e-Payment

Staying Safe in Online Banking

Speaker:
Abdul Rahim Bahadzar
Vice President
Al Rajhi Bank

Online Banking – Test your skills

How should I access my Internet Banking?

A) Click on hyperlinks provided in email

B) Type in https://bankABC.com.my

C) Google Bank ABC and click on any link

Online Banking – Test your skills

You have accidently accessed a phishing site! What is your next course of action?

A) Log out immediately and pretend it never happened

B) Do not log in. Close the page immediately and alert the Bank Customer Service

C) Try to log in for experimental

Online Banking – Test your skills

Q :How many security measures should you have on your PC?

i) Latest version of Firefox/Chrome/IE
ii) Latest Operating system
iii) Firewall
iv) Anti Virus software

A) All of the above
B) Less than two of the above
C) None

Online Banking – Test your skills

Q: Which of these password is the most secure?

A) Password

B) 22228888

C) Pymt@Frm15

Online Banking – Test your skills

Q : How can you tell if your Computer is infected with malware?

i) You see pop up advertisements when you are not connected to the internet
ii) Your computer takes longer than usual to complete certain task
iii) You experience a sudden rise in computer crashed
iv) Your browser search settings have changed without your knowledge

A) i and iii
B) i, ii, iv only
C) All of the above

Online Banking Fraud

❑What is Online Banking fraud?

- Online Banking Fraud is an attempt to gain access to personal bank accounts by misleading the public.

❑How can my personal account be controlled by others?

- By misleading bank customers to surrender their PIN number to be used for Internet Banking registration. With that cyber criminals may register a client's account and be in control through Internet Banking.

Online Banking Fraud

- **How do I identify a phone call / SMS / E-mail that is not performed by the Bank?**
  - Always remember that the Bank will never request for customer's PIN / password, because it is private and confidential.

Online Banking Fraud

- **If you think you have been a victim of online banking fraud:**
  - Customers are advised to contact the Bank as soon as possible for advice and further action.
  - If you accidently supplied your account details, immediately change your password and report it to your bank so they can freeze your account and make alternate arrangements
  - Report unauthorised financial transaction to your bank, credit card company as soon as you detect them

Type of Cyber Crooks

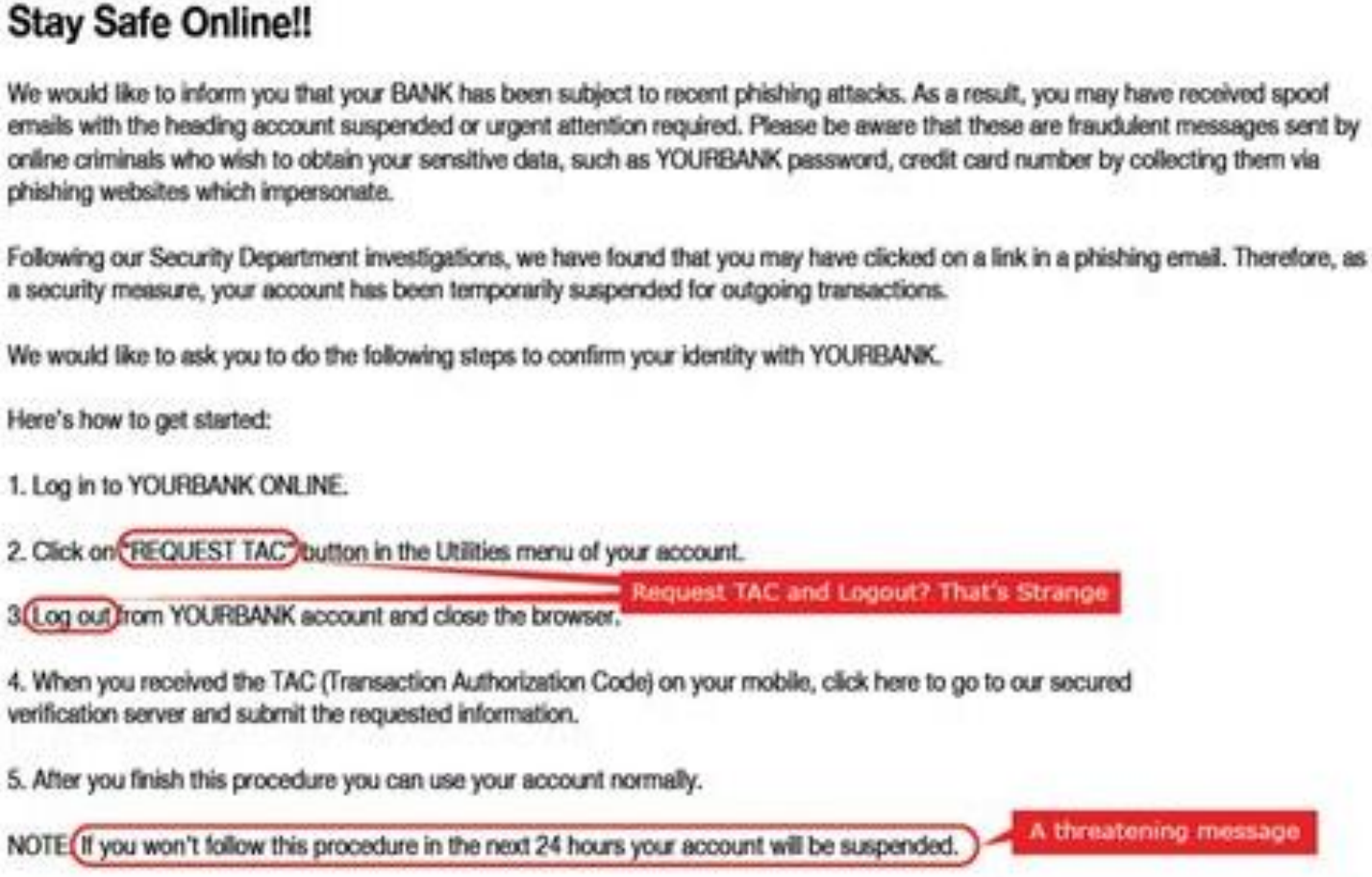
Phone: Act as someone you can trust and calls you e.g. alert that your banking account has been compromised by possible scams. The 'çrooks' will instruct you to perform a banking transaction to a third party account to rectify the losses

Phishing : Attempt to act on behalf of a bank and request you to open the attach link via **email** . The phishing links will bring to an identical **fake website** that requires your personal information for usage of malicious purposes

Malware : Commonly known malwares are like viruses, worms and trojan horses. Hazardous software that is installed in your electronic device without your knowledge or consent

Online Banking Fraud – Modus Operandi

- **What are the example of misleading tactic usually being used?**
  - Email



Stay Safe Online!!

We would like to inform you that your BANK has been subject to recent phishing attacks. As a result, you may have received spoof emails with the heading account suspended or urgent attention required. Please be aware that these are fraudulent messages sent by online criminals who wish to obtain your sensitive data, such as YOURBANK password, credit card number by collecting them via phishing websites which impersonate.

Following our Security Department investigations, we have found that you may have clicked on a link in a phishing email. Therefore, as a security measure, your account has been temporarily suspended for outgoing transactions.

We would like to ask you to do the following steps to confirm your identity with YOURBANK.

Here's how to get started:

1. Log in to YOURBANK ONLINE.

2. Click on "REQUEST TAC" button in the Utilities menu of your account.

3. Log out from YOURBANK account and close the browser.

Request TAC and Logout? That's Strange

4. When you received the TAC (Transaction Authorization Code) on your mobile, click here to go to our secured verification server and submit the requested information.

5. After you finish this procedure you can use your account normally.

NOTE: If you won't follow this procedure in the next 24 hours your account will be suspended.

A threatening message

Online Banking Fraud – Modus Operandi

- **What are the example of misleading tactic usually being used?**
  - SMS

Online Banking Fraud – Modus Operandi

- **What are the example of misleading tactic usually being used?**
  - Phone calls

Good evening, Sir
I am calling from Bank Negara Malaysia to verify your Personal Identity Card Number XXXXX

Morning Sir, I am calling from Bank Mesra Berhad. Our record shows that you have to update your Internet Banking account.

Congratulations Mrs. We are from the United Scratch and Win. Congratulations you have won a car!!!

Online Banking - Security Features

Individual Internet Banking:

1. Secured Web page : **(https)**

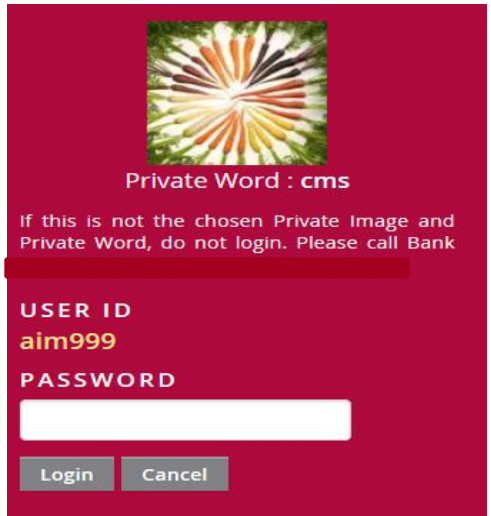
Online Banking - Security Features

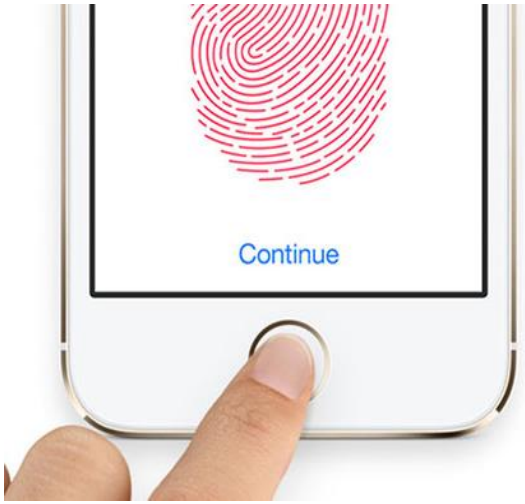
Individual Internet Banking:

2. Combine all the security features including Transaction Authorization Code (TAC) and the ID name and Password (or security token)

3. Verification via a Private image & secret word

4. Biometrics Authentication via smart phones





Online Banking - Security Features

Business Internet Banking:

1. Business Internet Banking Transaction authentication security has two stages of verification process.
   - A maker and checker concept
   - multi layer of approval (two approval and above)
   - approval based on amount ie Group A and Group B

2.Usage of physical security devices as a two factor authentication

Safety Tips - Malware

- Avoid rooting or jailbreaking your mobile device
- Always update the latest anti-virus program
- Do not access online banking through unprotected PC eg Cyber Café. Avoid using public access WiFi.
- Do not download any unregistered or free unknown software

Safety Tips - Malware

- Do not store login ID and password in Computer or smart phone

- Change passwords regularly. If you feel your password has been compromised, please change immediately.

  - please use high level password combination such as with alpha numeric and alien character (!@#)

- Take care of the security device

Safety Tips - Phishing

- Never login with your personal information via email links, attachment of pop ups
- Never respond to unsolicited emails requesting for private information such as ID, password, identification number
- Please type the secured web address, for example: https//www.Bank.com.my

Safety Tips - Phone

- Ask the caller to identify you personally and opt to call bank the Bank Contact Centre
- Never provide private information over the phone, unless you are making the call yourself
- Ignore any SMS, WhatsApp, WeChat, Telegram messages from unknown numbers

Online Banking – Test your skills

Who is responsible in ensuring your PC or mobile devices are safe online?

A) The Bank
B) The Internet service provider
C) Me

Credits

- Association of Banks in Malaysia
  - www.abm.org.my / www.aibim.com
- Banks Corporate Website – Security
- Suruhanjaya Komunikasi Dan Multimedia
  - www.skmm.gov.my

Internet itu mesra pengguna, bersifat global dan dibuka setiap waktu. Dengan Internet anda boleh:

- Mencari dan berkongsi maklumat dengan lebih efektif.
- Memudahkan urusan harian dan perniagaan.
- Berkomunikasi dan berinteraksi bersama keluarga dan rakan-rakan tidak kira di mana mereka berada.
- Mendapatkan berita terkini dan mengetahui hal ehwal semasa.

Di sebalik kebaikan Internet, anda juga mungkin terdedah kepada kandungan yang berunsur negatif.

Risiko-risiko yang mungkin anda hadapi:

Melalui Internet seseorang itu terdedah kepada sesiapa sahaja yang ingin memanipulasi anda.

Melalui Internet anda terdedah kepada kandungan - kandungan yang tidak sihat dan tidak bermoral.

Terdapat beribu - ribu iklan di dalam Internet yang boleh memperdayakan anda.

Di sini terdapat beberapa panduan penggunaan Internet secara selamat dan berhemah untuk dikongsi bersama :

JANGAN BERKONGSI KATA LALUAN DAN NAMA YANG DIGUNAKAN

- Tukar kata laluan anda sekerap yang mungkin.
- Gunakan kata laluan yang kompleks dan panjang tetapi mudah untuk anda ingati.
- Jangan berkongsi maklumat peribadi seperti nama sebenar, alamat dan nombor telefon dengan orang yang tidak dikenali.

BIJAK APABILA BERKONGSI

- Fikirkan dahulu sebelum meletakkan apa-apa gambar atau kandungan-kandungan yang ingin dikongsi bersama rakan-rakan maya anda.
- Ingat, apa-apa kandungan yang dikongsi atau dimuatnaik oleh anda berkemungkinan tidak dapat dikeluarkan sepenuhnya dari alam siber.
- Kandungan ini juga boleh diungkit-ungkit oleh orang lain pada masa akan datang.

BERBUDI BAHASA DAN JANGAN SEBARKAN FITNAH

- Hormati orang lain ketika anda berkongsi pandangan dan jangan membiarkan emosi mempengaruhi anda.
- Jangan sebar khabar angin. Rujuk dahulu dengan sumber yang boleh dipercayai.
- Elakkan daripada menggunakan perkataan yang berbaur perkauman atau lucah.

BACA DENGAN TELITI DAN FAHAMI SYARAT-SYARAT SERTA TERMA PERKHIDMATAN DAN GUNAKAN KEMUDAHAN PRIVASI DAN LAPORAN YANG DICADANGKAN OLEH LAMAN SOSIAL TERSEBUT

- Fahami syarat-syarat dan terma yang disediakan.
- Tingkatkan keselamatan akaun anda dengan menetapkan tahap privasi yang berpatutan.
- Buat laporan penyalahgunaan di ruangan yang disediakan pihak pentadbir laman web.

MEMASANG PERISIAN KAWALAN DAN ANTI-VIRUS

- Memasang perisian kawalan (filtering software) di komputer masing-masing adalah salah satu mekanisma memastikan kandungan yang kurang sopan tidak boleh diakses dan dapat disekat dengan cara yang lebih komprehensif dan efektif.
- Berhati-hatilah! Pelbagai virus dan program (malware) terdapat di Internet yang boleh menyerang dan menjejaskan keupayaan komputer anda.
- Dengan memasang perisian kawalan dan anti-virus , anda dapat melindungi komputer anda dari dipergunakan oleh pihak ketiga.

Ingat, bersama-sama kita KLIK DENGAN BIJAK untuk membudayakan penggunaan Internet secara SELAMAT dan BERTANGGUNGJAWAB