

REAL WORLD SITUATION (Phishing Attack)



DISCLAIMER / AMARAN

- GODAM TANPA KEBENARAN ADALAH JENAYAH!
- PRESENTER TIDAK SESEKALI AKAN MENUNJUKKAN STEP 'GODAM'
- SEMUA 'CONTENT' YANG DIPAPARKAN HANYALAH UNTUK PENCEGAHAN DAN 'EDUCATIONAL PURPOSES ONLY'!



Apakah itu Phishing?

Phishing adalah satu kaedah yang hacker gunakan sebagai teknik 'social engineering' untuk menipu mangsa melalui pelbagai platform seperti email, pautan url palsu, dan lain-lain.

Macam mana ia terjadi?

Hacker akan menghantar satu 'phishing link' yang akan membawa mangsa ke satu laman web. Laman web tersebut telah dikawal oleh 'hacker' untuk menyerang mangsa dengan cara memaksa mangsa untuk memasukkan sebarang data peribadi atau memuat turun sebarang aplikasi 'suspicious' untuk 'hacker' menanam 'backdoor' di peranti mangsa. Penyerang iaitu 'hacker' juga dapat mengakses sistem mangsa seperti kamera dan mikrofon melalui link yang di tekan oleh mangsa melalui beberapa kaedah dan alatan.



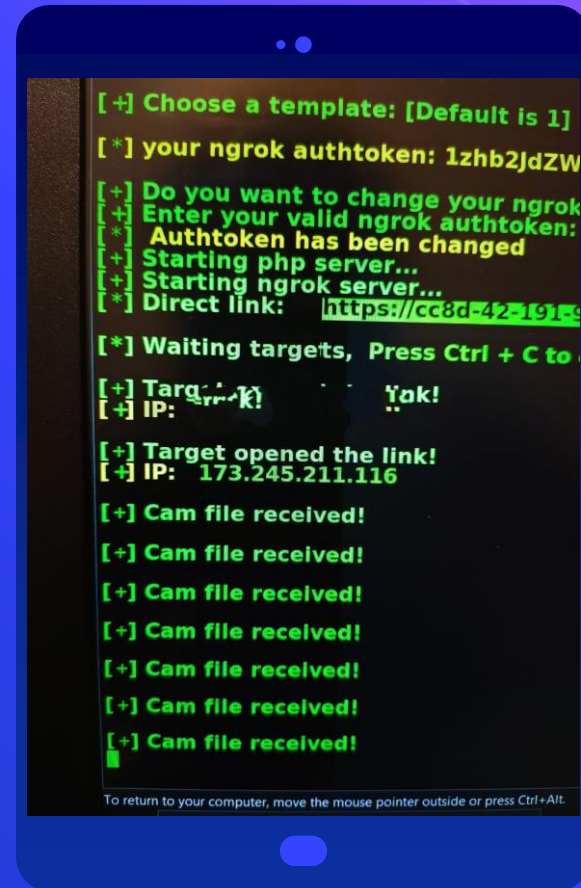
PERSOALAN

Dengan hanya menekan link, “**Hacker**”
dapat detect ‘IP Address’ & ‘Device
Camera’?

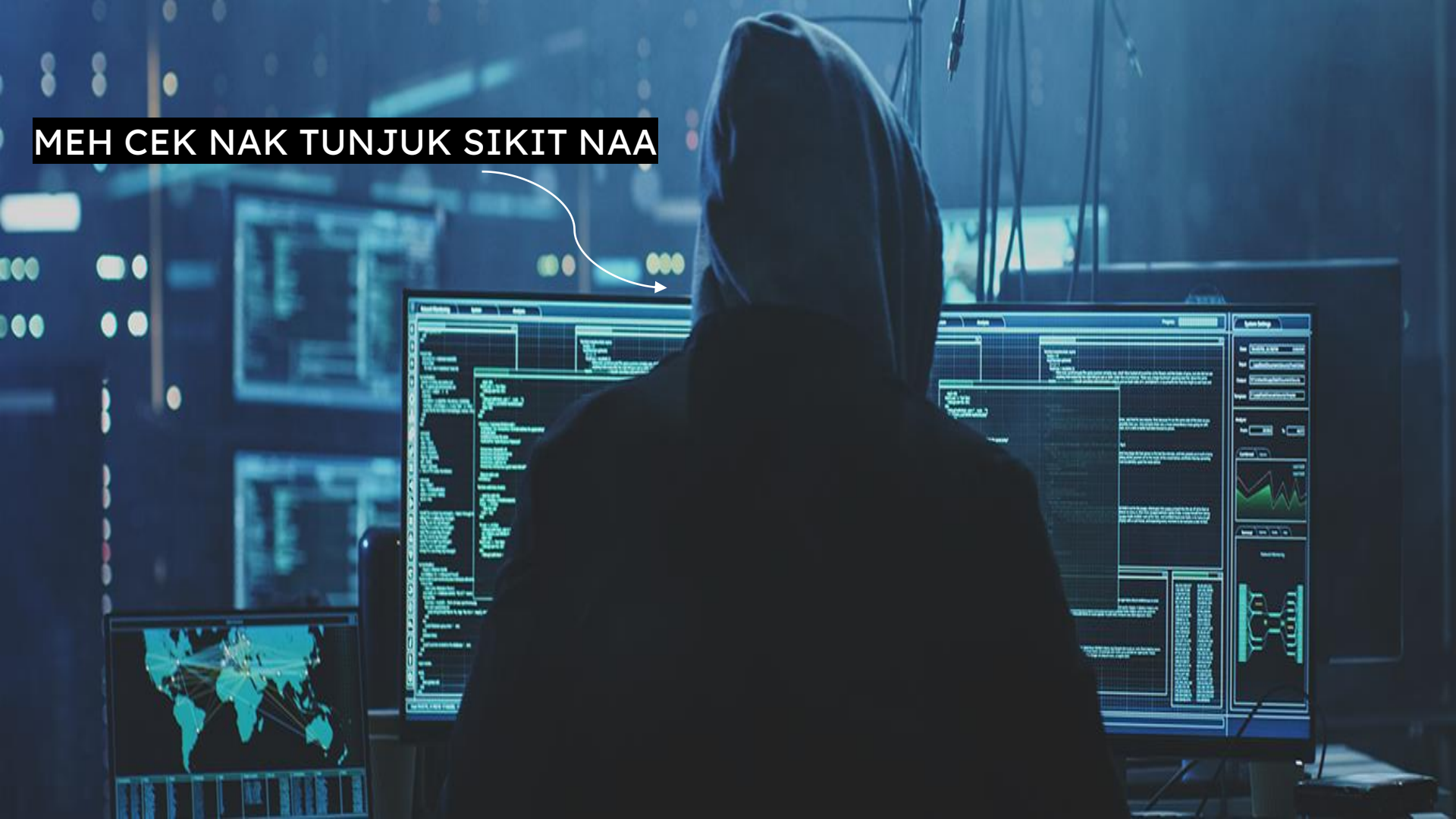
SERIOUS LA?!



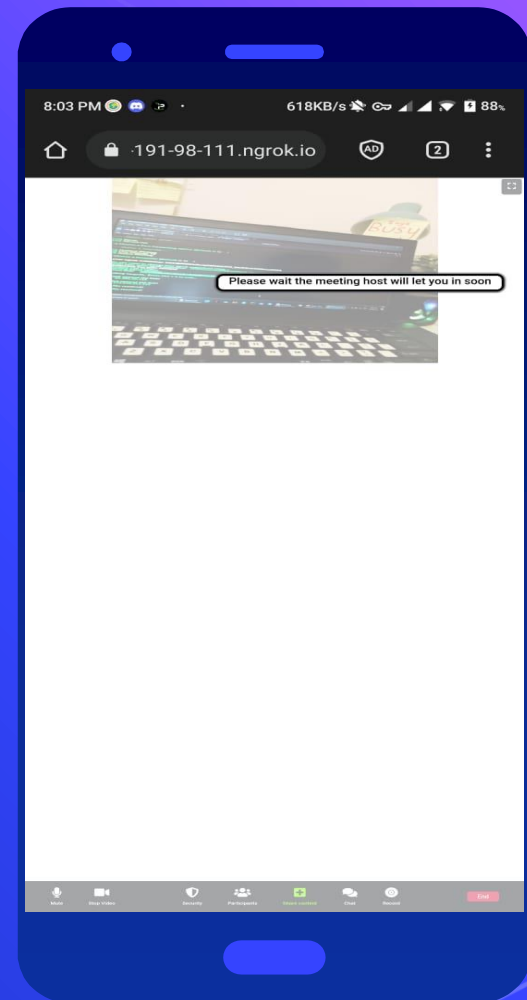
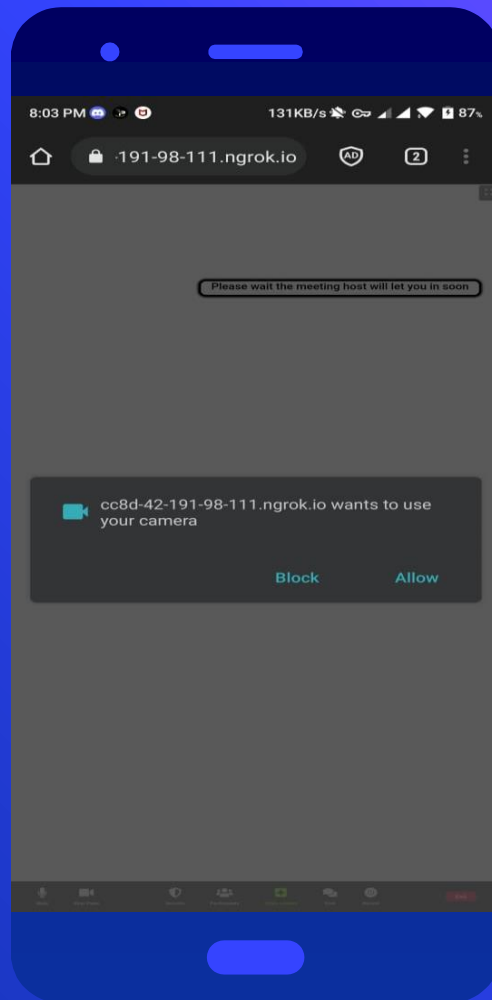
Contoh bagi paparan skrin device “Hacker”



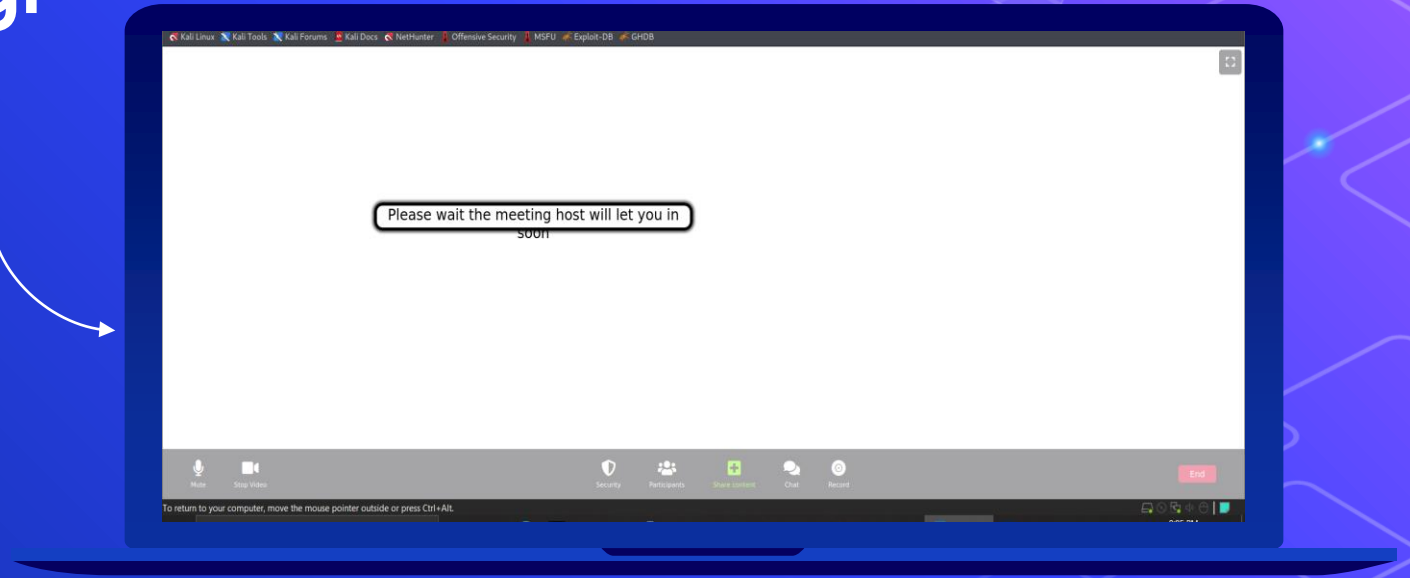
MEH CEK NAK TUNJUK SIKIT NAA



-Selepas tekan link tersebut, website akan mintak kebenaran untuk guna kamera.



Contoh bagi Laptop



Langkah Pencegahan!!

- Pakai VPN setiap kali nak masuk ke mana-mana website @ guna internet 'Public Wifi'.
- Tidak menekan link yang sembarangan 'suspicious link'.
- Security di Browser 'diketatkan' seperti slide yang seterusnya. Aktifkan 'standard protection' atau 'enhanced protection' untuk kawalan yang ketat.





Settings

Search settings

You and Google

Autofill

Privacy and security

Appearance

Search engine

Default browser

On startup

Advanced

Extensions 

About Chrome

Safe Browsing

Enhanced protection

- ☐ Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.



Standard protection

- ☒ Standard protection against websites, downloads, and extensions that are known to be dangerous



Detects and warns you about dangerous events when they happen



Checks URLs with a list of unsafe sites stored in Chrome. If a site tries to steal your password, or when you download a harmful file, Chrome may also send URLs, including bits of page content, to Safe Browsing.

Help improve security on the web for everyone

Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.



Warn you if passwords are exposed in a data breach

Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.



No protection (not recommended)

- ☐ Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.