KnowBe4
Human error. Conquered.

Malicious Browser Notifications

The New Phishing Attack Not Blocked by Your Current Cyber Defense

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

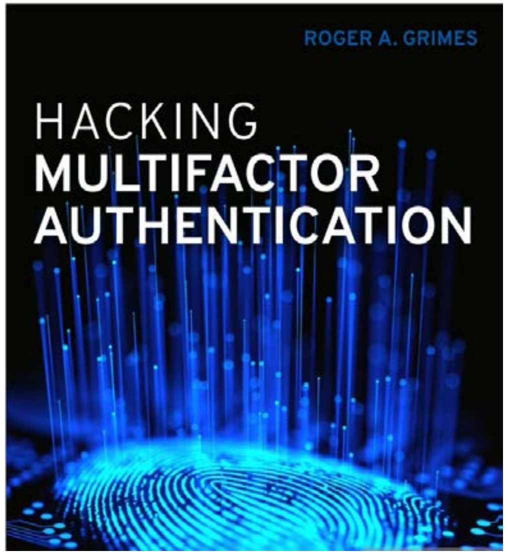
About Roger

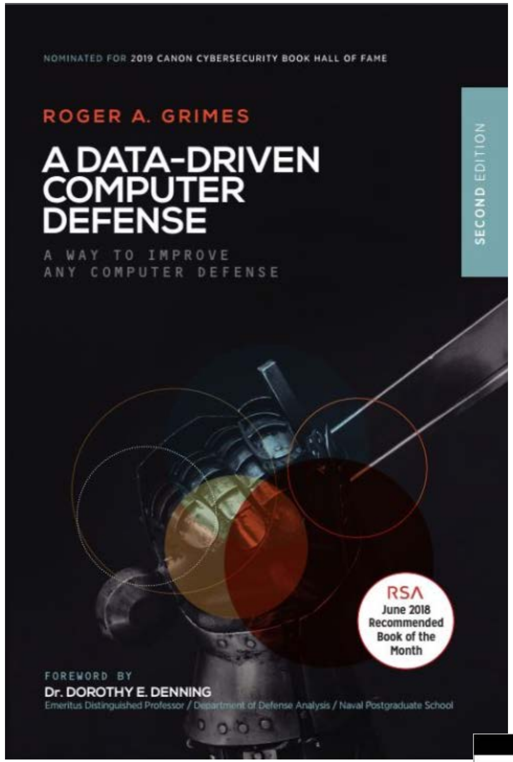
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

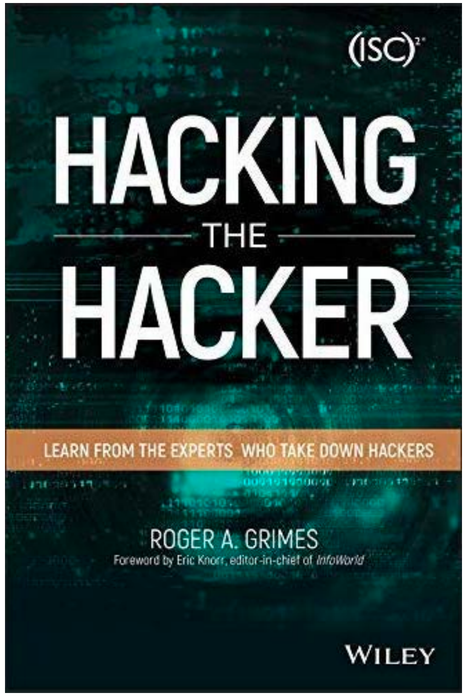
Certification exams passed include:

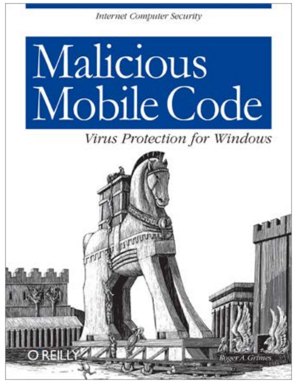
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

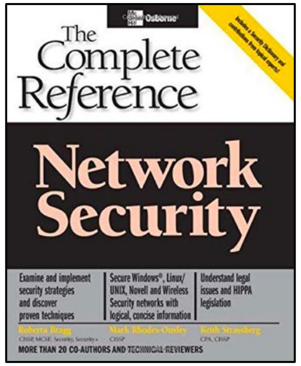
Roger's Books

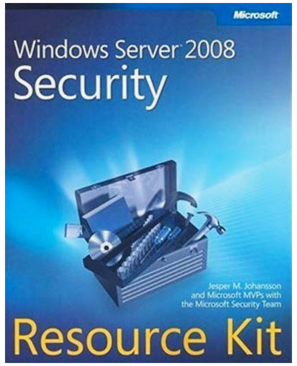


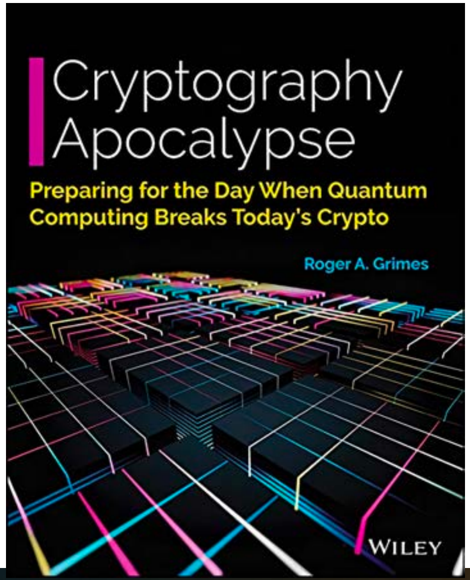

NOMINATED FOR 2019 CANON CYBERSECURITY BOOK HALL OF FAME
ROGER A. GRIMES
A DATA-DRIVEN COMPUTER DEFENSE
A WAY TO IMPROVE ANY COMPUTER DEFENSE
SECOND EDITION
RSA June 2018 Recommended Book of the Month
FOREWORD BY Dr. DOROTHY E. DENNING
Emeritus Distinguished Professor / Department of Defense Analysis / Naval Postgraduate School

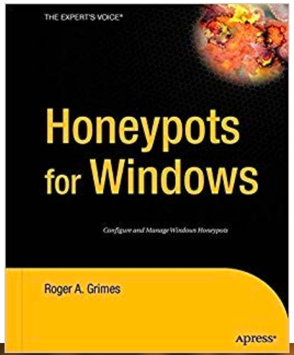

(ISC)²
HACKING THE HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

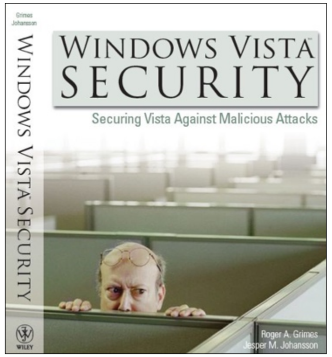


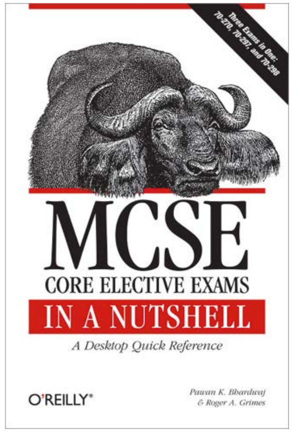



Microsoft
Windows Server 2008 Security
Jesper M. Johansson and Microsoft MVPs with the Microsoft Security Team
Resource Kit


Cryptography Apocalypse
Preparing for the Day When Quantum Computing Breaks Today's Crypto
Roger A. Grimes
WILEY






MCSE
CORE ELECTIVE EXAMS
IN A NUTSHELL
A Desktop Quick Reference
O'REILLY
Pawan K. Bhardwaj & Roger A. Grimes

TRAIN
PHISH
ANALYZE

About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

AMERICA'S FASTEST-GROWING PRIVATE COMPANIES Inc. 500

Entrepreneur | cultureiQ TOP COMPANY CULTURES 2017

Learn

- Notification basics
- How legitimate websites are targeted to deliver these stealthy phishing attacks
- Why browser notification phishing attacks bypass your cyber defenses
- Other sneaky browser attacks the bad guys use to infiltrate your network
- How to shore up your defenses and to protect against them all

Before Notification Maliciousness

For decades, malware writers and phishers have exploited “transitive” trust:

- Banner ads

Typical scenario#1:

1. Legitimate vendor asks trusted marketer for help with web campaign
2. Marketer reaches out to trusted web campaign firm for help
3. Web campaign firm promises a certain number of views
4. Web campaign firm subcontracts with another sometimes dodgy vendor who is really adware group

Typical scenario#2:

1. Malware/phisher group poses as legitimate company and buys ads
2. They create online content for display in ad
3. Legitimate content is switched out for malicious content when wanted

Before Notification Maliciousness

For decades, malware writers and phishers have exploited “transitive” trust:

- Malicious banner ad campaigns
  - Very sophisticated
  - One innocent-looking element replaced
  - Ex: https://www.domain.com/counter.html
    - Original URL points to a normal “counter” applet
    - Then counter.html is switched out on the fly with malicious JavaScript
  - Not shown to anyone legitimate involved with ad buy/sell
  - People checking reports of maliciousness don’t find anything wrong
  - Fact: Most major websites have no clue about what is executing on their web sites
  - 50% to 90% of all client-side executing code is from third parties
    - Much of it is not good
  - Many companies hiring companies, like The Media Trust, dedicated to quickly detecting maliciousness on legitimate web pages

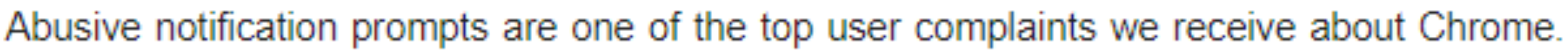
Before Notification Maliciousness

For decades, malware writers and phishers have exploited “transitive” trust:

- Banner ads

- Rogue applets
- Code snippets
  - “Must retain counter to reuse” or “Must retain source URL to reuse”
- Web site “well poisoning”

- And now hackers/phishers are starting to abuse browser/desktop notifications
- Google says



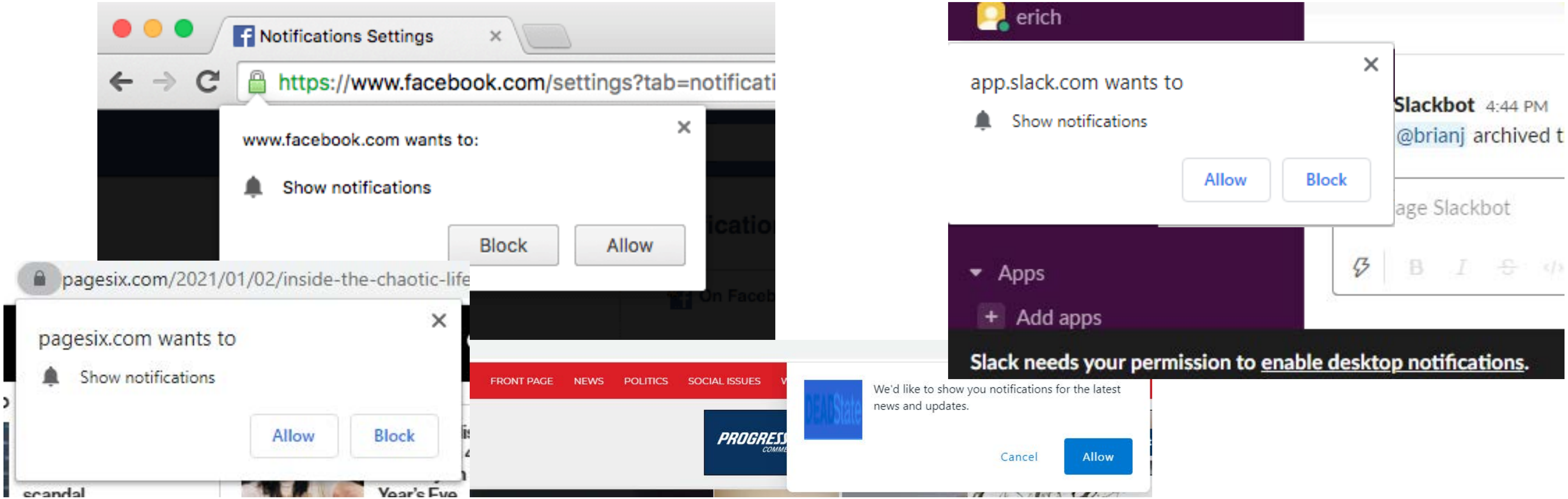
Abusive notification prompts are one of the top user complaints we receive about Chrome.

Learn

Notification Basics

Notification Basics

- Known as **browser/desktop notifications** or **push notifications**
- Allows display messages to be sent to user outside of their browser/tab or app after the notification permission was given by the user



Notifications Settings

https://www.facebook.com/settings?tab=notificati

www.facebook.com wants to:

Show notifications

Block Allow

pagesix.com/2021/01/02/inside-the-chaotic-life

pagesix.com wants to

Show notifications

Allow Block

FRONT PAGE NEWS POLITICS SOCIAL ISSUES

We'd like to show you notifications for the latest news and updates.

Cancel Allow

erich

app.slack.com wants to

Show notifications

Allow Block

Slackbot 4:44 PM

@brianj archived t

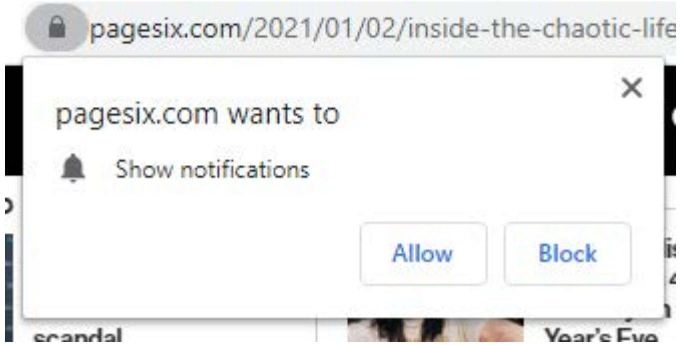
Apps

Add apps

Slack needs your permission to enable desktop notifications.

Notification Basics

- Each app/website must first ask user permission to send future notifications
  - **Default**
    - User can be asked to approve; else deny by default
  - **Granted**
    - User approved, future notifications can be sent
  - **Denied**
    - User denied, notifications cannot be sent for that app or website



pagesix.com/2021/01/02/inside-the-chaotic-life

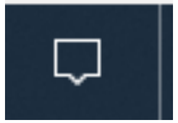
pagesix.com wants to

Show notifications

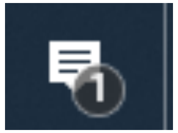
Notification Basics

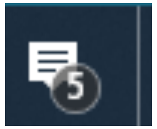
Desktop notifications

- May be shown on desktop over other apps or a gentle reminder shown
  - Windows 10 shows an empty message dialog box in lower right taskbar when there are no notifications waiting



  - Shows a message dialog box along with notification message count when notifications are waiting

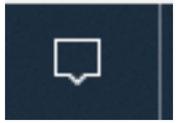




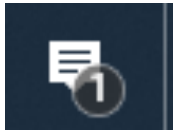
Notification Basics

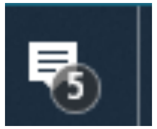
Desktop notifications

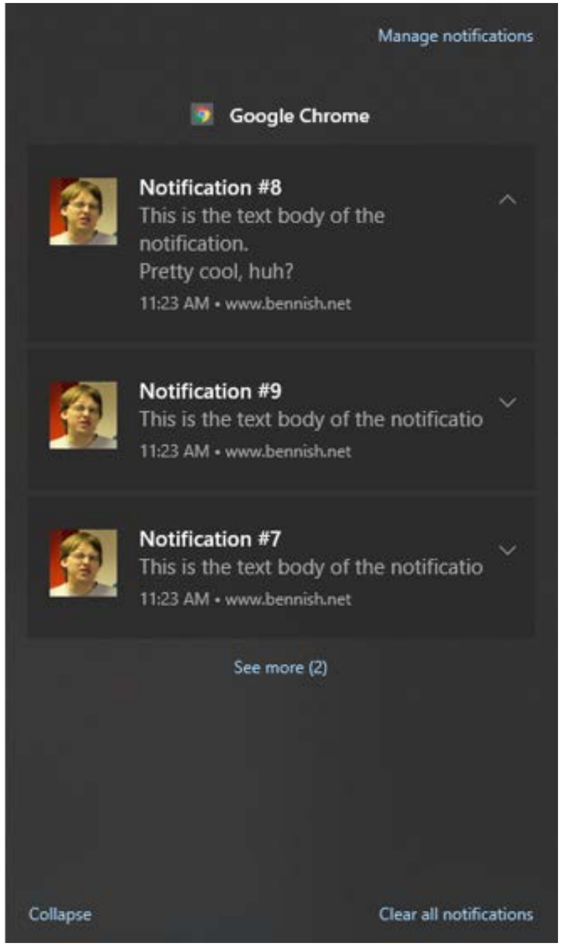
- May be shown on desktop over other apps or a gentle reminder shown
  - Windows 10 shows an empty message dialog box in lower right taskbar when there are no notifications waiting



  - Shows a message dialog box along with notification message count when notifications are waiting







Manage notifications

Google Chrome

Notification #8
This is the text body of the notification.
Pretty cool, huh?
11:23 AM • www.bennish.net

Notification #9
This is the text body of the notificatio
11:23 AM • www.bennish.net

Notification #7
This is the text body of the notificatio
11:23 AM • www.bennish.net

See more (2)

Collapse

Clear all notifications

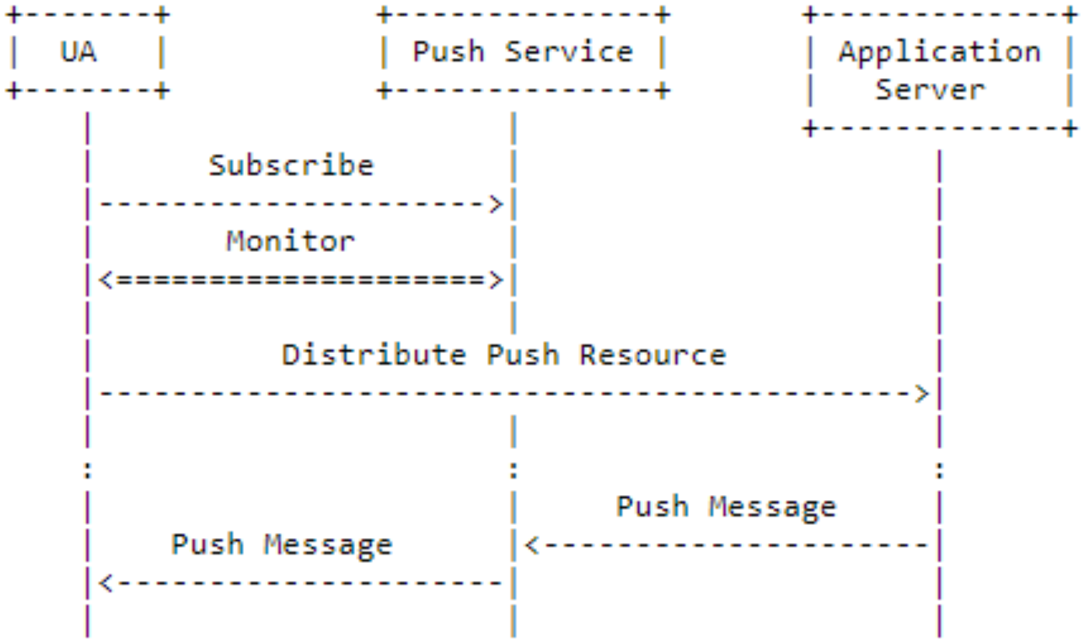
Notification Basics

- Based on a standard to allow developers to send messages to end-user's cross-platform using a single programming method
- Early versions introduced around 2009 (known as JavaScript Desktop Notification API then)
- W3C introduced an updated HTML5 version called the **Notification API** in 2014 (may be treated/merged with Push Notification API)
- Started to be more abused in 2019
- Browsers and operating systems must support the Notification API
- Supported on Microsoft Edge, Google Chrome, Apple Safari (desktop only), Opera, Mozilla Firefox, but not Internet Explorer
  - Desktop and mobile versions may support different feature sets

Notification Basics

It’s Even an RFC (Request for Comments)

- **RFC 1030 - Generic Event Delivery Using HTTP Push**
- Created Dec. 2016
- RFCs are essential Internet standards and rules
- https://tools.ietf.org/html/rfc8030
- Originally used registered port TCP 1001, but now uses 443 to get past firewall issues



```
+-------+           +--------------+       +-------------+
|  UA   |           | Push Service |       | Application |
+-------+           +--------------+       |   Server    |
    |                      |               +-------------+
    |      Subscribe       |                      |
    |--------------------->|                      |
    |       Monitor        |                      |
    |<====================>|                      |
    |                      |                      |
    |          Distribute Push Resource           |
    |-------------------------------------------->|
    |                      |                      |
    :                      :                      :
    |                      |     Push Message     |
    |    Push Message      |<---------------------|
    |<---------------------|                      |
    |                      |                      |
```

Figure 1: WebPush Architecture

Notification Basics

Browser Version First Supported

- Chrome version 22
- Edge version 14
- Firefox version 22
- Opera version 25
- Safari version 7

*Not all features supported by all browsers (for example, Safari does not support opening new browser windows)

Notification Basics

Notifications Service Workers

- Each allowed notification process is called a “service worker” in developer-speak
- Service workers can update themselves, changing what they display and do
- Service workers can install other service workers
- Service workers can modify network content from their own pages
  - So what you see may not be what you get
- They don’t need your permission after the first allow

- Be careful of giving that initial trust

Notification Basics

Service Workers in General

- "A service worker is a JavaScript file that runs separately from the main browser thread, intercepting network requests, caching or retrieving resources from the cache, and delivering push messages"
  - From https://developers.google.com/web/ilt/pwa/introduction-to-service-worker

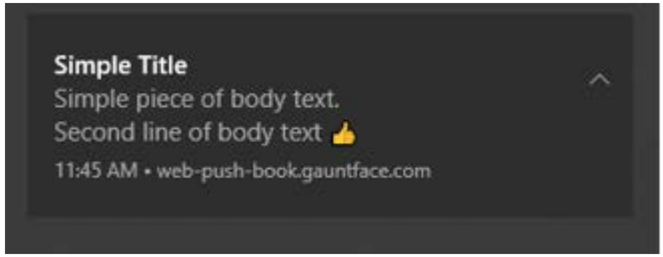
Service workers must be:

- Registered
  - They are registered before you get the (first) Allow prompt
- Installed
- Activated

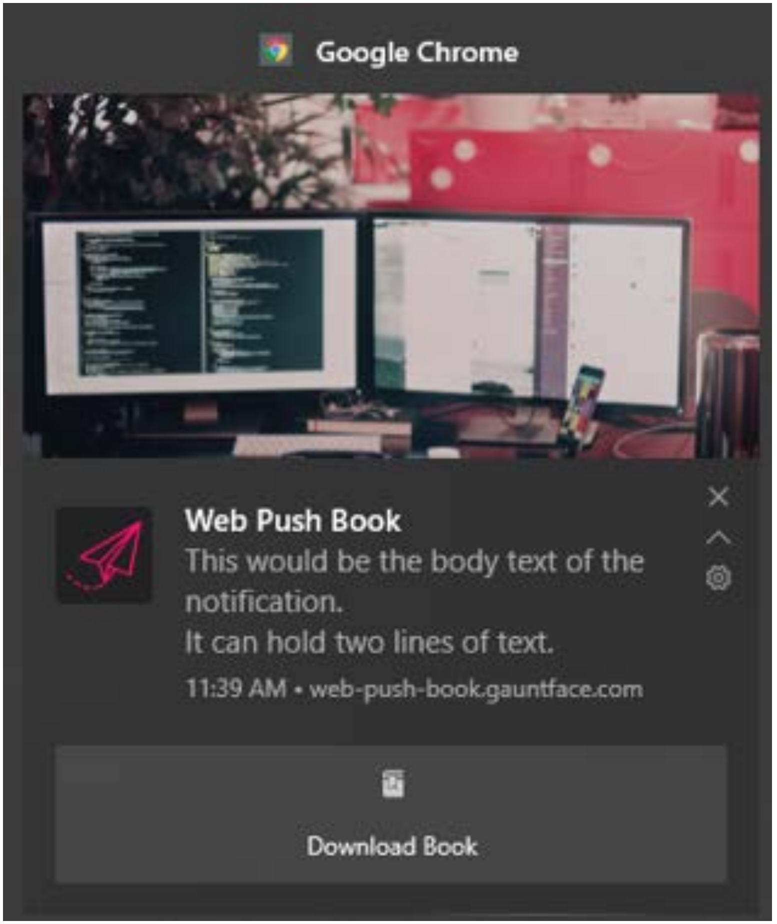
Notification Basics

Notifications are Multimedia

- Can display more than just text
- Icons/Emoticons, badges, etc.
- Pictures, content, URL links



Simple Title
Simple piece of body text.
Second line of body text 👍
11:45 AM • web-push-book.gauntface.com



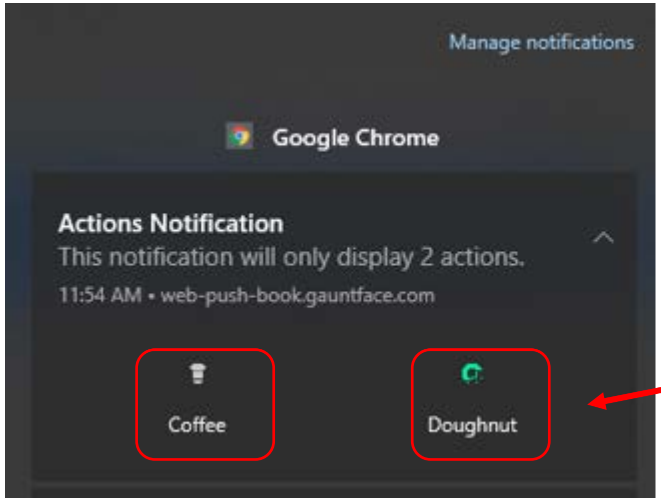
Web Push Book
This would be the body text of the notification.
It can hold two lines of text.
11:39 AM • web-push-book.gauntface.com

URLs significantly increase potential maliciousness

Notification Basics

<u>Notifications have Actions</u>

- Can create any button label(s) and link it to allowed actions
- Often limited to two actions at a time



Manage notifications

Google Chrome

Actions Notification

This notification will only display 2 actions.

11:54 AM • web-push-book.gauntface.com

buttons and labels

Actions may not always be good

Notification Basics

Notifications Actions

- Code example

```
self.registration.showNotification(‘New message from Vendor', {
  actions: [
   {action: ‘like', title: ‘Like'},
   {action: ‘reply', title: ‘Reply'}]
});
```

```
self.addEventListener('notificationclick', function(event) {
  var messageId = event.notification.data;
  event.notification.close();
  if (event.action === 'like') {
    silentlyLikeItem();
  }
  else if (event.action === 'reply') {
    clients.openWindow("/messages?reply=" + messageId);
  }
  else {
    clients.openWindow("/messages?reply=" + messageId);
  }
}, false);
```

Notification Basics

Notifications Actions

- Code example

```
self.registration.showNotification(‘Important alert from Microsoft Corporation!!!', {
  actions: [
   {action: ‘open', title: ‘Open'},
   {action: ‘open', title: ‘Ignore'}]
});
```

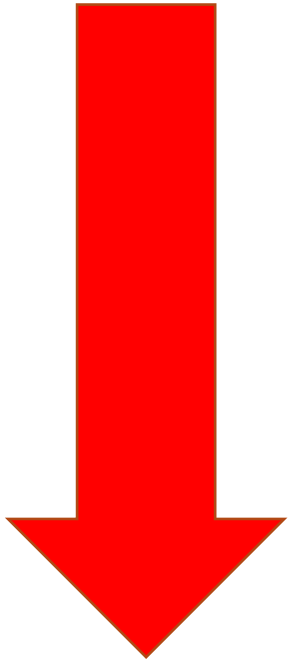
```
self.addEventListener('notificationclick', function(event) {
  var messageId = event.notification.data;
  event.notification.close();
else if (event.action === ‘open') {
    clients.openWindow((“https://microsoft.com.badurl.com”);
  }
  else {
    clients.openWindow(“https://microsoft.com.badurl.com”);
  }
}, false);
```

Notification Basics

Some Possible Notifications Actions

- Vibrate mobile devices
- Send sounds
- Display alerts
- Use Unicode characters
- Can open/delete/archive email
- Can initiate dialing telephone numbers
- Can require interaction (user can only click “OK”)
- Have OnClick, OnClose, OnError events
- Can open new browser windows at predetermined URLs

Growing risk



Notification Basics

Comments on Notifications Actions

- From https://developers.google.com/web/updates/2016/01/notification-actions

"The interesting thing is that the actions don't have to open up a new window, they can perform general application interactions without creating a user interface. For example, a user could "Like" or "Delete" a social media post that would perform the action on the user's local data and then synchronize it with the cloud without opening a UI…"

Notification Basics

Some Notification API Testing Sites

- https://web-push-book.gauntface.com/demos/notification-examples/
- https://www.bennish.net/web-notifications.html
- https://tests.peter.sh/notification-generator/#actions=3
- https://www.acme.com/webapis/notification.html

Notification Basics

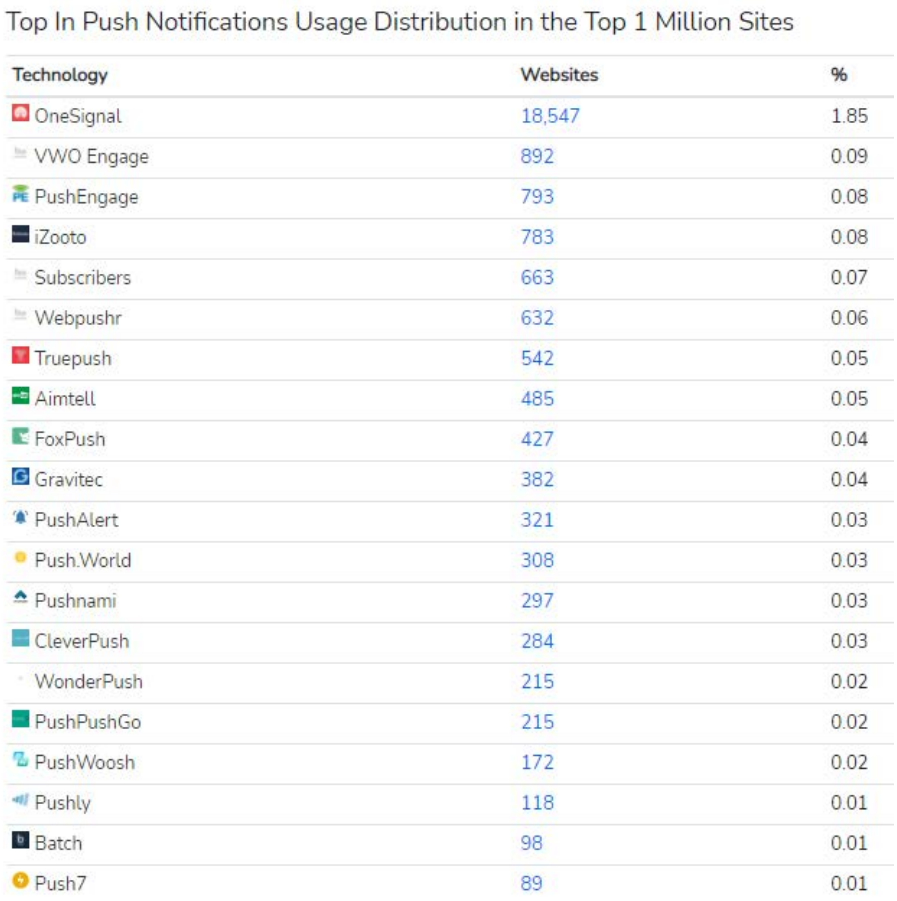
Web Sites/Apps/Organizations Use Notifications

- Many legitimate web sites use
- Many legitimate apps use
- Many legitimate organizations buy and sell access to other site's and app's notifications and the customers who allow them

Notification Basics

Push Notification Networks

- Many organizations exist to sell access to other subscribed notifications forming "push networks"
- **Sometimes not so legitimate organizations are involved**
- Table source: https://trends.builtwith.com/widgets/push-notifications

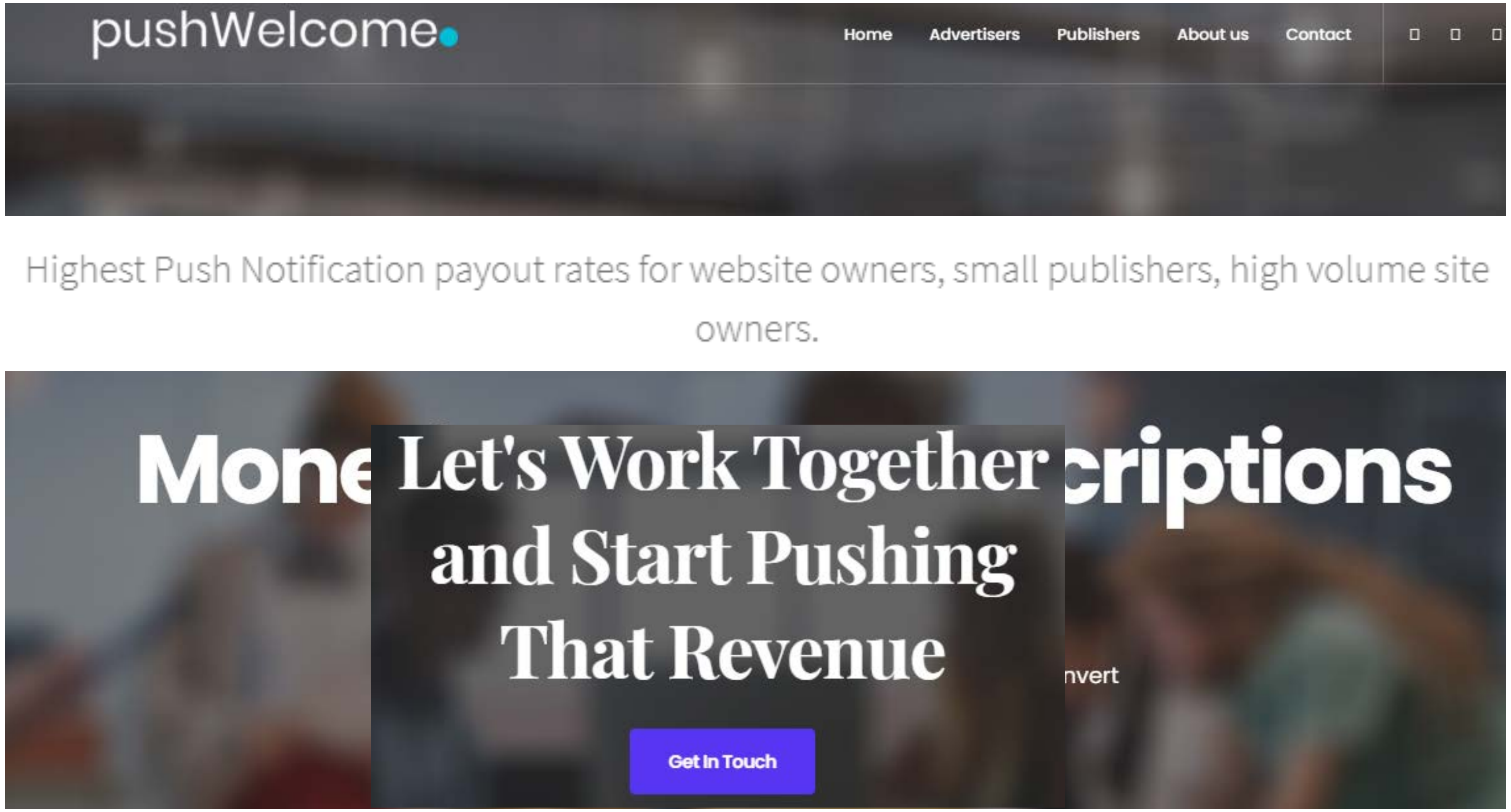


Top In Push Notifications Usage Distribution in the Top 1 Million Sites

Technology	Websites	%
OneSignal	18,547	1.85
VWO Engage	892	0.09
PushEngage	793	0.08
iZooto	783	0.08
Subscribers	663	0.07
Webpushr	632	0.06
Truepush	542	0.05
Aimtell	485	0.05
FoxPush	427	0.04
Gravitec	382	0.04
PushAlert	321	0.03
Push.World	308	0.03
Pushnami	297	0.03
CleverPush	284	0.03
WonderPush	215	0.02
PushPushGo	215	0.02
PushWoosh	172	0.02
Pushly	118	0.01
Batch	98	0.01
Push7	89	0.01

Notification Basics

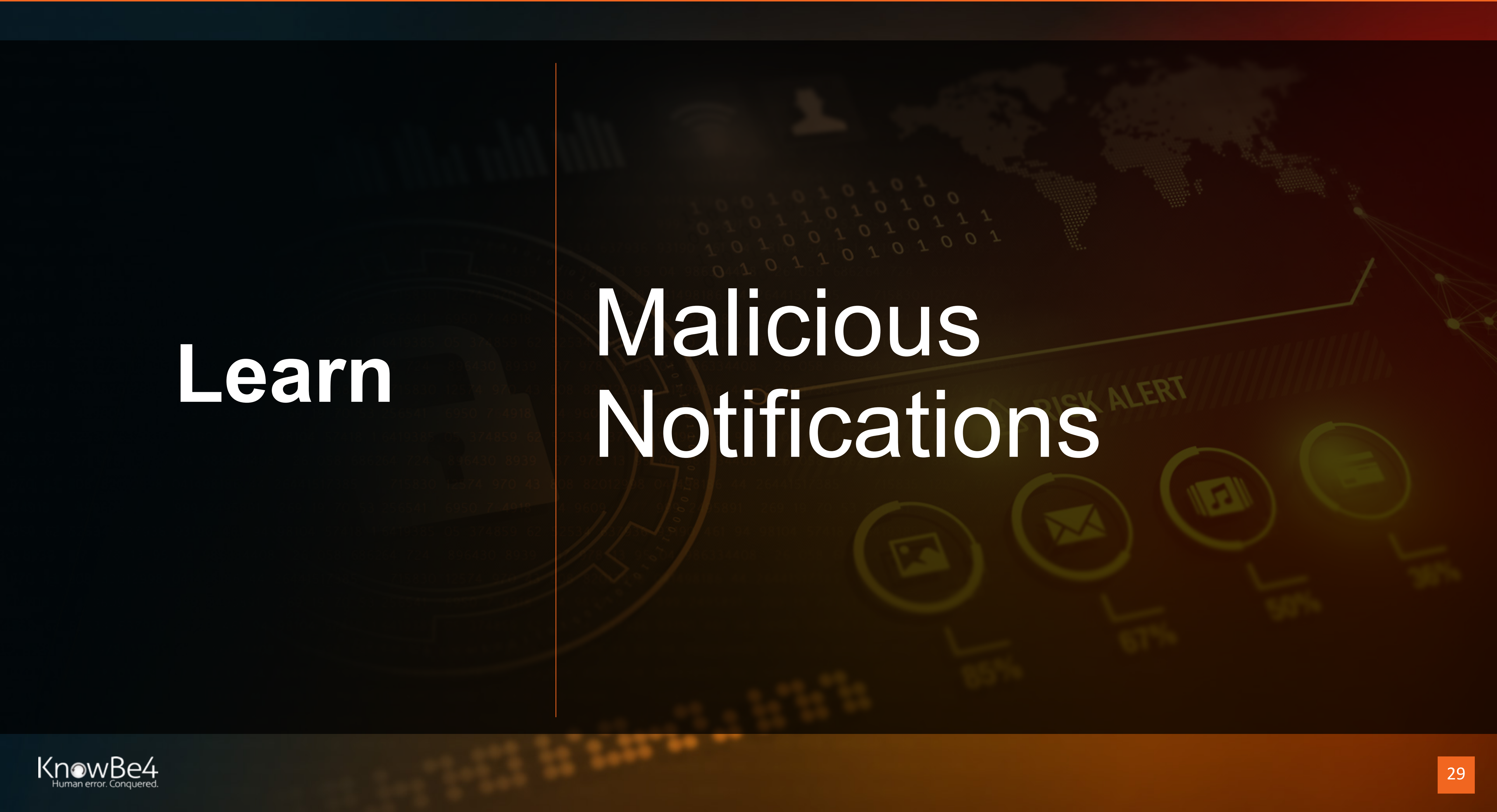
Push Notification Monetization Networks



Highest Push Notification payout rates for website owners, small publishers, high volume site owners.

Mone Let's Work Together criptions and Start Pushing That Revenue

nvert



Learn

Malicious Notifications

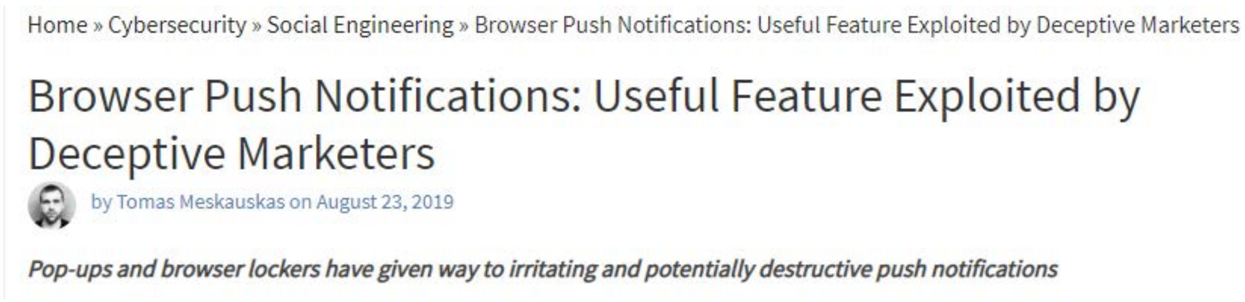
Malicious Notifications

Example

1. Malware group or push network will pose as 100% legitimate vendor asking web site to allow their “affiliate” code to be executed when a user allows notifications
2. At first, all seems legit
3. Later, network switches out harmless code for malicious code
   a) When vendor/victim complains, usually malicious network doesn’t respond, is slow to respond, or denies it’s happening
   b) When proven that it is happening, then they say something bad accidentally slipped through and/or blame it on some other “rogue” person or company who will be “punished”
   c) It always seems to take a long time for bad code to be removed
   d) Rinse and repeat

Malicious Notifications

Headlines

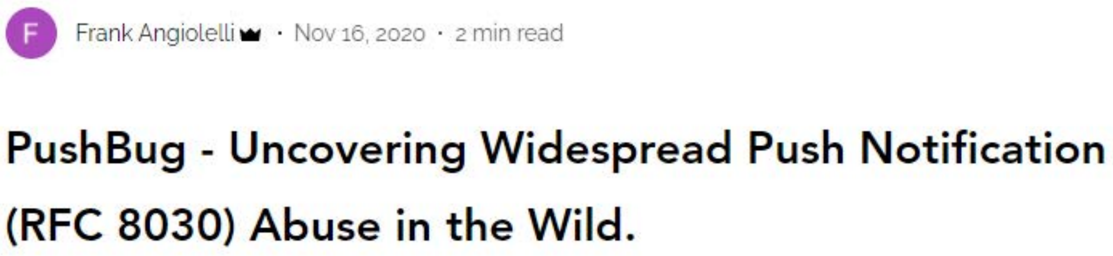


Home » Cybersecurity » Social Engineering » Browser Push Notifications: Useful Feature Exploited by Deceptive Marketers

Browser Push Notifications: Useful Feature Exploited by Deceptive Marketers

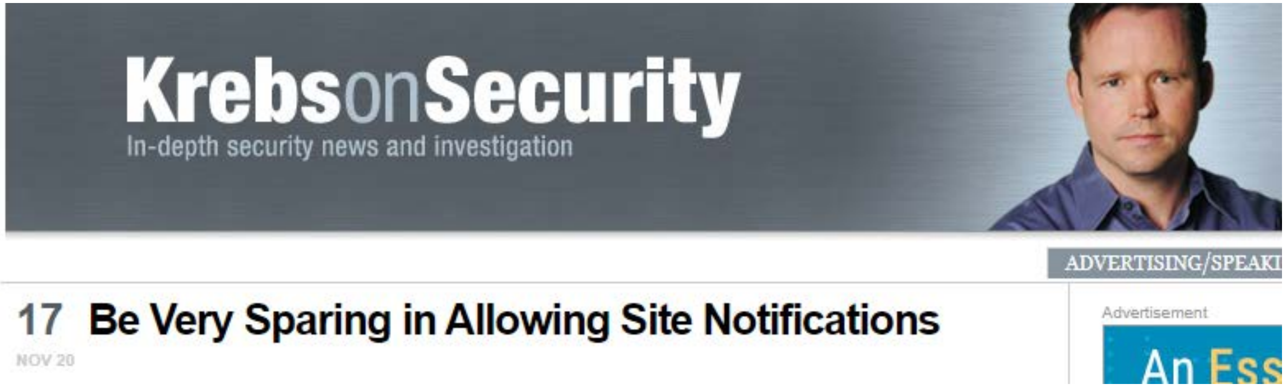
by Tomas Meskauskas on August 23, 2019

Pop-ups and browser lockers have given way to irritating and potentially destructive push notifications



F Frank Angiolelli · Nov 16, 2020 · 2 min read

PushBug - Uncovering Widespread Push Notification (RFC 8030) Abuse in the Wild.

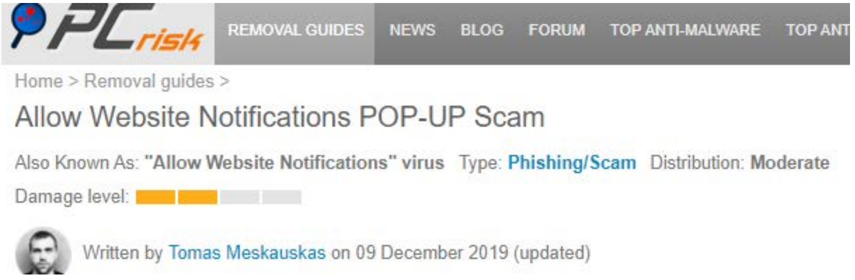


KrebsonSecurity

In-depth security news and investigation

17 Be Very Sparing in Allowing Site Notifications

NOV 20



Home > Removal guides >

Allow Website Notifications POP-UP Scam

Also Known As: **"Allow Website Notifications" virus** Type: **Phishing/Scam** Distribution: **Moderate**

Damage level: 🟧🟧⬜⬜

Written by Tomas Meskauskas on 09 December 2019 (updated)

Malicious Notifications

Example Maliciousness/Objectives

- Phishing
- Install malware
- Track user’s activities
- Advertisements
- Redirectors

- Maliciousness can be replaced on the fly as wanted
- Often do multiple bad things at once

Malicious Notifications

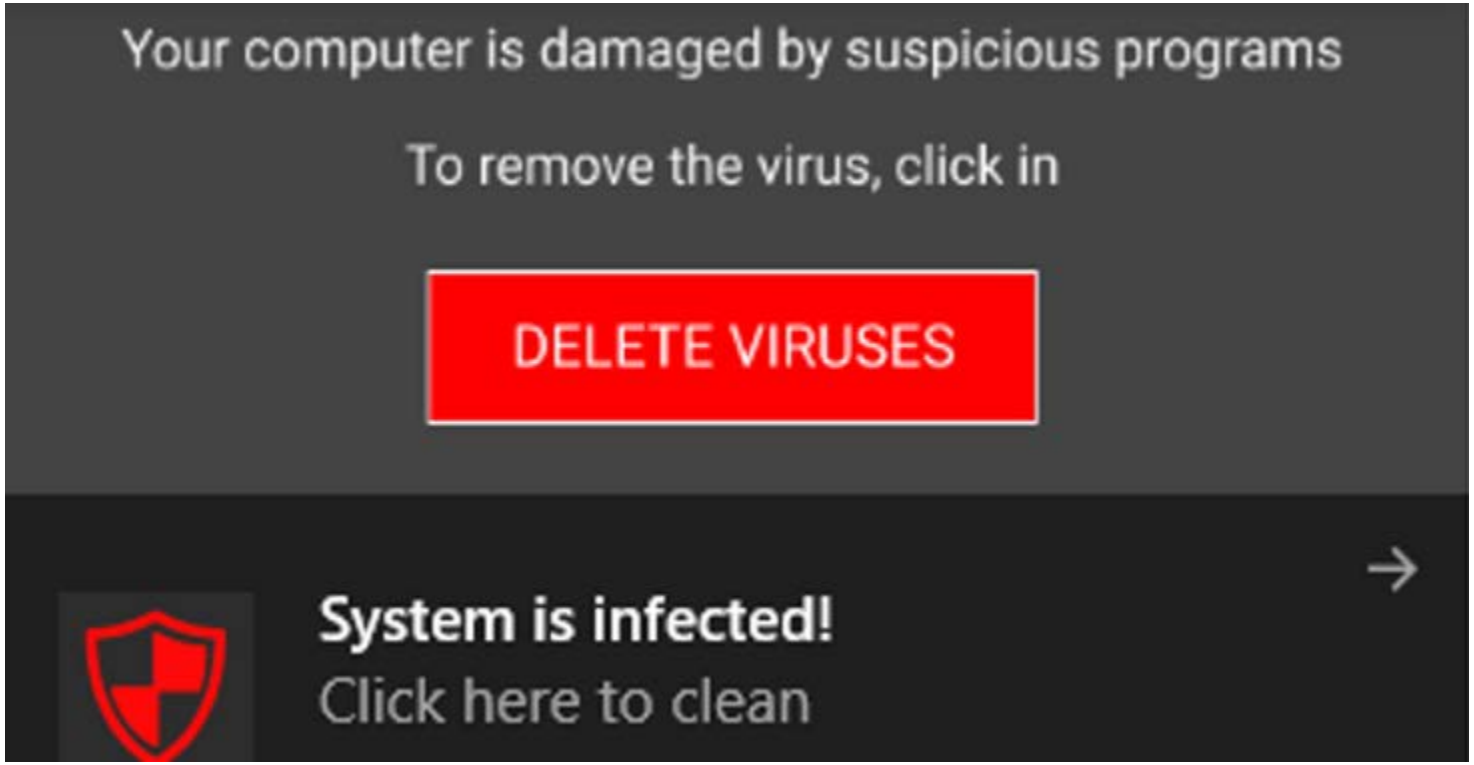
Example Maliciousness/Objectives

Why Notification Phishing Is Especially Dangerous

- Notifications happen outside the app or browser where it was approved
- Can even be displayed on "lock screen"
- Can be used to do credential phishing
- Once initial approval is allowed, the sky is the limit

Malicious Notifications

Fake AV Message Example



Your computer is damaged by suspicious programs

To remove the virus, click in

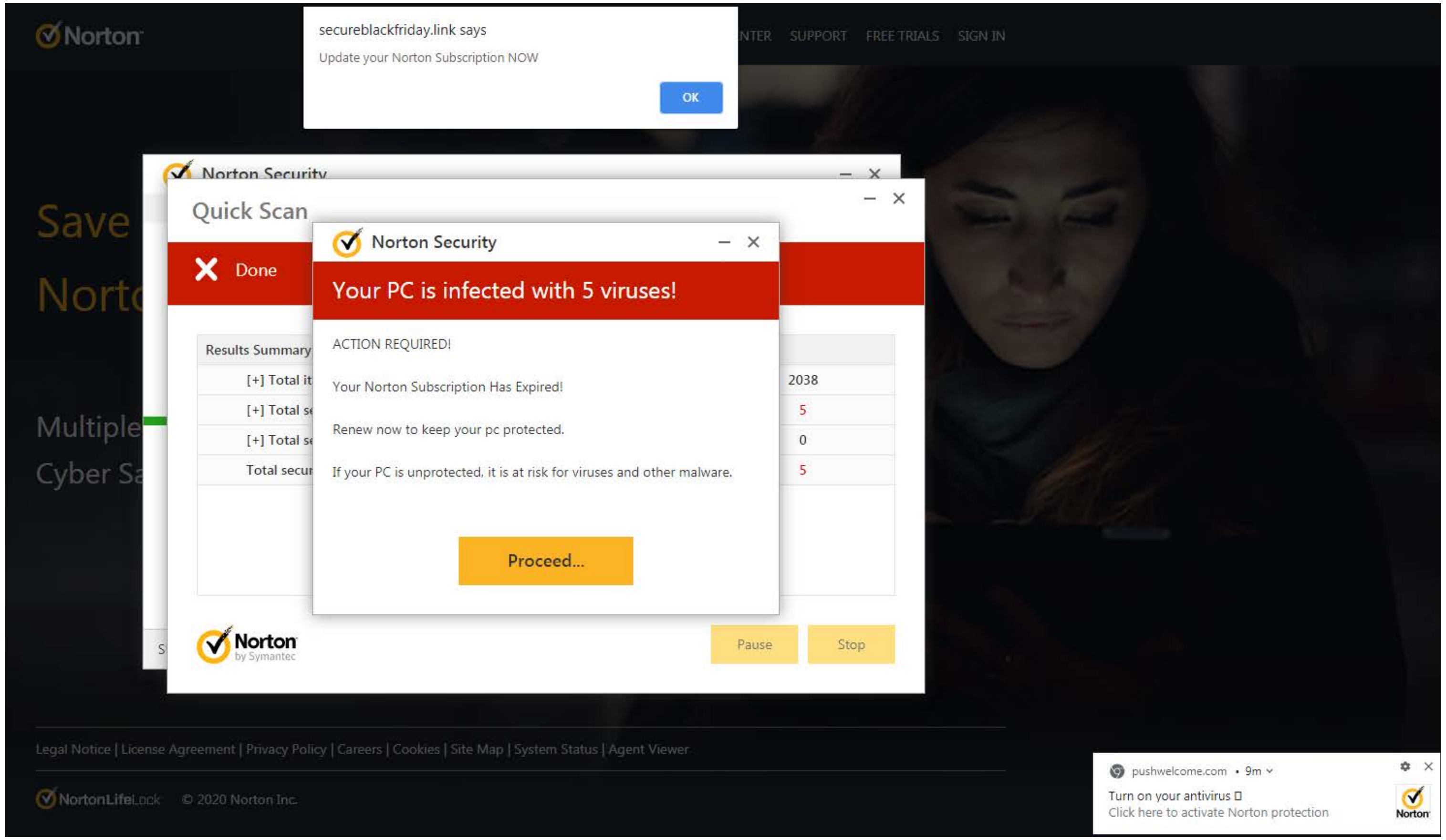
System is infected!

Click here to clean

Example from: https://www.indelible.global/post/pushbug-uncovering-widespread-push-notification-rfc-8030-abuse-in-the-wild

Malicious Notifications

Fake AV Message



secureblackfriday.link says

Update your Norton Subscription NOW

Norton Security

Quick Scan

Your PC is infected with 5 viruses!

ACTION REQUIRED!

Your Norton Subscription Has Expired!

Renew now to keep your pc protected.

If your PC is unprotected, it is at risk for viruses and other malware.

pushwelcome.com • 9m

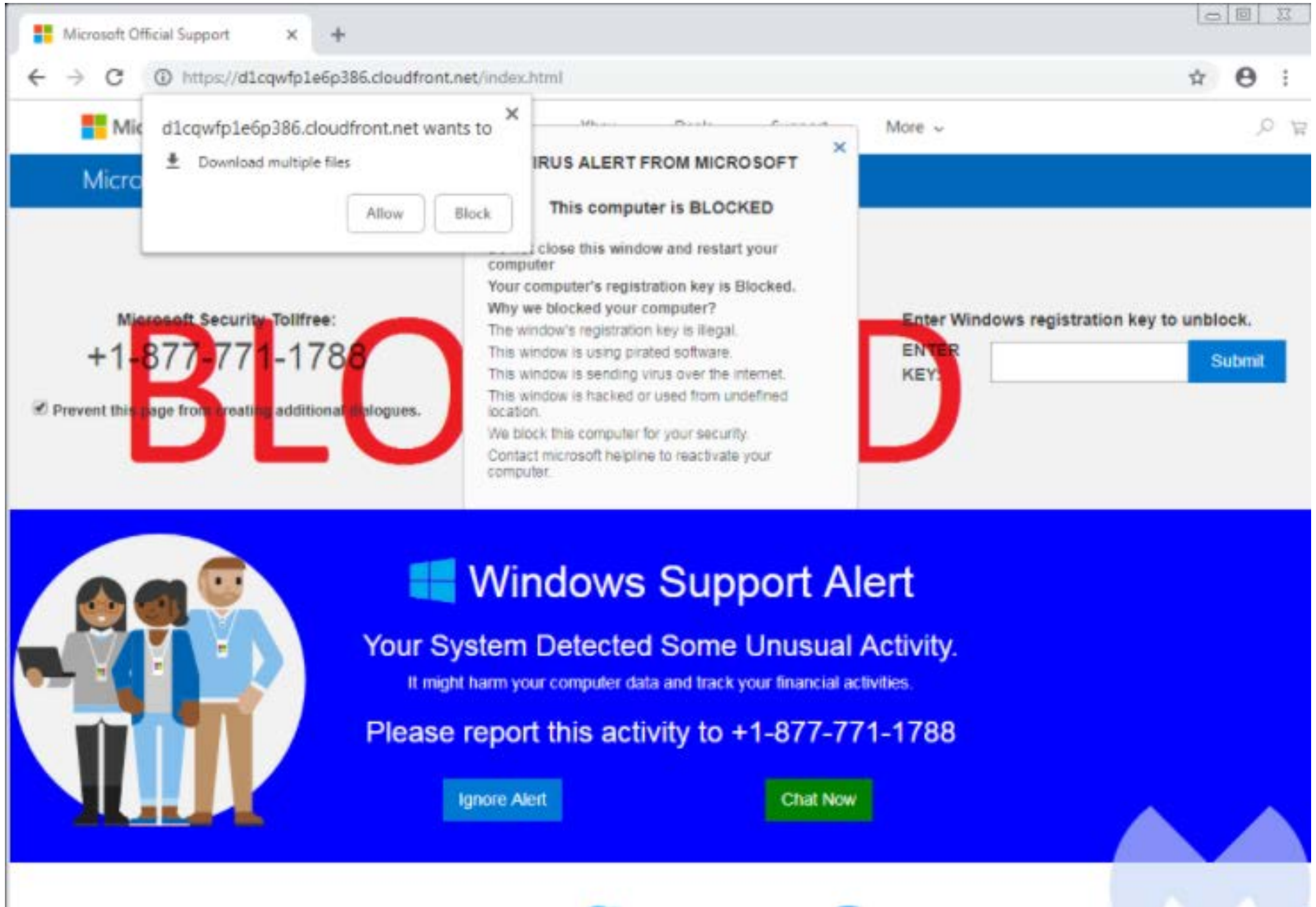
Turn on your antivirus

Click here to activate Norton protection

Example from: https://krebsonsecurity.com/2020/11/be-very-sparing-in-allowing-site-notifications/

Malicious Notifications

Fake AV Message


Microsoft Official Support
https://d1cqwfp1e6p386.cloudfront.net/index.html
Mic
Micro
More
BLO
D

d1cqwfp1e6p386.cloudfront.net wants to

Download multiple files

IRUS ALERT FROM MICROSOFT

This computer is BLOCKED

close this window and restart your computer

Your computer's registration key is Blocked.

Why we blocked your computer?

The window's registration key is illegal.

This window is using pirated software.

This window is sending virus over the internet.

This window is hacked or used from undefined location.

We block this computer for your security.

Contact microsoft helpline to reactivate your computer.

Microsoft Security Tollfree:

+1-877-771-1788

☑ Prevent this page from creating additional dialogues.

Enter Windows registration key to unblock.

ENTER KEY:

Windows Support Alert

Your System Detected Some Unusual Activity.

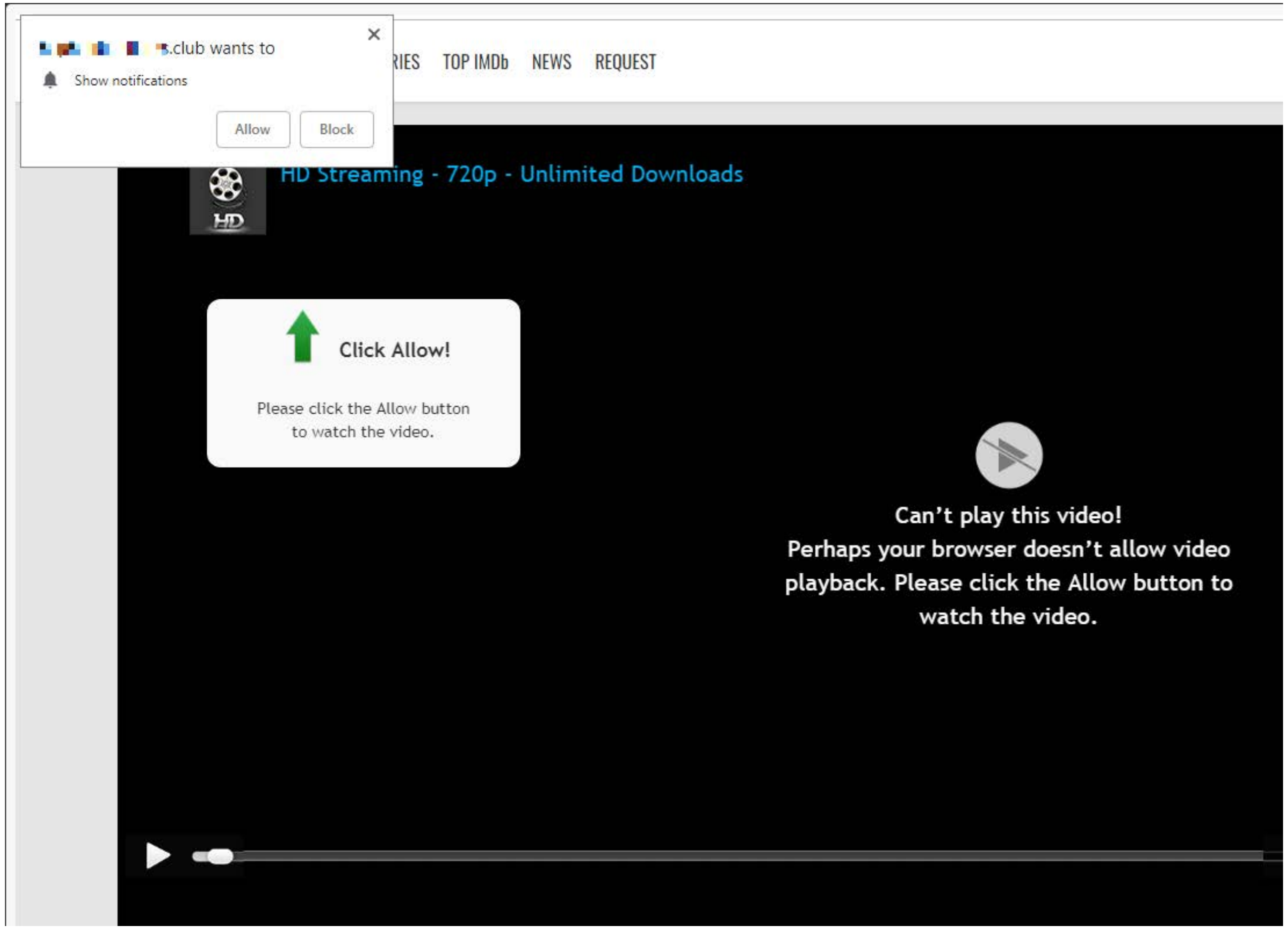
It might harm your computer data and track your financial activities.

Please report this activity to +1-877-771-1788

Example from: https://blog.malwarebytes.com/threat-analysis/2018/10/scammers-use-old-browser-trick-to-create-fake-virus-download//

Malicious Notifications

Fake Video Error



.club wants to

Show notifications

Allow Block

HD Streaming - 720p - Unlimited Downloads

Click Allow!

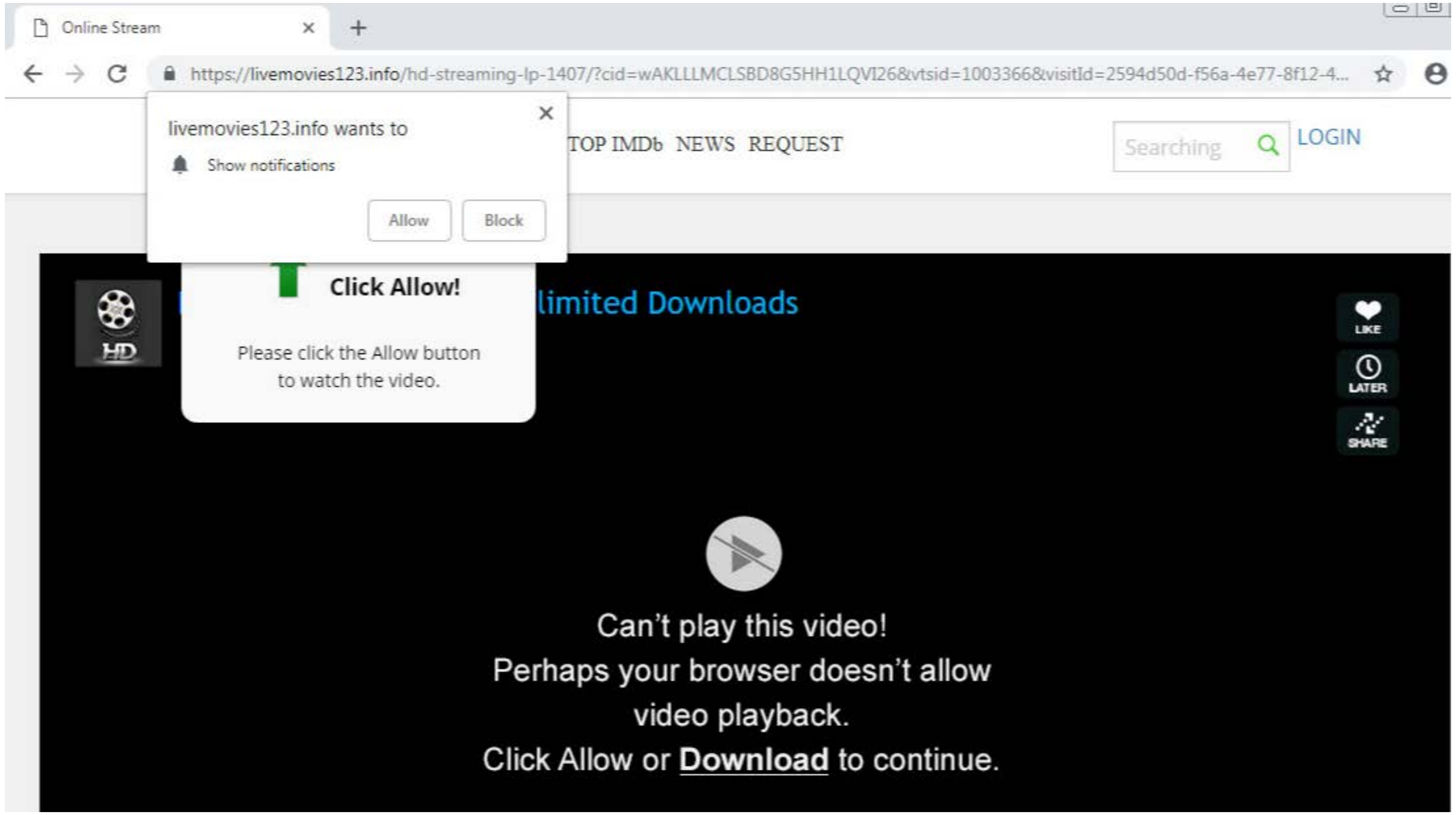
Please click the Allow button to watch the video.

Can't play this video!
Perhaps your browser doesn't allow video playback. Please click the Allow button to watch the video.

Example from: https://blog.malwarebytes.com/security-world/technology/2019/01/browser-push-notifications-feature-asking-abused/

Malicious Notifications

Fake Video Error Message



https://livemovies123.info/hd-streaming-lp-1407/?cid=wAKLLLMCLSBD8G5HH1LQVI26&vtsid=1003366&visitId=2594d50d-f56a-4e77-8f12-4...

livemovies123.info wants to

Show notifications

Click Allow!

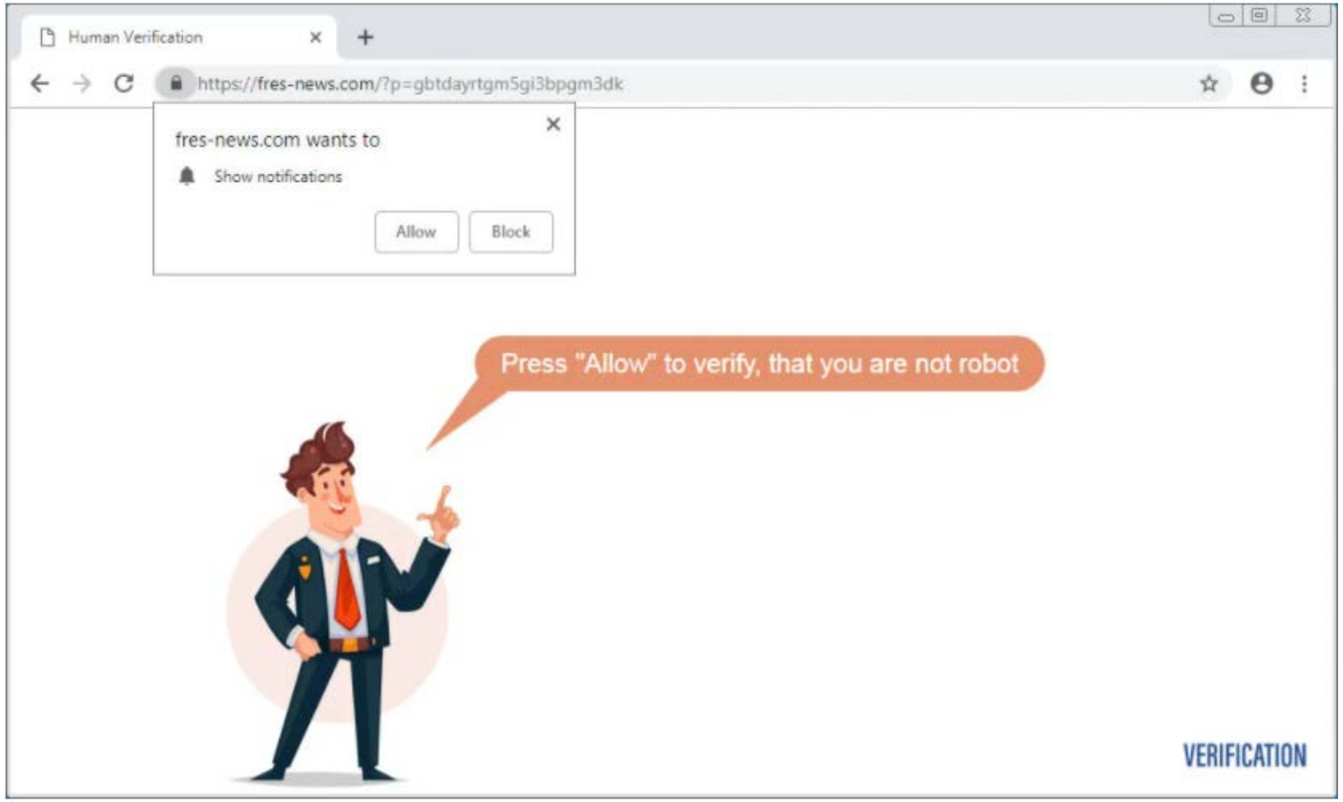
Please click the Allow button to watch the video.

Can't play this video!
Perhaps your browser doesn't allow video playback.
Click Allow or **Download** to continue.

Example from: https://statics.esputnik.com/photos/shares/Blog/images/abusive/image5.png/

Malicious Notifications

Verify You’re Not a Robot Scam



Human Verification

https://fres-news.com/?p=gbtdayrtgm5gi3bpgm3dk

fres-news.com wants to

Show notifications

Allow Block

Press "Allow" to verify, that you are not robot

VERIFICATION

Example from: https://www.bleepingcomputer.com/news/security/scam-browser-notification-prompts-increased-by-69-percent-in-2019/

Learn

Defending Against Malicious Notifications

Why Malicious Notifications Evade AV

General

- Relatively new abuse method
- Often coming from legitimately, trusted sites and apps
- Dynamic domain use
- No easy way to review/fix configuration issues

- Victims intentionally “allowed it”!

Note: Some AV vendors are becoming better at recognizing it.

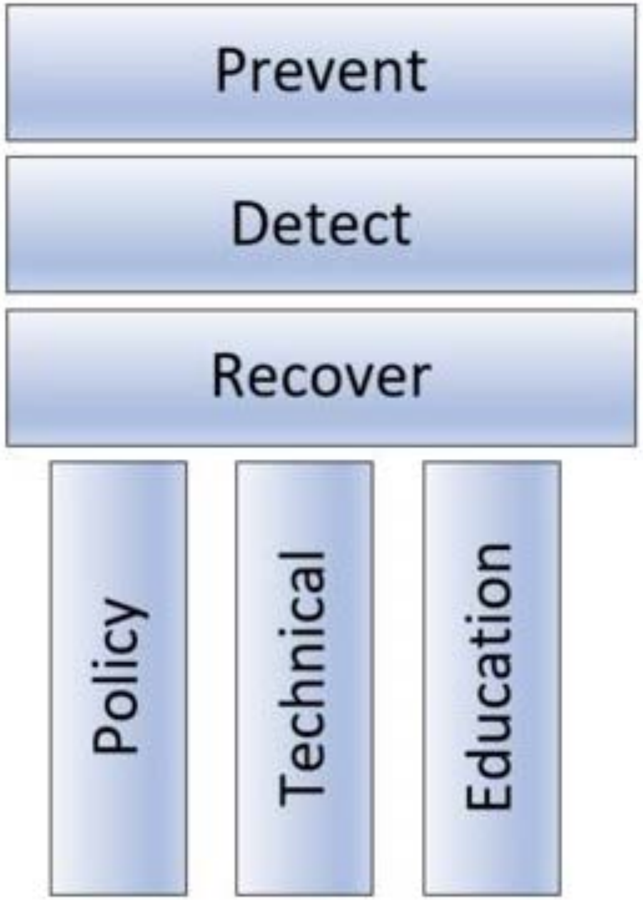
Phishing Cannot Be Beat by Intelligence

- Anyone can fall victim to social engineering
- “Smart people” are just as likely to fall victim to phishing as anyone else
- Scammers use “stressors” to make people bypass their normal skepticism survival skills
- Whether or not someone clicks on a “phish” or falls victim to a fake notification, has more to due with awareness of digital crime than anything else
- Once people are aware of social engineering, phishing, and all it’s forms, the less likely they are to fall victim to it

Defending Against Phishing

General Defense Methods

- Policies
- Technical Controls
  - Anti-Malware Software
  - Anti-Spam/Phishing
  - Content Filtering
- Security Awareness Training



https://blog.knowbe4.com/the-three-pillars-of-the-three-computer-security-pillars

Defending Against Notifications

Overview

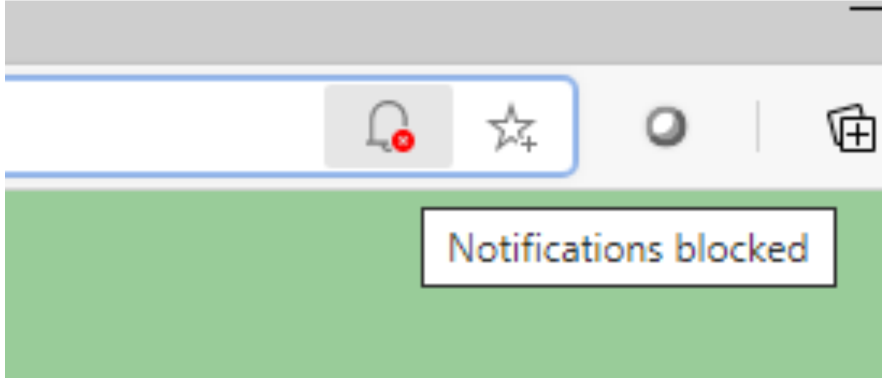
- Education
- Review and remove unneeded existing notifications on desktop and browser(s)
- Configure desktop and browsers to reject notifications by default
- Find out if your AV/EDR solution is aware of malicious notification scams
- Run latest browser versions
- Report notification scam domains to Google and Microsoft

Defending Against Notifications

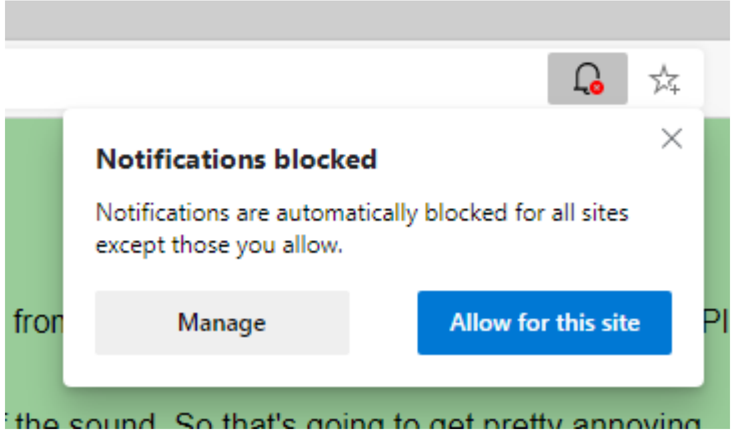
<u>You Can Disable Them In the Browser</u>

- You can enable or disable them globally in the browser or OS
- How you do that varies per browser and OS

Example: Microsoft Edge



Notifications blocked



Notifications blocked

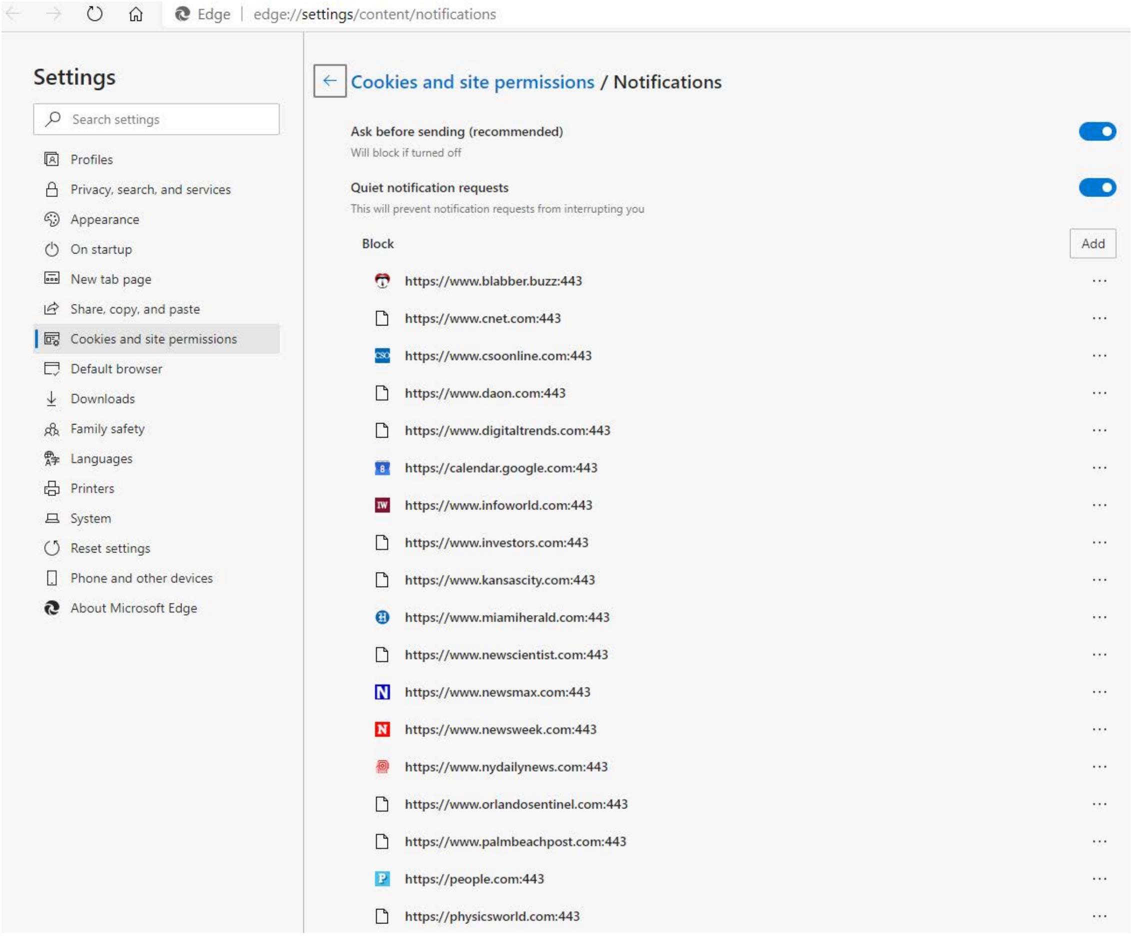
Notifications are automatically blocked for all sites except those you allow.

Defending Against Notifications

You Can Disable Them In the Browser

- You can enable or disable them globally in the browser or OS
- How you do that varies per browser and OS

Example: Microsoft Edge



Cookies and site permissions / Notifications

Ask before sending (recommended) — On
Will block if turned off

Quiet notification requests — On
This will prevent notification requests from interrupting you

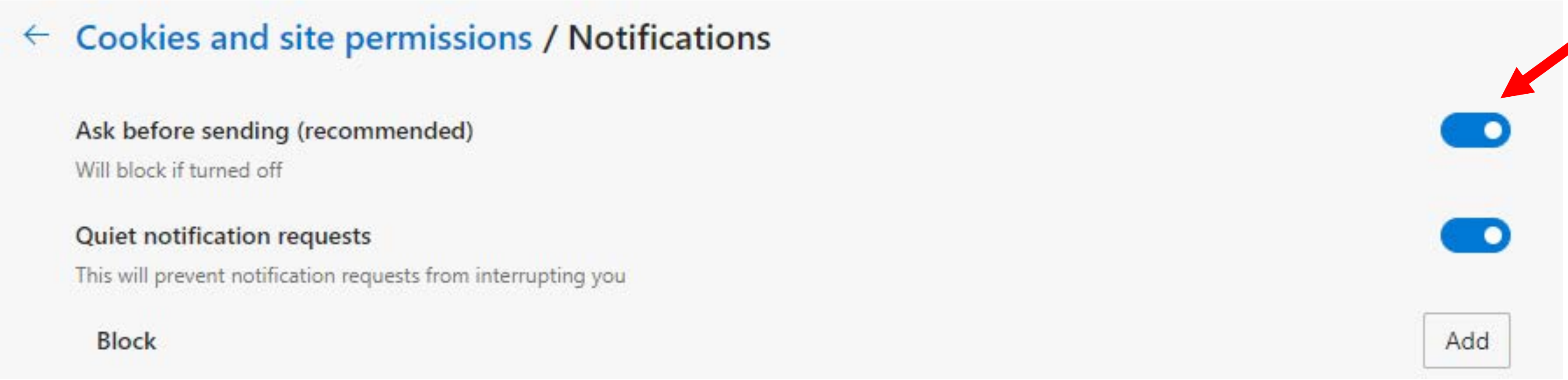
Block

https://www.blabber.buzz:443
https://www.cnet.com:443
https://www.csoonline.com:443
https://www.daon.com:443
https://www.digitaltrends.com:443
https://calendar.google.com:443
https://www.infoworld.com:443
https://www.investors.com:443
https://www.kansascity.com:443
https://www.miamiherald.com:443
https://www.newscientist.com:443
https://www.newsmax.com:443
https://www.newsweek.com:443
https://www.nydailynews.com:443
https://www.orlandosentinel.com:443
https://www.palmbeachpost.com:443
https://people.com:443
https://physicsworld.com:443

Defending Against Notifications

You Can Disable Them In the Browser

Example: Microsoft Edge



← Cookies and site permissions / Notifications

Ask before sending (recommended) — on

Will block if turned off

Quiet notification requests — on

This will prevent notification requests from interrupting you

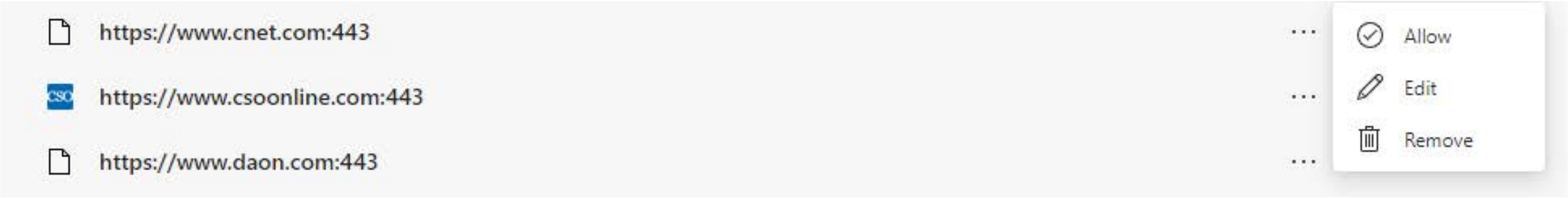
Will globally block if disabled

Defending Against Notifications

You Can Disable Them In the Browser

Example: Microsoft Edge

Can individually block or allow per site, or if you remove it will allow the site to ask permission again



https://www.cnet.com:443

https://www.csoonline.com:443

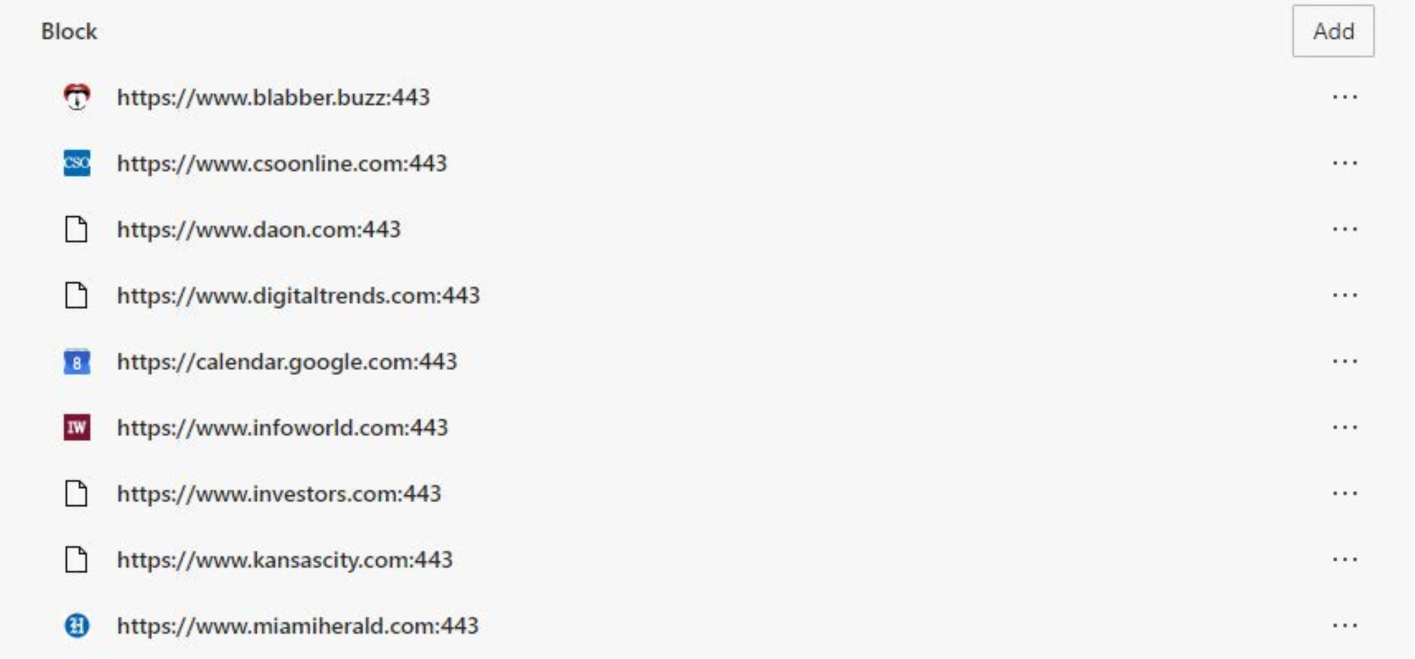
https://www.daon.com:443

Defending Against Notifications

You Can Disable Them In the Browser

Example: Microsoft Edge

These sites have already been denied permission (blocked) and can’t ask again



https://www.blabber.buzz:443 ···

https://www.csoonline.com:443 ···

https://www.daon.com:443 ···

https://www.digitaltrends.com:443 ···

https://calendar.google.com:443 ···

https://www.infoworld.com:443 ···

https://www.investors.com:443 ···

https://www.kansascity.com:443 ···

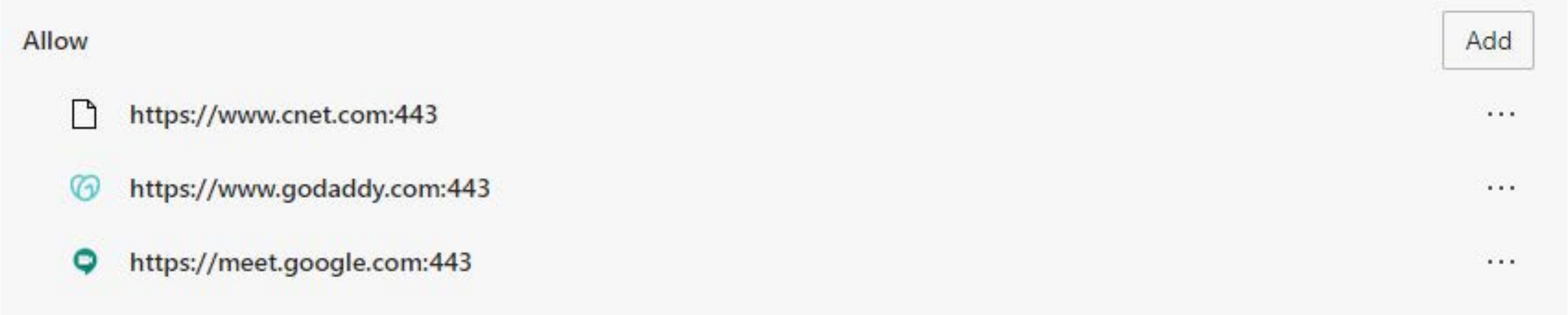
https://www.miamiherald.com:443 ···

Defending Against Notifications

You Can Disable Them In the Browser

Example: Microsoft Edge

These sites have already been allowed permission (allow)



https://www.cnet.com:443

https://www.godaddy.com:443

https://meet.google.com:443

Changes often require a tab or browser restart

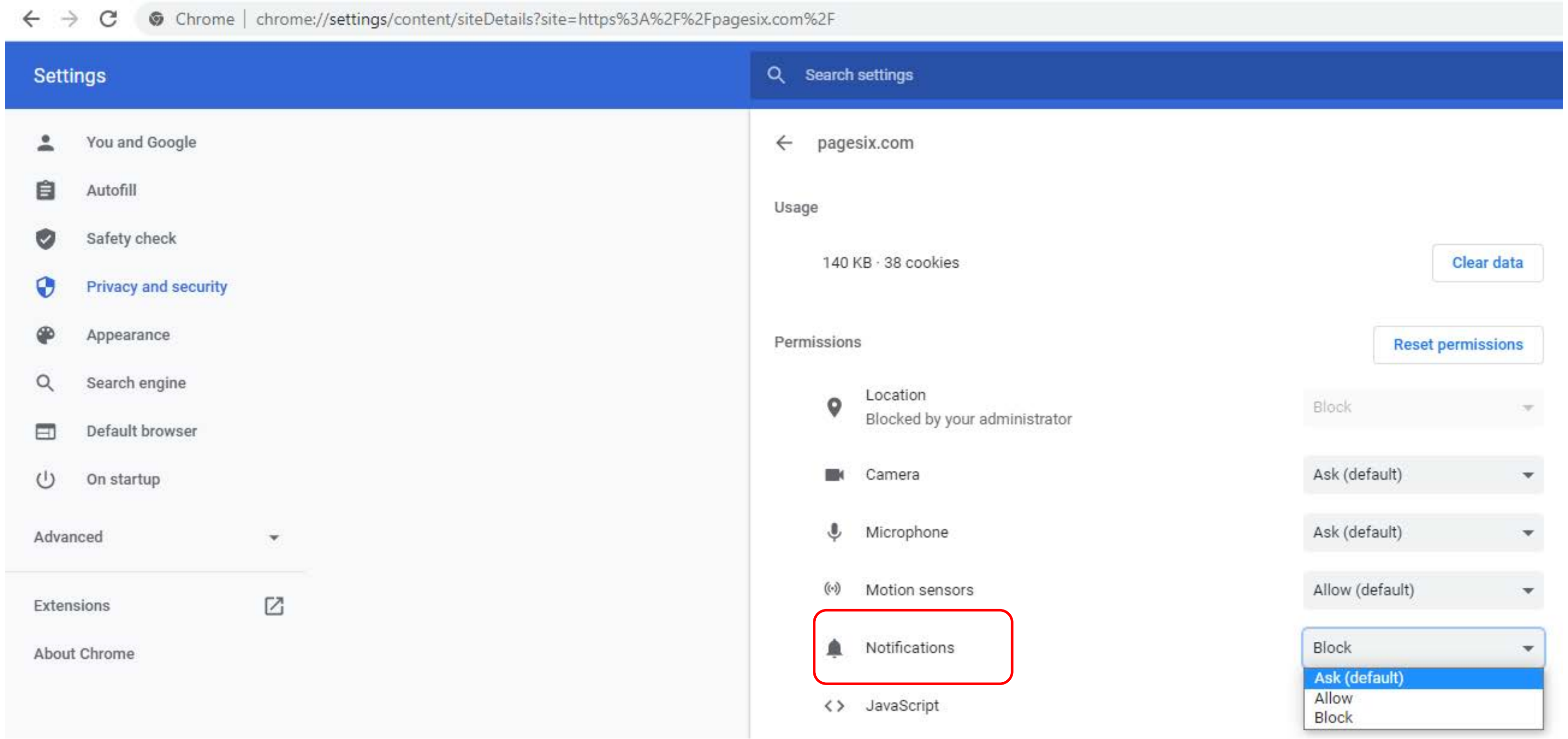
Defending Against Notifications

<u>You Can Disable Them In the Browser</u>

Example: Google Chrome

You can configure per site

chrome://settings/content/



Chrome | chrome://settings/content/siteDetails?site=https%3A%2F%2Fpagesix.com%2F

pagesix.com

Usage

140 KB · 38 cookies

Permissions

Location — Blocked by your administrator — Block

Camera — Ask (default)

Microphone — Ask (default)

Motion sensors — Allow (default)

Notifications — Block

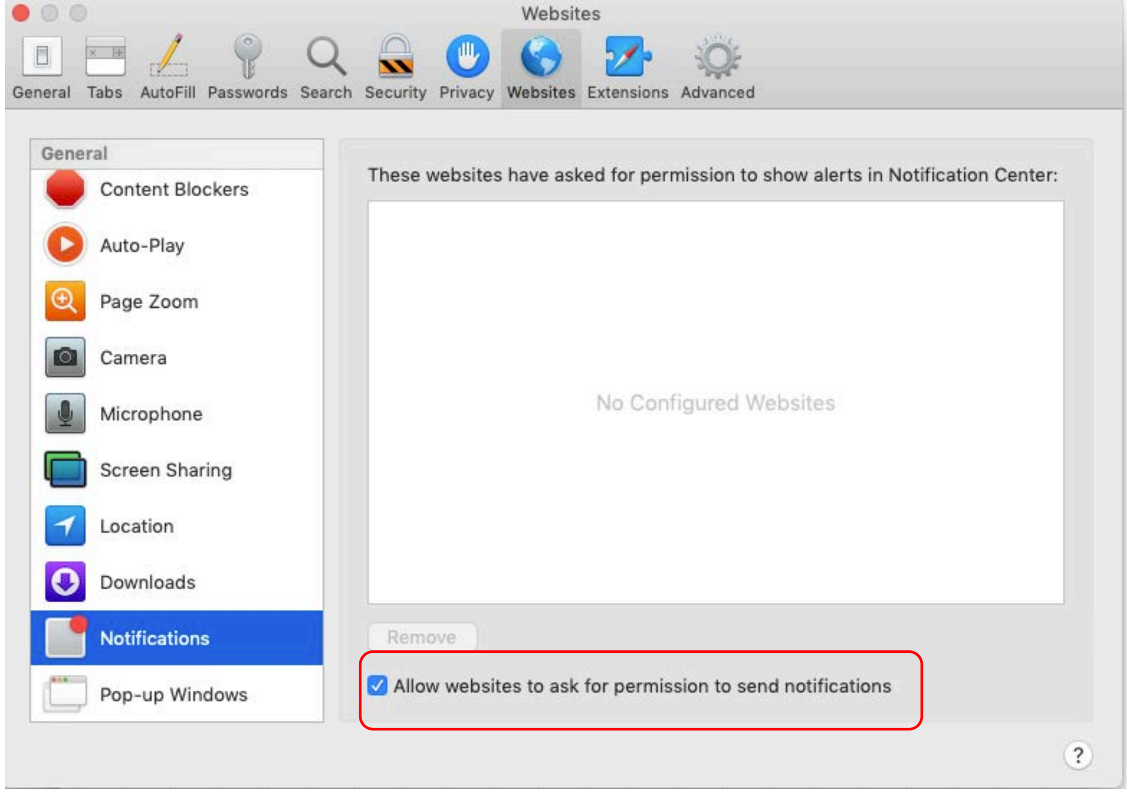
JavaScript

Defending Against Notifications

You Can Disable Them In the Browser

Example: Apple Safari

- You can configure per site
- Safari > Preferences > Websites > Notifications



These websites have asked for permission to show alerts in Notification Center:

No Configured Websites

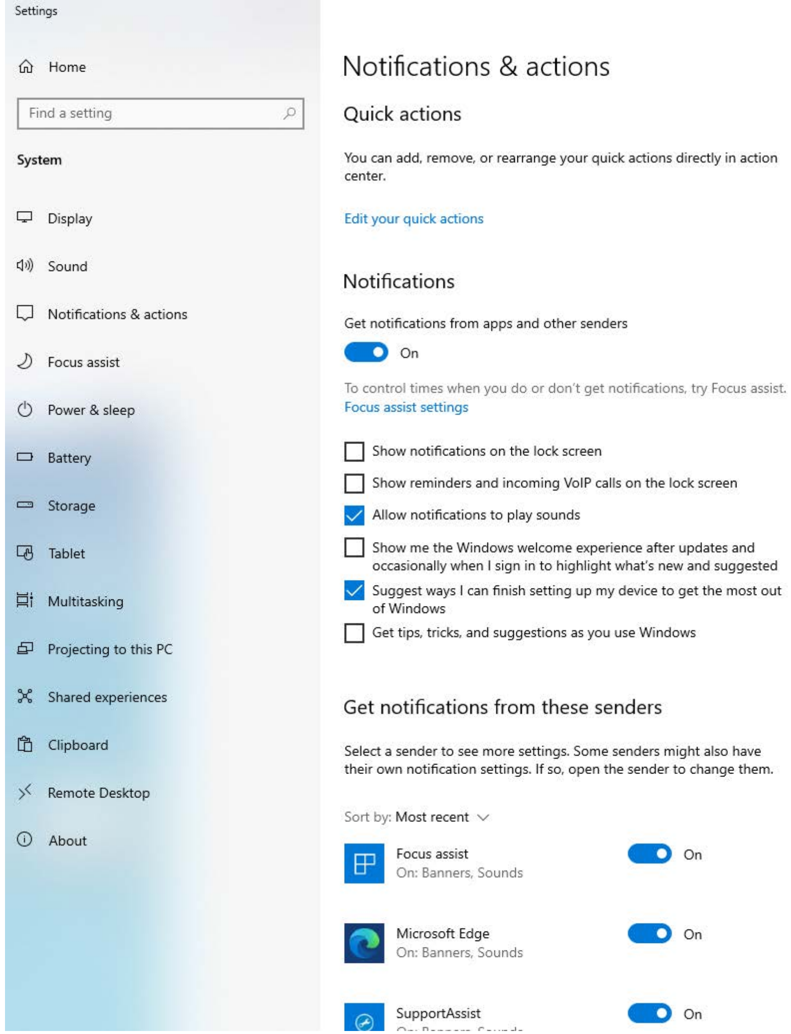
☑ Allow websites to ask for permission to send notifications

Defending Against Notifications

You Can Configure Them In OS

Example: Microsoft Windows

Settings/Notification & actions



Notifications & actions

Quick actions

You can add, remove, or rearrange your quick actions directly in action center.

Edit your quick actions

Notifications

Get notifications from apps and other senders

On

To control times when you do or don't get notifications, try Focus assist.
Focus assist settings

□ Show notifications on the lock screen

□ Show reminders and incoming VoIP calls on the lock screen

☑ Allow notifications to play sounds

□ Show me the Windows welcome experience after updates and occasionally when I sign in to highlight what's new and suggested

☑ Suggest ways I can finish setting up my device to get the most out of Windows

□ Get tips, tricks, and suggestions as you use Windows

Get notifications from these senders

Select a sender to see more settings. Some senders might also have their own notification settings. If so, open the sender to change them.

Sort by: Most recent

Focus assist — On: Banners, Sounds — On

Microsoft Edge — On: Banners, Sounds — On

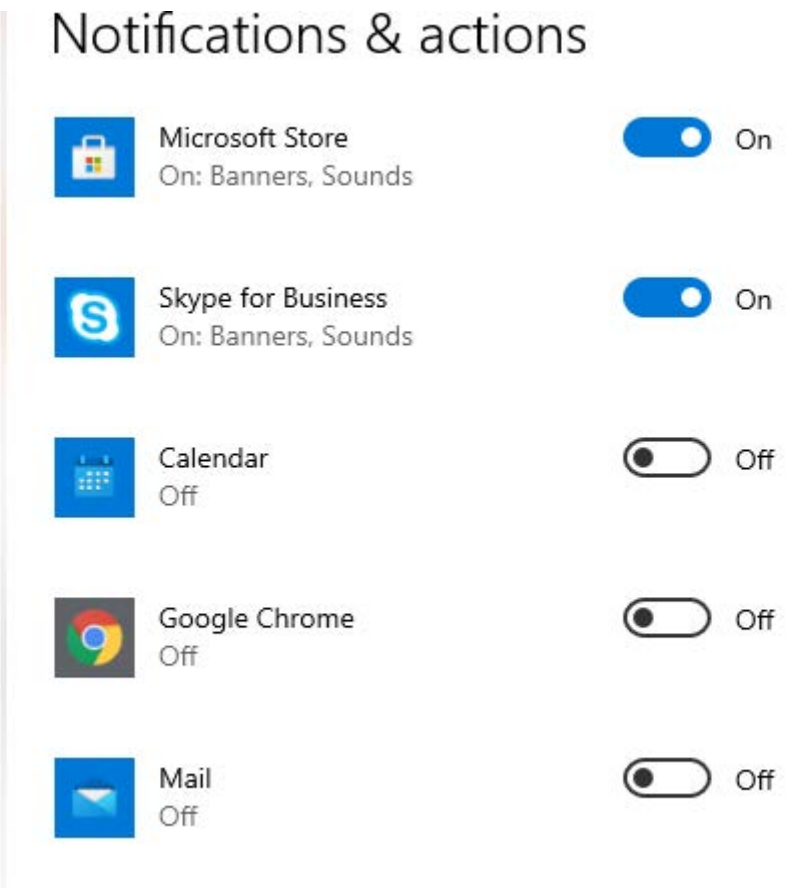
SupportAssist — On

Defending Against Notifications

<u>You Can Configure Them In OS</u>

Example: Microsoft Windows

Settings/Notification & actions



Notifications & actions

Microsoft Store
On: Banners, Sounds
On

Skype for Business
On: Banners, Sounds
On

Calendar
Off
Off

Google Chrome
Off
Off

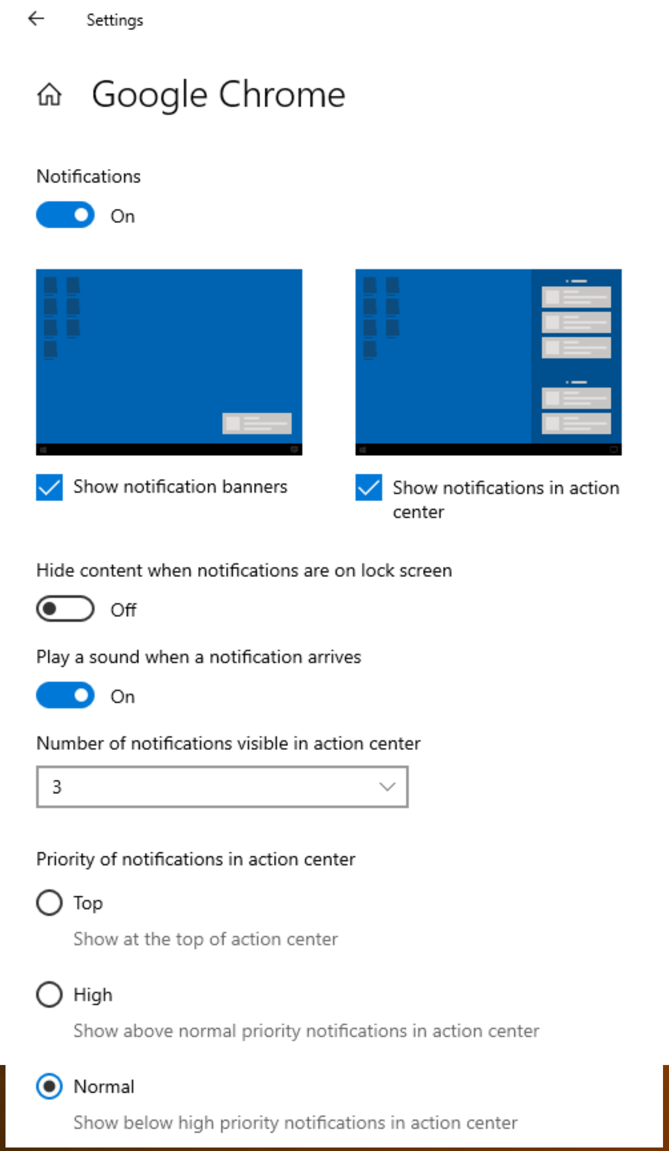
Mail
Off
Off

Defending Against Notifications

You Can Configure Them In OS

Example: Microsoft Windows

Settings/Notification & actions



← Settings

Google Chrome

Notifications

On

☑ Show notification banners

☑ Show notifications in action center

Hide content when notifications are on lock screen

Off

Play a sound when a notification arrives

On

Number of notifications visible in action center

3

Priority of notifications in action center

○ Top
Show at the top of action center

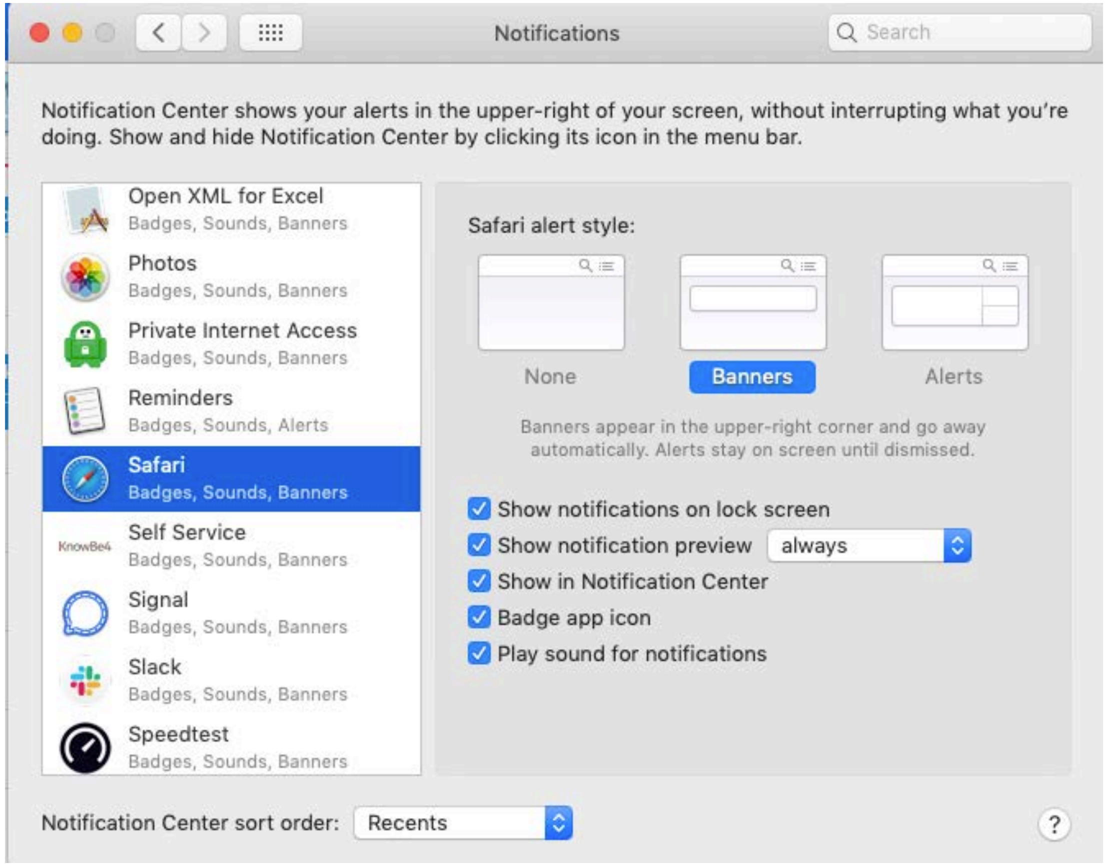
○ High
Show above normal priority notifications in action center

● Normal
Show below high priority notifications in action center

Defending Against Notifications

You Can Configure Them In OS

- Example: Apple MacOS
- Apple > System Preferences > Notifications



Notification Center shows your alerts in the upper-right of your screen, without interrupting what you're doing. Show and hide Notification Center by clicking its icon in the menu bar.

Open XML for Excel	Badges, Sounds, Banners
Photos	Badges, Sounds, Banners
Private Internet Access	Badges, Sounds, Banners
Reminders	Badges, Sounds, Alerts
Safari	Badges, Sounds, Banners
Self Service	Badges, Sounds, Banners
Signal	Badges, Sounds, Banners
Slack	Badges, Sounds, Banners
Speedtest	Badges, Sounds, Banners

Safari alert style:

Banners appear in the upper-right corner and go away automatically. Alerts stay on screen until dismissed.

- ☑ Show notifications on lock screen
- ☑ Show notification preview: always
- ☑ Show in Notification Center
- ☑ Badge app icon
- ☑ Play sound for notifications

Notification Center sort order: Recents

Source: https://support.apple.com/guide/safari/customize-website-notifications-sfri40734/mac

Defending Against Notifications

Example Step by Step Browser Instructions

- https://blog.malwarebytes.com/security-world/technology/2019/01/browser-push-notifications-feature-asking-abused/
- https://www.theverge.com/2019/7/18/18716041/website-notification-prompts-pop-ups-how-to-stop
- https://hackingvision.com/2019/09/25/malicious-browser-push-notifications/
- https://www.androidpolice.com/2020/06/18/track-block-rogue-ads-android/

Remember to disable in OS **and** browsers

Defending Against Notifications

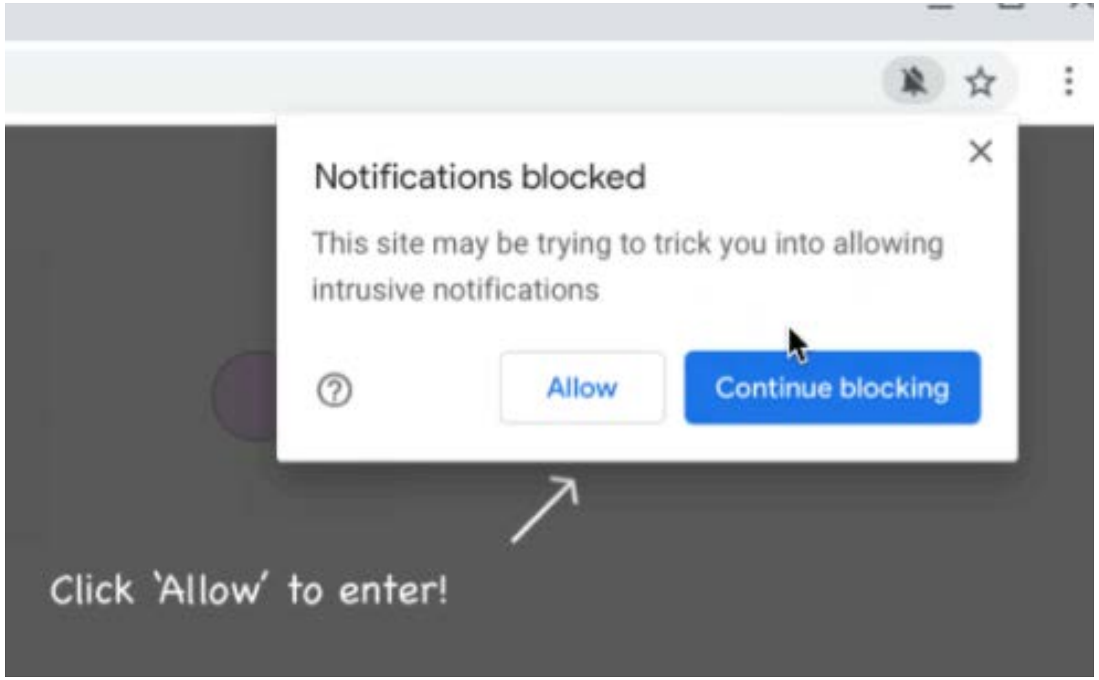
Some Browsers Will Warn You If They Recognize Potentially Malicious Notifications

- https://blog.chromium.org/2020/10/reducing-abusive-notification-content.html
- Google proactively subscribes to notification pushes and monitors behavior
- They will warn users if notification request comes from a known rogue domain
- Chrome browser v. 80 (released Feb. 4, 2020) and above have this feature

Defending Against Notifications

Some Browsers Will Warn You If They Recognize It

- https://blog.chromium.org/2020/10/reducing-abusive-notification-content.html
- Google proactively subscribes to notification pushes and monitors behavior
- They will warn users if notification request comes from a known rogue domain
- Chrome browser v. 80 (released Feb. 4, 2020) and above have this feature



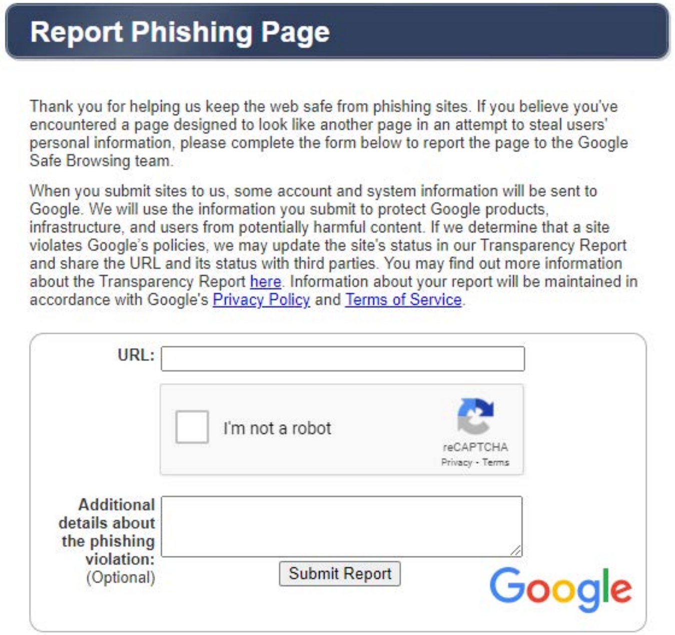
Notifications blocked

This site may be trying to trick you into allowing intrusive notifications

Defending Against Notifications

Report Sites With Malicious Notifications

- https://safebrowsing.google.com/safebrowsing/report_phish/
- https://www.microsoft.com/en-us/wdsi/support/report-unsafe-site-guest



Report Phishing Page

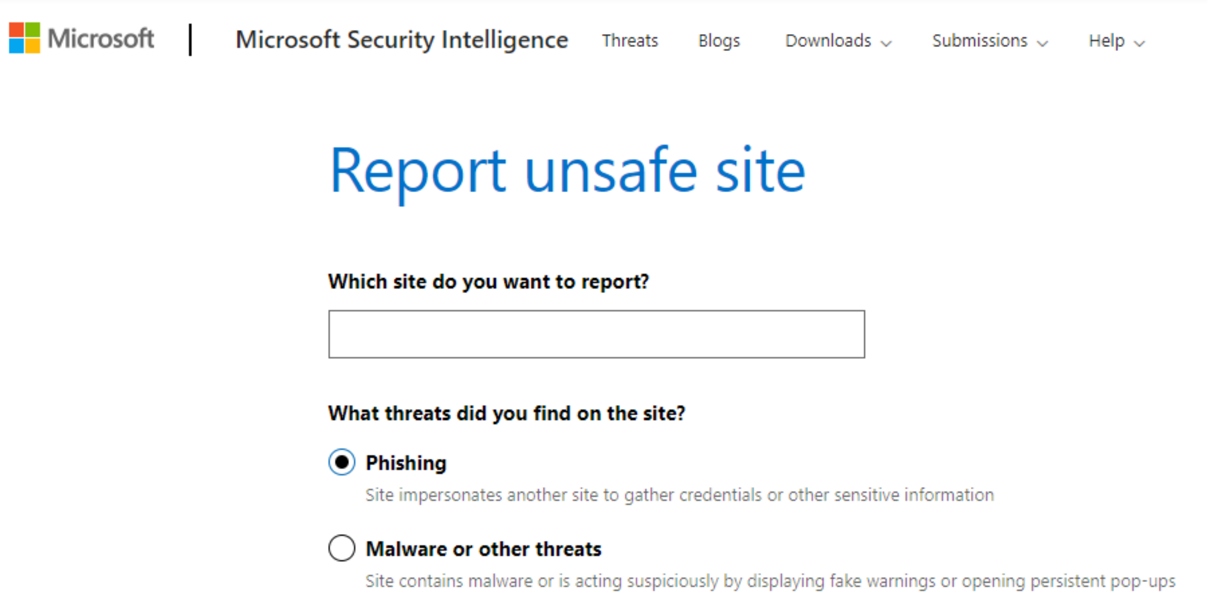
Thank you for helping us keep the web safe from phishing sites. If you believe you've encountered a page designed to look like another page in an attempt to steal users' personal information, please complete the form below to report the page to the Google Safe Browsing team.

When you submit sites to us, some account and system information will be sent to Google. We will use the information you submit to protect Google products, infrastructure, and users from potentially harmful content. If we determine that a site violates Google's policies, we may update the site's status in our Transparency Report and share the URL and its status with third parties. You may find out more information about the Transparency Report here. Information about your report will be maintained in accordance with Google's Privacy Policy and Terms of Service.

URL:

□ I'm not a robot

Additional details about the phishing violation: (Optional)



Report unsafe site

Which site do you want to report?

What threats did you find on the site?

● Phishing
Site impersonates another site to gather credentials or other sensitive information

○ Malware or other threats
Site contains malware or is acting suspiciously by displaying fake warnings or opening persistent pop-ups

Defending Against Notifications

Resetting Browser Settings Automation

- 3rd party device management programs which allow application/registry setting editing
- Microsoft Edge
  - Requires custom Administrative Template and Group Policy or Microsoft Intunes
  - https://www.techrepublic.com/article/how-to-manage-the-new-microsoft-edge-through-group-policy/
- Google Chrome
  - https://support.google.com/chrome/a/answer/188446?hl=en

Defending Against Notifications

Education

- Share this presentation
- General security awareness training, including specific training on notification phishing

Good links to review and share:

- https://www.indelible.global/post/pushbug-uncovering-widespread-push-notification-rfc-8030-abuse-in-the-wild
- https://krebsonsecurity.com/2020/11/be-very-sparing-in-allowing-site-notifications/

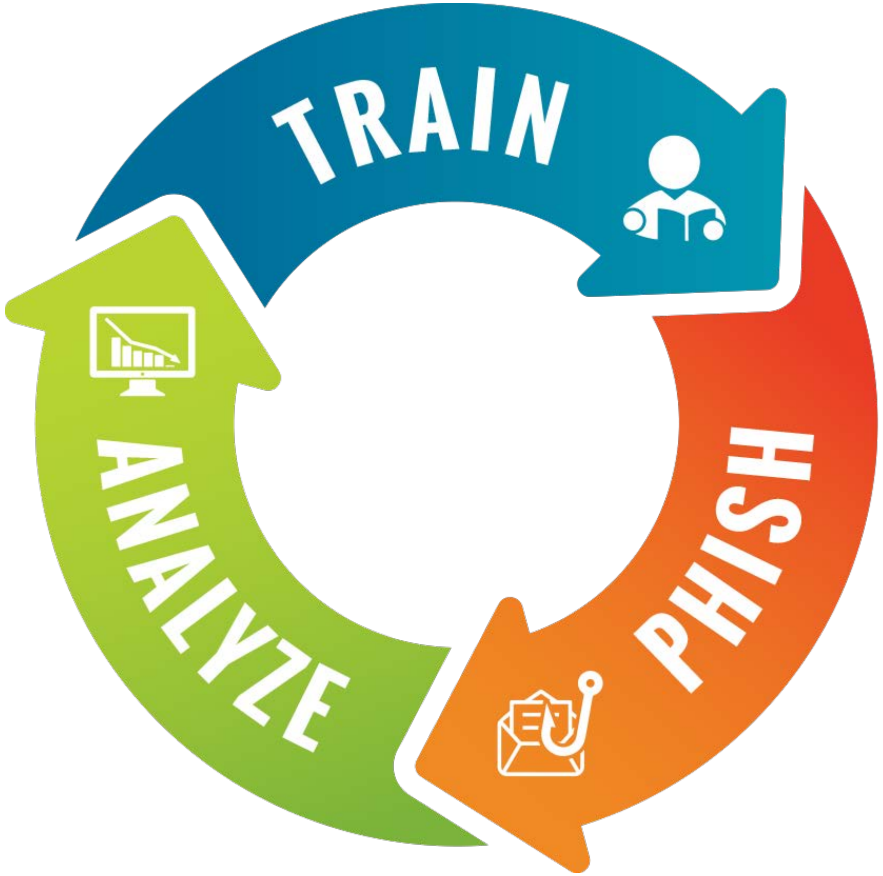
KnowBe4 Security Awareness Training

Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

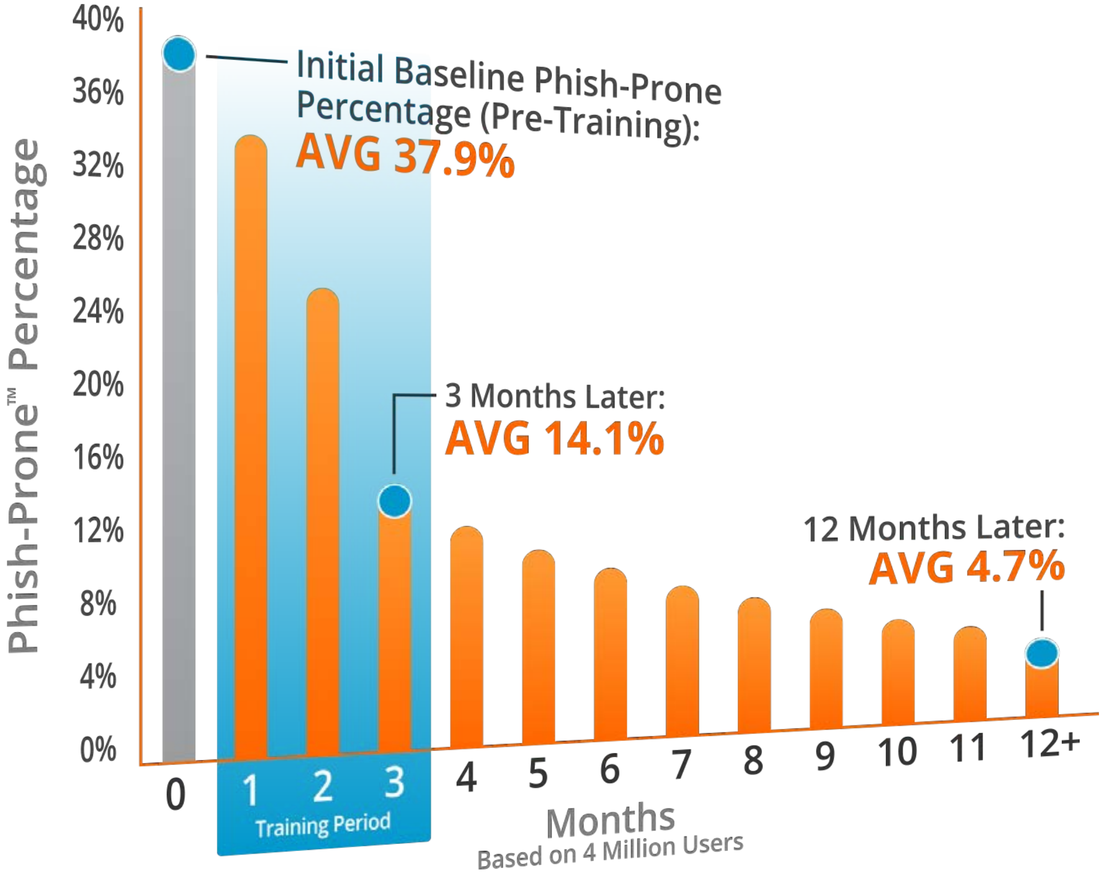


Generating Industry-Leading Results and ROI

- Reduced Malware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

87% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.

Source: 2020 KnowBe4 Phishing by Industry Benchmarking Report

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com