DIGITAL IDENTITY THEFT

Story & Design: Poornima Meegammana

Artist: Maeve Tan

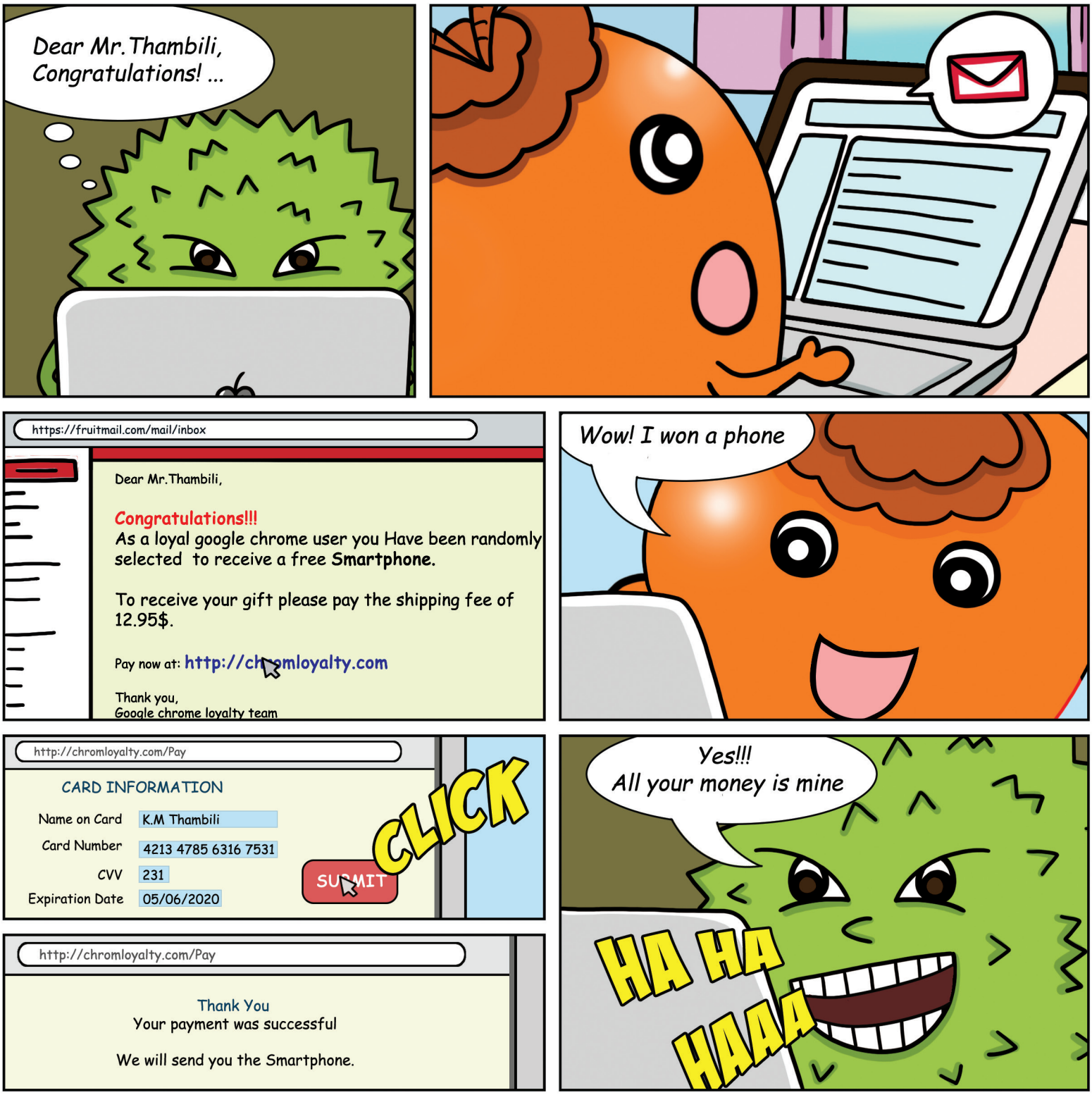
Digital Identity Theft

Introduction

Identity theft can happen both online and offline. It is collecting personal information about someone without his or her consent and using that information for criminal activity. For example using the credit or debit card details of another person and spending money which doesn't belong to them.

There are several ways in which somebody's identity can be stolen, one of the ways is phishing. This method is used by criminals to pretend to be other organisations (like a bank or company) which makes you think you are being contacted by the actual bank/company. Usually this is done using email or SMS and will include asking people to enter personal financial details.


CITY BANK
WELCOME
CITY BANK
Check
Thambili Enterprises
M K Thambili
Thambili@fruitmail.com
+94 7781 854 872
It's my lucky day
City Bank Alert
A transaction for
LKR 100,000.00 has been
credited to your account
Current account balance
LKR 446,000.00
CITY BANK


Dear Mr.Thambili,
Congratulations! ...
https://fruitmail.com/mail/inbox
Dear Mr.Thambili,
Congratulations!!!
As a loyal google chrome user you Have been randomly selected to receive a free Smartphone.
To receive your gift please pay the shipping fee of 12.95$.
Pay now at: http://chromloyalty.com
Thank you,
Google chrome loyalty team
Wow! I won a phone
http://chromloyalty.com/Pay
CARD INFORMATION
Name on Card K.M Thambili
Card Number 4213 4785 6316 7531
CVV 231
Expiration Date 05/06/2020
SUBMIT
CLICK
Yes!!!
All your money is mine
HA HA HAAA
http://chromloyalty.com/Pay
Thank You
Your payment was successful
We will send you the Smartphone.


ALERT
CITY BANK
How could this happen?
WHAT
City Bank Alert
A transaction
for LKR 446,000.00
has been debited
from your account
Current account balance
LKR 0.00
NOOO
All my money is gone.
Mr. Thambili lost all his savings because he trusted a phishing email and shared his personal information online.
Be careful when you provide personal information online.

Lessons Learned

Tips on safeguarding against phishing

- Beware of accessing suspicious URLs that require you to enter your bank details.

- Keep track of your credit card and banking statements to check for any suspicious transactions.

- Use only secure websites for financial transactions. If you enter credit card information online to make a purchase, you should see a lock in your browser's status bar, usually in the left corner. If you don't see the lock, don't enter your information.

- Don't reply to emails or follow the links in emails claiming to be from reputable institutions like your bank or university that ask for personal information. Contact the institution in question via phone or their website about these emails.

- Use common sense. If an offer sounds too good to be true ("Just enter your credit card number for a free trip to Paris!"), it is likely to be a scam!

- Don't send any personal information when using public WiFi. Public WiFis have low security and can be easily hacked.

- Look out for emails claiming to be from companies such as Norton Anti-Virus that prompt you to download something. Get in touch with the company on your own (do not reply to the email itself) to check if the information is true or not.