MUO

13 BEST SECURITY GOOGLE CHROME EXTENSIONS

by Philip Bates

13 Best Security Google Chrome Extensions You Need to Install Now

Written by Philip Bates

Published March 2018.

Read the original article here: https://www.makeuseof.com/tag/best-security-chrome-extensions/

Table of contents

Are Chrome Extensions Safe? 4

1. HTTPS Everywhere 5

2. Credit Card Nanny 6

3. Webutation 7

4. Netcraft Extension 7

5. Click&Clean 8

6. Panic Button 9

7. Simple Blocker 10

8. Blur 11

9. LastPass 12

10. Unshorten.link 13

11. No Script Suite Lite 14

12. Vanilla Cookie Manager 15

13. TunnelBear VPN 16

What Else Have We Missed? 16

Most people use Google Chrome to browse the internet. It's has a clean layout, is typically responsive, and, most importantly, secure.

Personal security should be high on everyone's checklist, and Chrome came joint top in **MakeUseOf's assessment of security and privacy** on the most popular browsers.

However, there's always space for further precautions. Here are 13 security extensions you should consider adding to Chrome.

Are Chrome Extensions Safe?

Let's get this out of the way right now: extensions aren't always safe.

They're all created by third-parties in order to solve a potential issue, or improve productivity. Equally, you have to remember that these add-ons sit in your browser and have access to *everything*. Your personal information, your browsing history, all the stuff you want to keep to yourself: that's a lot of data.

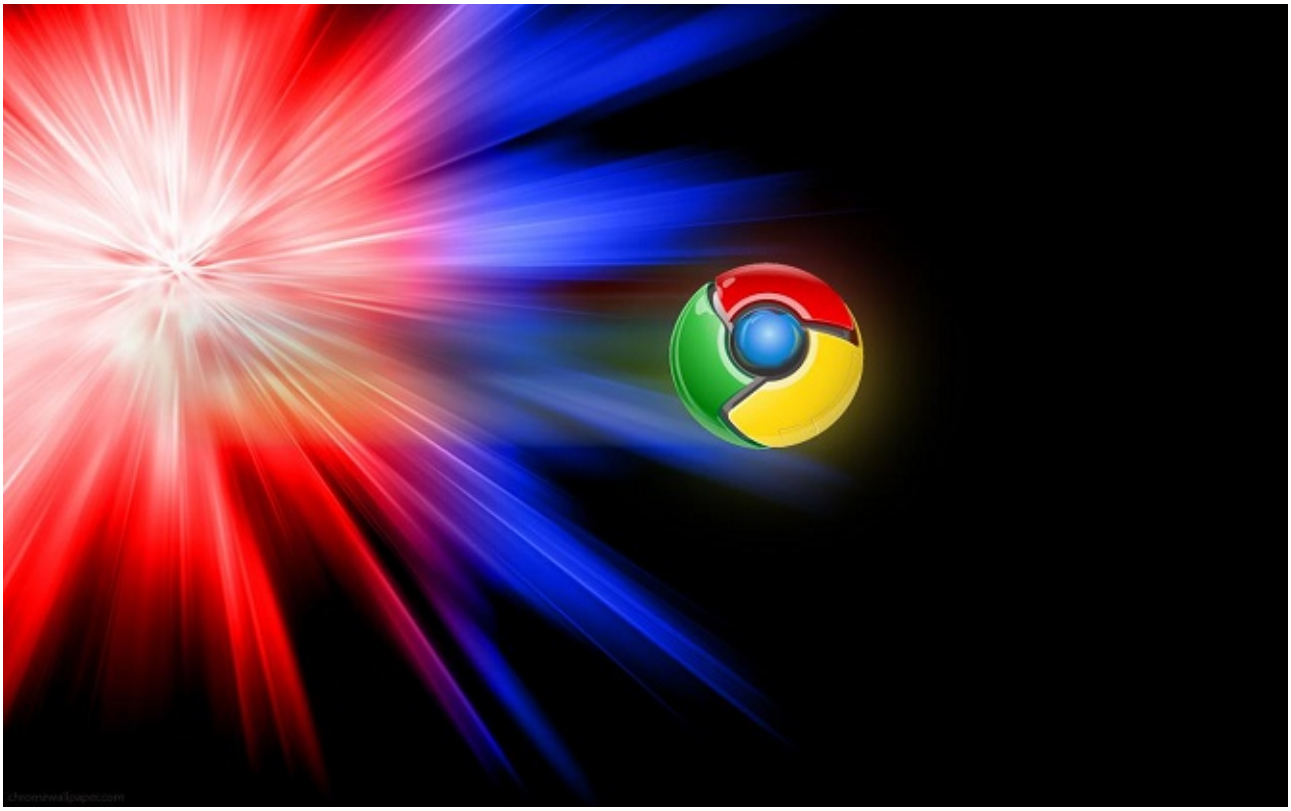


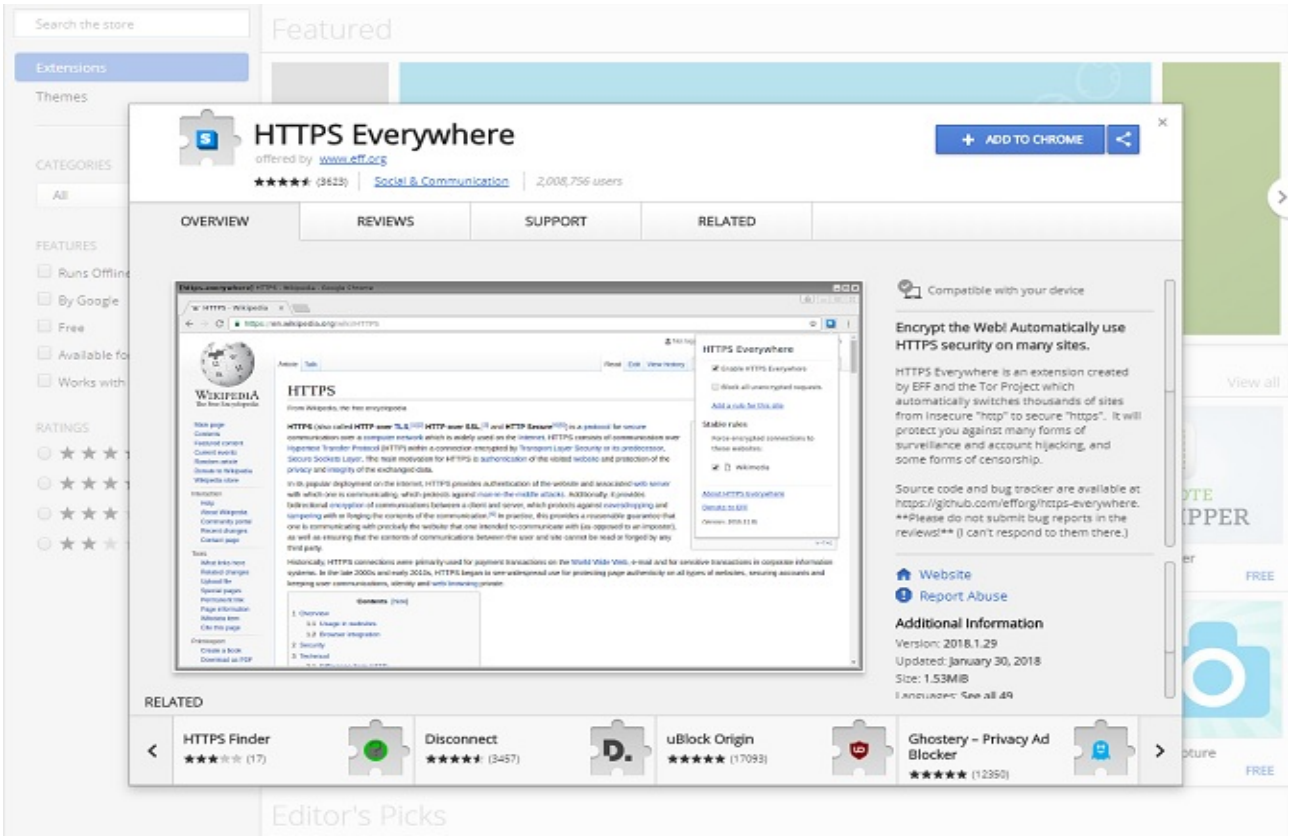
Image Credit: MoSsH/Flickr

That's not to say extensions are uniformly bad. In fact, quite the opposite. Google's screening program assesses extensions before they are added to the Chrome App Store, so anything malicious is filtered out of the market. In theory.

Sometimes, Google messes up. Sometimes, open-source code can change into something nasty.

We're only linking to the extensions that are safe at the time of writing. These are the ones that have gained traction, earned dedicated userbases, and are worthy of our support. You have to limit what you're adding to your browsing experience, and abide by basic safety precautions, including **buying solid security software**.

1. HTTPS Everywhere



We talk about this a lot, but that's because it's excellent at what it does. Most people use encryption, although in limited capacities: your iMessages, for instance, are encrypted, as are **SMS messages you send via WhatsApp**. It means information sent from one party to another is scrambled; anyone who intercepts can see randomized data, rendered unreadable. This is essential for e-commerce.

Everyone needs encryption, particularly when visiting sites that require personal information. Don't trust a page that asks for passwords but isn't encrypted. But how can you tell? Just check out the address bar: if the beginning reads "HTTPS", that's a sign of encryption. Indeed, the **extra "S" means "Secure"**. It all depends on the site using an SSL/ TSL certificate to ensure authenticity.

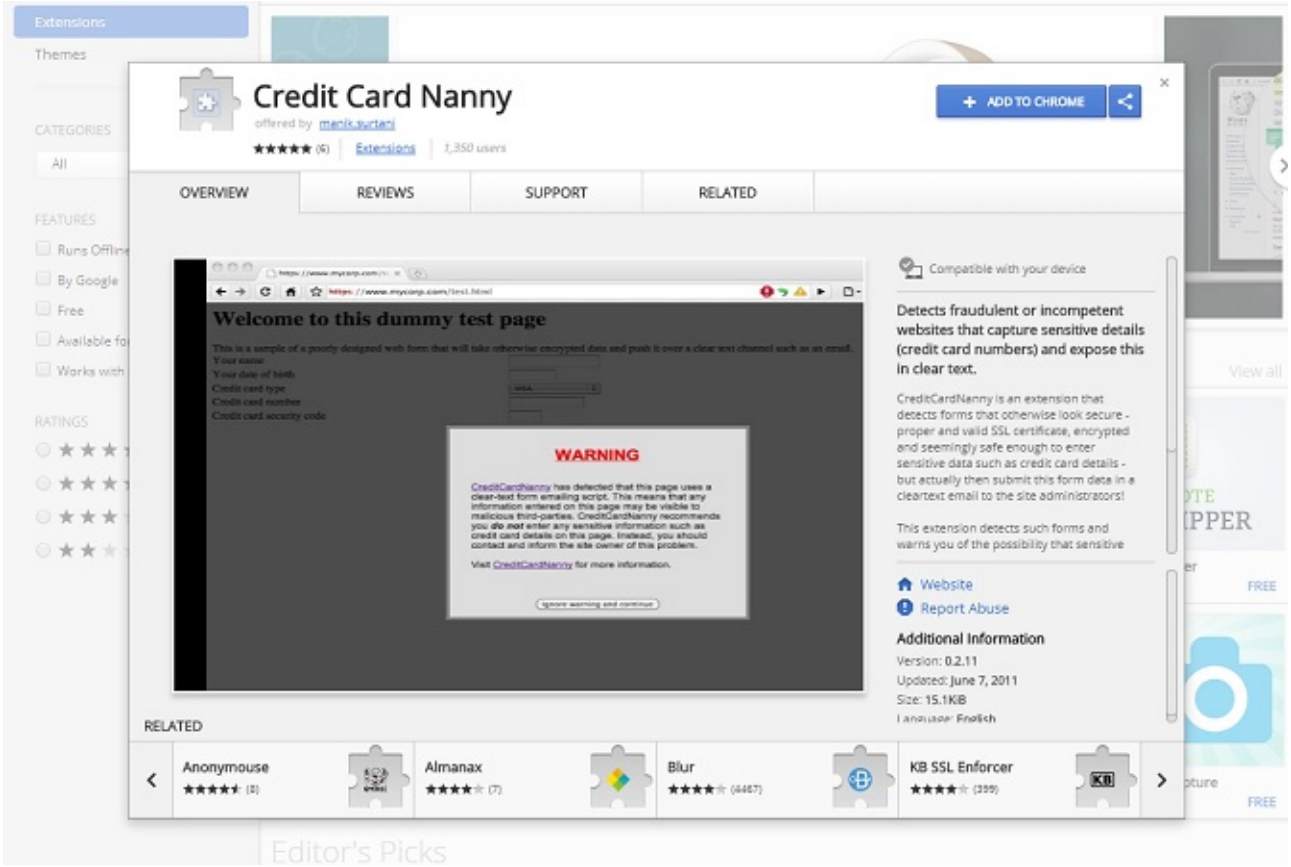
HTTPS Everywhere automatically switches thousands of sites from their "HTTP" copies to their securer "HTTPS" versions.

It doesn't work on everything, however. For smaller sites without SSL certificates, you'll see a privacy error—in which case you'll need to disable the extension for that site only. You risk your security by doing so, but just because a page doesn't have an encrypted alternative doesn't necessarily mean it's dodgy.

Nonetheless, the positives of HTTPS Everywhere far outweigh the negatives: it means that e-commerce sites, or any system that needs personal information, is afforded an extra layer of protection.

Download: **HTTPS Everywhere**

2. Credit Card Nanny



This sounds like a cash-loan company, but actually, it's a perfect companion to HTTPS Everywhere.

SSL/ TSL certificates give us peace of mind, yet we shouldn't trust them completely. Encryption is utterly pointless if your password is then communicated to administrators as Clean Text.

There are various means of **storing private information**, but Clean Text literally means that your password is readable. There's no subsequent encryption; no hashing; and no cryptographic nonce involved. If your password is "password123" (and we really hope it isn't), it's stored on servers as "password123". The site's system could get hacked and your details could be read as easily as a book.

That's worrying, but it's even more concerning if it does the same with payment information!

It's not done maliciously. Mostly, it's through ignorance.

Credit Card Nanny detects forms that send your private data in Clear Text form. If you visit a suspect site, a warning will come up and advise you to contact the owners to tell them they need better security measures. Of course, you can bypass the message and continue if you don't think the information is important enough to warrant a solid level of privacy. At least you're aware it's a concern.

Download: **Credit Card Nanny**

3. Webutation

For a while, Web of Trust (WOT) was the go-to add-on for reputability scores. Icons appear to show you which sites are secure. However, in late 2017, users realized the **consequences of the extension's privacy policy**, and began uninstalling. **WOT promised to tighten things up**, but until then, Webutation will see you right.

In the top right-hand corner, a shield will appear, rating the page out of 100. This shield is also color-coded, so you can easily avoid sites rated in red; be wary of those in yellow; and happily continue as intended when you see green. Anything that's especially dangerous will flag up a special message that will let you proceed regardless or safely return to your search.

You can also block access to adult websites, and any deemed "bad" by the system.

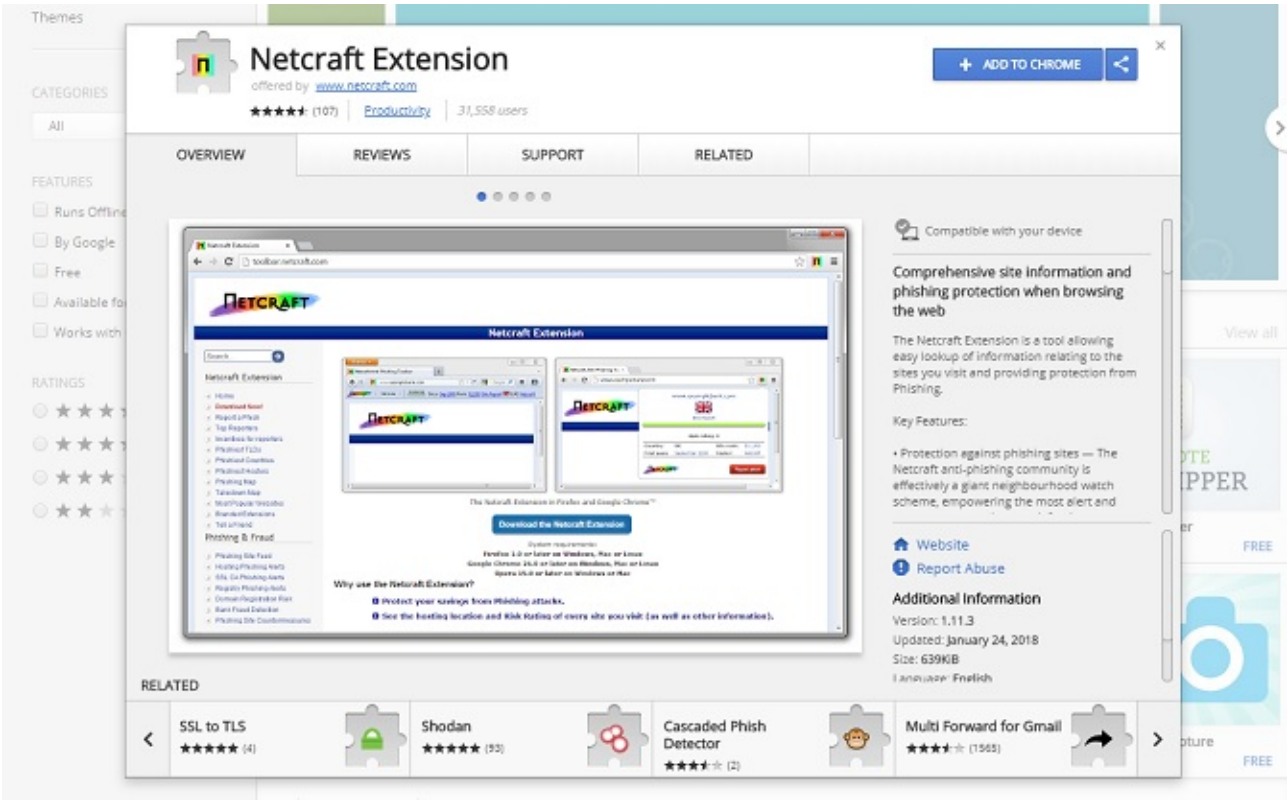
Webutation's ratings factor in a number of sources in its algorithm, but as an open community, it relies on its userbase. Click on the icon and you can find out more about the site on **webutation.net**, which also allows you to leave your own rating.

Obviously, you might not know whether a site really is a malware risk. That's why Webutation **checks for SSL certificates**, and scours other tools, including Google Safe Browsing, Norton Antivirus, and phishing blacklists. It also takes social reputation into consideration—if the site has an extensive, properly cited Wikipedia page, that's taken into account.

What makes this the natural successor to WOT? The fact that its algorithm also bases its ratings on the WOT Ratings Community! You get all the best stuff from that other popular extension, plus additional safety checks.

Download: **Webutation**

4. Netcraft Extension



Netcraft Extension is a similar tool to Webutation, so choose one or the other. Webutation certainly looks sleeker, while Netcraft appears a product of the early 2000s, at least visually. Nonetheless, they're both effective software.

Whereas Webutation gives you easy-to-see rating scores at the top of the page, you have to click on the Netcraft logo (located in the same place) to learn more. The available information, though, is excellent.

This is a community-supported add-on, so it warns of any phishing threats, and allows you to report a site as suspicious. You'll be able to see the flag for the country where the site is hosted; the actual host; and a numerical ranking to advise whether it's safe enough to visit.

There's also a site ranking, based on Netcraft users, and, most helpfully, full Site Reports. These list a whole host of interesting data, **like IP address** and any known web trackers operating through widgets and JavaScript. An extra bonus is its support of Perfect Forward Secrecy (PFS), which tells you if your personal data is secure in the event of an encryption key being compromised.

Netcraft works well, whether you're tech-obsessed or not. If a site is dubious, a warning will appear regardless. Again, you can ignore it, or return to safety.

Download: **Netcraft Extension**

5. Click&Clean

This is simply one of the best Chrome security add-ons of all time. Yes, really.

That's because it's **quick, easy, and thorough**, making your browsing sessions secure and private.

Click&Clean lets you delete all your private data with a single click. This can either be done *en masse*, or by selecting individual items. You can even choose the timescale that you wish to delete. You just select the icon in the toolbar and its menu will pop open: this has a **Windows 10-like design** so is eye-catching and colourful. All it takes to close your browser and delete browsing history is one click. In an emergency, this is essential.

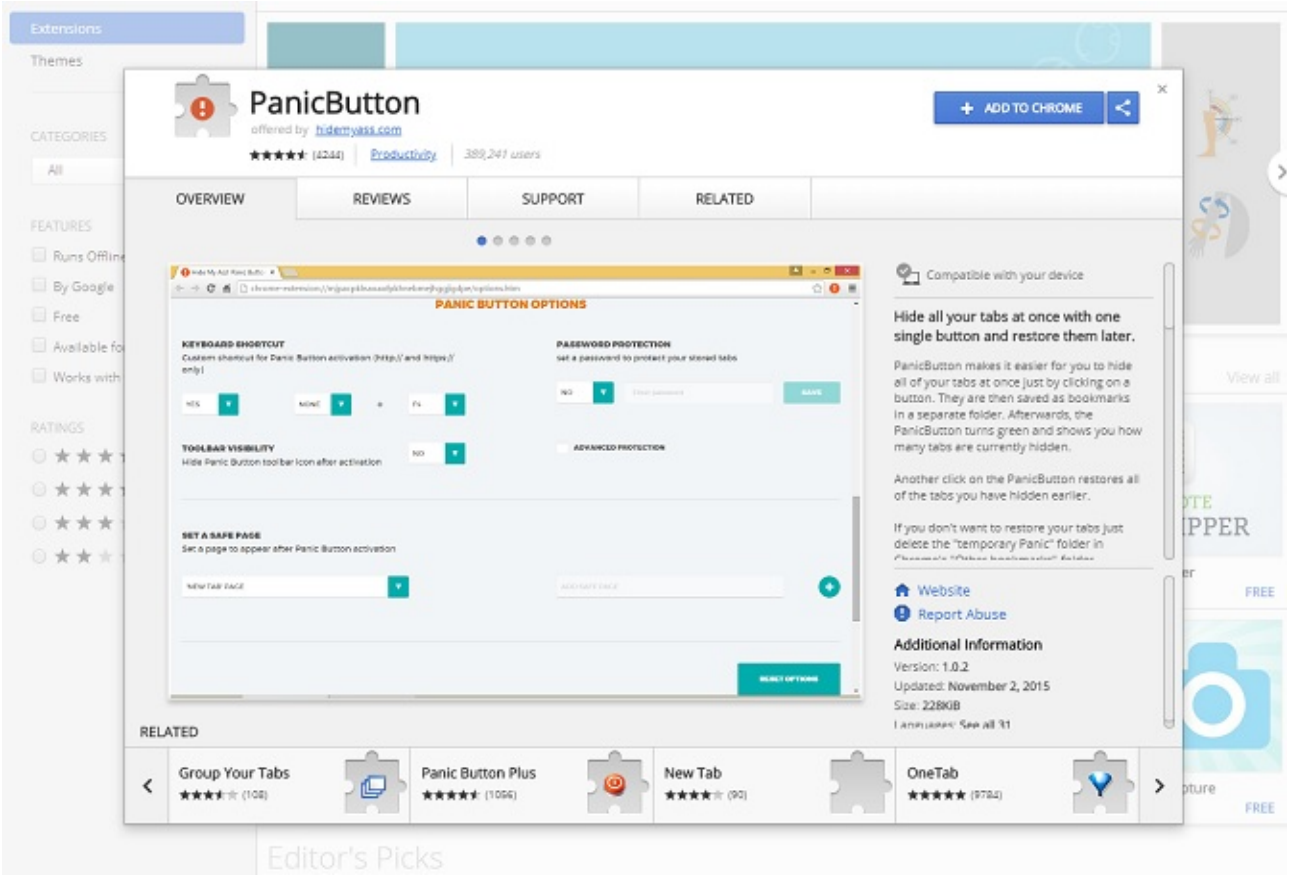
Your options are extensive, meaning you can get rid of your download history, cache, saved passwords and form data via cookies, and lots more. That's just from the Main tab; by switching, you can access information stored by other add-ons!

There are two added options that make Click&Clean extra special: password generation, which creates alphanumerical digits for any specified lengths; and clearing **data from Incognito Mode**.

You read that right: in-private browsing **isn't completely anonymous**. Of course, ISPs can still track you, and there's nothing you can do about that. But Click&Clean at least allows you to clear temporary files left on your PC by the sites you visit in order to recover data should a fault occur.

Download: **Click&Clean**

6. Panic Button



The easier you can browse securely, the better. That's why one-click extensions are so popular.

Panic Button takes this principle and applies it to your tabs. Just press a keyboard shortcut (thankfully customizable) and your tabs disappear. They then reset to a "safe page", i.e. whatever page you want displayed in emergencies.

Fortunately, you've not lost those tabs! They're stored in a list, which you can protect from prying eyes behind a password.

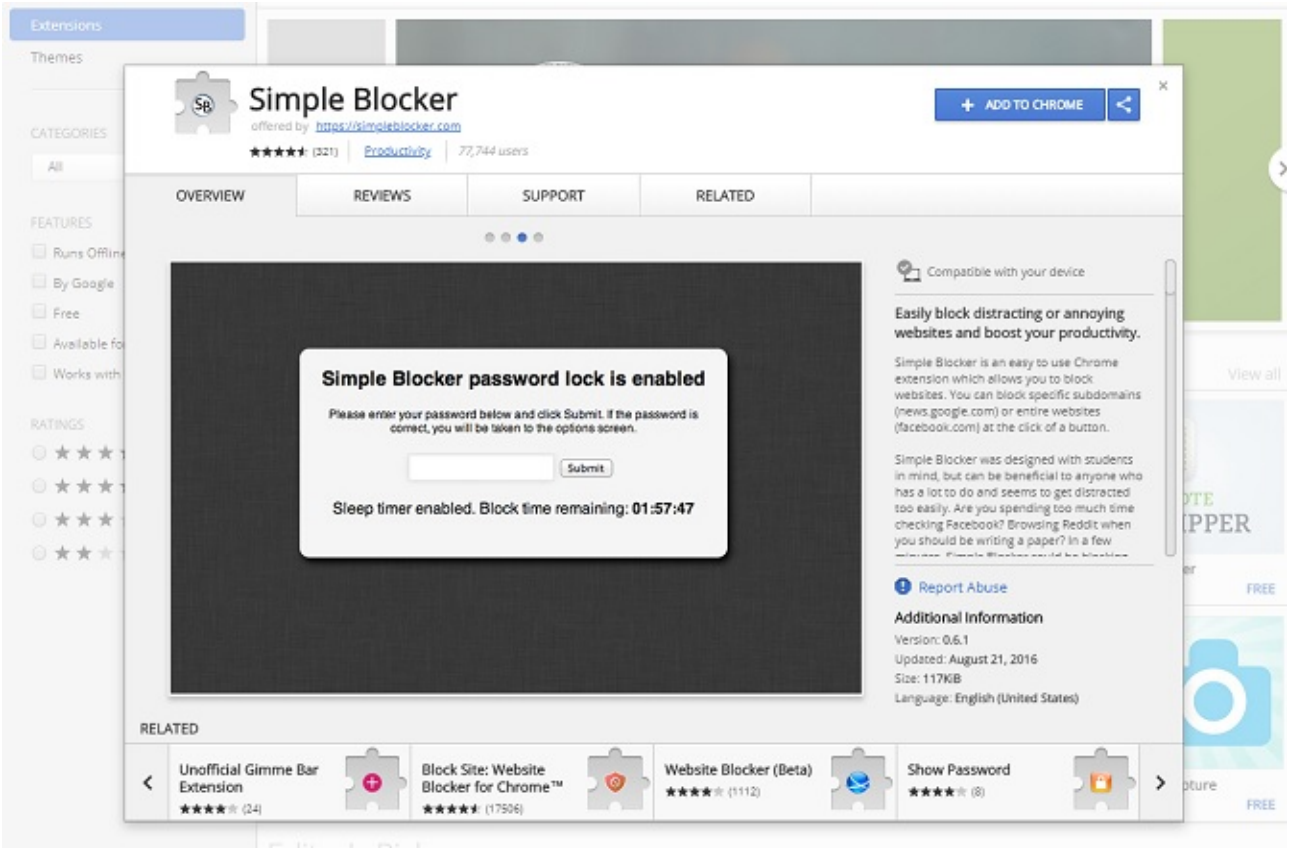
Obviously, this is designed for anyone viewing private stuff on their PC, **be it for Christmas shopping** or something more scandalous. It has a security purpose too.

Pop-ups can be annoying, right? But without an ad-blocker (**which are killing the net anyway**), there's little you can do to prevent them? Well, sort of.

Panic Button's list of tabs will include additional ads that have popped up in the background. Instead of restoring the full list, you can solely reopen the ones you actually *mean to*.

Download: **Panic Button**

7. Simple Blocker



There's a whole host of add-ons out there promising to lock individual tabs or your entire browser behind passwords. They're a neat idea, yet 9 times out of 10, they let you down. Take a look at the reviews, and those extensions prove troublesome. "Doesn't work," some will complain. "Makes Chrome crash," others will add.

Here's one that's designed as a productivity tool that doubles as a security measure. And it's brilliant at what it does, which is to simply lock you out of websites or subdomains.

Nearly 78,000 users trust it to block access to Facebook, Twitter, Reddit, and other distractions. Its initial **target audience was students**, hence the inclusion of a timer that lets you back into a site once you've finished studying.

However, it may also be used to prevent users from accessing suspicious sites. If you've young children, you can stop them viewing adult material. If you've found a page family members are likely to frequent but is now riddled with malware (which often happens when transferring ownership), this will stop that risk.

With Simple Blocker you have an unlimited blacklist, so block to your heart's content!

Download: **Simple Blocker**

8. Blur

Watch the Youtube video here: **Blur in One Minute**

Despite all the warnings, the majority of us use one or two passwords for *everything*. It's madness, of course: if it's leaked, hackers can easily find their way into your other accounts. It's even more concerning if you rely on "qwerty123" or "abcdefg".

Blur, however, requires you to remember one password. And that's it.

You need one code to access Blur, and **the extension does the rest for you**: namely, it masks your email address and password, filling in forms with anonymous data. If a data breach occurs, you've got no worries because your information isn't even held by the company!

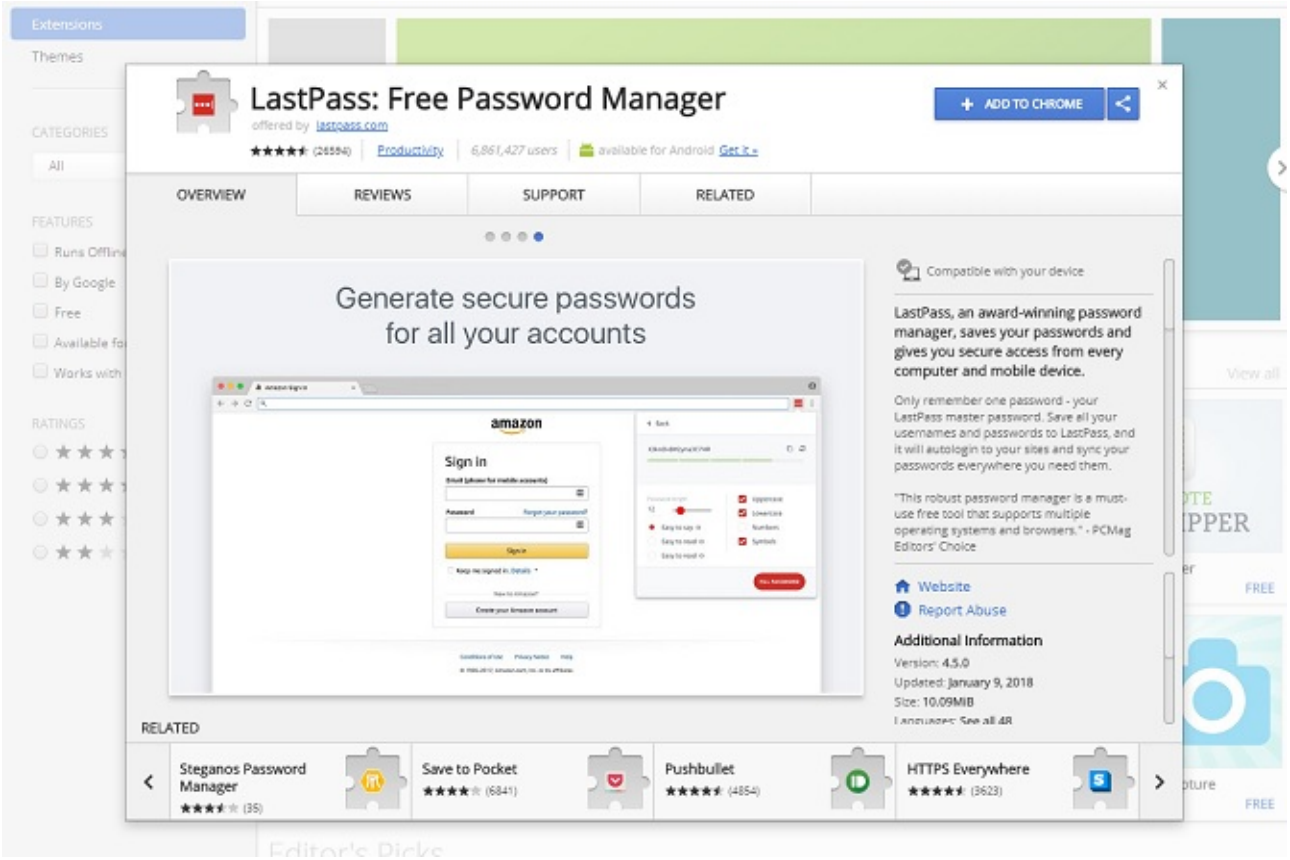
Let's say you're **setting up an account on PayPal**. You click on the email address field; Blur opens and generates a random one for you. The same goes for passwords. (Don't worry: emails from PayPal, or wherever, sent to this temporary address are automatically forwarded to your normal inbox. You can turn that function off if the company starts spamming you.)

There are two versions of Blur: your standard free one, and a Premium variant with annual or lifetime payment options. The former does a solid job, so there's no great need to upgrade; however, Premium further lets you mask credit card numbers. It adds a fantastic layer of added protection. Blur's available on numerous devices and browsers, so Premium users can sync with their smartphones or tablets.

This is a seriously genius add-on.

Download: **Blur**

9. LastPass



Or maybe you'd prefer to use the most **popular password managers** available.

You might recall the name, even if you're not *au fait* with the software. That's because it's hit the headlines a couple of times in the past few years, causing some to abandon ship. But right now, nearly 7 million users still trust it.

There were fears over CPU exploits, Meltdown and Spectre, which affect LastPass; further back, Google Project Zero found a vulnerability in the password manager.

Realistically, all software has vulnerabilities. What matters is how swiftly the companies react to them; typically, if an update is offered, you should install it. LastPass has rolled with the punches, so we don't see any reason you should avoid it.

It basically does the same stuff Blur does, except offers an extra layer of customization in its vault.

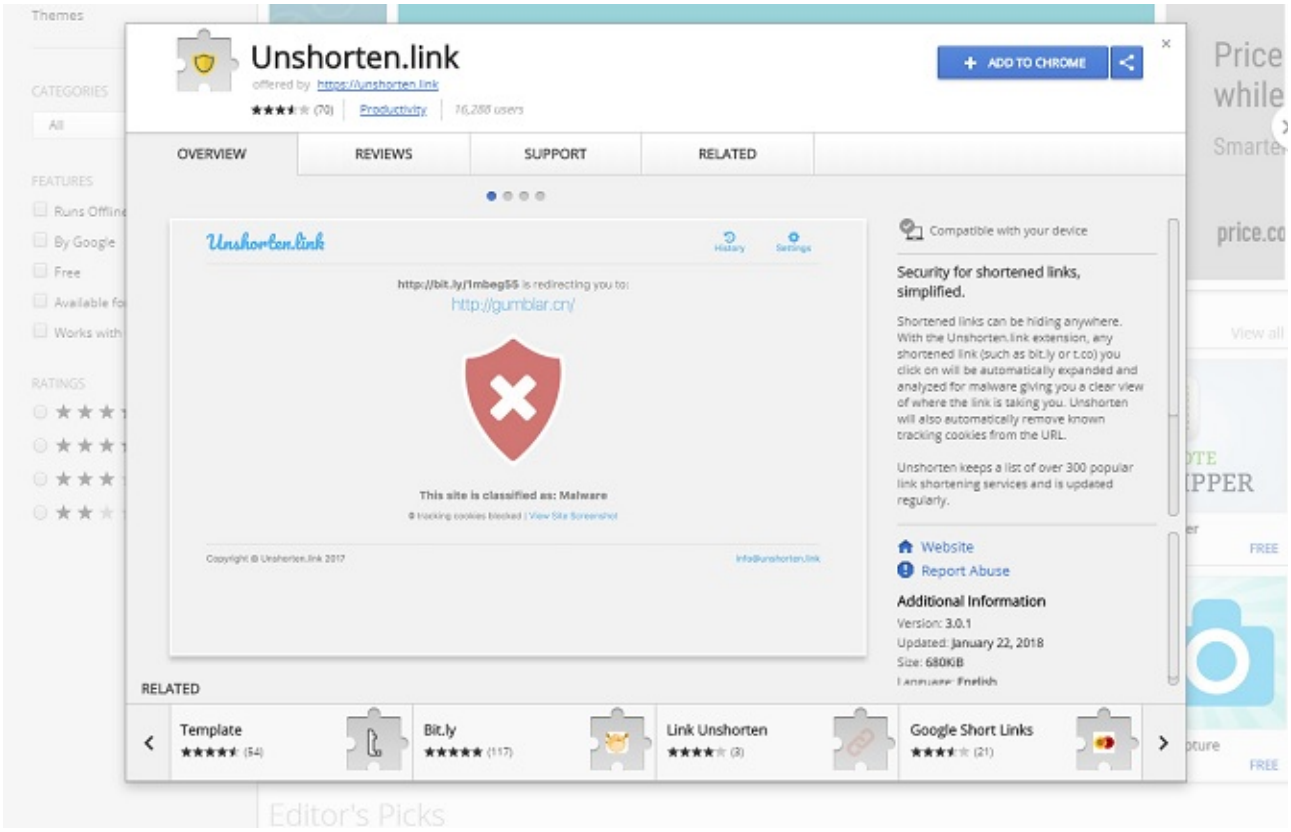
Yes, there are concerns. As the most popular manager, it attracts a lot of hackers. Its security, though, is top-notch.

Brute force attacks are rendered virtually pointless, as LastPass doesn't store your password. Instead, it verifies your identity using a one-way salted hash, then allows access to your vault using your decryption key (always stored on your device). Further encryption methods are used to when data is in transit.

This is a very strong system. Due to its swollen userbase, you'll hear about any potential (and comparatively rare) problems sharpish and then be notified by LastPass about what to do. In most cases, it'll involve updating and changing your master password.

Download: **LastPass**

10. Unshorten.link



Shortened links were all the rage a little while ago. Now, you don't see them so often. But they're deceptive: you'll still find them on social media, and affiliate schemes (Amazon, for instance).

Pages use them either as a quick way to redirect readers without including a lengthy URL or to hide the endpoint of a link. It's the latter you should be worried about. You could end up on a suspicious website, downloading malicious software.

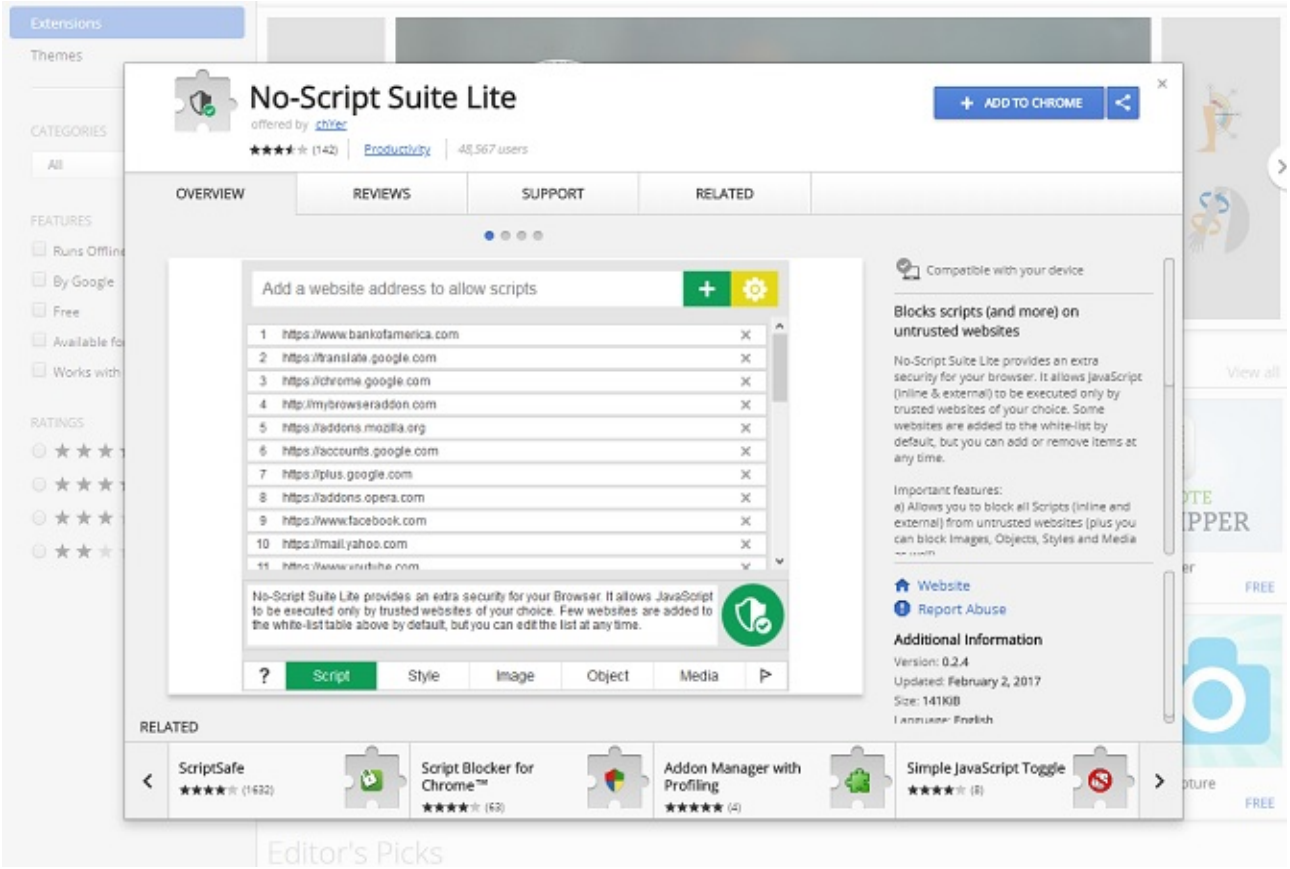
Unshorten.link does exactly what it says on the tin. Whenever you click on a condensed URL, you'll be sent to a "filter page" that shows you the full address. This might mean nothing to you, which is why you can choose to see a full screenshot of the destination.

Most importantly, it checks the link and warns you if it detects malware. You can choose not to see the filter page if Unshorten.link deems it safe too.

It might not be used all that frequently, but you may be surprised. And when it is used, you'll be thankful for it.

Download: **Unshorten.link**

11. No Script Suite Lite



JavaScript is a programming language that forms the foundations for much of the internet in its current form. It's an important part in our browsing experiences, and also forms the backbone of apps and online infrastructure. You can see why would-be programmers continue to learn it, and why many **consider it the language of the future**.

But sometimes, it's a bad thing.

Why? **It can hide malicious activity**, including snooping and ransomware. You could simply disable JavaScript, but functionality will decrease. Facebook won't look right (if it shows up at all); comments sections won't load (**although that can be a positive**); most seriously, YouTube and Netflix won't work.

Nightmare.

It really is a catch-22. Much of the web won't function properly without it; but by enabling it, you leave yourself open to all sorts of issues, most notably malware.

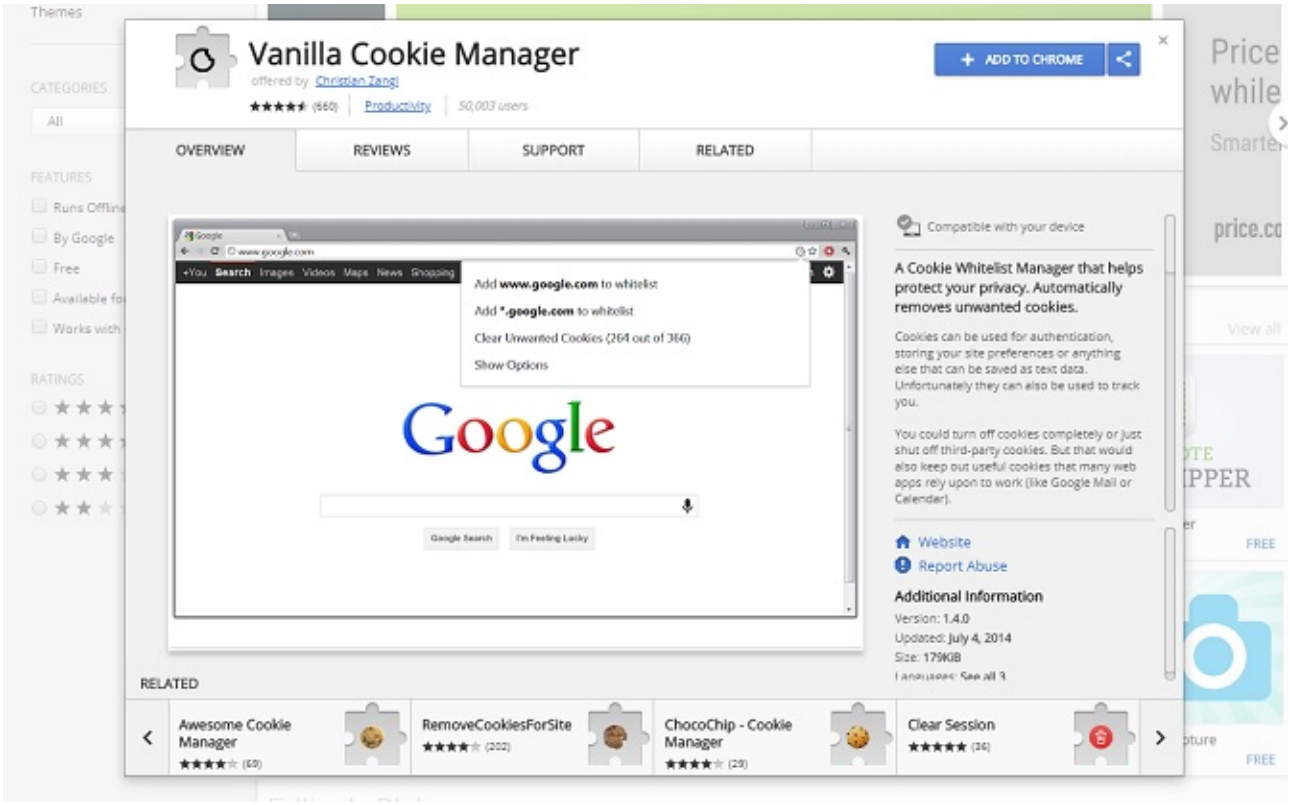
No Script Suite Lite is a solution to this problem.

It limits the sites that run JavaScript solely to the ones you trust. Just add them into your whitelist and you can carry on surfing. If you're worried you're not experiencing a site to its fullest but you're not certain enough to add it to your trusted list, you can also toggle the extension on and off in the toolbar.

No Script Suite Lite is best when running in conjunction with Webutation, Netcraft Extension, or a similar security add-on.

Download: **No Script Suite Lite**

12. Vanilla Cookie Manager



This actually works in a similar way to No Script Suite Lite. The idea behind Vanilla Cookie Manager is to limit a specific function when browsing without inhibiting performance.

Just like JavaScript, cookies can be a force for good. They're files stored on your PC, recording contractual agreements (ironically, including the use of cookies) and information you might type into forms. Autofill is a direct result of cookies. They speed up your interface by saving preferences. Anyone who uses Incognito Mode knows what a pain it can be to re-tread the same ground repeatedly.

However, they do track you. That's their direct function. How do you feel about businesses storing private data about you? It's a personal thing, and doesn't mean you're a privacy freak decked out in tin foil if you don't want **Google knowing loads about you**. In fact, it's very healthy to be privacy-conscious.

That's why Vanilla Cookie Manager clears cookies, except on sites in your whitelist.

Whenever you visit a site, go to the toolbar, and, if you trust it, add it to your whitelist. This means cookies will be saved. Any site you don't trust will be blacklisted.

Download: **Vanilla Cookie Manager**

13. TunnelBear VPN

You've probably heard a lot about **virtual private networks** (VPN). In case you're unfamiliar with them, picture a tunnel between your device and the website you're visiting. This tunnel is a form of encryption, meaning any personal information sent between the two is scrambled. Without it, you might be victim of intrusion, including **man-in-the-middle attacks** (MITM).

Chrome is already one of the safest browsers available, but it's somewhat inferior to Opera because the latter boasts **its own in-built VPN**. TunnelBear bolts on this extra level of privacy.

Search for "VPNs" in the Chrome store and you'll see vast amounts of them. It's very easy to fall in love with TunnelBear though. Over 20 million users across multiple platforms agree. Its creators appear to have good morals on their side, so don't log any data and publish security audits carried out independently by third parties.

Due to its fun graphics, you can use it to introduce the concept of encryption to children. Why not instil an interest in secure browsing at a young age?

Oh, and users can subsequently download **RememBear**, a neat password manager by the same makers. This is quickly becoming a brand you can count on for quality software suitable for all ages.

Download: **TunnelBear VPN**

What Else Have We Missed?

With the number of Chrome extensions constantly swelling, it's impossible to note down all the handy add-ons that sharpen up your security and privacy. It's also a very unpredictable thing: a popular extension can suddenly vanish from the store and you're back to stage one.

Read more stories like this at