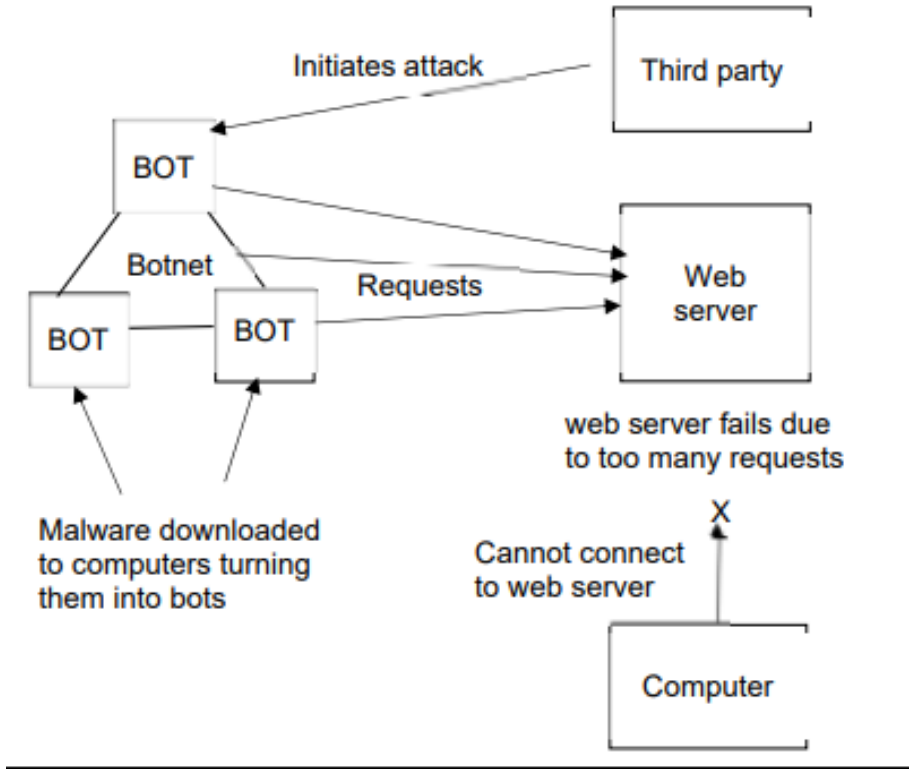
CYBER SECURITY THREATS

- Brute force attacks
  - Trying all the different combinations of letters, numbers and other symbols until can login to the system
- Data interception
  - It is a form of stealing data by tapping into a wired or wireless communication link. The intent is to compromise privacy or to obtain confidential information
  - Using packet sniffer software
- Hacking
  - Gaining data without permission

CYBER SECURITY THREATS

- Distributed Denial of Service (DDoS) attacks
  - Malware is installed to the target computer
  - Those computers become “bot” or “zombie”
  - Bots flood a server with high number of requests
  - If the server cannot handle the spam requests, it will out of service



CYBER SECURITY THREATS

- Malware : malicious software
  - Virus
    - They are programs or program code that replicate (copies themselves) with the intention of deleting or corrupting files, or causing a computer to malfunction
    - It requires a host
  - Worms
    - They are a type of stand-alone malware that can self-replicate with the intention of deleting or corrupting files, or causing a computer to malfunction
    - It doesn't require a host
  - Trojan horse
    - a program which is often disguised as legitimate software but with malicious instructions embedded within it
    - User might think the file is valid and run the file which will execute the malicious code
  - Spyware
    - software that gathers information by monitoring a user's activities carried out on their computer. The gathered information is sent back to the cybercriminal

CYBER SECURITY THREATS

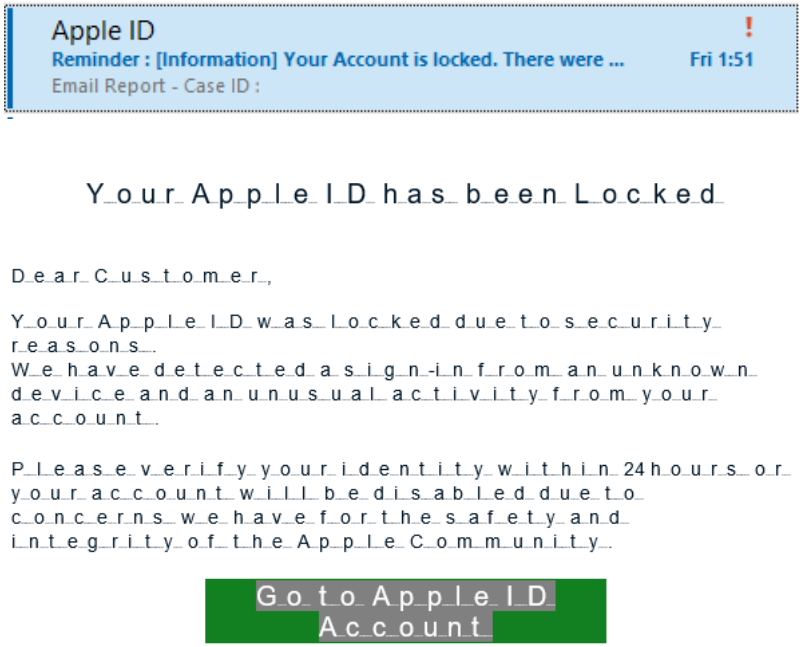
- Malware
  - Adware
    - software that floods a user's computer with unwanted advertising; usually in the form of pop-ups but can frequently appear in the browser address window redirecting the browser to a fake website which contains the promotional adverts
  - Ransomware
    - programs that encrypt the data on a user's computer; a decryption key is sent back to the user once they pay a sum of money (a ransom); they are often sent via a Trojan horse or by social engineering

CYBER SECURITY THREATS

- Phishing
  - The creator sends emails (copycat official emails) with fake links to the targets. When the targets click on those links, it will redirect to the fake websites. If the targets enter personal data the creator will gain those data
- Risks
  - Lose personal data
  - Fraud or identity theft

Protections

- Use ISP or email server that has filter out phishing email feature
- Be cautions when opening emails or links
- Do not open unknown email

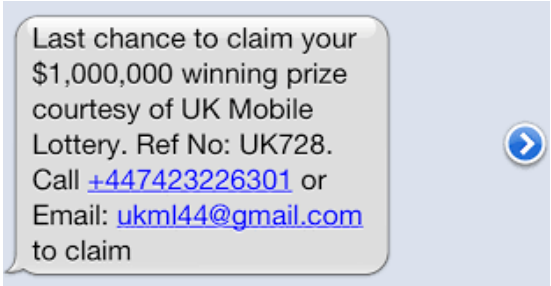



จัดการ Apple ID ของคุณ - Apple
appleid-apple.secureaccount-feedback-us.meiaprisi.com/IDMSWebAuth/?controls=login&sessionId=334561b2fd6b3b6f5bcb089e64960e5e23674861e6e50250c0d4219a39ac379a&country=TH
Incognito
Mac
iPad
iPhone
Watch
TV
Music
บริการช่วยเหลือ
Apple ID
ลงชื่อเข้า
สร้าง Apple ID ของคุณ
คำถามที่พบบ่อย
Apple ID
จัดการบัญชี Apple ของคุณ
Apple ID
จำ Apple ID ของฉัน
ลืม Apple ID หรือรหัสผ่านหรือไม่?
บัญชีของคุณสำหรับทุกสิ่งที่เป็น Apple

CYBER SECURITY THREATS

- Pharming
  - Malicious code is installed on a user's computer, the code will redirect to a fake website. (the user doesn't have to take any action)
  - DNS cache poisoning : changing real IP address with the fake one
- Risks
  - Lose personal data
  - Fraud or identity theft
- Protection
  - Anti-spyware can remove pharming code
  - The users should always be alert and look for clues

CYBER SECURITY THREATS



- Social engineering
  - It occurs when a cybercriminal creates a social situation that can lead to a potential victim dropping their guard
  - It involves the manipulation of people into breaking their normal security procedures and not following best practice
  - Example
    - SMS
    - Scare ware : pop up in browser that try to scare users e.g. virus infection warning
    - Phishing
    - Phone calls