CMSGu2016-01

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Online Identity Theft

CERT-MU

National Computer Board
Mauritius

Version 1.0

March 2016

Issue No. 1

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to give an insight on online identity theft, how it can happen and what precautions can be taken so as not to fall victims of the crime.

1.2 Audience

The target audience of this document include all users of the Internet.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on identity theft.

Section 3 explains how criminals use information on the Internet for identity theft.

Section 4 illustrates how to report online identity theft.

Section 5 gives some tips to minimize the risk of online identity theft.

Section 6 concludes the document.

Section 7 contains a list of references that have been used in this document.

2.0 Background

Identity theft is a crime whereby criminals impersonate individuals, usually for financial benefits. In today's society, you often need to reveal personal information about yourself, such as your social security number, signature, name, address, phone number, or even banking and credit card information. If a thief is able to access this personal information, he or she can use it to commit fraud in your name.

Having your personal information at hand, a malicious person could do various things, like apply for loans or new credit card accounts. They could even request a billing address change and run up your existing credit card without your knowledge. A thief could use counterfeit checks and debit cards or authorize electronic transfers in your name and withdraw funds in a bank account.

Identity theft can also go beyond a monetary impact. Thieves can use your information to obtain a driver's license or other documentation that would display their photo but your name and information. With these documents thieves could obtain a job and file fraudulent income tax returns, apply for travel documents, file insurance claims, or even provide your name and mailing address to police and other authorities if involved in other criminal activities.

3.0 Using Information on the Internet (Online) for Identity Theft

The outcome of identity theft is usually the same, regardless of how the thief obtains your information. However, the Internet is providing new ways for people to steal your personal information and to commit fraud. Thieves can accomplish their goal several ways such as using Internet chat rooms and spreading Trojan Horses that drop key loggers on your computer to transmit any passwords, usernames and credit card numbers you use on your computer back to the thieves. Many online businesses today also store personal information about customers and shoppers on their websites, and this provides another way for your personal information to be accessed, without your permission or knowledge.

Additionally, email phishing is another way that thieves can attempt to gather your personal information. Phishing emails falsely claim to be an established legitimate enterprise in an attempt to scam you into surrendering private information that will be used for identity theft. The e-mail will direct you to visit a website where you are asked to update personal information, such as password and credit card, social security, and bank account numbers — information the legitimate organization already has. The website, however, is bogus and set up only to steal your information.

3.1 Risks of Online Identity Theft

- Being tricked into divulging personal data in response to an email, text, letter or phone call.
- Theft of or access to paper documents (for example, bank statements, utility bills, tax returns, passport/driving licence).
- Sharing private information with family, friends or people who take you into their confidence.
- 'Shoulder surfing' – people looking over your shoulder at your computer or smartphone/tablet, or at the ATM.

3.2 Symptoms of Online Identity Theft

- Not receiving bills or other correspondence – suggesting that a criminal has given a different address in place of your own.
- Receiving credit cards which you did not apply for.
- Denial of credit for no apparent reason.

- Receiving calls from debt collectors or companies about things you have not bought.
- Unrecognisable entries on your credit history.
- You have recently lost or had stolen important documents such as your passport or driving licence.
- When buying or selling, you get complaints about non-delivery of or non-payment for goods you are not aware of.
- You see entries on your bank, credit or store card statement for goods you did not order.
- You cannot log into a site using your normal password (because a criminal has logged in as you and changed it).

4.0 Reporting Online Identity Theft

4.1 Should I report a case of online Identity Theft?

Online Identity Theft is a cybercrime and cybercrime can be particularly difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries. Moreover, many offenders disperse one online criminal operation only to start up a new activity with a new approach before an incident even comes to the attention of the authorities.

4.2 Who to contact?

Local law enforcement. Even if you have been the target of a multijurisdictional cybercrime, your local law enforcement agency has an obligation to assist you, take a formal report, and make referrals to other agencies, when appropriate. Report your situation as soon as you find out about it. Some local agencies have detectives or departments that focus specifically on cybercrime.

4.2.1 Collect and Keep Evidence

Even though you may not be asked to provide evidence when you first report the cybercrime, it is very important to keep any evidence you may have related to your complaint. Keep items in a safe location in the event you are requested to provide them for investigative or prosecutive evidence. Evidence may include, but is not limited to, the following:

- Certified or other mail receipts
- Chatroom or newsgroup text
- Credit card receipts
- Log files, if available, with date, time and time zone
- Messages from Facebook, Twitter or other social networking sites
- Printed or preferably electronic copies of emails (if printed, include full email header information)
- Printed or preferably electronic copies of web pages

5.0 Tips to minimize the risk of online identity theft

Once you discover that you have become a victim of cybercrime, your response will depend, to some degree, on the type and particular circumstances of the crime. Here are useful tips to follow for some specific types of cybercrimes:

In cases of identity theft:

- Make sure you change your passwords for all online accounts. When changing your password, make it long, strong and unique, with a mix of upper and lowercase letters, numbers and symbols. You also may need to contact your bank and other financial institutions to freeze your accounts so that the offender is not able to access your financial resources.
- Close any unauthorized or compromised credit or charge accounts. Cancel each credit and charge card. Get new cards with new account numbers. Inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions. Close accounts so that future charges are denied. You may also want to write a letter to the company so there is a record of the problem.
- Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft. For example, if a thief has access to your Social Security number, you should contact the Social Security Administration. You should also contact local authorities if your driver's license or car registration are stolen.
- File a report with your local law enforcement agency. Even if local police doesn't have jurisdiction over the crime (a common occurrence for online crime which may originate in another jurisdiction or even another country), you will need to provide a copy of the law enforcement report to your banks, creditors, other businesses, credit bureaus, and debt collectors.
- If your personal information has been stolen through a corporate data breach (when a cyberthief hacks into a large database of accounts to steal information, such as Social Security numbers, home addresses, and personal email addresses), you will likely be contacted by the business or agency whose data was compromised with additional instructions, as appropriate. You may also contact the organization's IT security officer for more information.

6.0 Conclusion

In online identity theft, victims and offenders can be on opposite sides of the world, that is, the cybercrime has no geographical boundaries. This is what makes it difficult for law enforcement agencies to investigate the crime, catch the perpetrator or help the victim. Therefore, it is crucial that we follow all best practices and not share too much information online. In case we need to share certain information online, we have to be vigilant so as not to fall into the trap of cyber criminals.

7.0 References

- **www.webopedia.com**
- **www.police.govt.nz**
- **https://staysafeonline.org**
- **www.staysafeonline.org**