SWCP Portal
April 2018

Easy Site Encryption

Webpages need to be sent encrypted to ensure privacy, which is essential when entering sensitive data. A very strong, sustained effort has risen across the net to require encryption for everything. But to use **SSL encryption**, as it is commonly called, on a website requires that site to have an **SSL site certificate**.

Getting and installing such certificates has always been an expensive, painful chore, and the workings have been a mystery. Now there is a cheap, automatic, and open-source method that makes it easy.

Let's Encrypt creates free site certificates for anyone with a domain. All that's needed is to verify domain ownership. Details are technical but this issuer makes SSL certification much simpler to implement and manage. Backed by Cisco, Google, and the **Electronic Frontier Foundation**, it should be trustworthy.

Southwest Cyberport is proud to offer this optional service to our members. Our one-time setup fee is *$50*, but renewal is free, and SWCP will handle setting it all up and maintaining the certificates.

There are some limitations, of course. These certificates are the most basic kind. No verification of the organization or the person or corporate entity controlling the site is involved. That means that phishers can easily get them too, so additional security beyond SSL encryption may be necessary.

For websites with critical needs, such as shopping or data collection, **commercial site certificates** that SWCP offers from GeoTrust are still available. GeoTrust certificates offer a Site Seal so users can verify the certificate is in good standing. Extended Validation certificates put the name of the company that owns the certificate in the browser location bar in green next to the lock icon.

But for everybody else with domains – such as our WordPress site owners – Let's Encrypt Domain Validated Certificates should be quite sufficient. They will protect passwords, content, and comments in transmission from prying eyes and prevent interference.

SWCP urges every web-publisher to take advantage of this service. For one thing, Google is beginning to downgrade ratings of websites without SSL certification, and come this July, as is explained on the back, Chrome will start warning users when they visit any non-SSL site. So sign up today!

Another fine free service from Southwest Cyberport

Send Secure Messages

By Mark Costlow, President

Have you ever wanted to send someone sensitive information quickly, easily, and securely? Now you can, for free, with SWCP's secure messaging service **Burn After Reading** (**https://burn.swcp.com/**)

Often the simplest approach is to call the other person on the phone. Other than the spooks at the NSA, that is probably a pretty private connection. But if the information is at all intricate, like a password or bank account number, voice communication is ripe for miscommunication and misunderstanding.

Secure encrypted email is a possibility, but so far (after more than 30 years of it being available) it is still too complicated for most of us to master.

And those who CAN figure it out are usually too busy to be bothered trudging through the steps to use it every time.

FAX is another trusty old technology that can work. Unless you are sending your message to a friend or family member who doesn't have access to a FAX machine. Or what if the receivers FAX is in a shared office space? You don't want the recipient's coworkers to read your private message as it slowly churns out of the machine.

Continued on back

Google and HTTPS Everywhere

By Mark Costlow, President

In the early days of the web, information was accessed in "clear text", meaning it was not encrypted. The rise of e-commerce demanded that websites protect those communications so an eavesdropper could not see sensitive data, such as credit cards, account numbers, and personal information.

Web encryption was always easy for users to deal with. If a web address starts with **`HTTPS://`** instead of **`HTTP://`** that extra "**S**" means the information is encrypted and secure. But it was expensive and complicated for webmasters. Usually only sites with obviously sensitive data would go to the trouble of using HTTPS.

So why are there now movements encouraging **HTTPS Everywhere**? It turns out there are side benefits to using HTTPS that are not so obvious. It prevents evesdroppers from injecting content into a connection. An evildoer with access to a router between you and the web site could inject malware into the connection, diguised as a link in the text or ad on the page. It's easy to fall prey when you trust the site you think they came from.

Another case of unwanted content injection occured when at least 2 very large ISPs were caught inserting **tracking headers** and **pop-up ads** into pages of their customers' browsing sessions. HTTPS resists this sort of meddling because nobody can inject new data into the stream without breaking the connection. In response to these and other revelations about Internet privacy, the **HTTPS Everywhere** movement is advocating that **ALL web sites use HTTPS**, regardless of content.

See the article on the front about how Let's Encrypt's low cost and automated management tools make it feasible for every site to eventually use HTTPS.

Google began forcing the issue 3 years ago. They began by giving HTTPS web sites slightly higher weight in their search algorithms. In late 2016, their Chrome browser began to mark any HTTP page with a credit card or password form on it as "Not secure". Firefox does this too. But starting in July, Chrome will **flag ALL HTTP web sites** as "Not secure".

At SWCP, we have enhanced our hosting platform to support this change. We can add Let's Encrypt SSL certificates to any site at a low one-time cost and with minimum effort from the site owner. There are some technical "gotchas" involved in converting a whole site to HTTPS, but we can help you through them quickly. Automated renewals will ensure that your certificate will never unexpectedly expire.

It is up to each site owner to decide if the small additional expense and effort for SSL is worth it. These changes have tipped the balance toward "HTTPS Everywhere" for the first time ever.

Continued from front

These problems are the inspiration behind **Burn After Reading**. It gives you a secure person-to-person communication and it's extremely easy to use – there is no software to set up or install. Here's how:

1. Visit **https://burn.swcp.com/** in your browser.
2. Type or copy/paste your message into the box.
3. Pressing **`More options`** will allow the program to send the message for you, and can create a password just for that message. Plus, you can set a time limit before the unopened message expires.
4. Copy the unique web link into an email to your friend, or have the website send it for you.
5. Your friend opens the email, uses the link to retrieve your message. And then it's gone.

A few things to remember:

- Your secret message is *only* held on the server until the unique web link is accessed. As soon as it is accessed, the server deletes it from memory.
- The message appears on your friend's screen as soon as they enter the link. If they want to save the information, they must copy/paste it from that screen. They *cannot* come back to it later.
- *Anyone* may use this. You and your friend do not have to be SWCP customers.
- SWCP logs some information for troubleshooting purposes (like time and IP address when a message is picked up). However we do *not* save the messages themselves, and they are truly "burned after reading" by deleting them from the server.
- If someone intercepts your email containing the link, they could steal the message. How is this better than just emailing the secret in the first place? It is different in two important ways:

1. The link is only good for a *single* use. If the interceptor finds the message days, weeks, or months later (say, in a legal "discovery" process), the link will not reveal the original secret.
2. If a bad guy does intercept the link, your friend will KNOW it happened because when they try to access it, they will be told it does not exist.

Enjoy!

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.