SWCP Portal
August 2019

Hardening the home front for unpleasant possibilities

Bracing for Cyberattacks

What has been warned about for years finally happened. On July 25, SWCP was hit with a **Distributed Denial of Service** (DDOS) attack. Though aimed at one specific customer rather than the network, the unrelenting onslaught degraded most of our members' connections throughout much of the day.

Though the hackers had hoped to extort payment from their victim, this DDOS attack was not intended to destroy anything. Its sole purpose was to deny internet access to one site by swamping servers with more requests than could be filled. These requests came rapid-fire from a network of infected computers – hacked devices, often those whose users have been tricked by a hacker who then placed hidden malware, thus owning the machine. But a lot of them were likely **compromised IoT devices**, consumer routers, and so on, which are **still being attacked**.

These kinds of DDOS attacks can be profoundly aggravating to users. During this recent incident, access to the network was still possible but very erratic. Pages wouldn't load, mail wouldn't send, and it was almost impossible to navigate between sites.

Yet, here in 2019, this is all just part of the "**new normal**". All of us, users and administrators alike, are on the front lines of this conflict. Each and every one of us is now a potential target that could be attacked – if only in order to get to other, more valuable targets.

Just as we have been advised by the government to prepare for **physical disasters**, everyone must also take precautions for their online lives. Because there is no way to gaurantee this will not happen again.

The bad guys constantly look for *any* way to break into systems, but the easiest vector nowadays is by **phishing.** These are deceitful attempts by hackers to get a response from users, usually through emails. The idea is to trick you into clicking a link to hidden malware in a message or snared on a webpage.

Phishing has become a remarkably easy and widespread crime, aided by markets on the dark web and untraceable cryptocurrencies, yet it's a very serious offence. **Three UNM students** were just arrested for their involvement in an international phishing scheme, for example, and could face long sentences.

Phishing messages range from obvious scams with misspelled words or padded text from "**Nigerian princes**" to sophisticated ploys specifically targeted for espionage purposes, like the kind used by the Russians to **hack the DNC** during the 2016 election.

While modern antivirus programs do a pretty good job of detecting viruses attached to an email, they can do nothing to prevent a user from clicking on a link to a webpage packed with malware. Though modern web browsers can alert surfers to certain kinds of bad pages, they cannot block them all.

Avoiding pitfalls

So it remains up to users to look out for themselves. Fortunately, there are ways to spot phishes. Messages will often appear to be from a trusted, important source, like a bank, credit card company, SWCP, or even a friend who claims to be in trouble somewhere. Usually the email will spin a story to prompt you to act quickly without properly considering it such as by claiming they've noticed suspicious activity or there's a problem with an account or your payment record.

These scammers can be very creative with doctored spreadsheets or files, demands for confirmation of private information or for immediate payments to avoid bad consequences – even offers of refunds.

Remember that their addresses *cannot* be the same as that of the legitimate institution they are **spoofing**, so they may go to great lengths to disguise their identity. Often the email or web address may look okay but may betray its true nature too late.

So **do not blindly click on any links in emails**. If you need to visit a website, simply look it up in Google or from a bookmark and go to it from there. If there's an attached file from someone you do not know, check the address and identity of the sender before opening. And it never hurts to run any **downloaded file** through an antivirus program before opening either.

For websites, **check site certification** (often signified by a padlock or shield icon in the location bar). While these can sometimes be hacked or stolen, sites lacking them are definitely suspect. If notified that the

Continued on back

Continued from front

certificate has **expired**, (which happens sometimes), the site could be legit, but use extra caution.

Forward any suspicious or bothersome messages to **help@swcp.com** to alert our Tech Support staff. We usually can tell if it's a scam or not, and notifying us promptly may allow us to set up email filters to prevent others from getting fooled by something similar.

Preparing for online attacks

Despite all our best efforts, another such attack could happen. DDOS assaults can be **mitigated** by special services like **Cloudflare** with lots of servers and tons of bandwidth, but their price could actually be steeper than the ransom demanded by the bad guys.

Be prepared and stay vigilant. DDOS floods could block access so back up your vital files locally. This also might be a good time to assess whether it's worth heavily relying on the **cloud** for storage and data services, especially with **Chrome** computers, which totally depend on Google in order to function.

We're all in this together, so please, whatever happens, **be patient**. We will let you know as soon as we can, but if you are unable to get through to us by phone, it's a good bet that everyone's in the same mess. Most importantly, you need to understand that **DDOS might not be the worst thing to happen**.

Cyberwar, as we have also been warning for years, is a very real thing. It is now quite possible for an adversary to **physically cripple infrastructure** by hacking. Already there have been attacks that **shut down power grids** for extended periods. It may be very hard to detect the cause or actor, and it might take weeks to get everything up and running again.

Such long-lasting outages should be prepared for much as you would for a hunker-down-in-place **natural disaster** with stocks of food, water, batteries, and extra medicines readily on hand. If you still have a landline at home, keep it. Unlike smart phones, regular **phone service** might still work once the power goes out. And you should include **electronics for disasters** in your plan. Safely commit vital online information, like addresses and passwords, to paper.

SWCP will stay alert to help keep us all safe.

Become a Power Publisher with WordPress

WordPress is the most popular webpublishing platform in the world because it's free, easy, and runs some amazing websites. Get in on the basics of this highly versatile site creation and management tool from our own VP and WordPress expert, Jamii Corley. The first session will be held **Friday, August 23, 11AM-12:30PM** at **Ideas & Coffee**. Sign up today!

Thinking of cutting the cord?

Judging by all the companies who are jumping into media creation and delivery, online streaming of videos and movies is the **Next Big Thing**.

Netflix, the most popular streaming service in the US, has *128 million* customers worldwide, and plans to spend *$15 billion* to produce content this year alone. Its recently-purchased **production hub** right here in Albuquerque is expected to add *1000 jobs* and *$1 billion* to the local economy, so it's a big deal.

With so much new, unique programming slated for all these outlets, there's a real temptation to cut the cable or abandon the antenna. Just be sure to do your homework to make sure you can affordably get the shows you want on the platform that you prefer.

That, however, may be a bit of a challenge. The whole field is still rapidly evolving, with new players, plans, and line-ups announced every day. **Amazon Prime** currently has the most programs, but **Disney+** is the **600-pound gorilla** set to arrive this fall. And with almost *300* streaming services now available, those **prices** can really **add up**, especially if there's just a single "must-see" show on a platform.

A few providers **aggregate streaming services**, but it's unsure how much of a bargain they are. Most, like **Reelgood**, allow users to combine and manage their favorite channels together, including Netflix, Amazon, HBO, Hulu and many more.

Streaming video, however, means just that – the video is stored on a server to play over the web. To be able to watch the production at any time without being online means that the show must first be downloaded and saved as a file on your computer.

This can be tricky since most streaming platforms aren't big fans of that option. But shows can also be recorded straight from your screen much as one would with an old VCR with a software **screen recorder** or plug-ins for **Chrome** and **Firefox**.

Streaming will be big, but it's still rapidly developing. There will be much more to talk about. Stay tuned.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-243-SWCP (7927) ◉ **SWCP.com** ◉ **Help@swcp.com**

5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**

Click on blue terms in PDF file to open links.