DigiKnow
CYBER SECURITY DEPENDS ON YOU

SYNTHETIC FRAUD - IT'S A REAL THING

January 2022 | Issue 2022:1

The Journey Continues
my.delaware.gov

Digital government services are rapidly expanding in the State of Delaware. Offering secure access to an individual with a proven identity via a single sign-on solution for constituents allows people to easily make purchases and transact personal business with multiple state agencies using a single, validated personal identity.

This solution offers identity and access management for Delaware's many digital government endeavors, offering a highly personalized experience to anyone with a relationship to state government.

This change in access is part of an overall hardening of the state's defenses of your personal information and other sensitive state data against bad actors. Data security breaches have the potential to incur great costs, both to the state and to individuals whose information is compromised. State of Delaware employees are the first to be invited to migrate to this new identity system.

A secure single sign on adds a measure of identity protection to employees and constituents. It offers another way to validate who a user is, prior to permitting them to access state services. It helps to ensure that the user is not actually a bad actor pretending to be a constituent.

DTI acts with the full knowledge of, and in concert with, the other state entities who are responsible for employee data: the Office of Management and Budget and the Department of Human Resources.

Be on the lookout for additional information on this transition. Presently the Team estimates that most state employees have created their my.delaware.gov identity by the end of the first quarter of 2022.

Solomon Adote
Chief Security Officer

The Fastest Growing Cybercrime

Synthetic identity theft is the fastest-growing cybercrime in identity fraud. Cybersecurity experts estimate that synthetic fraud costs banks $6 billion annually. Synthetic identity fraud differs from traditional identity theft because criminals don't steal an entire identity, they create one using a combination of real and fake information, explains the FBI. When this new identity is used to apply for credit, a new credit file is generated, making the fraud often difficult to detect.

Cybercriminals use this fake persona in two ways: a one-off use to get a credit card for a single large purchase or cash withdrawal or to create a persona to get a tax refund or unemployment benefits. Another scam is to use the synthetic identity to build up a high credit limit. When the desired limit is achieved the scammer goes on a giant spending spree and disappears into the wild.

Children, the elderly and the homeless are most vulnerable to fraud like this. As populations that don't use their credit as frequently (and therefore are much less likely to monitor it regularly) their Social Security numbers (SSN) are likely to be the ones that can be used and abused without notice. Children have become especially susceptible since the Social Security Administration (SSA) started randomizing the SSN in 2011.

Online banking has made complex fraud like synthetic identity theft easier to carry out. Data breaches have made valuable personal information like SSNs more susceptible to theft and sale on the dark web.

The My.Delaware.gov initiative is a tool in the fight against synthetic fraud by providing those who work for state government or access state services with a secure single sign on. This lessens the number of times personal information is potentially exposed by eliminating multiple sign-ins.

Here are some ways to protect your identity from synthetic fraud:

Leverage the power of your bank. Financial institutions have upped their synthetic fraud mitigation strategies and are taking steps to improve verification processes. For instance, they have two-factor authentication and may flag or question the use of a new email address or phone number.

Check your credit report. This is one of the best ways to see how your credit profile is being used to protect yourself against identity theft and have a quick recovery if your identity is stolen.

Opt-out of people search sites. If you don't want to appear in these types of search sites, the easiest and most reliable way is to use a deletion service.

Monitor and scan for the bad stuff. The information being sold on the dark web after a data breach is ideal fodder for thieves to piece together identities. Look into security software that performs regular scans of your devices. Your service provider may offer tools to protect your devices.