Beat: News

Protecting Against Personally Identifiable Information (PII) Theft

FBI Media Alert

Phoenix, Arizona, 25.05.2022, 19:30 Time

USPA NEWS - Fraudsters have been trying to steal your identity and personally identifiable information—or PII—for years. PII can include your name, Social Security number, date of birth, or financial information. In 2021, Arizona had more than 1,000 victims of a personal data breach, resulting in reported losses of almost $7.5 million.

Nationally, this scam claimed the third highest number of victims with 51,829 people reporting losses of $517 million in 2021. This scam has consistently shown an increase in victims and money lost over the last three years.

A personal data breach is defined as a leak/spill of personal data which is released from a secure location to an untrusted environment. It may also refer to a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Once a cyber-criminal obtains your PII, they can open credit card or bank accounts, apply for loans, or commit any number of crimes in your name. This theft takes many forms, from email phishing attacks to Point-of-Sale theft, to the more advanced hacking of vulnerabilities in servers where the information is hosted.

Both individuals and businesses can take steps to protect their financial future.

For individuals:

Watch for phishing attempts—unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.
Watch credit card, utility bills, and bank statements for unusual transactions.
Enable security functions on your phone and computer—especially if you have passwords stored or apps that link to your financial institutions.
Never respond to unsolicited requests for your personal information, whether online, by phone, or in person.

For businesses (Employers and plan administrators responsible for managing participant accounts):

Alert your workforce personnel to the latest methods criminals are utilizing to obtain Personally Identifiable Information.
Continue to encourage employees to scrutinize links and attachments contained in emails.
Direct employees to report any suspicious requests for personal information to your Information Technology or Information Security Department.
Establish multi-factor authentication for creating new online accounts and monitor accounts for unauthorized access, modifications, and anomalous activities.

If you believe you or someone you know has been victimized by an online scam or cyber fraud, the FBI asks you report it to the FBI's Internet Crime Complaint Center at www.ic3.gov, or call your local FBI office.

Thank you for reading my article. These are merely my thoughts and insights based on the facts. I use only verified sources. No fake news here. I write about a variety of subjects, mainly things I want to research and know more about. You can check out my website – Small Village Life at smallvillagelife.com, where I share useful articles and news.

Wendy writes for the United States Press Agency and is a former columnist with the Fulton County Expositor, Wauseon, Ohio.

Source: FBI Phoenix press release May 24, 2022

Article online:
https://www.uspa24.com/bericht-20875/protecting-against-personally-identifiable-information-pii-theft.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Wendy Westhoven

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Wendy Westhoven

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619