How to prevent identity theft

By Andera Lakai

25 Aug 2015

In this age of technology, having access to information at our fingertips, everyone once in a while lie awake at night losing sleep over identity theft and its consequences.

Andera Lakai

Identity theft can be a harrowing experience because of financial loss as well as mental trauma. Minors and teenagers are also fast becoming a favoured target.

This article aims at getting our readers acquainted with various identity theft scenarios and also how to arm themselves against such attacks. Even after this, if you find yourself falling prey to such scams, read on to know how to handle such crisis in an effective manner.

Let's begin by defining the culprit and know exactly what identity theft means in simple terms. It is misusing your personal information, hacking into your computers, laptops, phones, pads, tablets, breaking into your email accounts, sending phising spam emails, hacking into online bank accounts, using your passwords, PAN number, social security number, driving license number, buy phone or make any small or big investment, or purchase under your name without your authorisation or use a credit/debit card which is not pre-approved by you.

Here are the most effective methods to prevent identity theft:

Case 1

Filling in a seemingly innocent survey at a mall, some high-end store or even for some agency, asking for basic personal information like driver's license number or you phone number and e-mail id. All this information serves as 'consumer data' but could also be used to extract your personal data leading to invaluable loss.

Though you might wonder how such basic information could be used to hack your password protected accounts and information. We must keep in mind that most of us do not tend to change our passwords regularly; hence, making them more susceptible to attack. Further, all these snippets of information together is enough for professional hackers and other malicious activists to cause damage to your files and leak or misuse your information, be it personal or financial.

- So, step one is to question yourself every time you fill in a form/survey. Ask the personnel how is the personal information asked necessary for their database. Usually just filling in your phone number and/or email ID is sufficient and giving details such as your address, driving license number, PAN number etc., are not really necessary.
- Change your passwords regularly.
- Use passwords with strong strength i.e. using lower and upper case characters with various combinations of numerical and signs as !@#$%^&*().

Case 2

Purchasing products online or making payments of your bills online, or divulging your financial/personal information via text or email as they are not encrypted, hence, vulnerable to interception. Such identity theft is usually difficult to detect and prove. Though this must not put you off online shopping and payment as it is without a doubt convenient. Following a few simple steps will ensure you a safer online experience.

- Contact your bank regarding their policy of revealing or sending sensitive information via wireless communication.
- Use one time passwords (OTP) generated on the spot and valid only for few minutes which doing online payment.
- Do not reveal your full credit/debit card number. Only the last three digits are usually required.
- Clear your cookies, cache and temporary files regularly.

Case 3

Medical insurance fraud is very much prevalent. The consequences of these kinds of scams are more dangerous than just monetary losses. Falsified medical records, if went unnoticed, the fraudulent entry of medical history could lead to a misdiagnosis which could endanger the insured person's life and prevent them from getting the medical treatment and care that they deserve.

- Ask your medical service providers and insurance agencies to contact you whenever a claim is made.
- Have a family doctor to whom you could divulge your personal details without having to deal with the management staff, from where your information is more like to get mislaid.

Case 4

When your wallet gets stolen, leading to multiple accounts hack, and all your credit /debit/ identity cards falling into wrong hands. In such scenarios, by the time you will close one account, other might have had been misused.

- You could take services of Identity theft protection service providers. At present, ruling the roost is Lifelock Ultimate Plus (at $29.99/month), followed by Identity Force Ultra Secure+Credit (at $14.99/month).They give you monthly updates on your credit card scores with email and SMS notification.
These services ensure protection of your accounts and detection of any suspicious activity on your cards, personal and financial information. Though recently Lifelock came under the scanner by a certain agency for not meeting its obligation, it is reliable unless said otherwise by a federal court.
- Such services come with a traditional $1m identity theft insurance and/or they spend up to $1m on legal fees, application fees and other expenses to restore your identity.
- Some service providers as allclearid and creditsesame provide similar services for free.

Case 5

What if such a card protection service provider fails to do its job and they themselves misuse your data or compromise your data because of a breach, hack or a leak? It is then time to step up your game and take the matters in your own capable hands.

- Approach AnnualCreditReport.com to get your credit report from source itself in pdf of by calling (877)322-8228, no third party involved. Contact credit reporting agencies in writing and include copies of documents that support your claim along with in Identity Theft affidavit. Contact any one of Equifax, Trans Union and Experian.
- File a complaint with Federal Trade Commission at their hot line (877)438-4338.
- File an FIR at the police station.

Case 6

Identity theft via stolen smartphones. Our phones have lot of private data and also access to our e-mail accounts and financial details thanks to mobile banking and cloud back-up.

- Basic numerical or pattern password will not give your protection indefinitely but it will delay the access time; meanwhile you can remotely remove the data on your phone.
- Remote wiping software's allows you to ring, lock and erase your data.
- For android phones, android device manager (ADM) can be activated beforehand via a gmail account. Going to its website you can easily erase the data on your phone whenever it is powered up.
- For iOS based phones, ipads and Mac laptops, similar service can be activated from icloud on My iphone.

Case 7

Most regular case is if you accidentally click on some suspicious website of on a phising scam email claiming you have won something.

- Run an antivirus and antimalware software such as Malwarebytes, an effective and free software.
- Delete the email account in question.
- Do not click on pop-up ads. Block such pop-ups by going to the settings section of your browser.
- Send an email to your contact list to warn them against any email sent from your account to them.
- Increase the protection on your firewall.

All these small but effective measures will ensure you. Though this must not put you off online shopping and payment as it is without a doubt convenient. Following few small but effective measures will ensure you a safer online experience.

ABOUT THE AUTHOR

Andera Lakai is a writer, blogger, speaker and financial expert. She enjoys writing about personal finance for the site [[modestmoney.com]]. You can contact her on [[anderalakai@gmail.com]]