# Information Security Starts with You.

**Presented by**
May Oo Khaing

07th Feb 2022

WAVE MONEY

# About Me

- Currently working as a Chief Information Security Officer at Wave Money.
- has a successful track record both locally and internationally, having worked more than 12 years in in IT, and 8+ years specialising in Information Security & Compliance.
- Possess a Master’s degree in Computer Technology from University of Computer Studies, Yangon and also graduated from Nanyang Technological University, Singapore with an MSc in Computer Engineering.

# Women Empowerment at Wave Money

- **124** out of 272 total employees are female staff which is **46%** of entire workforce.

- 113 out of 204 employees from Head Office are female staff that is **55%** of the total head office employees.

- **14** out of 26 extended leadership team members are female leaders which is **46%** of entire ELT.
- Among them, **89%** are promoted within the organization that accounts for 92% of the current pool.

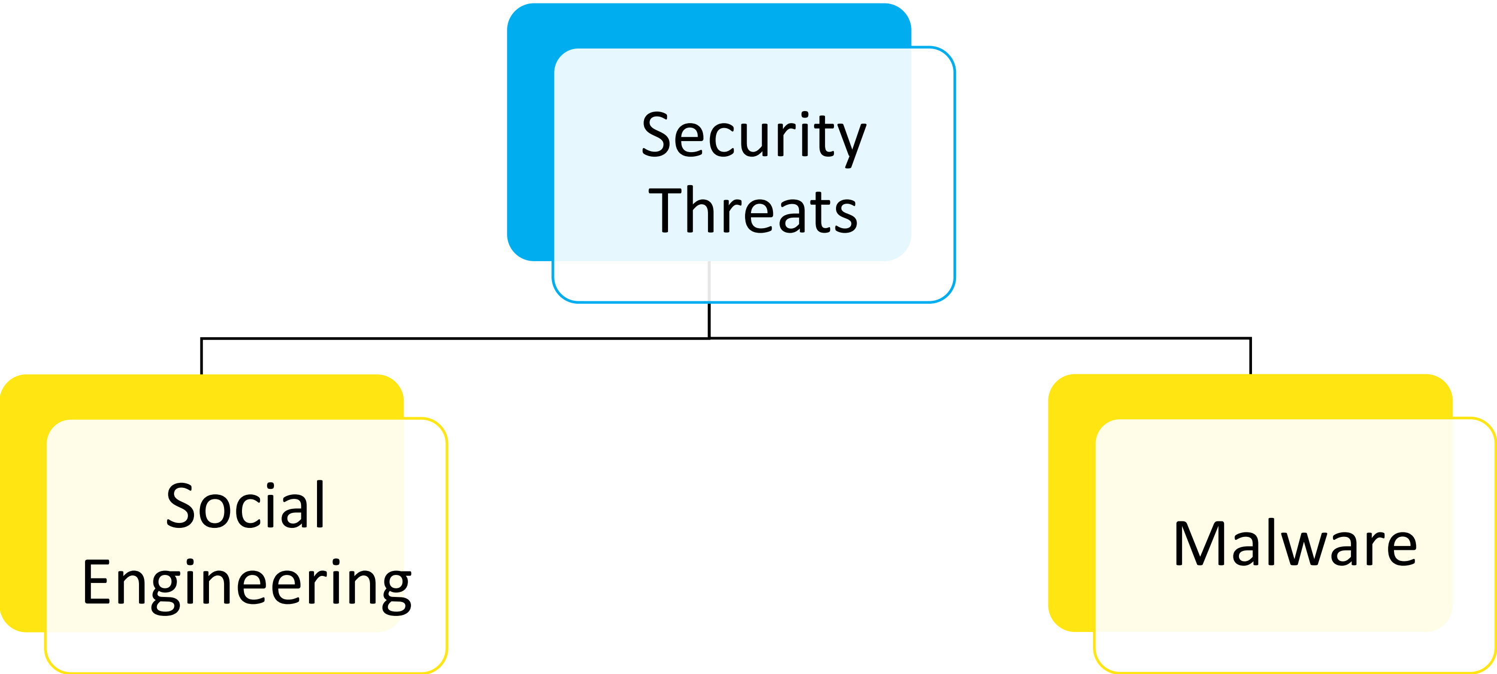
- 3 out of 7 leadership team are female leaders which accounts for **43%** in total.
- Among entire leadership teams, **100% of our female leaders are locally promoted.**

- Every female staff who went on maternity leave comes back, work full time and stay. (6 months paid maternity leave)
- Wave Money provide great insurance coverage and support for maternity,

# Why Information Security Starts with You?

Every time you use the Internet, you are making choices related to your information security. Should a link be clicked, website be accessed, and wireless networks be joined, data be shared? Your security and the security of your family, friends, coworkers, and people around you depend on making secure online decisions. Making the Internet more safe and secure requires all of us to take responsibility for our own cybersecurity posture.

# Types of Security Threats



Security Threats

Social Engineering

- Targets humans
- Phishing
- Tailgating
- Shoulder surfing

Malware

- Viruses
- Worms
- Trojans
- Ransomware

# Social Engineering

- ❑ Social Engineering is the term used for malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

- ❑ Preferred by Attackers

  - ❑ Psychological manipulation is easier than using Technology manipulation.

  - ❑ Hard to detect and track.

  - ❑ Uses a common tendency of trust

  - ❑ Target the weakest link, i.e. humans

Image Source: https://www.smartfile.com/blog/social-engineering-attacks/

Social Engineering is further **enabled** by

**YOUR Digital Footprint**

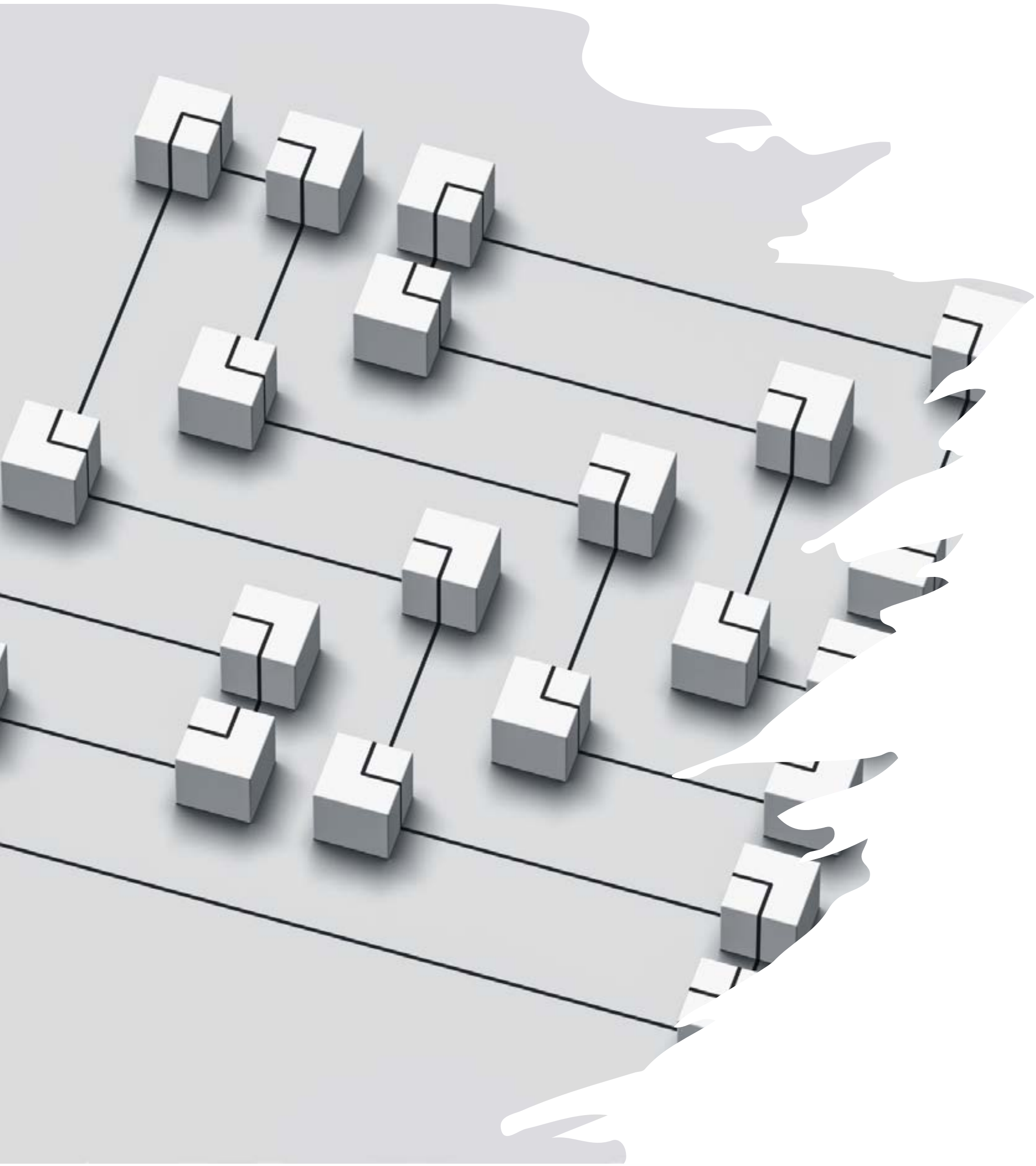
# Phishing

# Phishing

- ❑ A type of cyber crime where an attacker sends a fraudulent message designed to trick a human victim. It is easier than hacking and it exploit human psychology and take advantage of unaware users.

- ❑ Purpose of attacker is
  - To catch passwords, credit card details and other valuable information,
  - To inject malicious code on your computer, opening a door for further exploitation Eg. Trojans, Ransomware.

- ❑ Common characteristics of Phishing emails
  - Any email with an offer that is too good to be true
  - Any email with a threat of losing something vital if you don't act imminently
  - It always with a link to click or an attachment to open from unknown sender



# THiNK Before You Click

### Look for the Address

- Before clicking any link, check it by using your mouse to hover over the link.
  E.g. - [www.facebook.com/yourprofile](www.facebook.com/yourprofile)

### Read the domain name closely

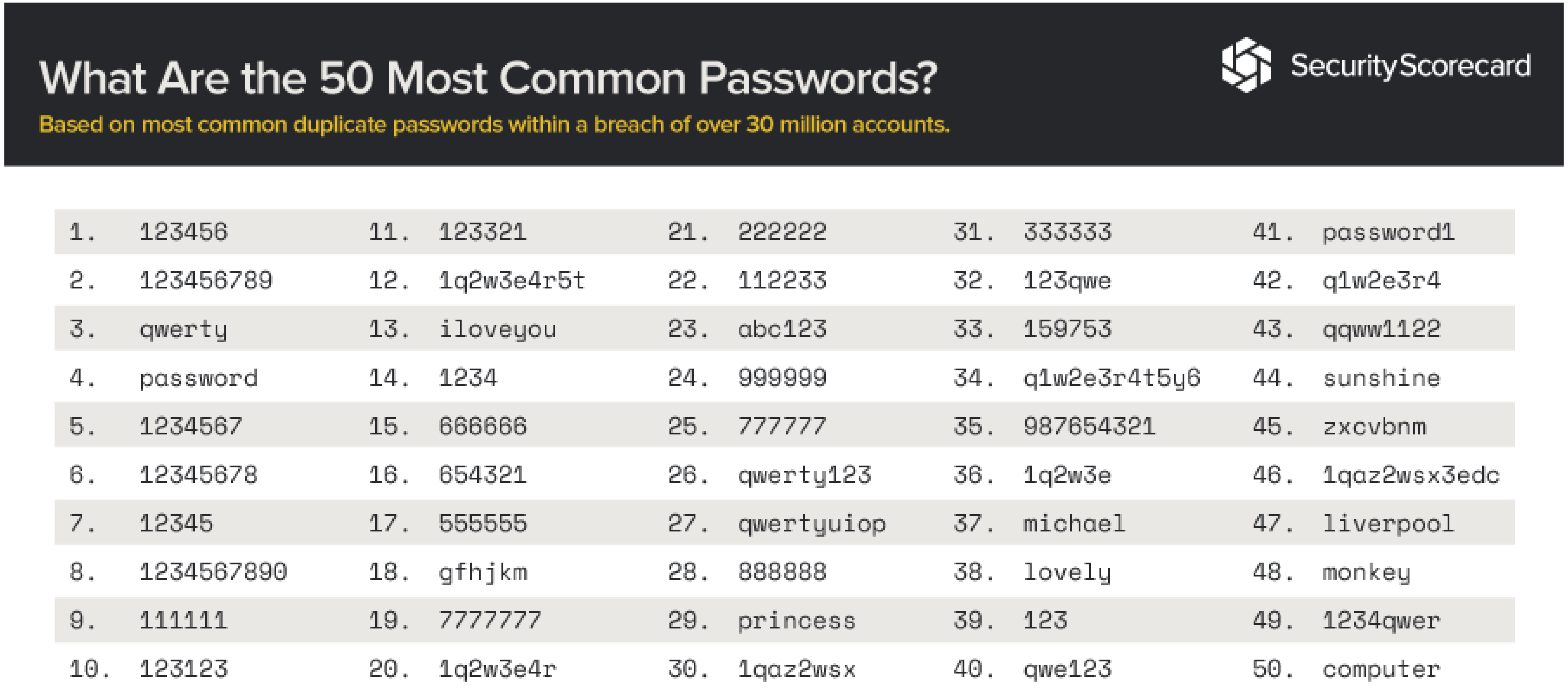
- Attackers commonly buy similar domain names or register the domain name on a different top-level domain.
  E.g. - [www.wavemoneymm.com](www.wavemoneymm.com) can be seemed like legitimate URL until you check it closely.

### Beware of Long addresses

- Some URLs are very long and consisting of a chain of cryptic-looking characters. Beware of these as they could be programmatically constructed to conceal the true destination.
  E.g. - https://t.redpoints.com/t/11100/c/5d904e72-64ff-4a4f-a30a-d08806adc9f7/NB2HI4DTHIXS653XO4XHEZLEOBXWS3TUOMXGG33NF5XW43DJNZSS2YTSMFXGILLQOJXXIZLDORUW63RPH5ZWE4TDHUYVQ5S7K5ZHI6DHMVDUC4LMONIVG43YIVXVMUJFGNCCKM2EEUZDI2TEJFPUW2TWGVRGESL2O5TEMZTHIRQU46KREUZUIJJTIQ======/www-redpoints-com-online-brand-protection

- When in doubt, seek for Security advice.

# Bad Password Practice



## What Are the 50 Most Common Passwords?

SecurityScorecard

Based on most common duplicate passwords within a breach of over 30 million accounts.

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. 1234567890
9. 111111
10. 123123
11. 123321
12. 1q2w3e4r5t
13. iloveyou
14. 1234
15. 666666
16. 654321
17. 555555
18. gfhjkm
19. 7777777
20. 1q2w3e4r
21. 222222
22. 112233
23. abc123
24. 999999
25. 777777
26. qwerty123
27. qwertyuiop
28. 888888
29. princess
30. 1qaz2wsx
31. 333333
32. 123qwe
33. 159753
34. q1w2e3r4t5y6
35. 987654321
36. 1q2w3e
37. michael
38. lovely
39. 123
40. qwe123
41. password1
42. q1w2e3r4
43. qqww1122
44. sunshine
45. zxcvbnm
46. 1qaz2wsx3edc
47. liverpool
48. monkey
49. 1234qwer
50. computer

# Follow Good Password Management Practices.

- ❑ Never reveal your passwords to others.
- ❑ Use different passwords for different accounts.
- ❑ Use two-factor authentication (2FA).
- ❑ Length trumps complexity.
- ❑ Make passwords that are hard to guess but easy to remember.

# Good Security Practices

Follow Good Password Management Practices.

Always be careful of the offers that are too good to be true. Be aware of scam calls, emails and messages.

Think carefully before sharing your personally identifiable information to others.

Make sure you are connected to a secured WiFi.

Think Before You Click!

# THANK YOU

WAVE MONEY