West Virginia Executive Branch
Privacy Tip – Data Privacy Day

6 Ways to be #PrivacyAware

1. Think critically about privacy – What information do you collect? How are you handling the personally identifiable information (PII) that crosses your desk? Are emails encrypted when they contain PII? Do you keep documents with PII in a secure area?

2. Stay up-to-date with recent privacy and security incidents in the news. Don't say, "This couldn't happen in my office!" Instead, learn from other's mistakes. How did it happen? Could your office also be at risk?

3. Take your privacy and security training SERIOUSLY. It isn't a punishment to complete the training – it may save you from making mistakes that could have far-reaching consequences.

4. Talk to your Department Privacy Officer if you have questions. They know the laws and procedures that are specific to your department. They are also trained in Executive Branch privacy policies, which are used in most state agencies.

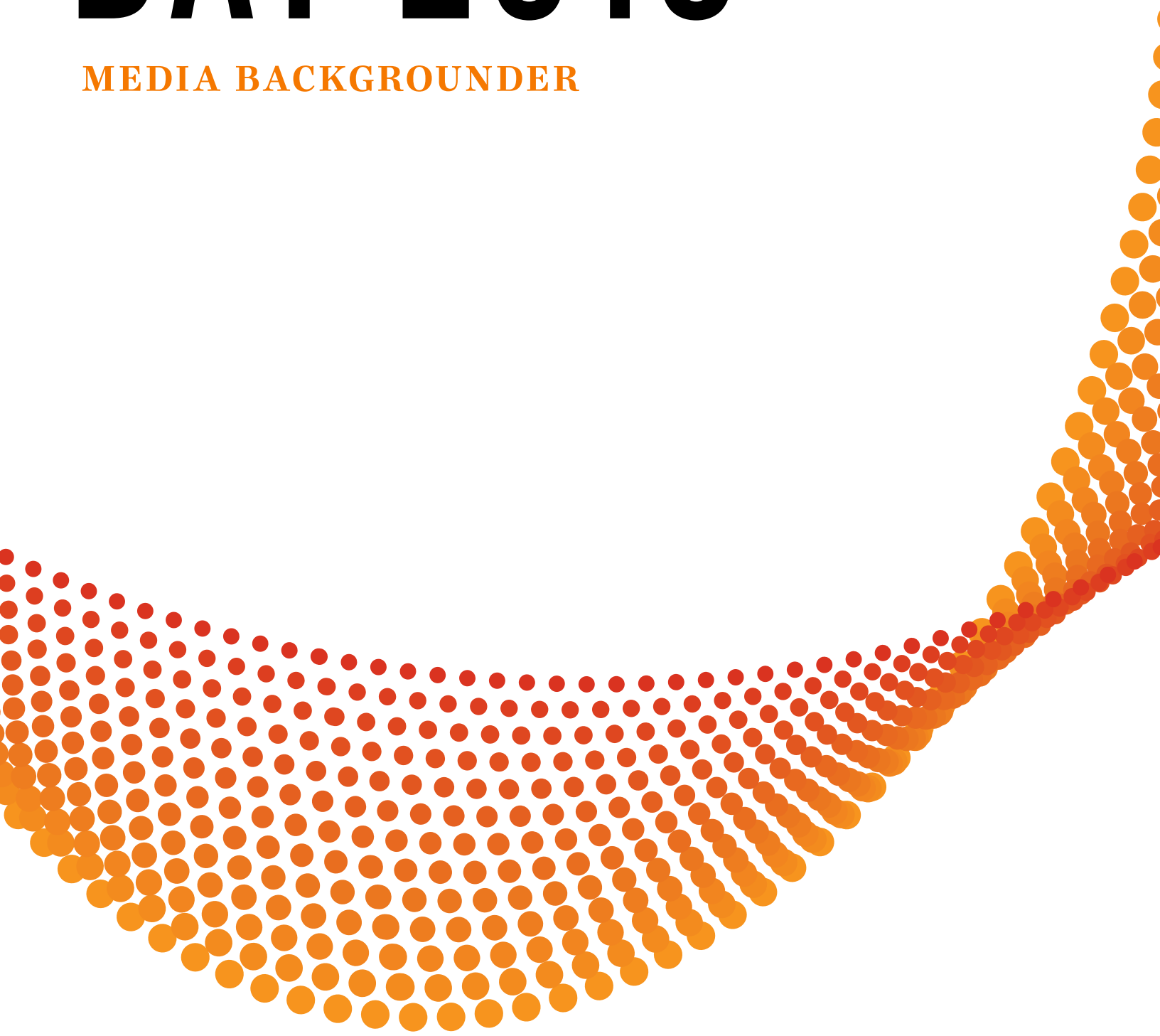
5. Utilize the State Privacy Office website! (www.privacy.wv.gov) There are many resources to help you learn the ins and outs of privacy.

6. Visit the Data Privacy Day website for more information: https://staysafeonline.org/data-privacy-day/

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.

DATA PRIVACY DAY 2018

MEDIA BACKGROUNDER



DATA PRIVACY DAY

WHAT IS DATA PRIVACY DAY?

Led by the National Cyber Security Alliance (NCSA) in the United States, Data Privacy Day – held every year on January 28 – commemorates the 1981 signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. Launched in Europe and adopted in North America in 2008, Data Privacy Day brings together businesses and private citizens to share the best strategies for protecting consumers' private information.

The 2018 Data Privacy Day theme centers on "Respecting Privacy, Safeguarding Data and Enabling Trust."

Following a year of massive data breaches at places like Equifax, Verizon, the NSA and Uber, it is necessary for people to learn how to better secure their personal information. And with 68 percent of consumers saying they don't trust brands to handle their personal information appropriately,[1] Data Privacy Day also encourages businesses to be more transparent about how they collect and use data.

> ***"Data Privacy Day highlights our ever-more connected lives and the critical roles consumers and businesses play in protecting personal information and online privacy,"*** says Michael Kaiser, executive director of NCSA. ***"Our personal information and our habits and interests fuel the next generation of technological advancement like the Internet of Things, which will connect devices in our homes, schools and workplaces. Consumers must learn how best to protect their information and businesses must ensure that they are transparent about the ways they handle and protect personal information. The future holds tremendous opportunities for improving our lives through connected technologies, but we can only build a safer, more trusted internet if everyone works in collaboration to make respecting and protecting personal information a priority."***

1. https://www.gigya.com/resource/report/2017-state-of-consumer-privacy-trust/

DATA PRIVACY DAY

WHY WE SHOULD CARE ABOUT ONLINE PRIVACY

We produce a nearly endless stream of data in our daily lives. Seventy-seven percent of Americans now own smartphones, up from a mere 35 percent in 2011.[2] Today we conduct much of our lives on the internet and on our connected devices, yet few people understand the enormous amount of personal information that is collected and shared from our devices and the services we use online. 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.

The absence of strong online consumer protection laws in the U.S. means that many companies have the opportunity to monitor their users and customers' personal behavior and sell the data for profit. Consumers need to understand the true value of their information and how it is collected, used and shared in order to make informed decisions and better manage their personal data.

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.

Although the U.S. Constitution does not explicitly define privacy, U.S. law has come to recognize that individuals have a right to privacy in many different contexts.

2. http://www.pewinternet.org/fact-sheet/mobile/

TIPS FOR STAYING SAFE AND PRIVATE ONLINE

As Americans become more concerned about how their online information is collected and used, NCSA recommends these tips to consumers and businesses for safeguarding their privacy:

PRIVACY INSIGHTS AND ADVICE FOR CONSUMERS: OWN YOUR ONLINE PRESENCE

+ **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.

+ **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. It's a good idea to review your social network friends and all contact lists to ensure everyone still belongs.

+ **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. It's OK to ask others for help.

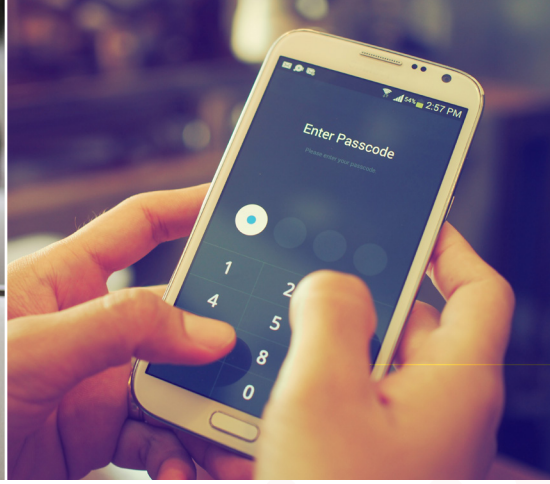
+ **LOCK DOWN YOUR LOGIN.** Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Choose one account and turn on the strongest authentication tools available, such as biometrics, security keys or a unique one-time code sent to your mobile device.

+ **KEEP A CLEAN MACHINE**. Keep all software, operating systems (mobile and PC) and apps up to date to protect data loss from infections and malware.

+ **APPLY THE GOLDEN RULE ONLINE.** Post only about others as you would have them post about you.

+ **SECURE YOUR DEVICES.** Every device should be secured by a password or strong authentication – finger swipe, facial recognition etc. These security measures limit access to authorized users only and protect your information if devices are lost or stolen.

+ **THINK BEFORE YOU APP.** Information about you, such as the games you like to play, your contacts list, where you shop and your location, has tremendous value. Be thoughtful about who gets that information and understand how it's collected through apps.



TIPS FOR STAYING SAFE AND PRIVATE ONLINE

PRIVACY INSIGHTS AND ADVICE FOR ORGANIZATIONS: PRIVACY IS GOOD FOR BUSINESS

+ **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.

+ **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.

+ **DON'T COUNT ON YOUR PRIVACY NOTICE AS YOUR ONLY TOOL TO EDUCATE CONSUMERS ABOUT YOUR DATA PRACTICES.** Consider features that allow consumers to opt-in to certain forms of data sharing rather than requiring them to opt-out.

+ **CONDUCT DUE DILIGENCE AND MAINTAIN OVERSIGHT OF PARTNERS AND VENDORS.** If someone provides services on your behalf, you are also responsible for how they collect and use your customers' personal information.

PSST! LET'S TALK PRIVACY

FAST FACTS AND STATISTICS

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:[3]

- 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 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 for a social media site or an app they wanted to use.

DEVICES IN THE 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. Your devices make it easy to connect to the world around you, but they can also track a lot of information about you and your friends and family, such as your contacts, photos, videos, location and health and financial data.

- According to a 2016 survey by NCSA and ESET, nearly one in four people (24%) use an app from their mobile device or computer to remotely access or control devices in their home (e.g., front door lock, home security system, TV, thermostat).[4]
- 42 percent of parents' households use either Google's voice assistant, Amazon's Alexa, Apple's Siri or Microsoft's Cortana multiple times a day.[5]
- 89 percent of people would like all of their household devices to be seamlessly connected together in the future.[6]
- Up to 50 connected or Internet of Things (IoT) devices will be in use in the average connected home by 2020.[7]
- In 2016 alone, 2.2 billion data records were compromised and vulnerabilities were uncovered in IoT products from leading brands.[8]
- 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.[9]
- 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.[10]

3. https://staysafeonline.org/resource/keeping-generation-app-2017/
4. https://staysafeonline.org/resource/2016-ncsaeset-survey-summary-increasingly-connected-lives/
5.http://www.adweek.com/brand-marketing/why-babies-will-drive-internet-of-things-marketing/
6. https://www.gsma.com/newsroom/press-release/internet-of-things-is-transforming-family-life/
7. https://www.gsma.com/newsroom/press-release/internet-of-things-is-transforming-family-life/
8. https://www.ciodive.com/news/smart-watches-lighting-cities-is-the-iot-the-newest-weapon-of-the-cyber/505255/
9. http://www.businessinsider.com/consumers-holding-off-on-smart-home-gadgets-thanks-to-privacy-fears-2017-11
10. http://www.businessinsider.com/internet-of-things-security-privacy-2016-8

PSST! LET'S TALK PRIVACY

FAST FACTS AND STATISTICS

SOCIAL MEDIA

Social media – which includes everything from personal news updates, photo sharing and live streaming video – continues to be a very popular online activity. As convenient and fun as these platforms are for all age groups to communicate, privacy settings don't always prevent personal information from being shared beyond the intended audience and without a user's knowledge.

- 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.[11]
- Eighty-two percent of cyberstalkers use social media to find out information about potential victims – for example, where they live and which school they attend.[12]
- 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:
  - 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%)

RETAIL AND YOUR DATA

In today's connected environment, retail businesses are a treasure trove for cybercriminals – housing banking information, shipping and billing addresses and other customer browsing preferences and data. Today's online shoppers need to be more careful than ever about protecting their personal data and ensuring they are doing business over secure networks.

- 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.[13]
- More than 70 percent of consumers are unaware of tools they can use to control or limit the usage of their personal data.[14]
- 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.[15]
- Almost 77 percent would like more transparency on the ads being targeted to them based on the personal data the internet companies collect.[16]
- 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 with a credit card in the last six months.[17]

11. http://www.pewinternet.org/2017/07/11/online-harassment-2017/
12. http://socialbarrel.com/social-media-privacy-infographic/101217/
13. https://www.chainstoreage.com/technology/study-withheld-personal-data-jeopardizes-customer-experiences/
14. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/)
15. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/)
16. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/)
17. https://www.aarp.org/money/scams-fraud/info-2016/dangers-of-free-public-wifi-ea.html

PSST! LET'S TALK PRIVACY

FAST FACTS AND STATISTICS

HEALTHCARE AND DIGITAL RECORD KEEPING

Medical and health information is among the most sensitive and personal information about people. Technology can greatly improve the delivery of medical and health services and outcomes for patients. We have already seen medical professionals moving into digital record keeping and are in the first phase of connecting medical devices to the internet. 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:

- Four in five U.S. physicians have had cyberattacks in their practices, according to an Accenture survey.[18]
- 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.[19]
- Under the Health Insurance Portability and Accountability Act, it's illegal for healthcare providers to share patients' treatment information. More than 30,000 reports regarding privacy violations are received each year.[20]
- According to a recent HIMSS study, the vast majority of provider respondents (77%) cited medical identity theft as cybercriminals' primary motivation.[21]
- 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.[22]

18. 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
19. https://healthitsecurity.com/news/78-of-providers-report-healthcare-ransomware-malware-attacks
20. http://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust
21. http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf
22. http://www.healthcareitnews.com/news/insiders-hackers-causing-bulk-2017-healthcare-data-breaches

SPREAD THE WORD

ONLINE PRIVACY TOPICS TO EXPLORE

Data Privacy Day is more than just another day. For American consumers and business alike, it's an annual day of awareness and critical reminder to everyone about the importance of **respecting privacy, safeguarding personal data and enabling trust.**

To help educate and inform your audiences, NCSA has compiled a cross-section of story buckets and ideas about everyday privacy concerns and challenges.

PARENTING

- Are You Oversharenting? How to Manage Your Family's Online Exposure
- The New Tech Talk: How to Talk to Your Kids About Privacy

EDUCATION

- Privacy 101: Protecting Your Personal Information in the Age of Social Media
- Connected Classrooms Raise Privacy Concerns

ALL ABOUT APPS

- How to Read a Privacy Policy in 60 Seconds
- Location Tracking Apps: 3 Privacy Settings You Need to Know
- What Kind of Data Is Your App Collecting about You?

HEALTHCARE

- How to Practice Good Data Hygiene
- Why Your Employees Might be Your Biggest Security Threat
- Is Your Doctor/HCP Protecting Your Medical Information?
- Fitness at All Costs: What Your Wearable Reveals About You

GENERAL

- Is Your Phone Spying on You?
- How to Protect Your Privacy When Using Free Public WiFi
- Take Your Password from Good to Great: Authenticate!
- The Robot in Your Home
- Living in an Age When Your Privacy Is For Sale

MANAGING YOUR SOCIAL MEDIA LIFE

- Three Questions to Ask Yourself Before Posting That Picture to Social Media
- How to Review or Change Your Settings on Popular Web Services
- Just Some Social Media Fun? Think Again! The Privacy Dangers of Popular Quizzes and Games
- Managing Your Privacy and Online Reputation

RANSOMWARE

- What You Need to Know About Ransomware
- To Pay or Not to Pay: What to Do When Your Data Is Held Hostage

JOIN US IN PERSON OR ONLINE

DATA PRIVACY DAY EVENTS

LINKEDIN

To generate awareness about Data Privacy Day and its importance, NCSA will host a timely event streamed live from LinkedIn in San Francisco, CA on Thursday, Jan. 25. The event will showcase fast-paced, cutting-edge panel discussions and TED-style talks with leading experts focusing on issues business and consumers must know about privacy. Topics will include "Looking into a Crystal Ball: What Your Data Says About You," "Five Things You Can Do to Manage Your Privacy Now" and "Staying Competitive – Why Privacy is Good for Your Business."

TWITTER CHATS

#ChatSTC Twitter Chat | Wednesday, Jan. 10, 3 p.m. EST/noon PST

Privacy Matters – Why You Should Care and What You Can Do to Manage Your Privacy

Data about yourself and your friends and family is continuously being collected and shared, which could affect your life in many ways. Data about you can be used in a variety of ways, sometimes in ways you wouldn't expect or even approve. That's why it is important to understand the value of your personal information and how to manage it when possible. This Twitter chat will discuss why privacy is important and what you can do to protect your personal information.

#ChatSTC Twitter Chat | Wednesday, Jan. 17, 3 p.m. EST/noon PST

Privacy in a Growing Internet of Me

The Internet of Things – the increasingly connected world in which we live – is rapidly expanding. We love our convenient and fun tech devices – like personal assistants, wearables, speakers, cameras, TVs, cars, toys and appliances. However, it's important to remember that connected devices are fueled by information about us, such as our behaviors and preferences – in effect, creating an 'Internet of Me' rather than just an Internet of Things. This Twitter chat – in honor of Data Privacy Day on Jan. 28 – will share how you can manage your Internet of Me and the personal information it collects.

#ChatSTC Twitter Chat | Wednesday, Jan. 24, 3 p.m. EST/noon PST:

Fostering a Culture of Privacy Awareness at Work

Data Privacy Day is a great time to think about how your business collects, stores, manages and uses data. Personal information about customers, vendors and/or employees may be valuable to your business – but the protection of that data and transparency of its use is something consumers highly value, too. In this Twitter chat, we'll discuss the importance of safeguarding data at your organization, things to consider in protecting this information and how you can foster a culture of privacy awareness at all levels.

DATA PRIVACY DAY 2018

SPONSORS

LEADING SPONSORS

"Good privacy is good for business. In the digital economy, data is perhaps the single most critical asset and business driver. We must protect it and respect it."

Michelle Dennedy, Vice President and Chief Privacy Officer, Cisco

"Designing privacy into devices and services continues to be critical, and we are committed to that process at Intel."

David Hoffman, Associate General Counsel and Global Privacy Officer at Intel Corporation

CONTRIBUTING SPONSORS

SUPPORTING SPONSOR

NONPROFIT PARTNER

PROTECTING YOUR PRIVACY

CHAMPIONS AND RESOURCES

I AM #PRIVACYAWARE

Americans everywhere can join the #PrivacyAware campaign – it's easy to do and will help generate awareness about the importance of data privacy. Empower others to protect their personal online data by tweeting, "I am #PrivacyAware, are you?" Find out at staysafeonline.org/DPD.

Another great way for organizations and individuals to officially show support is to 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; government organizations; and individuals. For more information on how to become a Data Privacy Day 2018 Champion, visit https://staysafeonline.org/data-privacy-day/become-dpd-champion/.

PROTECTING YOUR PRIVACY

CHAMPIONS AND RESOURCES

CONSUMER RESOURCES

There are a variety of consumer-friendly resources designed to educate the public about protecting their privacy. Check out the following:

Here's How to Get Involved Infographic Learn simple, actionable advice you can use to educate people about privacy at home, at work and in your community.

Internet of Me Infographic You are continuously generating data about yourself and others, and your personal information is the fuel that makes connected devices work (possibly update). Learn what you can do now to manage your privacy.

STOP. THINK. CONNECT.™ Tips and Advice: Practice good online safety habits by following these tips and advice from STOP. THINK. CONNECT.™, the global online safety education and awareness campaign.

Check Your 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: 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.

#CyberAware Newsletter: #CyberAware is NCSA's monthly newsletter for families. Each month, the newsletter shares family online safety news and resources and the latest from the Stay Safe Online blog. Sign up to receive the newsletter here.

U.S. Department of Homeland Security (DHS): DHS provides privacy-related and cybersecurity resources through its Stop.Think.Connect. Campaign toolkit. From tip cards and information covering identity theft, mobile security, phishing and more, digital citizens can share resources with their communities, colleagues and families to keep their data safeguarded.

AT&T: The CyberAware website from AT&T is a resource for consumers seeking simple yet helpful details on how to improve their cybersecurity and fight online fraud. It includes information about new threats and common scams – along with plenty of links and tips.

Federal Trade Commission (FTC): IdentityTheft.gov is the FTC's one-stop resource for identity theft victims. IdentityTheft.gov provides personal recovery plans for more than 30 types of identity theft and an Identity Theft Report that victims can use in place of a police report in most cases to resolve the problems identity theft causes.

Identity Theft Resource Center: : In the face of major #data breaches, large hacking events & other "out of my hands" threats, here are seven #Privacy habits you can start today from @ITRCSD.

PROTECTING YOUR PRIVACY

CHAMPIONS AND RESOURCES

BUSINESS RESOURCES

Here's an assortment of business-focused resources created to educate companies about transparent online practices:

Here's How to Get Involved Infographic
Learn simple, actionable advice you can use to educate people about privacy at home, at work and in your community.

Are You Doing Enough to Protect Your Consumers' Data Infographic Personal information may be valuable to your business, but it's also something consumers value.

Five Ways to Help Employees To Be #PrivacyAware Infographic

Privacy is Good for Business Tip Sheet

CyberSecure My Business is a comprehensive, national program comprised of interactive training based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, webinars and web resources to help businesses be resistant to and resilient from cyberattacks.

ForgeRock: As we move into the GDPR era, it is more important than ever to be able to engage customers in the protection of their data - this includes clarifying and enforcing consent, privacy protections and incident management capabilities to ensure that customers are active partners in the data relationship. In this webinar you will gain an understanding of the four pillars of privacy and consent; learn what obligations data-breach reporting, EU GDPR and other regulations place on companies globally; and learn how to develop secure and effective privacy policies – and communicate them to your customers throughout your digital transformation.

Cisco Trust Center: Learn how Cisco is protecting and respecting customer data and privacy.

PROTECTING YOUR PRIVACY

CHAMPIONS AND RESOURCES

Privacy Sigma Riders Podcast Series: Essential listening for anyone interested in cybersecurity, data protection and privacy. Hosted by Cisco Chief Privacy Officer Michelle Dennedy and team. Guest experts and innovators explore increasing the value of data with novel approaches to data privacy.

EDUCAUSE: EDUCAUSE provides free activities and resources to help the higher education community promote privacy awareness to students, faculty and staff. Read the latest EDUCAUSE Review blog post on protecting personal information, "Privacy Is Our Shared Responsibility."

Federal Trade Commission (FTC): The FTC has created a webpage FTC.gov/SmallBusiness that has advice to help small business owners protect not only the networks and systems that are the backbone of their business, but also their employees' and customers' sensitive data. The website also includes videos that show steps small business owners can take to ensure their business has secure networks.

- FTC Resources for Small Business
  - FTC.gov/SmallBusiness
  - Start with Security: how businesses can protect their computers and networks against threats
  - Order free publications from the FTC and share them with your employees

Health Information Management Systems Society (HIMSS): How we think about privacy and how we achieve privacy has changed with the evolution of IT and connectivity. Bits and bytes of our data are everywhere. Information cannot be private, unless it is also secure in the technical, administrative, and physical realms. To learn more about good information privacy and security practices, please visit www.himss.org/dpd today.

International Association of Privacy Professionals (IAPP): IAPP is Privacy After Hours. Privacy After Hours is coming to a city near you! In recognition of Data Privacy Day, the IAPP sponsors events around the world for anyone interested in privacy – IAPP member or not. Visit our website for a full listing and register today! Don't see your city? Volunteer to host!

ABOUT US

ABOUT THE NATIONAL CYBER SECURITY ALLIANCE

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 the U.S. Department of Homeland Security (DHS) and NCSA's Board of Directors, which includes representatives from ADP; Aetna; AT&T Services Inc.; Bank of America; Barclays; CDK Global, LLC; Cisco; Comcast Corporation; ESET North America; Google; Facebook; LifeLock, Inc.; Logical Operations; NXP Semiconductors; RSA, the Security Division of EMC; Symantec Corporation; Intel Corporation; Marriott International; MasterCard; Microsoft Corporation; PayPal; Raytheon; PKWARE; Salesforce; SANS Security Awareness; TeleSign; Visa and Wells Fargo. NCSA's core efforts include National Cyber Security Awareness Month (October); Data Privacy Day (Jan. 28) and 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. 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.TM – 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. Cisco and Intel are Leading Sponsors of the 2017 privacy awareness campaign. ForgeRock and AT&T Services Inc. are Contributing Sponsors. Yubico is a Supporting Sponsor. The hashtag for NCSA's privacy campaign efforts is #PrivacyAware.

MEDIA ROOM AND PRESS RESOURCES:

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