Cybersecurity Report

Q3 2018

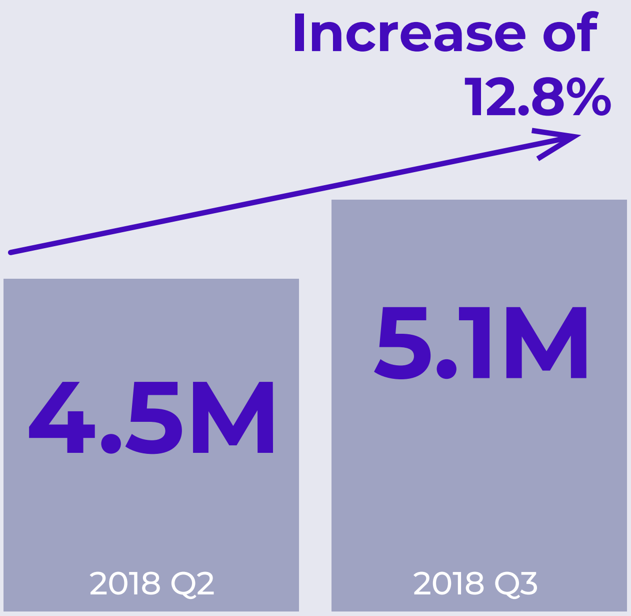
dfndr lab

CONTENTS

Q3 KEY FINDINGS

9.6M

malicious URL detections in
the last six months



38
malicious URLs
detected per minute

♂ 58.2%
of the victims were male

METHODOLOGY

dfndr lab's software relies on proprietary artificial intelligence (AI) and machine learning technologies that enable computer programs to acquire knowledge and skills in order to learn, detect, analyze and alert our security team about cyberattacks, the latest malware and viruses, online scams, or cyber crime trends.

Approximately 200 million digital files are collected daily, analyzed and indexed by dfndr lab's data processing system to keep our products current when it comes to protecting users' devices and staying steps ahead of cybercriminals.

This report contains data from cyberattack detections in Android smartphones from more than 21 million active users of our dfndr security app. The analysis is based on data collected between July 1, 2018 and September 30, 2018.

Q3 SUMMARY

Marco DeMello
CEO of PSafe
Global Head of dfndr lab

In the third quarter, dfndr lab detected and blocked over 5.1 million malicious links, an increase of 12.8% compared to 4 million detections from the previous quarter. That breaks down to 2,300 malicious links identified per hour, or 55,600 malicious link detections per day. Some key developments stand out this quarter, particularly:

- PSafe's security experts increased their ability to detect malicious URLs by setting bots to search the Internet and collate new threats automatically, resulting in faster detection rates.

- Cybercriminals took advantage of online shoppers searching for back to school deals, as well as overall summer sales. These peak buying times created opportunities to increase attacks.

Fake news was the category with the highest increase of detections **(312.6%)**, compared to Q2.

The rise in unverified news stories may be related to the midterm elections this year, or also a general upward trend in fake news. One highlight this quarter was uncovering a story that spoofed the popular shopping site, Amazon. The fake article promised a 'work at home opportunity with Amazon'. The hackers used a segmentation strategy with the headline, by adding a user's city name, which changed depending on the IP location detected. This personalization fooled individuals into believing the opportunity was locally based and the temptation of working remotely was another draw. Over 1 million detections of this scam were blocked by our proprietary software.

The second highest category of detections in Q3 were fake promotions or giveaways, with an increase of 205.1% from last quarter. One scam was significant in increasing detections. A phony offer to obtain a $100 Visa gift card spread to 377,926 people, with the intent to steal personal data.

Fraudulent advertisements remain the most detected category but decreased 6.2%, compared to Q2. The drop in detections could be attributed to Google changing their policies on fraudulent ads and implementing stronger tools to combat this pervasive issue.

MALICIOUS URL DETECTIONS

Q3 2018
5,120,380

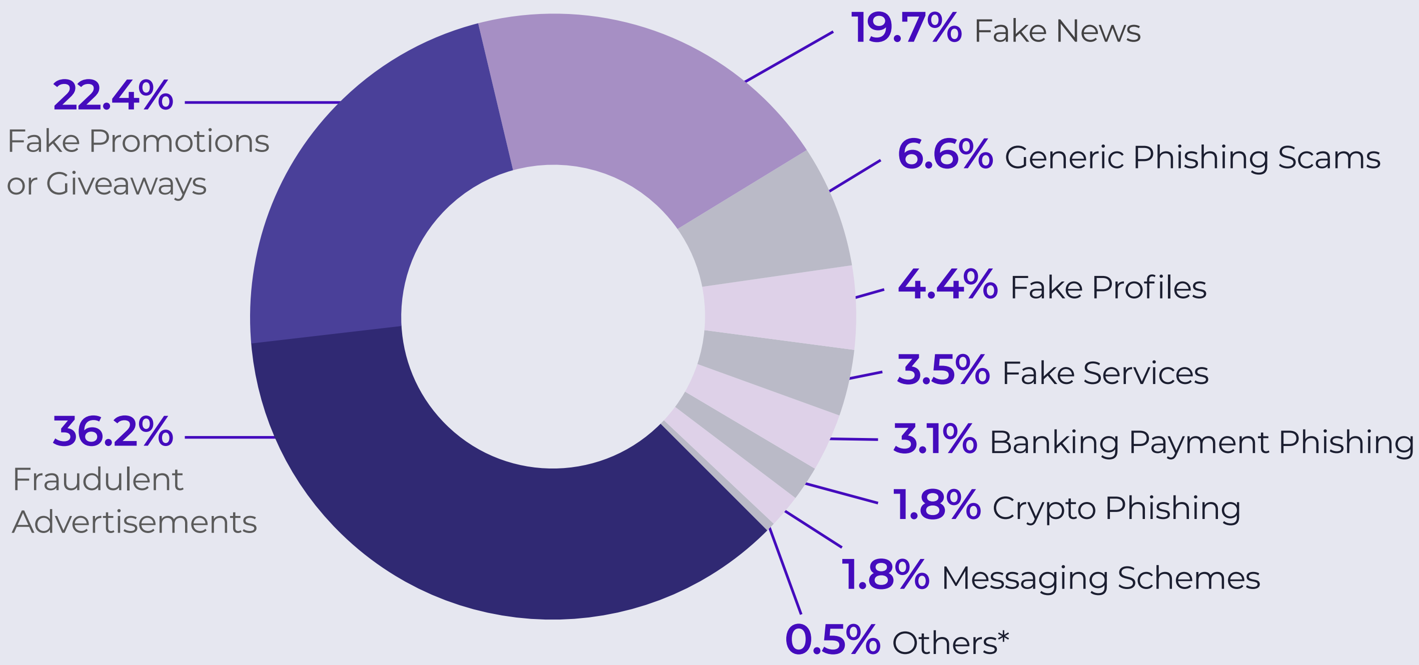
Q2 2018
4,537,976

12.8% increase

JULY	AUGUST	SEPTEMBER
2,517,744	**1,427,987**	**1,174,649**

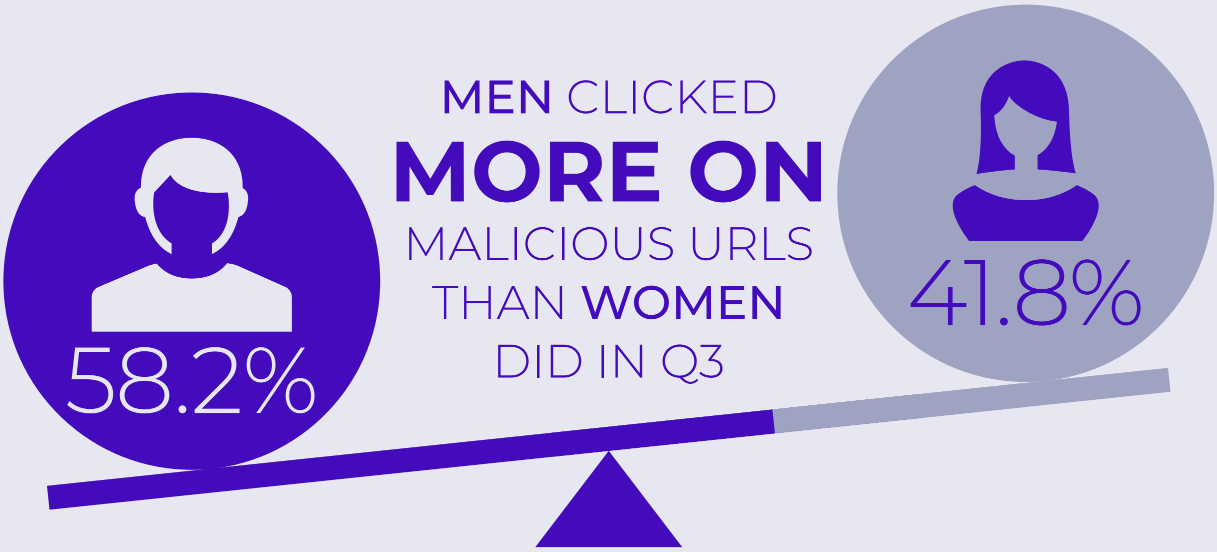
55.6K /DAY **2.3K**/HOUR **38**/MINUTE

Categories of Malicious URLs Detected



*Social Media Phishing, Malware Downloads, Generic Malicious Links, Paid Mobile Service.

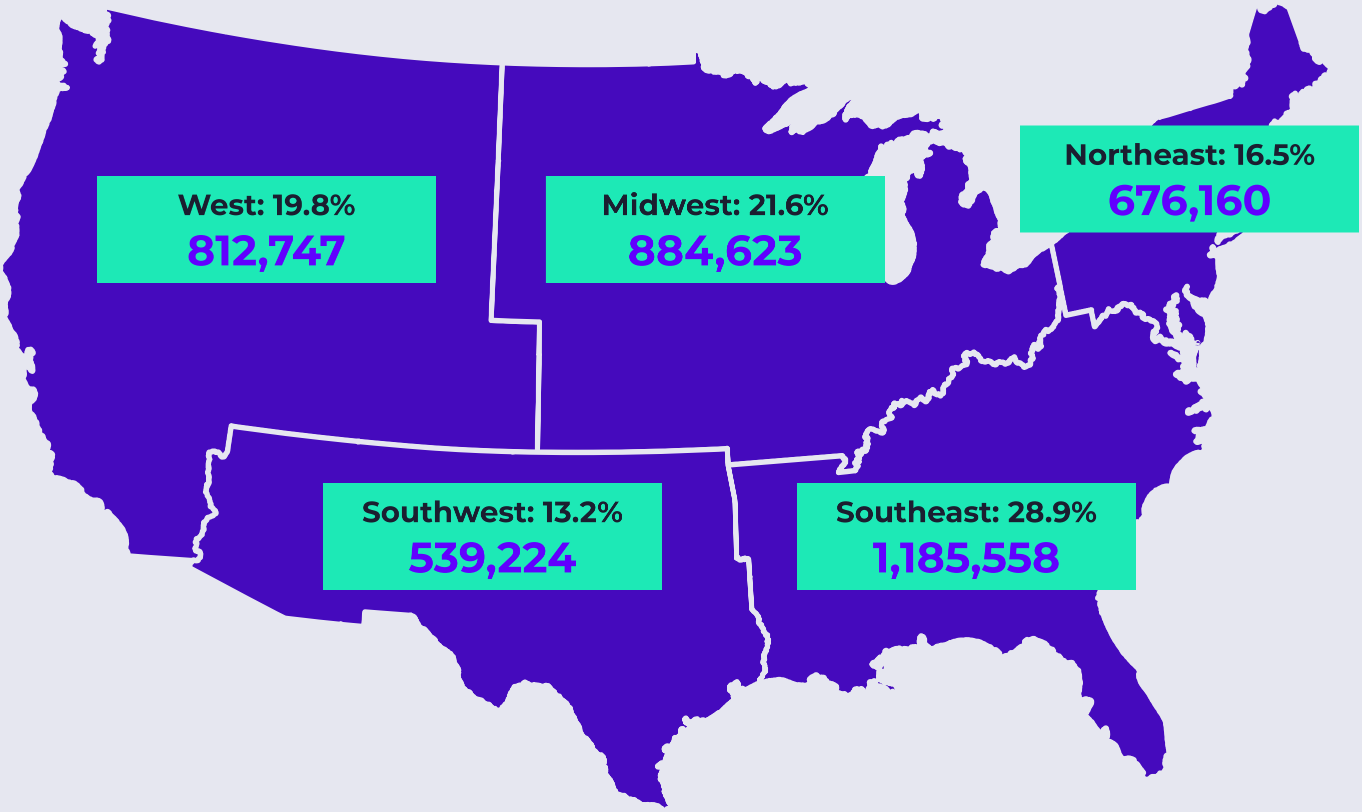
DETECTIONS BY GENDER



MEN CLICKED
MORE ON
MALICIOUS URLS
THAN **WOMEN**
DID IN Q3

DETECTIONS BY REGION

In Q3, the Southeastern region experienced the highest detections at 1.1 million detections, a slight increase from last quarter. The top 5 states with the most detections were California at 490,411, Texas at 395,292, Florida at 357,788, Illinois at 268,822, and New York at 209,681.



DETECTIONS BY STATE

Northeast	
Connecticut	36,520
Delaware	11,944
Maine	5,217
Maryland	67,484
Massachusetts	73,598
New Hampshire	5,219
New Jersey	113,104
New York	209,681
Pennsylvania	146,412
Rhode Island	6,981

Midwest	
Illinois	268,822
Indiana	39,899
Iowa	22,505
Kansas	15,006
Michigan	203,323
Minnesota	65,567
Missouri	45,617
Nebraska	20,271
North Dakota	2,986
Ohio	152,885
South Dakota	3,920
Wisconsin	43,822

West	
Alaska	2,722
California	490,411
Colorado	70,827
District of Columbia	37,164
Hawaii	15,129
Idaho	10,625
Montana	5,925
Nevada	45,565
Oregon	27,750

10% of the detections don't have a region identified

DETECTIONS BY STATE

West	
Utah	29,284
Washington	74,864
Wyoming	2,481

Southwest	
Arizona	76,054
New Mexico	21,044
Oklahoma	46,834
Texas	395,292

Southeast	
Alabama	59,260
Arkansas	20,406
Florida	357,788
Georgia	209,674
Kentucky	27,067
Louisiana	35,080
Mississippi	32,364
North Carolina	149,839
South Carolina	61,841
Tennessee	109,165
Virginia	112,887
West Virginia	10,187

10% of the detections don't have a region identified

TOP 3 CATEGORIES OF MALICIOUS URLS

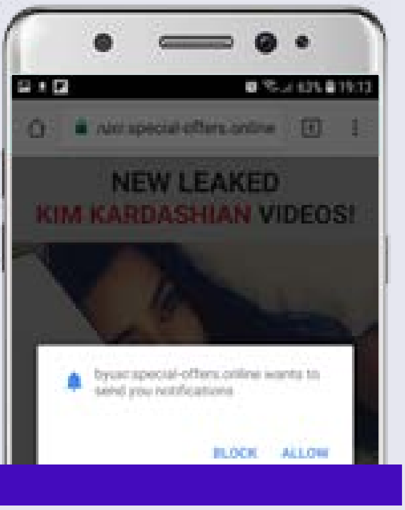
1 FRAUDULENT ADVERTISEMENTS

Pop-up ads with clickbait copy that trick consumers into granting permissions to access deceptive content or to receive false notifications, with the payload being malware or spam bots delivering more malicious ads.

2,060,965 detections in Q2 2018

1,932,445 detections in Q3 2018

Decrease of **-6.2%**

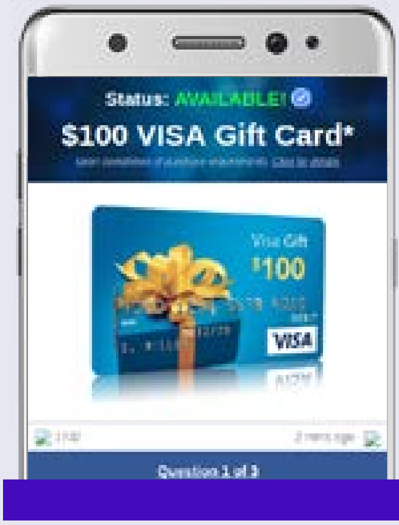


NEW LEAKED
KIM KARDASHIAN VIDEOS!

byuac.special-offers.online wants to send you notifications

2 FAKE PROMOTIONS OR GIVEAWAYS

Illegitimate contests and sweepstakes that trick users into entering in the hopes of winning valuable prizes such as electronics, vacation packages, and other high-end items.



Status: AVAILABLE!
$100 VISA Gift Card*

Question 1 of 3

391,907 in Q2 2018

1,195,760 in Q3 2018

Increase of **+205.1%**

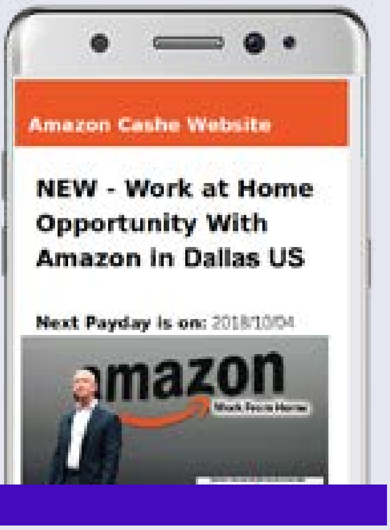
3 FAKE NEWS

A form of yellow journalism that consists of deliberate disinformation or hoaxes that is spread online with the intent of misleading the user to gain either financially, socially, or politically.

254,983 in Q2 2018

1,052,072 in Q3 2018

Increase of **+312.6%**



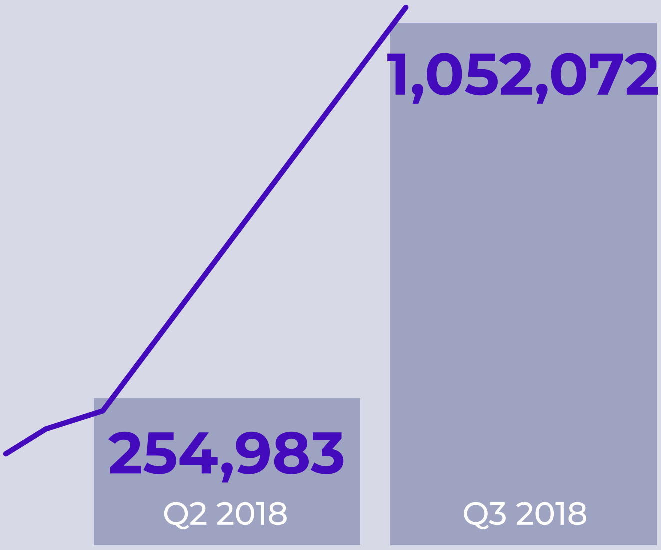
Amazon Cashe Website

NEW - Work at Home Opportunity With Amazon in Dallas US

Next Payday is on: 2018/10/04

FAKE NEWS IN Q3

INCREASED 312.6% between Q2 and Q3



In Q3, fake news detections increased significantly, likely due to the midterm elections this year and the spread of biased articles, along with higher concentrations of where fake news is discovered and shared.

Top 3 fake news sources:

SMS

Browser

Facebook

11.4K/DAY

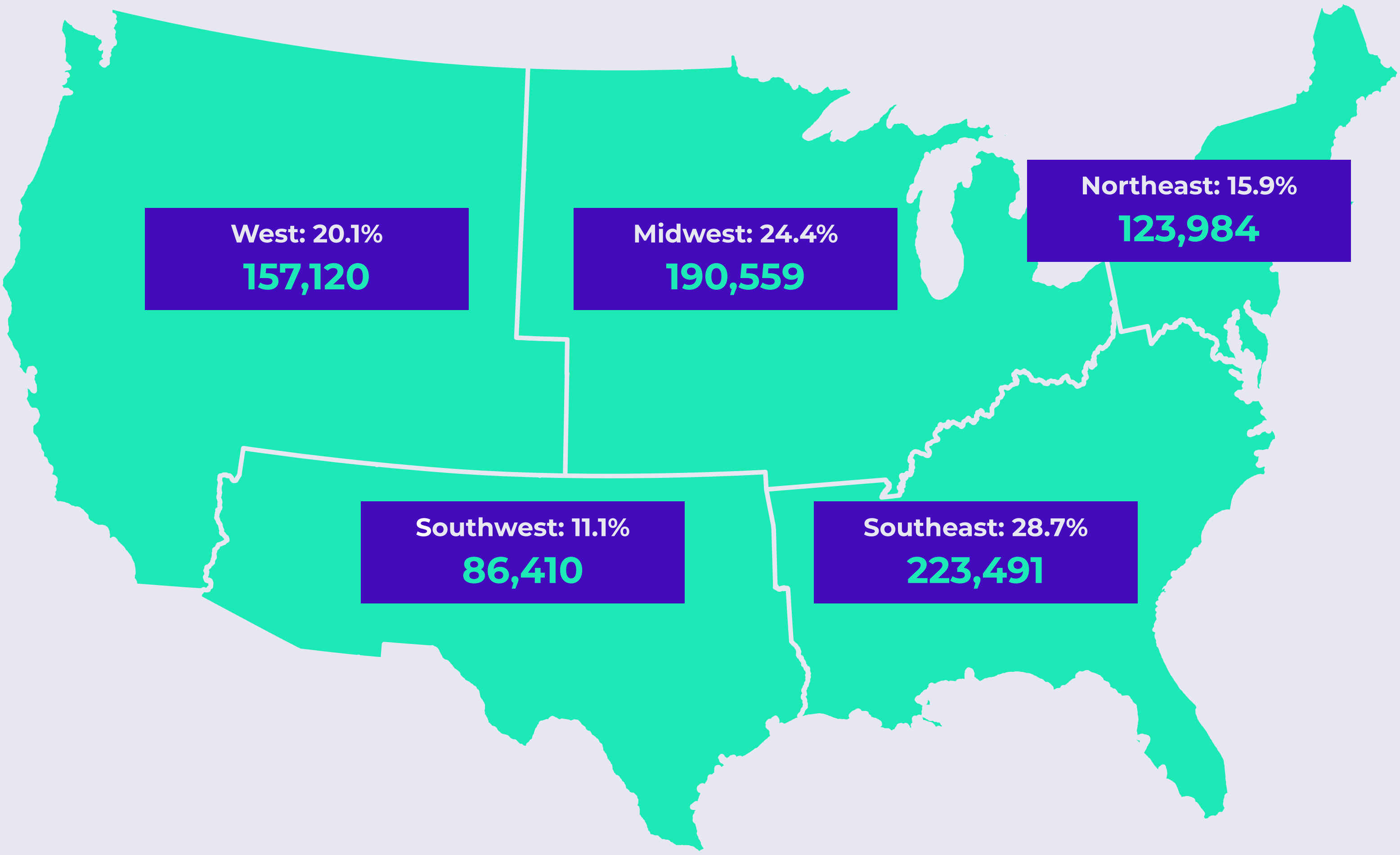
476/HOUR

HOW dfndr LAB DETECTS FAKE NEWS

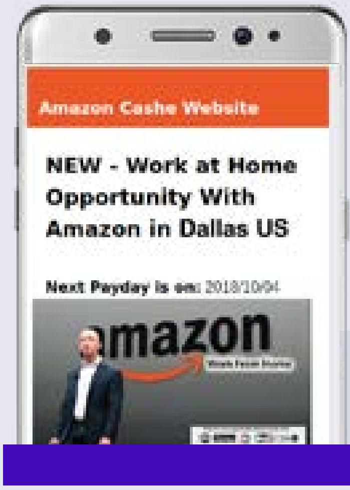
The dfndr lab team uses intelligent software to scour the Internet for potentially harmful stories. Our security experts then analyze all flagged content for legitimacy, updating our database daily to promptly alert the public of new threats.

Users are encouraged to assist our security team with these efforts by submitting suspicious content for analysis by visiting dfndrlab.com and pasting a suspicious link into the URL checker tool. This tool not only identifies dangerous links for users, but also supports our quest to uncover fake news sites.

FAKE NEWS DETECTIONS BY REGION



TOP 5 FAKE NEWS


Amazon Cashe Website

NEW - Work at Home Opportunity With Amazon in Dallas US

Next Payday is on: 2018/10/04

1

NEW - WORK AT HOME OPPORTUNITY WITH AMAZON

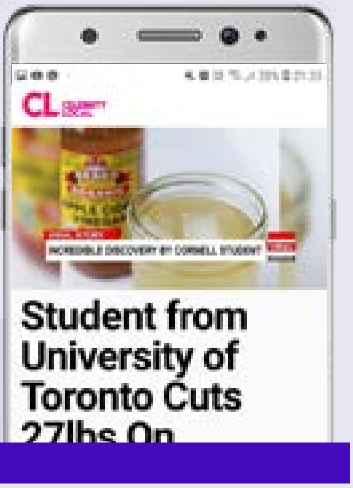
An article spoofing popular online retailer, Amazon, that promises a locally based 'work at home' opportunity.

1,021,136 DETECTIONS

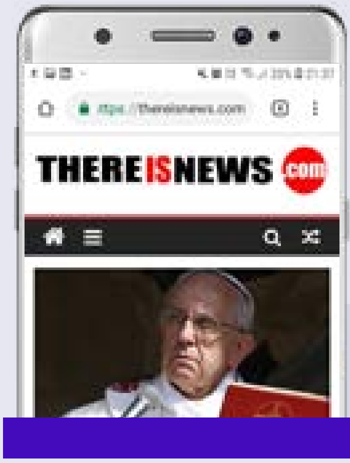
2

STUDENT FROM UNIVERSITY OF TORONTO CUTS 27LBS ON UNIVERSITY BUDGET

An article masked as an advertisement for a purported weight loss product.


Student from University of Toronto Cuts 27lbs On

22,636 DETECTIONS


https://thereisnews.com

3

POPE FRANCIS CANCELS THE BIBLE AND PROPOSES TO CREATE A NEW BOOK A SATIRICAL ARTICLE ABOUT THE POPE.

A satirical article about the Pope.

567 DETECTIONS

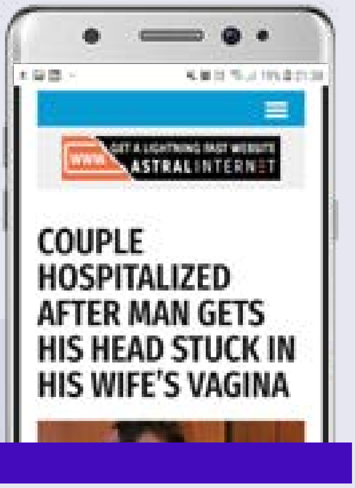
TOP 5 FAKE NEWS

4

COUPLE HOSPITALIZED AFTER MAN GETS HIS HEAD STUCK IN HIS WIFE'S VAGINA

An article consisting of outrageous and unsubstantiated claims.

257 DETECTIONS



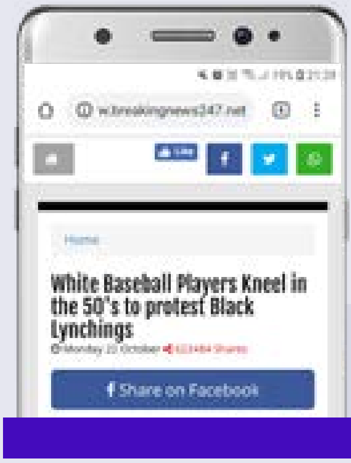
COUPLE HOSPITALIZED AFTER MAN GETS HIS HEAD STUCK IN HIS WIFE'S VAGINA

5

WHITE BASEBALL PLAYERS KNEEL IN THE 50'S TO PROTEST BLACK LYNCHINGS

A fake photo posted on a satirical website.

185 DETECTIONS

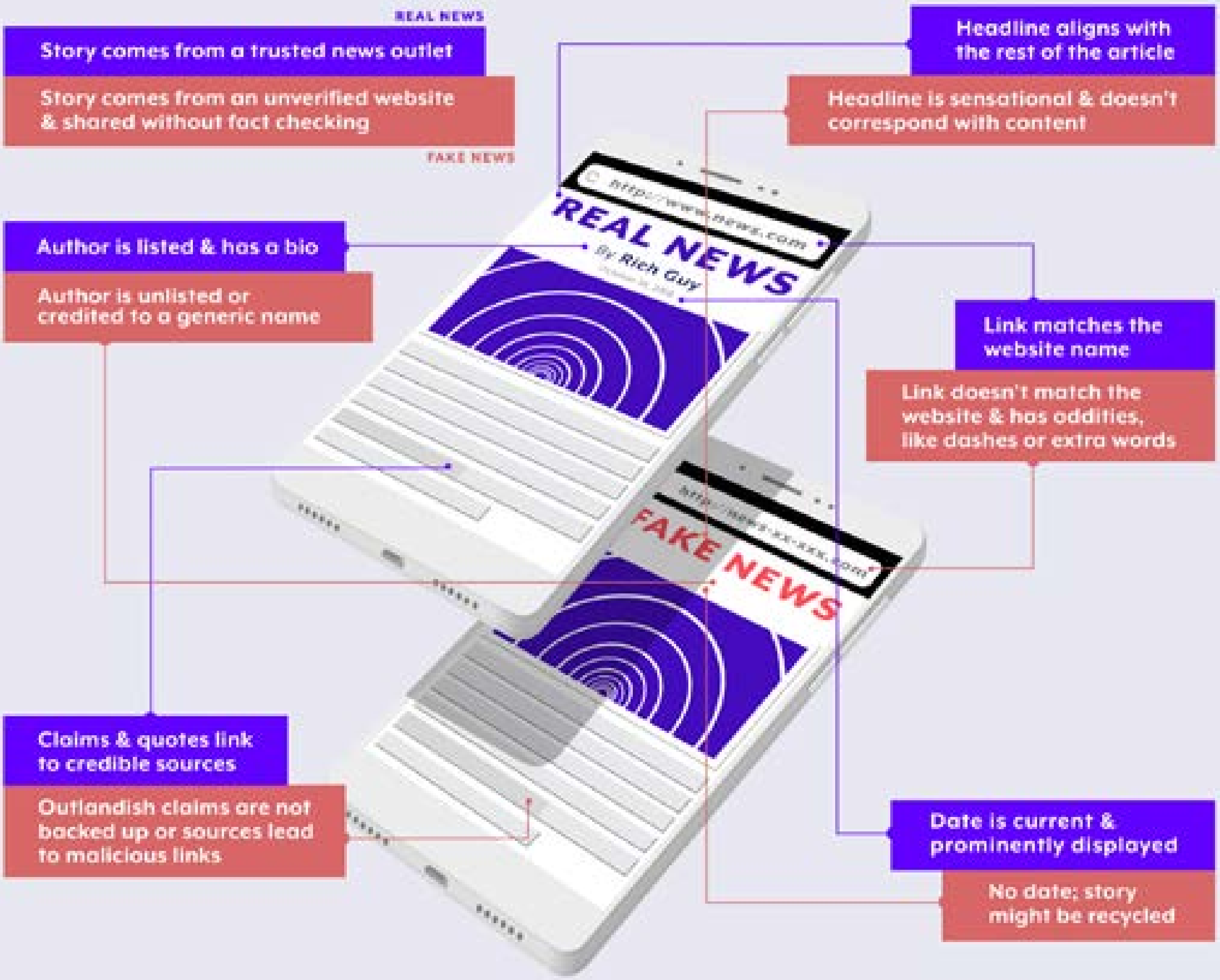


White Baseball Players Kneel in the 50's to protest Black Lynchings

Monday 22 October 122484 Shares

TIPS TO IDENTIFY FAKE NEWS

dfndr lab compiled tips to help you identify the difference between fake and real news.



REAL NEWS

Story comes from a trusted news outlet

Story comes from an unverified website & shared without fact checking

FAKE NEWS

Headline aligns with the rest of the article

Headline is sensational & doesn't correspond with content

Author is listed & has a bio

Author is unlisted or credited to a generic name

Link matches the website name

Link doesn't match the website & has oddities, like dashes or extra words

Claims & quotes link to credible sources

Outlandish claims are not backed up or sources lead to malicious links

Date is current & prominently displayed

No date; story might be recycled

FAKE NEWS FINDINGS

dfndr lab conducted a survey on fake news.

Top age group:

45-54
years of age

Top gender group:

55.3%
males

43.5%
females

47.9%

seek articles on major news websites.

Top 3 news sources:

61.9%	ABC, NBC, CBS
48.2%	Fox News
35.3%	CNN

46.8%

use social media to find news articles over

44.3%

who say 'no'.

most used social platform to find news at

75.6%

FAKE NEWS FINDINGS

52.9%
have encountered a fake news story

25.9%
have NOT encountered a fake news story

82%
WOULD NOT TRUST THE CONTENT OF A FAKE NEWS STORY

YET **38.7%**
MIGHT STILL READ A STORY IF IT WERE FLAGGED AS FAKE NEWS

Who should be responsible for identifying and flagging fake news?

44.7%
Social media platforms

43.9%
An independent body, like a trusted security company

35.5%
The public

54.3% OF PEOPLE THINK IT'S MORE DANGEROUS TO EXPOSE PASSWORDS TO IMPORTANT ACCOUNTS THAN TO ENCOUNTER FAKE NEWS (**24.5%**) FILLED WITH MALICIOUS LINKS.

GLOSSARY

Cyberattack
Any illegal activity carried out on the Internet, or by means of an electronic device. Such activities include fraud, identity theft, phishing, etc.

Paid Mobile Service
Sites that automatically register or coerce individuals to register for a paid SMS service.

Hacker
Also known as 'black hat hacker', is an individual that breaches defenses or exploits vulnerabilities in devices, software, or networks out of maliciousness or personal gain.

Malicious Link
Links created for malicious purposes, such as phishing scams, downloading malware to devices, or gaining control of devices.

Malware
Software that contains malicious code, such as viruses, trojans or worm.

Fake News
A form of yellow journalism that consists of deliberate disinformation or hoaxes that is spread online with the intent of misleading the user to gain either financially, socially, or politically.

Phishing
A cyber crime which targets by email, phone, or SMS, by posing as a legitimate service or institution to lure victims into providing sensitive data such as passwords, mobile numbers, and Social Security Numbers.

Banking Payment Phishing
A cyber crime that spoofs banking institutions webpages with the intent to access banking credentials like tokens, passwords, account numbers, credit card details, etc.

Crypto Phishing
Fraudulent trading sites for cryptomoedas.

Fake Promotions or Giveaways
Illegitimate contests and sweepstakes that compel individuals to enter to win valuable prizes such as electronics, vacation packages, and other high-end items. Once an individual enters, he or she may be required to download an app, provide personal data, or register for a paid service.

Fake Profiles
Fraudulent social profiles that redirect individuals to phishing links, with the intent to steal sensitive data.

Social Media Phishing
When attackers use social networking sites like Facebook, Twitter and Instagram to obtain personal information or get clicks on malicious links.

Fake Services
Fraudulent service(s) that requires an individual to share sensitive data, install a fake application, or register for a paid service that doesn't exist.

Messaging Schemes
Type of social engineering attack that uses humans to spread a phishing link in messaging apps like WhatsApp or Facebook Messenger.

Fraudulent Advertisements
Web pages or pop-ups that mislead individuals. For example, stating that the mobile phone has a virus and prompting a user to sign up for services or install applications.

Malware Download
A deceptive link created to induce an individual to unknowingly install malware that damages or takes over a device, or accesses personal data.

ABOUT US

dfndr lab

dfndr lab is the research facility of PSafe Technology. It is made up of a global team of security experts and uses artificial intelligence, proprietary technology and community collaboration to uncover cyberattacks and scams. Our mission is to protect consumers from highly sophisticated cybercriminals and give everyone the freedom and peace of mind to safely connect, share, express and explore.

PSafe

PSafe Technology is a leading provider of mobile security, privacy, and performance optimization apps. The company is dedicated to delivering innovative products that protect consumers' freedom to safely connect, share, play, express, and explore online. The flagship antivirus and anti-hacking app, dfndr security, with 150+ million installs globally, has been named as a top-rated antivirus software by AV-TEST Institute — the world leader in security and antivirus research. The company's application portfolio continues to grow and now includes a cleaning and boosting app—dfndr performance, a virtual private network app—dfndr vpn, a private storage app—dfndr vault, and a battery performance app—dfndr battery. PSafe is funded by Redpoint Ventures, e.ventures, RPeV, Pinnacle Ventures and Index Ventures. The company is headquartered in San Francisco, CA with satellite offices in Brazil.

Global Headquarters
45 Belden Place, 3rd Floor, San Francisco, CA 94104
Tel: 415-530-5900
www.psafe.com

dfndr lab