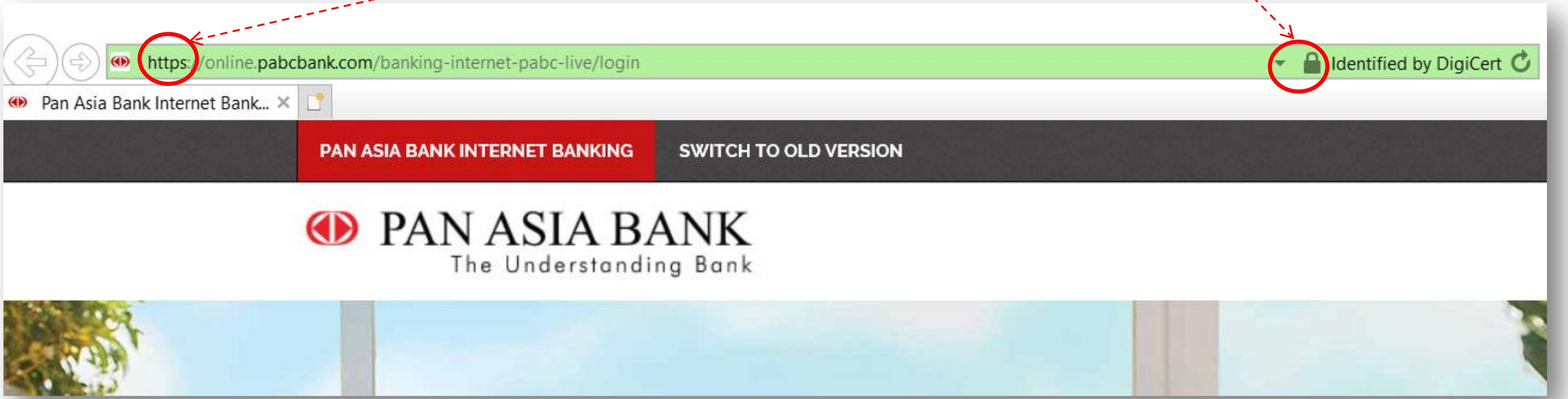
PAN ASIA BANKING CORPORATION PLC

DIGITAL BANKING USER AWARENESS

HOW TO PROTECT YOUR INTERNET BANKING IDENTITY ?

IS YOUR BROWSER SESSION SECURED?

Before making a transaction or entering personal information on a web site, check that your browser address window is green, the URL (web address) has changed from 'http' to '**https**' and that a closed **padlock** icon is present.

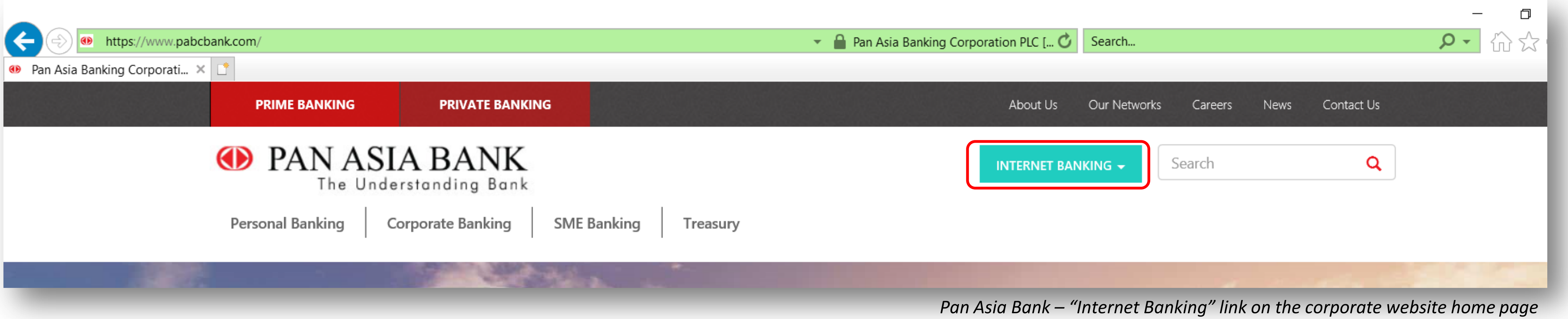


https://online.pabcbank.com/banking-internet-pabc-live/login
Identified by DigiCert
Pan Asia Bank Internet Bank...
PAN ASIA BANK INTERNET BANKING
SWITCH TO OLD VERSION
PAN ASIA BANK
The Understanding Bank

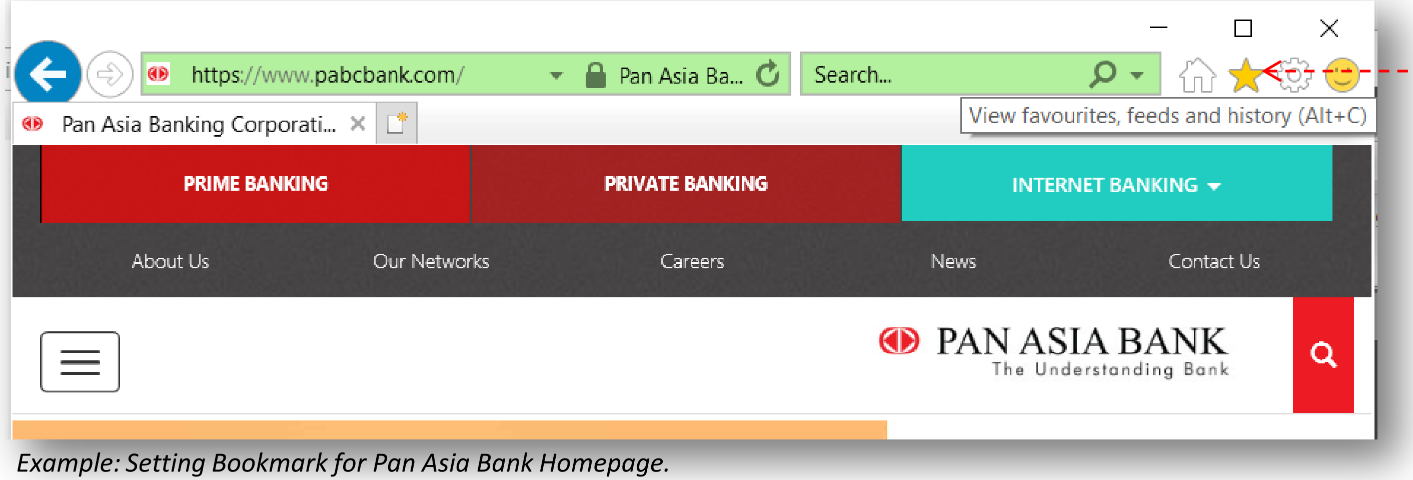
Pan Asia Bank - Internet Banking Login Page

SECURE ONLINE BANKING

Access *Online Banking* from the home page of our website or by typing the URL directly into the address bar.



Pan Asia Bank – "Internet Banking" link on the corporate website home page



...and bookmark it.

Example: Setting Bookmark for Pan Asia Bank Homepage.

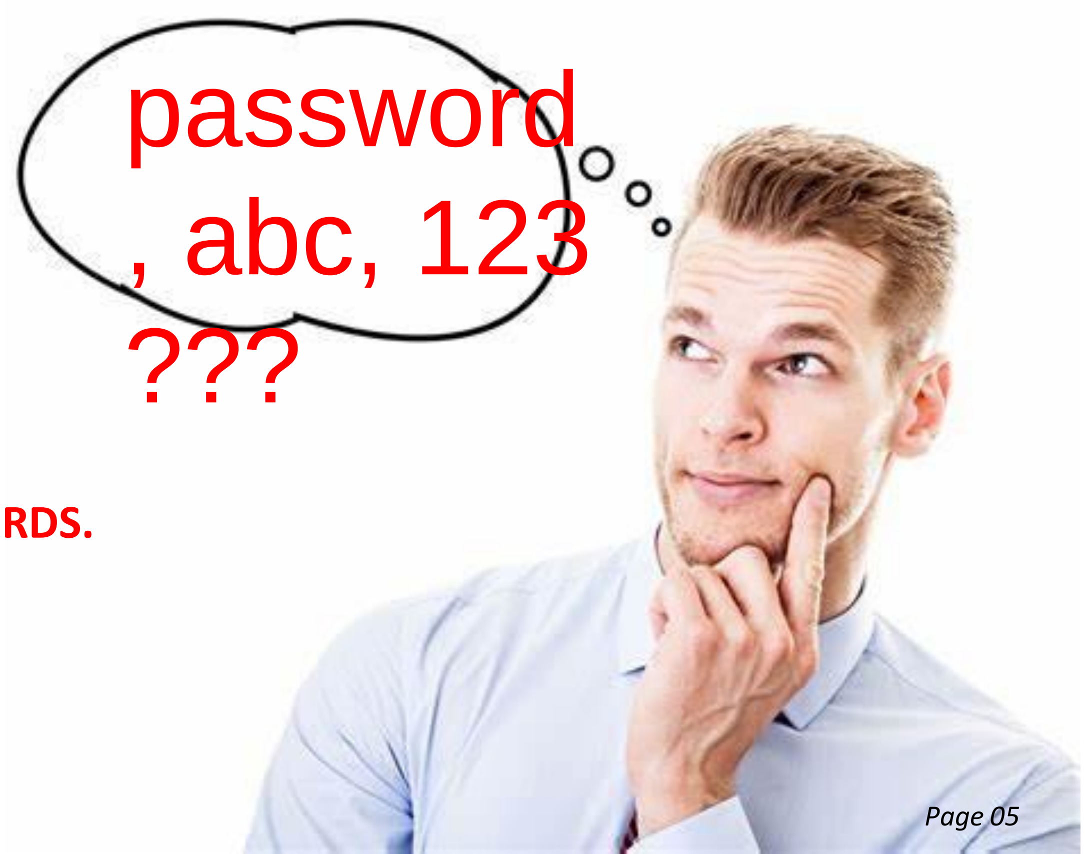
Review your account statements on a regular basis.

CREATE STRONG, UNIQUE PASSWORDS

Choose passwords for your online services that are difficult for anyone else to guess.

A strong password is:

- *long and complex (a variety of letters, numbers and other characters),*
- *unique (not re-used for other apps),*
- *current (changed at least every 90 days) and*
- *not obvious (avoid dictionary words, dates, names etc.).*



REFER NEXT TO LEARN ABOUT HOW TO CREATE STRONGER PASSWORDS.

CREATE STRONG, UNIQUE PASSWORDS

Contd...

A STRONG AND SECURE PASSWORD IS:

- Minimum of 8 characters – *the longer and more complex your password, the harder it is for someone to decipher / break it;*
- Made up of a variety of letters, numbers and symbols - *an upper (A-Z) & lower (a-z) case letter, a number (0-9), a special character(!, @, #, $, %, ^, &, * etc.);*
- Unique – *never reuse it for other websites or applications*;
- Current – *change it frequently, at least every 90 days (three months);*
- Easy to remember, difficult to guess – *avoid words in the dictionary, special dates (your date of birth etc., which others can easily remember / guess), your name or part of it; and*
- Never share it with anyone, even family or friends.

4ET%1ge6
✓
1234
✗

Image Source: Safeonline

CREATE STRONG, UNIQUE PASSWORDS

Contd...

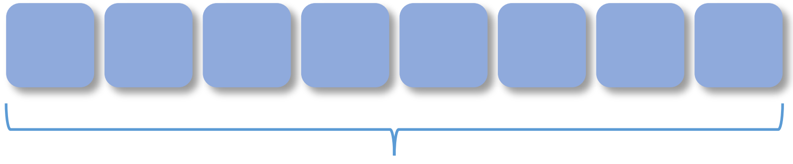
- Shorten a memorable phrase
  Create a password based on a phrase that only you know.

  Example: Assume your name is Nilmini and year born 1980.

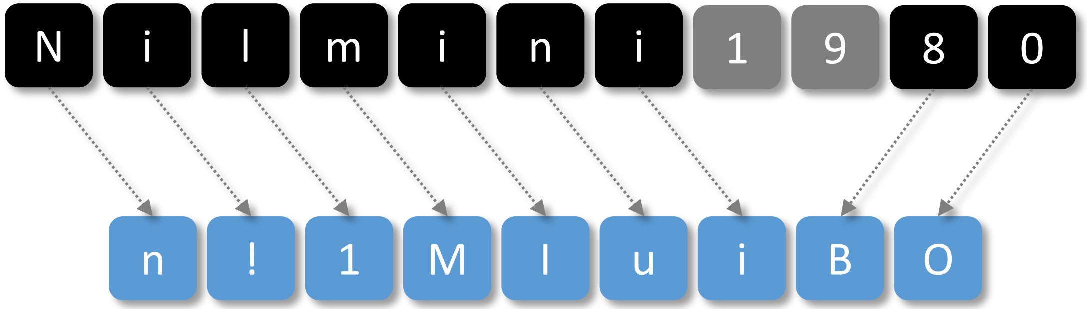
✓ We have to use combination of:

- A-Z and a-z
- 0-9
- !@#$%^&*()_+-={}|[]\:”;’<>?,./

✓ Minimum length



8 Characters



Don’t use exact example.

MOBILE DEVICE SECURITY

ALWAYS DOWNLOAD MOBILE APPLICATIONS FROM LEGITIMATE SITE(S)

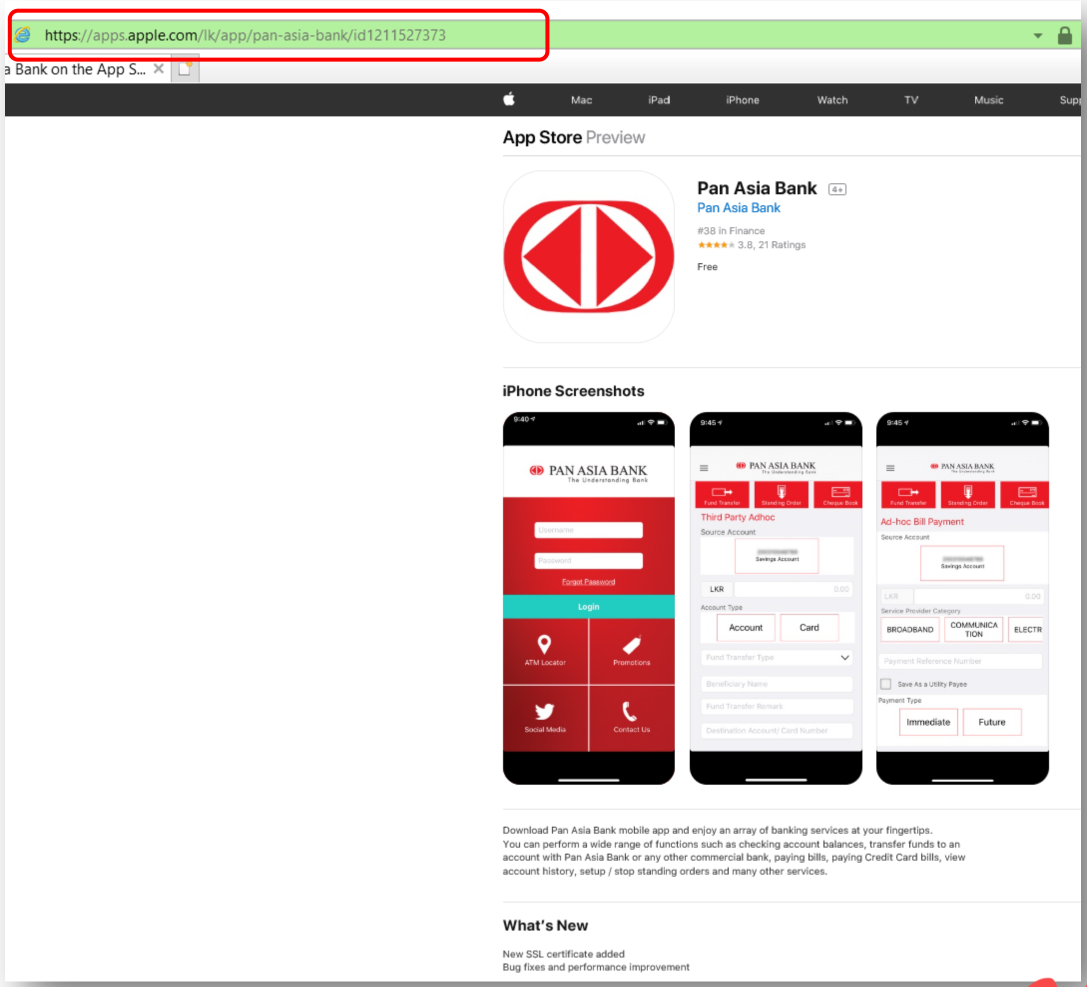
The way you use and download apps plays an important role in keeping your phone secure:

- Only install apps from official stores, such as ***Apple's App Store*** or ***Google Play*** (for Android phone or tablet);
- **Check the name of the publisher** before downloading the app; and
- **Avoid installing apps** from links received in an **email, social media* post, text message or a web page** that doesn't look right. The best way to download an app is to go to the store and download it from there.

**Social Media* - *Ccollection of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration.*

MOBILE DEVICE SECURITY

Contd...



App Store Preview

Pan Asia Bank 4+
Pan Asia Bank
#38 in Finance
★★★★★ 3.8, 21 Ratings
Free

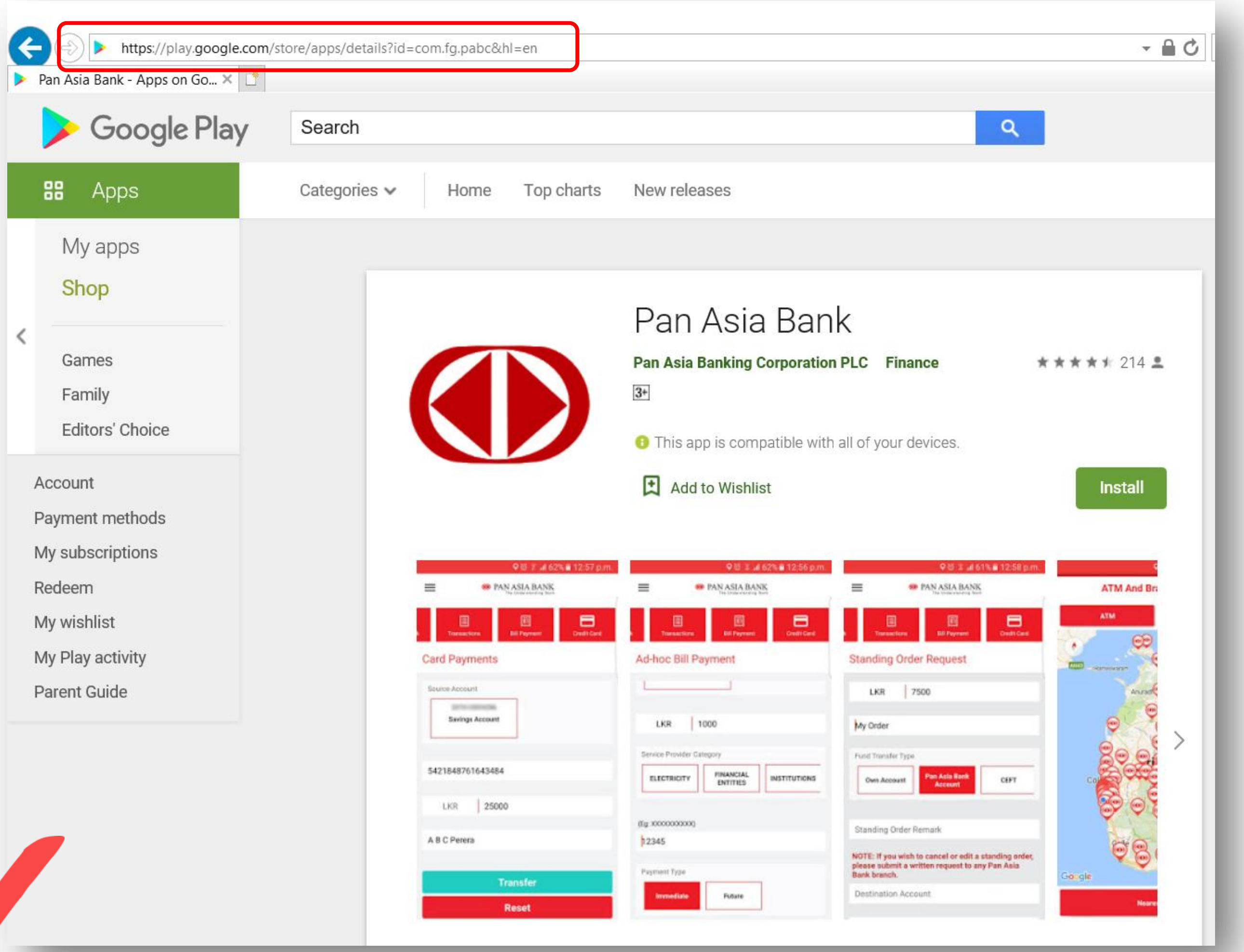
iPhone Screenshots

Download Pan Asia Bank mobile app and enjoy an array of banking services at your fingertips.
You can perform a wide range of functions such as checking account balances, transfer funds to an account with Pan Asia Bank or any other commercial bank, paying bills, paying Credit Card bills, view account history, setup / stop standing orders and many other services.

What's New

New SSL certificate added
Bug fixes and performance improvement

Pan Asia Bank, Mobile App – Apple App Store



Pan Asia Bank
Pan Asia Banking Corporation PLC Finance ★★★★★ 214
3+
This app is compatible with all of your devices.
Add to Wishlist
Install

Pan Asia Bank, Mobile App – Google Play Store

MOBILE DEVICE SECURITY

Contd...

PIN-lock your mobile phone and don't use unsecured (without password) WiFi.

Image Source: Psafe Blog

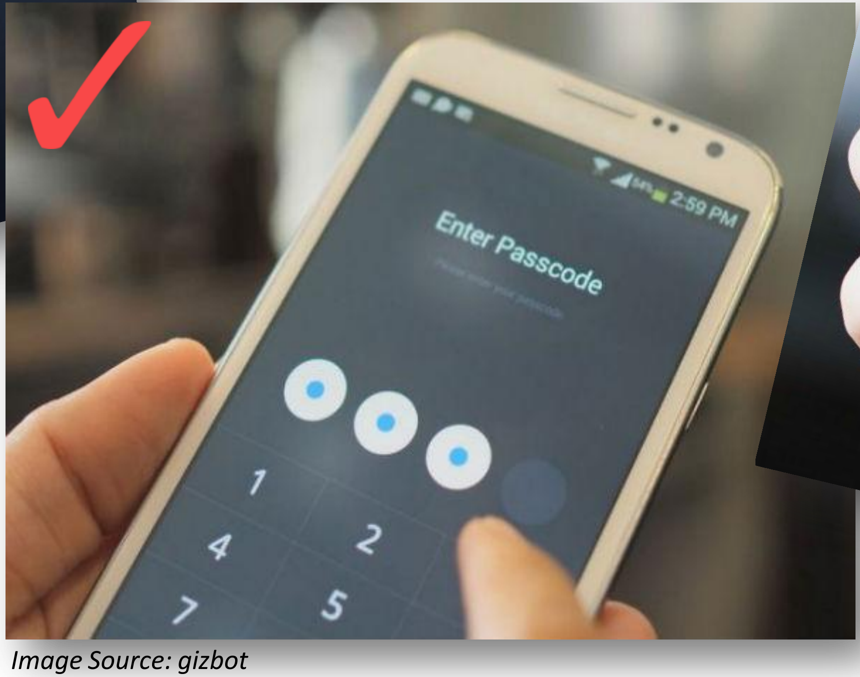
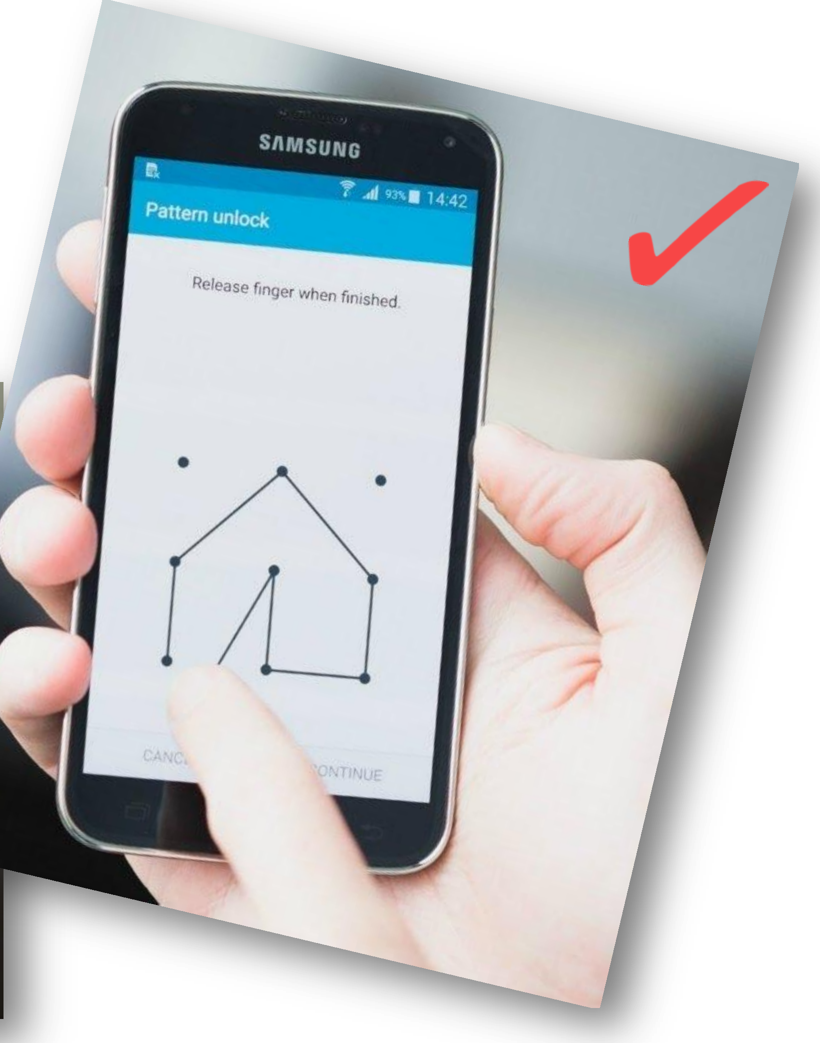


Image Source: gizbot



WHAT IS JAILBRAKING AND ROOTING?

JAILBREAKING

Jailbreaking is the process of removing software security restrictions placed on a device by either the manufacturer or carrier of iOS devices.

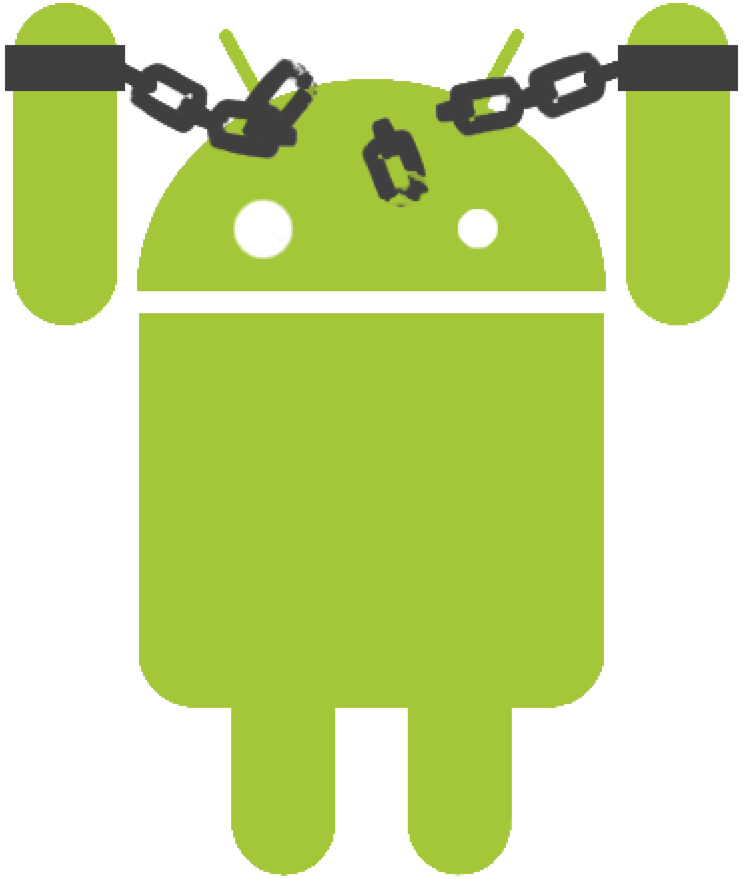
- Jailbreaking **removes** built-in features that keep your phone **SAFE** and **RELIABLE**;
- Once an Apple device has been Jailbroken the patches and software updates may not possible to download and install. Manufacturer will push updates more often to keep the device up to date;
- Some of the best applications for Jailbroken devices cost more than the applications found in the app store;
- Jailbreaking your device leaves you vulnerable to malware, and spyware; and
- Jailbreaking will also affect your devices battery life and data usage

Image Source – New Atlas

ROOTING

Rooting is the term used to describe the process of gaining root access or privileged control over devices, most commonly Android smart phones and tablets.

- Phone warranty turns void;
- Poor performance ;
- Official updates installation problems;
- Harmful Viruses can easily infect your Android OS, because rooting allows you to bypass restrictions and install any apps developed for Android



BE SAFE WHILE ONLINE BANKING AND SHOPPING

- Look for the **https://** and the padlock symbol in your browser to determine whether the site is secure;
- Check reviews on the online store to confirm it is legitimate or not;
- Never send your bank or credit card details via email, SMS or social media; and
- Make sure the computer or mobile device you use for online shopping has the latest security software updates

Image Source: RioMar

BE SAFE WHILE BANKING AND SHOPPING ONLINE

Contd...

MAINTAIN YOUR PRIVACY

- Take charge of what you reveal about yourself online
- Think twice about handing over any personal details unless you are confident it is absolutely necessary

TAKE EXTRA CARE WHEN SHOPPING AND BANKING

Take extra security precautions whenever you login to online banking or make other financial transactions.

Image Source: This is Money

ATM SECURITY

ATM SECURITY

ATM's give attackers another opportunity to get at your money, and you should take steps to reduce your risk. Most of us can stay out of trouble with simple common sense, but you should periodically review some proven strategies. Follow these simple tips, and you'll improve your odds against the scammers.

Use secure ATM machines, ones that are equipped with video surveillance or inside of a bank lobby - *they are less likely to be tampered with.*

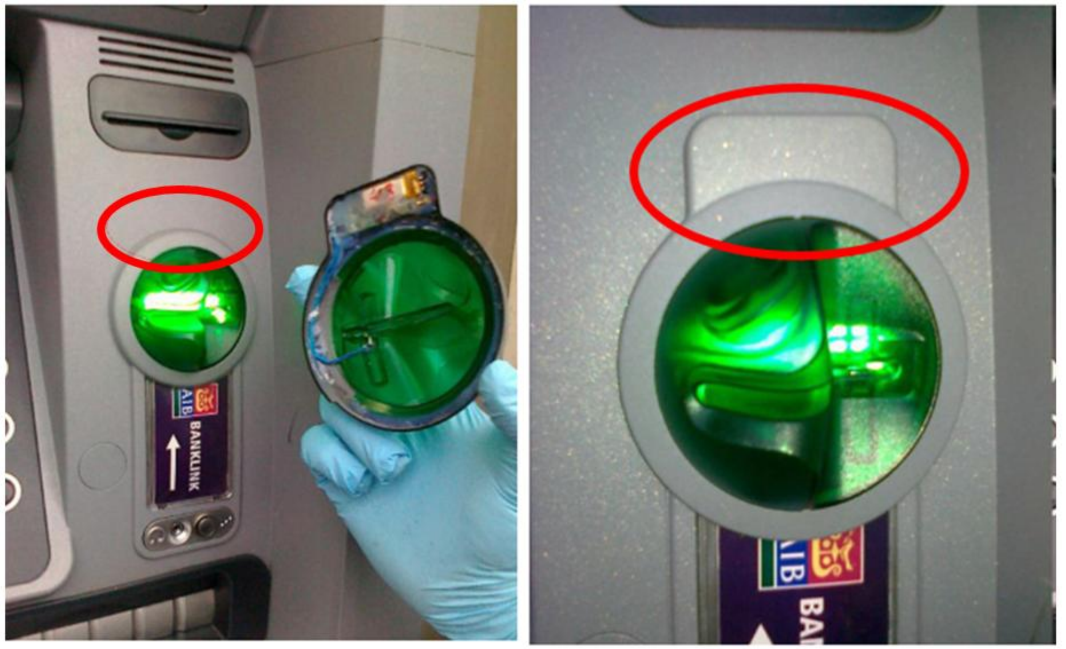
Hackers have to take high risk when installing skimmers where there are security cameras and security guards around.

Legitimate Card Reader – ATM
Image Source – WTTW

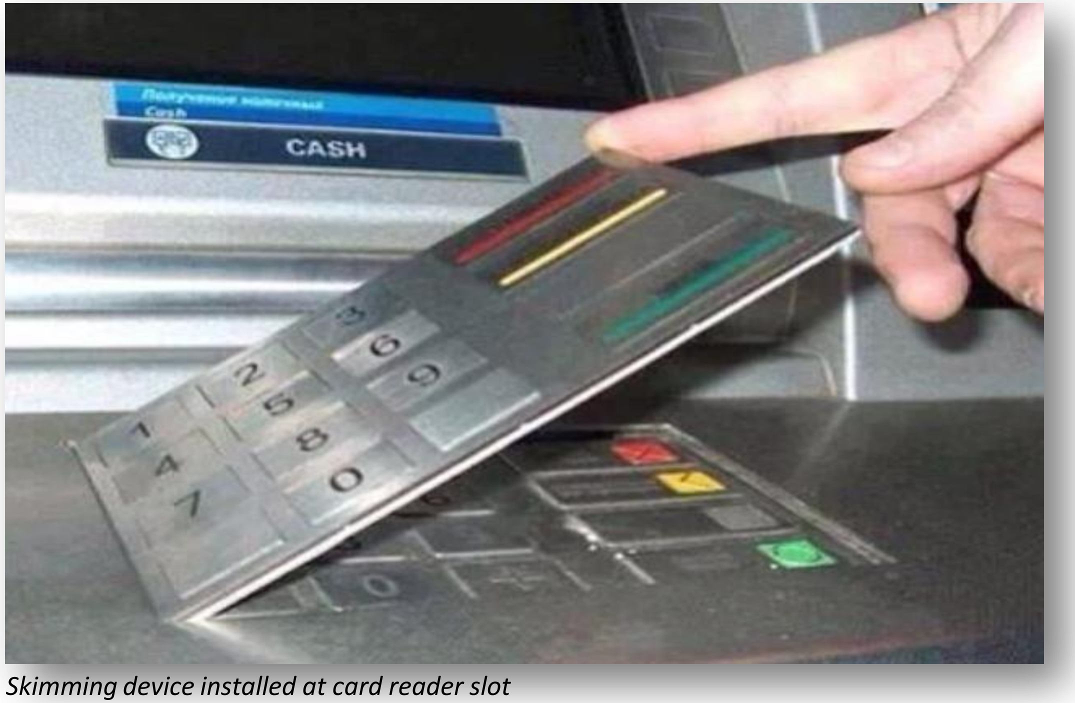
ATM SECURITY

Contd...

- Look over the machine before inserting your card - *If you realize something that looks unfamiliar on the machine, it could be part of an ATM scam which can be used to compromise your bank account.*



Card skimming device installing to the card reader slot
Image Source – engadget



Skimming device installed at card reader slot
Image Source – engadget

- *Some of the scam devices are:*
  - Card skimmers (external readers); and
  - Hidden cameras.

ATM SECURITY

Contd...

- Do not print account balance receipts if not required - *with advanced technology, there are highly skilled hackers who can trace patterns in combinations to crack codes. Therefore*
  - ✗ *Do not throw your ATM receipt in and around the bin near ATM machine (s) – Refer the picture, ATM receipts near ATM machine ;*
  - ✗ *Do not leave the ATM receipt on the ATM machine.*
- *Your information may be valuable source for hackers to gather information.*
  - *ATM receipts typically show the "**Date**" and "**Time**" of a transaction, the "**Transaction type**", "**Amount Transacted"** and the "**Available Amount**" of account holder.*
  - *It also displays **part of** an account holder's **account number** and that of a person whose account is being credited, with only the **last four digits** revealed.*
- Spend a minimum amount of time at the ATM.
- Be aware of your surroundings - *If you notice something or someone suspicious, inform to the Bank's staff / security officer. If security officer is not around go to another ATM or come back later.*
- Do not use an ATM that appears unusual appearance or offers options with which you are not familiar or comfortable.

ATM receipts near ATM machine

ATM SECURITY

Contd...

- Make sure the lighting around the ATM is adequate, if not, go to another ATM and inform to the Bank if possible.
- Be wary of people trying to "help" you with your ATM transaction – *Do not allow unknown people to handle your ATM transactions. If needed get required support from security officer or from the Bank staff (get the required instructions only);*
- Do not allow people to look over your shoulder as you enter your PIN- *Cover the ATM keypad as you're entering your PIN (in case there's a hidden camera around and be cautious of people around you with cell phones since many of them are now equipped with camera / video capabilities);*
- Do not re-enter your pin if the ATM card got stuck - *contact a bank official immediately or call to our hotline;*
- Do not write your PIN and keep it along with the ATM card;
- Do not display cash, quickly insert it to your wallet and count it later when you are in secure location;
- Immediately report all lost or stolen cards to Pan Asia Bank via our hotline;
- Closely monitor your bank statements, as well as your balance and immediately report any problems to your bank.
- Do not victim for carjacking - *When your car is stopped and you're picking up the cash, just lock your car doors before you count your money.*

SECURE YOUR DEBIT CARD AND CREDIT CARD

- Do not send your card number through email;
- If you have forgotten your PIN, request ne PIN from Pan Asia Bank;
- When selecting a PIN, don't use a number that appears in your wallet, birth date, phone number etc.;
- Ensure no one sees your PIN when you enter it;
- Memorize your PIN;
- Don't write down your PIN anywhere and never share it with anyone;
- Cancel and shred / destroy unused cards. If you receive a replacement card, destroy your old card;
- Shop with merchants you know and trust;
- Always log off from any website after transactions made with your credit or debit card. - *If you cannot log off, close your browser to prevent unauthorized access to your account information; and*
- Safe-keep or securely dispose of your transaction receipts.

Image Source: UniBul's Money Blog

PROTECT YOUR IDENTITY AND PRIVACY

- Adjust your social media privacy settings to ‘private’;
- Do not share personal or confidential information such as your date of birth, address, bank details and passwords on social media sites;
- If emailing identification documents such as a National Identity Card (NIC) Driver License or Passport details, ensure you delete the email after sending, and also delete from the trash;
- Set smart passwords and use 2 factor authentication where possible to apply an additional layer of protection;
- Never provide your personal or security details, including customer ID’s or passwords, in response to any email, even if it looks legitimate; and
- Avoid transactions online where you are using public or complimentary public Wi-Fi.

Source: iGeeks Blog

HOW CAN YOU KEEP YOUR BUSINESS SAFE ?

- ✓ Educate staff (particularly those who manage payments) about risks related to business email compromise;
- ✓ Before react to the message (*e.g. clicking on any links, opening attachments, or following any instructions*) contact the sender company of the message (using a phone number from their website) to confirm the legitimacy of the sender;
- ✓ Follow the correct and complete usual business process when completing fund transfers;
- ✓ Report any incidents related to your Pan Asia Bank Account to us as soon as you identify that you are a victim of such;
- ✓ Ensure your computer operating system, software, browser version and plug-ins are up-to-date. Before download an update to your computer, first go to the relevant company's website to confirm the update is legitimate;
- ✓ Install a firewall on your network and keep anti-virus software installed and up-to-date;
- ✓ Consider having a security audit conducted on your network to point out and correct any issues that may cause problems;
- ✓ Review the privileges of users, at least quarterly; and
- ✓ When an employee is resigning from your business, make sure to revoke his / her access rights to corporate resources immediately.

INTERNET BANKING ATTACKS

1. PHISHING

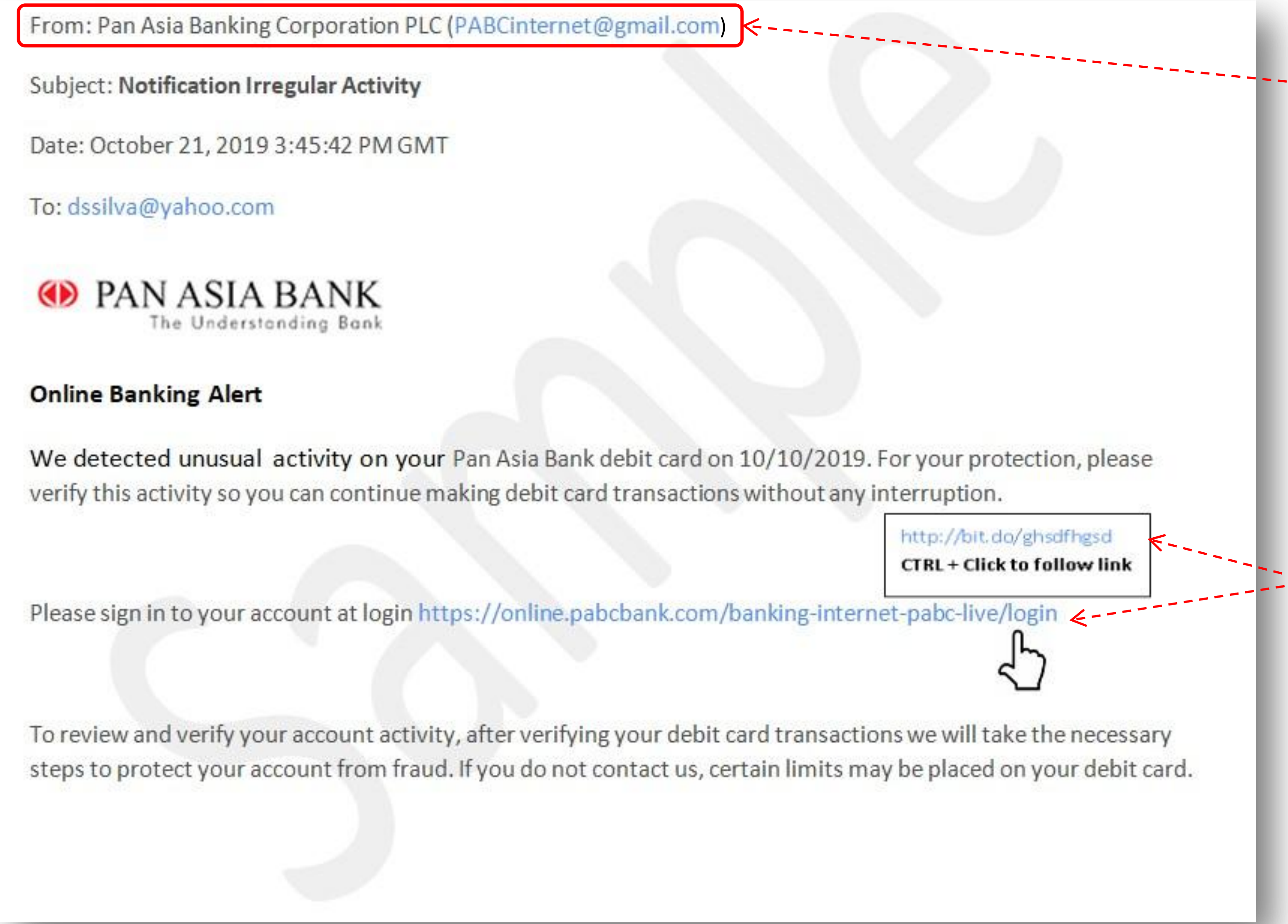
- With this type of threat, attackers send out fake emails that look like secure message(s) from legitimate bank(s).
- The email usually includes a link to a spoof website that looks more or less indistinguishable from the real deal.
- When you enter your login details on the site, you’re inadvertently sending your most confidential login credentials directly to hackers.
- Alternatively, the email may include an attachment that appears to be an important document.
- When opened, the attachment installs malicious software on your system.

Refer next pages for example.

Image Source: vector-phishing-concept

1. PHISHING

Contd...



From: Pan Asia Banking Corporation PLC (PABCinternet@gmail.com)

Subject: **Notification Irregular Activity**

Date: October 21, 2019 3:45:42 PM GMT

To: dssilva@yahoo.com

PAN ASIA BANK
The Understanding Bank

Online Banking Alert

We detected unusual activity on your Pan Asia Bank debit card on 10/10/2019. For your protection, please verify this activity so you can continue making debit card transactions without any interruption.

http://bit.do/ghsdfhgsd
CTRL + Click to follow link

Please sign in to your account at login https://online.pabcbank.com/banking-internet-pabc-live/login

To review and verify your account activity, after verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limits may be placed on your debit card.

*Sample phishing email for **demonstration** here only. Strictly prohibited to reuse.*

Pan Asia Bank never use free email service (gmail, yahoo etc.) to communicate with customers.

Hover over (move mouse pointer) web links with your cursor to check website URL (unexpected / wrong web addresses) before you click.

Phishing emails often contain links to dangerous sites.

1. PHISHING

Contd...

Learn more about email security and phishing by reading the following;

HOW TO DETECT PHISHING

Phishing is bogus emails created by fraudsters.

The aim of these emails is to trick you into clicking on links to fake websites, opening malicious attachments or revealing personal information. Signs of a phishing email include:

- *They may not address you by your name;*
- *Misspelling and inconsistent graphics / images are common;*
- *They may ask for sensitive information;*
- *Creating a sense of urgency – scammers may try to test your better judgment by stating that something needs your immediate attention;*
- *Sender's address – does it look unfamiliar or peculiar?; and*
- *They may contain unfamiliar or unexpected attachments – don't open them as they may contain malicious software.*

1. PHISHING

Contd...

REPORTING A HOAX OR SCAM

Pan Asia Bank may at times email customers with important updates, but we'll never send emails asking customers to confirm, update or disclose personal or banking information.

Most financial institutions follow the same practice.

If you receive an email that looks like it's from Pan Asia Bank that you believe may be a hoax, please forward it as an attachment to *digital.banking@pabcbank.com*.

It's important you never click on links or attachments in an email you think is a hoax. If you clicked on a link and you are suspicious, that your system is infected with virus or not use your security antivirus/anti-malware software to run a scan of your computer or device.

2. FRAUDULENT WEBSITES (PHISHING / SPOOFED WEBSITES)

Attackers may attempt to direct you to phishing / spoof websites via emails, pop-up windows or text messages. These websites are used to obtain your personal information. One way to detect these type of website is to consider how you got to the site. Possible use cautions will be:

- *If you may have followed a link in a suspicious email;*
- *If you may have followed a link in a text message;*
- *Online chat; or*
- *Other pop-up window requesting your personal or account information.*

3. POP-UP WINDOWS

- Hackers may use pop-up windows / small windows or advertisements to obtain personal information.
- These windows may be generated by programs hidden in free downloads such as screen savers or music software.
- If you encounter a suspicious pop-up window, close it.
- To protect yourself from harmful pop-up windows, avoid downloading programs from unknown sources on the Internet and always **run anti-virus software** on your computer.

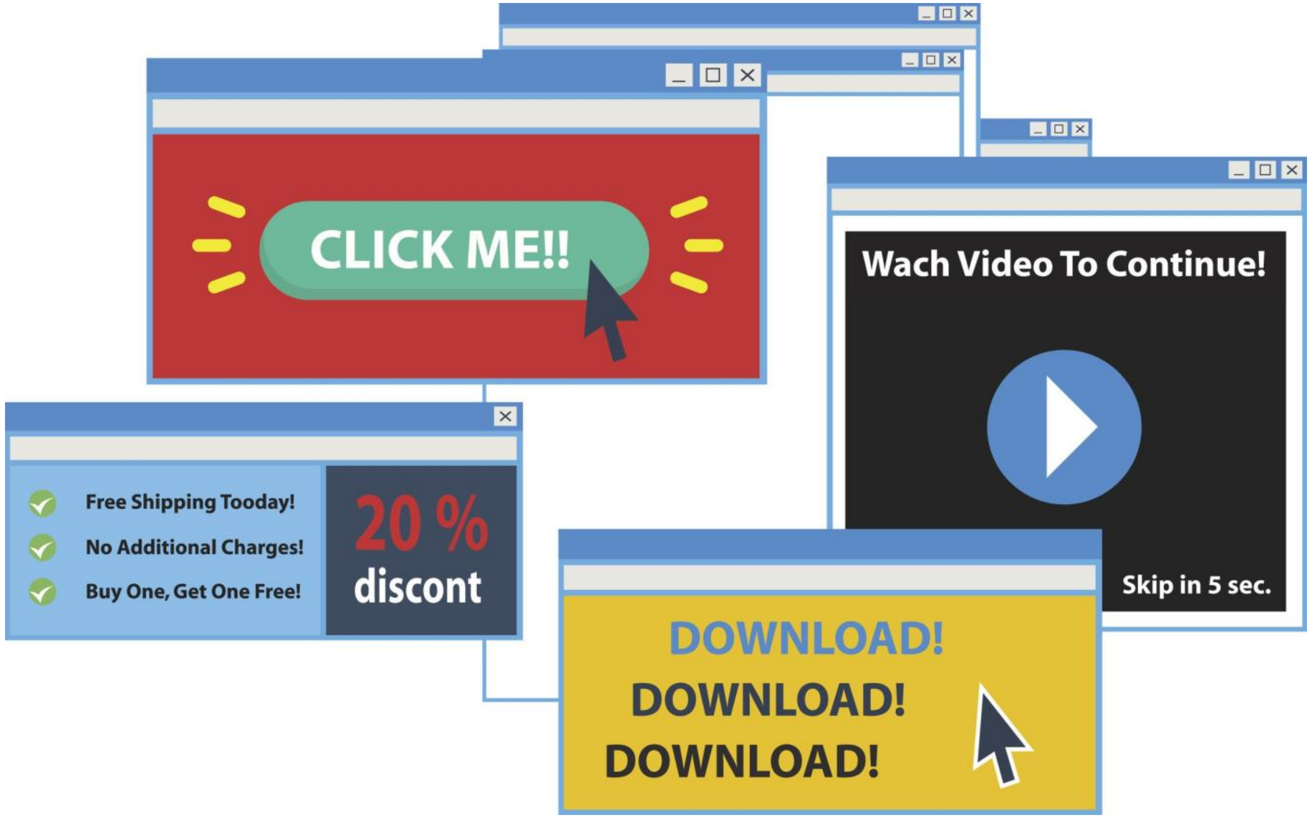
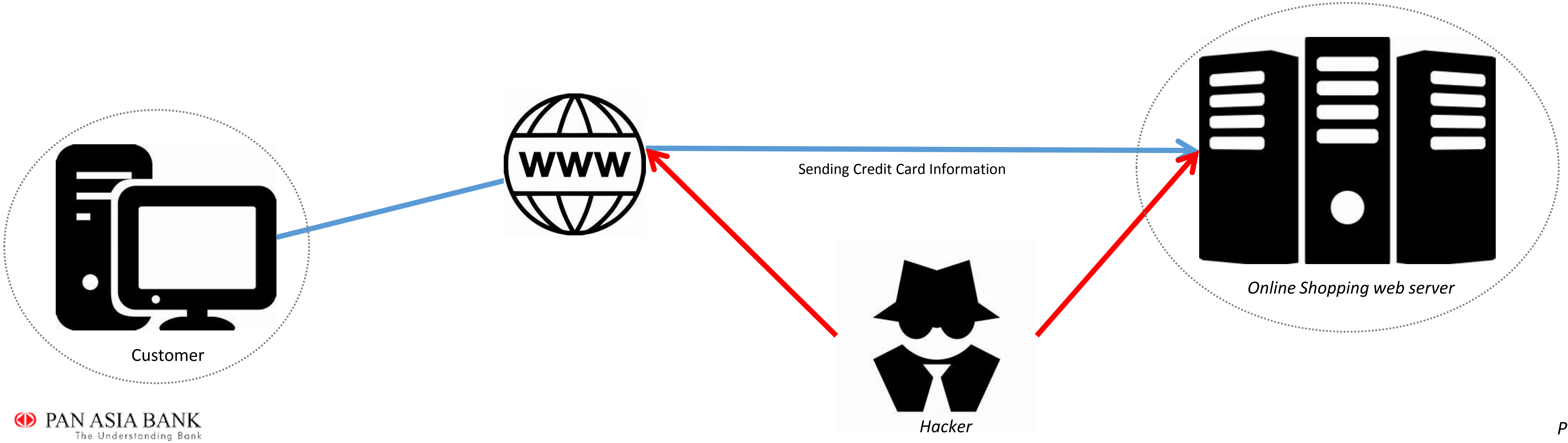


Image Source: The Balance Small Business

4. MAN IN THE MIDDLE ATTACKS

- Man-in-the-middle / MITM means that the communication between two partners has been interrupted.
- This makes it possible for attackers who can successfully take off each endpoint (i.e. you and your bank) to not only spy on your communications but also manipulate the conversation for their own purposes.

  For instance, you might think that you're communicating directly with your bank over a private connection, but the messages are actually being sent and received by the attacker.
- In the case of "man in the browser" attacks, the attack is performed directly in your browser. In this scenario, SSL encryption, which is designed to protect you from conventional "man in the middle" attacks, is ineffective.



5. MALWARE

- Malware designed to steal banking credentials;
- Malware targeting bank information not only knows which websites you open and exactly what you are doing on these sites, including all user details and passwords that you type in and also able to manipulate the website displayed, without your knowledge;
- This is particularly harmful to you as a victim if the transfers you make are manipulated and redirected to other accounts;
- Even existing forms on bank websites can be subtly modified so that more than one *Transaction Authentication Number* (TAN) can be requested; and
- These TANs and the copied login details enable the attackers to gain full control of your account.

6. TEXT-MESSAGE PHISHING (SMISHING)

A phishing attempt sent via SMS (Short Message Service) or text message to a mobile phone or device.

This method is also referred to as smishing, which is a combination of SMS and phishing.

The purpose of text message phishing is the same as traditional email phishing -*influence recipients to share their confidential information.*

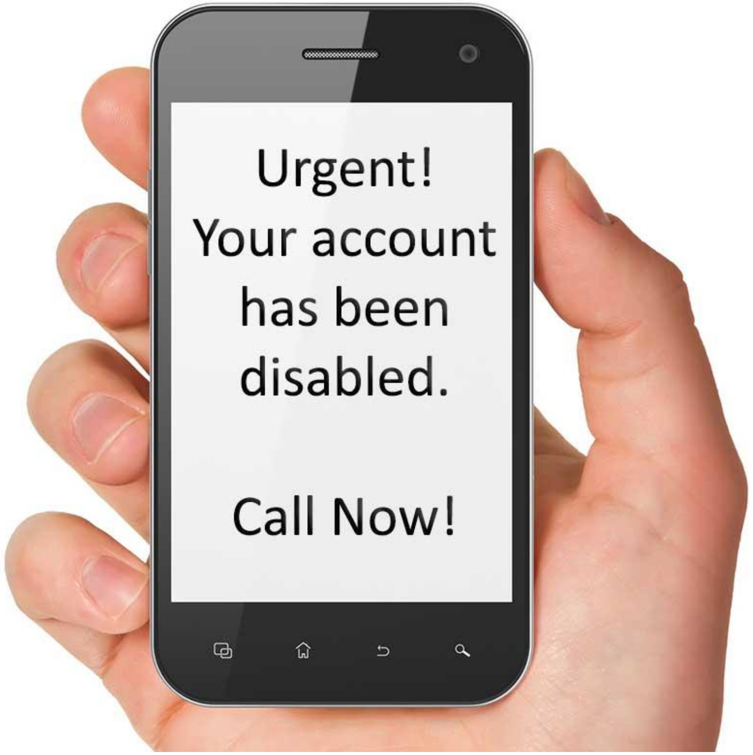


Image Source: hoax-slayer

7. TELEPHONE OR VOICE PHISHING (VISHING)

- This method is a phishing attempt made through a telephone call or voice message.
- Hackers may have the ability to spoof / takeoff their caller ID so it could appear that the telephone call is coming from a legitimate company.
- Hackers may also have identifying customer information, such as your name, which they may use to make the call appear more authentic.

Refer "Physical Security", next section to know the steps that you have to follow in such situation.

8. PAPER MAIL OR FAX PHISHING

- Some fraudsters still use low-tech methods to obtain your personal and financial information.
- Phishing attempts can be made through regular mail or fax machines.
- If you are suspicious about a piece of mail or fax you have received requesting personal or financial information, you should discard it.
- If you responded to a suspicious mailing or fax and provided confidential information, contact the company the mail or fax appears to be from.
- Use a legitimate source such as the phone number listed on the company's website, billing statement, or on the back of your ATM, debit or credit card to determine if your information was compromised.

PHYSICAL SECURITY

PHYSICAL SECURITY

1. Be alert to your surroundings and other people around you.
2. Never display cash in parking lot near ATM.
3. When you conduct banking business during the evening hours, if it is dark, have someone accompany you.
4. Park as near as possible to your destination, such as the branch entrance, ATM or night depository.
5. Carry only necessary information with you. Leave unused credit cards in a safe and secure location.
6. Make photocopies (front and back) of vital information you carry regularly and store them in a secure place - *if your purse or wallet is lost or stolen, you have contact information and account numbers readily available.*
7. Unusual phone calls from unknown numbers which representing the Pan Asia Bank, ask for the purpose of the call but don't give any of your account or personal information, ask him / her to call back later and contact the Pan Asia Bank using legitimate sources such as contact phone numbers found our website, your bank statements, and those listed on your ATM, debit or credit card.
8. Never provide payment information on a call that you did not initiate.

PHYSICAL SECURITY

Contd...

9. Shred documents containing personal or financial information before discarding - *Many fraud and identity theft incidents happen as a result of mail and garbage theft.*
10. Review your credit report at least once a year to look for suspicious or unknown transactions.
11. Know your billing and statement cycles - *contact the Pan Asia Bank's customer service department if you stop receiving your regular bill or statement.*
12. Store new and cancelled checks in a safe and secure location.
13. Carry your chequebook with you only when necessary.
14. Tear up or shred receipts, bank statements and unused credit card offers before throwing them away.
15. Report loss of credit and debit cards immediately to the Pan Asia Bank.
16. Report loss of your cheque book immediately to Pan Asia Bank.
17. Do not discard / donate / sale a computer without deleting all your files first.

SOME IMPORTANT TIPS

TIPS

Contd...

Source: UFS Explorer

Keep your Laptop / PC:

- *operating system;*
- *security software;*
- *web browser; and*
- *add-ons*

up-to-date by ensuring automatic updates are enabled or installed as soon as they are available.

This dramatically reduces your device's exposure to malware.

Be sure to read reviews of security software (such as anti-virus) to assess its reputation before you download them.

Source: Norton | Security

TIPS

Contd...

MOBILE DEVICE SECURITY

Your mobile phone is normally under your watchful eye, but we all know someone who has lost their phone or had it stolen.

Set your phone up to required level of secure to protect your confidential information in the event of any of the following happens to you:

Source: Enterprise Mobility Exchange

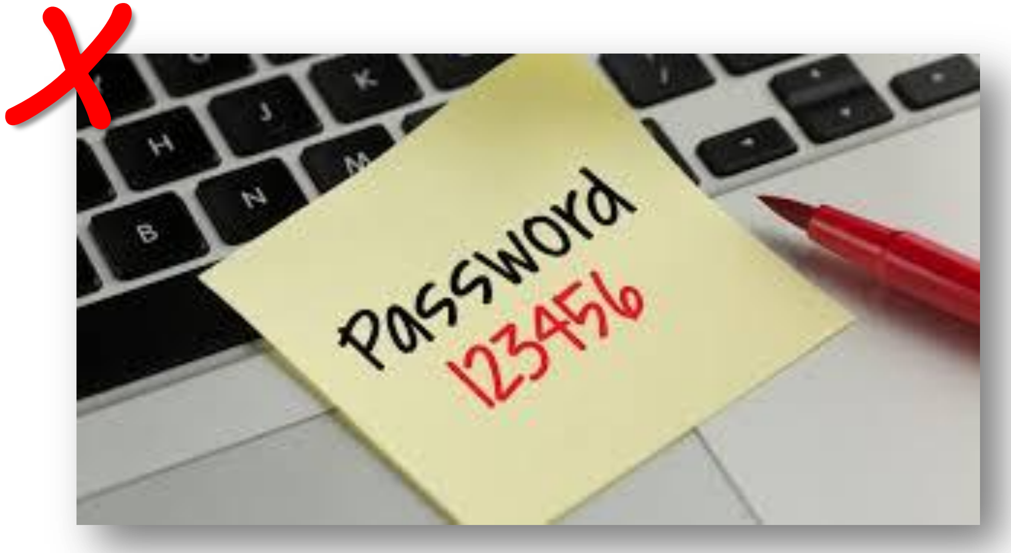
- Set your mobile device to lock after a short period of non-use;
- Use a strong, secret PIN / Pass code and / or fingerprint detection;
- Sign out of websites when you've finished browsing;
- Use Apple's Find my iPhone or Google's device manager for Android, to help you locate your phone and wipe the data should it fall into the wrong hands;
- Set up an automatic data wipe-out function in case your device gets lost;
- Avoid connecting to random WiFi-networks;
- Control application access and permission; and
- Avoid downloading dodgy apps. Only use official apps store (like Google play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

TIPS

Contd...

PASSWORDS

- Don't write down your passwords or PINs;
- If you need to write down a hint, disguise it;
- Remember, your passwords unlock your accounts so never share them with anyone;
- If you need to record a hint, make sure it is disguised and secured;
- Make your password hard to guess – *avoid using of your Name / part of your name / the username for your account, date of birth, spouse's name etc.; and*
- Avoid default passwords - *password, guest, user, admin are some examples. They are widely available on the internet.*



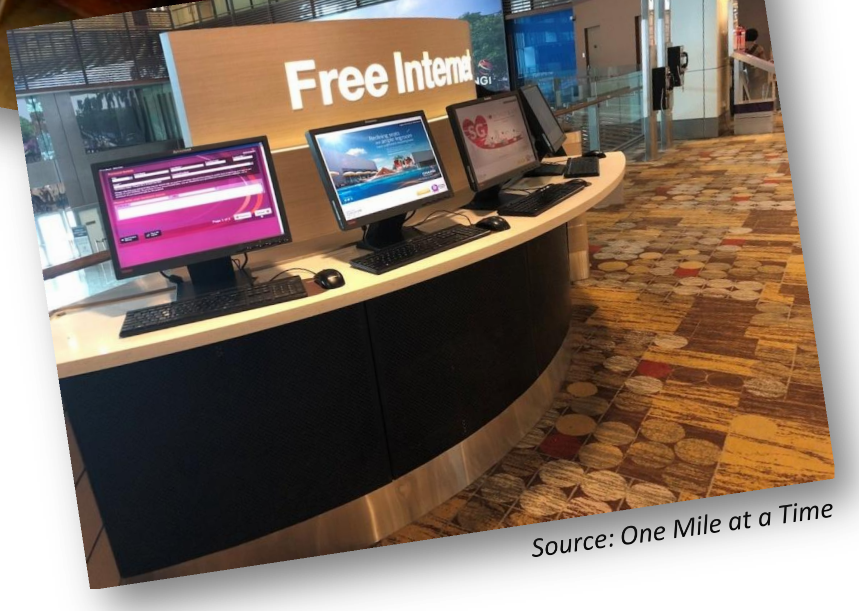
TIPS

Contd...

- Do not access private accounts on a public use computer – *computers in cyber cafes,*
  libraries,
  airports, or
  courtesy computers in common areas of an office;

Source: sheriph

Source: WBUR



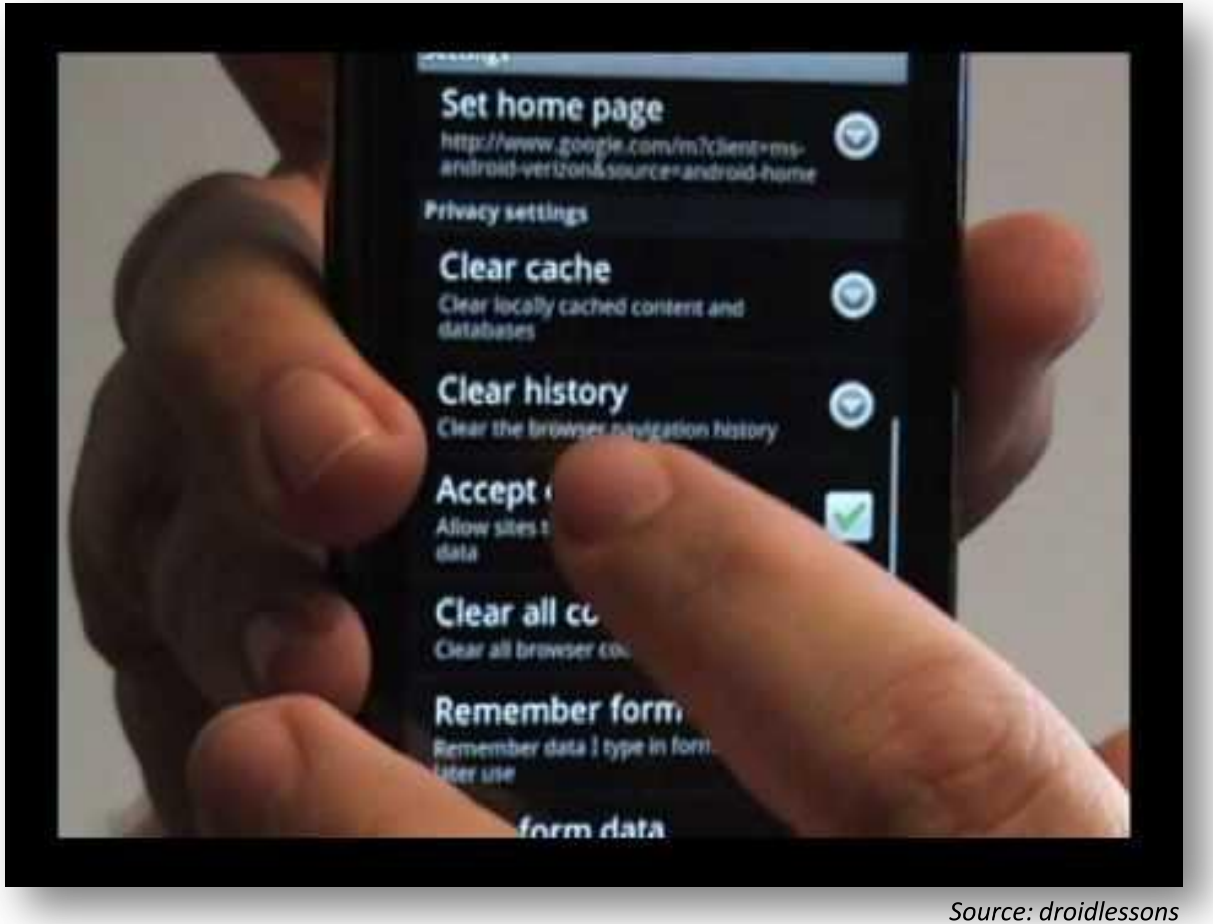
Source: One Mile at a Time

TIPS

Contd...

- If must use a public computer - *avoid logging into secure sites that store your information, and erase your browsing history (including cookies, refer Cookie policy in our website for more details) before leaving; and*

- Browsing on your phone - *be careful of public Wifi networks that don't require a password. If your phone is connected to public Wifi, don't disclose your personal information or enter password-protected sites.*


Set home page
http://www.google.com/m?client=ms-android-verizon&source=android-home
Privacy settings
Clear cache
Clear locally cached content and databases
Clear history
Clear the browser navigation history
Accept
Allow sites t
data
Clear all co
Clear all browser co
Remember form
Remember data I type in form
later use
form data

Source: droidlessons

TIPS

Contd...

- It’s important we have your most current contact information so we can contact you if we notice unusual Internet Banking activity.
- Make sure you provide us with your most up-to-date phone number and call us if you lose your phone.
- Also be vigilant to signs a fraudster may be attempting to port (transfer) your mobile phone number to a new device or carrier in order to intercept your messages.
- Tell-tale signs of this are unexpected loss of signal or where your mobile phone displays 'SOS or emergency calls' only.

Source: Steveston-London Secondary School

TIPS

Contd...

You can reduce your risk of falling victim to identity theft with these tips:

- Create strong, secure passwords, and change them regularly.
- Be suspicious of unexpected or unusual emails.
- Make sure your bank has your up-to-date contact details so they can get in touch quickly if they see any unusual activity on your accounts.
- If throwing out any personal or financial information such as bank statements or bills, shred or destroy them. If filing them away, make sure they are kept in a secure place in your home/office.

Source: Network World

TIPS

Contd...

- The best way to protect yourself against online identity theft is to limit the 'digital crumbs' a stranger can gather about you.
- This means being careful about putting personal information such as your home address, phone number or account details on public forums and social networks.
- Why don't you try checking your 'digital footprint' now? Just log out of all of your social media accounts and then look up your name in a search engine and assess the results.

TIPS

Contd...

MANAGING YOUR COOKIES

- Cookies are text files that are downloaded to your computer or mobile device when you visit a website.

- When you’re browsing, cookies gather information about how you use the website.

- Cookies can be useful as they help you have an enriched and more personalized experience online by allowing sites to track your preferences as you browse.

- From time to time, it’s a good idea to check that you're comfortable with what cookies your desktop or device has collected.

- You can usually manage your cookies and browsing history via your web browser.

TIPS

Contd...

MANAGING YOUR COOKIES

Has your identity been stolen?

The moment you spot suspicious activity on your bank account contact your bank as soon as possible.

Other signs of identity theft could be receiving bills for goods and services you didn't buy or use.

You might also notice you've stopped receiving expected mail, which could mean it's being stolen from your mailbox or your mailing address has been fraudulently changed.

REPORTING SCAM ATTEMPTS OR FRAUDS

REPORTING SCAM ATTEMPTS OR FRAUDS

Contd...

- **If You Receive a Suspicious Message Representing Pan Asia Bank Identity?**
  - *Before clicking any links, attachments, or following any instructions, contact Pan Asia Bank.*
  - *It is important to use a phone number from the Pan Asia Bank's website to confirm the legitimacy of the message instead of use contact number mention on the message.*

- **If You Click on a Suspicious Link or an Attachment?**
  - Disconnect your computer / laptop from the internet to prevent the cybercriminal from sending any personal or confidential information from your device.
  - Back up your files to a personal computer, external hard drive, network, or the cloud.
  - Scan your computer or device for any malware using legitimate antivirus software, or obtain assistance from professional technical support provider.
  - Immediately contact Pan Asia Bank if you see any signs of unexpected transactions.

REPORTING SCAM ATTEMPTS OR FRAUDS

Contd...

- **What you do if You Suspect Your Banking Identity has been stolen?**
  - Immediately contact Pan Asia Bank and inform;
  - Reset your passwords related to all banking functions and social media profiles;
  - Take action to keep your mobile device and apps secure; and
  - Run legitimate antivirus software to scan your computer or mobile device for malware.

- **What you do if You Victim for Unexpected Credit Limits?**

  If you're receiving bills, credit and loan statements or calls from creditors that you know nothing about or if you are experiencing difficulty obtaining a credit card or a loan due to an inexplicable bad credit rating you should request a credit report from "***Credit Information Bureau of Sri Lanka***" - http://www.crib.lk

THANK YOU