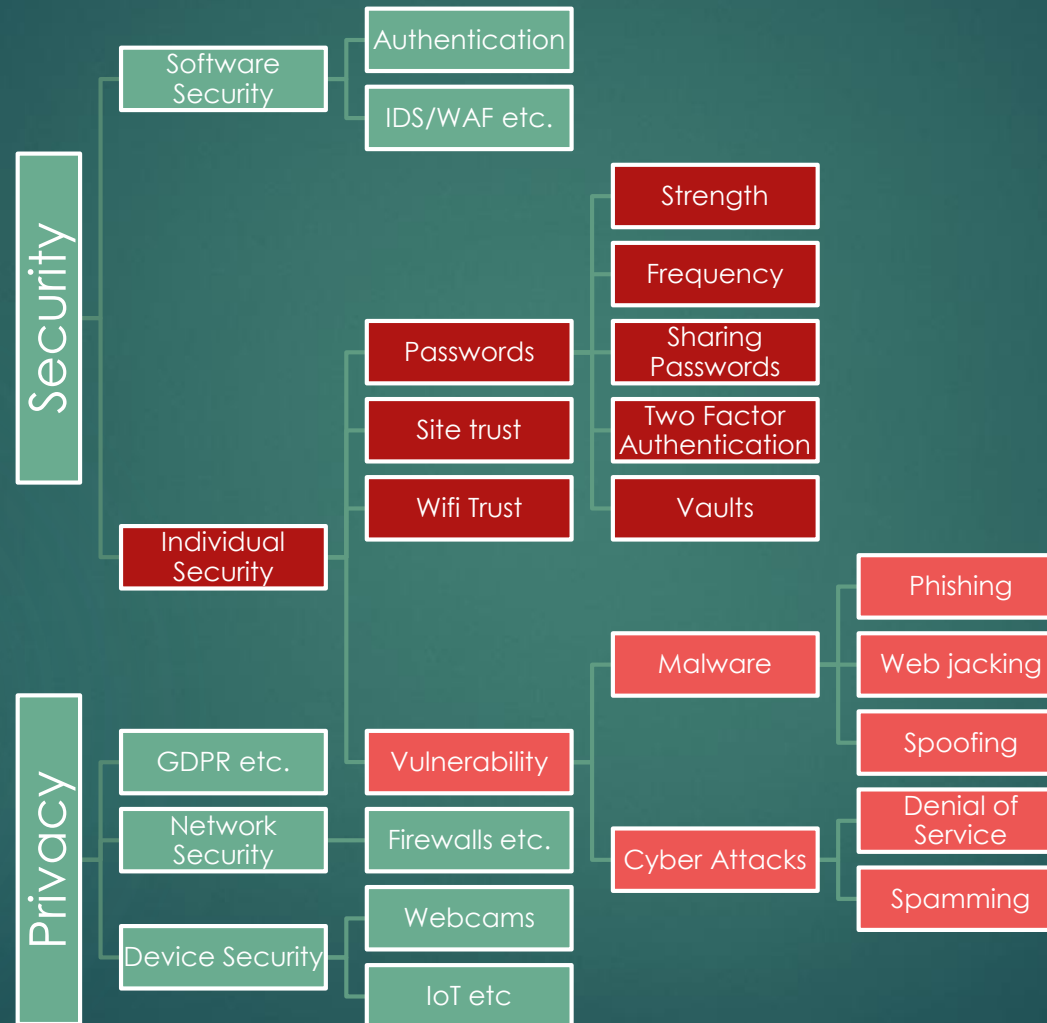


INDIVIDUAL SECURITY

WHY IS IT SO EASY TO SCREW UP YOUR TECHNOLOGY BUSINESS?

Aqeel Ahmad
CTO

SECURITY LANDSCAPE



Personal data is a **tradable commodity**



Dark web

Breach monetization

Malware

Marketplaces

Forums

Repositories

Account
Passwords
(\$1 per
account)

Email
Addresses

Social
Security
Numbers

Credit cards

Documents

**Coworker
Data**

Hire a Cyber
Hitman





















Spying


Ransomware


Custom
Malware

have I been pwnd?



285	5,070,707,149	70,549	77,227,844
pwned websites	pwned accounts	pastes	paste accounts
Largest breaches		Recently added breaches	
	711,477,622 Onliner Spambot accounts		26,151,608 Ticketfly accounts
	593,427,119 Exploit.In accounts		777,649 ViewFines accounts
	457,962,538 Anti Public Combo List accounts		24,853,850 VNG accounts
	393,430,309 River City Media Spam List accounts		7,485,802 17173 accounts
	359,420,698 MySpace accounts		10,371,766 TGBUS accounts
	234,842,089 NetEase accounts		188,847 ILikeCheats accounts
	164,611,595 LinkedIn accounts		6,844,490 CashCrate accounts
	152,445,165 Adobe accounts		27,971,100 Taringa accounts
	112,005,531 Badoo accounts		386,489 Smogon accounts
	105,059,554 B2B USA Businesses accounts		13,873,674 HiAPK accounts



[Home](#) [Notify me](#) [Domain search](#) [Who's been pwned](#) [Passwords](#) [API](#) [About](#) [Donate](#) 

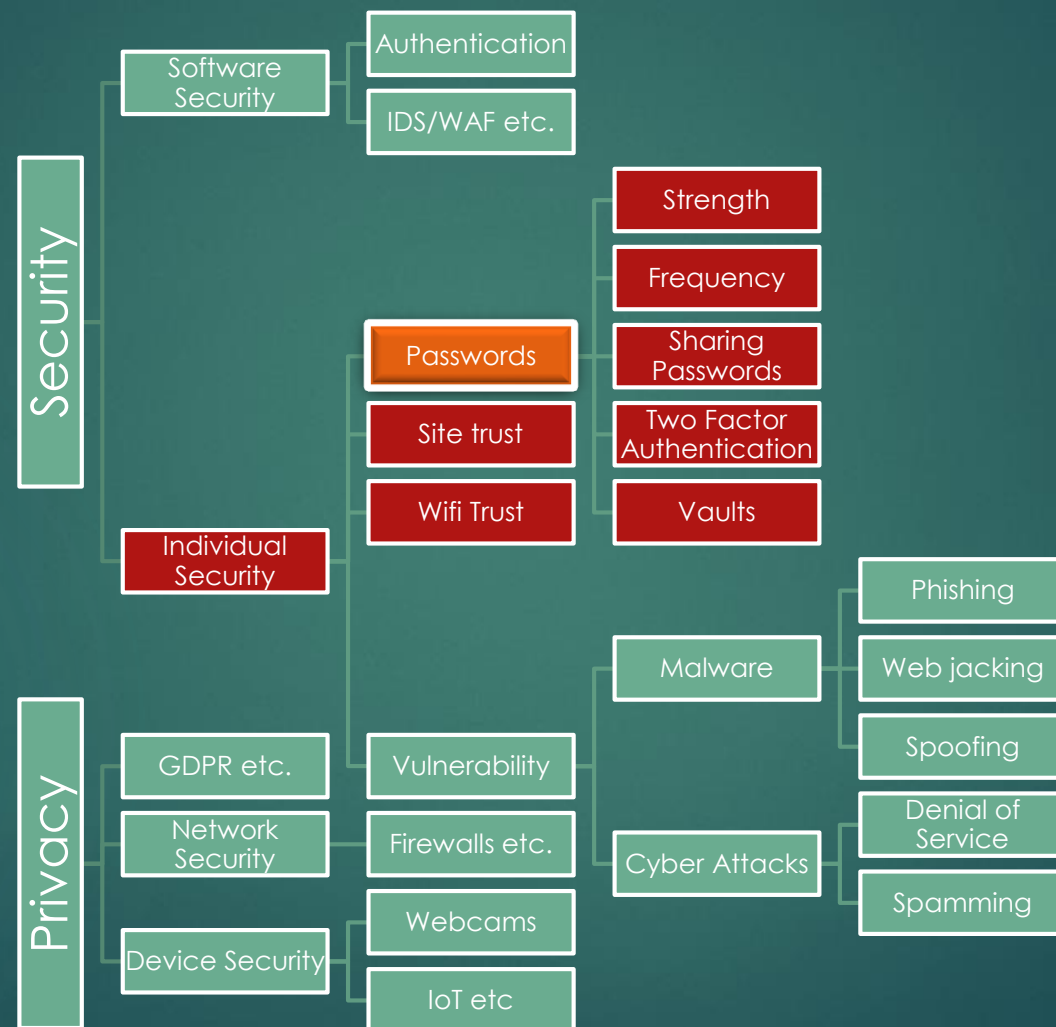
';--have i been pwned?

Check if you have an account that has been compromised in a data breach

<https://haveibeenpwned.com>

SECURITY LANDSCAPE

Any questions?



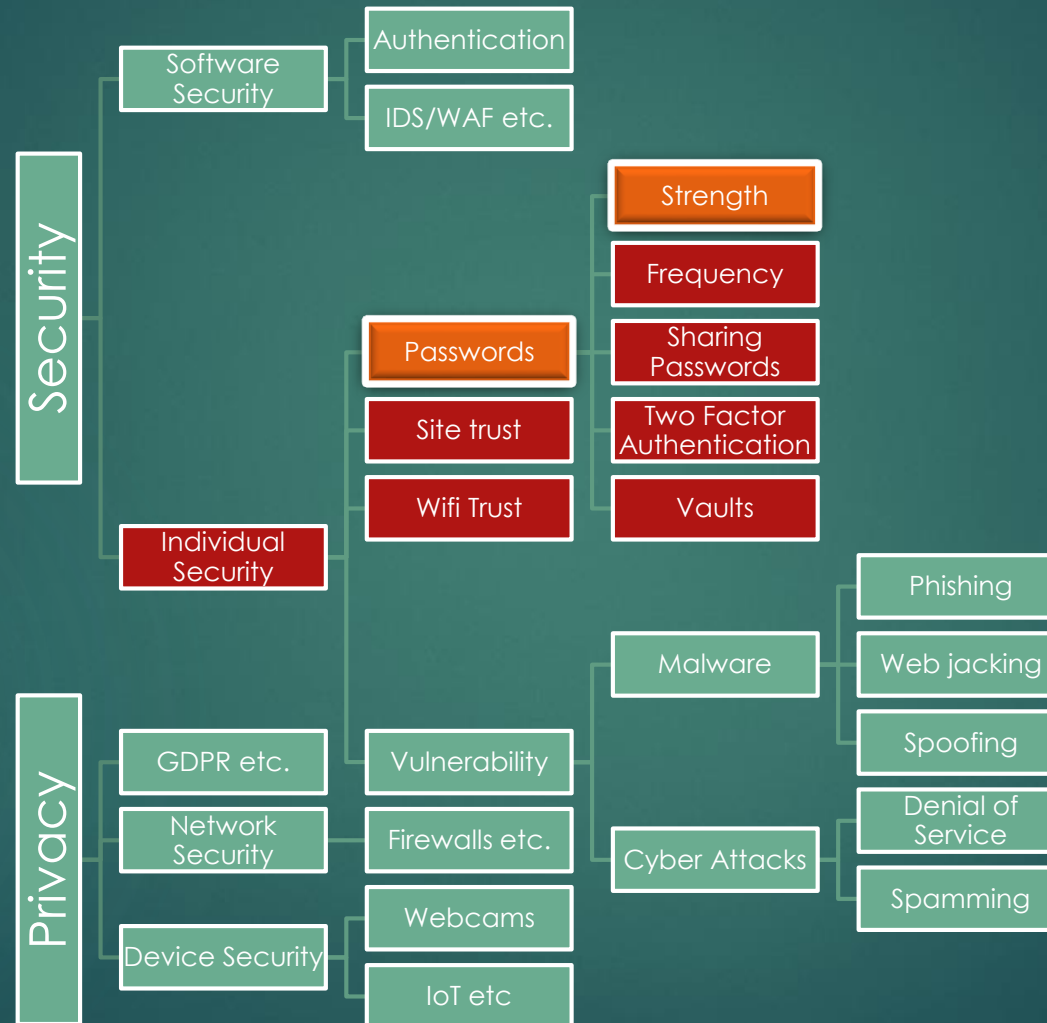
Two Biggest Causes



1. Weak Passwords

2. Same password across sites

SECURITY LANDSCAPE



Weak Passwords

- ▶ Common components of easy-to-hack passwords:
 1. Repeating previously used passwords
 2. Names of close family members or friends
 3. Your name
 4. Words in the dictionary
 5. Common names
 6. Repeating your user id
 7. Keyboard patterns and swipes (i.e., 123456 or QWERTY)

- ▶ <https://howsecureismypassword.net/>



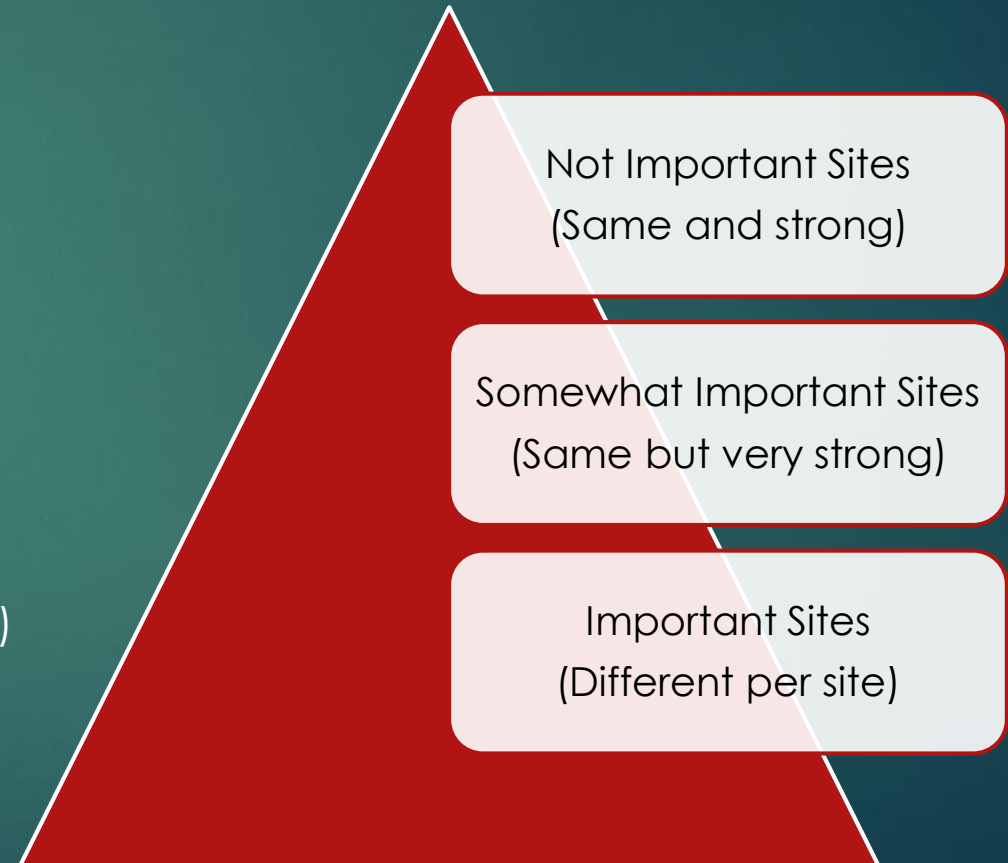
Different Passwords for different sites



Huge Pain but Ideal

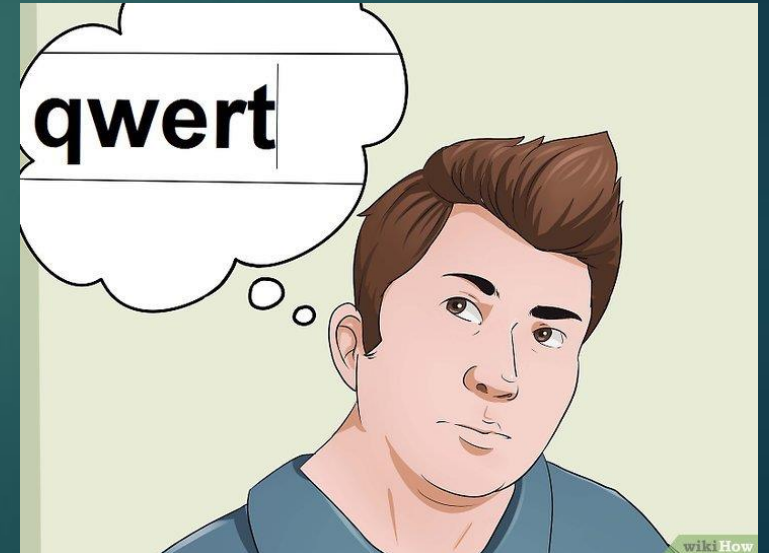
Middle Ground:

- ▶ Sensitivity segments:
 - ▶ **Low** (News websites, etc.)
 - ▶ **Medium** (Facebook, Twitter, etc.)
 - ▶ **High** (EBanking, Google Account, etc.)



Strong memorable passwords - **Problem**

- ▶ Human brain sucks at remembering random character sequences.
- ▶ However, we're good at remembering meaningful phrases.
- ▶ Associative memory works much better than “random” memory.



Strong memorable passwords - **Solution**

- ▶ A quote from a movie.
- ▶ A line from a song.
- ▶ A proverb or idiom, etc., etc.
- ▶ IDEAL = Words from two languages

*Wilhelmus van Nassouwe. Ben ik van
Duitsen bloed*



Wilhelmus van Nassouwe. Ben ik van Duitsen bloed

Wilhelmus van **worstenbroodje**. Ben ik van Duitsen bloed

Wilhelmus van **worstenbroodje**. Ben ik van Duitsen bloed

WlhlmsvnrstnbrdjBnkvnDtsnbld

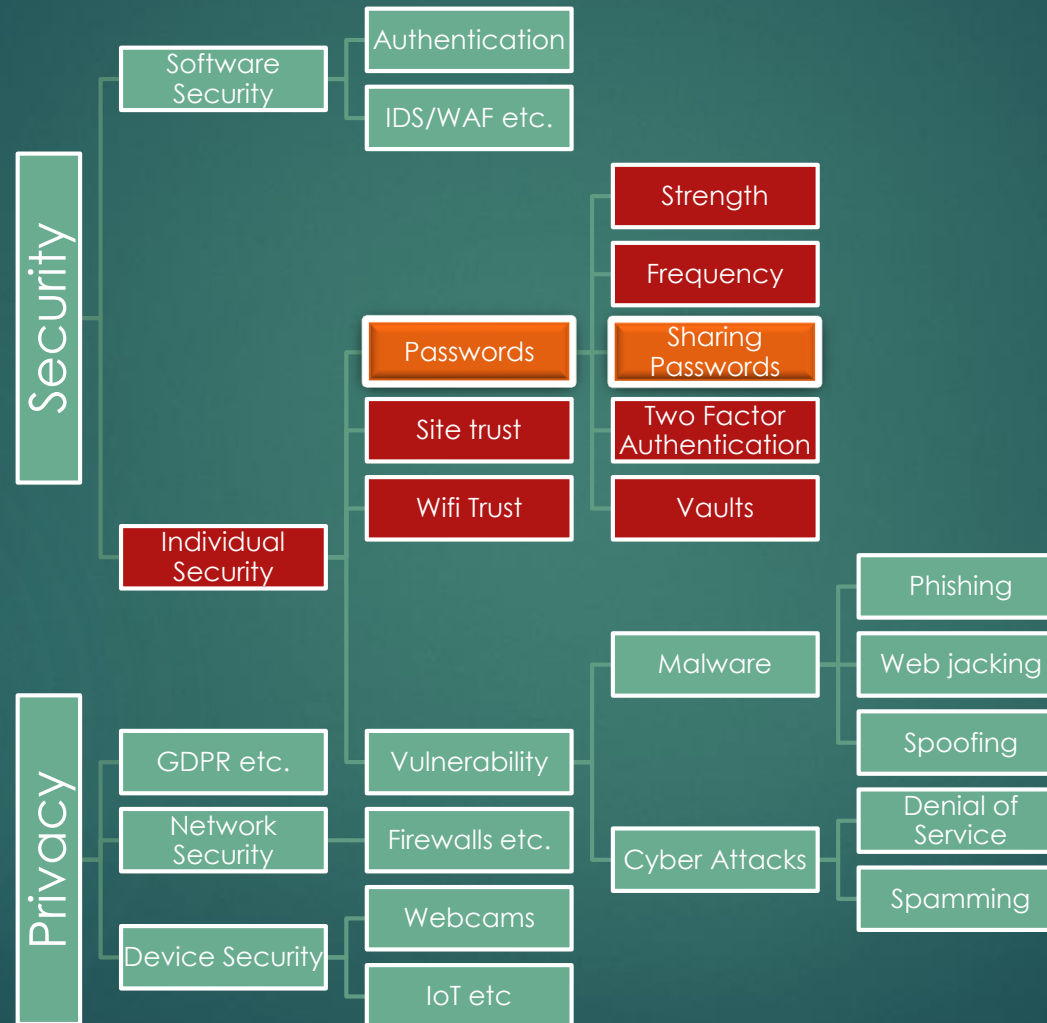
Wlhlmsvnrstnbrdj

W1hlmsvnr\$tnbrdj



SECURITY LANDSCAPE

Any questions?



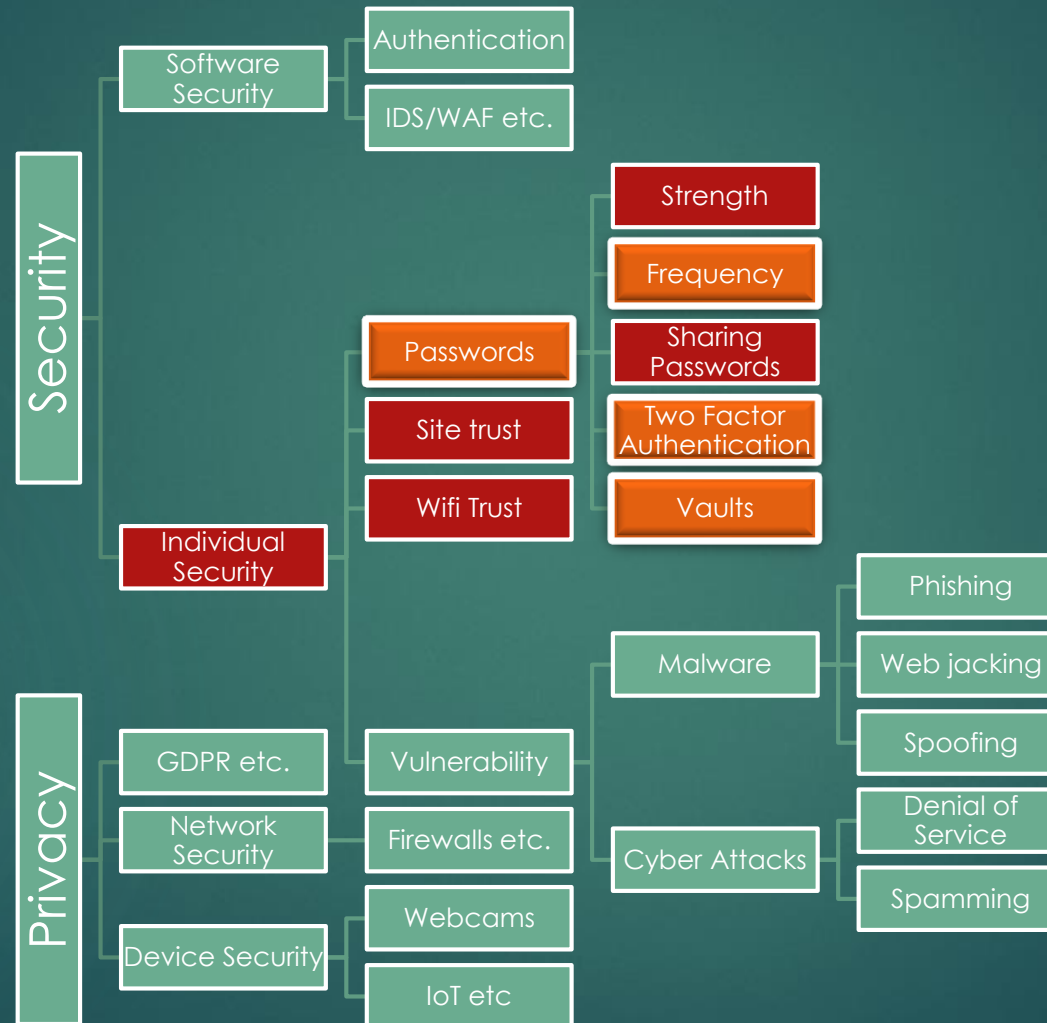
Sharing Passwords



- ▶ Self-destruct One time use messaging

<https://codebeautify.org/send-snap-message>

SECURITY LANDSCAPE



Use Password Managers

Say **NO** to

- Text files
- Emails to self
- Chat
- Etc.



Change Password Frequently

Best case: **Once a month**
Worst case: **Every **SIX** months**



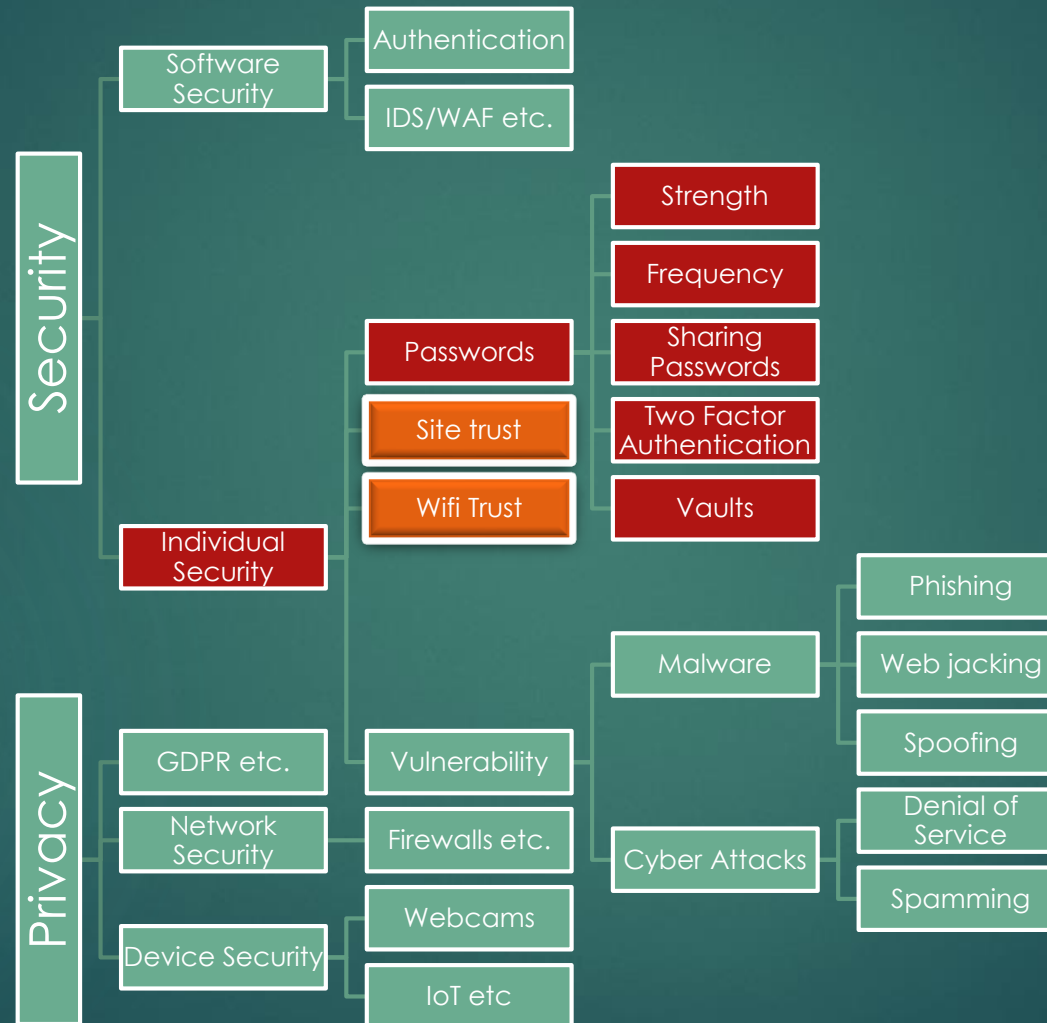
Use 2 Factor Authentication + Single Sign-on

1. Set your google account to use 2FA
2. Use Google Account as your Login Identity

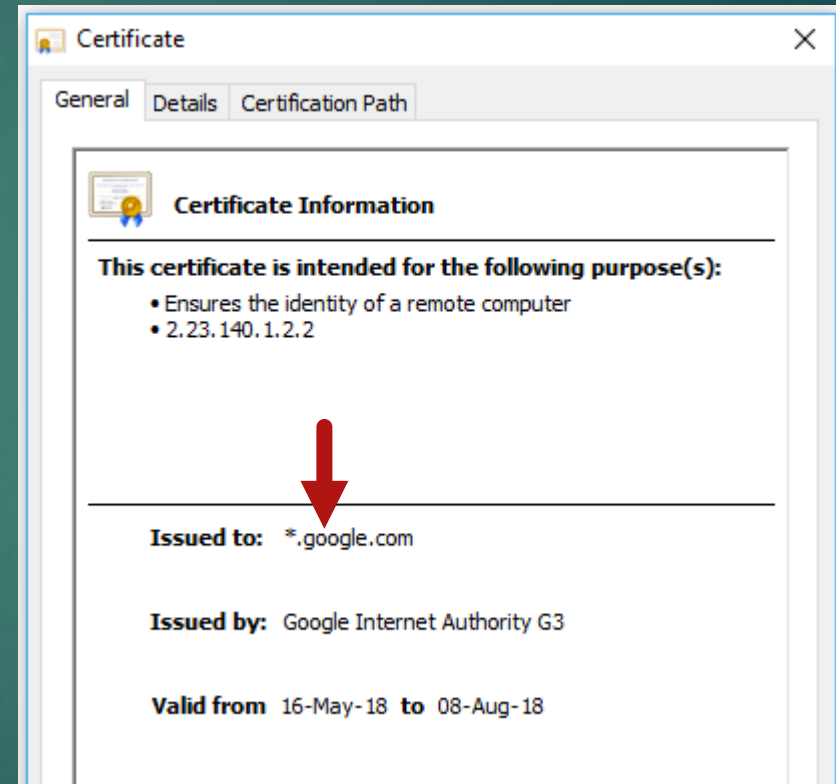
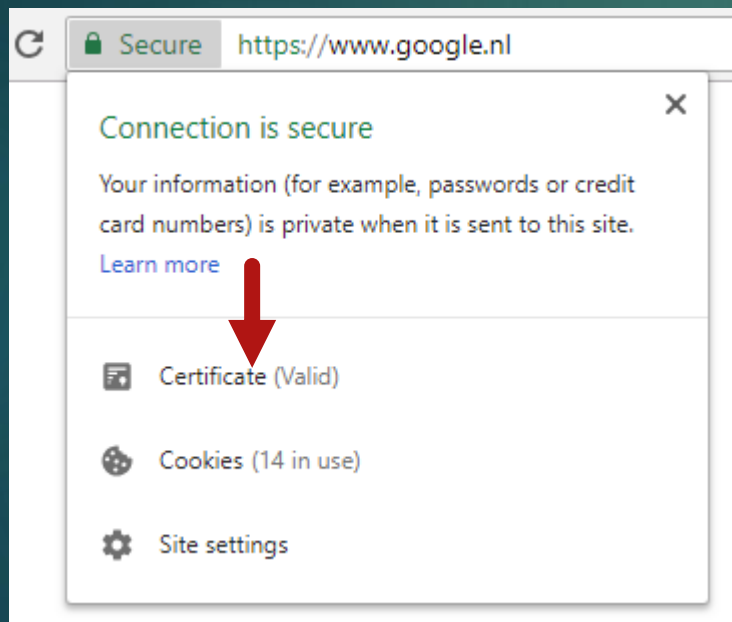


SECURITY LANDSCAPE

Any questions?



Trusting a site



Trusting a Public WiFi



Sorry.
you CANNOT trust a public WiFi

So please stay away!

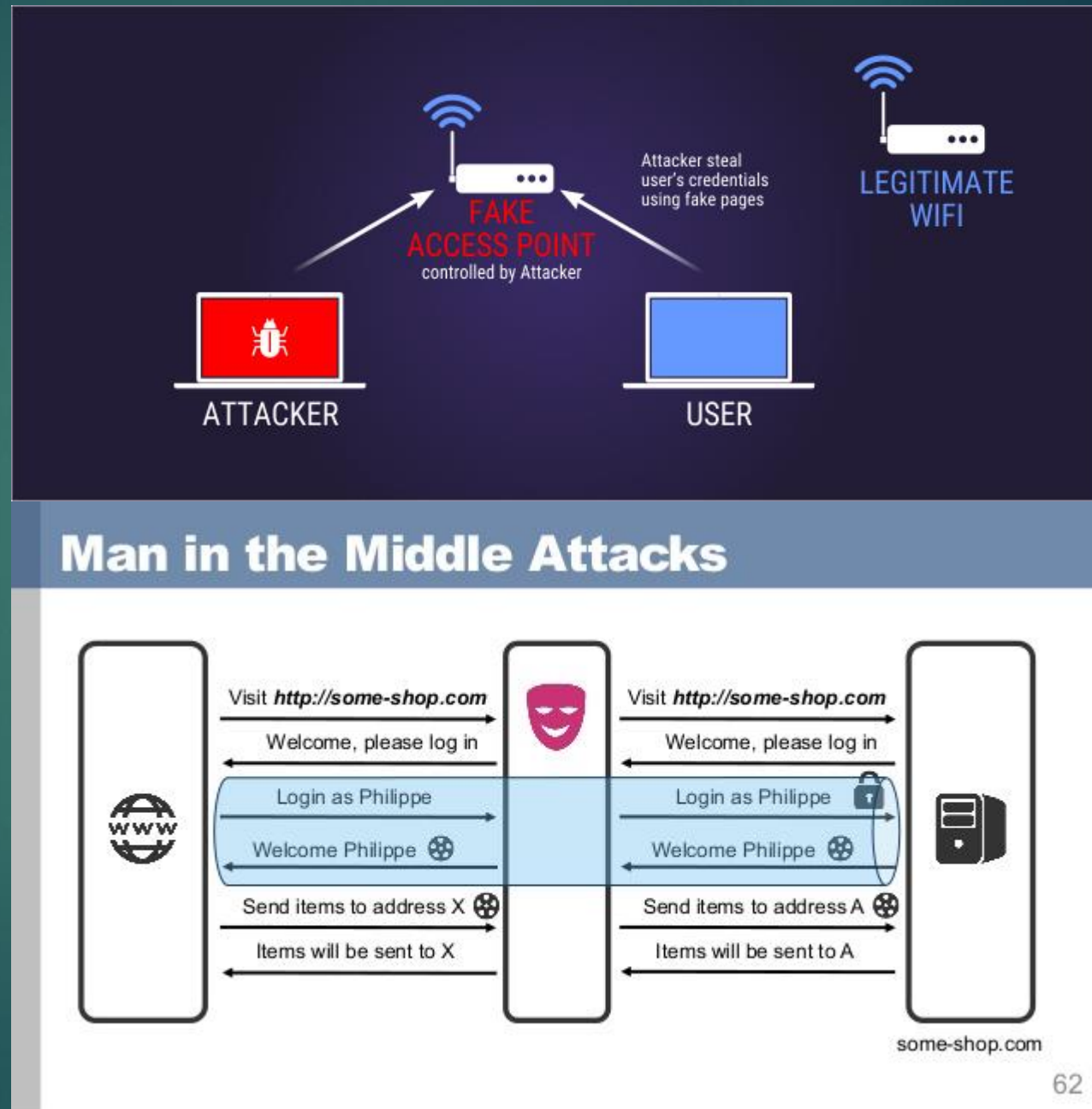
Man in the Middle Attack (MiTM)

Complete Manipulation of Data Packets

- Monitoring
- Eavesdropping
- Altering
- Discarding

If Public Wifis are Unavoidable

- Use a secure VPN

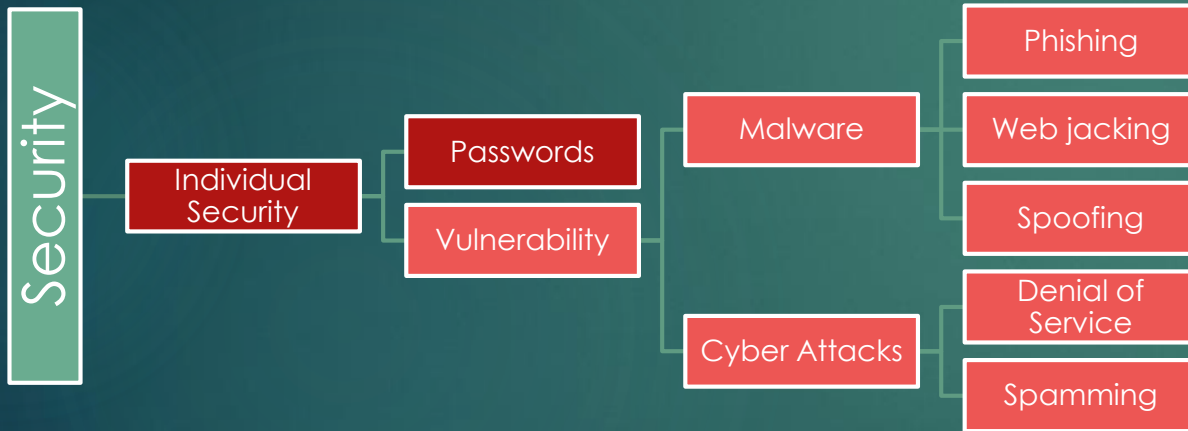


Dedicated Devices to prevent MiTM attacks

- Keezel
- Cujo
- Dojo
- etc.



Vulnerability – 3 Victims



Berry



Shoaeb



Sven

Interested in a tech-talk about vulnerability?



Helpful Resources



- ▶ <https://haveibeenpwned.com/>
- ▶ <https://howsecureismypassword.net/>
- ▶ <https://codebeautify.org/send-snap-message>
- ▶ <https://www.lastpass.com/>
- ▶ <https://1password.com>
- ▶ <https://www.dashlane.com/>
- ▶ <https://eu.keezeel.co/>
- ▶ <https://vimeo.com/154958732>
(Presentation by the author of Have I been Pwned)



SOFTWARE SERVICES

About e2e Group

- ▶ International Software Company (Rotterdam, Lahore, San Francisco)
- ▶ Software Venturing, Incubation, Technology Consultancy
- ▶ Achieving the right architectural mix of Open Source and Commercial technology for the enterprises
 - ▶ Scalability, Security, Sustainability
- ▶ Smooth journey from MVP to full-scale enterprise systems

Thank You & Questions

<https://e2egoc.com>

Aqeel Ahmad

Download this presentation

<https://e2egoc.com/individual-security/>