Cybersecurity Report

Q1 2018

dfndr lab

Contents

Methodology.....4
Q1 Summary.....5
Malicious URL Detections in the US.....6
Most Common Categories of Malicious URLs Detected.....6
Top 3 Scams Detected.....7
Detections by Gender in the US.....9
Detections by Region.....10
How dfndr lab Detects Fake News.....11
Fake News Detections in the US.....12
Fake News Detections by Gender.....13
Fake News Detections by Region.....13
Tips to Identify Fake News.....14
Looking Ahead.....16
About Us.....17

Q1 Key Conclusions

+3 million

online scams detected

Men were
twice as likely to click
on malicious URLs than women

On average, Americans accessed
23 suspected malicious URLs per minute

Fake news detection increased by 19.6%

15.7K
in Q4 2017

→

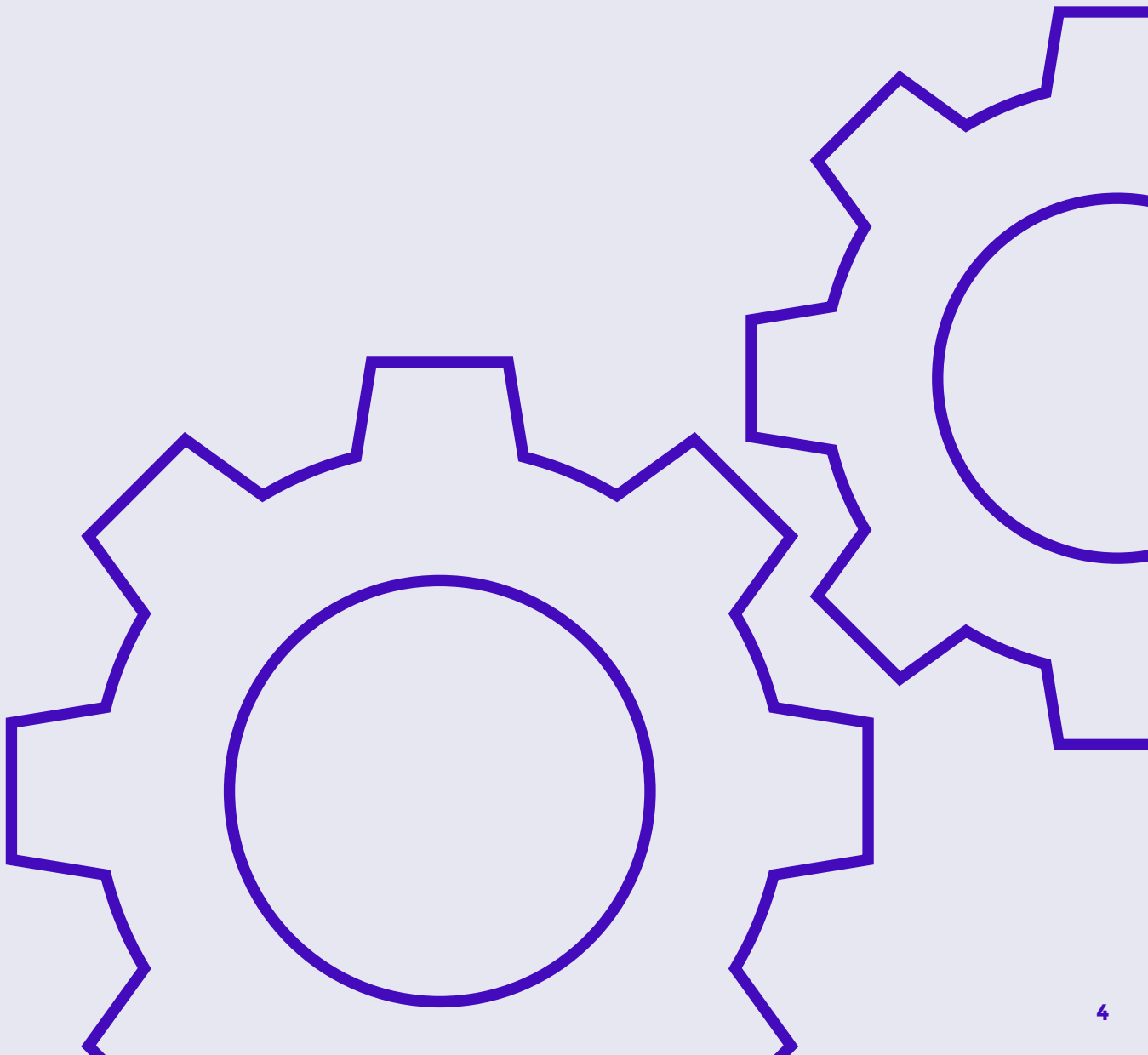
18.8K
in Q1 2018

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 cyber attacks, the latest malware and viruses, online scams and cyber crime trends.

Approximately 200M digital files are collected, 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 cyber criminals.

This report contains data from cyber attack detections in Android smartphones from more than 21M active users of our dfndr security app. The analysis is based on data collected between January 1, 2018 and March 31, 2018.



Q1 Summary

dfndr lab detected a total of 3M cyber crimes during the first three months of 2018, an increase of 10.0% from 2.9M during the last quarter of 2017. Scams directly related to phishing made up 1.4M of the total detections, down from 2M in the last quarter, suggesting that other types of online attacks are on the rise and hackers might be trying new and more targeted tactics.

Two of the top three scams detected in Q1 remained the same as those detected in Q4 2017. Fraudulent advertisements that involve spoofing well known and trusted brands continued to hold the top spot with 1.5M detections, up over half a million from 971K detections from last quarter.

Generic phishing attacks maintained second place as the most common type of threat this quarter with 566K detections but saw a decline of 16.0% from 658K in Q4. Phishing involves the use of spoofed emails and SMS messages that appear to come from well-known organizations asking users for personal information, such as social security numbers, bank account credentials, credit card numbers, and passwords.

Fraudulent advertisements that involve spoofing well known and trusted brands continued to hold the top spot with 1.5M detections.

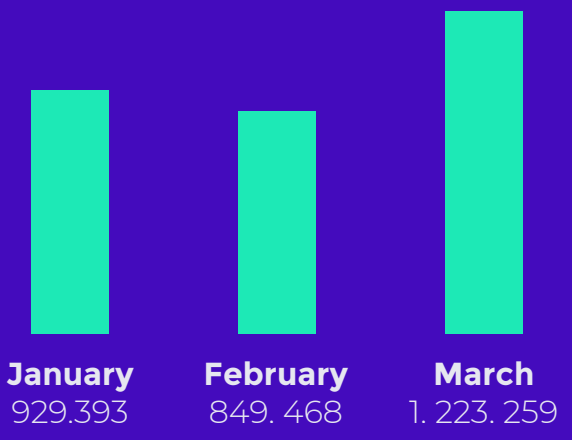
Often times phishing attempts appear to come from websites, services, and businesses with which the user may not even have an account. Common tactics involve requesting the user to update personal information, alerting the user to fabricated issues with an order, or a problem processing a payment.

Scams using messaging apps, such as WhatsApp and Facebook Messenger, moved up the list, bumping fake promotions out of the top three from the previous quarter. Although attacks related to messaging apps were down 32.0% overall (from 475K detections in Q4 2017 to 326K detections in Q1 2018), counterfeit promotions saw a more significant reduction in detections from 537K to 215K, down 60.0%. Data trends suggest that hackers are increasing their focus

Malicious URL Detections in the US

Q4 2017 → Q1 2018

2,969,140 → 3,002,120

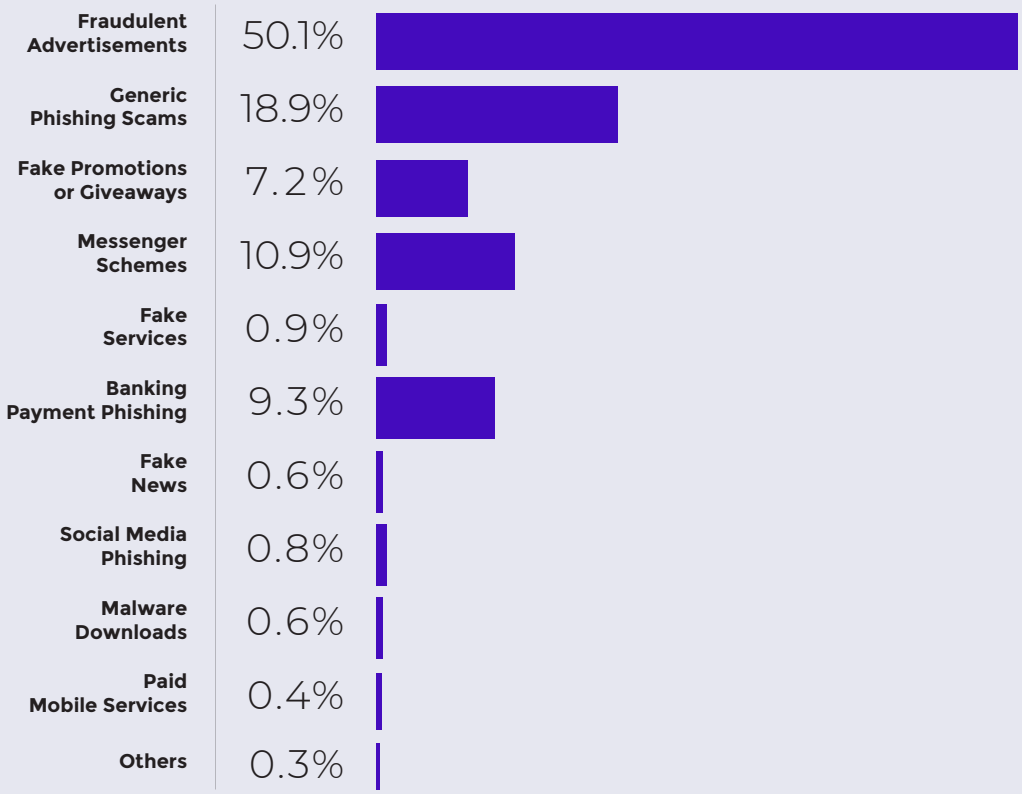


Americans accessed an average of

23 malicious URLs

per minute in Q1 2018

Most Common Categories of Malicious URLs Detected



Top 3 Scams Detected

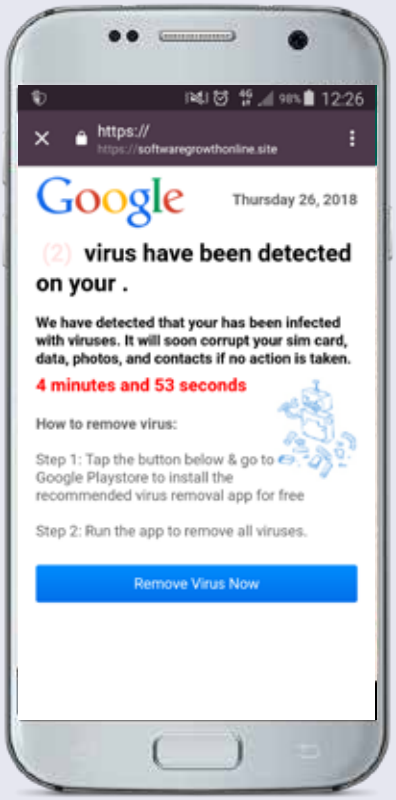
1 FAKE VIRUS ALERT

Fraudulent Advertisement

558,221

DETECTIONS

Fake virus alerts are an example of fraudulent advertising. In these spoofed ads, a false virus warning pops up as a banner that looks like a system alert and claims the device is infected by malware. This tricks the user into urgently downloading and installing bogus antivirus software. Fraudulent advertisements represented 50.1% of detections and was the primary means by which hackers spread their attacks in Q1. Compared to 2017 Q4, the detections in this category saw an increase of 54.0% - from 970K to 1.5M.



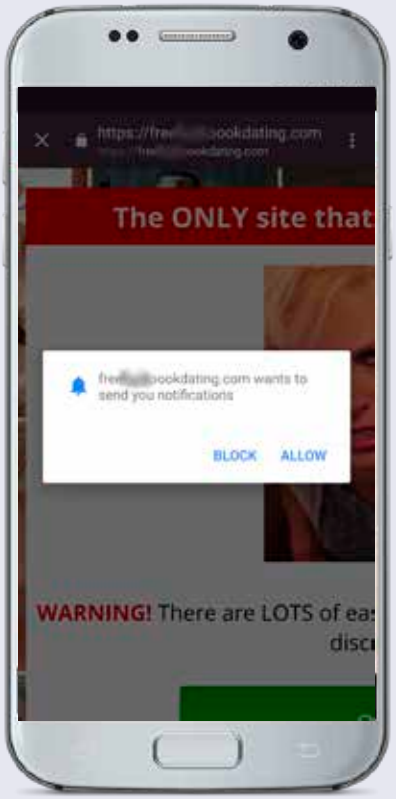
2 ADULT DATING SITE

Generic Phishing Scam

175,423

DETECTIONS

Spoofed dating sites featuring pornographic material threaten users' security in two ways. First, these sites request user permission to send update notifications that could install malware. Second, hackers redirect users to pages with advertisements that earn them a commission based on click-throughs and ad engagement. Although the first three months of 2017 saw a 13.0% reduction of this type of attack compared to the previous quarter, generic phishing still accounted for 566K detections and represented 18.9% of total malware detections between January and March of 2018.



Top 3 Scams Detected

3 GET REWARDED

Fake Promotions or Giveaways

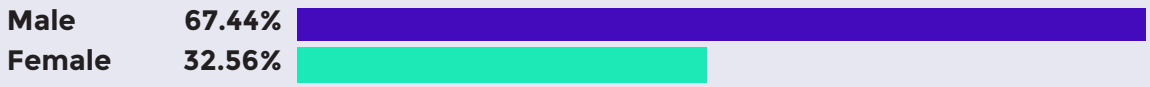
108,106

DETECTIONS

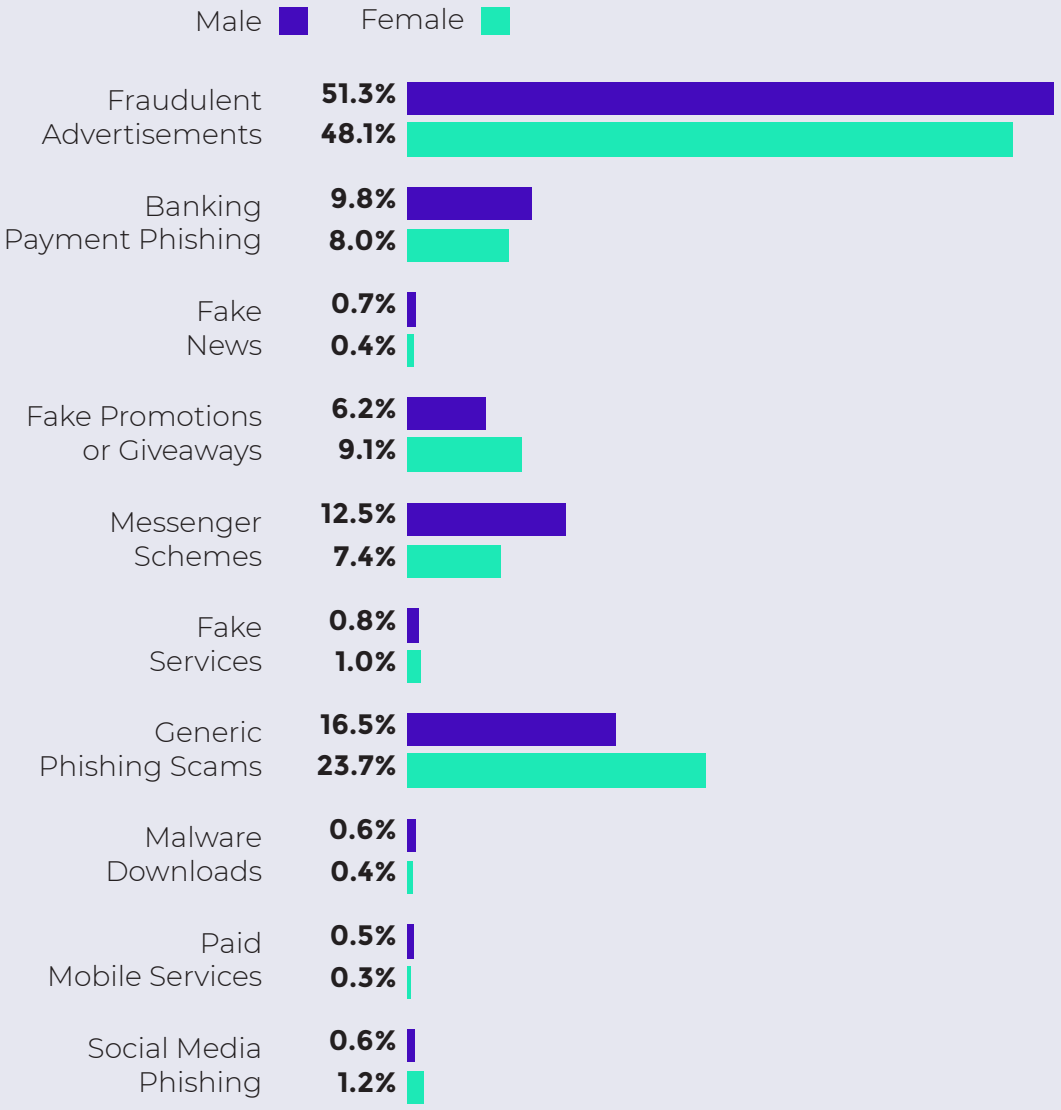
“Spoofed giveaways” are promotions and sweepstakes that trick users into registering for prizes in order to steal sensitive data and often bait victims with expensive items, such as smartphones, gaming consoles or other high-value merchandise. Similar to fraudulent advertisements, these scams involve asking the user to install an app, subscribe to a paid SMS service or register by clicking a link infected with malware. Although these attacks were down significantly from 537K in the previous quarter to 215K, these scams still accounted for 7.2% of cyber attacks in Q1 2018. The 59.0% reduction in these bogus contests might be explained by the huge jump in fraudulent advertisement detections.

Detections by Gender in the US

Men clicked on malicious URLs twice as often as women did in Q1

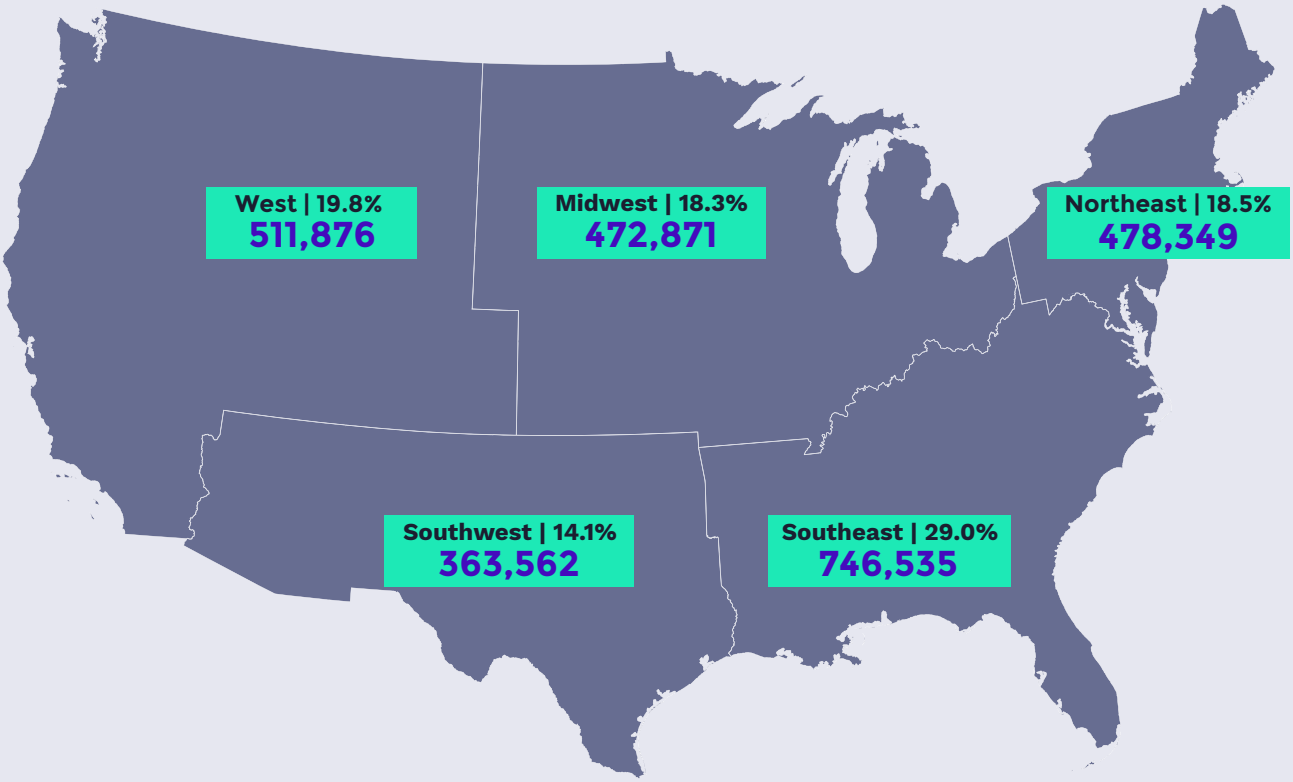


The data suggests that women are more susceptible to fake giveaways compared to other schemes, whereas men are more susceptible to messenger schemes.



Detections by Region

The Southeast region was the primary target of cyber criminals using malicious links during the first quarter of 2018, reaching 746K detections. California, Texas, and Florida were the top three states where such activity was detected, accounting for 31.4% of all the malicious link detections this quarter.



The top 5 affected states accounts for almost half of all detections

	January	February	March	%
California	97,698	88,211	140,621	12.6%
Texas	83,335	80,244	116,348	10.8%
Florida	66,476	56,432	79,517	7.8%
New York	60,430	43,354	60,803	6.4%
Georgia	52,142	46,457	68,951	6.5%

FAKE NEWS

Why you should care

"Fake news" stories contain misleading or false information that is published by an unreliable and often unverifiable source. Many times, misinformation comes from websites that spoof legitimate news agencies or other reputable websites. Authors typically are not experts on the subject about which they are writing, and in some cases, are paid trolls that profit from spreading false information.

Fake news is harmful because it can diminish the credibility of individuals or organizations who repost these stories or cite them as sources of factual information. Stories that contain false information about an individual or business can cause irreparable damage to their reputations. Additionally, websites that post bad information such as false medical advice can be dangerous and physically harm users.

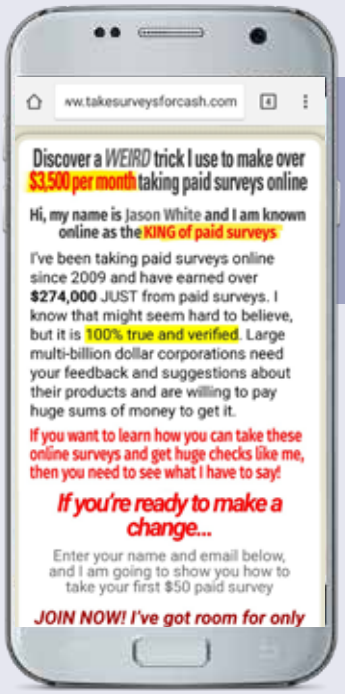
Source: Butler Libraries & Archive, Butler Community College published April 2, 2008. Butlercc.libguides.com

How dfndr lab Detects Fake News

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

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.

Top Fake News Detected in Q1



5,485 detections

2,212 detections

Fake news detection increased by 19.6%

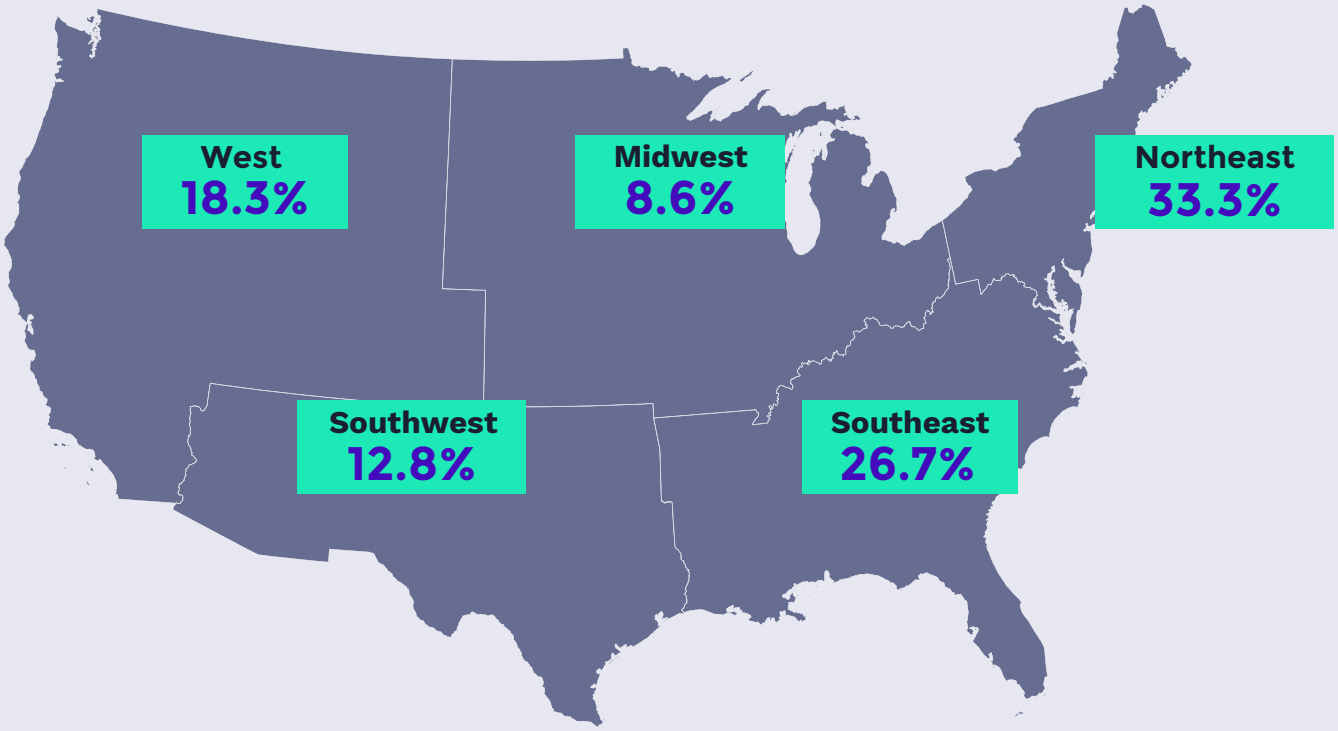
15.7K in Q4 2017 → **18.8K** in Q1 2018

Fake News Detections **by Gender**

Male	**74.8%**
Female	**25.1%**

Fake News Detections **by Region**

The Northeast region saw the most attacks involving malicious links spread through fake news in Q1 2018. The top three states affected were California, New Jersey, and New York, comprising 38.0% of all fake news related attacks in the first part of this year.



California
2,698
DETECTIONS

New Jersey
2,494
DETECTIONS

New York
2,013
DETECTIONS

Tips to Identify Fake News

dfndr lab compiled some useful tips to help you identify fake news.

1. Look beyond the headline. Many readers never actually read the article itself. According to an article in the New York Post published last June, a joint study between computer scientists at Columbia University and The French National Institute, revealed 59.0% of news stories shared on social media hadn't received any clicks, which means the articles were not opened or read. This suggests that they were reposted solely based on the story's headline.

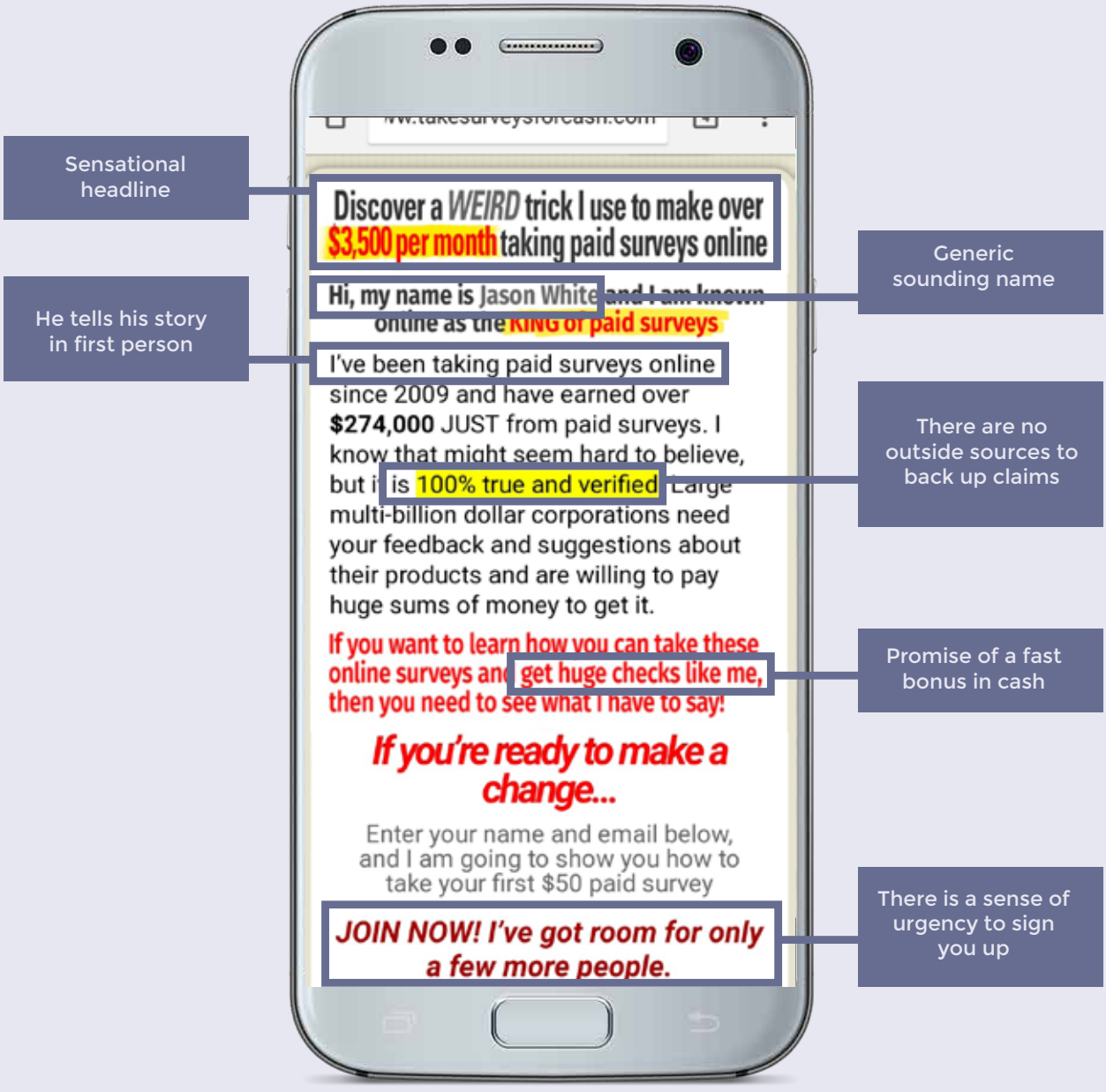
2. Check for verifiable sources in the story. A dependable article should reference quotes from experts or people directly involved. Valid sources should be easy to fact check online. Even if an article has cited sources, it is still a good idea to double check them. Frequently, fake news writers will post bogus links that don't really back up what their story claims.

3. Satirical websites are on the rise and often use legitimate sounding names that can confuse readers. Stories posted from these sources sound believable. It is a good idea for users to look for disclaimers in fine print on websites identifying themselves as parodies or satirical in nature. Additionally, doing a little research on a source will often reveal whether or not it is a legitimate news agency or an entertainment site.

4. Finally, beware of breaking news being reposted on Twitter, Facebook, Snapchat, and other social media sites. Unverified rumors can be spread quickly by well meaning users wanting to be among the first to share it with their followers. Before sharing anything hot off the press, it is wise to check several established news sources, such as your local radio or tv station, to determine whether they are also reporting the story.

Source: "What is fake news? How to spot it in an age of misinformation" by Will Nicol published 2/24/18 by digitaltrends.com

Tips to identify fake news



LOOKING AHEAD

2018 marks a daunting year for cybersecurity, particularly for mobile phone users. Mobile security attacks will continue to rise in 2018. Here are dfndr lab's forward-looking observations:

1. At least a 50.0% increase in large-scale data leaks and hacks of large institutions, more than in 2017.

2. As artificial intelligence becomes more prominent, the first wave of AI threats will surface - a menace few are ready to defend against.

3. New attacks will be aimed at AI assistants, such as Amazon Echo and Google Home. It will also be aimed at the automation communications layer, such as ZWave- and Zigbee- enabled devices, which control home locks, garage door openers, home lights, TVs, and more.

4. Network carriers can now sell your information legally. Your data will be sold as a commodity to third-parties.

5. Your data is being sold, stolen, and shared in order to better train AI "agents", and not always to your benefit. Be mindful of your privacy, particularly your passwords. Do not fill out data forms if you don't absolutely need to, especially for online promotions or from sites/ sources you don't really know and trust.

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 cyber attacks and scams. Its missions is to protect consumers from highly sophisticated cyber criminals 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 130+ million installs globally, has consistently been named as a top-rated antivirus software by AV-TEST Institute – the world leader in security and antivirus research. To safeguard and enhance users' online experiences, the company's app 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 offices in Brazil and numerous satellite employees around the globe.

Global Headquarter
45 Belden Place, 3rd Floor, San Francisco, CA 94104
dfndrlab@psafe.com

dfndr lab

dfndrlab.com