Protect financial information from theft

chicagotribune.com/business/yourmoney/sc-cons-0130-save-20140131,0,6417852.story

Debbie Carlson Special to Tribune Newspapers

12:10 p.m. CST, January 31, 2014

News about the data breach at Target, and subsequent data breaches at other major retailers, are reminders that theft can occur at any time and any place, and information security experts say that it's also a good time for people to review how secure they keep their financial data.

Initially, Target said malicious software took payment card information at infected point-of-sale terminals at checkout counters, but later the retailer said information such as email addresses were also taken during the breach, separate from the payment information.

As the breach is investigated, consumers need to understand what it means and how to protect themselves, said Neil Chase, vice president of education at LifeLock, an identity theft-protection firm.

And that doesn't mean moving to a cabin in the woods with no electricity and never shopping, he said.

There are a lot of ways to have information stolen, he said, such as a credit card or debit card falling out of a wallet and into the wrong hands; someone physically stealing the card; or a person who goes through garbage looking for statements.

The Target breach also showed that shopping in person isn't necessarily safer than online or by phone, he said, as payment information goes through a number of hands, no matter what the shopping method.

Credit cards offer more protection. If a person's credit card or debit card had fraudulent activity on it, their liability is very low and may be zero, depending on the card. Federal law says credit card holders won't be responsible for more than $50 in charges, but many companies say they have a zero fraud guarantee, Chase said.

Sometimes credit card or debit card companies will notify cardholders if they see unusual activity and cancel the card for the person. If the person sees unusual activity on their card, he or she should call the issuing company right away and cancel the card.

With a credit card, the issuing company usually cancels the charges and reissues the card, which is generally the end of the problem, Chase said. With debit cards, it's a slightly different story.

Chase said federal law says a person doesn't have to pay if there's fraud or abuse on a debit card as long as the cardholder quickly reports an unusual activity, so the onus is on the cardholder to act fast.

The Council of Better Business Bureaus said that because debit cards don't offer the same protection as credit cards, cardholders should vigilantly monitor their accounts, especially since debit card transactions take money straight from a bank account. Individuals who are concerned that their data was compromised may want to pre-emptively ask for new debit card or put a security block on the account.

Chase agreed, adding: "If someone misuses your debit card … and if they take out as much as you had for the rent or mortgage payment the day before the auto payment comes out, yes, the bank will fix it eventually. Meanwhile, your mortgage company or landlord is mad at you and you start running into the late payments."

For those who use debit cards to avoid racking up debt, other payment options include using a prepaid card or cash, but then there's also the risk of loss, he said.

Once a credit card or debit card is canceled, the next step is to monitor credit reports, said Chase and Tony Anscombe, senior security evangelist for AVG Technologies, an Internet security provider.

People can get a free report once a year from each of the credit reporting agencies — Equifax, Experian and TransUnion. The credit reports will show whether new lines of credit or loans were opened.

Anscombe said customers affected by the Target breach can receive free identity-theft protection services, and he urged they take up Target on the offer. Identity theft protection looks beyond just credit reports and sees if a thief is building a new identity based on the person's data. By piecing together information such as a birthday, email addresses and so on, thieves can start to get more aggressive and do greater damage, such as creating fake IDs or perhaps using information for medical treatment, they said.

Killing phish. Because Target is offering identity-theft protection, scammers are trying to piggyback on the news by sending out fake emails, known as phishing scams, the experts said.

Scammers will tell you that your card was compromised and suggest actions to "fix" the problem, the Better Business Bureau said.

Many of these emails will have deceptive links, or ask for a Social Security number or other personal information. Instead of clicking on the link or calling a phone number in the email, Anscombe said to go the official website (**target.com**) and call the company if you're not sure if the email is legitimate.

There are other simple steps to take to prevent identity theft, Chase and Anscombe said. Leave the Social Security card at home; have more than one email address in case hackers get access to the primary email address; and don't use the same password for all accounts. Regarding passwords, add capitalization or punctuation to make them harder to crack. If it's a password for a bank account, make it as cryptic as possible. Don't use common passwords like "123456" or "password," they said.

Finally, Anscombe said, realize that personal data is important and safeguard it. Question why someone needs it.

"You should value your information highly. If it's for a loyalty card, do they need your phone number or birthday so you can get $10?"