



SOCIAL MEDIA HABITS
AND YOU

TREND ANALYSIS

2018



IDENTITY THEFT
RESOURCE CENTER

idtheftcenter.org • 1-888-400-5530

THANKS TO OUR PARTNERS AT:

 **CYBERSCOUT®**






THE STUDY

This study was conducted by CyberScout® and the Identity Theft Resource Center and shows the growing concern amongst consumers of managing personal data and privacy online.

PRIVACY:

35.37% completely private
54.02% semi private
7.56% completely public
3.05% don't know settings


DON'T USE

 9.03%  47.27%  41.98%  25.25%  42.95%

NEVER

 2.26%  6.28%  5.29%  2.62%  5.08%






RARELY

 12.42%  23.97%  22.48%  13.44%  10.98%






1-2 TIMES A WEEK

 11.30%  11.74%  10.58%  11.97%  8.03%

3-5 TIMES A WEEK

 10.97%  5.45%  5.12%  9.18%  7.38%

DAILY

 24.84%  4.79%  7.77%  17.05%  15.74%

MULTIPLE TIMES A DAY

 37.26%  2.64%  9.09%  24.26%  14.10%

HOW DID YOU KNOW YOU WERE A DATA BREACH VICTIM?

13.16% 3RD PARTY WEBSITE

25.26% MEDIA

40% LETTER

21.58% I DON'T KNOW



WHAT HAVE YOU shared ONLINE?

Personally Identifying Info: 52.45%
Kids Info: 48.05%
Pet Info: 52.62%
Location: 32.99%
Travel: 42.30%



HAVE YOU experienced

Identity Theft: 15.23%
Online Account Takeover: 22.84%
Direct Attack: 38.41%
Breach: 43.32%

COMMUNICATION THAT CAUSED HARM:



34.31%



15.09%



15.27%



34.13%



20.75%

INFO YOU SHARED ONLINE IS SAFE OR HARMFUL?



SAFE 28.64%



I DON'T KNOW 12.86%



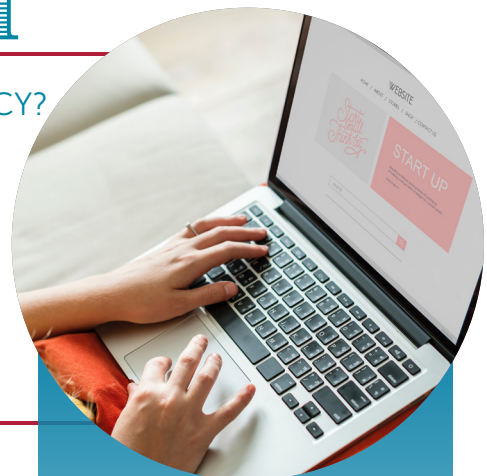
USED AGAINST 51.80%



NOT THOUGHT ABOUT 6.69%

AWARE OF CAMBRIDGE ANALYTICA (FACEBOOK) CHANGES TO PRIVACY?

Yes/No Change	20.83%
Yes/Change	32.29%
Yes/No Log-in	10.07%
No/No change	20.49%
No/Someone Told	3.47%
I Don't Know	12.85%




CONCERNS ABOUT THEIR CHILDREN'S SAFETY?

Yes & I monitor it:	51.52%
Yes & I have no way of addressing it:	27.27%
Not concerned:	12.12%
Not concerned & parents job:	7.07%
Not concerned/ it's up to their parents:	2.02%

DO YOU HAVE children IN YOUR LIFE?

YES	0-5	10.07%
YES	5-12	12.67%
YES	13-18	11.81%
NO		65.45%



In an effort to gain a better understanding of the current sentiment of today's digital native consumers, the Identity Theft Resource Center (ITRC) collaborated with CyberScout® to gauge their attitudes and behaviors in how they manage their personal data on social media channels (Facebook, Twitter, LinkedIn, Instagram and Snapchat). In light of the growing concern of the use (and misuse) of an individual's personal information on social platforms, the ITRC and CyberScout® polled over 600 social media users to gain better insights on how they are managing their own data on their active social media platforms.

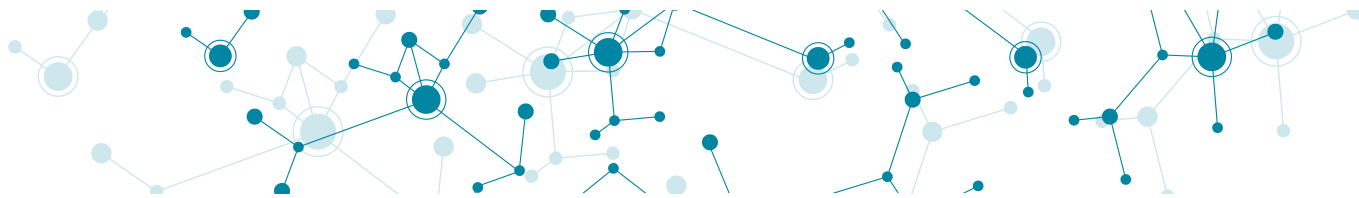
“IN THIS AGE OF DIGITAL NATIVISM, CONSUMERS ARE FINDING THAT THEIR PERSONAL DATA IS A HOT COMMODITY”

“In this age of digital nativism, consumers are finding that their personal data is a hot commodity,” said Eva Velasquez, CEO of the Identity Theft Resource Center. “And as with other commodities, their data is being bought and sold at a tremendous rate—and many times unbeknownst to the individual. We (ITRC) strongly advocate to consumers that they understand how their data is being managed and used by the service provider. Those ‘Terms of Service’ define all of that for the user if they actually read it rather than just clicking accept.”

“Many consumers have privacy and security concerns, yet they continue to share sensitive data publicly, putting themselves at greater risk for cyber threats,” said Matt Cullina, CEO, CyberScout®. “In this shifting social media landscape, it is in their best interest to use the right tools to protect help minimize, monitor and manage online threats.”

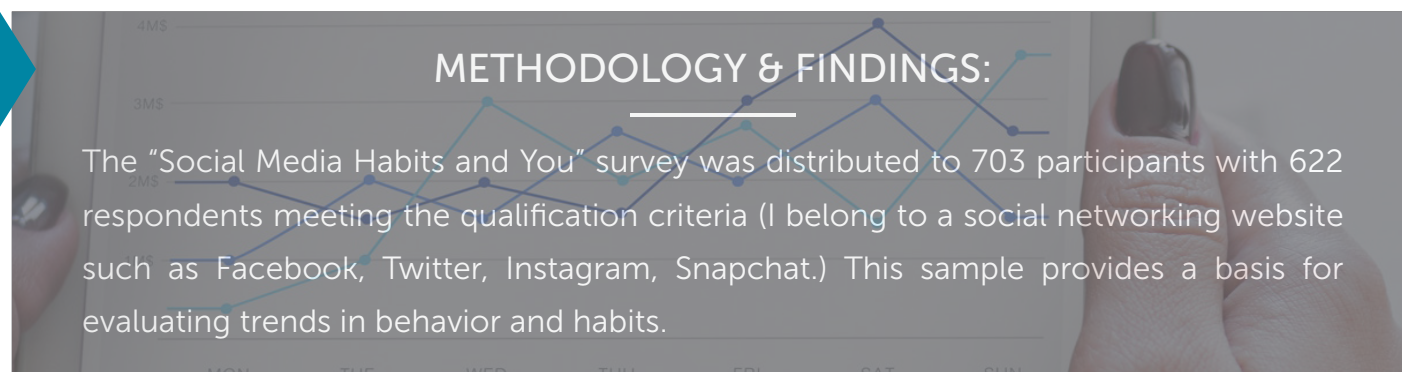
EXECUTIVE SUMMARY

Many of today's social media users are digital natives who aren't defined by their age or generation. Rather, they grew up interacting with the internet, computers and mobile phones. This early exposure gives them a greater understanding of technology, and that familiarity translates into the way they behave on social platforms. They choose to live their lives in real-time, sharing personal information with their networks online.



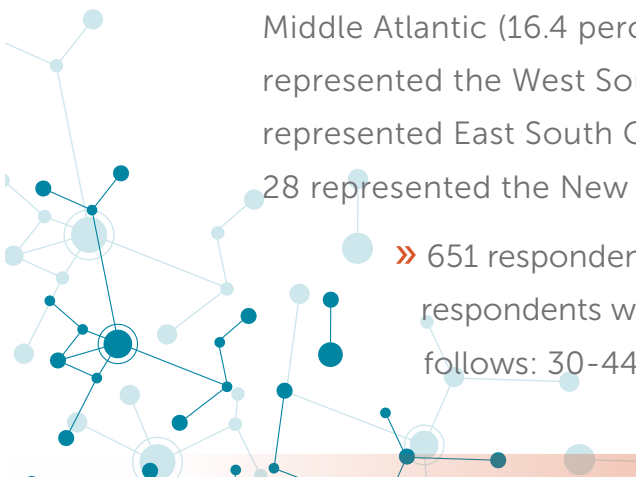
Data breaches on various social platforms such as Reddit and LinkedIn, and data misuse, such as the Facebook-Cambridge Analytica, have put digital natives on notice: The intimate details on their profiles are not so private, and they're being used by more than their friends and followers. Hackers have taken to using the data they scrape to dive deeper into their victims' personal data. Got a new puppy? Heading to your 10-year high school reunion? Just announced the birth of your youngest child? Hackers hit the security question lottery when they mine all those juicy details from a social media profile. That leads to credential cracking—the practice of flooding sites with the usernames and passwords they've acquired to see if they can access other accounts.

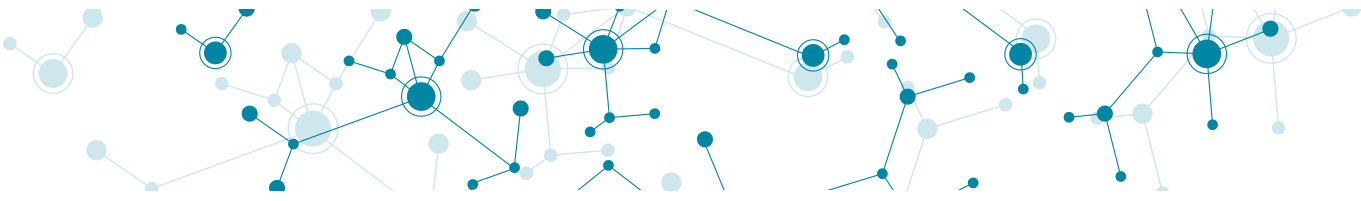
With privacy and security concerns top of mind for digital natives, the ITRC and CyberScout® set out to find out if users have concerns about how their data is being used, as well if they've taken any steps to secure their own privacy on social media channels.



SURVEY POPULATION:

- » 652 of respondents provided their gender; 363 indicated female (55.7%) and 289 male (44.3%).
- » 636 of respondents indicated their regional location; 107 represented the South Atlantic (16.8%), 105 represented the Pacific (16.5%), 104 represented the Middle Atlantic (16.4 percent), 92 represented the East North Central (14.4%), 69 represented the West South Central (10.8%), 56 represented Mountain (8.8%), 44 represented East South Central (6.9%); 32 represented West North Central (5.0%) and 28 represented the New England region (4.4%).
- » 651 respondents provided their ages. Most notably, 43.3 percent of respondents were ages 18-29 years old. Other age categories were as follows: 30-44 (32.1 percent); 45-60 (18.6 percent); over 60 (5.9 percent).





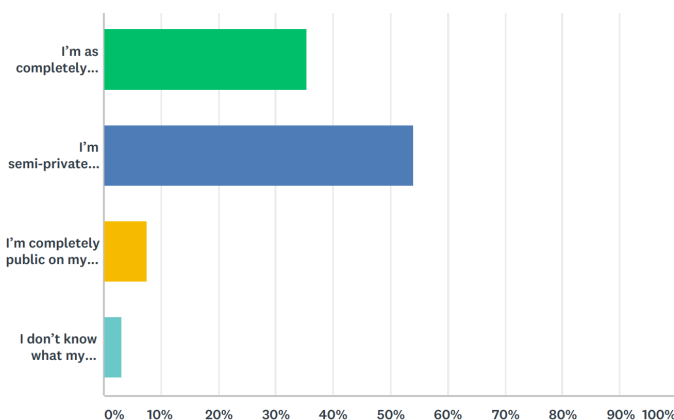
As a part of the survey panel, ITRC asked participants to share their behavior in using social media platforms, their habits in their privacy and security and their perspectives on how their data is used. Lastly, ITRC asked respondents to assess if their behavior and habits may be opened them up to vulnerabilities beyond the social space. The findings are shared in the following assessments.

KEY FINDING 1:

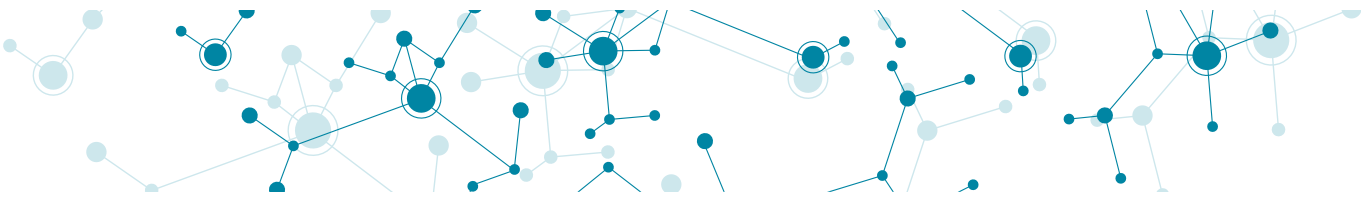
MOST FELT THEY WERE PRIVATE ON THEIR SOCIAL PLATFORMS

What level of privacy do you use on your social media profiles?

The ITRC asked participants to qualify the level of their social media privacy settings on their profiles. Of the 622 respondents, 89.39 percent responded that they utilized the privacy settings. Of that, only 35.37 percent of those classified their privacy setting as completely private. The other 54.02 percent of respondents qualified themselves as “semiprivate,” meaning that some of their personally identifiable information and posts were available publicly beyond their immediate network.



In this day and age of account spoofing and takeovers, it's interesting to see that a majority of users (64.63 percent) continue to allow their data to be shared publicly to some extent. With the rise of data scraping, users that have more data available for public consumption are at a higher risk for exposure of sensitive information. As a baseline, ITRC recommends regularly checking your privacy settings to ensure that they are at the level each consumer is most comfortable. And for maximum privacy and security, setting your social media profiles to the highest privacy setting is most prudent.




Additionally, when asked about their awareness around the Facebook-Cambridge Analytica data misuse and whether that prompted a change in their habits, over half (54.17 percent) of respondents either made no change or were unaware of the incident. The other 45.83 percent of respondents took some sort of action as a result of the incident—either changing their privacy settings or discontinuing using the Facebook login feature on other sites. With this trend, we can see that a majority of digital natives feel that the impact of the misuse (in this case) doesn't negatively impact them enough to warrant a change in behavior.



KEY FINDING 2

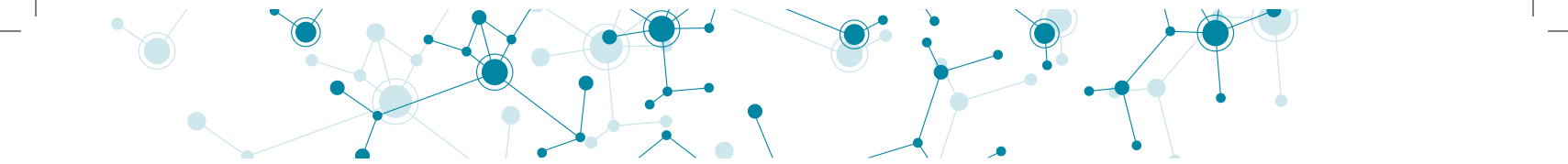
SHARING IS STILL NOT SEEN AS A RISK FOR EXPOSURE

The ITRC asked participants about their sharing habits on their social media channels. The channels with the most frequency of monitoring were Facebook and Instagram (37.26 and 24.26 percent respectively for multiple times a day). It is interesting to note that respondents largely identified that they were not using LinkedIn (47.25 percent), Twitter (41.98 percent) or Snapchat (42.95 percent). And while the monitoring of their channels is inconsistent, we do see that digital natives still are sharing sensitive information. Respondents are continuing to share personally identifiable information such as birth dates, mother's maiden names, phone numbers and images of themselves, family and property (52.45 percent). And don't forget about the specifics around their pets (name, breed, activities, etc.—52.65 percent). All things that can be used as a security challenge question. Respondents who are parents continue to share data about their children as well—including birthdays, pictures, school information, activities, etc. And with over one million children impacted last year by identity theft, it doesn't seem that parents and relatives understand the potential impact for that young person¹.



Location data also continued to rank high on things to share—including check-ins and travel. While this data is less impactful from an identity theft perspective, it does potentially create another point of intrusion by those attempting to social engineer to gain access to other data points.

¹2018 Child Identity Fraud Study, Javelin Strategy & Research



The awareness that social sharing could be used against digital natives seems to be on the rise with 51.80 percent acknowledging that their sharing might be used against them or to their detriment. Over 19 percent either didn't recognize or hadn't thought about the impact of their sharing on their identity.

That doesn't stop at adults. Those participants were also asked about the children in their lives. Over 22 percent said that they had children under the approved age for social media (13 years) using social media. And of those with children using social media, 51.52 percent not only had concerns but took some steps to monitor those children's social media accounts with over 27 percent expressing concern but feeling that they had no way to monitor that activity. Of those stating that they didn't monitor, a number of them said that they felt they could trust their child to make good decisions on social media.



KEY FINDING 3


DIRECT ATTACK IS THE POINT OF ENTRY FOR MOST DIGITAL NATIVES

When asked if digital natives had experienced some type of hostile data compromise (identity theft, account takeover, direct attack or data breach), a majority of participants (81.83 percent) were compromised by a direct attack personally or through a data breach incident. Of those that received a direct personal attack, 34.13 percent received it through an email versus those that received it through a SMS message (15.09 percent) or through an instant messenger platform (15.27 percent). Of those that identified as being impacted by a data breach, 40 percent stated that they heard about it through a notification later from the breached entity.

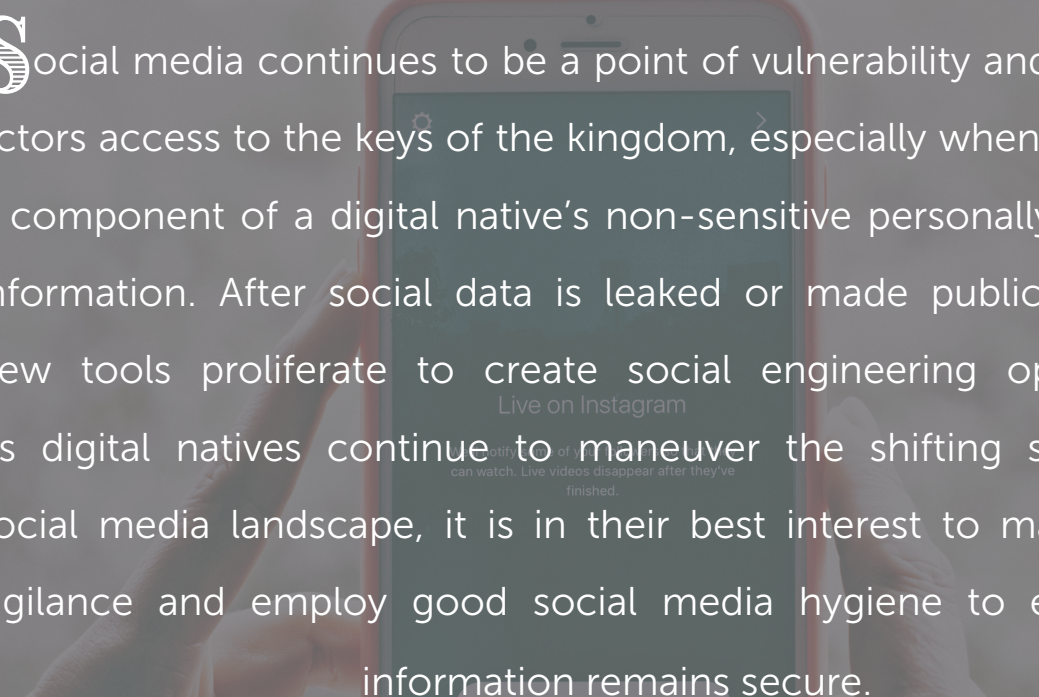




SUMMARY



Social media continues to be a point of vulnerability and allows bad actors access to the keys of the kingdom, especially when it comes to a component of a digital native's non-sensitive personally identifying information. After social data is leaked or made publicly available, new tools proliferate to create social engineering opportunities. As digital natives continue to maneuver the shifting sand of the social media landscape, it is in their best interest to maintain their vigilance and employ good social media hygiene to ensure their information remains secure.



IDENTITY THEFT
RESOURCE CENTER

idtheftcenter.org • 1-888-400-5530

3625 Ruffin Road #204
San Diego, CA 92123

THANKS TO OUR PARTNERS AT:



PG 8 OF 8