The Weekly Briefing

The latest cybersecurity updates from the Information Security Office.

Becoming Someone Else

Have you ever wanted to be someone else for a day or two? Cybercriminals have. In fact, they're actively searching for ways to become someone else all the time via a scam called identity theft.

Identity theft typically involves the use of stolen or leaked personal information to commit fraud. The most common type is financial identity theft, where the thief opens new credit card accounts or applies for bank loans in the victim's name. Let's walk through a few other examples.

Synthetic Identity Theft

A synthetic identity is completely or partially fabricated. Commonly, a legitimate national identification number is used in combination with a fake name, address, phone number, and birthdate to create a fake person.

Child Identity Theft

This scam targets children by using their information to open a new account or line of credit. What makes child identity theft especially unfortunate is that it is often carried out by a family member, and most victims don't realize they've been scammed until they're much older.

Medical Identity Theft

If an identity thief seeks medical care under the stolen identity of another person, the thief's medical history may be added to the victim's medical records. This information is difficult to correct and may affect future insurability.

Business Identity Theft

Also known as corporate or commercial identity theft, this scam occurs when someone poses as an owner, executive, or employee of an organization. The goal is to leverage that organization's credit or reputation for financial gain.

In all cases, identity theft is costly, emotionally distressful, and and often requires a long recovery period for victims. Don't let it happen to you or anyone associated with our organization! Take extra precautions when handling confidential information to ensure it never ends up in the wrong hands.

15 July 2022