ARMY CRIMINAL INVESTIGATION DIVISION

12 September 2024

Cybercrime Prevention Flyer

National Public Data Breach 2024

National Public Data (NPD), a Florida based consumer data broker that performs background checks, was the target of a massive cyberattack impacting hundreds of millions of Americans.

The hacker, using the moniker “USDoD,” successfully breached NPD’s database in April 2024. Stealing 2.9 billion records, USDoD began posting the stolen data for sale on the dark web for $3.5 million. The records consisted of names, addresses, phone numbers, and social security numbers of over 272 million people.

Though everyone in the U.S. has not been impacted by the data breach, it is important to monitor for indicators of compromised personal information. It is also recommended to secure all accounts using two-factor or multi-factor authentication and routinely change passwords. As of October 2023, the Federal Trade Commission announced the three main credit bureaus have permanently extended a program entitling everyone to a free credit report every week.

Tips for Individuals Impacted by a Data Breach

• **Change passwords:** Use a combination of upper and lowercase letters, numbers, and symbols. Make sure it’s not easily guessable, like “password123.”

• **Use different passwords:** It is recommended that passwords are not reused for any account.

• **Enroll in two-factor or multi-factor authentication:** This adds an extra layer of security by requiring a second form of verification beyond just your password.

• **Authentication requests:** Do not approve authentication requests you do not recognize.

• **New accounts:** When opening a new account, immediately configure the privacy and security settings.

• **Monitor accounts:** Monitor your credit card and bank accounts for suspicious transactions and notify the financial institution if you notice anything suspicious.

• **Monitor credit reports:** Obtain free credit reports, AnnualCreditReport.com, to identify credit changes or suspicious accounts. Consider placing a free credit freeze or fraud alert notification with the three national credit reporting agencies, Experian®, TransUnion®, & Equifax®.

• **Keep software updated:** Software updates fix bugs and resolve security issues.

• **Be suspicious:** Be suspicious of unsolicited phone calls or emails requesting additional information. Do not click on any unknown links or download any unknown files provided in emails.

ADDITIONAL RESOURCES

Federal Trade Commission: You now have permanent access to free weekly credit reports

Social Security Administration: Fraud Prevention and Reporting

Authorized for widest release, without restrictions.

CPF 00075-2024-CID461

To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

Cyber Field Office