savannahnow
Savannah Morning News.

Are you at risk for identity theft?

By DeAnn Komanecky
Posted Oct 14, 2017 at 7:55 PM

We all battle an unseen enemy each day, and this war won't likely end soon.

The prize is your personal identifying information. Every bit of information that shows who you are is at risk, and the enemy could be anyone, anywhere.

Your name, date of birth, address, Social Security number or other information can be stolen and used in a variety of nefarious ways.

The battlefield has recently expanded as, once again, identifying consumer information held by a large corporation has been compromised. By some estimates, every one may have been affected in some way. The breaches are large and cover a diverse group across the country and beyond.

Credit monitoring giant Equifax admitted in early September that the personal data of 145 million consumers, including Social Security numbers and dates of birth, were available for theft by hackers.

The list and numbers have grown over the past few years: Yahoo, all 3 billion email accounts; Target, up to 110 million customers' credit/debit card numbers; Ebay, all 145 million users' names, dates of birth, addresses and passwords; U.S. Office of Personnel Management — personal information of 22 million current and former federal employees, including in some instances, security clearance information and digital fingerprints of employees.

The OPM case is especially troubling for federal employees with security clearances, as forms they file have extensive personal information listing former address, foreign travel, family members and other financial information. The FBI arrested a Chinese national in relation to the hack in August.

What can you do?

To protect yourself takes knowledge — and persistence.

"It takes constant vigilance," Keith Fletcher, CEO of Savannah business tech firm, Speros.

Fletcher said caution is a must while online, whether you are reading email, shopping, or just surfing the web.

“It goes back to don’t talk to strangers,” Fletcher said. “Better yet, even if you know the email sender, always ask ‘was I expecting something,’ if not don’t open it.”

Fletcher said people must also be careful when visiting web sites.

“Don’t just go around willy-nilly,” Fletcher said.

When visiting websites be alert for those that may look like that of your bank, or other account.

Data thieves are good at making counterfeit sites, Fletcher said.

One help is to place a freeze on your credit.

“You have to do it all three credit bureaus,” Flethcher said.

The big three are Equifax, TransUnion and Experian.

Freezes can be lifted by you as needed.

Business responsibility

Businesses have a responsibility and a legal obligation to properly protect the information of customers, Fletcher noted.

“Businesses must have a good fully complainant firewall,” Fletcher said. “And it has to be continually updated.”

Fletcher’s tip for small businesses? “Rent a firewall, don’t buy it,” Fletcher said. “Then it’s their responsibility to keep it updated. If something happens, they are on the hook — it’s not your problem.”

Personal responsibility

For the rest of us, the work of making sure someone doesn’t take out a loan or file a tax return in our name, falls on us.

“The burden is all on the consumer,” said Savannah attorney Ben Karpf, an attorney at Bouhan Falligant. Those who’ve discovered their information is part of the Equifax breach aren’t likely to know what personal data was exposed.

“There’s a patchwork of laws across the United States about notice,” Karpf said. “There’s wiggle room in the Georgia statute and it doesn’t require you to be told what data was compromised.”

People have to visit equifax.com and follow instructions to find if their information may have been compromised.

Having your information stolen is one thing, having your information stolen — and then used — is another.

They both require vigilant monitoring, but the second can involve serious problems.

More than online theft

Your identifying information isn’t being only stolen online, notes Brian Tanner, U.S. Attorney for the Southern District of Georgia.

Tanner pointed to a growing number of prosecutions that have gone through his office.

Tax fraud grows

In one case, 13 people, mostly from Statesboro, were convicted in a stolen identity and tax fraud case.

Using personal information stolen from medical records in a doctor’s office the criminal group used the information to file fraudulent tax returns.

“We see a lot of this,” Tanner said of filing fraudulent tax returns. He said the attorney’s office has enough of these cases that they have their own acronym for them, SIRF — Stolen Identity Refund Fraud.

Tanner said the victim rarely knows someone has filed their return — and received their refund — until the victim’s actual return is rejected by the IRS.

Another case prosecuted here in the Southern District involved a Savannah man “befriended” two Wells Fargo bank employees, convincing them to get people’s identities in order to steal cash from Wells Fargo bank accounts. The man targeted the elderly for his victims. He was convicted of 15 counts of bank fraud, aggravated identity theft, and aiding and abetting theft by a bank employee.

In yet another case, a Jesup man pleaded guilty to using the stolen identities of at least 26 people and filing 35 fraudulent tax returns. The man received over $280,000 in fraudulent refund payments.

These tax refund thieves aren't stealing your W-2 forms, Tanner said. "They dummy up W-2s." They also adjust income and deductions to result in a refund, he said.

Many of those who file false tax returns are caught because of addresses, Tanner said. Tanner added they tend to have the refund checks sent to only a few different addresses.

'The IRS keeps track of where refund checks are sent," Tanner said. The criminals will trigger notice by having dozens of refunds sent to each address.

Legal remedies fall short

Generally for a person who has had their information used in some sort of online hack, there isn't much legal recourse, Karpf said.

"The person who stole the information is the least likely person to be found," he said. "There are also jurisdiction problems."

The chances of collecting a dime from those perpetrators are nil, Karpf said. But, he said, ID theft where there is a personal relationship is easier to pursue for financial damages. Examples include using an elderly person's information by a family member or caretaker, along with parents who use their child's Social Security number to obtain credit. In those cases, there is someone known to hold accountable.

Direct financial remedies are still hard to collect, but they can be prosecuted, he said.

Karpf, Fletcher and Tanner all agree on a number of points:

File a police report if your information is being used fraudulently.

"Start with local police if you think you've been a victim," Tanner said. "You can also contact the local FBI office," Tanner said. "It may be that everyone in the country has been a victim."

Checking your accounts often for unusual activity. Many may have heard similar advice before, but it bears repeating — and following, Fletcher said.

"Make it a habit," Tanner said. "It may be now that everyone in the country has been a victim."

MOST POPULAR STORIES