Cyber Protect LLC Announces Commitment to Respecting Data by Becoming a 2022 Data Privacy Week Champion

This year's initiative emphasizes educating businesses on data collection best practices that respect data privacy and promoting transparency

WARREN, MICHIGAN, US, January 14, 2022 /EINPresswire.com/ -- Cyber Protect LLC today announced its commitment to Data Privacy Week by registering as a Champion. As a Champion, Cyber Protect LLC recognizes and supports the principle that all organizations share the responsibility of being conscientious stewards of personal information.

Data Privacy Week is an expanded effort from Data Privacy Day -- taking place annually from January 24 - 28 -- that generates awareness about the

Cyber Protect LLC Logo

importance of privacy, highlights easy ways to protect personal information, and reminds organizations that respecting privacy is good for business. This year, we are encouraging individuals to learn more about how to manage and protect their valuable online data. We are also encouraging businesses to respect customer data and learn about the responsibility they hold for keeping individuals' personal information safe from unauthorized access and ensuring fair, relevant, and legitimate data collection and processing.

According to a Pew Research Center study, 79% of U.S. adults report being concerned about the way their data is being used by companies. As technology evolves and the COVID-19 pandemic continues to influence how consumers interact with businesses online, data collection practices are becoming increasingly unavoidable, making it imperative that companies be open and

honest about how they collect, use and share consumers' personal information and communicate their policies clearly and concisely.

The National Cybersecurity Alliance has offered up the following tips to help guide individuals and businesses to better data privacy practices, such as:

 For Individuals:

 Understand the privacy/convenience tradeoff: Many accounts ask for access to personal information, such as your geographic location, contacts list, and photo album, before you even use their services. This personal information has tremendous value to businesses and allows some to even offer you their services at little to no cost. Make informed decisions about whether or not to share your data with certain businesses by considering the amount of personal information they are asking for, and weighing it against the benefits you may receive in return. Be thoughtful about who gets that information and wary of apps or services that require access to information that is not required or relevant for the services they are offering. Delete unused apps on your internet-connected devices and keep others secure by performing updates.

 Manage your privacy: Once you have decided to use an app or set up a new account, check the privacy and security settings on web services and apps and set them 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. Get started with NCA's Manage Your Privacy Settings page to check the settings of social media accounts, retail stores, apps, and more.

 Protect your data: Data privacy and data security go hand in hand. Keep your data secure by creating long, unique passwords and storing them in a password manager. Add another layer of security by enabling multi-factor authentication (MFA) wherever possible, especially on accounts with sensitive information. MFA has been found to block 99.9% of automated attacks when

NCSA Data Privacy

"

Since our inception, Cyber Protect has been a Data Privacy Champion as it is important to educate as many people as possible about cybersecurity."

Cheyenne Harden

enabled and can ensure your data is protected, even in the event of a data breach.

◻   For Businesses:

◻   Conduct an assessment: Conduct an assessment of your data collection practices. Whether you operate locally, nationally, or globally, understand which privacy laws and regulations apply to your business. Follow reasonable security measures to keep individuals' personal information safe from inappropriate and unauthorized access and make sure the personal data you collect is processed in a fair manner and only collected for relevant and legitimate purposes.

◻   Don't forget to maintain oversight of partners and vendors as well. If someone provides services on your behalf, you are also responsible for how they collect and use your consumers' personal information.

◻   Adopt a privacy framework: Researching and adopting a privacy framework can help you manage risk and create a culture of privacy in your organization by building privacy into your business. Get started by checking out the following frameworks: NIST Privacy Framework, AICPA Privacy Management Framework, ISO/IEC 27701 - International Standard for Privacy Information Management

◻   Educate employees: Create a culture of privacy in your organization by educating your employees of their and your organization's obligations to protecting personal information. Educate employees on your company's privacy policy and teach new employees about their role in your privacy culture during the onboarding process. Engage staff by asking them to consider how privacy and data security applies to the work they do on a daily basis. Better security and privacy behaviors at home will translate to better security and privacy practices at work. Teach employees how to update their privacy and security settings on work and personal accounts. Learn more.

For more information about Data Privacy Week 2022 and how to get involved, visit https://staysafeonline.org/data-privacy-week/

Cheyenne Harden
Cyber Protect LLC
+1 586-719-8838
info@cyberprotectllc.com
Visit us on social media:
Facebook
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/560639030