August 22, 2024

The Dizzying Heights of Cyberattacks to Steal Personal Information

By Ethan Shapiro

It is bad enough that foreign governments continue to attack and successfully steal valuable information from the US government. Recently, Americans have also learned that much of their personal information has been stolen due to an April cyberattack against National Public Data (NPD), a company that obtains and reviews personal information for background checks to employers and investigators.

Officials first realized the severity of the breach when they discovered that a group of hackers offered to sell the data for $3.5 million in an online forum for cybercriminals. According to the Washington Post, the extent of the theft allegedly includes every American social security number.

National Public Data's wishy-washy explanation of the "security incident" is troubling. The statement neither confirms nor denies the theft, stating that "there appears to have been a data security incident that may have involved some of your personal information."

Clearly, America needs to do much more to protect sensitive electronic information. We must up our game.

Implications

The ramifications of the NPD hack are personal. Nearly three billion people from the UK, US, Canada, and elsewhere are now vulnerable as a direct result of the cyberattack, according to the Los Angeles Times. Those affected could face fraud and identity theft.

With that in mind, now is a good time to start practicing better online habits, like creating harder-to-guess passwords, freezing your credit, using two-factor login, and monitoring whether any of your passwords have been compromised on the dark web.

Potential Solutions

Jen Easterly, director of the US Cybersecurity and Infrastructure Security Agency (CISA), believes the war on cybercrime "will be won when we are truly able to catalyze an approach to secure by design software."

For context, the secure by design principle requires vendors to beef up their protective measures. Nearly 200 companies have pledged to incorporate and implement safer digital practices.

Still, Easterly and CISA cannot win this critical fight alone. At the government level, cybersecurity needs to be prioritized. Current practices have not significantly deterred or prevented digital crimes. There needs to be an overarching government effort towards improving cybersecurity.

The government's current approach shows future criminals that they can steal from the American people and often get away with it—not exactly disincentivizing. The government must coordinate much better to protect American private information from bad actors.

Ethan Shapiro is the Program Manager at the Lexington Institute, a public policy think tank in Arlington, Virginia.