Safe Website Browsing Tips

by SSNDCP Web Team – Diane Maidl and Amber Norkett

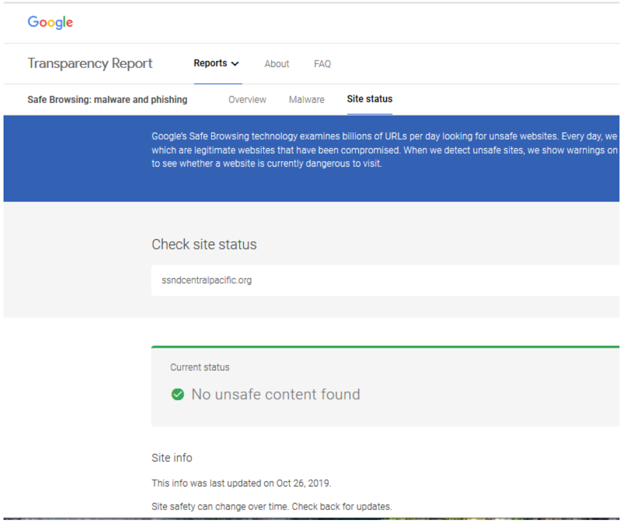
Would you like to be more confident when exploring online? Want to stream video without accidentally getting malware instead of your favorite TV show? Doing some online shopping and want to verify that the e-commerce store is legit before you enter your bank details or credit card number?

It is good to be cautious, and it is absolutely vital to check that a website is safe before sharing any personal information (e.g., credit card numbers, passwords, addresses, etc.). Below are some quick and easy tips to help you avoid questionable URLs and verify the trustworthiness of any website.

Tip #1: Use a website safety-check tool

To quickly check if a site or a specific URL is safe, you can use an objective website safety checker like Google Safe Browsing (https://transparencyreport.google.com/safe-browsing/search). According to their page, "Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites", which makes this a great website safety-check tool. Just copy/paste or type in the address into the search box and hit **Enter**. Google Safe Browsing will test the URL and report back on its reputation in just seconds. It's that easy.

Be sure to bookmark the page to use later — it's especially important to test URL safety before you do anything sensitive, like enter your credit card details.



Google's Safe Browsing technology examines billions of URLs per day looking for unsafe websites. Every day, we which are legitimate websites that have been compromised. When we detect unsafe sites, we show warnings on to see whether a website is currently dangerous to visit.

Check site status

ssndcentralpacific.org

Current status

✓ No unsafe content found

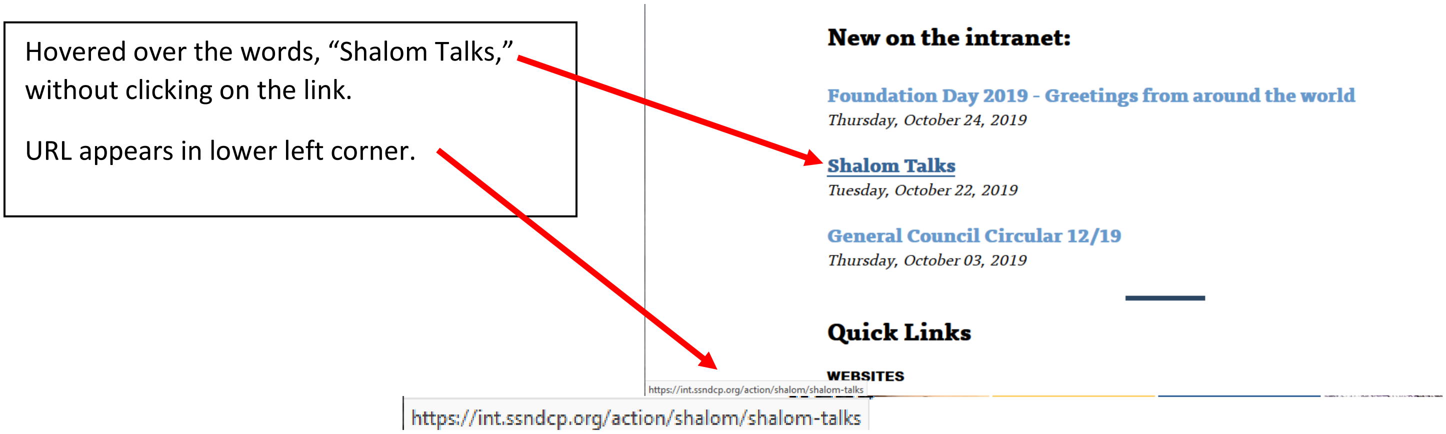
Site info

This info was last updated on Oct 26, 2019.

Site safety can change over time. Check back for updates.

Tip #2: Double-check URLs

There's a nice simple way to perform your own website safety test: check the URL (website address). In other words, make sure you know where a link is going to take you ***before*** you click on it. How? Just mouse over any link to verify the URL it's really linked to. When using browsers such as Chrome, Edge or Firefox, when you hover your mouse over the link, you should see the URL that it links to at the bottom-left of your browser.



Hovered over the words, "Shalom Talks," without clicking on the link.

URL appears in lower left corner.

New on the intranet:

Foundation Day 2019 - Greetings from around the world
Thursday, October 24, 2019

Shalom Talks
Tuesday, October 22, 2019

General Council Circular 12/19
Thursday, October 03, 2019

Quick Links

WEBSITES

https://int.ssndcp.org/action/shalom/shalom-talks

https://int.ssndcp.org/action/shalom/shalom-talks

Make sure the URLs are spelled correctly, too. Most people only glance over text on the web. Hackers know this and will often substitute visually similar characters (e.g., "Yah00.com" instead of "Yahoo.com" or "Paypa1.com" instead of "Paypal.com") to trick you into visiting their phishing sites and unwittingly giving them your passwords, credit card numbers, and other private data. Don't fall for this trick. It only takes a moment to verify a URL is safe. And it's worth it.

Tip #3: Check for HTTPS

Making sure any website you visit uses HTTPS is another way to make sure the site is safe.

HTTP (Hypertext Transfer Protocol) is the fundamental protocol for sending data between your web browser and the websites you visit. And HTTPS is just the secure version of this. (The "S" simply stands for "secure".)

HTTPS is often used for online banking and shopping, because it encrypts your communications to prevent criminals from stealing sensitive information like your credit card numbers and passwords.

So how do you know if a site uses HTTPS? Check for the padlock (🔒) in your browser's navigation bar. If you see it, you know the site you're on is using a trusted SSL digital certificate — in other words, your connection is protected.

The main takeaway is this: If a website doesn't have that padlock, don't enter your password or credit card number.

Tip #4: Look for a privacy policy

If you're already on a website, but can't easily tell if it's legitimate, look for a privacy policy. Reputable websites should have a privacy policy page, as it's the law in many countries. So, take a few extra seconds to click around the site and see if you can find their privacy policy. The privacy policy is often located at the bottom of the page in small font.

And what if the privacy policy is incomprehensible? Unfortunately, many privacy policies are full of legalese and can be hard to make heads or tails of. It's a good idea to search for words like "third-parties" "data" "store" "retain" and similar terms using Ctrl-F (or Command-F on Mac) to understand how the site handles your personal data and what they intend to do with it (such as keep it forever or sell it to third-parties).

We're getting a bit off topic now, as many legitimate sites can also have shady data practices, such as Facebook. However, it's still a good idea to make sure a site you're using at least has a privacy policy, as that's one good indicator of legitimacy.

Tip #5: Learn some obvious signs that a site is fake

Sometimes a website looks so spammy, you can tell immediately without even having to do a formal check of the site's reputation. If you accidentally land on a website like this, there are some fairly obvious signs of malware you can look for:

- **On-site spam:** if a site has lots of flashing warnings or exclamation marks, it's probably scammy. (And who wants to read a site with a strobe light, anyway?)
- **Pop-ups:** if you arrive on site and tons of pop-ups appear, it's best to close all of them immediately and navigate away.
- **Malicious redirects:** if you get immediately redirected to a completely different website, especially a shady one, this is a malicious redirect.
- **Search engine warnings:** when you search for something, you might find that the search engine (such as Google) displays warnings next to some links, such as "This site might be hacked" or "Visiting this site may be harmful to your computer." Although these warnings aren't 100% accurate, it's a good idea to choose a different option instead.

Tip #6: Call the company

Still not sure if the company is legit? Find their contact details and give them a call. Really, you can learn a lot by who answers the phone. If the number doesn't exist — or if some teenage voice answers with "Dude?" — then something's probably up. Just trust your instincts.

Where do you find a website's contact details? Look for a "Contact us" or "About us" link near the very top or very bottom of the homepage.

As we do our part in ensuring the SSNDCP website is secure, both public and sisters intranet, we ask that you protect yourself. As you browse the web, be sure to look for https and the lock (🔒) before entering any confidential information. If you have any questions, contact our IT help desk @ 1-800-373-7521 or via email at helpdesk@ssndcp.org. We are available Monday-Friday, 9-5 CST with extended hours until 7 PM on Tuesday. If you leave us a message, please know we will respond as soon as one of us is available.

Tips provided by AVG Technologies