

The Life of Breached Data & The Dark Side of Security.

Jarrold Overson
@jsoverson
QCon SF 2016

Ashley Madison hack is not only real, it's worse than we thought

Intimate data for more than 30 million accounts, keys to Windows domain published.



Tech » Gadgets | Cyber Security | Innovation Nation

Live TV

U.S. Edition +



menu



50 million compromised in Evernote hack



By Doug Gross, CNN

Updated 4:34 PM ET, Mon March 4, 2013

Windows domain published.

Sony: PlayStation Breach Involves 70 Million Subscribers

Chris Morris | @MorrisatLarge

Tuesday, 26 Apr 2011 | 5:24 PM ET



Sony: PlayStation

LinkedIn Lost 167 Million
Account Credentials in Data
Breach

Sony: PlayStation

Link

Yahoo confirms biggest data breach ever

If you've got a Yahoo mail account, there's cause for concern. The internet giant says hackers have stolen the personal information of some 500 million users. It is the biggest data breach in history.

It's more than just massive breaches
from large companies, too.

@dumpmon

Hi there! I'm a bot which monitors multiple paste sites for password dumps and other sensitive information.

 **Dump Monitor** @dumpmon · 32m
dumpmon.com/raw.php?i=hBqf... Emails: 827 Keywords: 0.22 #infoleak



 **Dump Monitor** @dumpmon · 47m
dumpmon.com/raw.php?i=93Sw... Emails: 168 Keywords: 0.0 #infoleak



 **Dump Monitor** @dumpmon · 53m
dumpmon.com/raw.php?i=B2tk... Emails: 663 Keywords: 0.33 #infoleak



 **Dump Monitor** @dumpmon · 53m
dumpmon.com/raw.php?i=iG3S... Emails: 1638 Hashes: 1 E/H: 1638.0 Keywords: 0.19 #infoleak



It's small continuous, streams of exploitable data



**grand
theft
auto**

tumblr.





2.2 Billion

Leaked credentials in 2016 alone

YAHOO!

Every breach adds a piece of *you* to a criminal's database.



Passwords, emails, names, security questions & answers, addresses, and more

JOIN ME!



Traditional security is like flossing.



We know we're supposed to care,
but is it ***really*** that important?

OWASP Top 10

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-Site Scripting (XSS)

A4 – Insecure Direct Object References

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-Site Request Forgery (CSRF)

A9 – Using Known Vulnerable Components

A10 – Unvalidated Redirects and Forwards

OWASP Automated Threats

OAT-020 Account Aggregation

OAT-006 Expediting

OAT-019 Account Creation

OAT-004 Fingerprinting

OAT-003 Ad Fraud

OAT-018 Footprinting

OAT-009 CAPTCHA Bypass

OAT-005 Scalping

OAT-010 Card Cracking

OAT-011 Scraping

OAT-001 Carding

OAT-016 Skewing

OAT-012 Cashing Out

OAT-013 Sniping

OAT-007 Credential Cracking

OAT-017 Spamming

OAT-008 Credential Stuffing

OAT-002 Token Cracking

OAT-015 Denial of Service

OAT-014 Vulnerability Scanning

These attacks aren't cost effective unless *automated*

BY EVIL
ROBOTS



Our **user-friendly APIs** enable our attackers

nerdBase

nerdBase REST API

[Contact the developer](#)

[Apache 2.0 License](#)

user : Operations for Users

Show/Hide | List Operations | Expand Operations | Raw

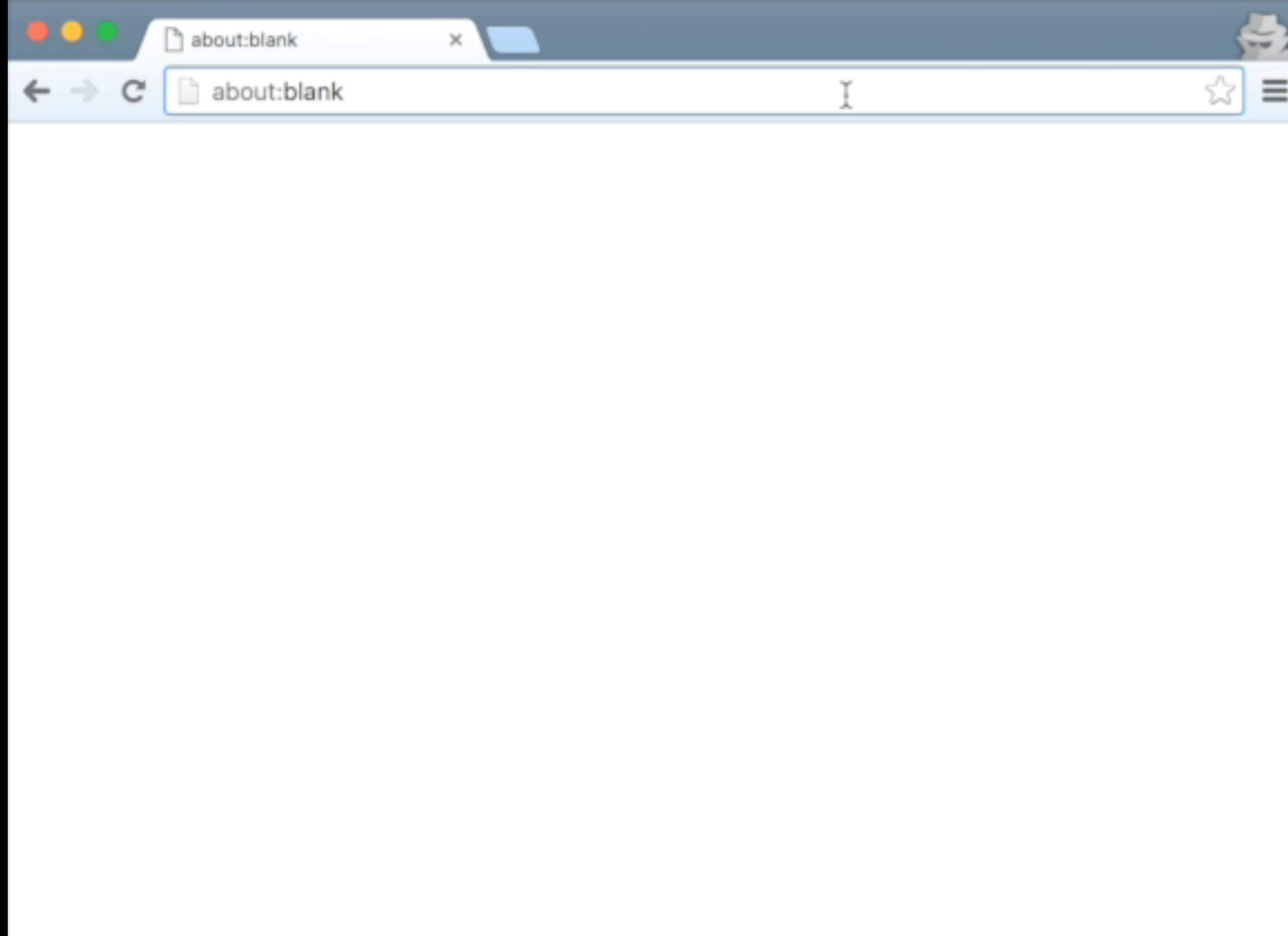
GET	/user/list	List Users
DELETE	/user/delete/{id}	Deletes User
POST	/user/save	Creates and updates a User
GET	/user/edit/{id}	Get User by id

role : Operations for Roles

Show/Hide | List Operations | Expand Operations | Raw

GET	/role/list	List Roles
DELETE	/role/delete/{id}	Deletes Role
POST	/role/save	Creates and updates a Role
GET	/role/edit/{id}	Get Role by id

Not just these APIs



The APIs we expose unintentionally.

The image shows a browser window displaying the Amazon sign-in page. The browser's address bar shows the URL: `https://www.amazon.com/ap/signin?_encoding=UTF8&openid.assoc_handle=usflex&o...`. The page features the Amazon logo at the top, followed by a "Sign in" heading. Below this, there are two input fields: "Email (phone for mobile accounts)" containing `jsoverson@gmail.com` and "Password" containing a masked password. A "Forgot your password?" link is positioned to the right of the password field. A yellow "Sign in" button is centered below the inputs. At the bottom of the sign-in box, there is a link for "New to Amazon?" and a "Create an account" button. A footer note states: "By signing in you are agreeing to our [Conditions of Use and Sale](#) and our [Privacy Notice](#)."

The browser's developer console is open on the right side of the screen, showing the following JavaScript console log:

```
> $(' [name=email] ').value='jsoverson@gmail.com'  
< "jsoverson@gmail.com"  
> $(' [name=password] ').value='noneofyourbusiness'  
< "noneofyourbusiness"  
> |
```

The APIs we expose unintentionally.

The image shows a browser window displaying the Amazon sign-in page. The browser's address bar shows the URL: `https://www.amazon.com/ap/signin?_encoding=UTF8&openid.assoc_handle=usflex&o...`. The page features the Amazon logo at the top, followed by a "Sign in" heading. Below this, there are two input fields: "Email (phone for mobile accounts)" containing `jsoverson@gmail.com` and "Password" containing a masked password. A "Forgot your password?" link is positioned to the right of the password field. A yellow "Sign in" button is located below the password field. At the bottom of the sign-in box, there is a link for "New to Amazon?" and a "Create an account" button. A footer note states: "By signing in you are agreeing to our [Conditions of Use and Sale](#) and our [Privacy Notice](#)."

The browser's developer console is open on the right side of the screen, showing the following JavaScript execution log:

```
> $(' [name=email] ').value='jsoverson@gmail.com'  
< "jsoverson@gmail.com"  
> $(' [name=password] ').value='noneofyourbusiness'  
< "noneofyourbusiness"  
> $('#signInSubmit').click()  
< undefined  
>
```

The APIs we expose unintentionally.



Data Breaches Top 800 to Date in 2016

24/7 Wall St. - Oct 28, 2016

Anyone who bought a “Never Hillary” poster or donated funds to the National Republican Senatorial Committee (NRSC) between March and ...



US bank authority warns of data breach that took 10000 records

Engadget - Oct 31, 2016

Government **data breaches** aren't always the work of foreign intruders ... a policy in August 2016 that bars employees from transferring data to ...

Federal bank regulator reveals employee data breach

FedScoop - Oct 31, 2016

[View all](#)



Health data breaches in Q3 2016 outpace first two quarters

Healthcare IT News - Oct 14, 2016

Some 118 security incidents were either reported to the Department of Health and Human Services or first disclosed in the media in Q3 2016, ...



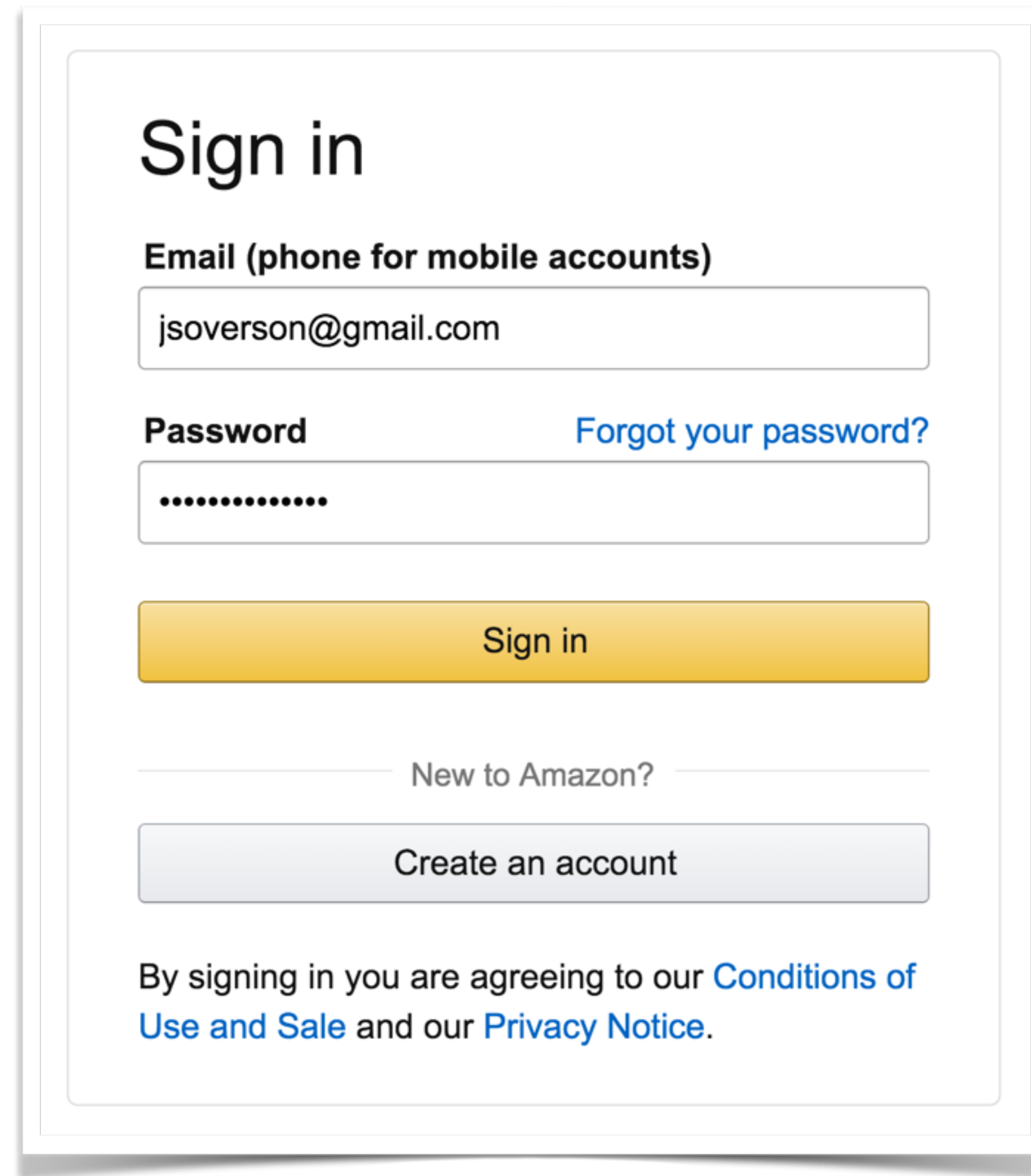
Data Breaches Up 20% to Date in 2016

24/7 Wall St. - Oct 20, 2016

The issue of voter security and potential vote fraud have been swirling as the political campaigning approaches the November 8 election day.

When you read about breaches, what do you do?

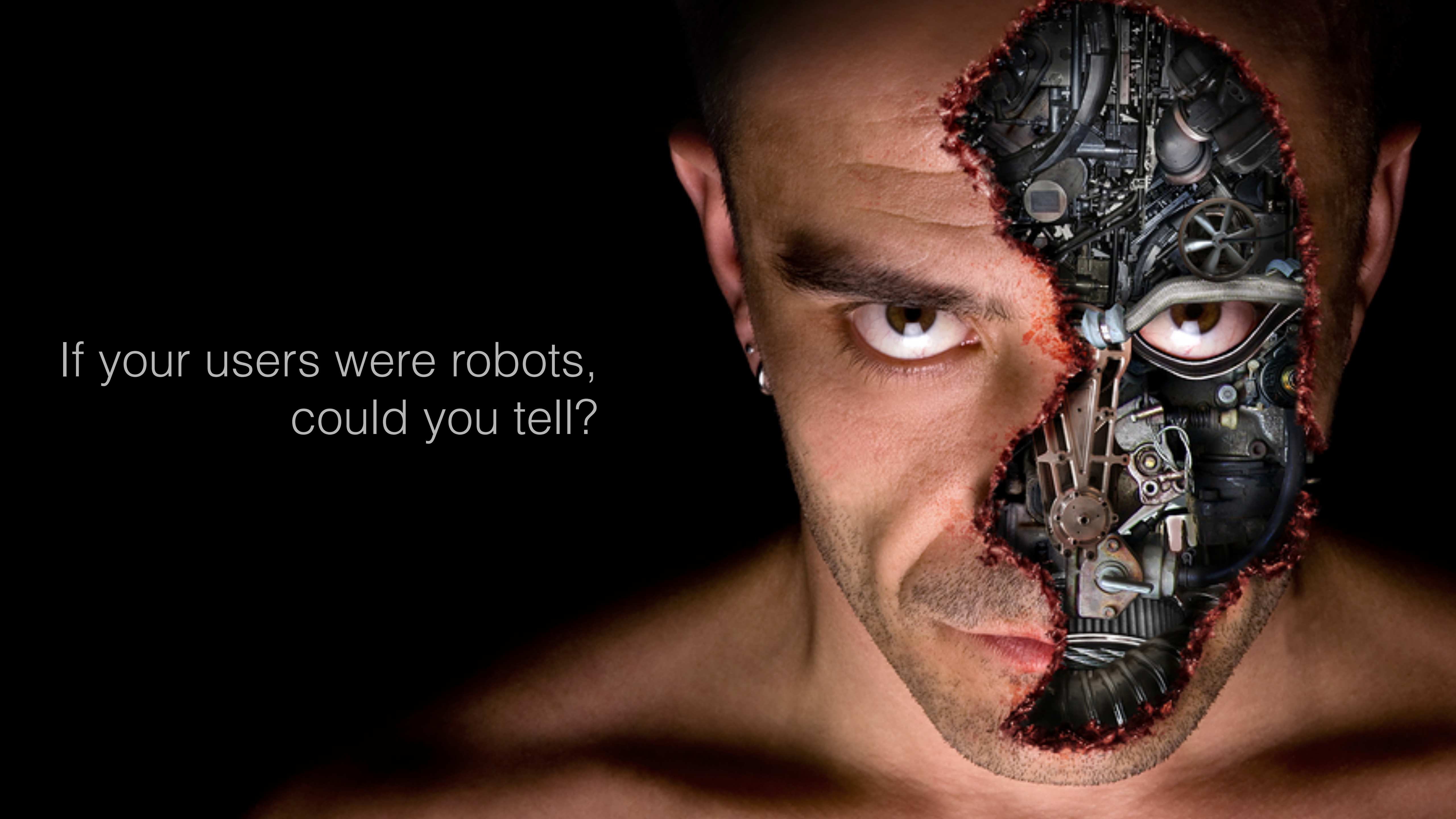
Even if you have the most secure site in the world,

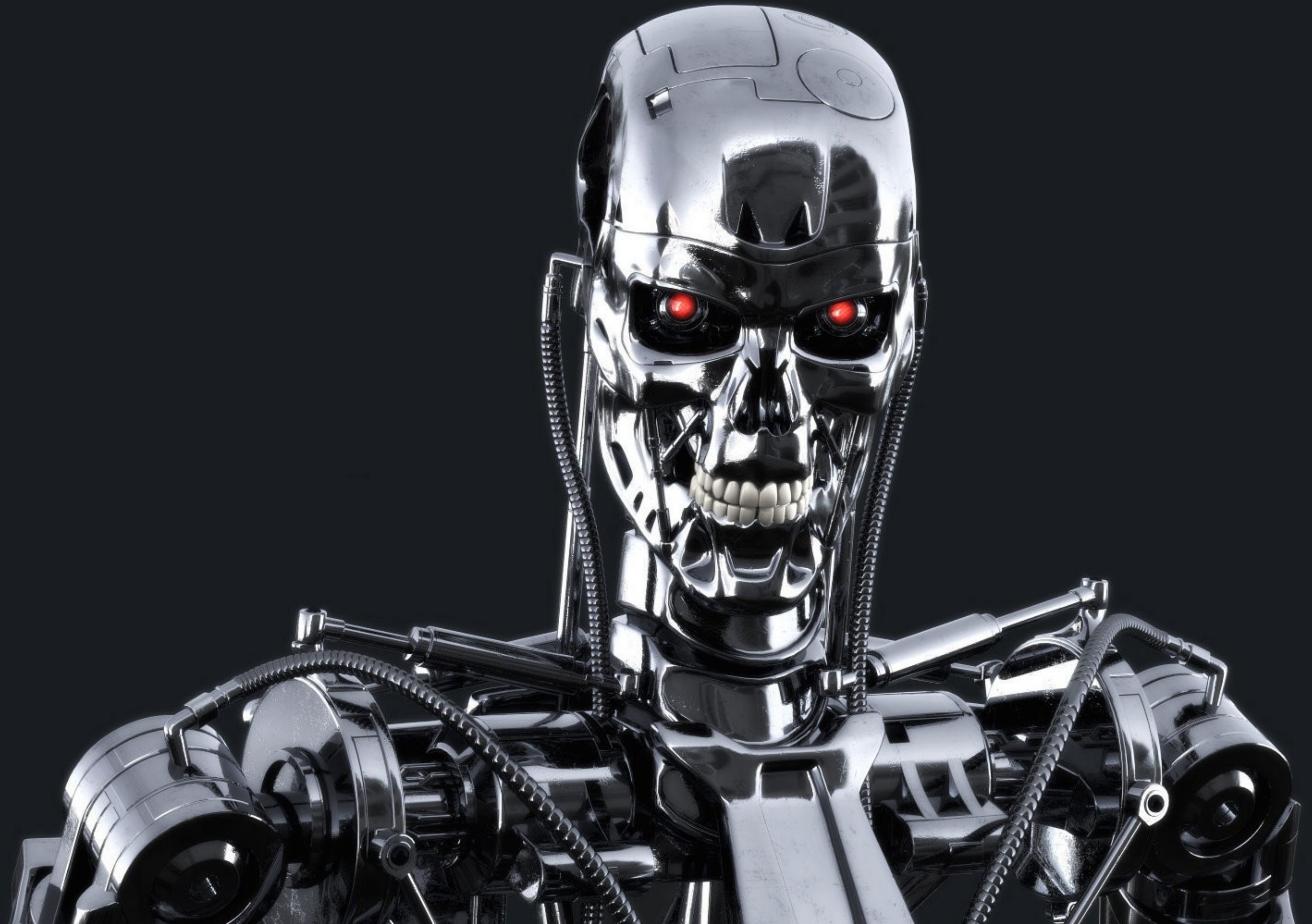


The image shows a screenshot of a web form titled "Sign in". The form is contained within a white box with a thin border and a subtle drop shadow. At the top, the title "Sign in" is displayed in a large, bold, black font. Below the title, the label "Email (phone for mobile accounts)" is followed by a text input field containing the email address "jsoverson@gmail.com". Underneath, the label "Password" is followed by a password input field filled with ten black dots. To the right of the password field is a blue link that says "Forgot your password?". Below these fields is a prominent yellow button with the text "Sign in" in black. Further down, there is a horizontal line with the text "New to Amazon?" centered between two short dashes. Below this line is a light gray button with the text "Create an account" in black. At the bottom of the form, there is a line of text: "By signing in you are agreeing to our [Conditions of Use and Sale](#) and our [Privacy Notice](#)."

you don't usually protect against legitimate user logins.

If your users were robots,
could you tell?





What percentage of traffic is from bots?

What percentage of traffic is from bots?

95%

(Current record for automation against a login page, via Shape Security)

Why?

Do you...

For example

Store a type of currency?

actual money, point values, gift cards

Sell goods?

physical, digital, services

Have unique PII?

health care, social networks

Have user generated content?

forums, social networks, blogs, comments

Have time sensitive features?

tickets, flash sales, reservations

Pay for digitally validated behavior?

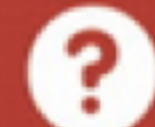
ad clicks, reviews, "uber for X"

If you have value, there is value in **exploiting you**.

Targeted Fraud can take many forms.

morning overlooks

Type the two words:



reCAPTCHA™

stop spam.
read books.

But we have captchas!

SCIENTIFIC
AMERICAN™

TECH

Time to Kill Off Captchas

How the bot-proofing of the Internet is bringing humans down

By David Pogue on March 1, 2012  16

But captchas don't work.

Estimated 200 million+ hours* spent every year deciphering squiggly letters.

* Luis Von Ahn, creator of captcha



FASTEST DISCOUNT CAPTCHA SOLVERS



Advertisement

English Русский 简体中文

Home

F.A.Q.

API

Order CAPTCHAs

DBC Points

Testimonials

Contact Us

Login

CAPTCHA Bypass done right

With Death by Captcha you can solve any CAPTCHA. All you need to do is implement our API, pass us your CAPTCHAs and we'll return the text. It's that easy!

Please note that our services should be used only for research projects and any illegal use of our services is strictly prohibited. Any bypass and CAPTCHA violations should be reported to help@deathbycaptcha.com

Death By Captcha Offers:

- Starting from an incredible low price of **\$1.39** (\$0.99 for **Gold Members** !) for **1000** solved CAPTCHAs.
- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.
- An **average response time of 11 seconds**, with an **average accuracy rate of 90% or more**. And you always pay for correctly solved CAPTCHA only!
- Easy-to-use **API** available for most popular programming languages.

STATUS: OK

Average solving time 1 minute ago: 9 sec

5 minutes ago: 9 sec

15 minutes ago: 9 sec

Today's average accuracy rate: **92.8 %**
(updated every minute)

Create a **FREE** account

Log In

Username:

Services have been made making captcha bypass even easier.



FASTEST DISCOUNT CAPTCHA SOLVERS



Highly Annonymous HTTP / HTTPS Proxies

FRESH PROXIES! NO BLOCKS!

www.SearchScrape.com



Advertisement

English Русский 简体中文

Home

F.A.Q.

API

Order CAPTCHAs

DBC Points

Testimonials

Contact Us

Login

STATUS: OK

Average solving time 1 minute ago: 9 sec

5 minutes ago: 9 sec

CAPTCHA Bypass done right

Starting from an incredible low price of **\$1.39** (\$0.99 for **Gold Members !**) for **1000** solved CAPTCHAs.

Please note that our services should be used only for research projects and any illegal use of our services is strictly prohibited. Any bypass and CAPTCHA violations should be reported to help@deathbycaptcha.com

Death By Captcha Offers:

- Starting from an incredible low price of **\$1.39** (\$0.99 for **Gold Members !**) for **1000** solved CAPTCHAs.
- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.
- An **average response time of 11 seconds**, with an **average accuracy rate of 90% or more**. And you always pay for correctly solved CAPTCHA only!
- Easy-to-use **API** available for most popular programming languages.

Create a FREE account

Log In

Username:

Services have been made making captcha bypass even easier.

**Work At Home
Mum Makes**

\$7,397

A Month!

SEE MORE >>>

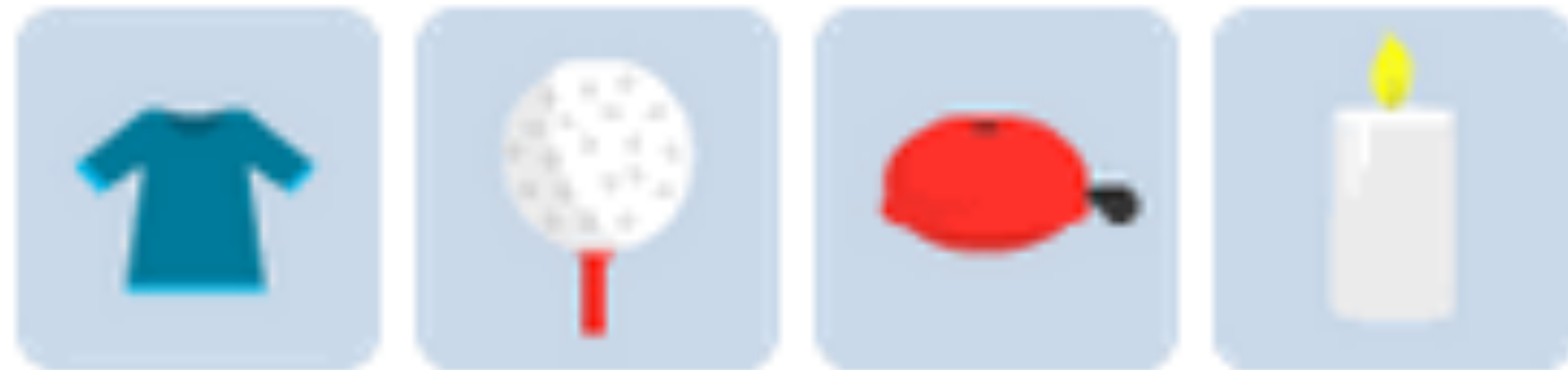
Ever wonder where these ads go?

Data Entry Job Description


- ➔ we will provide you the image files
- ➔ you will have to type the content as it is given in image files in notepad
- ➔ No editing, No framework, No tagging, No correction, No justifications
- ➔ It is just simple. Just see and type what is there in the image files

There's big money in "Work from Home Data Entry" jobs

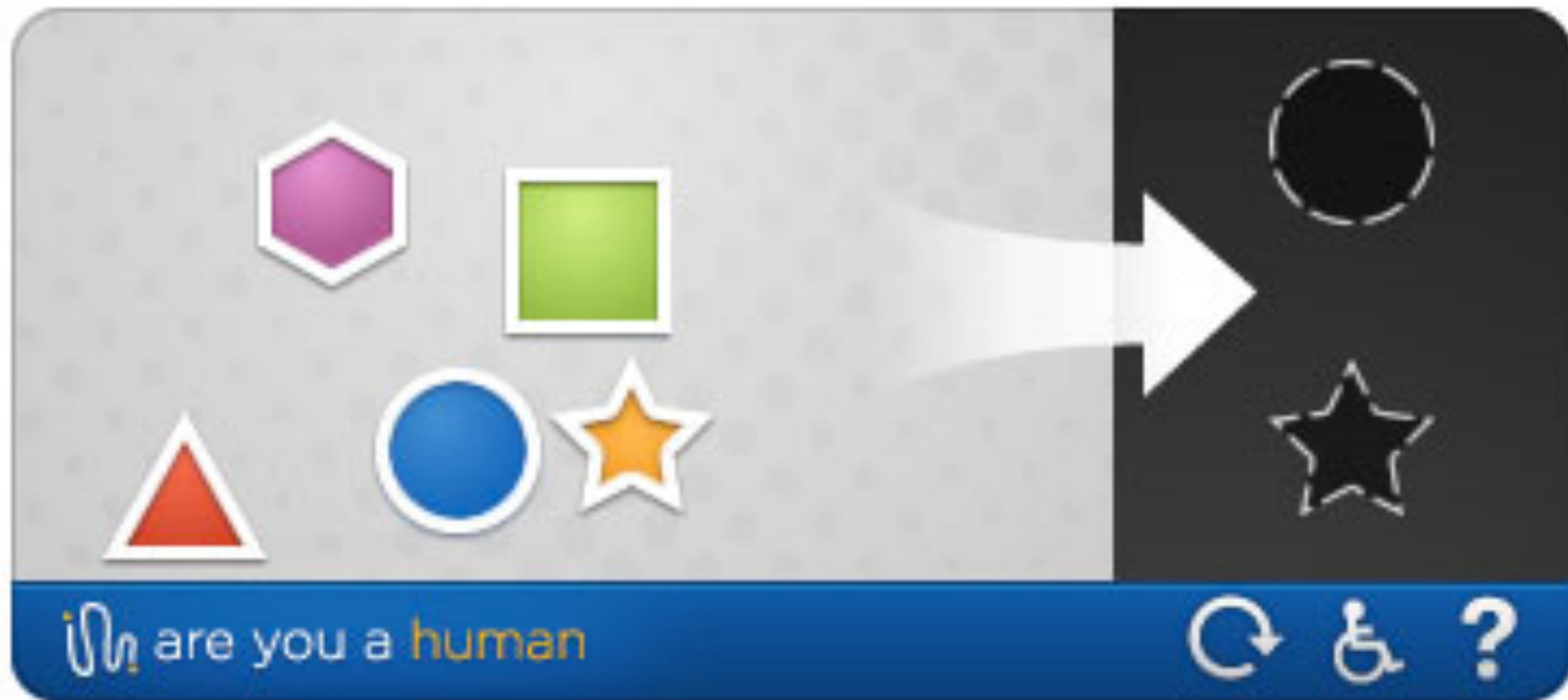
Verify your real existence
Drag the bell to the bike



Reset

Powered by sweetCapcha 

So we seek alternatives.



Some rely on simple behavior analysis

Click 3 pictures of kittens to submit



Some rely on kittens

SILENCE
SILENCE

Band's name here



METAL CAPTCHA
HEAVY/CIFTS

DISMEMBERS

Band's name here



METAL CAPTCHA
HEAVY/CIFTS

W

Band's name here



METAL CAPTCHA
HEAVY/CIFTS

BAT
SANTH

Band's name here



METAL CAPTCHA
HEAVY/CIFTS

Some rely on a love for death metal

Google new reCAPTCHA using JavaScript



I'm not a robot



reCAPTCHA

[Privacy](#) - [Terms](#)

Some are very high profile

How?

They use a lot of the same tools we already use.

[SOURCE CODE](#)[DOCUMENTATION](#)[API](#)[EXAMPLES](#)[FAQ](#)

Full web stack No browser required

PhantomJS is a headless WebKit scriptable with a JavaScript API. It has **fast** and **native** support for various web standards: DOM handling, CSS selector, JSON, Canvas, and SVG.

[Download v2.1](#)[Get started](#)

```
// Simple Javascript example

console.log('Loading a web page');
var page = require('webpage').create();
var url = 'http://phantomjs.org/';
page.open(url, function (status) {
  //Page is loaded!
  phantom.exit();
});
```

Community:

[Read the release notes](#)[Join the mailing list](#)[Report bugs](#)

PhantomJS is an optimal solution for

HEADLESS WEBSITE TESTING

Run functional tests with frameworks such as Jasmine, QUnit, Mocha, Capybara, WebDriver, and many others.

[Learn more](#)

SCREEN CAPTURE

Programmatically capture web contents, including SVG and Canvas. Create web site screenshots with thumbnail preview. [Learn more](#)

PAGE AUTOMATION

Access and manipulate webpages with the standard DOM API, or with usual libraries like jQuery.

[Learn more](#)

NETWORK MONITORING

Monitor page loading and export as standard HAR files. Automate performance analysis using YSlow and Jenkins. [Learn more](#)

PhantomJS is an optimal solution for

PhantomJS is a headless WebKit scriptable with a JavaScript API. It has **fast** and **native** support for various web standards: DOM handling, CSS selector, JSON, Canvas, and SVG.

```
var page = require('webpage').create();
var url = 'http://phantomjs.org/';
page.open(url, function (status) {
  //Page is loaded!
  phantom.exit();
});
```

Download v2.

Community:

Report bugs

PAGE AUTOMATION
 Access and manipulate webpages with the standard DOM API, or with usual libraries like jQuery.
[Learn more](#)

HEADLESS WEBSITE TESTING
Run functional tests with frameworks such as Jasmine, QUnit, Mocha, Capybara, WebDriver, and many others.
[Learn more](#)

SCREEN CAPTURE
Programmatically capture web contents, including SVG and Canvas. Create web site screenshots with thumbnail preview.
[Learn more](#)

PAGE AUTOMATION
Access and manipulate webpages with the standard DOM API, or with usual libraries like jQuery.
[Learn more](#)

NETWORK MONITORING
Monitor page loading and export as standard HAR files. Automate performance analysis using YSlow and Jenkins.
[Learn more](#)

or

Selenium WebDriver

The biggest change in Selenium recently has been the inclusion of the WebDriver API. Driving a browser natively *as a user would* either locally or on a remote machine using the Selenium Server it marks a leap forward in terms of browser automation.

Selenium WebDriver fits in the same role as RC did, and has incorporated the original 1.x bindings. It refers to both the language bindings and the implementations of the individual browser controlling code. This is commonly referred to as just "WebDriver" or sometimes as Selenium 2.

Selenium 1.0 + WebDriver = Selenium 2.0

- WebDriver is designed in a simpler and more concise programming interface along with addressing some limitations in the Selenium-RC API.
- WebDriver is a compact Object Oriented API when compared to Selenium1.0
- It drives the browser much more effectively and overcomes the limitations of Selenium 1.x which affected our functional test coverage, like the file upload or download, pop-ups and dialogs barrier
- WebDriver overcomes the limitation of Selenium RC's [Single Host origin policy](#)

WebDriver is the name of the key interface against which tests should be written in Java, the implementing classes one should use are listed as below:

[AndroidDriver](#), [ChromeDriver](#), [EventFiringWebDriver](#), [FirefoxDriver](#), [HtmlUnitDriver](#),
[InternetExplorerDriver](#), [PhantomJSdriver](#), [RemoteWebDriver](#), [SafariDriver](#)

For More information on Selenium WebDriver, please see [the documentation](#) and [Remote Control to WebDriver Migration Notes](#).



Selenium is a suite of tools to automate web browsers across many platforms.

Selenium...

- runs in [many browsers](#) and [operating systems](#)
- can be controlled by many [programming languages](#) and [testing frameworks](#).



Selenium WebDriver

The biggest change in Selenium recent releases is the ability to drive a browser natively *as a user would* either through a native browser or through a remote browser. This marks a leap forward in terms of browser automation.

Selenium WebDriver fits in the same category as Selenium Remote Control. It refers to both the language bindings and the server-side code. This is commonly referred to as Selenium.

Selenium 1.0 + WebDriver = Selenium

- WebDriver is designed in a simple way, addressing some limitations in Selenium 1.0
- WebDriver is a compact Object Model
- It drives the browser much more efficiently, which affected our functional test code barrier
- WebDriver overcomes the limitations of Selenium 1.0

WebDriver is the name of the key interface for implementing classes one should use to drive a browser.

[AndroidDriver](#), [ChromeDriver](#), [EventFiringWebDriver](#), [InternetExplorerDriver](#), [PhantomJS](#)

For More information on Selenium WebDriver, see [WebDriver Migration Notes](#).



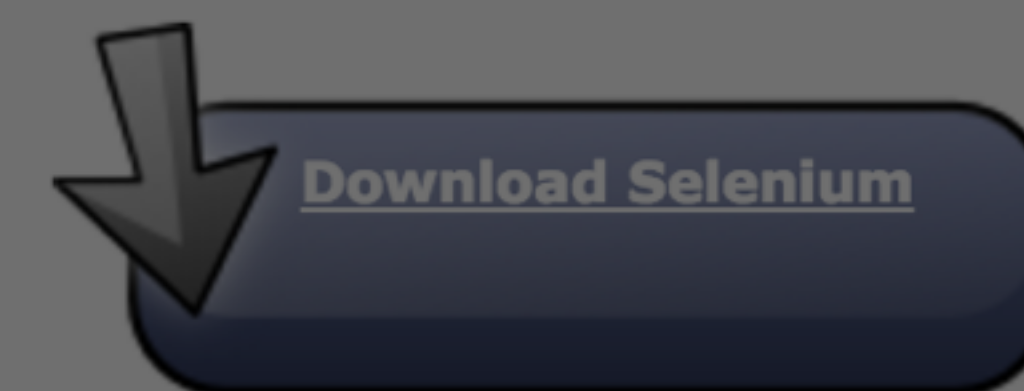
Selenium is a suite of tools to automate web browsers across many platforms.



Selenium is a suite of tools to automate web browsers across many platforms.

Selenium...

- runs in [many browsers](#) and [operating systems](#)
- can be controlled by many [programming languages](#) and [testing frameworks](#).

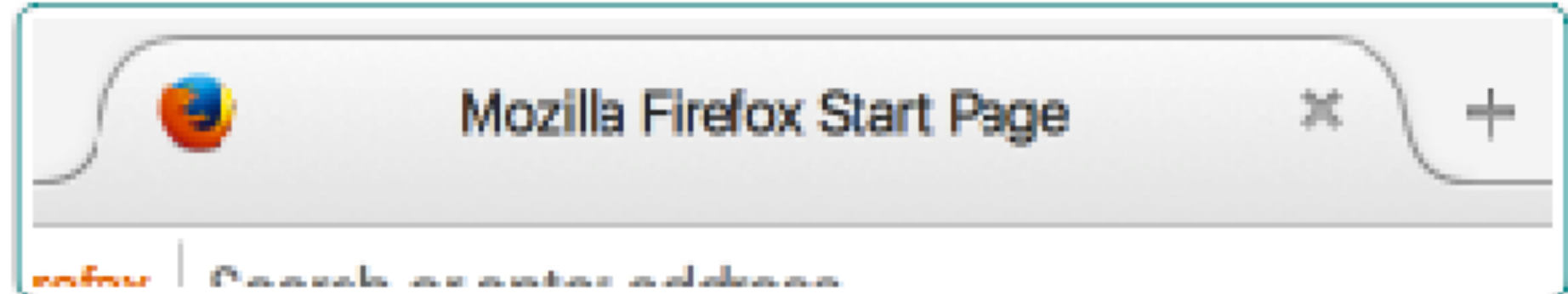





Sikuli Script

1
2
3
4
5
6
7

```
App.open("Firefox")
```

```
wait(  )
```

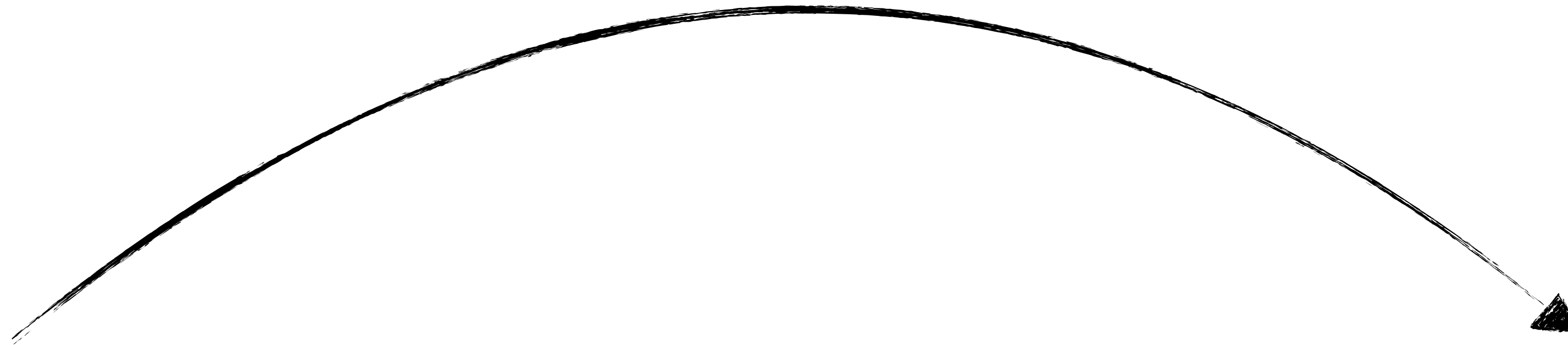
```
type(  , "images.google.com\n")
```

```
type(  , "Fluent Conf\n")
```

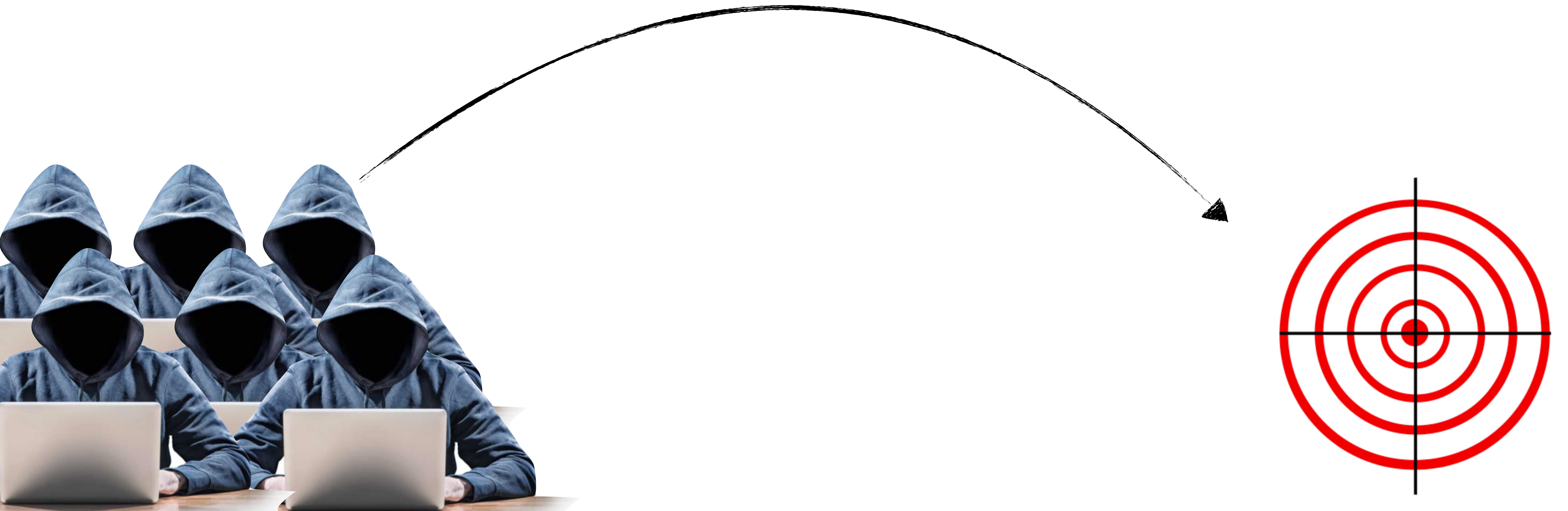
Once you detect an attacker, they are easy to block.

Right?

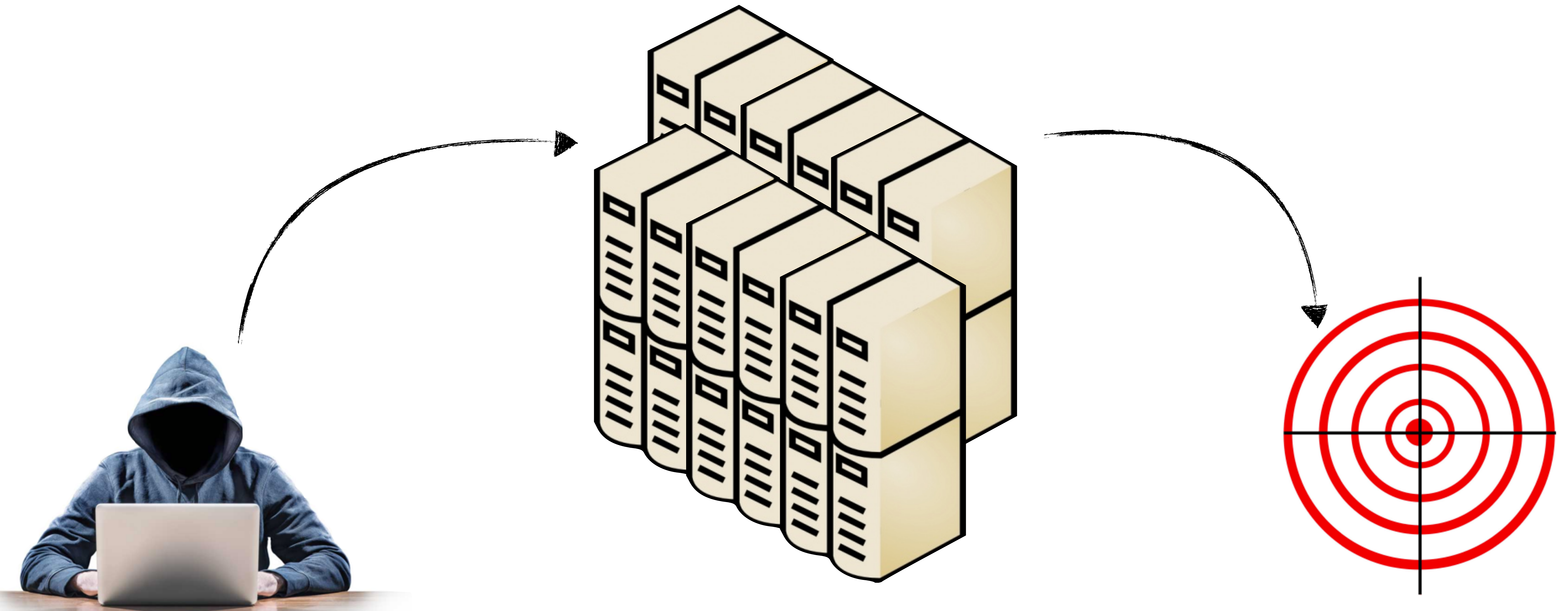
One attacker from one machine
can be blocked by IP.



Many attackers sound dangerous but aren't as common as they are made out to be.



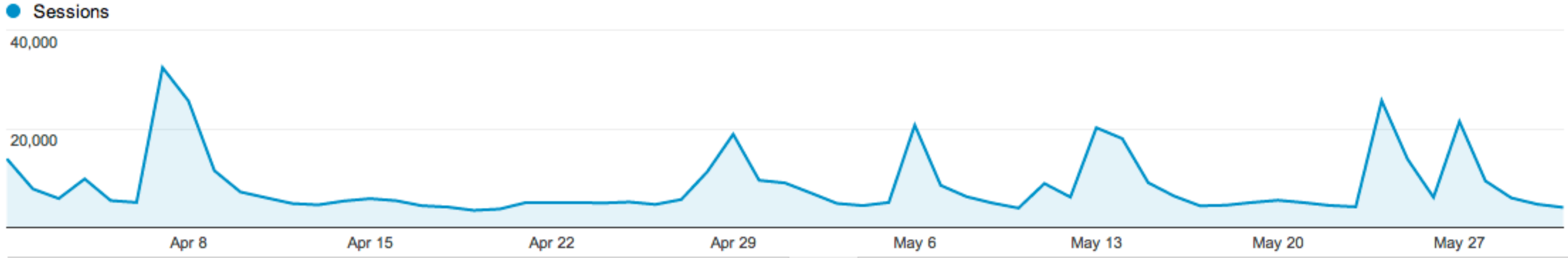
One attacker using proxies to look like thousands of users across the globe is difficult to detect and block.



Overview

Sessions vs. Select a metric

Hourly Day Week Month



Sessions

515,894



Users

358,862



Pageviews

1,083,170



Pages / Session

2.10



Avg. Session Duration

00:02:07



Bounce Rate

71.58%

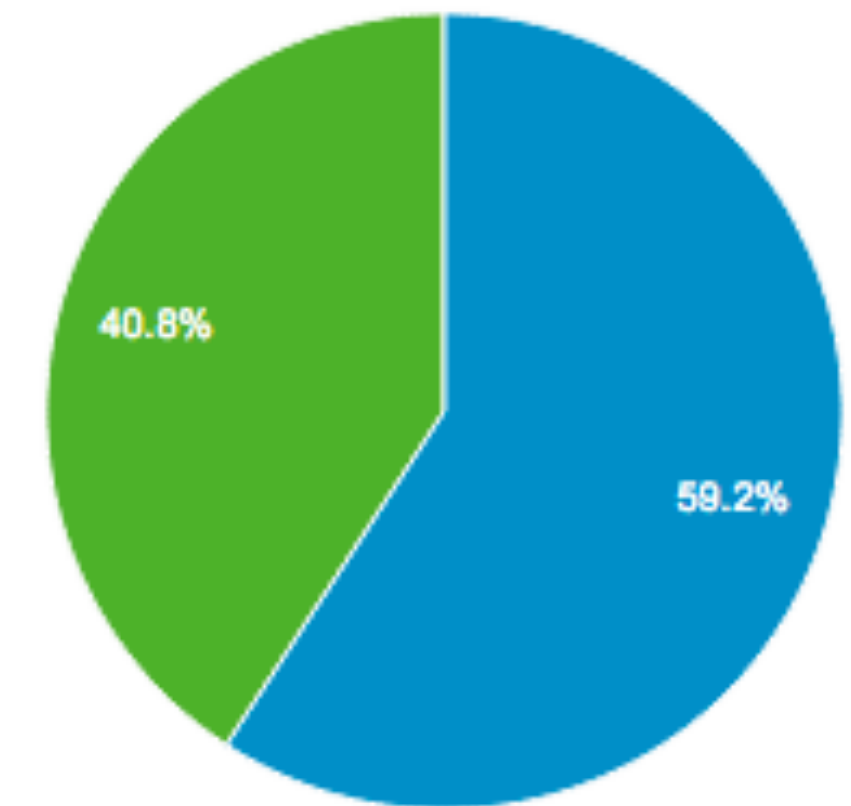


% New Sessions

59.14%



■ New Visitor ■ Returning Visitor



Spikes of traffic across many IPs are normal, except when they aren't



The devices themselves leave fingerprints

Change SKin | Reset ALL to default | System Resolution: 1024x768 | Apply

Profiles & Generator

Directories, to save with profiles and load with profiles:

Empty text input field for directories.

Configs:

Save | Load

Current profile: DEFAULT

Firefox Exactly Generator

Browser Type Rand | Version Rand | Or YOUR version:

Google Chrome | 32.0.1667.0 | Static UA

Language | Or YOUR language: | Platform: | Resolution(FF&Flash): | Or YOUR Resolution:

English | x86 | Random

OS Rand | Flash Ver Rand | FF Plugins Count Disable All Plugins

Windows NT 6.2 | 12.0.0.77 | 10

FF Flash MODE II

Stuff (This affect FF & Chrome ONLY!)

appName: | UA & appVersion: | Vendor: | Product: | appCodeName:

Netscape | Mozilla | Gecko | Mozilla

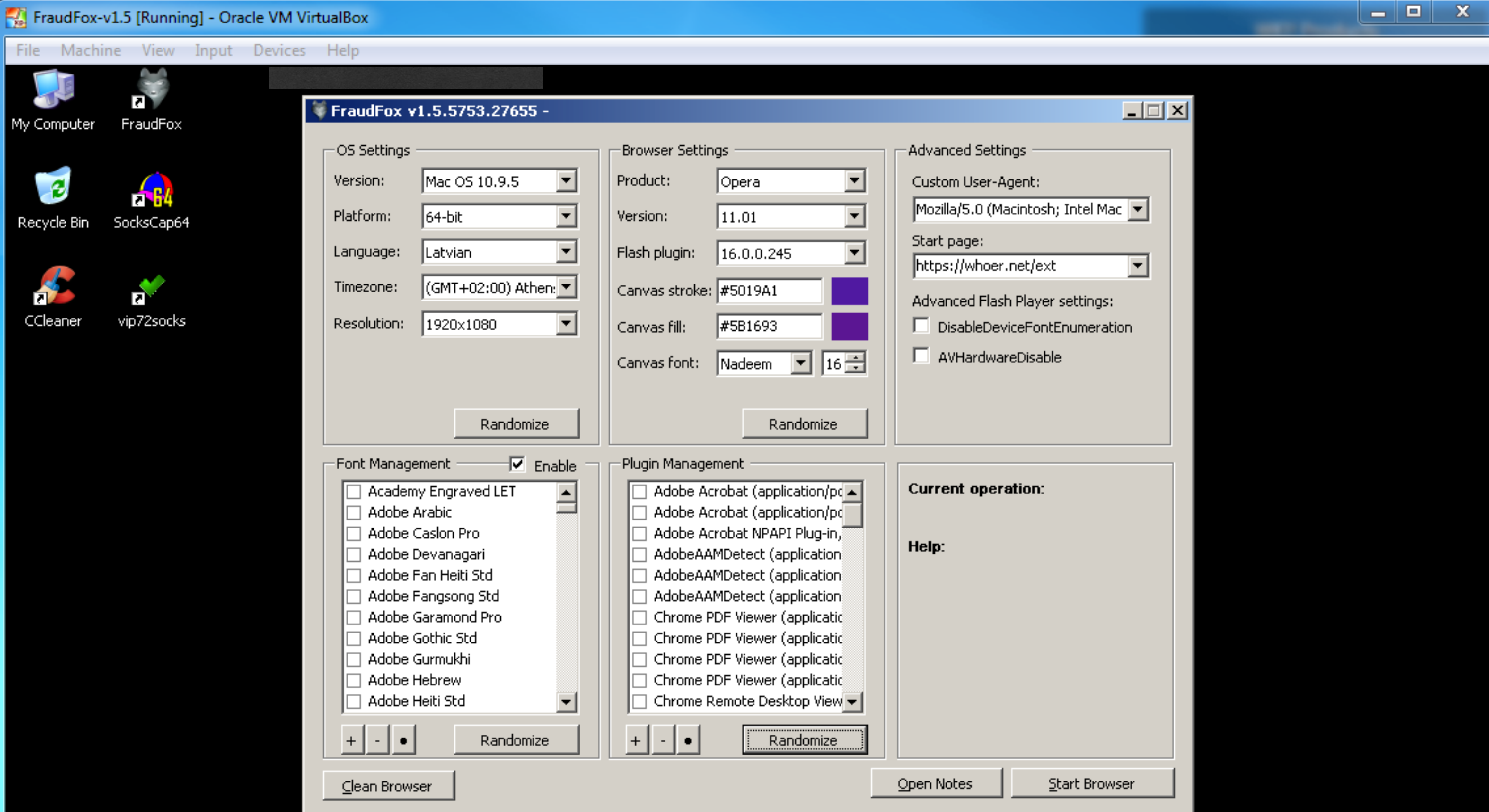
Generate

CONFIG | FLASH CONFIG | NOTES | DECODER | PHONES | SETTINGS | FONTS | PLUGINS

- Google Update | npGoogleUpdate3.dll | Google Update
- GEPlugin | npgeplugin.dll | Google Earth Plugin
- RealPlayer(tm) LiveConnect-Enabled Plug-In | nppl3260.dll | RealPlayer(tm) G2 LiveConnect-f
- RealPlayer Download Plugin | nprpplugin.dll | RealPlayer Download Plugin
- VLC media player Web Plugin 2.0.6 | npvlc.dll | VLC Web Plugin
- RealNetworks(tm) RealDownloader Chrome Background Extension Plug-In | nprndlchromebro
- RealNetworks(tm) RealDownloader PepperFlashVideoShim Plug-In | nprndlpepperflashvideosh
- RealNetworks(tm) RealDownloader HTML5VideoShim Plug-In | nprndlhtml5videoshim.dll | Real
- RealDownloader Plugin | npdlplugin.dll | RealDownloader Plugin
- iTunes Detector Plug-in | npitunes.dll | iTunes Application Detector
- McAfee MSS+ NPAPI Plugin | npMcAfeeMSS.dll | McAfee Security Scanner +
- The plugin allows you to have a better experience with Microsoft Lync | npMeetingJoinPluginC
- The plugin allows you to have a better experience with Microsoft SharePoint | NPSPWRAP.DL
- Next Generation Java Plug-in 10.21.2 for Mozilla browsers | npjp2.dll | Java(TM) Platform SE
- NPRuntime Script Plug-in Library for Java(TM) Deploy | npDeployJava1.dll | Java Deployment
- iTunes Detector Plug-in | npitunes.dll | iTunes Application Detector
- NPWLPG | NPWLPG.dll | Windows Live\u0099 Photo Gallery
- 4.0.50401.0 | npctrl.dll | Silverlight Plug-In
- The plug-in allows you to open and edit files using Microsoft Office applications | NPSPWRAP.
- Zeon PDF Plugin For Mozilla | nppdf.dll | Zeon Plus
- 5.1.20913.0 | npctrl.dll | Silverlight Plug-In
- BT DesktopHelp plug-in for Mozilla Browsers | npMotive.dll | BT DesktopHelp plug-in
- BT Management plug-in for Mozilla Browsers | npMotiveRequest.dll | BT Management plug-in
- Next Generation Java Plug-in 10.21.2 for Mozilla browsers | npjp2.dll | Java(TM) Platform SE
- NPRuntime Script Plug-in Library for Java(TM) Deploy | npdeployJava1.dll | Java Deployment
- Adobe PDF Plug-In For Firefox and Netscape 10.1.3 | nppdf32.dll | Adobe Acrobat
- Adobe PDF Plug-In For Firefox and Netscape 10.1.3 | nppdf32.dll | Adobe Acrobat

Use my plugins set when i click "Generate"

And tools are made to leave no fingerprints








Lots of tools.

Go !! Abort

Site: Switch Site: Progress: List:

Settings

-  General
-  HTTP Header
-  Proxy Settings
-  Fake Settings
-  Keywords

Site Settings

Timeout (s): Bot relaunch delay (s): Resolve Hostname

Combo Settings

 <USER>:<PASS> filter: Minimum Length: Maximum Length: Letters Digits Alphanumeric EmailForbidden Chars: Allowed Chars: Lowercase and Uppercase Letter and Digit Special Character <EMAIL> filter:

General Settings

 Save automatically valid usernames and expired combos Save automatically "To Check" combos Annoying sound on Hit -> Browse Popup Memo containing Hit debug information Minimize to Tray Float Statistics in Progression Detect "network lost" conditions while bruteforcingProgression updates:


Lists

History

Tools


Progression

About

Snap Shots Enable Snap Shots 

Load Settings from Snap Shot (*.ini)

Save Settings to Snap Shot

Images Database 

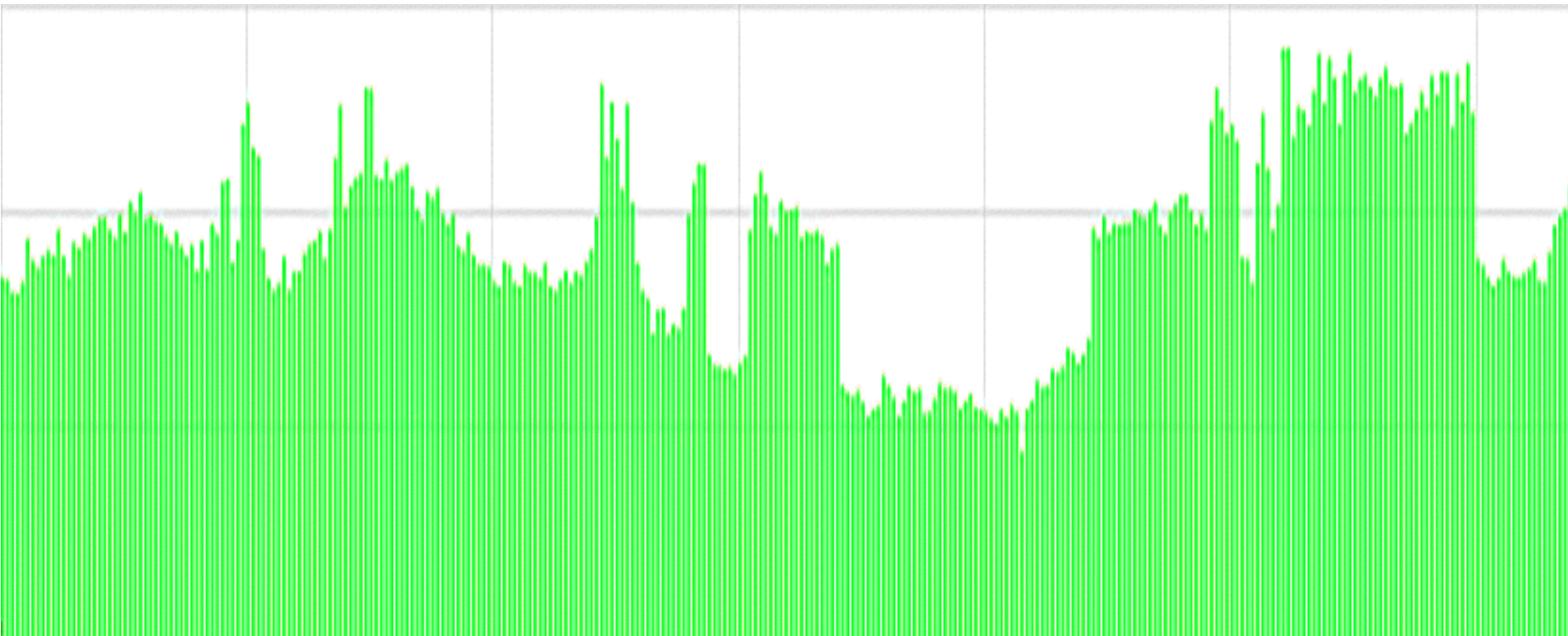
Update Images Database from Directory

Update Images Database from File

We can't patch our way through this.

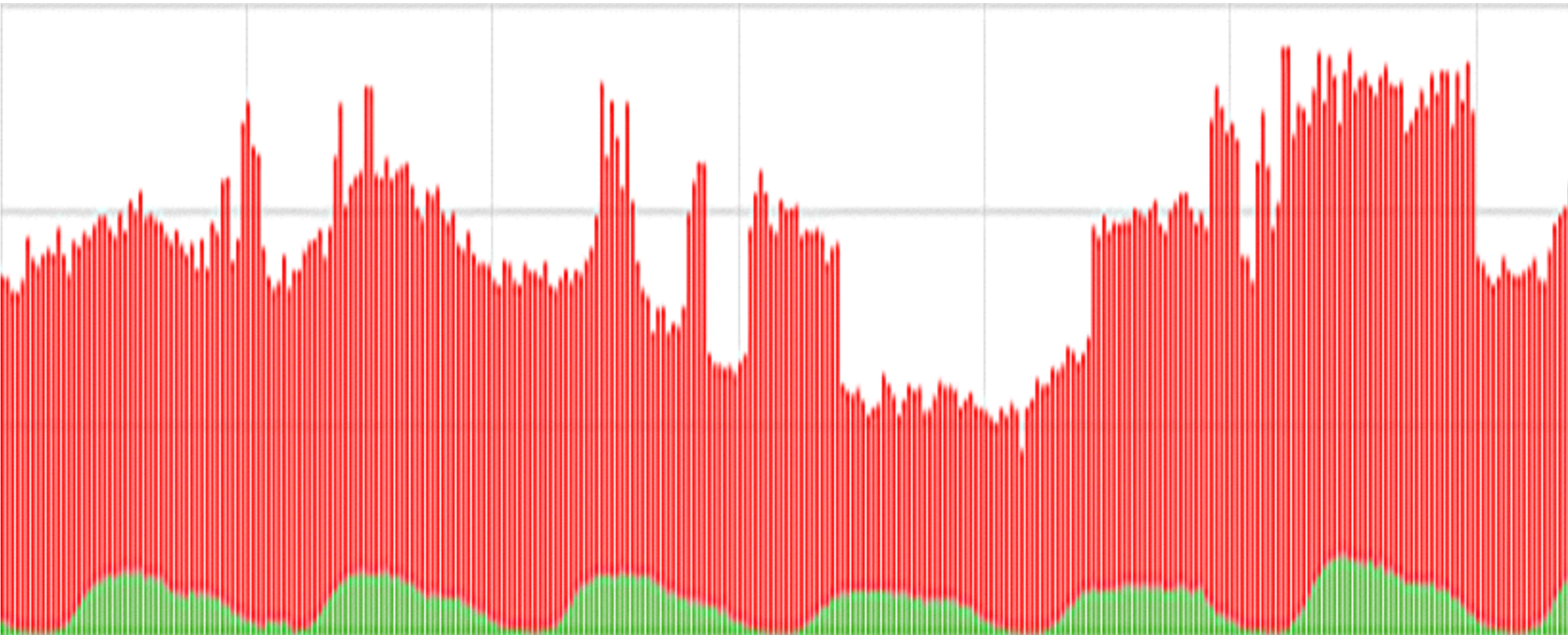
How would you react if you went from ...

■ Legitimate traffic



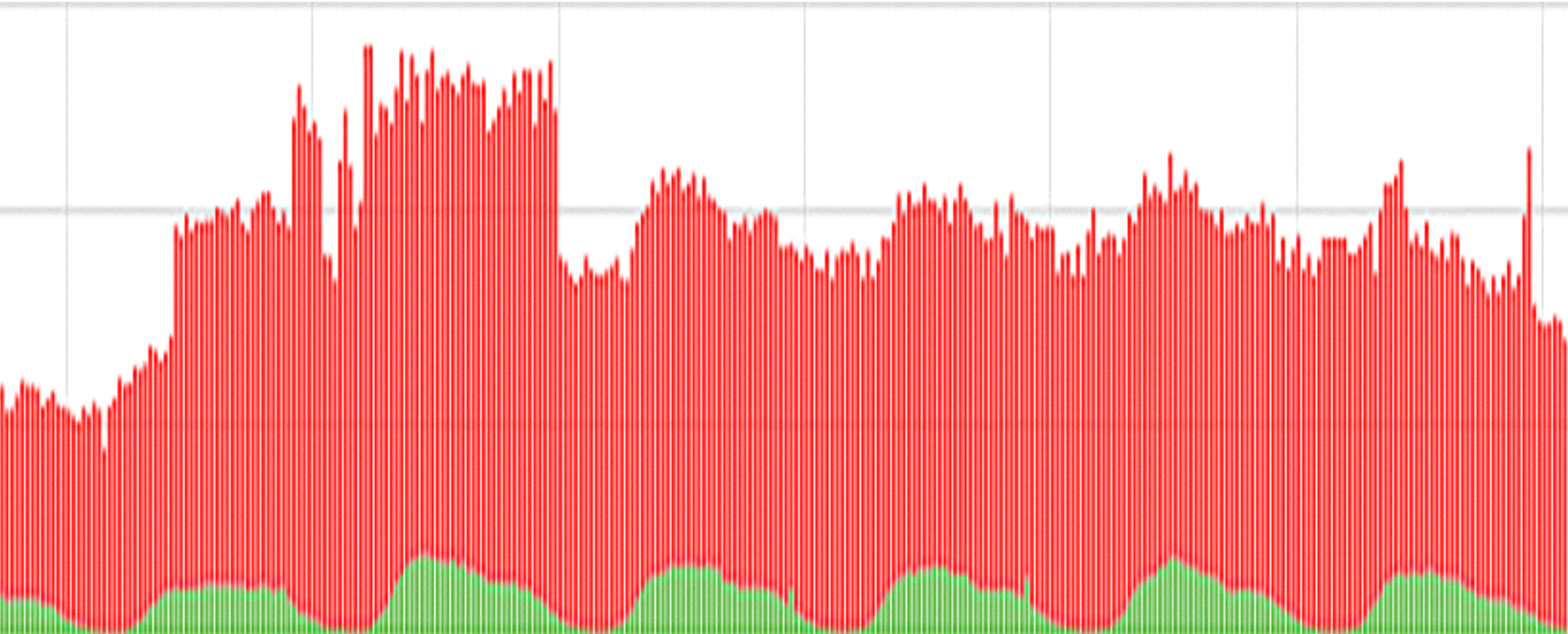
To this

- Automation detected and blocked
- Legitimate traffic



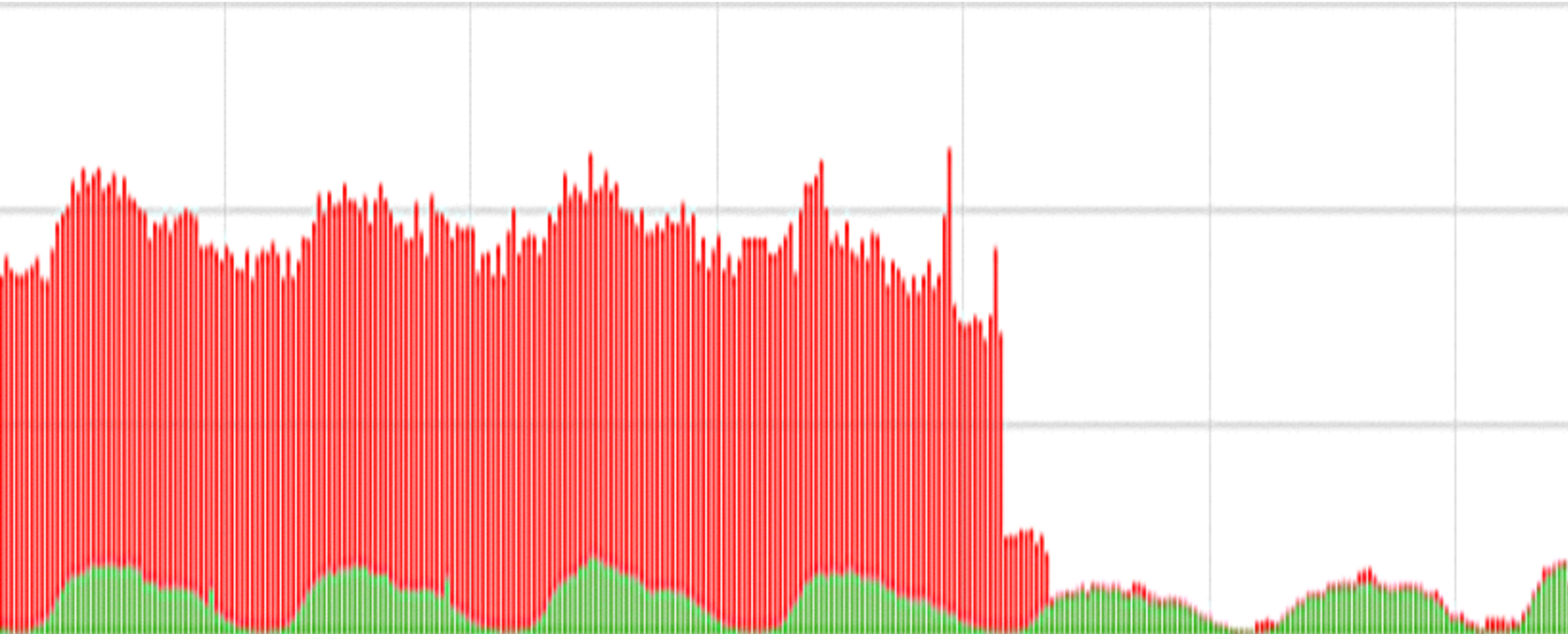
To this

- Automation detected and blocked
- Legitimate traffic



To this

- Automation detected and blocked
- Legitimate traffic



Not sure if you have a problem?

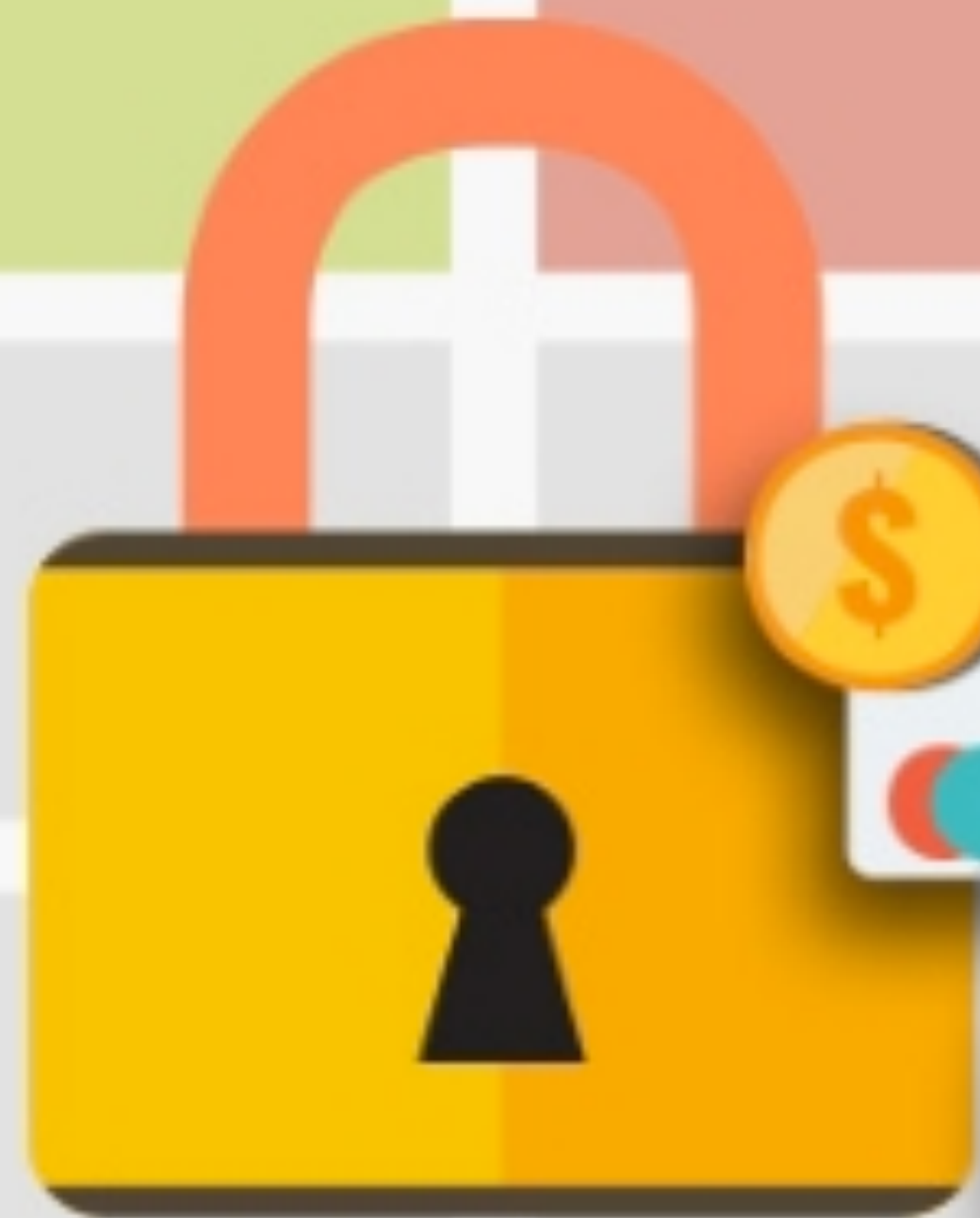
To get an idea, search for :

- <your company, service, or CMS> fullz
- <your company, service, or CMS> sentrymba
- <your company, service, or CMS> carding
- <your company, service, or CMS> <tool> tutorial

How do *you* protect *you*?

Make every password unique. Really.

Use a password manager.





LastPass, 1Password, any locally encrypted database.



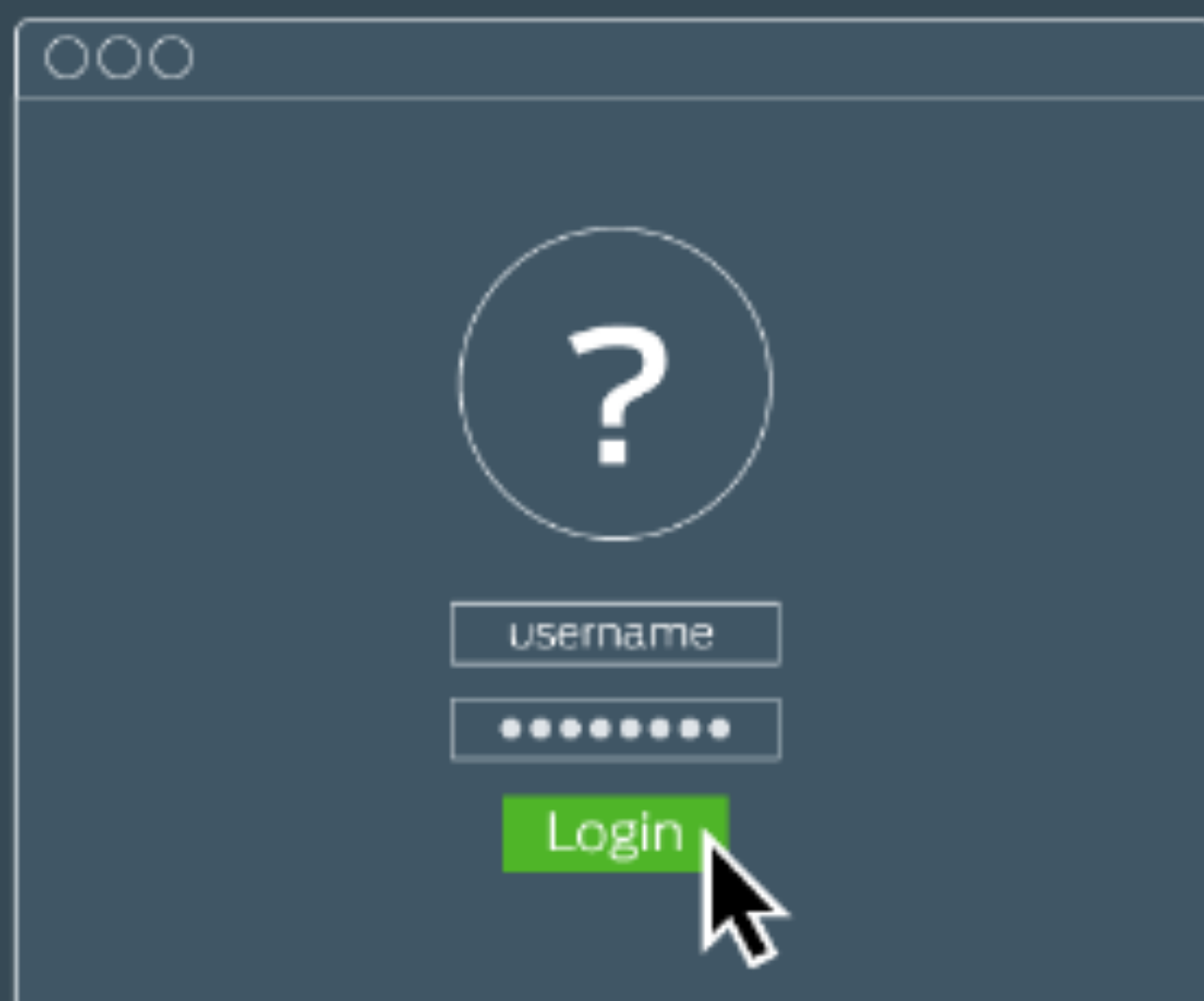
Use a password algorithm

Use a base password + a site specific string.

For example: "hyatt small blue cup"

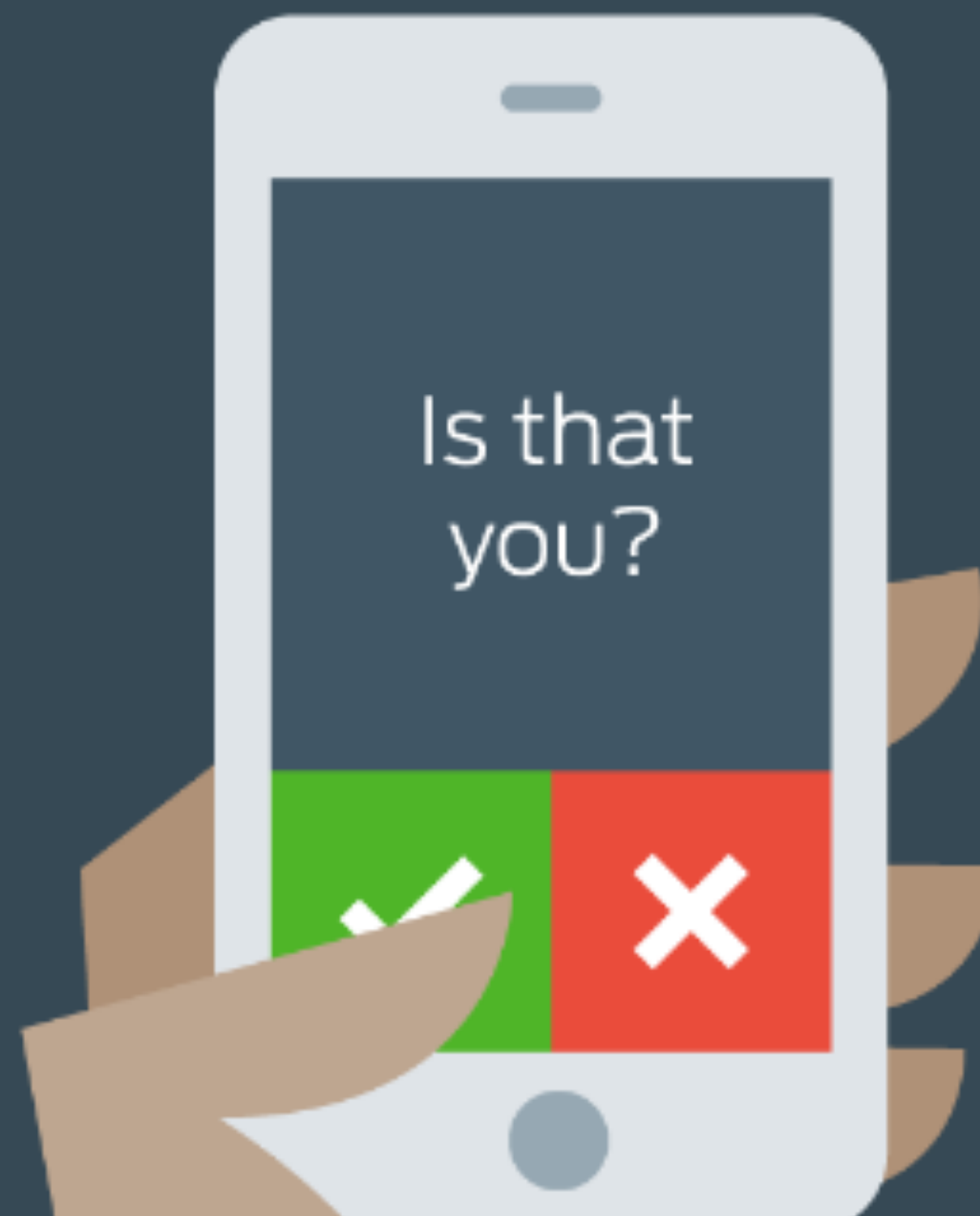
Turn on Multi-Factor Authentication.

PASSWORD



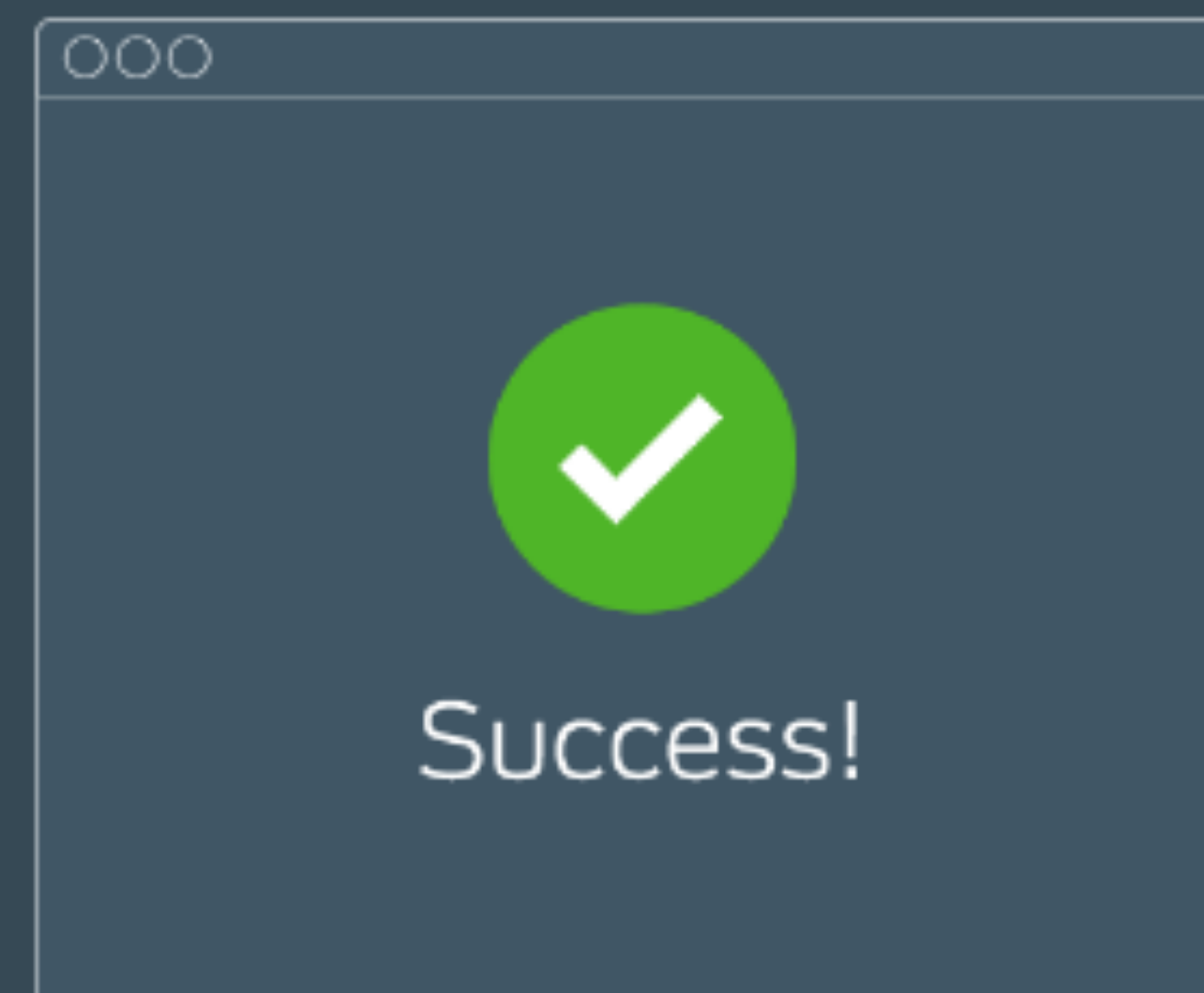
+

PROOF



=

ACCESS

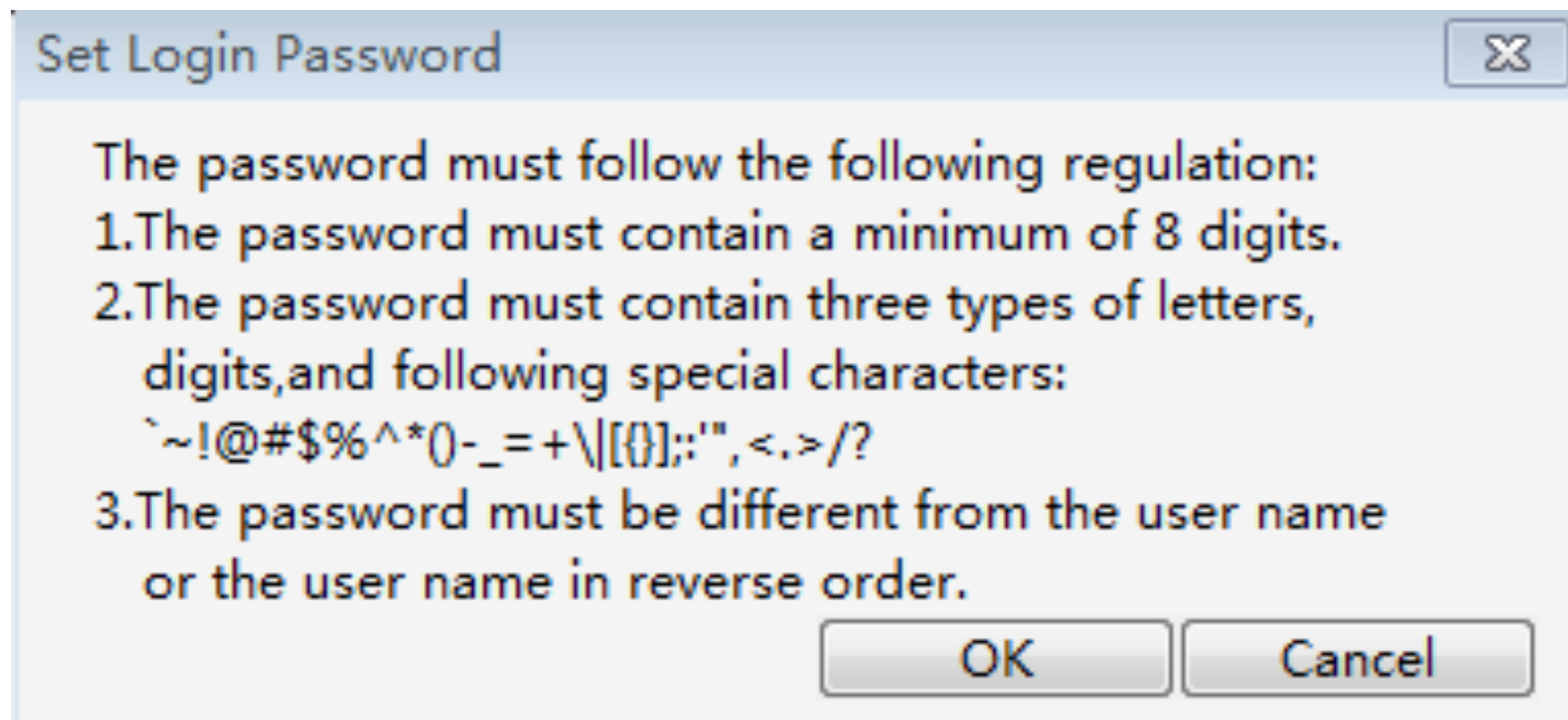


How do you protect *your users*?

First, throw away the myth that the primary risk to passwords is how crackable they are.

The biggest risk to you and your users is reused passwords.

Don't add unnecessary password rules



8 char minimum, >64 char maximum, allow ANY character (including spaces)

Do prevent users from using common passwords

- 123456
- password
- 12345678
- qwerty
- 12345
- 123456789
- football
- 1234
- 1234567
- baseball
- welcome
- 1234567890
- abc123
- 111111
- 1qaz2wsx
- dragon
- master
- monkey
- letmein
- login
- princess
- qwertyuiop
- solo
- passw0rd

Maintain and use a banned password list

Don't expire passwords unless necessary



Expire when accounts are compromised or a user's credentials are leaked.

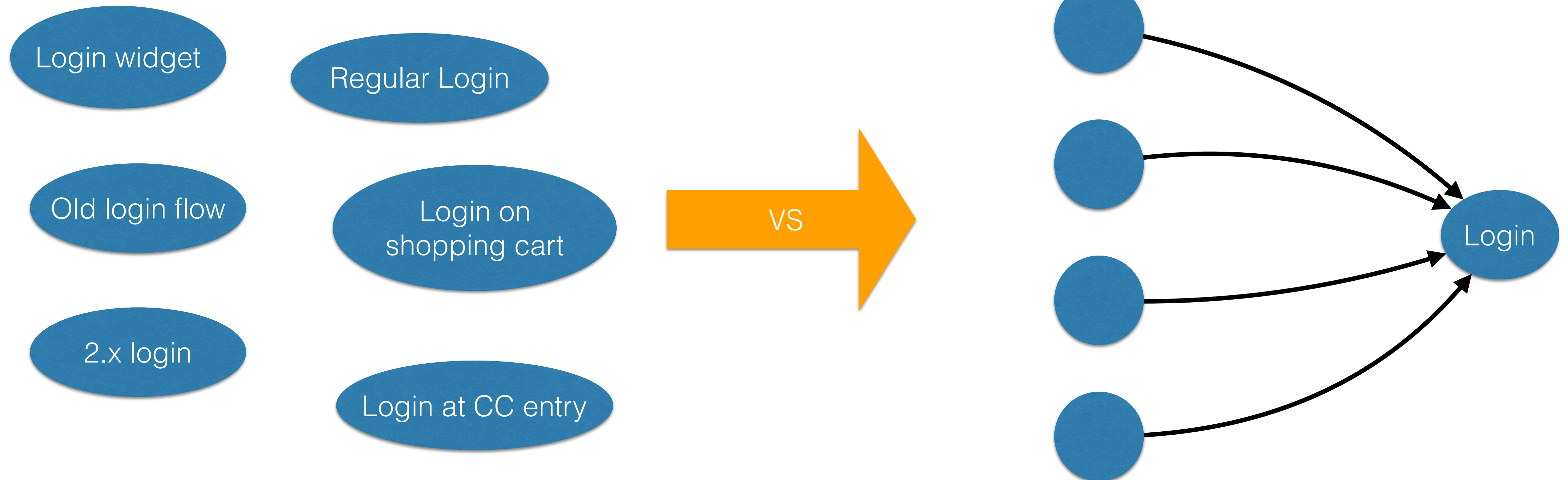
Offer Multi-Factor Authentication.



There are many options and services that make this easy and tolerable.

How do you protect *your business*?

Use single flows for important transactions.



Reduce the attack surface area as much as possible.

Ask and be ready for tough questions

Value

A hand in a dark suit sleeve, palm up, holding the word "Value" written in green, cursive-style text.

Cost

A hand in a dark suit sleeve, palm up, holding the word "Cost" written in red, cursive-style text.

You may need to re-evaluate costs & value with new parameters.

Get help. You're not alone.



**“Alone we can do
so little; together
we can do so much.”**

- Helen Keller

The Life of Breached Data & The Dark Side of Security.

Jarrold Overson
@jsoverson
QCon SF 2016