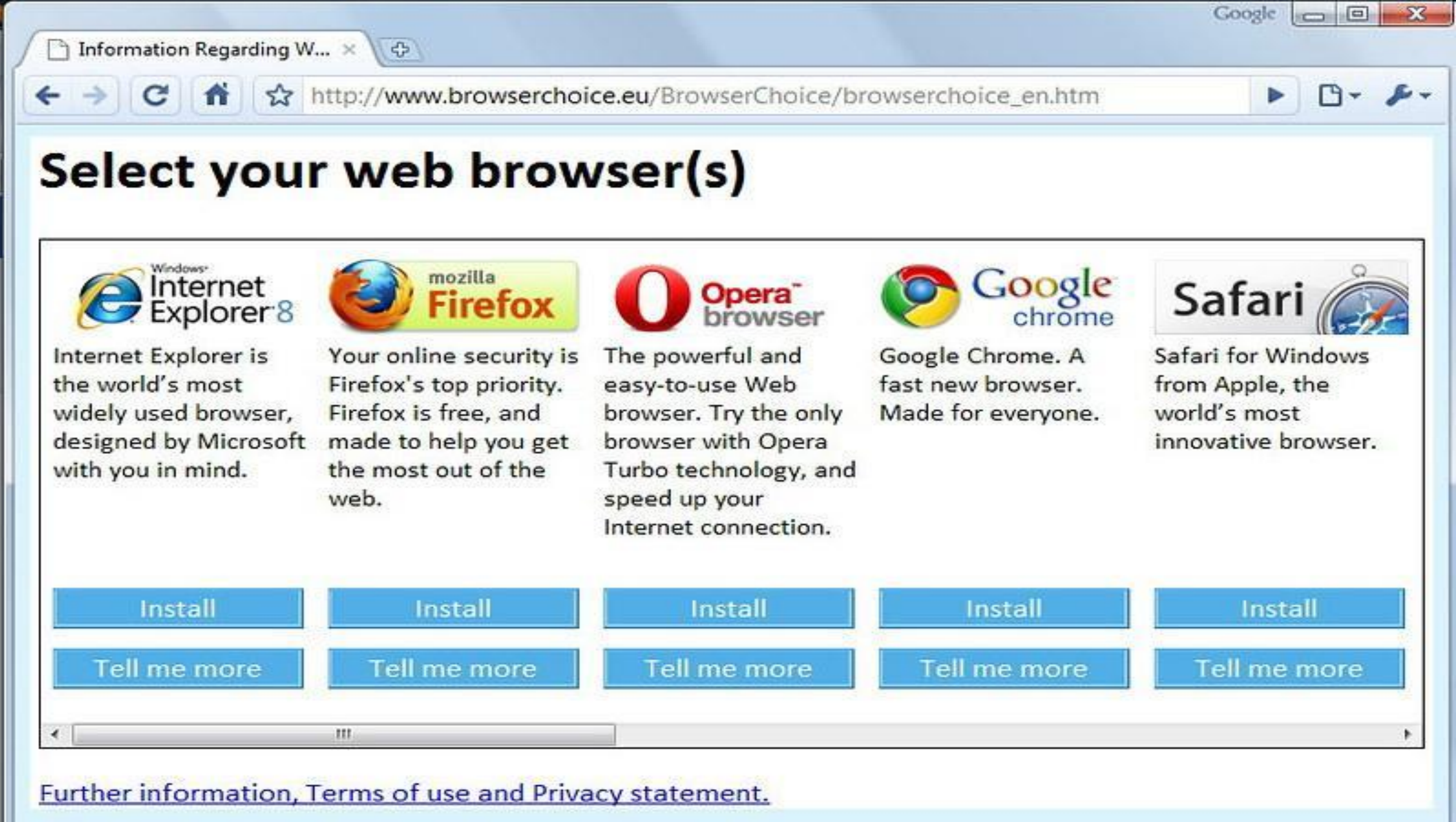
CYBER SECURITY

STOP. THINK. CONNECT



Google
Information Regarding W...
http://www.browserchoice.eu/BrowserChoice/browserchoice_en.htm

Select your web browser(s)

Windows Internet Explorer 8

Internet Explorer is the world's most widely used browser, designed by Microsoft with you in mind.

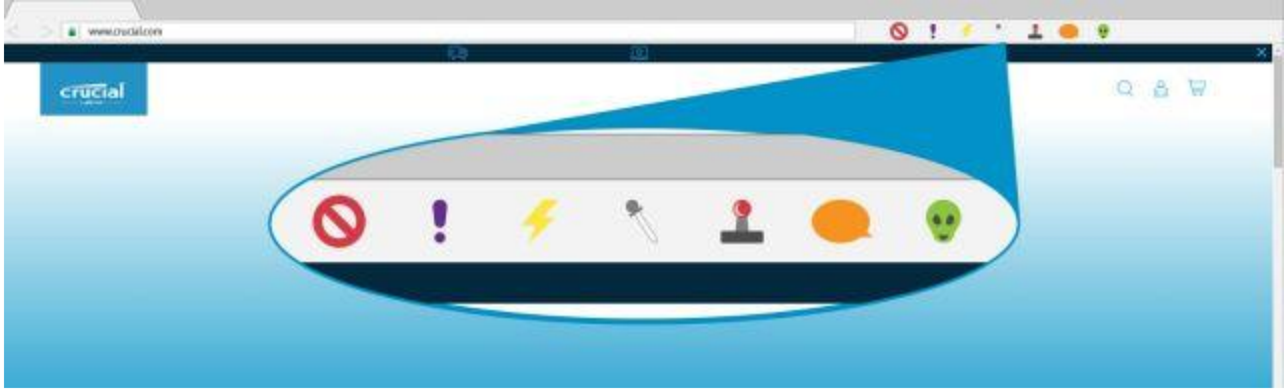
Your online security is Firefox's top priority. Firefox is free, and made to help you get the most out of the web.

The powerful and easy-to-use Web browser. Try the only browser with Opera Turbo technology, and speed up your Internet connection.

Google Chrome. A fast new browser. Made for everyone.

Safari for Windows from Apple, the world's most innovative browser.

Further information, Terms of use and Privacy statement.



Web Browser Extensions

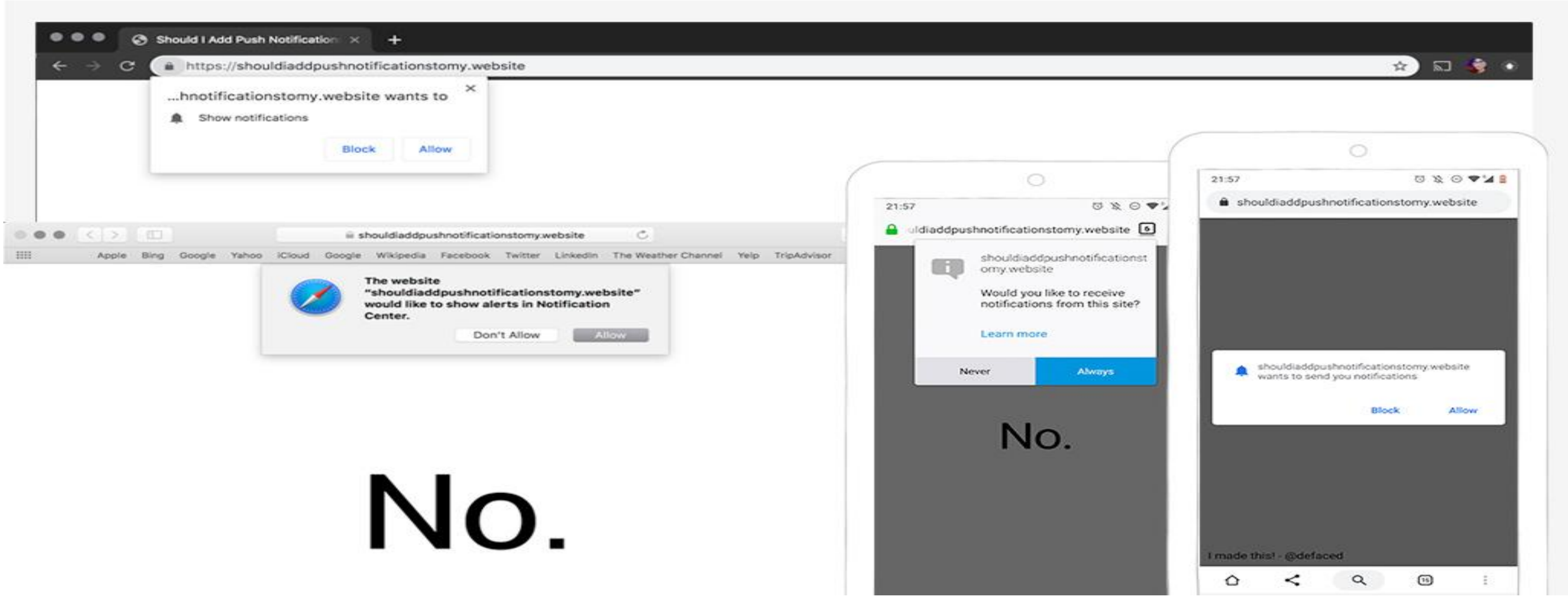
The wild west meets a double edge sword.

Useful and dangerously unregulated.

- Privacy
- Security
- Pop-up Ads

https://shift.com/blog/tips-tricks/the-10-best-browser-extensions-for-productivity

READ the POP-UP before clicking!



...hnotificationstomy.website wants to

Show notifications

The website "shouldiaddpushnotificationstomy.website" would like to show alerts in Notification Center.

shouldiaddpushnotificationstomy.website

Would you like to receive notifications from this site?

shouldiaddpushnotificationstomy.website wants to send you notifications

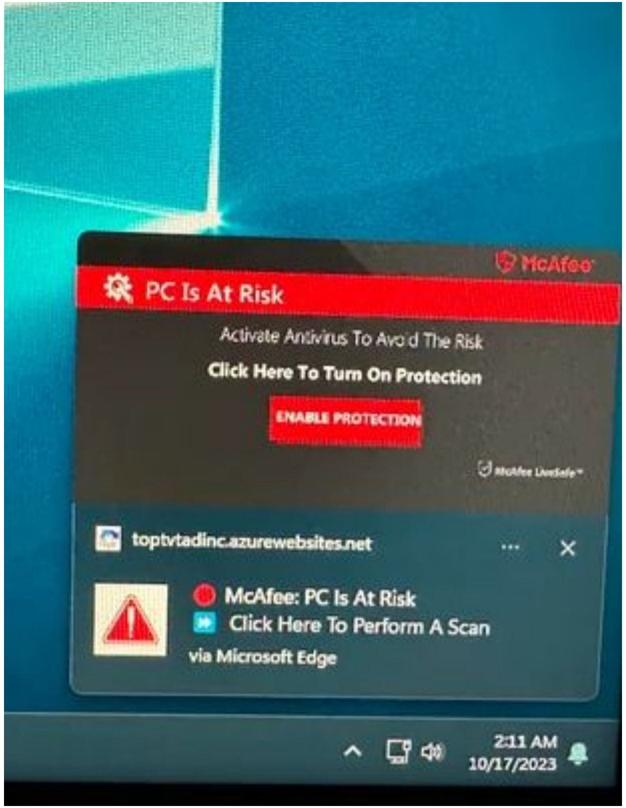
No.

No.

I made this! - @defaced

Should I Add Push Notification
https://shouldiaddpushnotificationstomy.website
Block
Allow
shouldiaddpushnotificationstomy.website
Apple
Bing
Google
Yahoo
iCloud
Google
Wikipedia
Facebook
Twitter
LinkedIn
The Weather Channel
Yelp
TripAdvisor
Don't Allow
Allow
21:57
uldiaddpushnotificationstomy.website
Learn more
Never
Always
21:57
shouldiaddpushnotificationstomy.website
Block
Allow

https://stephaniewalter.design/blog/the-ultimate-guide-to-not-fck-up-push-notifications/



McAfee

PC Is At Risk

Activate Antivirus To Avoid The Risk

Click Here To Turn On Protection

ENABLE PROTECTION

McAfee LiveSafe™

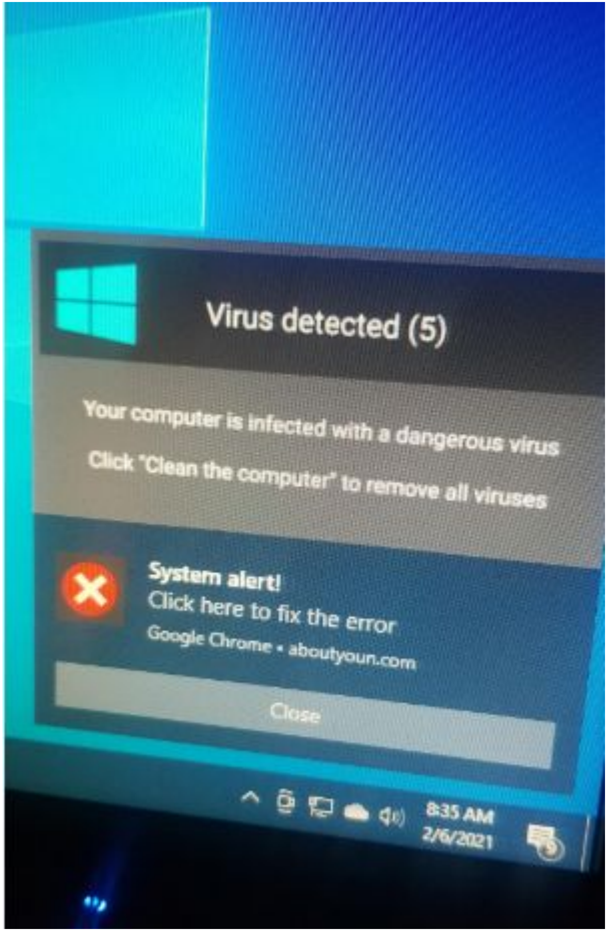
toptvtadinc.azurewebsites.net

McAfee: PC Is At Risk

Click Here To Perform A Scan

via Microsoft Edge

2:11 AM
10/17/2023



Virus detected (5)

Your computer is infected with a dangerous virus

Click "Clean the computer" to remove all viruses

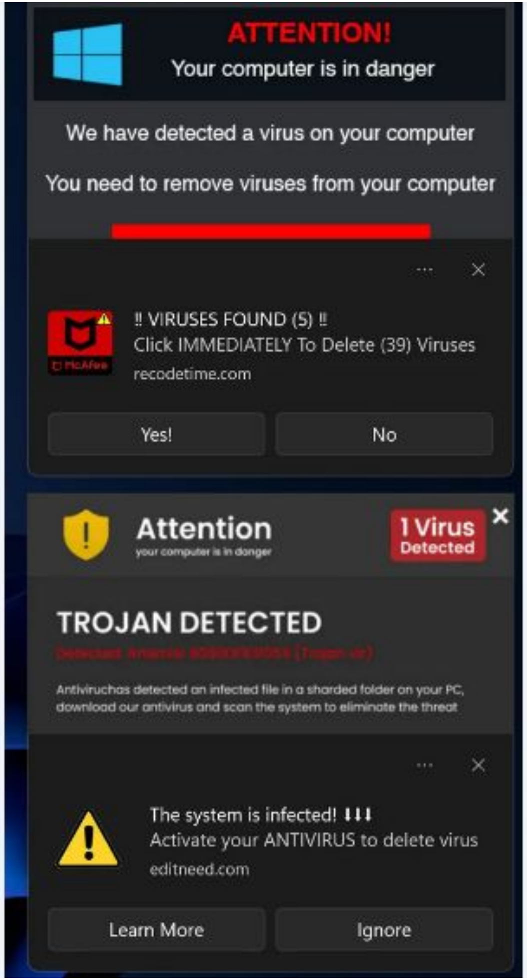
System alert!

Click here to fix the error

Google Chrome • aboutyoun.com

Close

8:35 AM
2/6/2021



ATTENTION!

Your computer is in danger

We have detected a virus on your computer

You need to remove viruses from your computer

‼ VIRUSES FOUND (5) ‼

Click IMMEDIATELY To Delete (39) Viruses

recodetime.com

Yes! | No

Attention

your computer is in danger

1 Virus Detected

TROJAN DETECTED

[illegible]

Antiviruchas detected an infected file in a sharded folder on your PC, download our antivirus and scan the system to eliminate the threat

The system is infected! ⬇⬇⬇

Activate your ANTIVIRUS to delete virus

editneed.com

Learn More | Ignore

People get hacked primarily through social engineering tactics that exploit human vulnerabilities, often combined with malicious software or exploiting vulnerabilities in systems.

https://haveibeenpwned.com

Common methods include:

Phishing:
Deceiving users into clicking malicious links or revealing sensitive information through seemingly legitimate emails, texts, or calls.

Malware:
Installing harmful software like viruses, Trojans, or spyware that steals data or controls the device without the user's knowledge.

Weak Passwords:
Using easily guessable or reused passwords, making them vulnerable to brute-force attacks or dictionary attacks.

Fake Websites:
Tricking users into entering login credentials on fake, but convincingly designed, websites.

Social Engineering:
Manipulating users into revealing sensitive information through trust-building tactics, often posing as a trusted entity.

Unpatched Vulnerabilities:
Exploiting security flaws in software or operating systems that haven't been updated with patches.

Data Breaches:
Hackers acquiring large amounts of user data from compromised systems, which can then be used for further attacks.

Spam Emails:
Using deceptive emails to lure users into clicking malicious links or downloading infected attachments.

https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware

DO I NEED AN ANTIVIRUS?

answer:
DO YOU TRUST YOURSELF?

IF YES

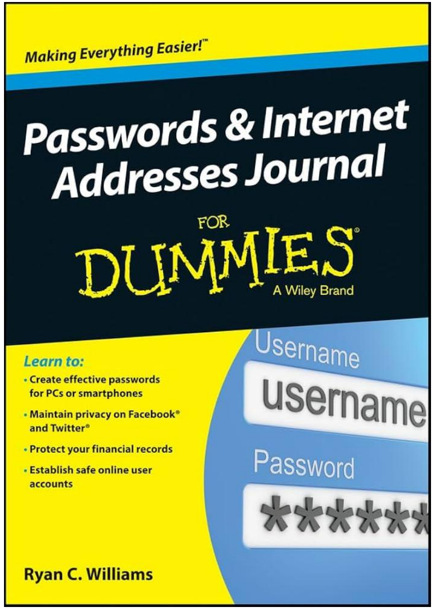
Windows Defender

Malwarebytes®

IF NO

eset®
Digital Security
Progress. Protected.

B Bitdefender®



Making Everything Easier!™

Passwords & Internet Addresses Journal

FOR DUMMIES®

A Wiley Brand

Learn to:

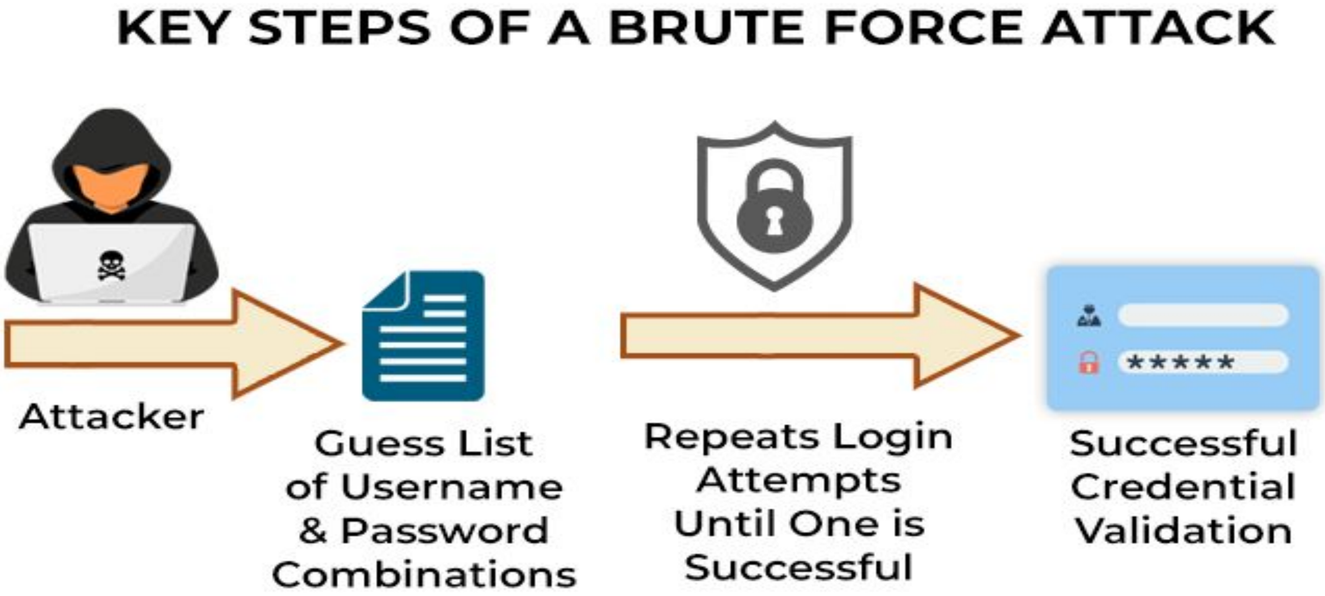
- Create effective passwords for PCs or smartphones
- Maintain privacy on Facebook® and Twitter®
- Protect your financial records
- Establish safe online user accounts

Ryan C. Williams

Account Name + **Password**

- Email
- Username
- Phone #

16 to 20 Characters
Letters, Symbols, & Numbers



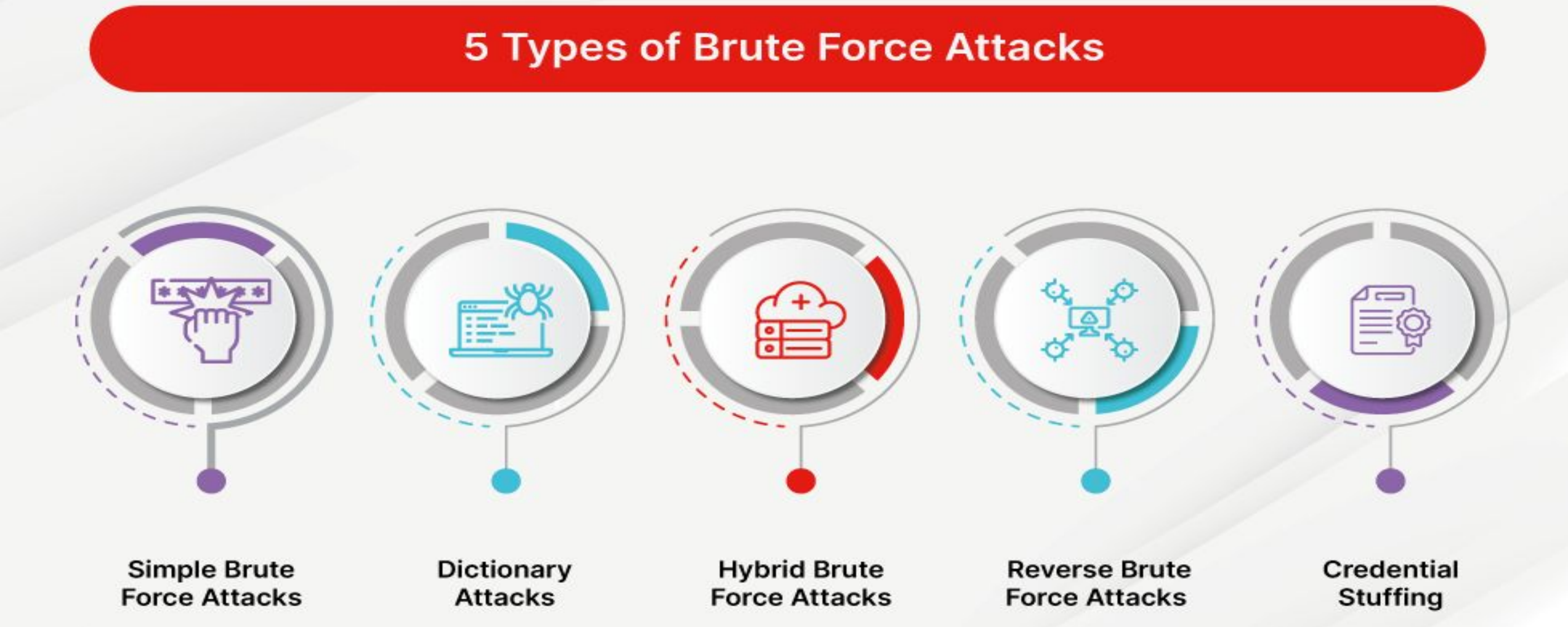
KEY STEPS OF A BRUTE FORCE ATTACK

Attacker

Guess List of Username & Password Combinations

Repeats Login Attempts Until One is Successful

Successful Credential Validation



5 Types of Brute Force Attacks

Simple Brute Force Attacks

Manually attempting to guess a user’s login credentials.

Dictionary Attacks

Using software to try multiple passwords from a list of common words and phrases.

Hybrid Brute Force Attacks

Combination of Brute Force & Dictionary Attacks

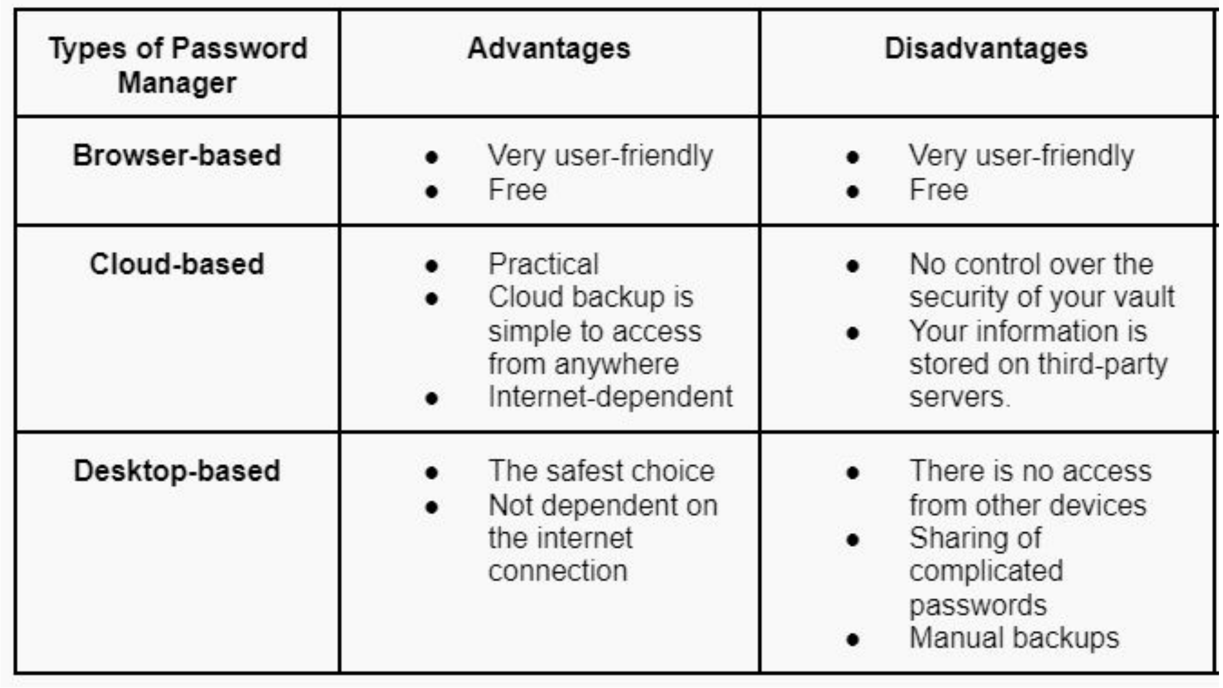
Reverse Brute Force Attacks

Hacker tries one password on as many accounts as possible

Credential Stuffing

Using already combined user credentials and passwords together.

GOAL: To stop you from using simple and repeat passwords on multiple sites.



Types of Password Manager	Advantages	Disadvantages
Browser-based	• Very user-friendly • Free	• Very user-friendly • Free
Cloud-based	• Practical • Cloud backup is simple to access from anywhere • Internet-dependent	• No control over the security of your vault • Your information is stored on third-party servers.
Desktop-based	• The safest choice • Not dependent on the internet connection	• There is no access from other devices • Sharing of complicated passwords • Manual backups

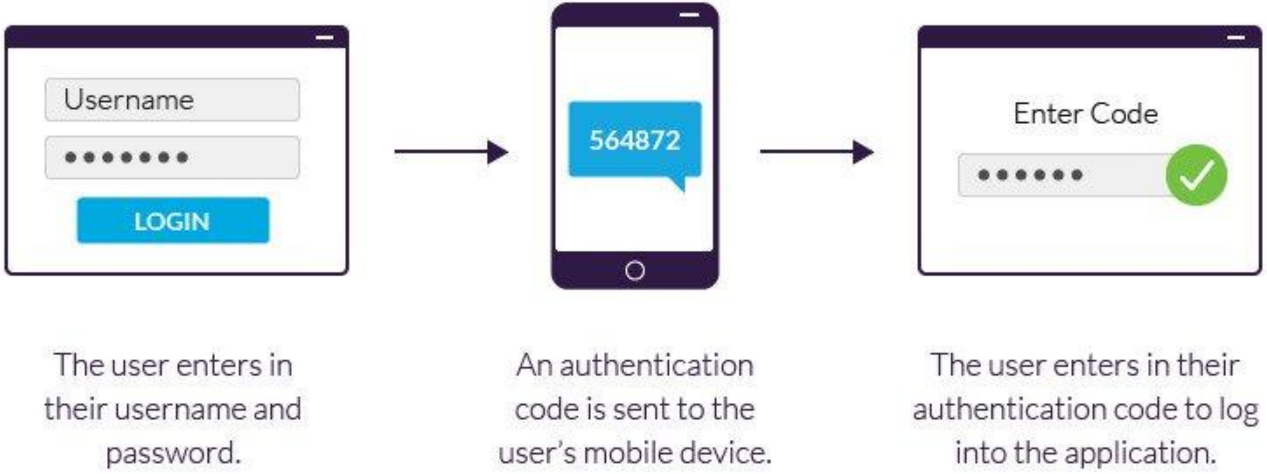
https://blog.1password.com/how-1password-protects-your-data/

If you store your passwords in a browser, those passwords can be hacked.

If your passwords are stored online YES it can be hacked.

Password Managers do store your passwords in the cloud and are stored using encryption.

Two Factor Authentication
2FA



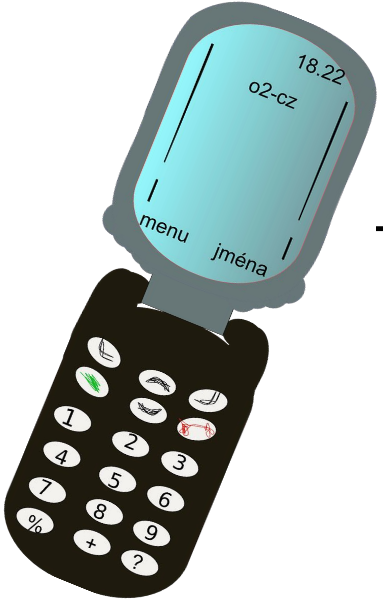
The user enters in their username and password.

An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.

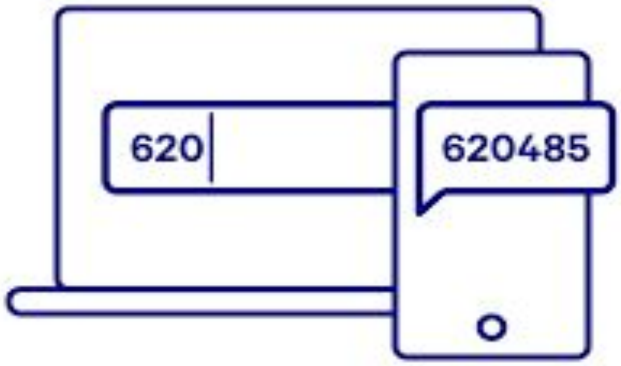
GOAL: Adds an extra barrier to entry if password gets leaked.

2FA just like password managers can be on the cloud or locally stored.
IF IT'S ONLINE IT CAN BE HACKED. STILL USE STRONG PASSWORDS.

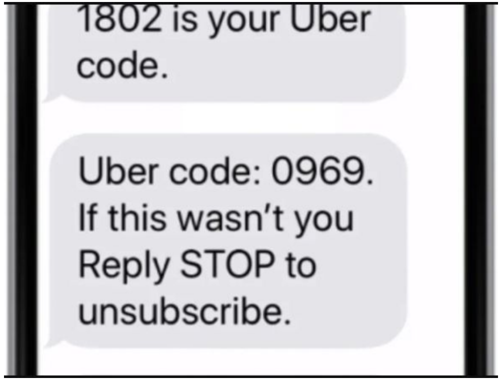


Two Factor Authentication: Flaw of Text Messages

To login enter the code we sent to your phone:



Example: Uber



1802 is your Uber code.

Uber code: 0969. If this wasn't you Reply STOP to unsubscribe.

If you don’t have access to your phone **OR** don’t have the phone number.

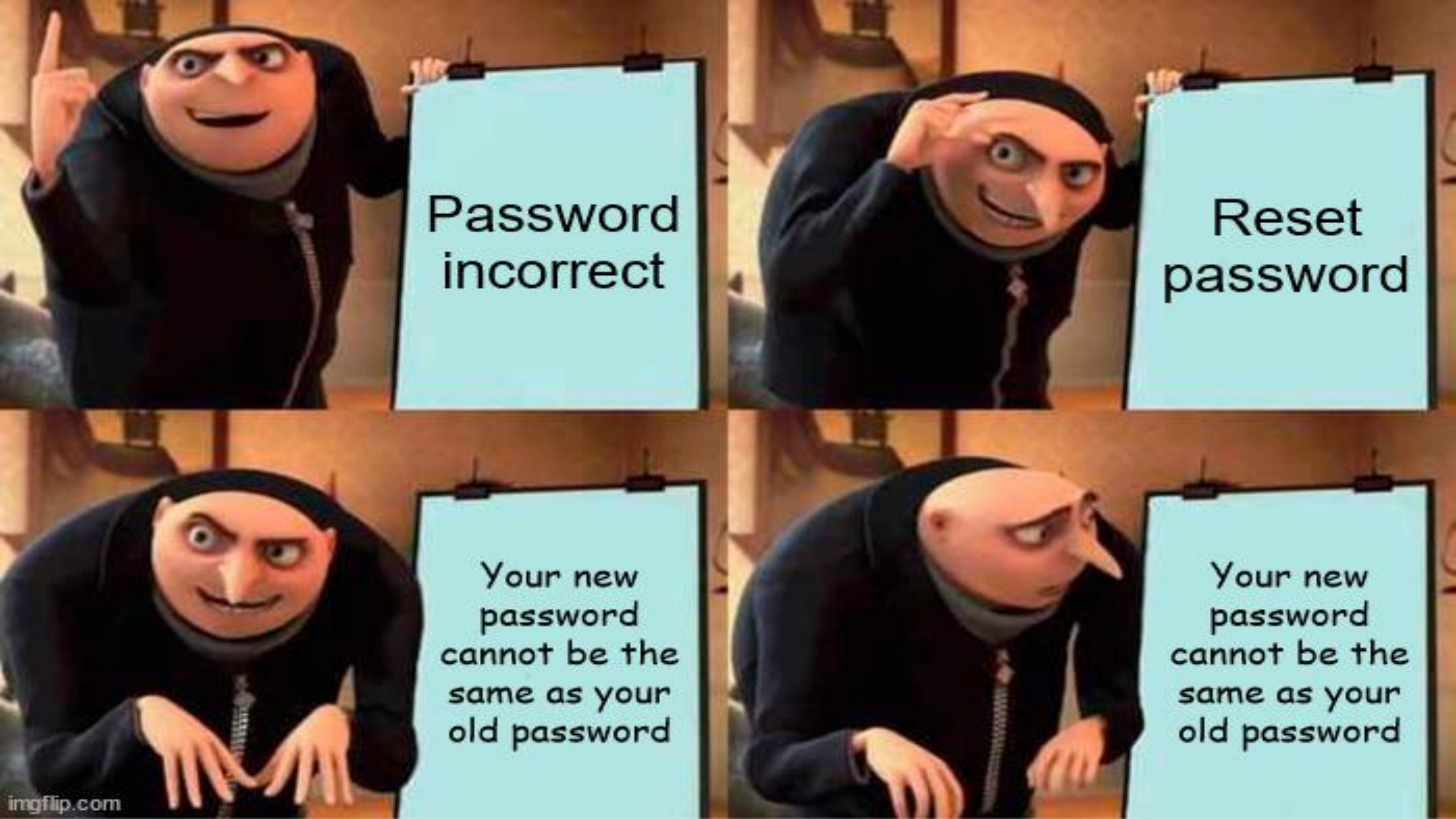
Say “Good-Bye” to that account.

FREE

2-Factor Authenticators

Authentication Codes

- Require a master encrypted password.
- Can be accessed on multiple devices.
- Better security than text message


Password incorrect
Reset password
Your new password cannot be the same as your old password
Your new password cannot be the same as your old password
imgflip.com

What are passkeys?

Passkeys are HERE and they're SECURE! Learn this today...

Crosstalk Solutions ✓

440K subscribers

Even if you do all of this if the website or company gets hacked your info is at risk of getting stolen / leaked.

By using good security practices it prevents that leaked info from being used to access your other accounts.

YES YOUR APPLE DEVICE CAN GET HACKED!*

https://us.norton.com/blog/mobile/can-iphones-get-hacked

*and it’s your fault.

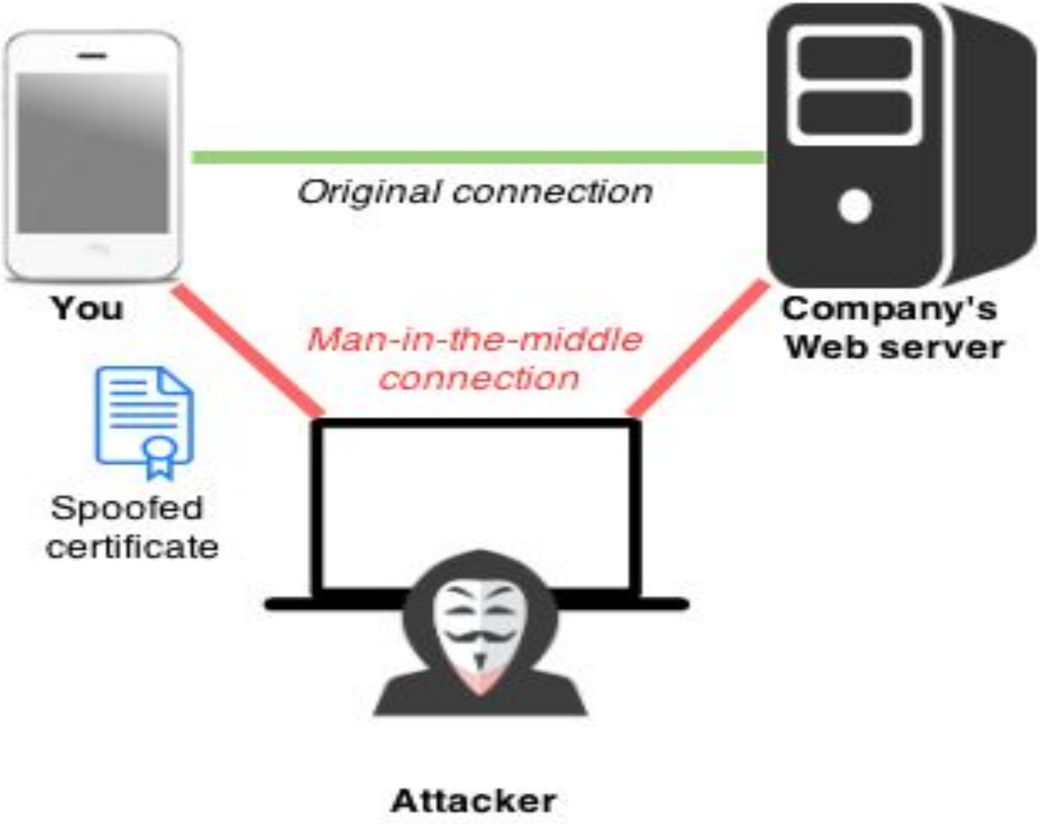
1. You went to a website and downloaded something bad.
2. You gave your data to an unreliable source.
3. You didn’t update the software and apps being used.
4. Using bad / malicious web browser extensions.

A. UPDATE YOUR DEVICES.

B. FOLLOW CYBER SECURITY GUIDELINES

C. LOOK OUT FOR SHOULDER PEEKERS

YES, your home could get hacked.
PUBLIC & PRIVATE Wi-Fi can be hacked too.



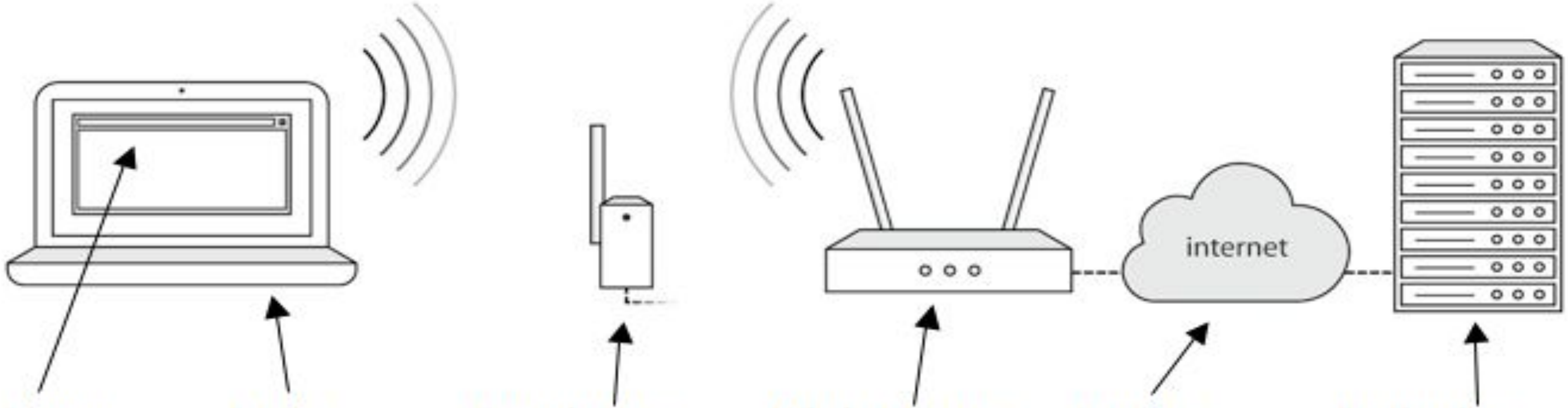
facebook

airbnb

The Weather Channel

THE HOME DEPOT

https://uk.norton.com/blog/iot/keep-your-home-wifi-safe



Browser
Your browser is software that allows you to view and send information over the internet.

Device
Your device uses its WiFi connection to transmit information to and from the browser.

Eavesdropper
The data you transmit is sent over the air. It can be intercepted by anyone within range who knows the WiFi password.

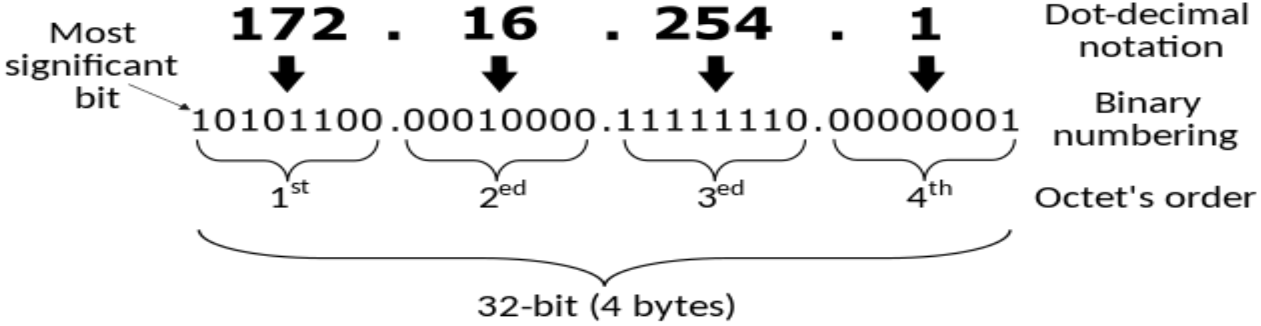
Wireless Router
The router receives the WiFi communication from your device and sends information to and from the internet.

Internet
The Internet is an interconnected system of computer networks that link devices to each other.

Destination
The information reaches the server(s) that host the website you're visiting, and those servers send back the information you requested.

https://www.tp-link.com/us/wifi7/

https://whatismyipaddress.com



172 . 16 . 254 . 1 Dot-decimal notation

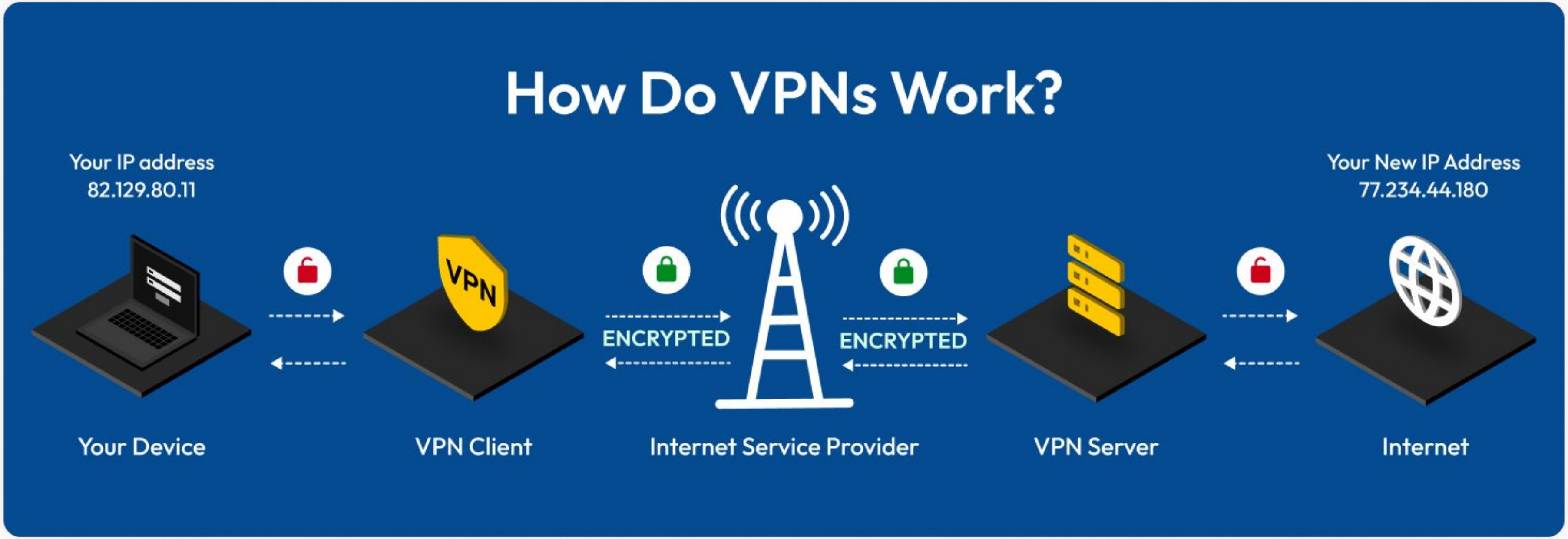
Most significant bit

10101100.00010000.11111110.00000001 Binary numbering

1st 2ed 3ed 4th Octet's order

32-bit (4 bytes)

$15,00
SWATTING EXPLAINED



VPN can keep your IP address secret and safe but it’s not going to prevent cyber threats or prevent viruses & malware.

Next-Gen Wi-Fi Security - WPA3 Explained

Techquickie

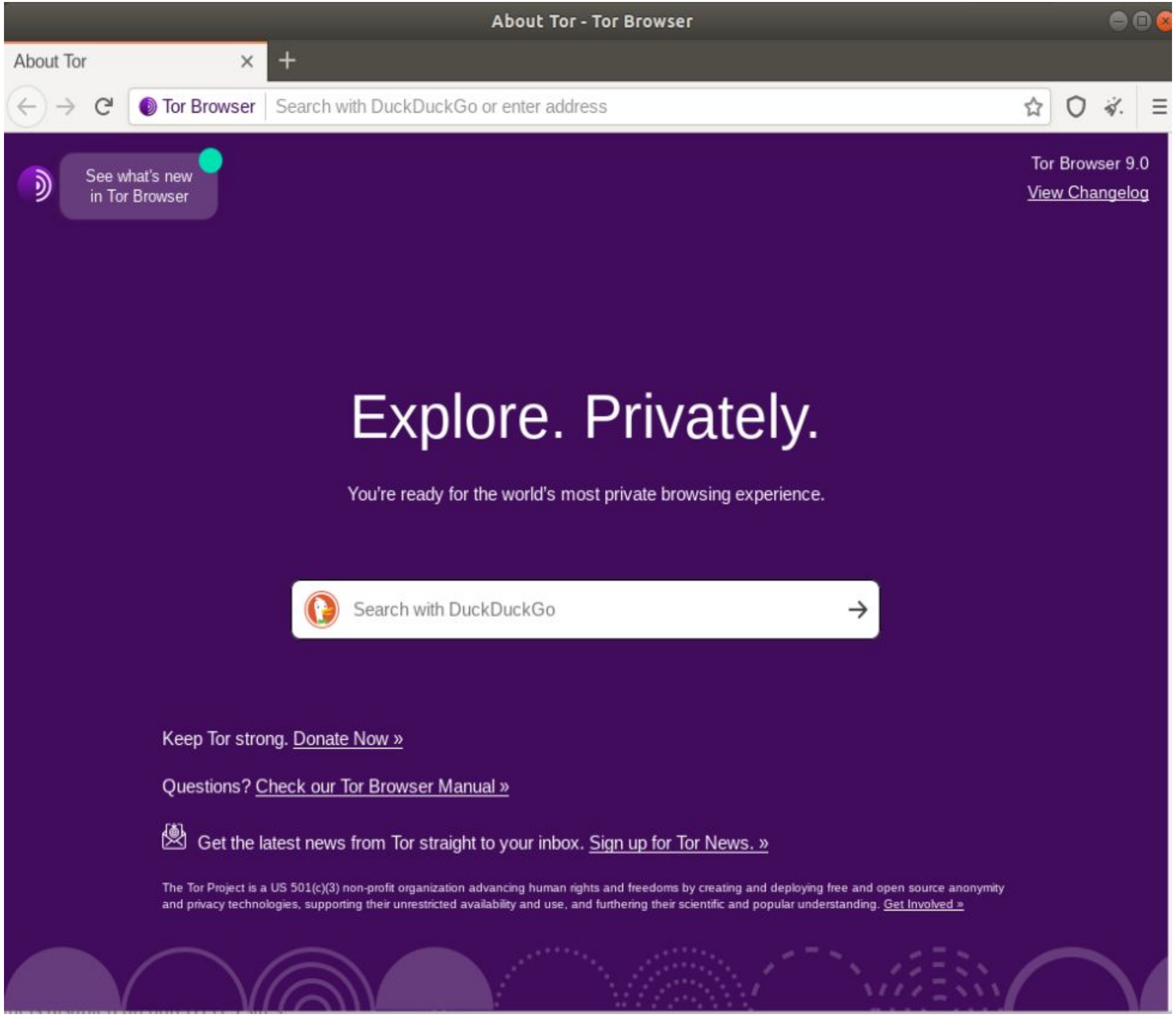
4.29M subscribers

Should you be using WiFi 7 or WPA3? Best Wi-Fi setup?

David Bombal

2.57M subscribers

Private Browser / Incognito Mode



Explore. Privately.

You're ready for the world's most private browsing experience.

Keep Tor strong. Donate Now »

Questions? Check our Tor Browser Manual »

Get the latest news from Tor straight to your inbox. Sign up for Tor News. »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »

Prevents your automatic data such as location from being typed in automatically into the website.

Prevents your web browser cookies and data from being shared.

Common reasons to use private browsing include:

Sharing a device:

When using a computer shared with others, like a public terminal or a family computer, you can avoid leaving traces of your browsing activity.

Managing multiple accounts:

Accessing different accounts on the same website without the browser remembering your logins or influencing future recommendations.

Gift shopping:

Preventing the recipient from seeing hints about the surprise gift you're buying online.

Sensitive content:

Accessing websites with potentially embarrassing or sensitive content without it appearing in your browsing history.

Avoiding personalized advertising:

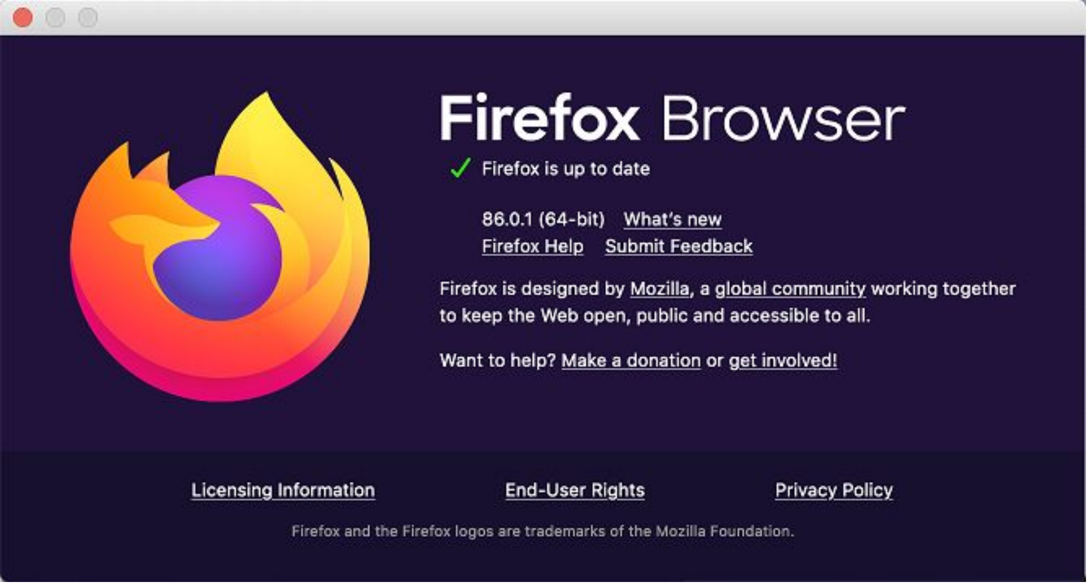
Limiting the tracking of your online activity to avoid personalized ads based on your recent searches.

Price manipulation:

Avoiding potential price increases on sites that might detect repeated visits and adjust prices accordingly.

Privacy concerns:

Generally limiting the amount of data collected about your browsing habits.



Firefox Browser

✓ Firefox is up to date

86.0.1 (64-bit) What's new

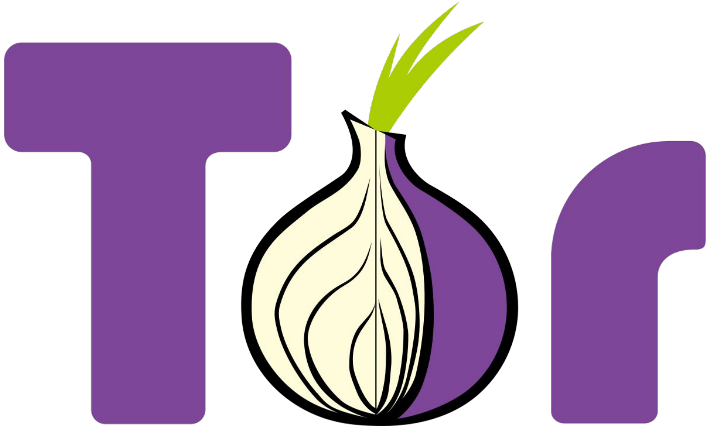
Firefox Help Submit Feedback

Firefox is designed by Mozilla, a global community working together to keep the Web open, public and accessible to all.

Want to help? Make a donation or get involved!

Licensing Information End-User Rights Privacy Policy

Firefox and the Firefox logos are trademarks of the Mozilla Foundation.



https://cookie-script.com/blog/social-media-privacy-issues

https://www.cnet.com/tech/mobile/you-might-be-giving-up-your-location-when-you-share-photos-on-your-iphone/

How to Be Invisible on the Internet. 10 Identifiers to Eliminate

Rob Braxman Tech
467K subscribers

https://www.youtube.com/watch?v=0bhYyZNennA

1. Use Multi-Factor Authentication (2FA)
2. Get a Password Manager
3. Learn how to spot a Phishing Attack
4. Update Everything
5. Start using a VPN
6. Keep in mind your digital footprint

https://www.wired.com/story/how-to-prevent-getting-hacked