I received one of those dreaded notices a few weeks back. There has been a breach of data — not on a credit card account, but on my health insurance. Medical identity theft is the latest in a series of types of identity theft.

If someone gets control of your identity and health insurance, they can schedule a doctor’s appointment, get prescriptions, use your insurance to pay bills and get many types of medical care. If their medical records get mixed in with yours, it can change treatments, bills and insurance claims and can even affect your credit report.

The number of people affected by medical identity is going up. A recent report shows that the incidence of medical ID theft has nearly doubled in the last five years, with a half million more victims in 2014 than in 2013.

In addition, the cost to victims has also gone up with twice as many people having to pay out of pocket expense. These thefts have caused financial costs when victims have to pay to correct their medical identities and the resulting problems.

The greater problem is that victims are being misdiagnosed, mistreated and have been delayed in receiving health care as a result of mixed medical information.

How do you discover if you are a victim of medical identity theft? Read your medical statements and the explanation of benefits provided by your insurance company. These records can show warning signs of identity theft. If you have a bill from a provider that you don’t recognize or if you did not receive the treatment charged for, someone else might have stolen your medical plan. If you see a mistake or do not recognize a charge, contact your insurance company immediately.
The Federal Trade Commission lists these signs of medical identity theft: a bill for medical services you didn’t receive; a call from a debt collector about a medical debt you don’t owe; medical collection notices on your credit report that you don’t recognize; a notice from your health plan saying you reached your benefit limit; and a denial of insurance because your medical records show a condition you don’t have.

Your medical insurance and information is valuable to thieves. Watch for these techniques to steal your information.

An offer of free health services may seem to be a great deal. But if they require that you provide health care information before treatment, run. They may tell you they work for a doctor, a clinic, a pharmacy or even your insurance company and will try to trick you into giving the information they need to compromise your identification.

If you get a phone call or an email, don’t give out your medical or insurance information. Only share the information if you started the call or you are certain who you are talking to.

Procedures designed to deter other types of identity theft also work with medical records. Keep records in a safe place and shred insurance forms, prescription statements, physicians’ reports and labels from prescription bottles before throwing them away.

If you are entering information on an Internet site, make sure you know the website is legitimate. Be sure you know who will be receiving the information, why it is needed and how it will be secured.

A safe site has a lock icon on the browser bar. Or check for an address that says “https.” The “s” signifies a secure site.

Medical identification theft is on the rise. Don’t be a victim.

Roxie Rodgers Dinstel is associate director of Cooperative Extension Service, a part of the University of Alaska Fairbanks, working in cooperation with the U.S. Department of Agriculture. Questions or column requests can be e-mailed to her at rrdinstel@alaska.edu or by calling 907-474-7201.