Identity Theft:

An Overview on Staying Safe

By Jessica Hendon
Vice President Physical & Information Security, Blackhawk Bank

Credit. It seems simple enough. Borrow money, pay it back, and repeat if necessary. But, what if someone else is borrowing in your name, not paying it back and leaving you virtually helpless when you need to secure a loan? You've just become a victim of Identity Theft.

Unfortunately, this has happened to millions of people. According to javelinstrategy.com's *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*, there were 14.4 million victims of identity theft and fraud in 2018. Approximately $4 billion was taken in account takeover. And, worst of all, 23 percent of fraud victims had unreimbursed personal expenses.

We can imagine that every person affected by identity theft was left wondering, "How and where did they get my information?" There are a variety of ways that identity thieves can get your personal information. Sometimes you are unknowingly the source. Other times, there are circumstances out of your control. Here we explore common ways these thieves get personal information and how you can take steps to avoid it.

Data Breaches

What is a data breach? Probably the most common way criminals get personal information is through a data breach. A data breach occurs when an unauthorized user gains access to a company's computer network. In some cases the criminal can "attack" the system or trick an employee into clicking on a link that allows access to their computer. No matter the method of the breach, thousands or millions of pieces of personal information can be obtained in seconds.

The responsibility for avoiding a data breach nearly always falls on the company. Applying updates and patches to their systems can reduce the company's risk for a breach. Most importantly, training employees on appropriate computer system usage, limiting the ability to download information and teaching them how to spot a phishing attack are great steps any organization can take to circumvent unwitting attacks.

How to avoid a data breach. Data breaches can be the hardest form of identity theft to avoid. We trust that the companies and organizations we do business with are committed to safeguarding our information. So, when a data breach occurs, we feel betrayed and frustrated. Though you may not be able to avoid a data breach, you can take steps to limit the possibility of becoming a victim.

Don't wait for a data breach to occur. It's not a matter of *if,* but *when.* Take advantage of a credit monitoring service. Though there is typically a cost with this type of service, it can help you avoid paying much more should your personal information be illicitly obtained and used.

In addition, federal law allows you to check your credit report once a year. But, simply checking your credit score is not enough. Be sure you are getting your full credit report, which gives you a true picture of your credit worthiness. Visit the Federal Trade Commission website to obtain your free annual credit report.

Dumpster Diving

What is dumpster diving? Your trash can be a treasure trove for criminals, where they can find personal and work information, account numbers, mail, calendars, phone lists, etc. Once a dumpster diver has this information they can begin duplicating your profile. They now know where you live, work, play and bank. They may even know your friends and family, simply by taking the time to put the pieces together. All of this information can be used to gain access to your financial accounts, even your social media profiles.

How to avoid being a dumpster diving victim. While it seems unnatural, and quite frankly, disgusting, for someone to want to pick through garbage, it does happen. To avoid someone obtaining your information this way, always shred personally identifiable information, records and statements with a cross-cut shredder. This type of shredder allows you to shred your document into tiny particles that are nearly impossible to piece back together.

Another safeguard is to take advantage of area shred days. These are common among local businesses and are almost always free. Keep an eye out on social media and in the local paper and you're bound to come across one.

If you are going to put your trash out, do it in a well-lit area with lots of traffic. Criminals are less likely to cause a scene in public, since the risk of being caught is greater.

Phishing

What is phishing? According to phishing.org, "Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords." The victim is usually none the wiser, until they start getting calls on past due or overdrawn accounts.

How to avoid being caught in a "phishing" net. First and foremost, never give out personal information over the phone or through email, if you have not initiated the contact. Legitimate businesses and organizations will never ask you for information they should already have. If someone does contact you from a business, ask to call them back. Find the correct phone number listed for the business by looking it up on their website or in a phone book. Most likely, they had not attempted to contact you and will appreciate the heads up that someone is posing as an employee of their business.

Do not click on attachments or links within emails you are not familiar with. Links and attachments can be infected with malware that once downloaded onto your personal or work computer can invite a data breach, your personal information being stolen, or your company's confidential information being compromised. If you suspect an email of phishing, report it right away to your company's Technology Department. Or, if it is your personal computer, block the email address and delete the email right away.

Only visit secure websites. Websites can ask you for secure information when you are entering their site. This should be a red flag. If you do not have a previous account set up, do not enter any information. This is an elaborate way to look official, when in actuality they are attempting to get as much information from you as possible, either for legitimate or illegitimate use.

There are numerous other ways that criminals can steal your information, and they are coming up with new ways every day. The best way to be prepared is to be aware. Thinking "it won't happen to me" and becoming complacent allows you to become vulnerable to identity theft.

Learn more about how Blackhawk Bank can keep you safe with Watchdog Checking and ID Protect.

Blackhawk Bank

MEMBER FDIC EQUAL HOUSING LENDER