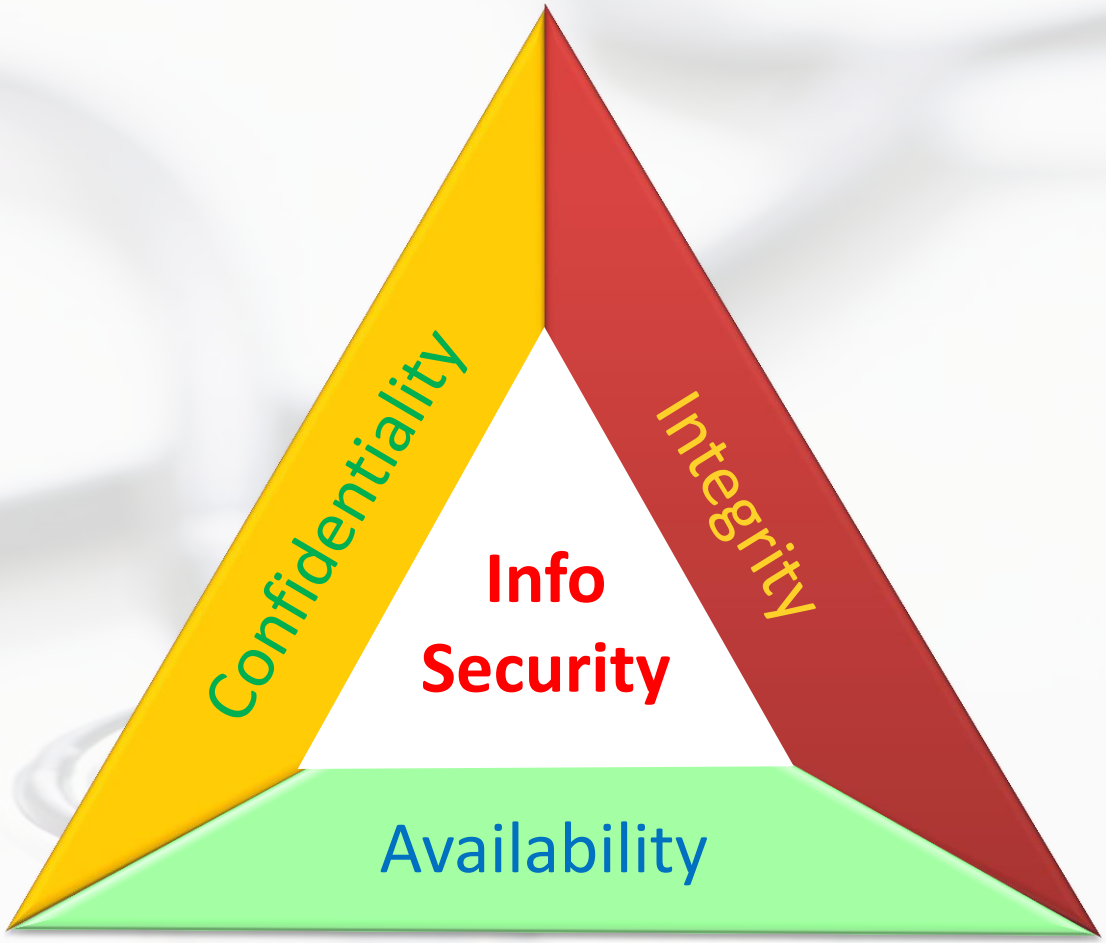
Keep eHRSS & your EMR Safe from Cyber-attacks

Clara Cheung
Chief Systems Manager
Hospital Authority

醫健通
ehealth
香港特別行政區政府 HKSAR GOVT


Confidentiality
Integrity
Info
Security
Availability

‘Inadvertent Weakness’

- Fall for Phishing
- Use of Weak Passwords
- Unsecured Personal Devices
- Delayed security patches, outdated software
- Poor security mindset

What you can do

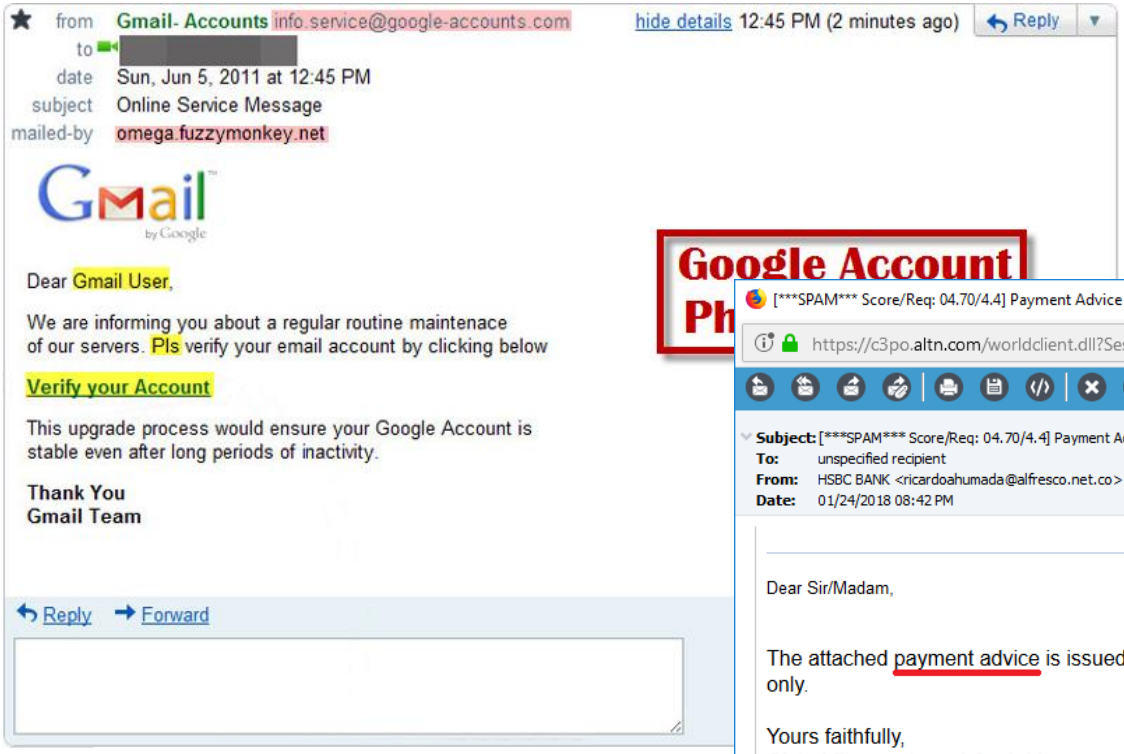
- Be suspicious

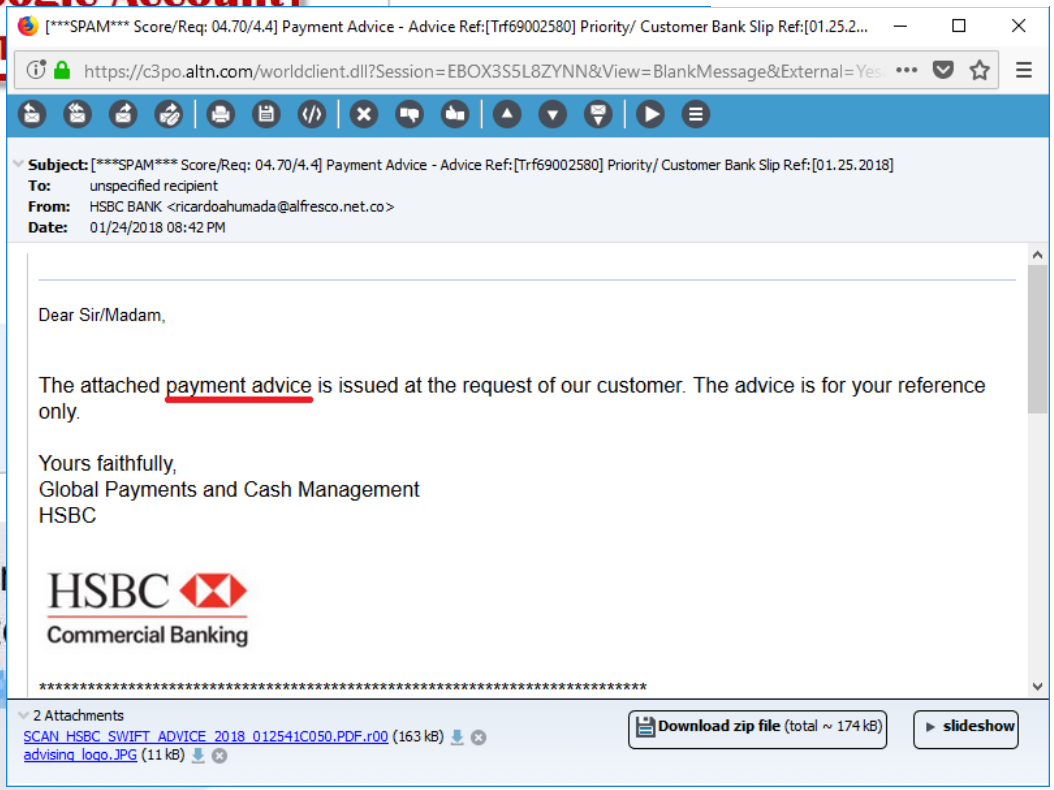
What is Phishing

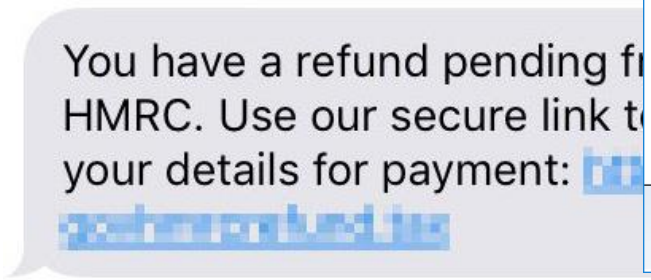
- **Phishing** is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
  - Compromised Credentials
  - Dropping Malware
  - Business Email Compromise (CEO Fraud)

Be Wary of Suspicious email/messages

Think before You Click







Learn Who to Trust

Beware of Identity Spoofing

Verified badge

What you can do

- Protect your account

Protect Your Account

- Separate professional & personal accounts ★
  - Do not use same user accounts and passwords for everything
- Distinguish ‘serious business’ vs. ‘fun’
- Develop your own method to help you remember the different accounts and passwords

Weak Passwords

What is Strong Password?

- Never disclose your passwords
- Use long password (passphrases)
  - “ipreferpassphrasesoverpasswords@”
  - easier to remember & more difficult to crack
- If limited by no. of characters, use combination of unrelated words, numbers, special characters (# @ ! |}…), capitals
- Do not use dictionary words or anything personal, e.g. own name, pets’ names, date of birth …
- Get Creative with Security Questions
  - For increased security, lie about your answers or use passphrases as the answers

Manage your eHRSS Accounts

- Do not share accounts
- Do not disclose your passwords
- Keep your token safe
- Keep an eye on who is watching when you login
- Logout when you won't use the system for a while
- For healthcare professionals, when you leave an employer
  - No need to return your token to your employer (can return to eHRSS Registration Office)
  - Change your password before you leave

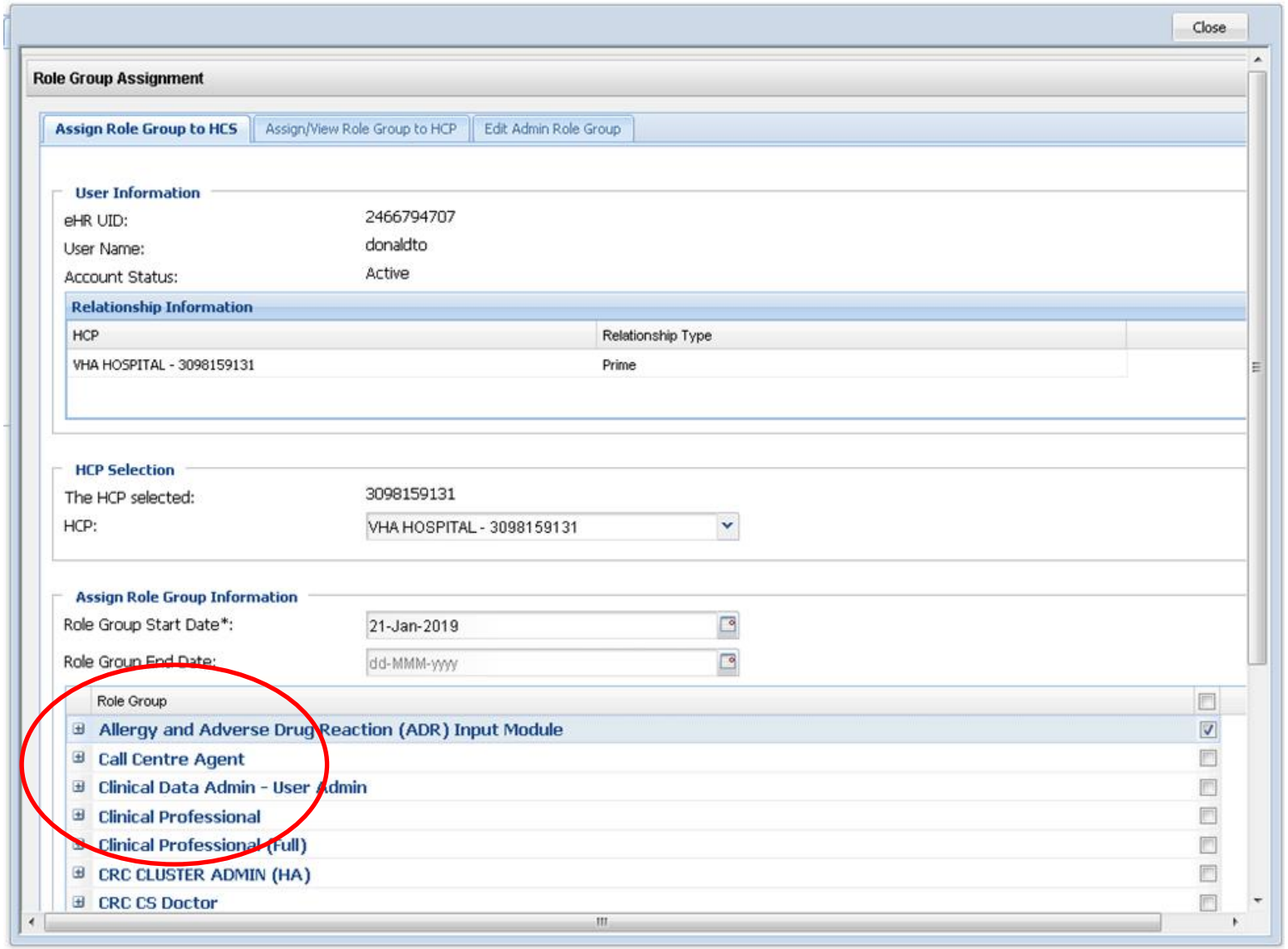
What your organisation can do

- Control access to your systems

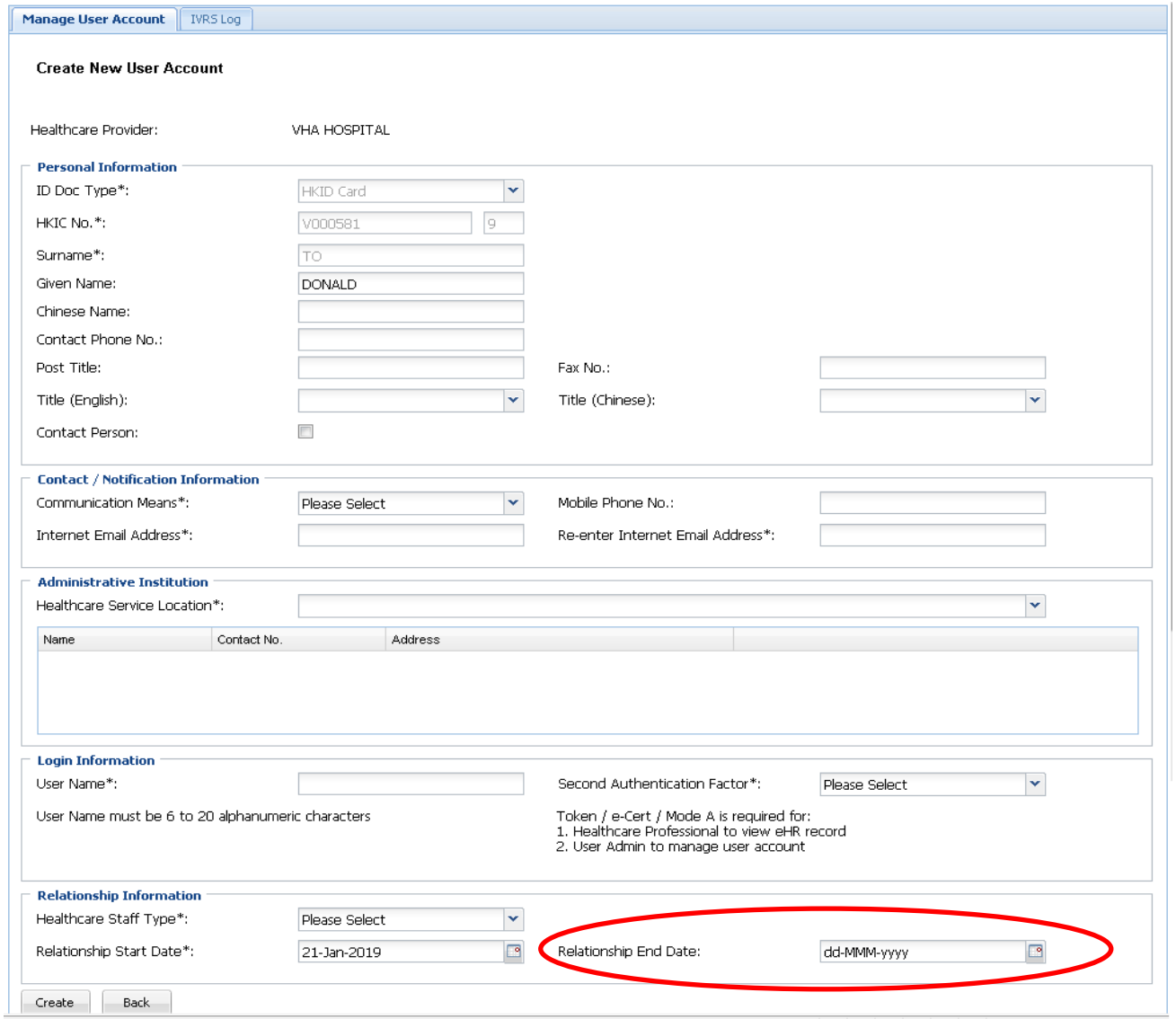
Manage Authorised eHRSS Accounts

- Do not allow sharing of accounts
- Assign appropriate user roles
- Install ELSA only on authorised workstations
- Check eHRSS User Access Log regularly
- Review your list of active accounts regularly
- When an employee leaves
  - ‘End the relationship’, or Terminate the account

Role Assignment



End Relationship



What your organisation can do

- Protect your Systems and Data

Protect Your Assets

- Back up valuable data
- Beware of unsafe storage devices
  - Do not connect other people's devices to your computer
  - Run antivirus scan, even if it is new, on a computer not connected to the network nor the internet
- Enforce screen saver with passwords
- Secure physical and cloud storage
- Learn to manage configurations of your EMR
- Password lock files with sensitive information
- Disable 'Guest' Login

Software Security

- Keep your software up-to-date (Browser & OS)
  - Backup your data and system before update / patches
- Use anti-virus & anti-malware & keep definitions up-to-date
- Check security features of your EMR
  - Require mandatory user login to system
  - Enforce clear delineated roles and access for different types of users
  - Support and enforce strong passwords
  - Encrypt sensitive data in transit and storage
  - Support current OS and Browser versions
  - Provide auto time-out or screen lock

Beyond electronic medical record

Security Mindset

- Security Awareness Training
- Lock up paper records / photocopies with personal data
  - Who will be there after-hours?
- Check twice before giving out patient reports
  - Aware mixing up photocopies
  - Aware mixing up patient identities in reports
- Place workstations appropriately to avoid prying
- Secure your backup storage