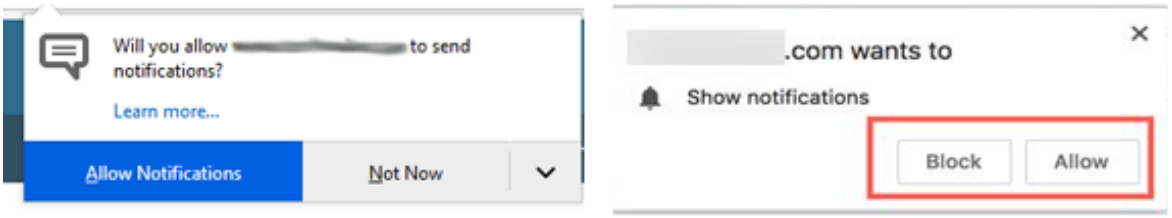
Be Very Sparing in Allowing Site Notifications

Published: 2020-11-18 · Archived: 2026-04-06 01:36:03 UTC

An increasing number of websites are asking visitors to approve “notifications,” browser modifications that periodically display messages on the user’s mobile or desktop device. In many cases these notifications are benign, but several dodgy firms are paying site owners to install their notification scripts and then selling that communications pathway to scammers and online hucksters.



Notification prompts in Firefox (left) and Google Chrome.

When a website you visit asks permission to send notifications and you approve the request, the resulting messages that pop up appear outside of the browser. For example, on Microsoft Windows systems they typically show up in the bottom right corner of the screen — just above the system clock. These so-called “push notifications” rely on an Internet standard designed to work similarly across different operating systems and web browsers.

But many users may not fully grasp what they are consenting to when they approve notifications, or how to tell the difference between a notification sent by a website and one made to appear like an alert from the operating system or another program that’s already installed on the device.

This is evident by the apparent scale of the infrastructure behind a relatively new company based in Montenegro called **PushWelcome**, which advertises the ability for site owners to monetize traffic from their visitors. The company’s site currently is ranked by Alexa.com as among the top 2,000 sites in terms of Internet traffic globally.

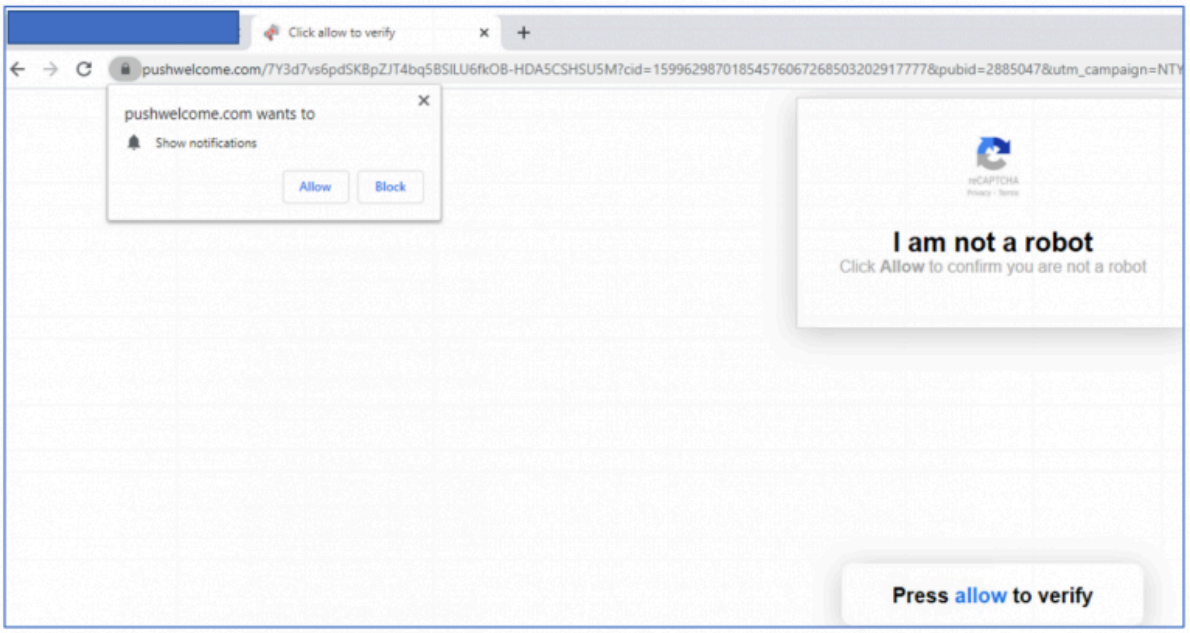
Website publishers who sign up with PushWelcome are asked to include a small script on their page which prompts visitors to approve notifications. In many cases, the notification approval requests themselves are deceptive — disguised as prompts to click “OK” to view video material, or as “CAPTCHA” requests designed to distinguish automated bot traffic from real visitors.

An ad from PushWelcome touting the money that websites can make for embedding their dodgy push notifications scripts.

Approving notifications from a site that uses PushWelcome allows any of the company's advertising partners to display whatever messages they choose, whenever they wish to, and in real-time. And almost invariably, those messages include misleading notifications about security risks on the user's system, prompts to install other software, ads for dating sites, erectile disfunction medications, and dubious investment opportunities.

That's according to a deep analysis of the PushWelcome network compiled by Indelible LLC, a cybersecurity firm based in Portland, Ore. **Frank Angiolelli**, vice president of security at Indelible, said rogue notifications can be abused for credential phishing, as well as foisting malware and other unwanted applications on users.

"This method is currently being used to deliver something akin to adware or click fraud type activity," Angiolelli said. "The concerning aspect of this is that it is so very undetected by endpoint security programs, and there is a real risk this activity can be used for much more nefarious purposes."



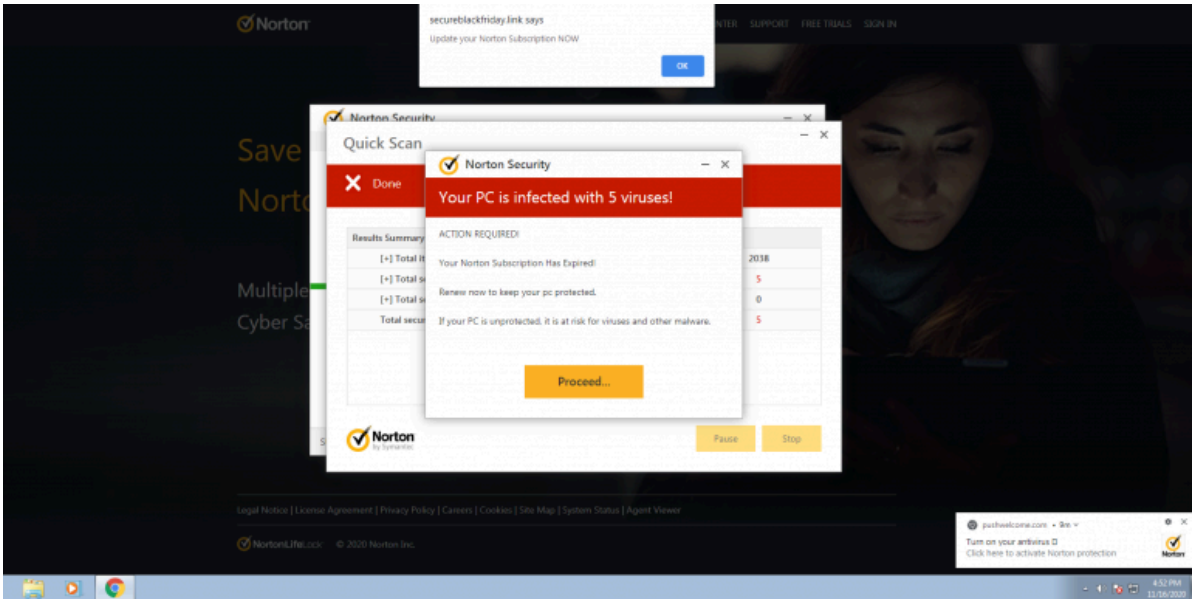
Sites affiliated with PushWelcome often use misleading messaging to trick people into approving notifications.

Angiolelli said the external Internet addresses, browser user agents and other telemetry tied to people who've accepted notifications is known to PushWelcome, which could give them the ability to target individual organizations and users with any number of fake system prompts.

Indelible also found browser modifications enabled by PushWelcome are poorly detected by antivirus and security products, although he noted Malwarebytes reliably flags as dangerous publisher sites that are associated with the notifications.

Indeed, Malwarebytes' **Pieter Arntz** warned about malicious browser push notifications in a January 2019 blog post. That post includes detailed instructions on how to tell which sites you've allowed to send notifications, and how to remove them.

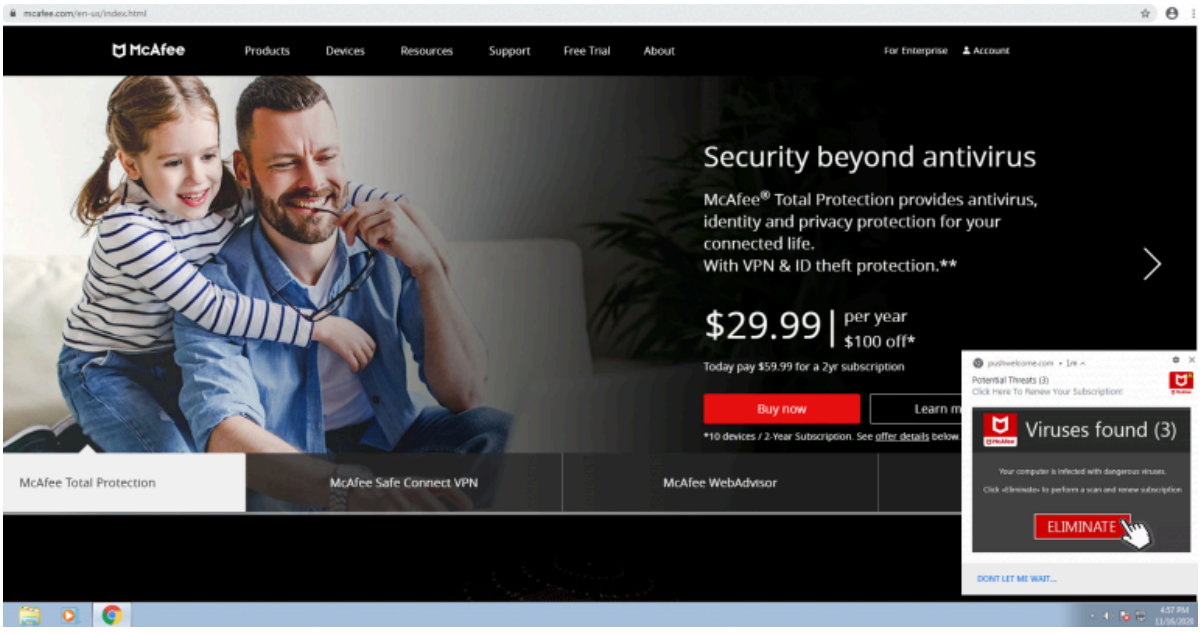
KrebsOnSecurity installed PushWelcome's notifications on a brand new Windows test machine, and found that very soon after the system was peppered with alerts about malware threats supposedly found on the system. One notification was an ad for **Norton** antivirus; the other was for **McAfee**. Clicking either ultimately led to "buy now" pages at either Norton.com or McAfee.com.



Clicking on the PushWelcome notification in the bottom right corner of the screen opened a Web site claiming my brand new test system was infected with 5 viruses.

It seems likely that PushWelcome and/or some of its advertisers are trying to generate commissions for referring customers to purchase antivirus products at these companies. McAfee has not yet responded to requests for comment. Norton issued the following statement:

> "We do not believe this actor to be an affiliate of NortonLifeLock. We are continuing to investigate this matter. NortonLifeLock takes affiliate fraud and abuse seriously and monitors ongoing compliance. When an affiliate partner abuses its responsibilities and violates our agreements, we take necessary action to remove these affiliate partners from the program and swiftly terminate our relationships. Additionally, any potential commissions earned as a result of abuse are not paid. Furthermore, NortonLifeLock sends notification to all of our affiliate partner networks about the affiliate's abuse to ensure the affiliate is not eligible to participate in any NortonLifeLock programs in the future."



Requests for comment sent to PushWelcome via email were returned as undeliverable. Requests submitted through the contact form on the company's website also failed to send.

While scammy notifications may not be the most urgent threat facing Internet users today, most people are probably unaware of how this communications pathway can be abused.

What's more, dodgy notification networks could be used for less conspicuous and sneakier purposes, including spreading fake news and malware masquerading as update notices from the user's operating system. I hope it's clear that regardless of which browser, device or operating system you use, it's a good idea to be judicious about which sites you allow to serve notifications.

If you'd like to prevent sites from ever presenting notification requests, check out this guide, which has instructions for disabling notification prompts in Chrome, Firefox and Safari. Doing this for any devices you manage on behalf of friends, colleagues or family members might end up saving everyone a lot of headache down the road.
