Two Factor Authentication (2FA) Briefing

VTC ITSD Security Team

Agenda

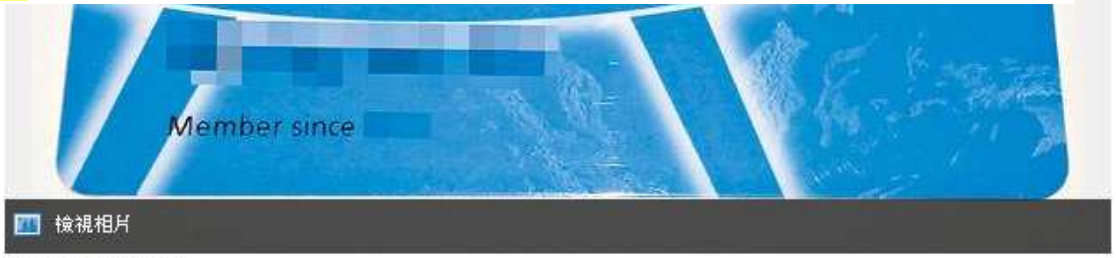
- Recent Security Incidents
- Statistics of Account Leakage
- What's the cause of these incidents?
- How to resolve it?
- What is the benefit of 2FA?
- How to Register and Use? Demonstration
- Usage & Milestone
- FAQ & Q&A

Recent Security Incidents

亞洲萬里通會員 10萬飛行里數失竊

東方日報 – 2016年12月11日星期日上午6:20

方小姐隨即報警並要求「亞洲萬里通」賠償，但該公司只肯賠償土耳其酒店房間的飛行里數，因房間未有人入住，但Amazon的電子購物券則拒絕賠償。她稱：「唔係因為你（亞洲萬里通）未做好網上保安，點會畀人偷走啲飛行里數，冇理由將損失轉嫁喺會員身上！」



檢視相片

東方日報 - 亞洲萬里通

飛行里數大盜又作案　亞洲萬里通拒負責捱轟

01月01日(日) 00:30

推介 121　Tweet　G+1 0　分享

陳女士發現其亞洲萬里通戶口的飛行里數遭盜用(紅框示)。(陳女士提供/資料圖片) 1/3

再有市民被盜走亞洲萬里通(Asia Miles)里數！國泰航空馬可孛羅會金卡會員陳女士及其夫共被盜走逾22萬里數換取埃及酒店住宿，亞洲萬里通堅持資訊系統運作正常，指屬個別事件，只酌情發還一半里數。陳女士質疑：「里數被人偷咗，國泰又唔報警，唔負責任，我哋原來無保障」，她已報警求助。

Recent Security Incidents

15/12/2016 09:25

【國際要聞】雅虎再被駭客入侵，逾１０億個電郵帳戶資料被盜

被盜用戶資料一覽

- ■用戶姓名
- ■電郵地址
- ■加密密碼
- ■電話號碼
- ■出生日期

雅虎五億帳戶 資料被黑客盜取

Recent Security Incidents

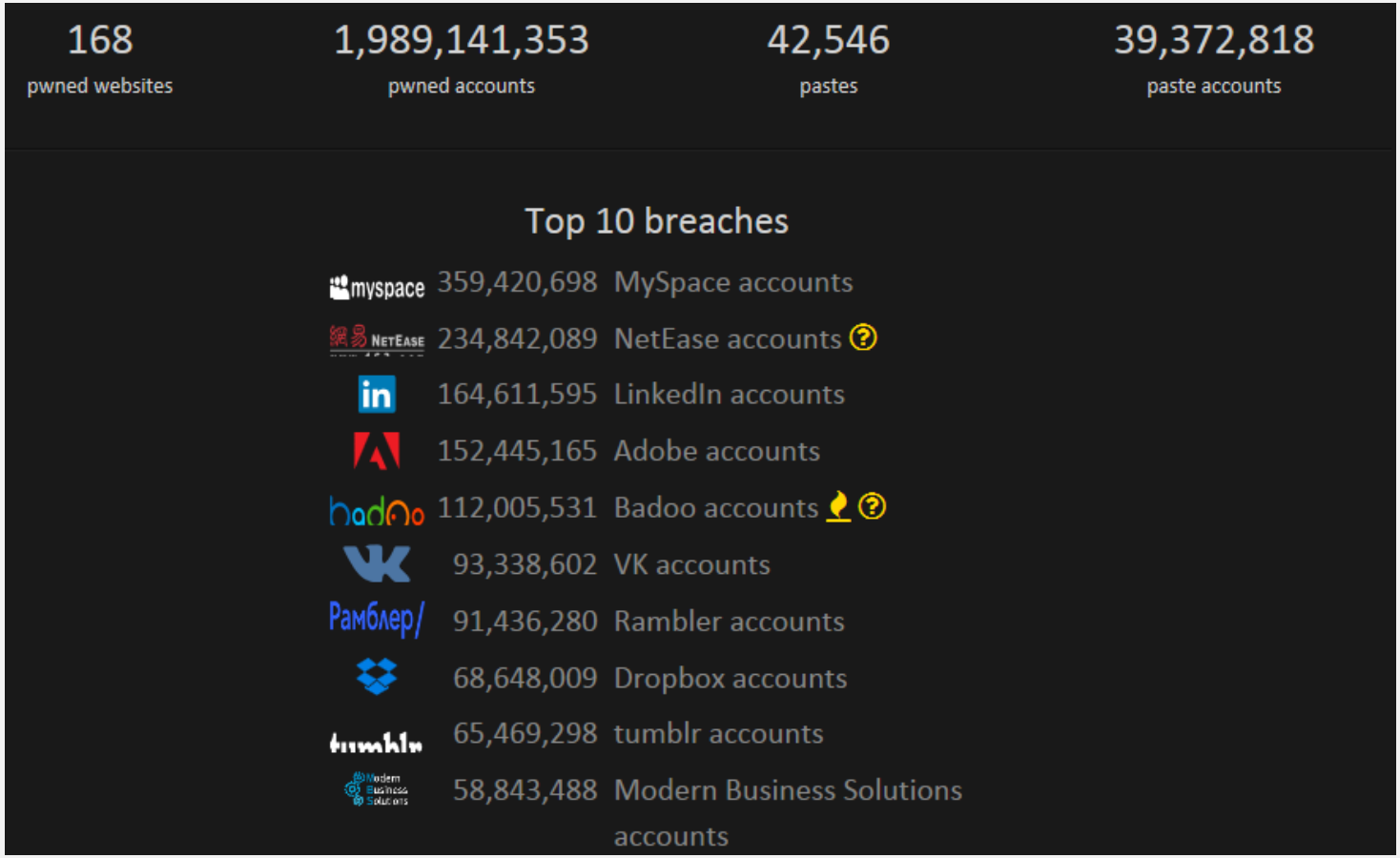
Dropbox證實6800萬帳號資料外洩　急提用戶更新密碼

星島日報 – 2016年9月1日星期四下午7:23

星島日報 - Dropbox證實6800萬帳號資料外洩 -

用戶資料外洩事件頻傳，今年上半年就有LinkedIn、MySpace、Tumblr 及VK.com等知名網站先後傳出數年前的用戶資料遭盜竊，或在流入黑客集團手中。

Statistics of Account Leakage



Reference:
https://haveibeenpwned.com/

Data Breaches in Universities

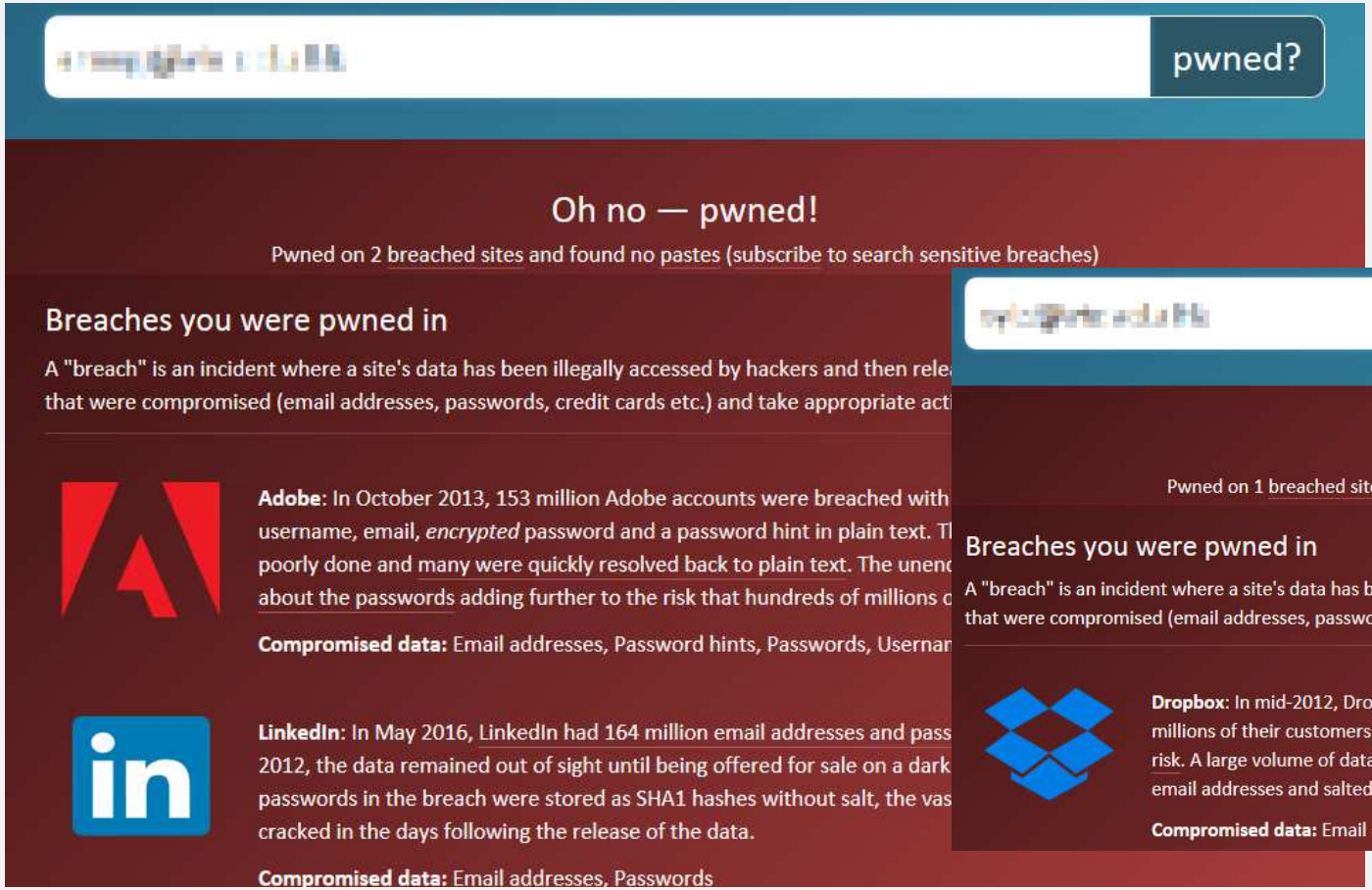
Institution	# Breached	Information Exposed	Cause	Date	Protection Services Offered?
University of Virginia (VA)	1,400 employees	W-2 forms	Phishing	2016/01	Yes
The University of Wisconsin (WI)	15,000	Names, Social Security numbers, email addresses and telephone numbers	Malware	2014/03	No
Olympia School District	2100	Employees' W-2 forms	Phishing scam: fake CEO email	2016/04	Yes
Harvard University (MA)	Administrative offices and students in 8 of Harvard's colleges	Network and email credentials	Hack	2015/05	No

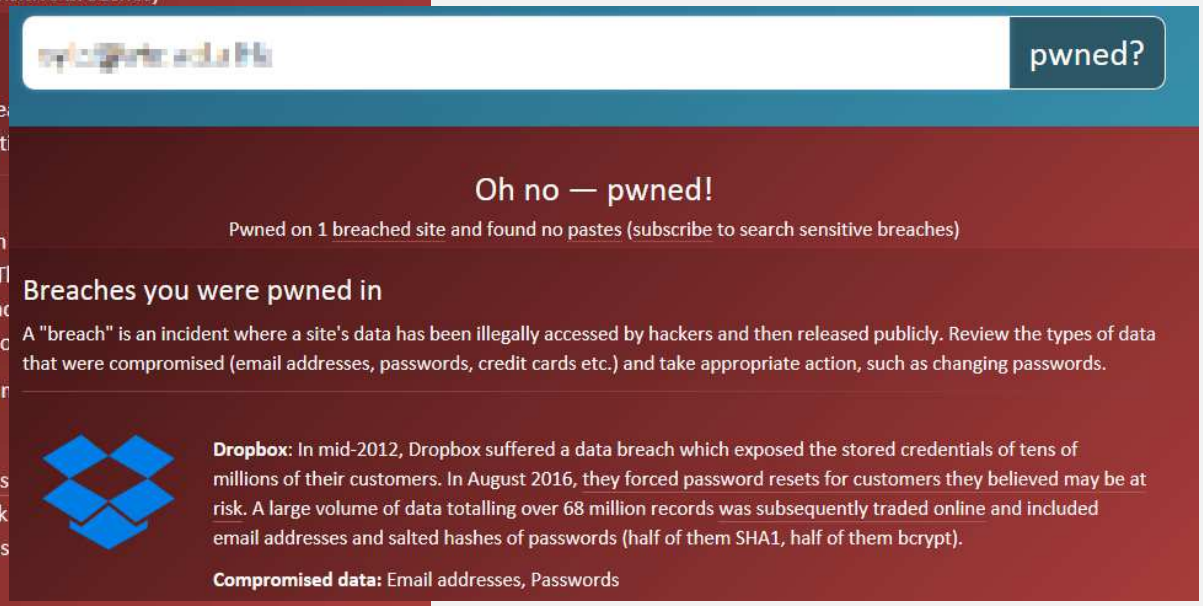
Reference:

https://fightingidentitycrimes.com/data-breaches-educational-institutions/

https://www.crypteron.com/recent-data-breaches/

You account has been leaked?





Reference:
https://haveibeenpwned.com/

What's the cause of these incidents?

前日 上午9:46

<重要通知　慎防偽冒網站>
近日發現有偽冒SmarTone的網站，傳送電郵給客戶並要求提供個人資料，當中包括信用卡資料。我們並無向客戶傳送這些電郵，建議客戶無須理會及刪除有關郵件。我們已向警方備案，同時亦提醒客戶，SmarTone從不會主動透過電郵，要求你提供信用咭資料。如有查詢或收到疑似偽冒電郵，請即致電熱線28802688。
更多詳情：
smartone.com/notice/s

Phishing Email and Website

From: Mail Services <xxxxxx@sbcglobal.net>
Date: 16 August 2016 at 15:21:56 GMT+10
To: <xxxxxx@vtc.edu.hk>
Subject: Your email has been blacklisted
Hello xxxxxx@vtc.edu.hk,

YOUR EMAIL HAS BEEN BLACKLISTED

To undo this kindly follow the instructions below;

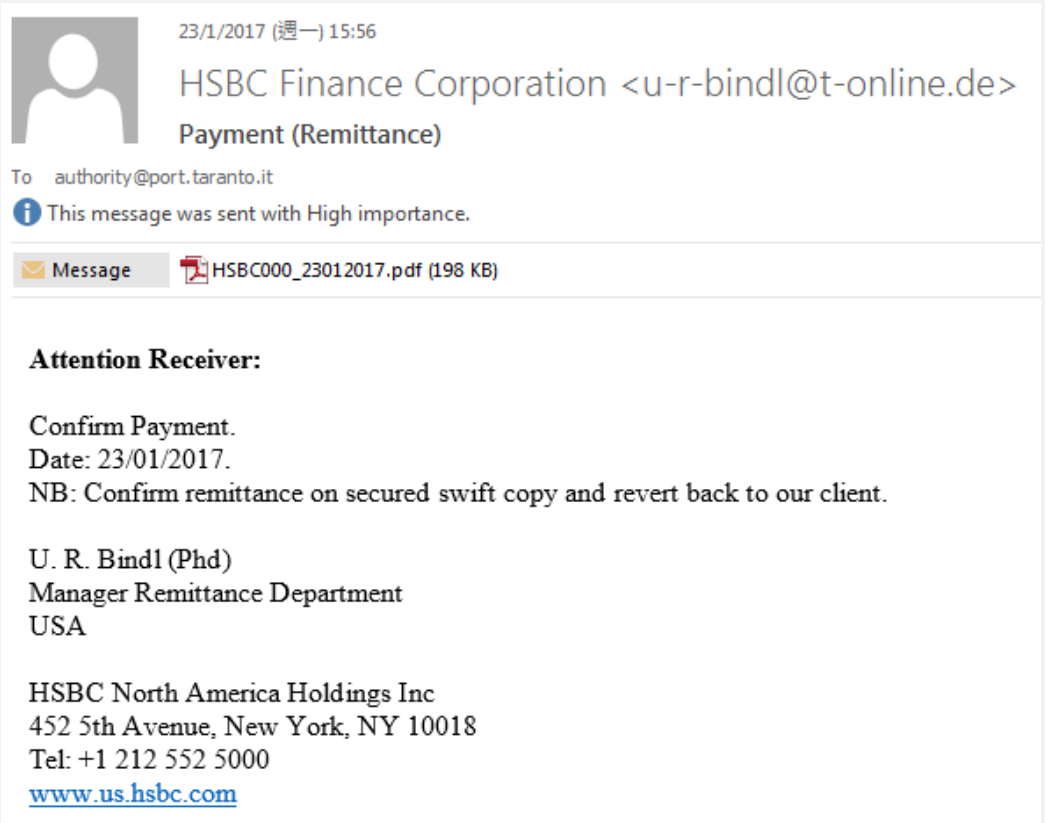
Click-here to Log in and restore your email account access.

Thank you.
Your email: xxxxxxx@vtc.edu.hk

What's the cause of these incidents?

DEMO

Phishing Email with malware



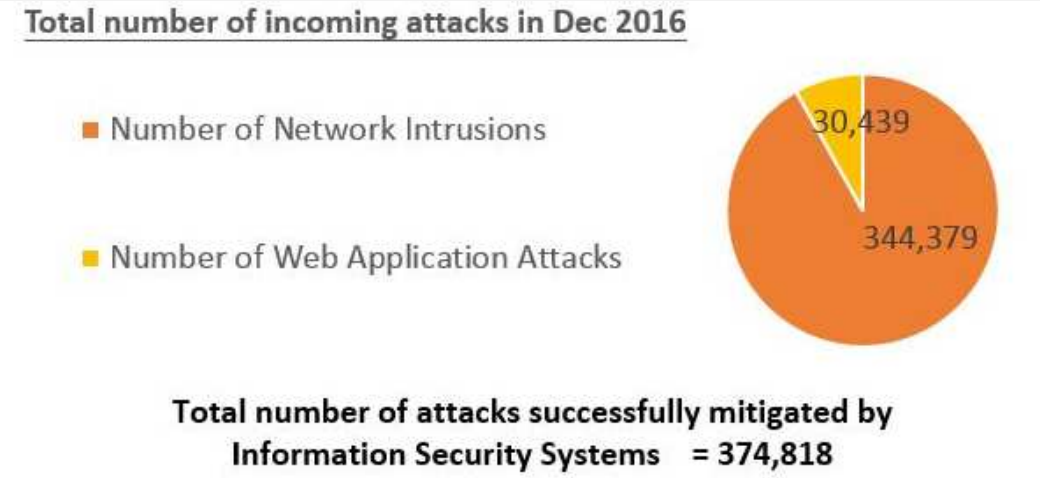
How come of these attack? Any value?

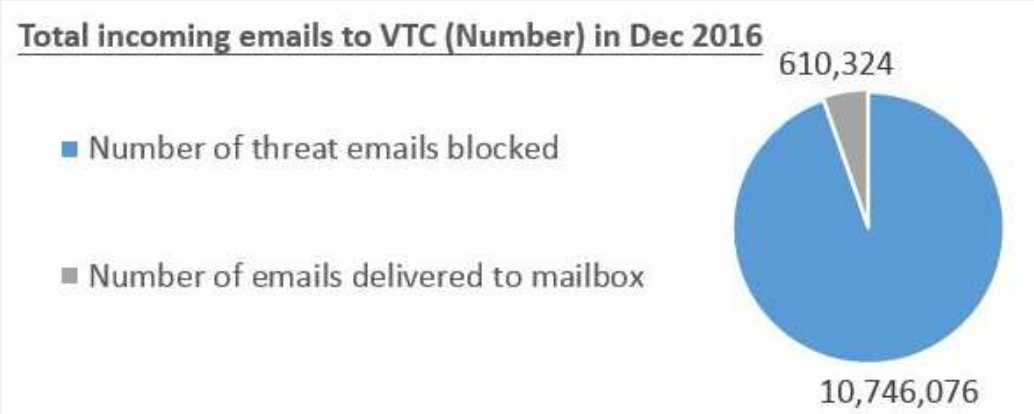
Email Addresses – Gmail	$200 for 1,000
Email Addresses – Hotmail	$12 for 1,000
Email Addresses – Yahoo	$10 for 1,000

Online Bank Account – EU	4 – 6% of account balance
Online Bank Account – USA	2% of account balance
PayPal Account	6 to 20% of account balance

How to minimize the risk?

Monthly Figure of Information Security Systems - Dec 2016

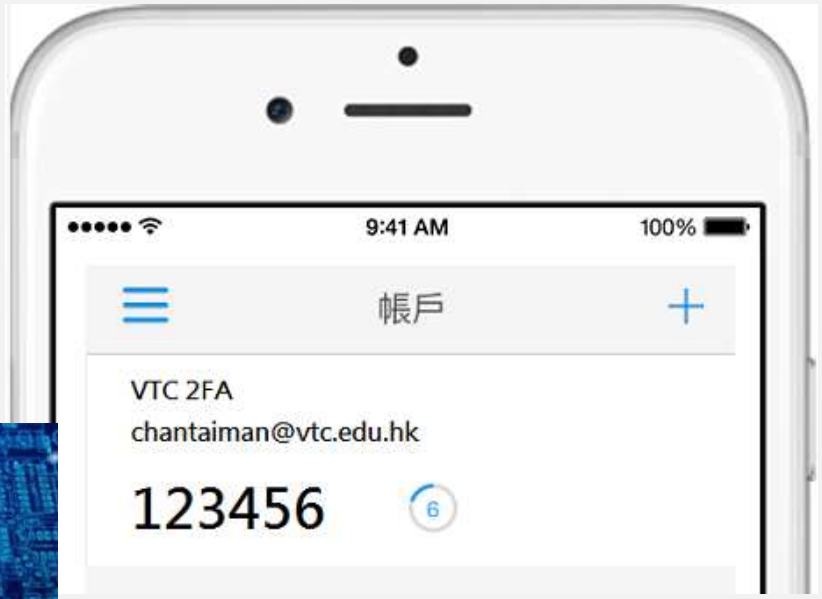




Reference:
https://intra.vtc.edu.hk/infosec/monthly-figure

How to minimize the risk?

- Two Factor Authentication (2FA)
  - Something You Know
  - Something You Have
  - Something You Are
- Secure Login Process



How to minimize the risk?

Resolve to eliminate usernames and passwords

Scott Simkin, senior threat intelligence manager, Palo Alto Networks:

With the rise of software-as-a-service (SaaS) applications, users have been trained to input their credentials into cloud-based authentication sites to access critical services, offering a golden opportunity to spoof these systems and trick users via a phishing email to hand over their valid credentials. Despite years of warnings, people continue to use the same username and password for multiple accounts. It's time to dump those usernames and passwords. In 2017, the industry must resolve to bid farewell to using usernames and passwords and adopt ID verification methods like multi-factor authentication and biometrics. Leading device OEMs, service providers and financial institutions have already started using them; the rest of us need to get on board, too.

Reference:
http://www.computerworld.com/

VTC – Two Factor Authentication (2FA)

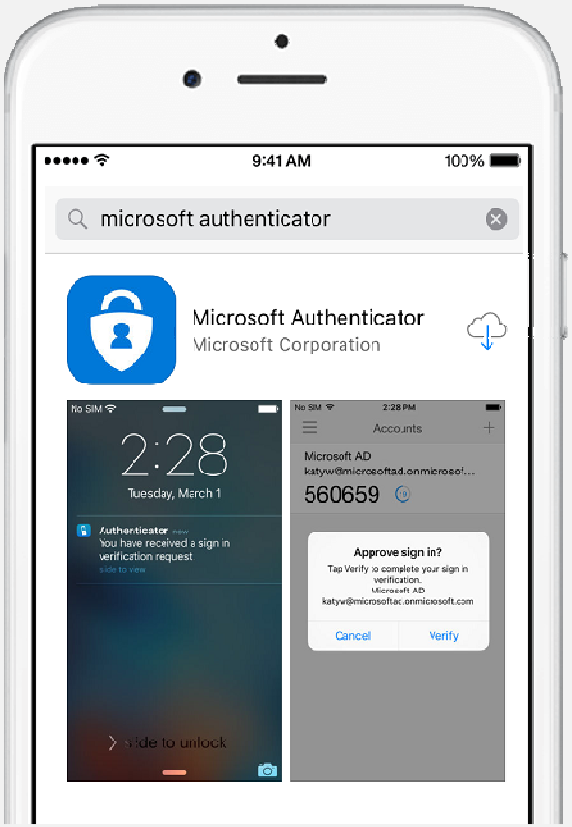
- 2FA service launched in Nov 2016

VTC – Two Factor Authentication (2FA)

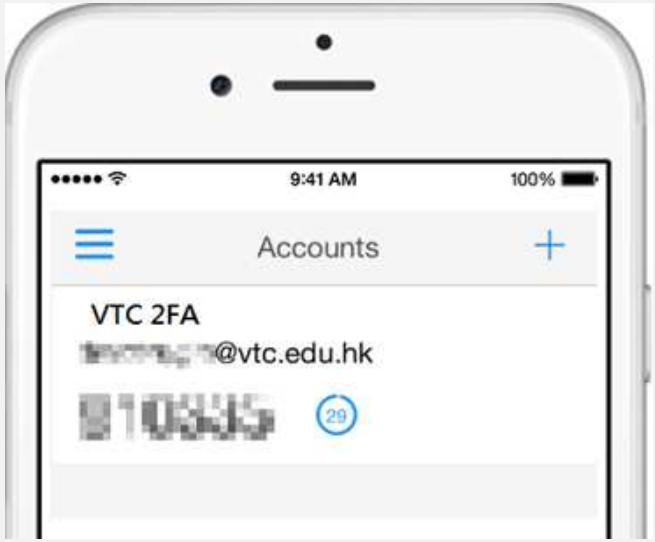
No Additional Hardware Cost

- Leverage mobile device

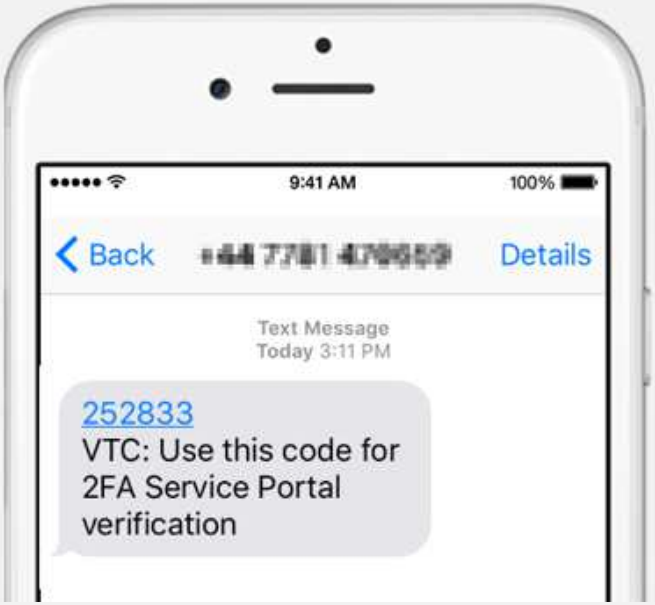
VTC – 2FA Methods (Two Methods)



- **Method 1:** Mobile Token / 移動保安編碼



- **Method 2:** SMS / 短訊



Two ways for authentication

- Easy to Use

VTC – 2FA Registration

步驟一：下載及安裝
STEP 1：Download & Install

Microsoft Authenticator

Authenticator

Available on the App Store

ANDROID APP ON Google play

* 以「短訊」認證，請直接按以下網址進行登記。
* Please click below URL to REGISTER "SMS" authentication.

步驟二：按以下網址進行登記
STEP 2：Please REGISTER at

https://2fa.vtc.edu.hk/portal

登記詳情 REGISTRATION PROCEDURES

iOS 用戶 Users	(	中文 ENGLISH	)	簡訊認證	(中文)
Android 用戶 Users	(	中文 ENGLISH	)	SMS Authentication	(ENGLISH)

- Easy to Register

Reference:
https://2fa.vtc.edu.hk/home/registration_chi.html

VTC – 2FA Demonstration

- Requirements
  - **PC** and **Your Mobile Device**
- Demonstration for 2FA Registration
  - By Mobile Token
  - By SMS
- Demonstration login VTC@Work from External Access
  - Without 2FA
  - With 2FA by Mobile Token
  - With 2FA by SMS
- Demonstration login OneDrive from External Access (Mandatory)
  - Without 2FA
  - With 2FA by Mobile Token
  - With 2FA by SMS

VTC – 2FA Usage and Milestone

- Services Applied
  - VTC@Work
  - ESS and Payroll System Enquiry
  - Telephone Directory
  - VTC Google Search
  - Office 365 (Office Pro Plus and OneDrive)
- Coming Services Integration
  - Webmail
  - New Single-Sign On Solution
  - VTC@HK Mobile App

Frequently Asked Questions

Q) Do I need register 2FA every time?

A) No. You just need to register once.

Q) Can I register 2FA at home?

A) Yes, you can register 2FA at Home or VTC Office.

Q) Any Data access is needed for Mobile Token Authentication?

A) No.

Q) Can I receive SMS message if outside of Hong Kong?

A) It depends on your mobile phone service provider. Recommended to use “Mobile Token” instead.

Frequently Asked Quesions

Q) What can I do if I lost my mobile device or replaced my mobile device?

A) Please contact our helpdesk service by 2836 1202.

Q) Can I Change Authentication between SMS & Mobile Token after registration? Can I have one more Mobile Device for authentication?

A) Yes. (Demo for 2FA Service Portal)

Q) Can I use mobile device to login 2FA Service Portal for Registration?

A) Not recommended. Registration process is best viewed with PC's IE/Chrome/FireFox.

Q&A

Useful Resources

- Two Factor Authentication (2FA) Service Portal
  - https://2fa.vtc.edu.hk/
- 2FA Home Page and FAQ Page
  - https://2fa.vtc.edu.hk/home
  - https://2fa.vtc.edu.hk/home/faq.html
- Enquiry
  - Email: itsd-helpdesk@vtc.edu.hk
  - Telephone: 2836 1202

THE END