Protecting What Matters Most

Insights, Trends, and Perspectives
on Protecting Your Digital World

Ponemon INSTITUTE

The Economic R
on Mobile Devic

Spon ored by L

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Global Agenda Council on the Future of Software & Society

Deep Shift
Technology Tipping Points
and Societal Impact

Survey Report, September

2016
Mining for
Database Gold

CHILD IDENTITY THEFT

New Evidence Indicates Identity Thieves are Tar
Children for Unused Social Security Numbers

By Richard Power,
Distinguished Fellow, Carnegie Mellon CyLab

CONSUMER SENTINEL NETWORK
DATA BOOK
for January – December 2016

Federal Trade Commis
March 2017

Published May 2017
Compiled and distributed by

IdentityForce®

Introduction | Protecting What Matters Most

Welcome to the first edition of IdentityForce's eBook, *Protecting What Matters Most: Insights, Trends, and Perspectives on Protecting Your Digital World*. By gathering some of the most impactful research, data predictions, news articles, analyst insights, and general knowledge around just how much our personal information is being shared through the entire connected digital world, we wanted to provide you with a single resource you can share with your family, friends, customers, and colleagues. With over 50 research and industry reports featured, along with some of our own primary research, *Protecting What Matters Most* will also provide you with ideas on how you can secure your digital footprint.

With virtually every retail transaction, online payment, social media post, online application, medical record, website registration, phone call, and email communication being captured and stored somewhere — now is the time to ensure you are well-informed about what's happening in the digital world surrounding you, your family, your employees, and your customers. While organizations everywhere work hard to keep personal information secure, you'll see in this eBook that it is never completely secure. **Thus, we are each at risk of losing control of what we spend every day of our lives creating: our identity.**

You'll also learn how as technology advances to keep personal information secure, so does the intelligence and technology of those seeking to access it maliciously. The threat continues to increase exponentially, outpacing the solutions designed to combat it. The financial impact can be significant, but the personal impact can take an even greater toll, ripping through an entire family — from children to spouses to grandparents — no one is immune. Compounding the stress is the time and energy needed to reverse the damage, coupled with the emotional trauma from someone taking control of the one thing most personal to you — your identity.

So, sit back and read our new eBook, *Protecting What Matters Most*. If you have any questions or general feedback, don't hesitate to send us an email at eBook@identityforce.com.

And, remember, at IdentityForce, nothing is more personal to us than your identity.

— Steven D. Bearak, CEO, IdentityForce, Inc.

BEARAK'S BELIEFS

Tips for Staying Secure

Here are some helpful suggestions you might want to consider for yourself, and even share with your family, friends, colleagues, employees, and customers, as you peruse this eBook:

- **Start Deleting** | Shed the unwanted risk of computer files you no longer need by deleting excess clutter
- **Create Strong Passwords** | No two passwords should be the same — remember, the most unhackable passwords are 12 characters consisting of random strings of upper and lower case letters, numbers, and symbols
- **Get a Password Manager** | Another great security asset is a password manager, which enables you to create a unique and strong password for every secure website — great for personal and business use!
- **Beware of Public Wi-Fi** | If you absolutely must use public Wi-Fi for sensitive transactions, use a Virtual Private Network (VPN); this encrypts your transmissions; at home ensure your Wi-Fi is secure
- **Stop Clicking Randomly** | Hackers put out links to lure people into clicking — triggering a virus download — so be vigilant
- **Know Your HTTPS** | If you're going to a website that has http instead of https in its URL, realize that no "s" means the site is not secure; this doesn't mean it's malicious, but an "s" is a sign of security reassurance
- **Use 2FA |** Two Factor Authentication is an extra layer of security for your accounts, requiring a one-time code sent to your phone or email address prior to login
- **Do an Operating System Reinstall** | At home, an annual reinstall will clean things up, speed up your computer, and get rid of bloatware; at work, ensure your security policies include standards around requiring regular system maintenance and upgrades
- **Use Credit Card Chips** | Try to make sure that you are using credit cards that have chips, both at work and personally, as they are more secure than swiping
- **Protect Your Home & Business** | Consider adding security cameras; place security company signs and window decals in plain sight; install motion sensor lights and top-grade deadbolts
- **Purchase Identity Theft Protection** | Having a solid service to watch your back, whether purchased for yourself or your family, or rolled out as an employee benefit within the workplace, is a must in today's digital world

Circle of Identity Theft

A Lifelong Process to Protect What Matters Most

The risk of identity theft is present in all the stages of your life. Both adults and children are vulnerable, and it can impact you in different ways. The sharing of Personally Identifiable Information (PII), including Social Security Numbers, phone numbers, home addresses, email addresses, medical records, tax returns, bank accounts, and credit card numbers all create innumerable opportunities for identity thieves to pounce.

Children

- About 1.3 million children are victims of identity theft annually, and 50% are younger than 6 years old
- 19 states in the U.S. require credit bureaus to help parents create credit reports for their children for the express purpose of freezing it*

Young Adults

- Since 2005, there have been over 727 breaches involving educational institutions, with more than 14 million breached records
- The Federal Trade Commission reports college students are about 5 times more likely to be victims of identity theft

Working Adults

- Nearly 75% of identity theft victims are between the ages of 20 and 59, the prime working years
- The percentage of identity theft cases originating in the workplace is estimated to be anywhere between 30% to 50%
- 60% of identity theft complaints in 2016 were from individuals greater than 40 years old

Older Adults

- Seniors are victims of identity theft every four minutes
- 2.6 million seniors are victims of identity theft each year

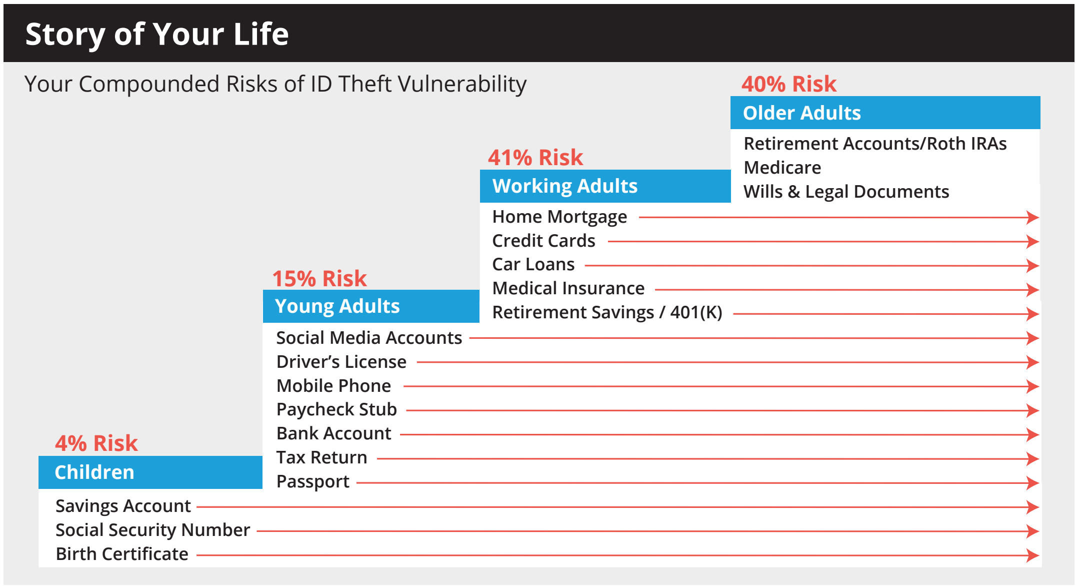
Fun Fact

Your Toys — The New Accomplice

Hello Barbie, Goodbye Privacy? According to researchers, all toys that connect to the Internet are vulnerable to being hacked. This includes Hello Barbie, the world's first interactive Barbie Doll. With these connected toys, thieves are able to steal user-specific information, which can then be used to find someone's household and personal information.

SOURCE | The Huffington Post, Hello Barbie, Goodbye Privacy? Hacker Raises Security Concerns

Story of Your Life



Your Compounded Risks of ID Theft Vulnerability

4% Risk
Children
Savings Account
Social Security Number
Birth Certificate

15% Risk
Young Adults
Social Media Accounts
Driver's License
Mobile Phone
Paycheck Stub
Bank Account
Tax Return
Passport

41% Risk
Working Adults
Home Mortgage
Credit Cards
Car Loans
Medical Insurance
Retirement Savings / 401(K)

40% Risk
Older Adults
Retirement Accounts/Roth IRAs
Medicare
Wills & Legal Documents

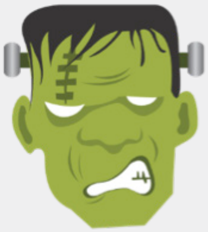
SOURCE | Consumer Sentinel Network Identity Theft Complaints by Victims' Age (2016)

Noteworthy: With over 10,000 identify theft rings in the U.S. looking for ways to steal the PII of you and your family members, it is virtually impossible to protect all aspects of your identity in the public and private domains. Identity thieves never rest. Thus, proactive monitoring of your identity throughout your life is necessary to safeguard your personal information, give you peace of mind, and mitigate your risk.

*Those states are: Arizona, Delaware, Florida, Georgia, Illinois, Indiana, Iowa, Louisiana, Maryland, Michigan, Montana, Nebraska, New York, Oregon, South Carolina, Texas, Utah, Virginia, and Wisconsin.

Are You Being Targeted?

A Myriad of Scams = Exposure at Every Angle



Fun Fact

Synthetic: The Frankenstein of Identity Theft

Synthetic identity theft occurs when thieves create new identities using a combination of real and fake information. This compiled identity can then be used to obtain credit, open bank accounts, and even obtain driver's licenses and passports. To avoid possible detection, fraudsters often seek out the SSNs of people who don't make use of credit, including children and the elderly. By some reports, synthetic identity fraud now accounts for 85% of all identity fraud in the U.S., costing an estimated $2 billion a year.

SOURCE | ABC News

> *"We've heard from victims who actually compare [identity theft] to having a disease where they feel that their identity theft issues are in remission, but they're never fully cured.* ***You can think you've taken care of it, and then it pops up again a year or so later."***

~ Eva Velasquez,
President & CEO,
Identity Theft
Resource Center

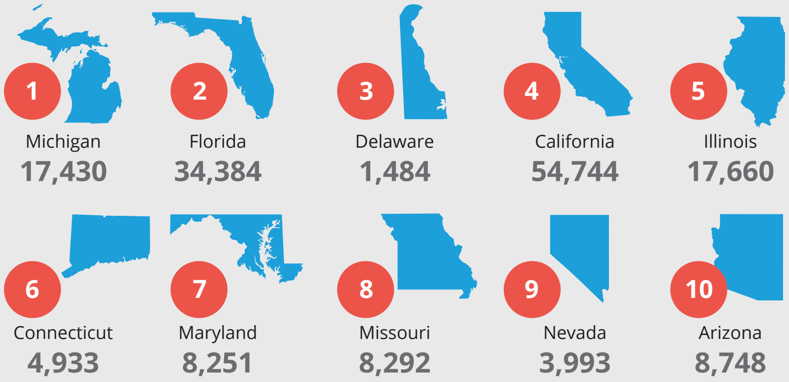
The reality of identity theft is that it's so much more than scams, credit card fraud, and fake e-mails — it's woven deep into our everyday lives. Identity thieves are everywhere, using a never-ending array of new techniques — vishing, phishing, SMiShing, skimming, pharming, social engineering, and more. What's even more alarming is that your everyday activities may unwittingly open you up to identity theft.

- The Nilson Report, a leading source of news and analysis of the global card and mobile payment industries, projects worldwide credit card fraud will reach $31.67 billion by 2020
- International travelers are nearly 3 times more likely to experience identity fraud
- Medical identities are 20 to 50 times more valuable to criminals than financial identities; 65% of medical identity theft victims had to pay an average of $13,500 to resolve the crime
- 60% to 80% of SSNs are estimated to have been stolen by hackers according to the lead data scientist for the Verizon Breach Report
- IBM found that nearly 40% of all spam emails sent in 2016 contained ransomware

Noteworthy: Anyone who has experienced identity theft first-hand knows it's a very stressful and potentially costly experience. 36% of identity theft victims reported moderate or severe emotional distress, 66% experienced direct financial losses, and victims spent 33 to 600+ hours on average to restore their identity. In a recent study of American fears, more than 37% of those surveyed ranked identity theft as something they are "very afraid" or "afraid" of. Although identity theft continues to flourish, having access to a 24x7 monitoring service can allay this fear by providing an early warning with rapid notification when your personal information is at risk.

Where Do You Live?

Top 10 Highest Ranking States for Identity Theft Complaints *As a Percentage of Total Population*



1	Michigan	17,430
2	Florida	34,384
3	Delaware	1,484
4	California	54,744
5	Illinois	17,660
6	Connecticut	4,933
7	Maryland	8,251
8	Missouri	8,292
9	Nevada	3,993
10	Arizona	8,748

High Risk Factors

Some states seem especially prone to identity theft, and there are several factors that tend to lead to higher fraud statistics. For example, Florida comes in at #2 as it is not only one of the most populous states, but it has a large number of retirees who are often targets of medical identity theft, bill collection scams, and tax identity theft. However, it's a fact that residents of any state, town or neighborhood can become part of the identity theft statistics. Protect yourself by employing strong passwords on your digital devices, being suspicious of any information requests by phone or email, and maintaining safe online behavior.

SOURCE | Consumer Sentinel Network State Complaint Rates (2016)

Your Digital Footprint | A Gateway for Personal Identity Exploitation

Fun Facts

Your Devices May Be Smart — But Are They Loyal?

Our modern society is full of innovation — different types of smart devices are being introduced to the market — Fitbits, smart cars, Amazon Echo, and Nest home devices to name just a few. These smart devices monitor your behavior and "learn" about your daily habits and preferences.

- **Interconnected Devices** | In 2017 a household with two teenagers will have 25 Internet connected devices; in 2022 this number will rise to 50
- **The Internet of Things (IoT)** | By 2022, 10% of the world's population will be wearing clothes connected to the internet; 10% of reading glasses will be connected to the internet by 2023
- **Vulnerabilities** | With 20 billion+ IoT devices online by 2020, they will be the top source for vulnerability and hacks related to cloud attacks

DATA SOURCES |

- OECD Insights, Smart Networks: Coming Soon to a Home Near You
- Business Insider, Nordic, 21 Technology Tipping Points We Will Reach by 2030
- Fortinet 2017 Cybersecurity Predictions: Accountability Takes the Stage

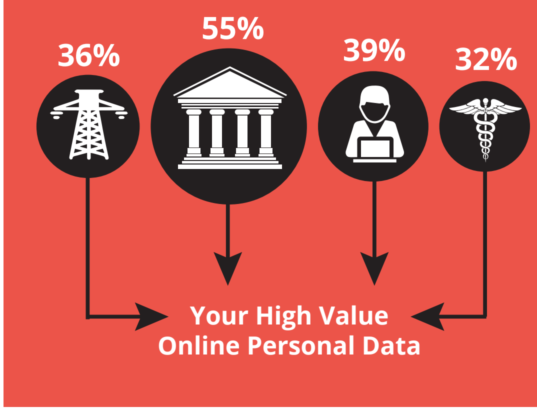
Your "digital footprint" can be assembled by combining data from all of your electronic devices — mobile phones, laptops, and tablets — along with any smart devices you may use (e.g., your appliances, car, and home thermostat), cloud apps, and even social networks. From your doctor's office to your favorite retailer to even the company you work for — they all maintain your personal data.

By 2020 the digital universe — the data we all create and copy annually — will reach 44 zettabytes, or 44 trillion gigabytes, according to IDC. To put this in perspective, one zettabyte is equivalent to the data on about 250 billion DVDs. Much of this increase is due to the surge of personal data. 75% of all data in the digital universe is created by consumers versus companies.

- 88% of mobile device users store a wealth of private and personal information on them
- LinkedIn was a key reconnaissance tool for the cybercriminals who executed Anthem Health's 2015 breach and its 80 million stolen records
- Facebook uses the 98 personal data points it collects from members to track on-site activity, location settings, and internet connection details in order to display targeted ads

Noteworthy: While digital transformation is an exciting step forward in technology, it's also an area that requires the vigilant monitoring and protection of Personally Identifiable Information (PII) by all digital users. More than 50% of the information in the digital universe that needs protection is not being protected — including PII, corporate financial data, medical records, and user account information. One place to start? Stop sharing passwords — 95% of people share up to 6 passwords with others, including financial, business, social media, and entertainment account passwords.

Personal Data Shared in High Value Accounts



Highly sensitive records can be especially damaging if others gain access to them and exploit them. A Pew Research Center survey asked about four general categories of these "high value" accounts and found that:

- 55% of Americans report having an online account with banks or other financial service providers
- 36% have an online account with household utility providers
- 32% have an online account with their healthcare providers
- 39% have some other kind of online account that involves bill payments or transactions

SOURCE | Pew Research Center, Americans and Cybersecurity

Getting Behind the Firewall | When Data Gets Breached

The Facts

Breach Blues

- 95% of data breach attacks on enterprise networks start with spear phishing, a targeted email engineered to look legitimate and fool even tech-savvy users; the email installs malware and tries to gain system access
- Gemalto's research shows that most data breaches are now perpetrated for identity theft rather than stealing credit card information

SOURCE | 10 Facts You Need to Know About Data Breaches

The inherent value of identity theft protection becomes clear when we lose control of our personal information in the public domain. Data breaches have become part of the digital landscape. Nearly every day there is a new headline about a large merchant, healthcare provider, or school suffering from a data breach. The stats are alarming — and no organization is immune. Not even the U.S. government is safe — in 2016 more than 100 million Social Security Numbers were leaked, per the American Institute of CPAs (AICPA).

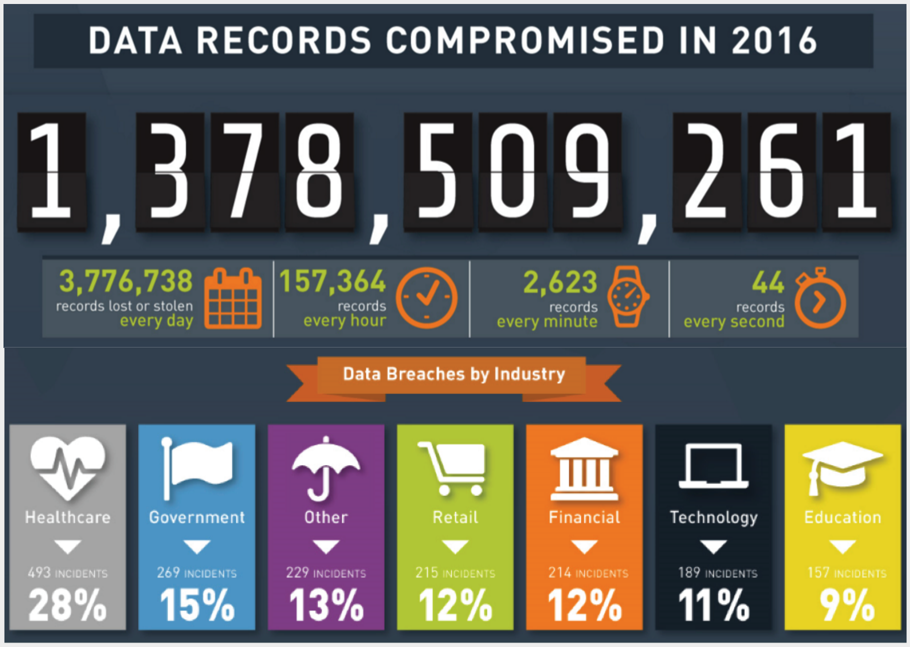
Organizations are spending billions of dollars on corporate IT security, yet they still fall prey to hackers and cybercriminals. In 2016, 225 organizations worldwide were impacted by data breaches every day, more than 20 times the rate of the consumer data breaches reported.

To paraphrase the famous bank robber Willie Sutton, "I go where the money is," and so do today's hackers. Fraudsters go after the "money making" personal and corporate data maintained inside the four walls of the enterprise.

- Data breaches increased by 40% in 2016
- The average total data breach cost = $7.01 million
- Your chances of being affected by identity theft are 1-in-3 if your information has been part of a breach
- 62% of security pros don't know where their sensitive data is being stored; analysts at Forrester report that organizations struggle with understanding and controlling sensitive data

Data Breaches by the Numbers

Keep in Mind! Due to legal requirements, not all breaches are disclosed.



SOURCE | gemalto

Noteworthy: When identity theft rears its head in the corporate environment, the impact is staggering. The toll on employee productivity and absenteeism is clear — whether it's a range of hours (from 33 to over 600) dedicated to completing forms, sending emails, copying documents, and running to the post office — or dealing with the emotional stress of taking control of a situation that is clearly out of control. Resolving identity theft also demands a lot of direct telephone interaction with a live person, typically during working hours. This means when an employee has his or her identity stolen, there's also an innocent bystander about to become collateral damage: **the employer**. This is why identity theft protection, offered by 35% of employers in 2015, could double to nearly 70% by 2018.

Mobile Mania

Navigating Mobile in the Workplace & Beyond

Fun Fact

Are You Literally Attached to Your Smartphone?

It's projected that the first implantable mobile phone will become commercially available in 2025. The device will potentially be able to track a person's health more accurately, while also allowing them to communicate thoughts via brainwaves or signal instead of verbally.

SOURCE | Business Insider, Nordic: The World Economic Forum's Global Agenda Council on the Future of Software & Society

Mobile phones are now a mainstay of everyone's existence. According to Cisco, "By 2021, more members of the global population will be using mobile phones (5.5 billion) than bank accounts (5.4 billion), running water (5.3 billion), or landlines (2.9 billion)." The average person checks his or her phone 47 times per day. For 18 to 24-year-olds that number rises to 82.

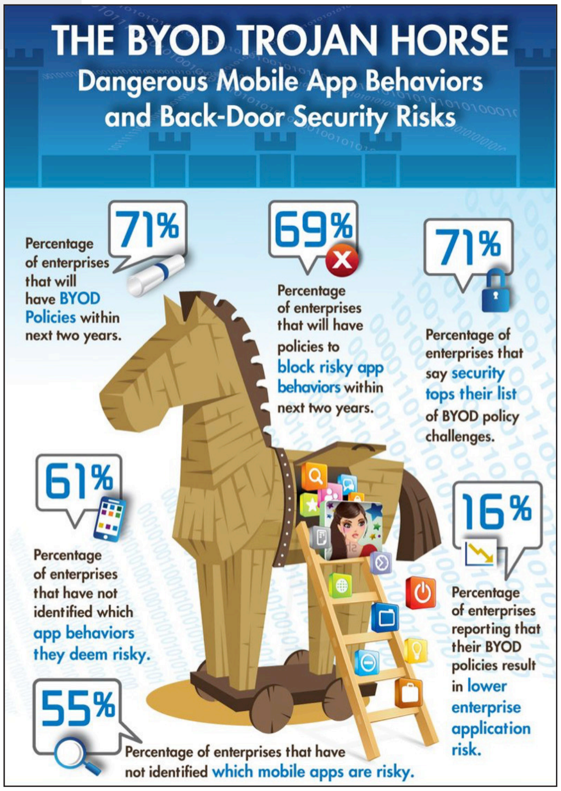
Let's look at the impact of mobile in the workplace. A study by Bank of America found that 55% of respondents sleep with their smartphones on their nightstands to avoid missing a call, text message, or other update during the night. The devices are also the first thing on their minds in the morning: while 10% reported thinking of their significant other, 35% reserved their first thought of the day for their smartphone.

According to Forsythe, a leading enterprise IT company, "Many people expect that iPhone or Android devices are secure by default, when in reality it is up to the user to make security configuration changes. With the right (inexpensive) equipment, hackers can gain access to a nearby mobile device in less than 30 seconds and either mirror the device and see everything on it, or install malware that will enable them to siphon data from it at their leisure." Here are just some of the ways the workplace is at risk:

- The average large enterprise has 2,000+ unsafe mobile apps installed on employee devices
- 52% of employees in a recent mobile security survey said they have access to sensitive work-related data such as employee's Personally Identifiable Information (PII); 43% have access to customer data; and 33% have access to classified or confidential information
- 74% of IT leaders from global enterprises report that their organizations have experienced a data breach as a result of a mobile security issue

Got BYOD? Don't let it be Bring Your Own Demise!

Organizations with a Bring Your Own Device (BYOD) strategy should stand vigilant. Gartner predicted that by the end of 2016, 50% of all employers will require you to BYOD. However, the Security for Business Innovation Council—a team composed of Global 1000 information security leaders—has a strong word of caution for these employers, as they cite lost or stolen BYODs as its #1 concern. The danger here is clear: Although BYODs that go missing certainly contain sensitive data, according to Osterman Research, less than 1 in 4 can be remotely wiped. That spells data breach!


THE BYOD TROJAN HORSE
Dangerous Mobile App Behaviors and Back-Door Security Risks
71%
Percentage of enterprises that will have BYOD Policies within next two years.
69%
Percentage of enterprises that will have policies to block risky app behaviors within next two years.
71%
Percentage of enterprises that say security tops their list of BYOD policy challenges.
61%
Percentage of enterprises that have not identified which app behaviors they deem risky.
16%
Percentage of enterprises reporting that their BYOD policies result in lower enterprise application risk.
55%
Percentage of enterprises that have not identified which mobile apps are risky.

SOURCE | Flexera Software's 2015 Application Usage and Value Survey, prepared jointly with IDC

Noteworthy: The prevalence of mobile devices, both in the workplace and throughout our society, means our PII is everywhere. 70% of the world population will be using a smartphone within the next three years — and right now, more Google searches are happening on smartphones than on desktop computers. Mobile is certainly everywhere, and that means your digital footprint exists everywhere. In order to protect yourself, and your employees, be sure to regularly refresh your company policies, train and test your employees on security measures, share with them best practices around social media, and work with your Human Resources (HR) department to identify potential employee behavior that may pose a security risk.

Want to Know More?

ABC News
Synthetic Identity Fraud: A New Kind of Costly ID Theft You've Never Heard of, September 2015
http://abcnews.go.com/Business/synthetic-identity-fraud-kind-costly-id-theft-youve/story?id=32596029

Bankrate
What Happened to the Mobile Wallet Revolution? October 2016
http://www.bankrate.com/card-shark/what-happened-to-the-mobile-wallet-revolution/

Bluefin Payment Systems
Higher Education — An Attractive Target for Data Breaches, August 2015
https://www.bluefin.com/bluefin-news/higher-education-an-attractive-target-for-data-breaches/

Bureau of Justice Statistics
17.6 Million U.S. Residents Experienced Identity Theft in 2014, September 2015
https://www.bjs.gov/content/pub/press/vit14pr.cfm

Victims of Identity Theft, 2014
https://www.bjs.gov/content/pub/pdf/vit14.pdf

Business Insider, Nordic
21 Technology Tipping Points We Will Reach by 2030, December 2016
http://nordic.businessinsider.com/21-technology-tipping-points-we-will-reach-by-2030-2016-12/

Cisco
Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021, February 2017
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf

CMSA Today
Zettabytes and Other Interesting "Big Data" Facts, March 2016
http://www.naylornetwork.com/cmsatoday/articles/index-v2.asp?aid=367612&issueID=39069

CSO
Study: 62% of Security Pros Don't Know Where Their Sensitive Data Is, January 2017
http://www.csoonline.com/article/3161028/data-protection/study-62-of-security-pros-dont-know-where-their-sensitive-data-is.html?upd=1485525164109

Daily Mail
Tired of Seeing Annoying Adverts on Facebook? Here's How to Fix It, August 2016
http://www.dailymail.co.uk/sciencetech/article-3753526/What-Facebook-REALLY-knows-Firm-reveals-98-pieces-data-uses-target-ads-them.html#ixzz4cS6yahj1

Dark Reading
Why Social Media Sites are the New Cyber Weapons of Choice, September 2016
http://www.darkreading.com/attacks-breaches/why-social-media-sites-are-the-new-cyber-weapons-of-choice/a/d-id/1326802

Deloitte
2016 Global Mobile Consumer Survey: US Edition, 2016
https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-us-edition.html

Detroit Free Press
1.3 Million Kids Have Identity Stolen Annually, 50% Under 6-Years-Old, August 2016
http://www.freep.com/story/money/business/2016/08/28/child-id-theft-problem/89352016/

Digital News Asia
70% of World's Population Using Smartphones by 2020: Ericsson, June 2015
https://www.digitalnewsasia.com/mobility/70pc-of-world-population-using-smartphones-by-2020-ericsson

Experian
Protecting Seniors from Identity Theft, September 2016
http://www.experian.com/blogs/ask-experian/protecting-seniors-from-identity-theft/

eWeek
IRS Tax Refund Fraud Expected to Hit Hard Again in 2016, March 2016
http://www.eweek.com/security/irs-tax-refund-fraud-expected-to-hit-hard-again-in-2016.html

Federal Trade Commission
Consumer Sentinel Network Data Book, March 2017
https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

Flexera Software
The BYOD Trojan Horse, April 2015
http://blogs.flexerasoftware.com/application-readiness/2015/04/mobile-application-management-and-byod-infographic.html

Forbes
New Study Says over 2 Million Americans are Victims of Medical Identity Theft, February 2015
https://www.forbes.com/sites/danmunro/2015/02/23/new-study-says-over-2-million-americans-are-victims-of-medical-identity-theft/#354ac8a115a0

Fortinet
Fortinet 2017 Cybersecurity Predictions: Accountability Takes the Stage, November 2016
https://blog.fortinet.com/2016/11/15/fortinet-2017-cybersecurity-predictions-accountability-takes-the-stage

Forsythe Focus
Mobile Device Security in the Workplace: 5 Key Risks and a Surprising Challenge, June 2016
http://focus.forsythe.com/articles/55/Mobile-Device-Security-in-the-Workplace-5-Key-Risks-and-a-Surprising-Challenge

Gemalto Breach Level Index
2016 Annual Infographic
http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2016-Gemalto-1500.jpg

GuardChild
Identity Theft Statistics
https://www.guardchild.com/identity-theft-statistics/

IDC and EMC
The Digital Universe of Opportunities, Rich Data and the Increasing Value of the Internet of Things, April 2014
https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

IdentityForce, Inc.
Medical Identity Theft Is on the Rise
https://www.identityforce.com/medical-identity-theft

Recent Data Breach Roundup: January 2017
https://www.identityforce.com/blog/recent-data-breach-roundup-january-2017

The Fear of Identity Theft: Unprecedented U.S. Study Ranks It within Top 10 Fears, October 2016
https://www.identityforce.com/business-blog/fear-identity-theft-ranks-within-top-10-fears

What are Your Odds of Getting Your Identity Stolen? January 2016
https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics

Infosecurity
Global Orgs See 82K Cyber Incidents in 2016, January 2017
https://www.infosecurity-magazine.com/news/global-orgs-see-82k-cyber/

ISBuzz News
User Information at Risk as Nine out of Ten Store Personal Data on Digital Devices, February 2016
http://www.informationsecuritybuzz.com/study-research/user-information-at-risk-as-nine-out-of-ten-store-personal-data-on-digital-devices/

KentWired.com
College Students More Likely to be Victims of Identity Theft, March 2015
http://www.kentwired.com/videos/article_4a0ca93e-c601-11e4-baaf-1b35893339a7.html

LastPass
Infographic: Keep Your Friends Close & Your Passwords Closer, February 2016
https://blog.lastpass.com/infographic-keep-your-friends-close

LevelTen
8 Signs You're too Attached to Your Mobile Phone, May 2013
http://getlevelten.com/blog/julie-miller/8-signs-youre-too-attached-your-mobile-phone

Living Rich with Coupons
Identity Theft and Children: Scary Statistics You Need to Know, May 2016
http://www.livingrichwithcoupons.com/2016/05/identity-theft-children-scary-statistics-need-know.html

Lookout Blog
Surprising New Research: Three-quarters of IT Leaders Have Experienced a Mobile Data Breach, October 2015
https://blog.lookout.com/blog/2015/10/05/mobile-data-breach-report/

Los Angeles Times
What Travelers Need to Know to Guard Against Identity Theft, May 2015
http://www.latimes.com/travel/la-tr-money-20150524-story.html

LVB.com
Identity Theft Takes its Toll on Our Workplaces, July 2013
http://www.lvb.com/article/20130715/LVB01/307119988/identity-theft-takes-its-toll-on-our-workplaces

MIT Technology Review
Big Data: Creating the Power to Move Heaven and Earth, September 2014
https://www.technologyreview.com/s/530371/bigdata-creating-the-power-to-move-heaven-and-earth/

NBC News
Ransomware: Now a Billion Dollar a Year Crime and Growing, January 2017
http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

NPR
Theft of Social Security Numbers is Broader Than You Might Think, June 2015
http://www.npr.org/sections/alltechconsidered/2015/06/15/414618292/theft-of-social-security-numbers-is-broader-than-you-might-think

OECD Insights
Smart Networks: Coming Soon to a Home Near You, January 2013
http://oecdinsights.org/2013/01/21/smart-networks-coming-soon-to-a-home-near-you/

OPSWAT
10 Facts You Need to Know About Data Breaches, September 2015
https://www.opswat.com/blog/10-facts-you-need-know-about-data-breaches

Pew Research Center
Americans and Cybersecurity, January 2017
http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Ponemon Institute and IBM
2016 Cost of Data Breach Study: United States
https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-2039&S_PKG=ov49599

Ponemon Institute and Lookout
The Economic Risk of Confidential Data on Mobile Devices in the Workplace, February 2016
https://info.lookout.com/rs/051-ESQ-475/images/Ponemon%20Report%20Enterprise%20FINAL.pdf

SHRM Society for Human Resource Management – The SHRM Blog
Identity Theft at Work — How to Protect Yourself and Employees, March 2015
https://blog.shrm.org/blog/identity-theft-at-work-how-to-protect-yourself-and-employees

SHRM Society for Human Resource Management
The Case for Legal Services and ID Theft Benefits, December 2015
https://www.shrm.org/ResourcesAndTools/hr-topics/benefits/Pages/legal-services.aspx

TechRepublic
10 Ways BYOD Will Evolve in 2016, January 2016
http://www.techrepublic.com/blog/10-things/10-ways-byod-will-evolve-in-2016/

TechTarget SearchSecurity
BYOD Security Strategies: Balancing BYOD Risks and Rewards, January 2013
http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards

The Huffington Post
Hello Barbie, Goodbye Privacy? Hacker Raises Security Concerns, November 2015
http://www.huffingtonpost.com/entry/hello-barbie-security-concerns_us_565c4921e4b072e9d1c24d22

The New York Times
Identity Theft Poses Extra Troubles for Children, April 2015
https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html?_r=0

The Real Strategy
100 Million Social Security Numbers Hacked for Sale Online for $20,000 USD, September 2016
https://therealstrategy.com/100-million-social-security-numbers-hacked-sale-online-20000-usd/

Think with Google
How People Use Their Devices, October 2016
https://www.thinkwithgoogle.com/articles/device-use-marketer-tips.html

Time
Study: 10,000 Identity Theft Rings in U.S, November 2012
http://business.time.com/2012/11/20/study-10000-identity-theft-rings-in-u-s/

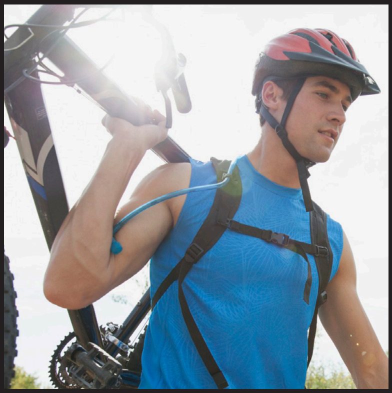
USA Today
Is Your Child Already a Victim of Identity Theft? September 2015
http://www.usatoday.com/story/money/personalfinance/2015/09/11/children-victims-identity-theft/72091926/

Veracode
Average Large Enterprise Has More Than 2,000 Unsafe Mobile Apps Installed on Employee Devices, March 2015
https://www.veracode.com/average-large-enterprise-has-more-2000-unsafe-mobile-apps-installed-employee-devices

Visual Rhetoric/Visual Communications
Iconography of the U.S., May 2014
https://swojtusik946.wordpress.com/2014/05/05/iconography-of-the-u-s/

Voice & Data
Mobile Phone Use Expected to Top 5.5 Billion Devices by 2021: Cisco, February 2017
http://www.voicendata.com/mobile-phone-use-expected-to-top-5-5-billion-devices-by-2021-cisco/

Willis Towers Watson's 2016 VBS Survey
Employers Expand Use of Voluntary Benefits, March 2016
https://www.willistowerswatson.com/en/press/2016/03/employers-expand-use-of-voluntary-benefits



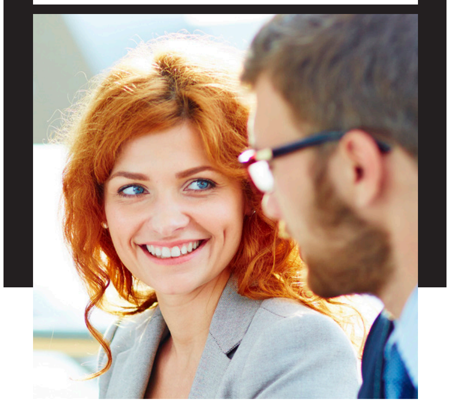
"After five years of relatively small growth — or even decreases in fraud — this year's findings drives home that fraudsters never rest, and when one area is closed, they adapt and find new approaches. The rise of information available via data breaches is particularly troublesome for the industry and a boon for fraudsters. To successfully fight fraudsters, the industry needs to close security gaps and continue to improve, and consumers must be proactive too."

~Al Pascual
Senior Vice President
Research Director and
Head of Fraud & Security
Javelin Strategy & Research

"Imagine making 20 copies of your house keys and giving them to 20 strangers — that's what you are doing when you re-use the same password on all of your accounts, which 40% of people do. Exploiting the bad habit of re-using passwords allows hackers to log directly into your accounts undetected and collect your entire identity for a big payoff later."

~David Sawin
Head of Distribution
Partnerships

dashlane



"I can't stress how important it is to make sure you are doing everything possible to stay protected — physically and digitally. More than a dozen free apps can turn most cellphones into a scanner that can steal credit and debit card information from an unsuspecting victim without the crook ever touching the card. Unfortunately, it's impossible to be 100% protected, but taking the proper steps to prevent and deter this new breed of criminal should be on everyone's to-do list. When an identity theft event occurs, catching it quickly can save you hundreds — if not thousands — of dollars and countless hours repairing the resulting damage. Having a company with a proven track record monitoring your identity and credit is no longer a luxury, but a necessity that you cannot afford to overlook."

~Chris Gilpin
President

SIGNALVAULT

About IdentityForce

For nearly 40 years, IdentityForce, Inc. has provided best-in-class, highly scalable, award-winning identity theft, privacy, and credit protection solutions to consumers, businesses, and government agencies. A pioneer of identity protection, IdentityForce's innovation and customer-centric approach has made the company a trusted partner for both organizations and individuals. IdentityForce also provides custom-tailored programs to organizations enabling them to build closer relationships and additional revenue streams. In 2015, the U.S. government awarded IdentityForce elite Tier-One status as an approved provider of identity protection services for data breaches affecting over 21.5 million people. Visit www.identityforce.com to learn more.

2017 STEVIE SILVER WINNER FOR SALES & CUSTOMER SERVICE | TopTenReviews GOLD 2016 | parent tested parent approved WINNER | BBB A+ ACCREDITED BUSINESS | 1ST PLACE WINNER ASECURELIFE.COM | GSA | best TOP 3 RANKED COMPANY 2015 bestIDTheftcompanys.com | 2016 JAVELIN Identity Protection Leader

Find **IdentityForce** on: