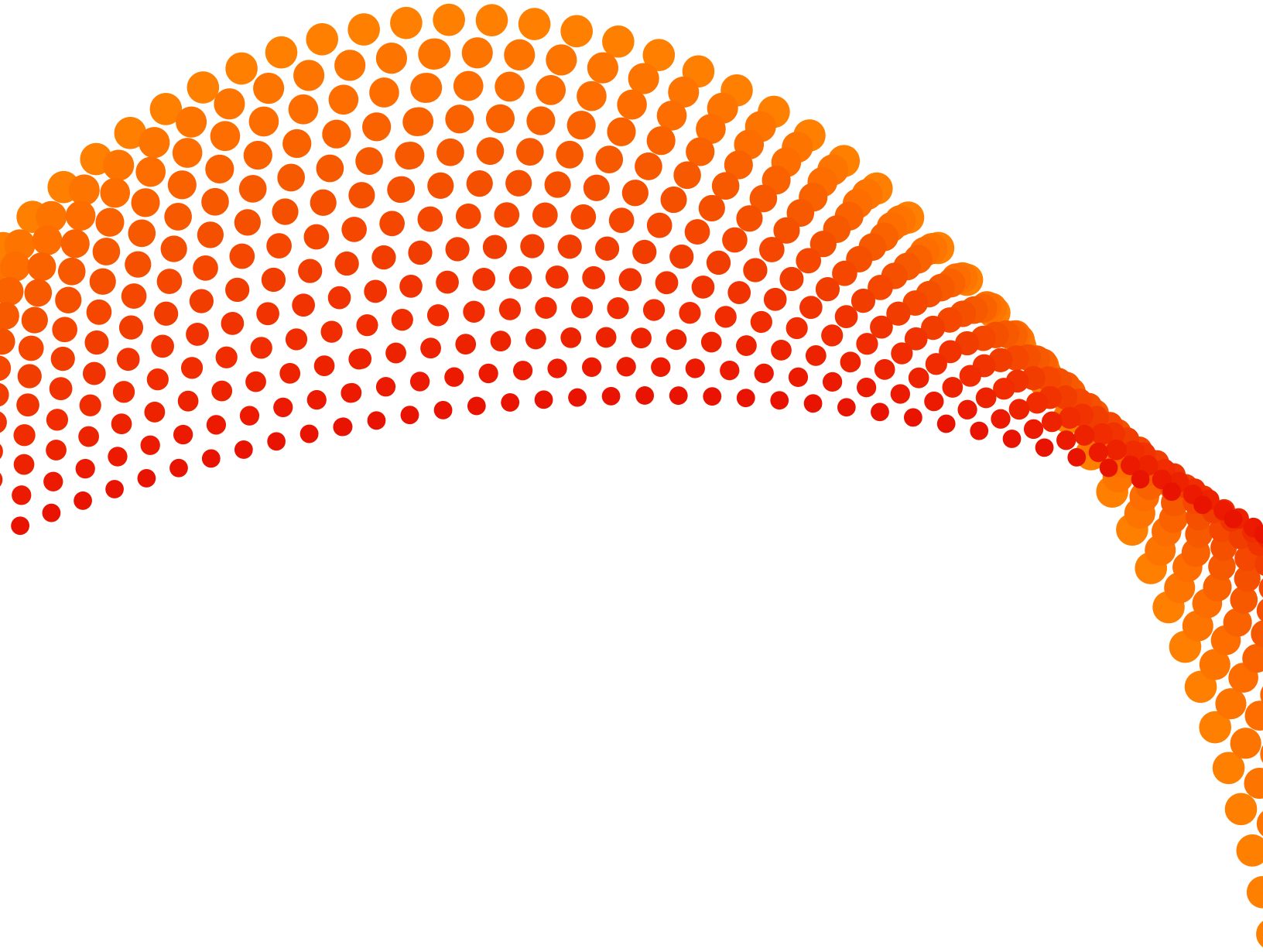


DATA PRIVACY DAY IS JANUARY 28TH

IT'S TIME TO GET #PRIVACYAWARE!

CHAMPION BACKGROUNDER

DATA PRIVACY DAY

WHAT IS DATA PRIVACY DAY?

Led by the National Cyber Security Alliance (NCSA), Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. Observed annually on January 28, Data Protection Day commemorates the Jan. 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection.

Each year, data breaches continue to grow in size and scope – exposing consumer's private data and valuable business information assets. Against this backdrop, Data Privacy Day helps spread awareness about privacy and educates citizens on how to secure their personal information. It also works to encourage businesses to be more transparent about how they collect and use data.

To promote these goals, Data Privacy Day's theme is "Respecting Privacy, Safeguarding Data and Enabling Trust.

> ***"Data Privacy Day is a concerted effort to make businesses more aware of the importance of respecting and protecting personal information," says Kelvin Coleman, executive director of NCSA. "More than ever before, businesses are collecting and using personal data. Data Privacy Day provides an annual opportunity to encourage businesses to improve data privacy and security practices and inform consumers about ways their personal information can be used and shared by businesses."***

WHY WE SHOULD CARE ABOUT ONLINE PRIVACY

Today we conduct much of our lives on the internet and on our connected devices, yet few people understand that enormous amounts of personal information is collected and shared. This data can be stored indefinitely, and our personal information can be used in both beneficial and unwelcome ways. Even seemingly innocuous information – such as your favorite restaurants or items you purchase online – can be used to make inferences about your socioeconomic status, preferences and more.

Many companies have the opportunity to monitor their users and customers' personal behavior and sell the data for profit. In order to make informed decisions and understand the true value of their data, consumers need to understand how it is collected, used and shared.

WHAT IS THE DIFFERENCE BETWEEN PRIVACY AND SECURITY?

Security refers to the ways we protect ourselves, our property and personal information. It is the first level of defense against unwanted intruders. Privacy is our ability to control access to our personal information.

PRIVACY TIPS FROM THE NCSA

ADVICE FOR ORGANIZATIONS: PRIVACY IS GOOD FOR BUSINESS

Create a culture of privacy in your organization. Educate employees on the importance and impact of protecting consumer and employee information as well as the role they play in keeping it safe.

Top Three Tips for Transparency and Trust

- **If you collect it, protect it.** Follow reasonable security measures to keep individuals' personal information safe from inappropriate and unauthorized access.
- **Be open and honest about how you collect, use and share consumers' personal information.** Think about how the consumer may expect their data to be used, and design settings to protect their information by default.
- **Build trust by doing what you say you will do.** Communicate clearly and concisely to the public what privacy means to your organization and the steps you take to achieve and maintain privacy.

ADVICE FOR CONSUMERS: SAFEGUARDING YOUR DATA

Personal info is like money: value it. Protect it. Information about you, such as your purchase history or location, has value — just like money. Be thoughtful about who gets that information and how it's collected through apps and websites. You should delete unused apps, keep others current and review app permissions.

CONSUMER-FRIENDLY TIPS TO HELP PROTECT YOUR PRIVACY

- **Share with care.** Think before posting about yourself and others online. Consider what it reveals, who might see it and how it could be perceived now and in the future.
- **Own your online presence.** Set the privacy and security settings on websites and apps to your comfort level for information sharing. Each device, application or browser you use will have different features to limit how and with whom you share information.
- **Think before you act:** Information about you, such as the games you like to play, your contacts list, where you shop and your geographic location, has tremendous value. Be thoughtful about who gets that information and understand how it's collected through websites and apps.
- **Lock down your login:** Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Strengthen online accounts and use strong authentication tools like a unique, one-time code through an app on your mobile device.

STORY IDEAS

Privacy affects every part of our life – at home and at work. To help encourage #PrivacyAware habits at home and on the job, NCSA has compiled a cross-section of story ideas about everyday privacy concerns and challenges.

ENTERPRISE AND SMALL BUSINESS

- What Do You Need to Know About GDPR or the new California Consumer Privacy Act
- Privacy, Customer Data and Customer Loyalty – How they Impact Eachother
- Artificial Intelligence, Machine Learning and Privacy, What Do You Need to Know
- Improving Your Company's Privacy Posture

RANSOMWARE

- Attacked by Ransomware? Here's What to Do.
- Ransomware is Surging. Here's Why.

EDUCATION

- Three Questions to Ask Your School District About Privacy
- Connected Classrooms and Students: Is Your Child's School Protecting Her Data

HEALTHCARE

- Is Your Doctor Practicing Good Data Hygiene?
- What Your Medical Data Says About You
- Can Blockchain Protect Your Healthcare Data?
- Why Ransomware Targets Healthcare

PARENTING

- Are You Oversharenting? How to Manage Your Family's Online Exposure
- How to Teach Your Teens About Privacy
- Five Ways Your Child's Data is Being Exposed

ALL ABOUT APPS

- How to Read a Privacy Policy in 60 Seconds
- Location Tracking Apps: 3 Privacy Settings You Need to Know
- How Your Apps are Collecting Your Data and What They're Doing with It

MANAGING YOUR SOCIAL MEDIA LIFE

- Three Questions to Ask Yourself Before Posting That Picture to Social Media
- Just Some Social Media Fun? Think Again! The Privacy Dangers of Popular Quizzes and Games
- How to Research Your Online Reputation

FAST FACTS AND STATS

PRIVACY IS GOOD FOR BUSINESS

GDPR and the California Consumer Privacy Act, among others, have made privacy a top priority for businesses in 2018 and 2019. Against this backdrop, Cisco's 2018 Privacy Maturity Benchmark Study showcased the importance of having good privacy processes well beyond GDPR compliance and also highlighted some of the financial benefits.[1] Some of the top findings from the study include:

- Sales delays due to data privacy concerns are widespread and significant in length. 65 percent of organizations reported that they have delays in their sales cycle, and among all respondents, the average sales delay was 7.8 weeks.
- The sales delays varied by country and industry. The longest delays by country occurred in Latin America and Mexico, and by industry in the government and healthcare sectors.
- Notably, the average sales delay was highly correlated with the privacy maturity level of the organization.
- Sales delays also varied significantly by the organizational model adopted for the privacy resources. A hybrid model, which has a mix of centralized and decentralized privacy resources, had shorter delays (4.6 weeks), compared to models with fully centralized (9.8 weeks) or decentralized resources (7.1 weeks).
- The level of privacy maturity also correlated with the likelihood and costs of data breaches. 74 percent of privacy-immature companies experienced a cyber loss of over $500,000 in the last year, compared to only 39 percent of privacy-mature companies.

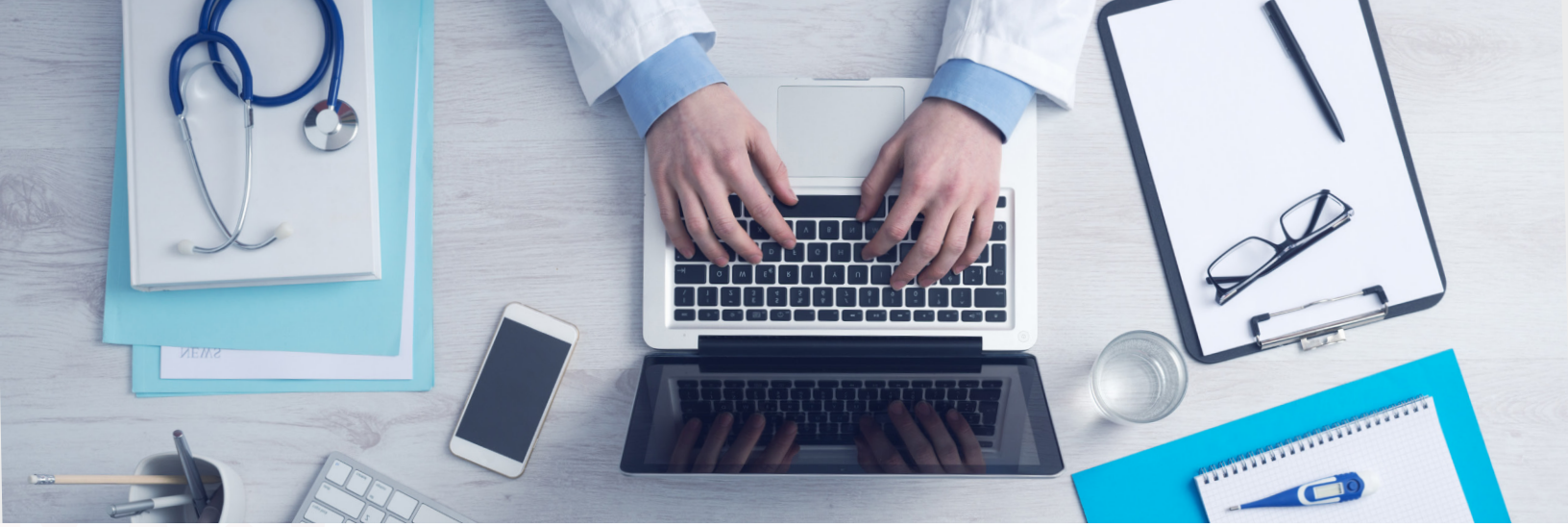
1. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-maturity-benchmark-study.pdf

RETAIL AND YOUR DATA

With online retail expected to exceed $410 billion in sales this year,[2] e-commerce is a thriving industry and one that provides a great convenience for consumers. However, it is an environment ripe for cybercrime, containing consumers' banking information, addresses, and browsing preferences and data. Online shoppers must be careful by protecting their personal data and ensure they are doing business over secure networks.

- 54 percent of consumers say they feel less secure purchasing from online retailers after hearing about recent data breaches.[3]
- Only 18 percent of consumers say they are "very confident" that retail sites are protecting their private information.[4]
- A majority of consumers are willing to walk away from businesses entirely if they suffer a data breach, with retailers most at risk: 62 percent of people said they would no longer do business with a retailer that had experienced a data breach compared to 59 percent who said the same for banks and 58 percent who said so about social media sites.[5]
- 66 percent of U.S. consumers want companies to earn their trust by being more open and transparent with how their information is being used.[6]
- More than 70 percent of consumers are unaware of tools they can use to control or limit the usage of their personal data.[7]
- Nearly one-third of consumers do not know that many of the "free" online services they use are paid for via targeted advertising made possible by the tracking and collecting of their personal data.[8]
- Almost 77 percent would like more transparency on the ads being targeted to them based on the personal data the internet companies collect.[9]
- A Fraud Watch Network survey found that about 4 out of 10 consumers use free Wi-Fi at least once a month, and among those, one-third had made a purchase on free Wi-Fi with a credit card in the last six months.[10]

2. http://www.digitaljournal.com/pr/3780610
3. http://www.digitaljournal.com/pr/3780610
4. https://www.prnewswire.com/news-releases/sas-survey-67-percent-of-us-consumers-think-government-should-do-more-to-protect-data-privacy-300761765.html
5. https://www.apnews.com/c9c1aa5d1c4546db91d85be1fe9fbca9
6. https://www.chainstoreage.com/technology/study-withheld-personal-data-jeopardizes-customer-experiences/
7. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/)
8. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/)
9. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/)
10. https://www.aarp.org/money/scams-fraud/info-2016/dangers-of-free-public-wifi-ea.html



HEALTHCARE AND DIGITAL RECORD KEEPING

Technology can greatly improve the delivery of medical and health services for patients. As healthcare companies turn to digital record keeping and internet-connected medical devices, patients outcomes are also improving. But these advances in healthcare technology also come with a risk: Medical organizations, including insurance companies, collect large volumes of data that we report on our devices, including our Social Security numbers, financial information, medical history and current health status. This data can be immensely valuable to cybercriminals and so intensely personal that patients would be deeply impacted if it was lost or stolen. Recent statistics found that:

- In the U.S. alone, healthcare data breaches occur at a rate of more than one a day, costing an average of $408 per record.[11]
- Four in five U.S. physicians have had cyberattacks in their practices, according to an Accenture survey.[12]
- About 78 percent of respondents to a recent survey of healthcare professionals said they'd had either a malware and/or ransomware attack in the last 12 months.[13]
- Under the Health Insurance Portability and Accountability Act (HIPAA), it's illegal for healthcare providers to share patients' treatment information. More than 30,000 reports regarding privacy violations are received each year.[14]
- According to a recent HIMSS study, the vast majority of provider respondents (77%) cited medical identity theft as cybercriminals' primary motivation.[15]
- Insiders are also remaining a constant challenge for healthcare, accounting for 96 incidents or 41 percent of data breaches this year so far. More than 1.17 million patient records were breached by insider error or wrongdoing.[16]

11. https://www.informationweek.com/big-data/curing-the-patient-data-security-and-privacy-epidemic/a/d-id/1333355
12. https://newsroom.accenture.com/news/four-in-five-us-physicians-have-had-a-cyberattack-in-their-clinical-practices-says-survey-by-accenture-and-the-american-medical-association.htm
13. https://healthitsecurity.com/news/78-of-providers-report-healthcare-ransomware-malware-attacks
14. http://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust
15. http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf
16. http://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches

CONSUMERS ARE CONCERNED ABOUT PRIVACY

As the issue of privacy become better known to the public, consumers are becoming more concerned about who will access their information and why. Nevertheless, some still don't take the precautions needed to better safeguard their personal information.

- In a recent survey by Blue Fountain Media, web users surveyed said they overwhelmingly object to how their information is being shared with and used by third-party vendors. A whopping 90 percent of those polled were very concerned about internet privacy.[17]
- While people are clearly dissatisfied with the state of internet privacy, they feel uninspired or simply ill-equipped to do anything about it.[18] In fact:
  - 60 percent say they download apps without reading the terms and conditions.
  - 17 percent say they will keep an app they like even if it breaches their privacy by tracking their whereabouts.
- In a separate poll by Janrain, 68 percent of respondents said they would like to see a law enacted that gives citizens greater control over how businesses use their personal data, similar to the GDPR law enacted in Europe.[19]
  - 35 percent of respondents said they are fine with businesses targeting them for ads based on consumers' interests as long as their data is protected and used responsibly.
- A survey by SAS found that 77 percent of people have changed privacy settings in order to better secure their data, 65 percent declined the terms of agreement for an app, 56 percent deleted an app from a mobile device, and 36 percent removed a social media account due to privacy concerns.[20]

PROTECTING THE CONNECTED HOME

Most households now run networks of devices linked to the internet, including computers, gaming systems, household assistants, home robots, TVs, tablets, smartphones and wearables. These devices make it easier to connect to the world around you, but they can also track your personal information, including your contacts, photos, videos, location and health and financial data.

- 36 percent of people in the U.S. own six web-connected devices or more[21], and 90 percent of Americans own a smart home device.[22]
- 47.3 million adults have access to a smart speaker[23], 20 percent of the U.S. adult population. Eight million Americans own three or more smart speakers.[24]
- Up to 50 connected or Internet of Things (IoT) devices will be in use in the average connected home by 2022.[25]
- In 2016 alone, 2.2 billion data records were compromised and vulnerabilities were uncovered in IoT products from leading brands.[26]
- Nearly 40 percent of people say they are concerned about connected-home devices tracking their usage and more than 40 percent said they are worried that such gadgets would expose too much about their daily lives.[27]
- While 85 percent of enterprises are in the process of or intend to deploy IoT devices, only 10 percent feel confident that they could secure those devices against security threats, according to AT&T's Cybersecurity Insights Report.[28]
- Recent events also have changed the way manufacturers think about collecting data. In Jabil's 2018 Connected Home and Building Technology Trends Survey, 69 percent of participants noted that the recent focus on data privacy has made them rethink their plans to collect and use data from smart devices.[29]

17. https://www.entrepreneur.com/article/314524
18. https://www.entrepreneur.com/article/314524
19. https://www.janrain.com/resources/industry-research/consumer-attitudes-toward-data-privacy-survey-2018
20. https://www.chiefmarketer.com/data-privacy-concerns-on-rise-report/
21. https://www.pymnts.com/news/payment-methods/2018/consumer-trends-mobile-voice-biometrics-cash
22. https://www.iottechnews.com/news/2018/may/15/research-us-consumers-smart-home-device/
23. https://techcrunch.com/2018/03/07/47-3-million-u-s-adults-have-access-to-a-smart-speaker-report-says/
24. https://www.theatlantic.com/magazine/archive/2018/11/alexa-how-will-you-change-us/570844/
25. https://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf
26. https://www.ciodive.com/news/smart-watches-lighting-cities-is-the-iot-the-newest-weapon-of-the-cyber/505255/
27. http://www.businessinsider.com/consumers-holding-off-on-smart-home-gadgets-thanks-to-privacy-fears-2017-11
28. http://www.businessinsider.com/internet-of-things-security-privacy-2016-8
29. https://www.iotforall.com/smart-home-data-security/

PRIVACY, PARENTING AND TEENS: INSIGHTS FROM THE NCSA/MICROSOFT KEEPING UP WITH GENERATION APP SURVEY

In this digitally-connected age, teens and parents continue to spend a lot of time online despite their concerns about security and privacy. Highlights from a recent parent-teen NCSA/Microsoft survey include:[30]

- 39 percent of teens said they were concerned about their personal information being leaked online and 36 percent had this same worry as it pertains to pictures and videos that are shared privately.
- Teens and parents are closely aligned on their top three concerns affecting online teens (ranked as something they are "very concerned" about), which are:
  - Someone accessing a teen's account without permission (teens 41% vs. parents 41%).
  - Someone sharing a teen's personal information about them online (teens 39% vs. parents 42%).
  - Having a teen's photo or video shared that they wanted private (teens 36% vs. parents 34%).
- 57 percent of teens say they have created an account that their parents are unaware of, such as a social media site or an app they wanted to use.

SOCIAL MEDIA

Social media is a great platform for connecting with friends and family through personal news updates, photo sharing and live streaming video. As convenient and fun as these platforms are, privacy settings don't always prevent personal information from being shared beyond the intended audience and without a user's knowledge.

- 61 percent of people think social media companies do not adequately protect consumer data.[31]
- 41 percent of Americans have been personally subjected to harassing behavior online and nearly one in five (18%) has been subjected to particularly severe forms of harassment online, such as physical threats, harassment over a sustained period, sexual harassment or stalking.[32]
- Eighty-two percent of cyber stalkers use social media to find out information about potential victims – for example, where they live and which school they attend.[33]
- The NCSA/Microsoft 2017 "Keeping up with Generation App" survey revealed that across the board from a privacy perspective, teens report that they are "very concerned" about someone:[34]
  - Accessing their accounts without their permission (41%)
  - Sharing personal information about them online that they prefer to keep private (39%)
  - Posting a private photo or video of them online (36%)

30. https://staysafeonline.org/resource/keeping-generation-app-2017/
31. https://www.apnews.com/c9c1aa5d1c4546db91d85be1fe9fbca9
32. http://www.pewinternet.org/2017/07/11/online-harassment-2017/
33. http://socialbarrel.com/social-media-privacy-infographic/101217/
34. https://staysafeonline.org/resource/keeping-generation-app-2017/

LIVE FROM LINKEDIN

JOIN US FOR DATA PRIVACY DAY 2019

The technology landscape is rapidly changing and is forging a new era in privacy. At Data Privacy Day 2019, privacy leaders with diverse perspectives will explain opportunities and challenges for the privacy road ahead.

This event provides an opportunity to hear from leading privacy experts – from government, industry and NGOs

EXECUTIVE PANELS INCLUDE:

+ A New Era in Privacy: GDPR and the California Consumer Privacy Act, among others have and will make great waves in privacy. Experts will bring the new privacy dynamic into focus and explain what it means for us.
+ Improving Your Company's Privacy Posture: ith so many changes in the privacy ecosystem how can companies not only comply but break through as leaders in privacy? Viewers/attendees will learn these key takeaways and more.
+ The Future of Privacy and Breakthrough Technologies: Advances in technology such as artificial intelligence to the human body acting as the computer interface mean privacy will take on even greater significance. Experts will highlight why our actions now will drive tomorrow's outcomes.

The latest agenda is available at: https://staysafeonline.org/dpd19-live/ as well as livestream details.

WHEN

MONDAY, JAN. 28, 2019
FROM NOON – 5:00 P.M.

WHERE

LIVESTREAMED FROM LINKEDIN
https://staysafeonline.org/dpd19-live/

CONTRIBUTING SPONSORS

VISA
verizon

PARTICIPATING SPONSORS

yubico
mozilla
TREND MICRO

NON-PROFIT PARTNERS

WOMEN IN SECURITY AND PRIVACY
ITRC IDENTITY THEFT RESOURCE CENTER

GET INVOLVED

BECOME A DATA PRIVACY DAY CHAMPION

I AM #PRIVACYAWARE

Organizations and individuals who want to officially show support for Data Privacy Day can become a Data Privacy Day Champion. Champions represent those dedicated to respecting privacy, safeguarding data and enabling trust. Being a Champion is easy and does not require any financial support. Champions receive a toolkit of privacy awareness materials that they can use to educate themselves and their communities. Champions can include: individuals, companies and organizations of all sizes; schools and school districts; colleges and universities; nonprofits; and government organizations. For more information on how to become a Data Privacy Day 2019 Champion, visit https://staysafeonline.org/data-privacy-day/become-dpd-champion/.

GET INVOLVED INFOGRAPHIC:

https://staysafeonline.org/resource/get-involved-data-privacy-day-2019/ Learn simple, actionable advice you can use to educate people about privacy at home, at work and in your community.

SOCIAL MEDIA: Use #PrivacyAware and share the importance of data privacy for your family, community and workplace. Empower others to protect their personal online data by tweeting, "I am #PrivacyAware, are you? Find out at https://staysafeonline.org/data-privacy-day/."

CHECK YOUR PRIVACY SETTINGS:

https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/ Want to view or change your privacy/security settings, but don't know where to find them? NCSA has an easy-to-use resource with direct links to update your privacy settings on popular devices and online services.

LOCK DOWN YOUR LOGIN:

https://www.lockdownyourlogin.org/ Usernames and passwords are no longer enough to keep your accounts secure. Anyone with your username and password can access your account. Visit LockDownYourLogin.com to easily learn how to move beyond the password and better secure your online accounts.

HELPING FAMILIES NAVIGATE THE DIGITAL WORLD:

With technology constantly changing, it can be challenging to keep up - and to manage your family's technology usage. That's why Verizon has partnered with leading online safety partners to provide you with resources so you and your family have the confidence to use technology safely and responsibly. Learn more here https://www.verizon.com/about/responsibility/online-safety

ABOUT US

ABOUT THE NATIONAL CYBER SECURITY ALLIANCE

NCSA is the nation's leading nonprofit, public-private partnership promoting cybersecurity and privacy education and awareness. NCSA works with a broad array of stakeholders in government, industry and civil society. NCSA's primary partners are DHS and NCSA's Board of Directors, which includes representatives from ADP; Bank of America; CDK Global, LLC; CertNexus; Cisco; Cofense; Comcast Corporation; ESET North America; Facebook; Google; InfoSec Institute; Intel Corporation; Marriott International; Mastercard; Microsoft Corporation; Mimecast; NXP Semiconductors; Raytheon; Salesforce; Symantec Corporation; Visa and Wells Fargo. NCSA's core efforts include National Cybersecurity Awareness Month (October); Data Privacy Day (Jan. 28); STOP. THINK. CONNECT.™, the global online safety awareness and education campaign co-founded by NCSA and the Anti-Phishing Working Group with federal government leadership from DHS; and CyberSecure My Business™, which offers webinars, web resources and workshops to help businesses be resistant to and resilient from cyberattacks. For more information on NCSA, please visit staysafeonline.org/about-us/overview/.

ABOUT DATA PRIVACY DAY

The National Cyber Security Alliance's (NCSA) privacy awareness campaign is an integral component of STOP. THINK. CONNECT.™ — the global online safety, security and privacy campaign. Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe and is officially led by NCSA in North America. VISA and Verizon are Contributing Sponsors of the 2019 privacy awareness campaign. Yubico, Mozilla and Trend Micro are Participating Sponsors. Women in Security and Privacy and Identity Theft Resource Center are Non-profit Partners. The hashtag for NCSA's privacy campaign efforts is #PrivacyAware.

MEDIA ROOM AND PRESS RESOURCES:

https://www.staysafeonline.org/about-us/news/media-room/

MEDIA CONTACT:

Jessica Beffa, Thatcher+Co.
ncsa@thatcherandco.com