Cybersecurity Report

Q2 2018

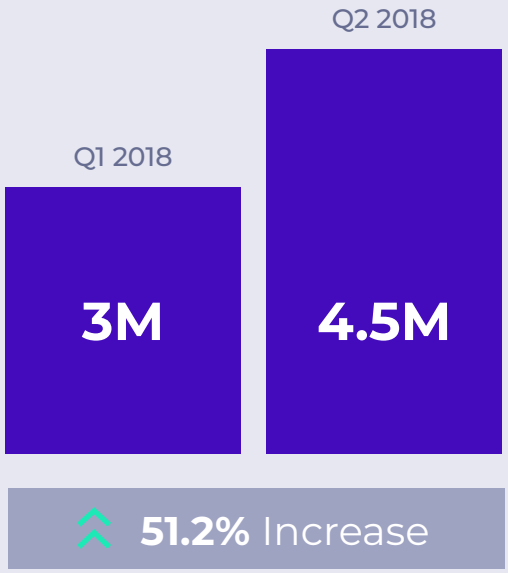
dfndr lab

Contents

Q2 Key Conclusions

7.5M

malicious URLs detected in the 1st Half of 2018



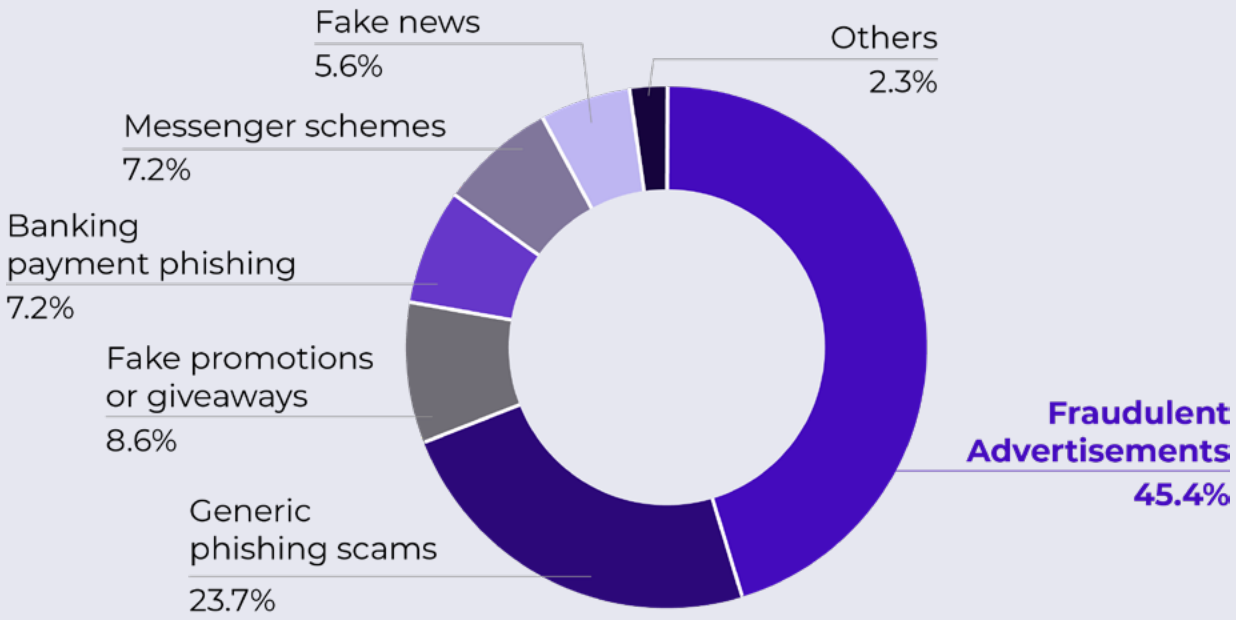
51.2% Increase

4.5 million malicious URLs detected in 2018 Q2

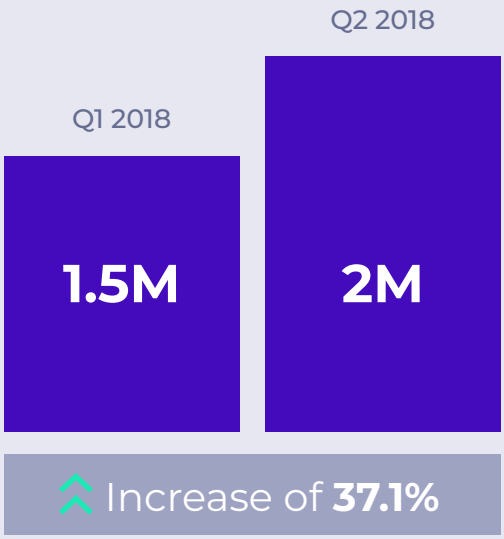
34 malicious URLs detected per minute

Men clicked on malicious URLs **twice as often** as women did

Malicious URLs Detected in Q2



Fraudulent advertisements increased **37.1%** between Q1 and Q2



Top 3 Fraudulent Advertisement Sources:

1. Porn Websites

2. General Trusted Websites

3. Movie Websites

More than 5,000 Android phone users were surveyed about online security and privacy

56.8%

worry more about privacy since the Facebook/Cambridge Analytica scandal

Financial data is what users worry the most about keeping on their phones.

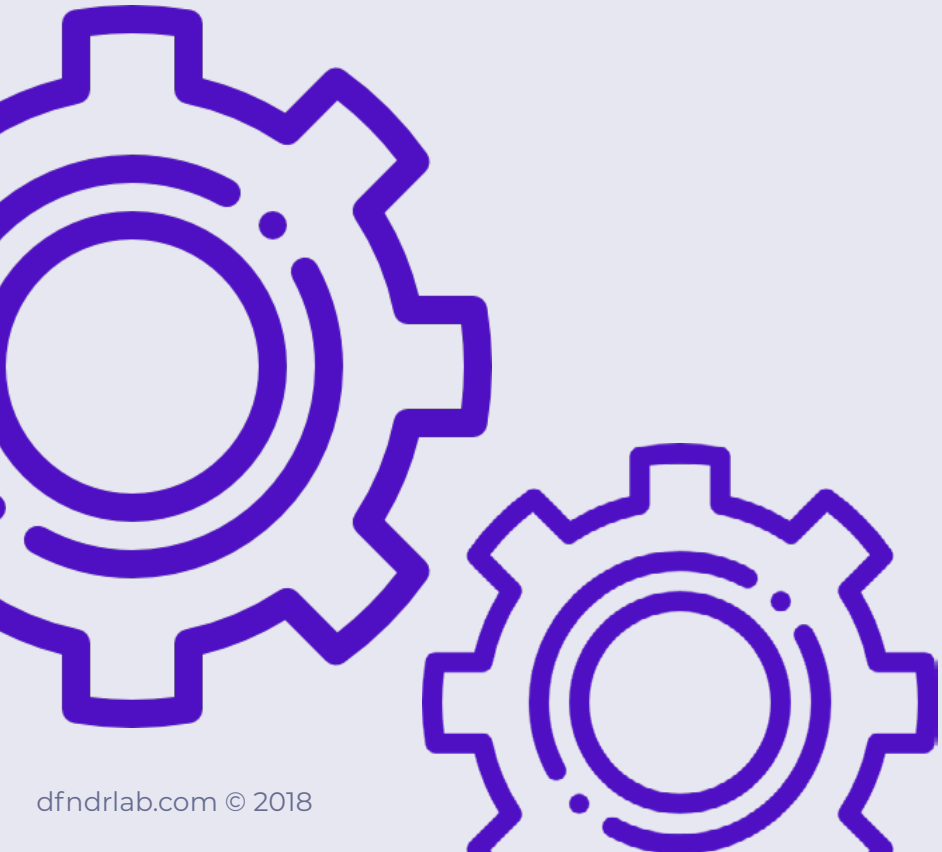
Downloading a virus and having **personal data stolen** are the top security concerns.

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 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 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 April 1, 2018 and June 30, 2018.



Q2 Summary

The latest installment of dfndr lab's Cybersecurity Report shows a disturbing trend: cyber crime has continued to increase at an alarming rate since the first half of 2018 with more than 7M detections.

In the second quarter, dfndr lab detected over 4.5M malicious links, an increase of 51.2% compared to 3M detections in the previous quarter. That breaks down to 34 malicious links identified per minute or 2,040 malicious link detections per hour.

Fraudulent advertising continued to be the top threat and increased by half a million detections compared to the first three months of 2018, from 1.5M to 2M making up 45.4% of all malicious activity. Scams involving false advertisements can be spoofed ads of trusted brands with a fake coupon or offer that tricks consumers into entering sensitive personal information or infects their phone with malware when

Marco DeMello
CEO of PSafe
Global Head of dfndr lab

Fraudulent advertising continued to be the top threat and increased by half a million detections

they attempt to click an offer to redeem it. Another common tactic is pop-up ads with clickbait copy that compels consumers to grant permissions to access deceptive content or receive false notifications, with the payload being malware or spam bots delivering more malicious ads.

Generic phishing remained the second biggest threat behind fraudulent advertisements, with an increase to 1M detections in Q2, up from 566K last quarter accounting for 23.7% of malicious activity. Fake promotions and giveaways retook the third-place spot in Q2, bumping down scams involving messaging services such as Facebook, SMS, or WhatsApp, which was third place in Q1. Fake promotions and giveaway scams had previously been the third most detected cybercrime for the final quarter of 2017. dfndr labs detected 391K fake promotions this quarter accounting for 8.6% of cybercrime in the past three months.

Among cybercrime trends detected this quarter, SMS messaging was the most common methods used to spread malicious URLs in the US. Data analyzed from Q2 detections showed that one in 25 links sent via SMS were malicious. Another notable highlight is the rise of a new channel hackers are using to reach mobile users: browser push notifications. First hackers trick users into giving a website permission to send notifications, then the hacker can send messages even when the user is not on that website. Once permission is granted, hackers spam users with fake virus alerts, malware links and other deceptive content that hackers profit from. The number of false advertisements that asked for notification permissions increased 712% in June (220K scams) compared to May (27K detections).

In addition to push notification exploitation, another reason for the increase in fake ad scams is the diversification of attacks. Previously, scams like these were concentrated in more dubious websites such as adult content. In recent months, however, evidence suggests that cybercriminals are imitating trusted sites to propagate fraudulent advertisements, accounting for almost 45.8% of these scams. Fake news is another category that has seen growth due to the greater sophistication and believability of the content and link to everyday situations.

SMS messaging was the most common methods used to spread malicious URLs in the US

A survey of Android users' privacy and security concerns was conducted by dfndr lab. The survey results found the most common security issue respondents experienced was malware, with 25% having downloaded a virus on their phone. Ranked second was being scammed by malicious links or fake websites at 18%. Though 17% of respondents cited malware or viruses as a first concern, data analyzed in Q2 points to malicious links as a growing threat (3M in Q1 > 4.5M in Q2), due to the easy manipulation of websites or applications to mask social engineering attacks. In terms of privacy, 27% of respondents indicated that keeping credit and debit data on their phones felt more vulnerable than potentially having photos (13%) or videos (9%) compromised.

Malicious URL Detections

Q1 2018
3,002,120

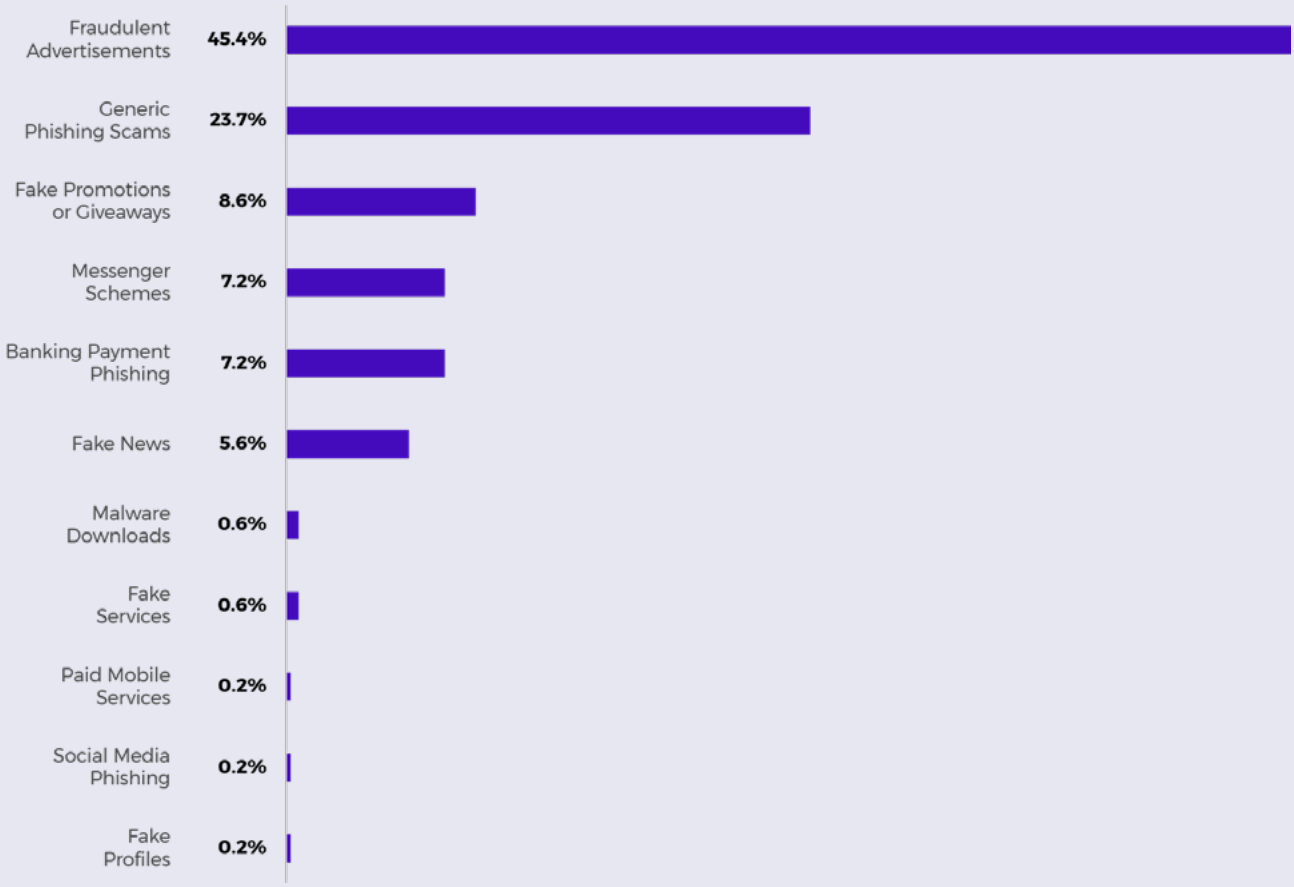
Q2 2018
4,537,976

51.2% increase

Americans accessed an average of **34 malicious URLs** per minute in Q2 2018

APRIL	MAY	JUNE
988,508	1,719,505	1,829,963

Most Common Categories of Malicious URLs Detected

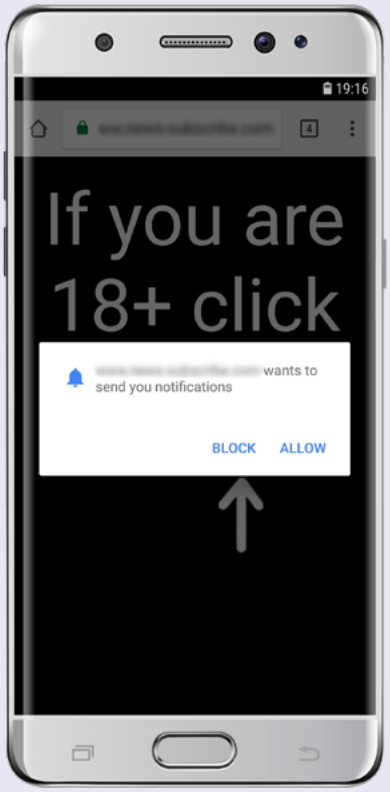


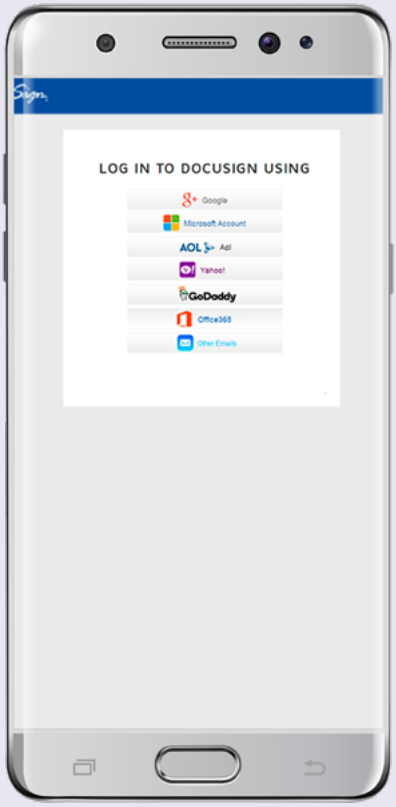
Top 3 Types of Scams

1 FRAUDULENT ADVERTISEMENTS

Q2 saw an increase in fraudulent ads of just over 2M up from 1.5M in Q1. 247K of these detections were related to push notifications and accounted for 12% of the activity in this category. Push notification detections saw a significant jump at the end of Q2 and were eight times higher in June than May. The increase in push notification detections accounts for a new methodology of cybercriminals. Hackers bait a victim by asking for permissions and when denied, simply redirects the user to another dummy page and requests the same permission again, until the user finally accepts and is then redirected to a malicious site. These scams prove effective due to their repetitive, high pressure tactics.

Although deceptive advertising was up in detections, it only accounted for 45.4% of the total detections in Q2 compared to 50.1% of detections in the previous quarter. The main reason for this is fake news increased by 5% in Q2.





*These brands were spoofed for this particular phishing scam.

2 GENERIC PHISHING SCAMS

Phishing is a tactic used by cybercriminals that involve stealing sensitive information by impersonating a well-known business or organization. Generic phishing scams are any phishing attack that doesn't include compromised banking information or is spread through social media.

One example of generic phishing is receiving a spoofed email that appears to originate from a service such as Gmail asking the user to update his or her password by clicking on a link. Once the cybercriminal gains access to the account, it is then used to spread malware by posing as the account owner. A common method of hackers is to misuse brand names to trick users into giving their credentials.

Generic phishing remained the second most common tactic used by hackers and saw a 90% increase this quarter from Q1 with over 1M detections. The most common method used was malware-infected links spread through SMS messages. Generic phishing remains a favorite tactic with cybercriminals, especially using SMS, because it is difficult to trace the origins of the text. Additionally, phone numbers can be spoofed making it appear that the message did, in fact, come from a known number.

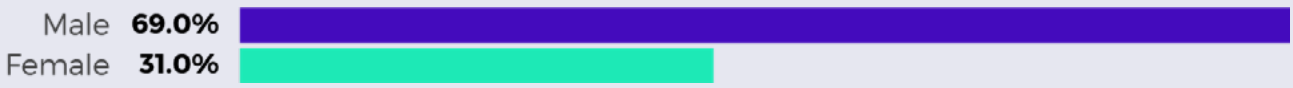
3 FAKE PROMOTIONS OR GIVEAWAYS

Fake promotions are illegitimate contests and sweepstakes that bait users into entering with the hopes of winning valuable prizes such as electronics, vacation packages, and other high-end items. Consumers risk having sensitive data stolen when they register for these giveaways, being exposed to links infected with malware or possibly downloading spyware to their phones.

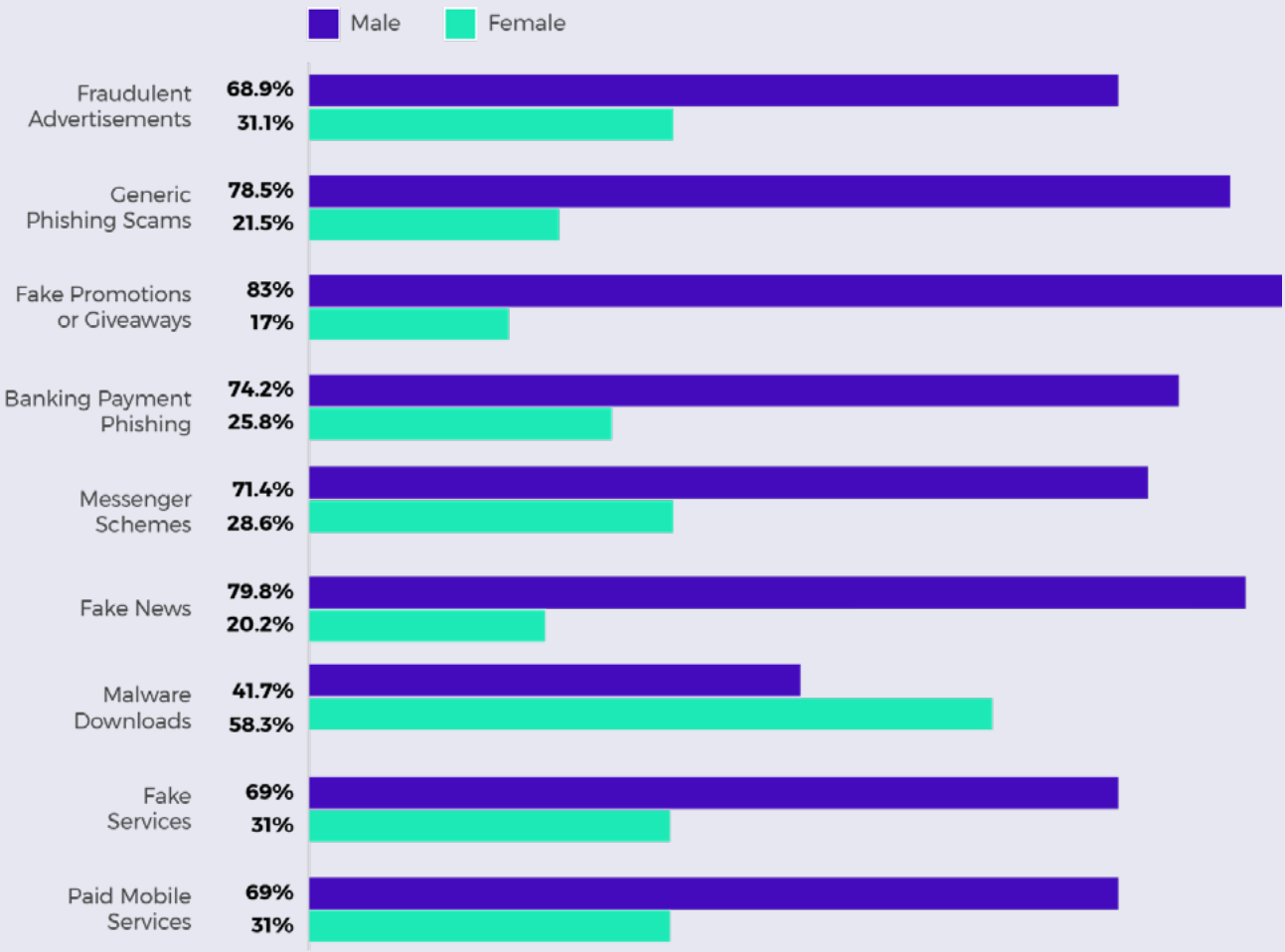
Fraudulent contests or sweepstakes continued to see an increase this quarter from 7.2% up to 8.6% and jumped from the fifth most detected scam in Q1 to the third most detected in Q2. Several factors could explain the rise in these types of scams.

First, contests or sweepstakes are often seasonal. Summer online shoppers are exposed to scams that focus on free vacations, high-value gift cards, or heavily discounted festival tickets which are seasonal specific, attractive items. Additionally, fake contests are easy to create, and there is no obvious way for entrants to verify that it is legitimate or if anyone has won or will win any of the promised prizes. Finally, many users don't recognize the risks of entering such promotions and take chances to win a desirable item at any cost.

Detections by Gender

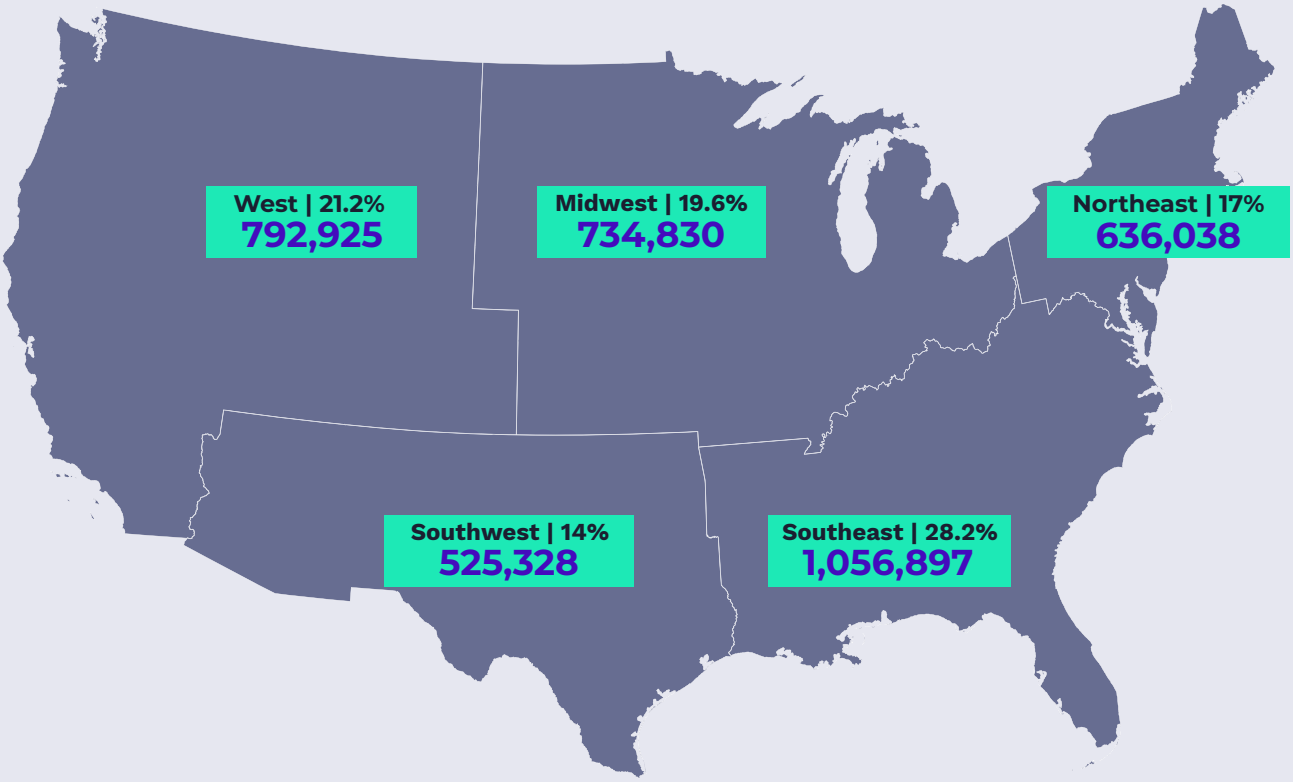


Men clicked on malicious URLs **twice** as often as women did in Q2



Detections by Region

The Southeast region was the primary target of cybercriminals using malicious links during the second quarter of 2018, reaching 1M detections. California, Texas, and Florida were the top three states where such activity was detected, accounting for 32.5% of all the malicious link detections this quarter.



The top 5 affected states accounts for almost 44.4% of all detections

	April	May	June	Q2	%
California	111,902	194,322	207,377	513,601	13.7%
Texas	97,886	155,431	147,552	400,869	10.7%
Florida	61,539	121,959	119,754	303,252	8.1%
Illinois	47,548	88,195	90,639	226,382	6%
Georgia	53,587	83,128	83,329	220,044	5.9%

Fraudulent Advertisements

Why These are Dangerous

False advertisements are damaging for both legitimate advertisers and consumers. Scammers will either create phony ads that are similar to brand advertising campaigns or create misleading ads to get victims to grant push notification permissions that lead to malicious sites.

Advertising platforms such as Google and Amazon do their best to expunge false advertisers, yet their presence persists, which can affect consumer trust. Not only do scammers take advantage of genuine advertising platforms, dubious affiliate networks also use these platforms to spread deceptive ads and generate revenue for clients in unethical ways. In Q2, dfndr lab saw a 37.1% increase in false advertisements from Q1, with the majority of detections originating from web browsers at 88.1%.

detections in Q1 2018

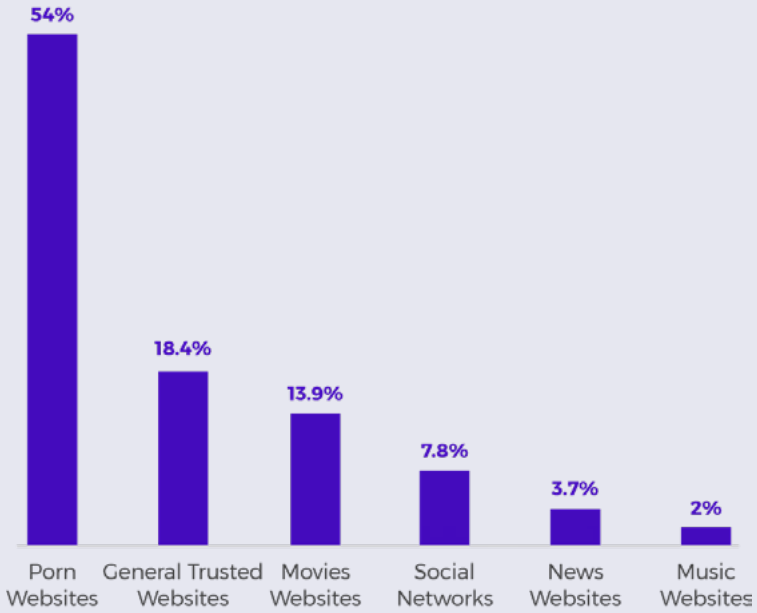
1,503,568

detections in Q2 2018

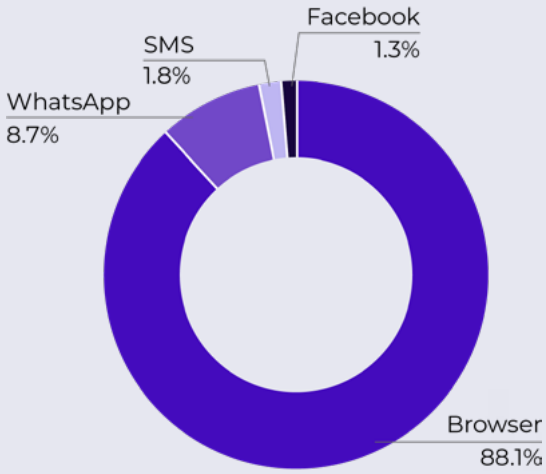
2,060,965

37.1% increase

Website Analysis



Source Analysis

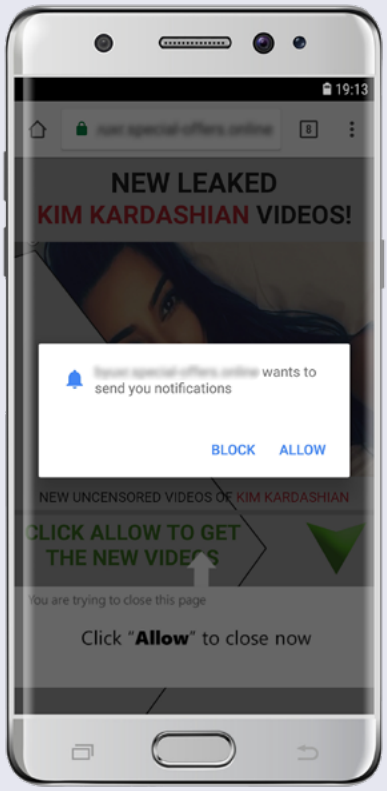


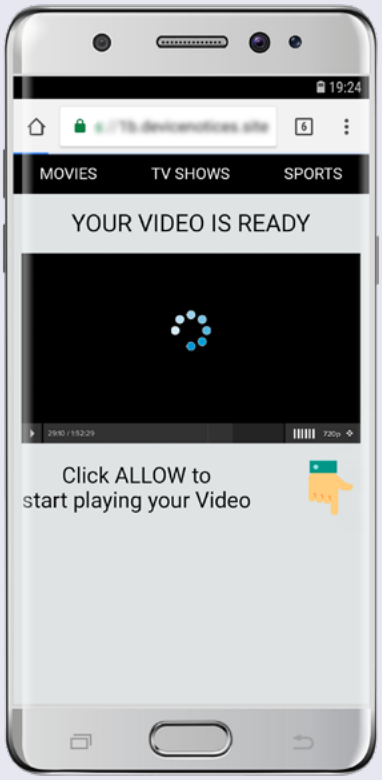
Top 3 Fraudulent Advertisements

1 KIM KARDASHIAN LEAKED VIDEO SCAM

268,207 DETECTIONS

This scam was distributed as a banner ad in various mobile phone apps and as a link on social media. The scam promised some "leaked" videos of reality star Kim Kardashian. In truth, the ad didn't reveal any videos. The user was asked to approve a push notification to allow the videos to load and play. A push notification generated by the false ad requested permission for a transaction, in this case, to "allow" access to alleged videos of a celebrity. The ad continued to ask for permission repeatedly until it was finally granted. Once approved, the scammer then spammed the user with more fake ads, many of which contained malware or directed the user to other ad sites where the hacker profited from click-through traffic.





2 "YOUR VIDEO IS READY" SCAM

127,641 DETECTIONS

Like the Kardashian video scam, this involved a fake advertisement and was spread using the same methods. It showed up as a screen with a spinning wheel that made it look like a video was trying to load. A message above the screen informed the viewer that their video was ready. Below, users were instructed to "Click ALLOW to start playing your Video." A navigation bar above the screen with buttons for "MOVIES," "TV SHOWS," and "SPORTS" implied that this was an installation for a video streaming app. The urgent message of a video loading tricked the user into granting permission by tapping 'allow.' Instead of seeing a legitimate video, the false ad spammed the user with even more ads.

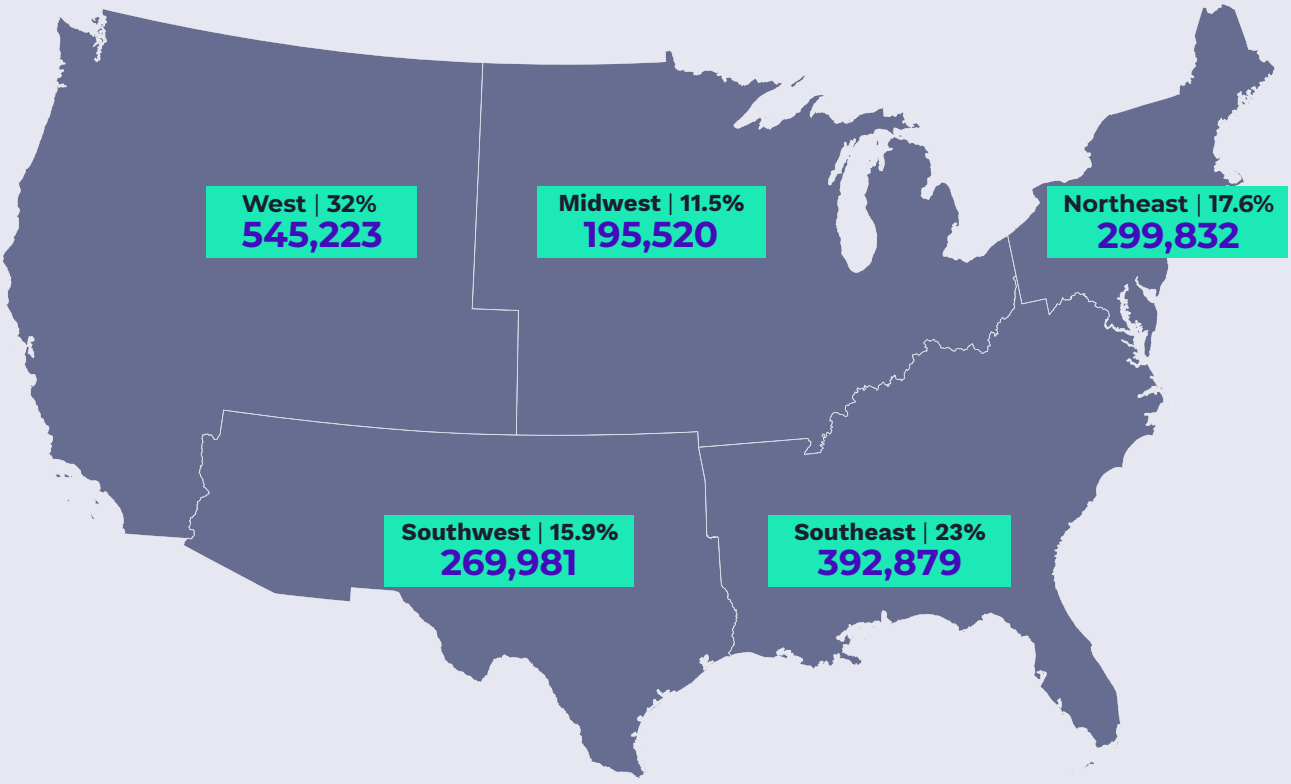
3 “ADULT SITE AGE VERIFICATION” SCAM

97,099 DETECTIONS

This scam is similar to the previous two. In this instance, a banner ad asked users to confirm they are over 18 years of age by clicking the “Allow” button. Although no description or information about the content was visible, the age restriction implied the user was accessing adult content. When users granted permission to the push notification, they were spammed with more false advertisements.

Fraudulent Advertisements by Region

The West region saw the most attacks involving malicious links spread through fraudulent advertisements in Q2 2018. The top three states affected were California, Texas, and Florida, comprising 32.5% of all fraudulent advertisement related attacks in the second part of this year.



California	220,111	12.9%
Texas	188,512	11.1%
Florida	145,671	8.5%
Illinois	106,862	6.3%
Georgia	105,331	6.2%

Data Privacy in the Current Landscape

Hackers use online scams such as fraudulent advertisements, phishing, and fake promotions to collect personal information. Commercial data breaches are another avenue where cybercriminals gather large amounts of personal data. This information is the equivalent to currency and is often sold on the Dark Web, an online black marketplace operated by cybercriminals where illegal activities are conducted like selling stolen credit card numbers, passports, social security numbers and more. The Dark Web also deals in other illegal goods such as top-secret military data or drugs. Due to the use of cryptocurrency as a standard payment method in the Dark Web, tracking criminal activity and transactions has proven difficult for law enforcement agencies.

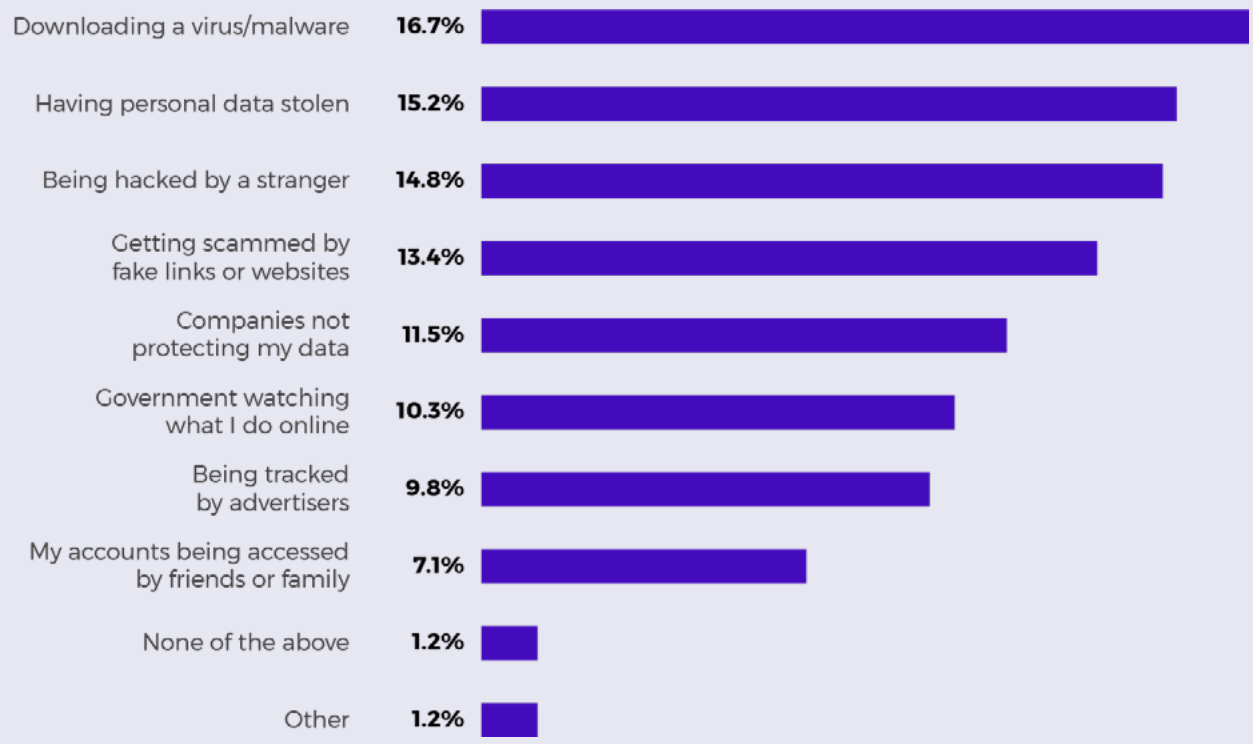
Data privacy is not just a concern when it comes to cyber crimes, but how services such as Facebook use personal data is still a looming issue. Many tech or software companies have revised privacy policies in the wake of the Facebook/Cambridge Analytica scandal and the roll-out of GDPR compliance. dfndr lab conducted a survey of Android users on privacy and security issues.

Privacy and Security Survey

Key Findings

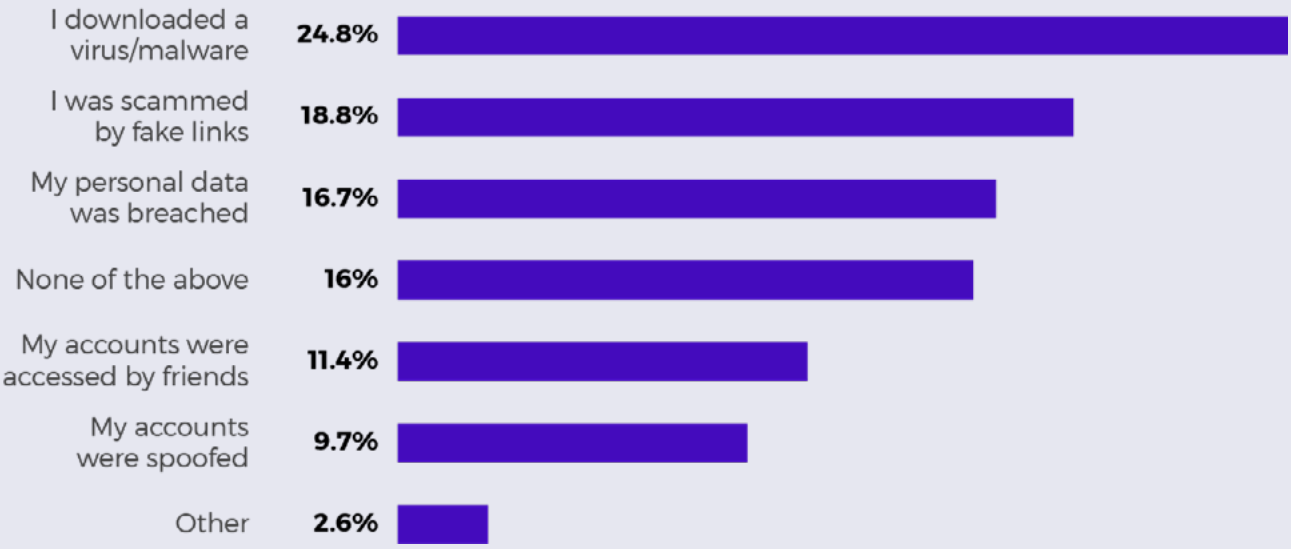
5,083 respondents took the dfndr lab survey. According to the results, no single issue had a significant lead regarding online privacy suggesting that Android users have a wide range of security concerns about data privacy. Consumers were slightly more worried about downloading a virus or having personal data stolen than being tracked by the government or by advertisers.

Which of the following mobile phone issues do you worry about?



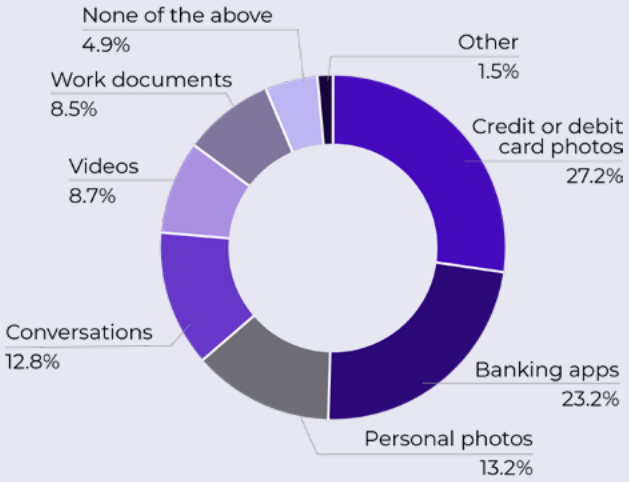
When it came to security issues that consumers had experienced, 25% downloaded a virus or malware and 19% clicked on an infected link.

Which of the following security issues ave you experienced?



When asked what items respondents were most concerned about keeping on their phones, almost half answered having financial information stored was the biggest worry. 28% were specifically concerned with debit and credit card information and 23% felt banking apps were most at risk.

Which of the following items are you afraid of keeping on your phone?

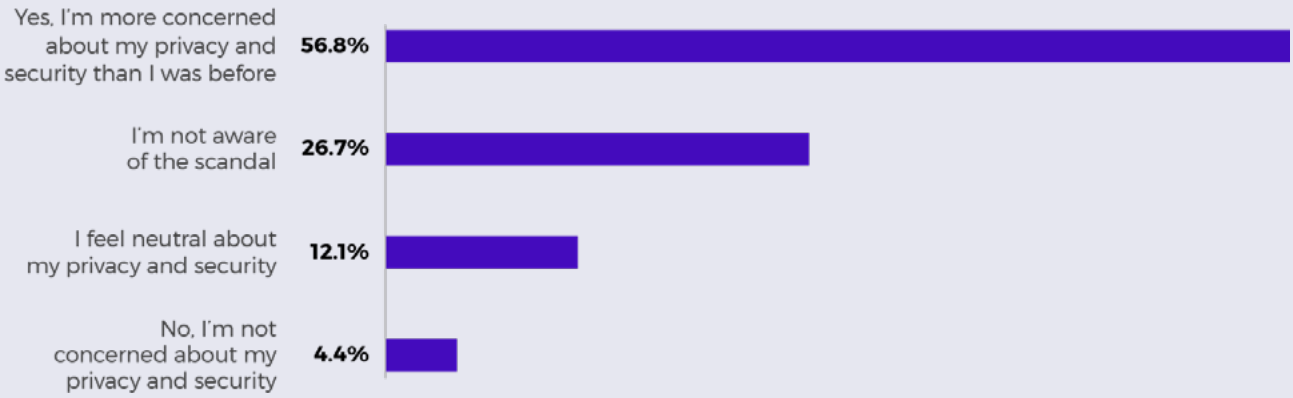


The Cambridge Analytica Scandal and Consumer Privacy

Cambridge Analytica was a British-based political consulting firm founded in 2015 that was involved in a Facebook data collection scandal that may have influenced the outcome of the 2016 US presidential election. It raised questions about the legality and ethics regarding the collection and use of personal data to profile voters.

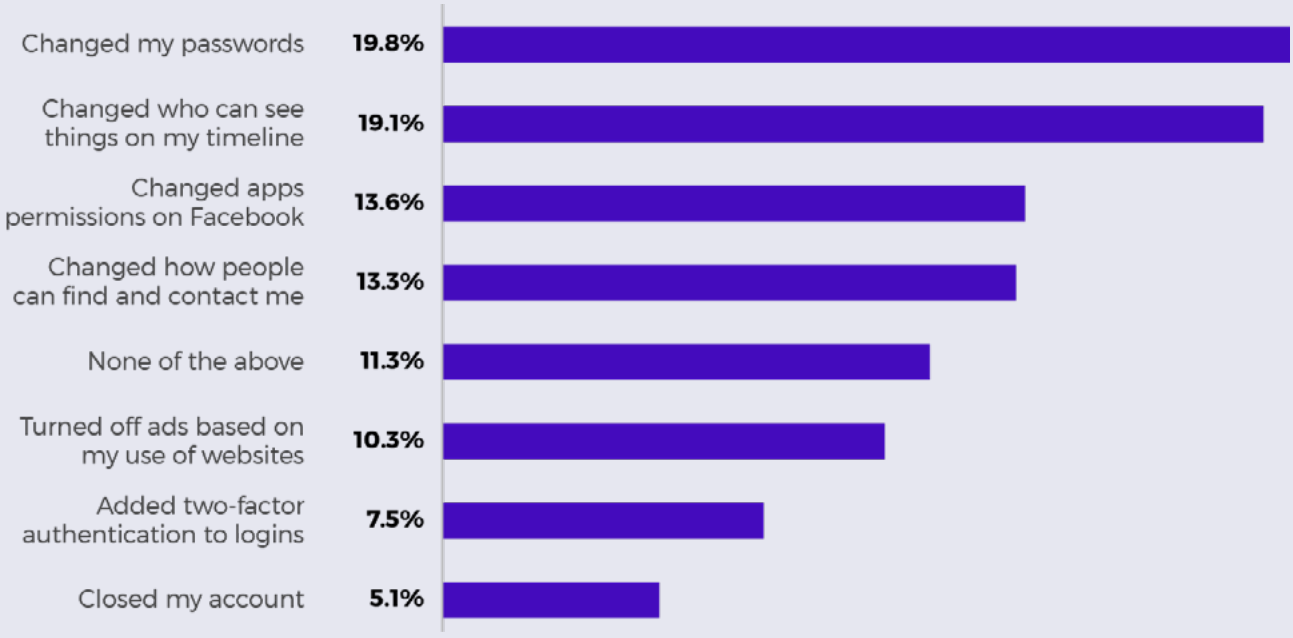
dfndr lab asked respondents if the scandal had changed their opinion about sharing data online. 57% indicated they have become more concerned about their online privacy as a result of the scandal. 12% were neutral on the issue, while only 5% felt the scandal had not changed their opinion. 27% indicated they did not know about the scandal.

Did the Facebook/Cambridge Analytica scandal change your opinion about sharing your personal data online?



Additionally, respondents were questioned about adjusting privacy or security settings in their Facebook accounts. The most common security precaution taken was changing their account password (20%), followed by adjusting privacy settings (19%). Only 14% modified settings dealing with app permissions, and 13% of users changed how people could contact them. 10% turned off advertising tracking used to tailor the types of ad content users see within Facebook. Only 8% added two-factor authentication when logging into their Facebook account. Approximately 11% had not made any changes to their security settings at all, while 5% said they closed their Facebook accounts and no longer used the service.

What following Facebook settings have you done to your account?



About the Survey

This survey was conducted online by dfndr lab between July 9 and July 18, 2018. The data collected was from 5,083 Android users across the United States. The margin of error for the total sample is +/- 2%.

How to Protect Your Privacy

There are several ways consumers can protect their personal data:

1

Use anti-phishing software like dfndr security

Regular antivirus software might only scan for malware or viruses, but not be able to detect phishing attempts. Anti-hacking and anti-phishing technology built into dfndr security proactively identifies and warns consumers about potentially infected malware links.

2

Be careful when entering contests or sweepstakes

Forms and apps are vulnerable to malware infection. Never fill out an online contest form if you are unable to verify the source.

3

Refrain from answering requests to update personal information

Be wary if the request stems from links in emails or SMS messages. When possible, only update sensitive data by calling a verified number or logging onto an official website through a secure connection.

4

Share less on all your accounts

When signing up for new accounts, only share what is necessary to activate the account. Return to accounts previously set-up and edit those down as well.

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. 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 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 satellite offices in Brazil.

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

dfndr lab

dfndrlab.com