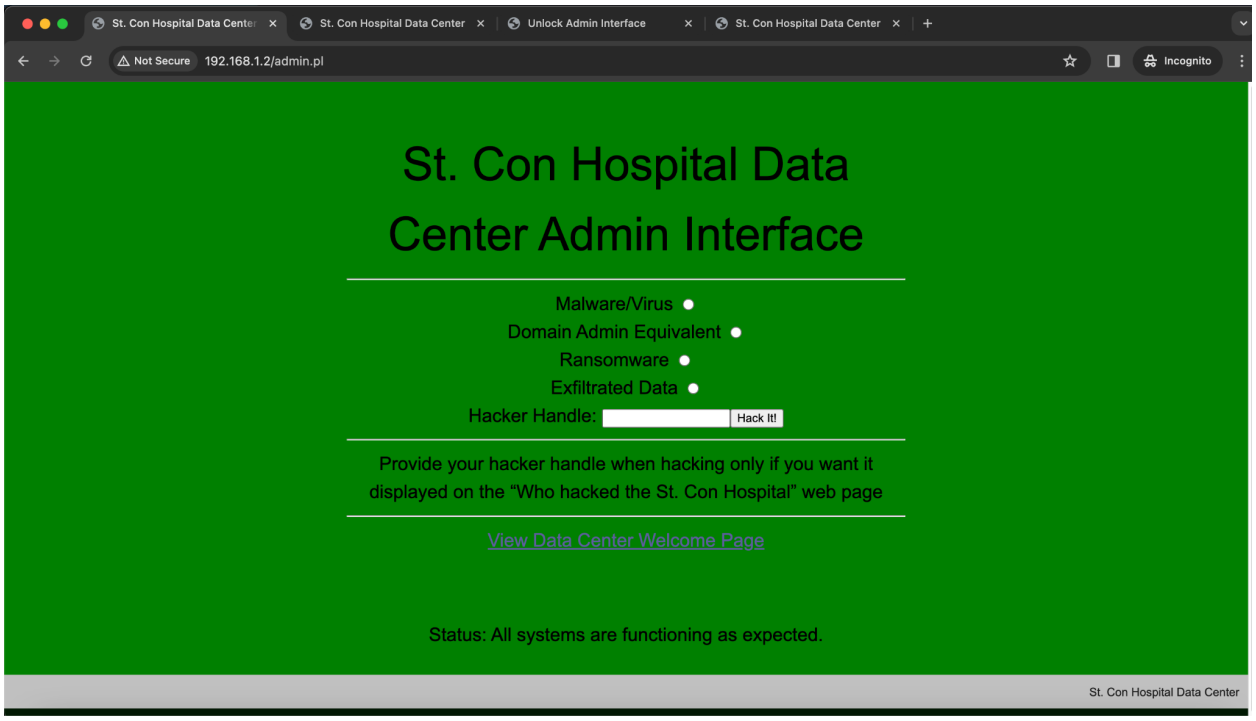
The attendee can then connect to the private Wi-Fi network:

- STCONHOSPITAL
- STCONHOSPITAL_5G

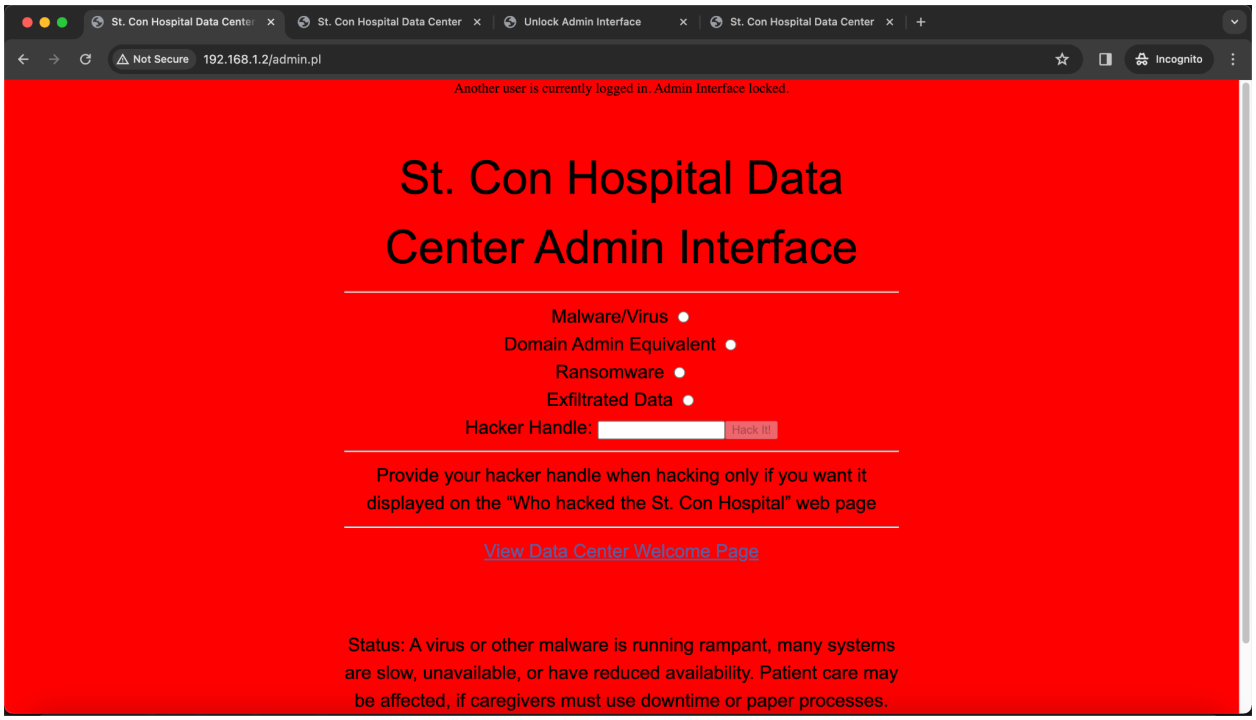
- STCONHOSPITAL_5G-2

They can then find the main St. Con Hospital Data Center web page at: http://192.168.1.2


They should quickly notice another “Admin” link in the lower left corner, this takes them to the Admin console for the data center:

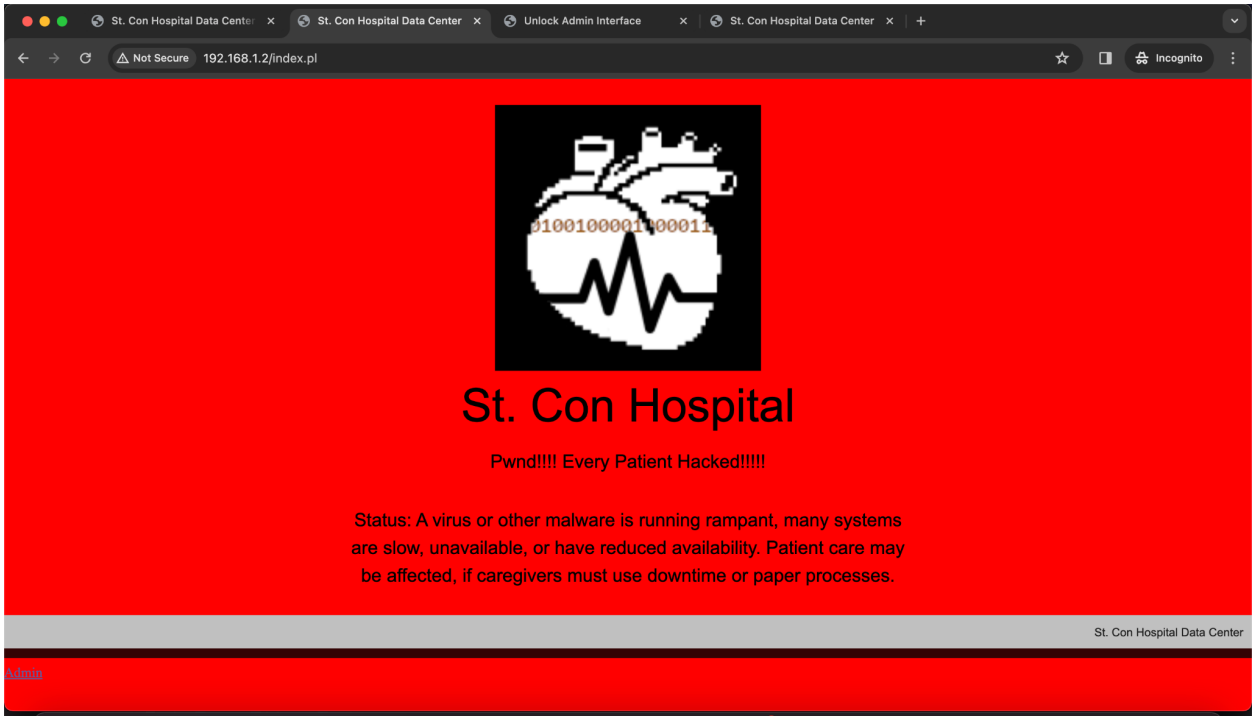


The attendee can choose 1 of 4 attacks. Each attack results in different displayed Status messages, and different strings of LEDs to light up in the hospital. They can also choose whether or not to supply a Hacker Handle to be displayed in a big list of attendees who have successfully hacked the hospital. Either way, once they click on the “Hack It!” button, all the screens change from a green to a red background. The Admin Interface locks, preventing others from hacking the hospital at that point. This is to prevent an overload of the Arduino and LED systems and to keep the displays from switching too quickly. The Admin console displays a message that another user is logged in and the console is locked.




The Status message is displayed in the Admin Console, but is actually easier to read on the Data Center main page. Here are the 4 Hacked Status messages:

1. Malware/Virus

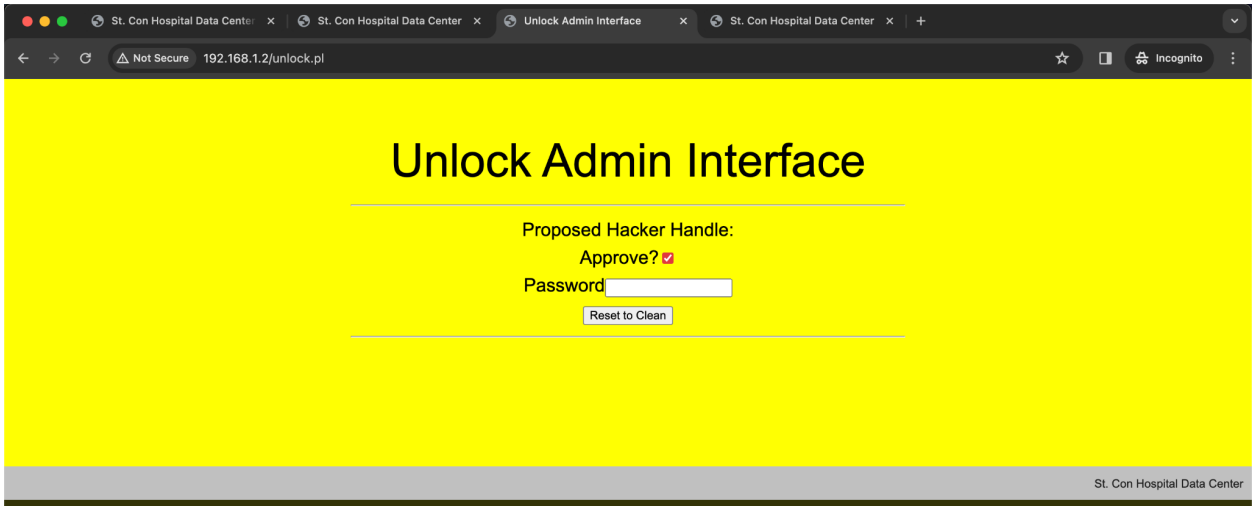



2. Domain Admin Equivalent


3. Ransomware

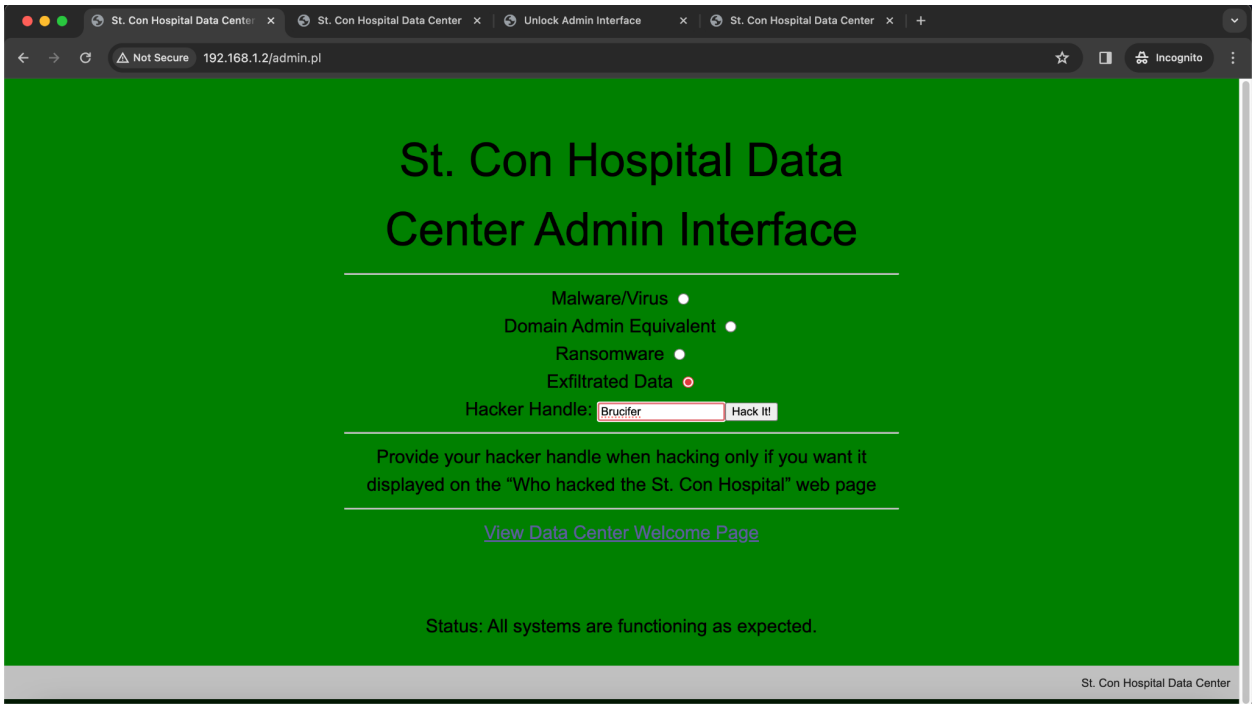

4. Exfiltrated Data


For the situation where the attendee does not supply a Hacker Handle, an HCHC Staff or Volunteer will need to reset the hack back to normal (green backgrounds and normal status). This is done by browsing to: http://192.168.1.2/unlock.pl.



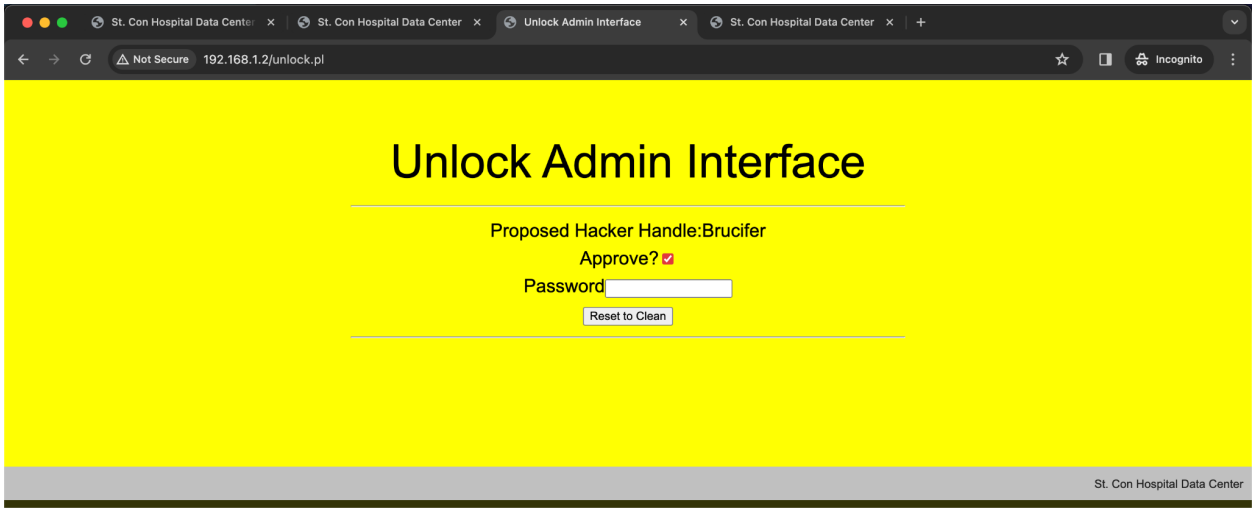

All that is needed to reset when no Hacker Handle was supplied, is to click on the “Reset to Clean” button. The hacked status is cleared, LEDs are turned off, and web pages go back to green backgrounds.

If a Hacker Handle is provided on the Admin Console:




The Admin Console locks, web page backgrounds turn red, and status messages are updated exactly the same as when no Hacker Handle was provided.

The unlock web page is slightly different:




The provided Hacker Handle is displayed. As long as it isn't something vulgar or inappropriate for attendees to see, the HCHC Staff or Volunteer can approve for it to be added to the big list of hackers. To approve, both the "Approve?" checkbox must be checked, and the correct password must be entered. The password is provided in the Hospital configuration document.
Once the "Reset to Clean" button is pressed, the hacked systems clear up as explained previously, and the hacker handle is immediately added to the big list of hackers.

The big list of hackers is available on yet another web page, intended to be displayed on booth monitors. It's background changes along with the good or hacked status of the hospital:



One final note: This is built to hopefully allow HCHC Staff and Volunteers to just use a web browser on the stconadmin laptop to manage the Lego Hospital. If anything does go wrong (either because I built it too fragile, or someone actually *really* hacks the systems), the stconadmin laptop will have images and other files needed to restore the system, and the web servers can be accessed either via SSH/SCP, or directly with a monitor, keyboard, and mouse to the Puppy Linux X console.