BAB IV
HASIL DAN PEMBAHASAN

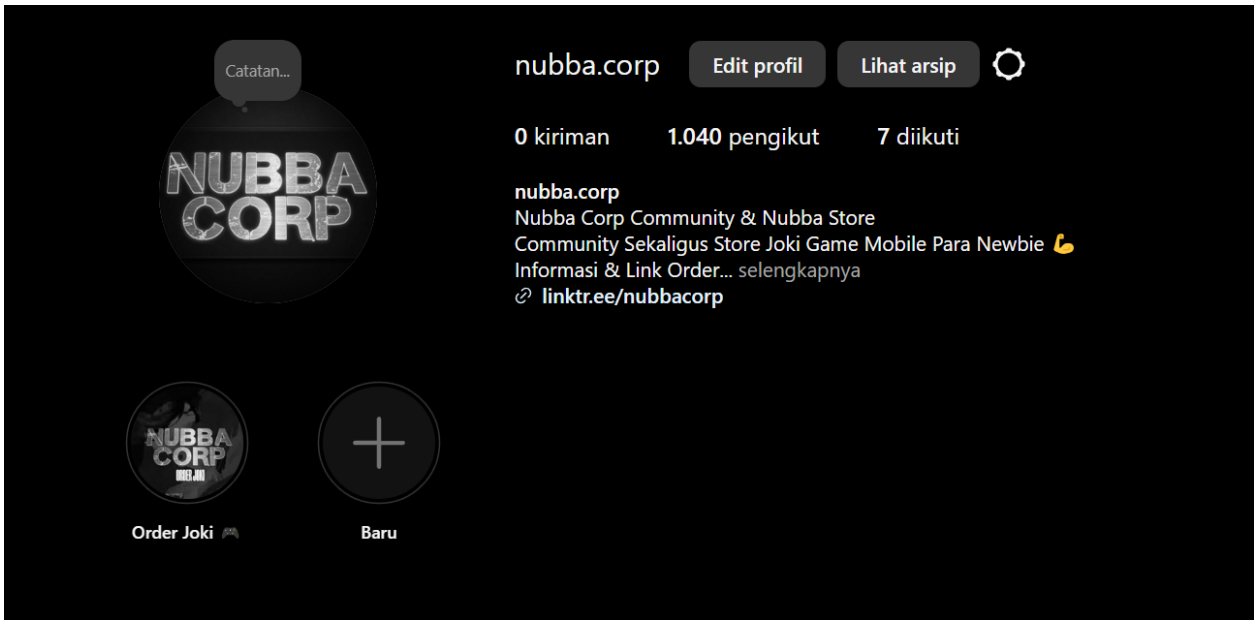
4.1 Pengujian Pretexting

Pengujian pertama yang dilakukan penguji menggunakan *social engineering* dengan pendekatan teknik social berupa *pretexting* yang menargetkan *player* PUBG Mobile dan Mobile Legends, tahapan pengujiannya adalah :

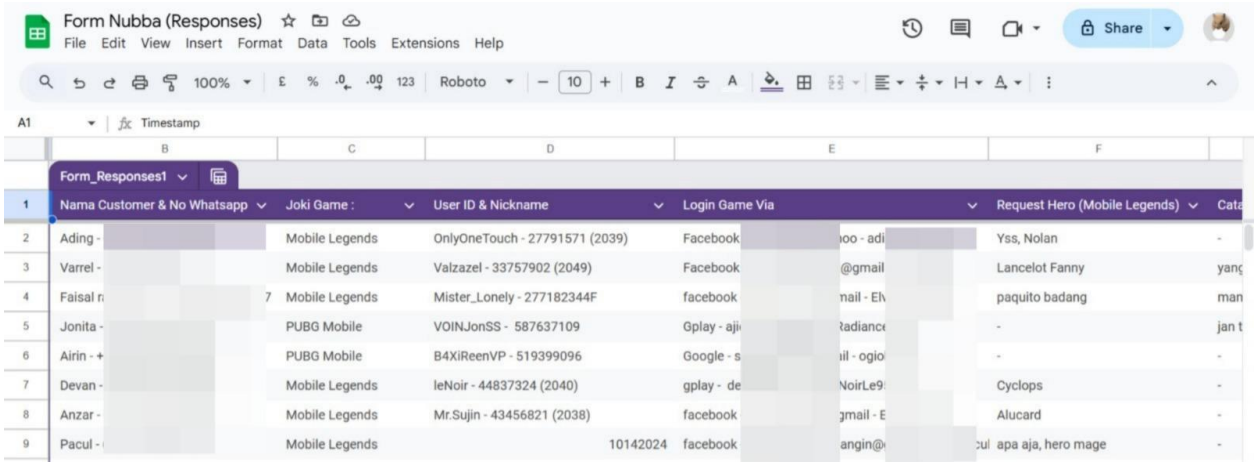
penguji pertama-tama akan membeli sebuah akun instagram sebagai store joki *game* PUBG Mobile dan Mobile Legends lalu mengubah namanya menjadi Nubba.Corp seperti pada gambar 4.1. Nama nubba.corp ini diambil karena merupakan salah satu komunitas *game* yang sangat aktif dengan anggota yang kurang lebih berjumlah 300 orang sehingga akan memudahkan penguji melakukan pengujian dengan berpura-pura menjadi salah satu pengurus komunitasnya. Alasan lainnya karena kebanyakan *player* akan lebih tertarik untuk bergabung ke sebuah komunitas tertentu dan memercayai orang-orang di dalamnya.

Setelah akun instagram selesai dibuat, penguji membuat google form yang harus diisi oleh target untuk menggunakan jasa joki store. Isi dari google form itu salah satunya akan meminta target untuk memberikan informasi pribadi berupa alamat email (bisa untuk akun media sosial seperti facebook, twitter ataupun tiktok) dan password dari alamat email tersebut untuk di *login* oleh penjoki(peneliti). Sample yang terkumpul akan masuk ke dalam google sheets untuk diuji oleh penguji seperti pada gambar 4.2.

Setelah google form selesai dibuat, pengujiakan menambahkan beberapa detail ke instagram Nubba.Corp seperti post tata cara untuk order joki, testimoni palsu para customer yang sudah memakai jasa store joki serta beberapa atribut lain agar akun instagram terlihat seperti sudah lama beroperasi untuk meyakinkan target.

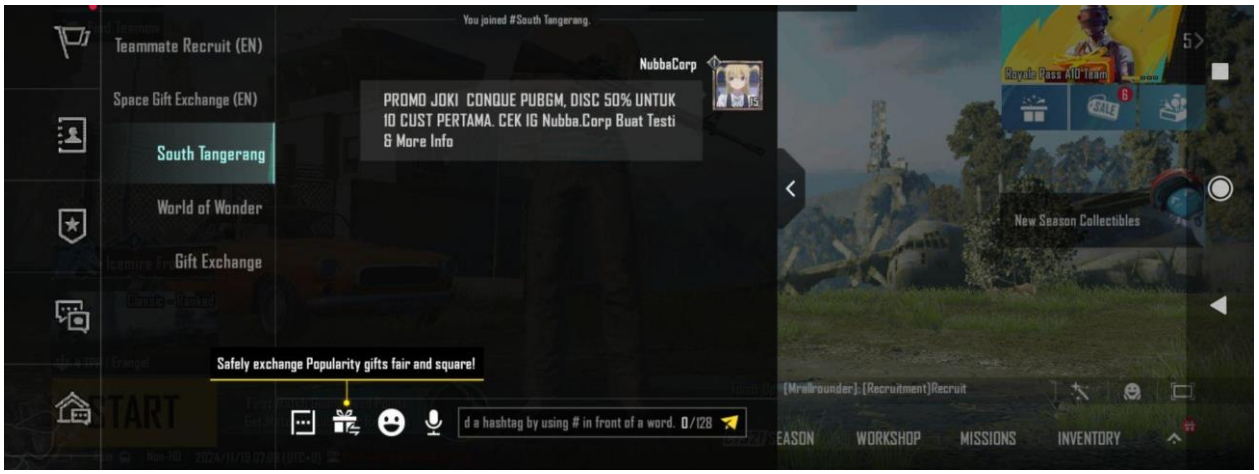


Gambar 4.1 Instagram Nubba.Corp

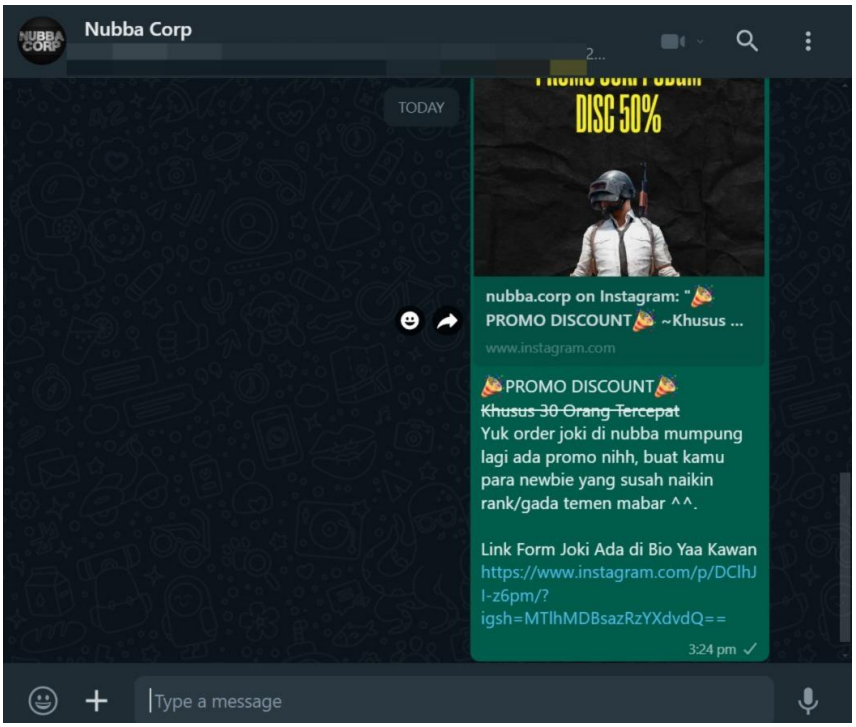


Gambar 4.2 Sample Google Form Order Joki

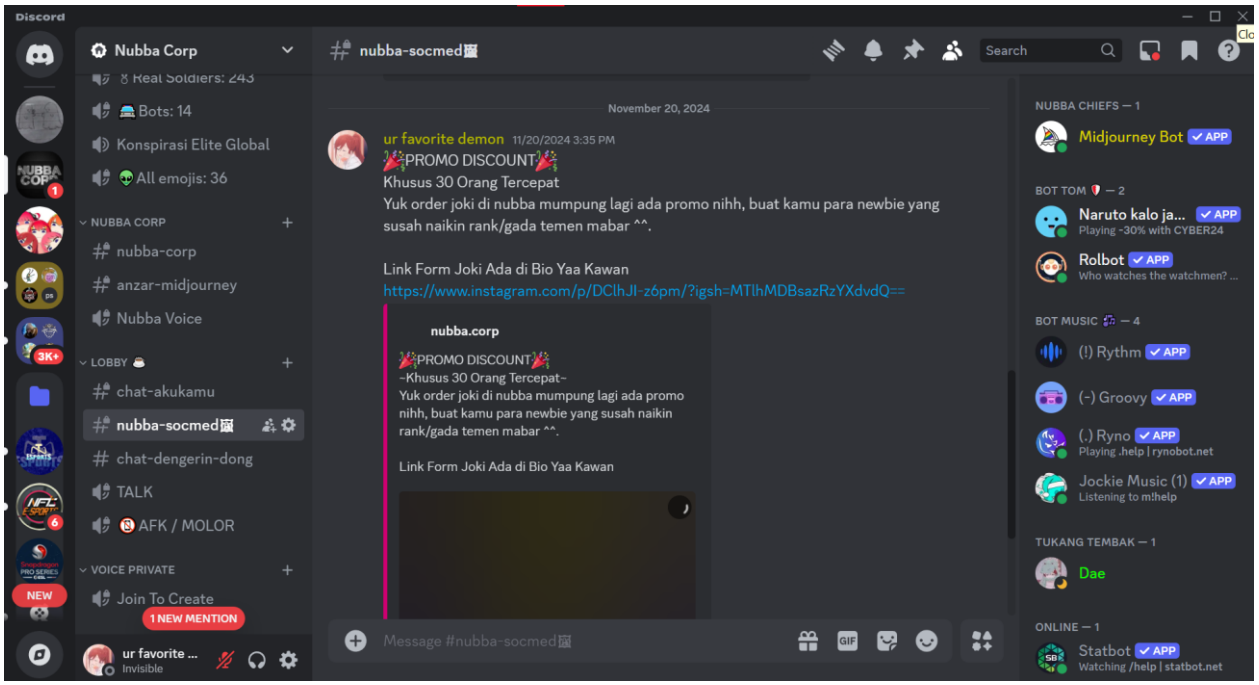
Setelah persiapan selesai, pengujiakan melakukan pengujian. Pertama- tama pengujiakan mempromosikan store melalui whatsapp, telegram, discord dan juga melakukan promosi melalui chat in-*game* masing-masing *game* yang diuj seperti pada gambar 4.3. pengujijuga akan melakukan promosi ke komunitas *game* dalam gambar 4.4 dan 4.5 tersebut untuk mendapatkan lebih banyak data yang bisa diuji.



Gambar 4.3 Promosi store di in-*game* PUBGM



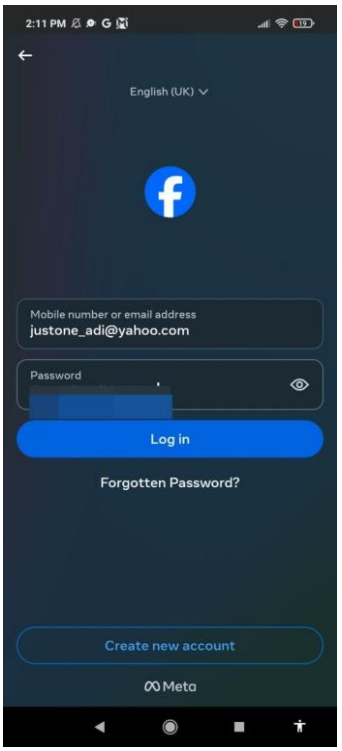
Gambar 3.4 Promosi store di grup komunitas



Gambar 4.5 Promosi store di discord komunitas

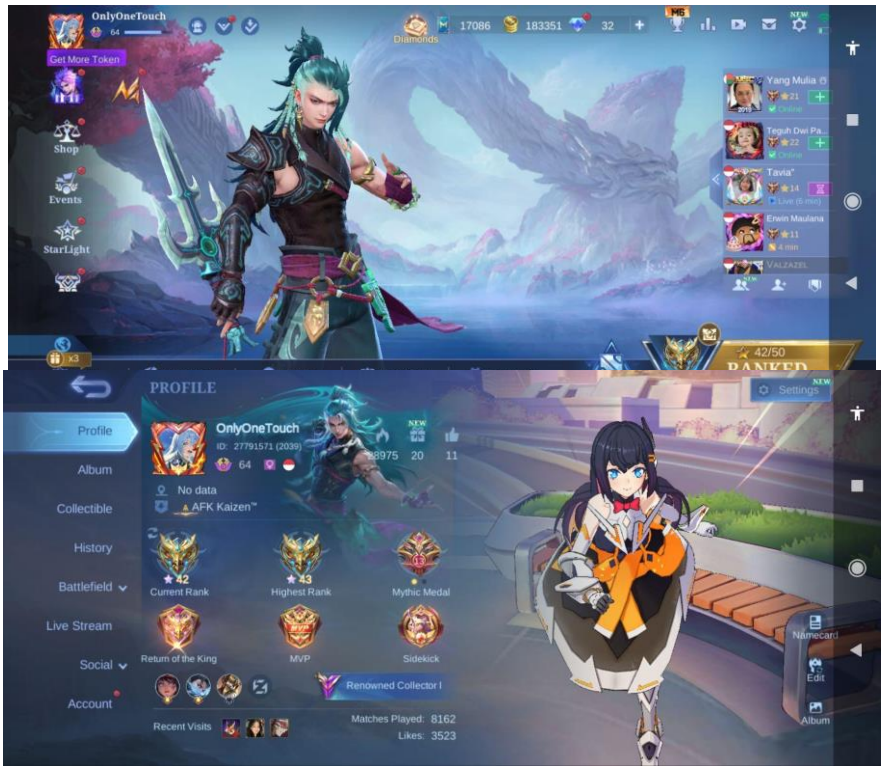
Penyerangan ini dilakukan dalam rentang waktu 24 jam, dimana setelah 24 jam terkumpul sebanyak 41 sample data dari google form jokinya. Dari data yang telah terkumpul penguji lalu melanjutkan ketahap untuk masuk ke akun target yang telah mengisi form dan memberi email serta password mereka. Penguji akan melakukan *login* ke akun media sosial target terlebih dahulu lalu dilanjutkan dengan *login* ke akun *game* target, dilakukan dengan *game* Mobile Legends terlebih dahulu lalu dilanjutkan ke *game* PUBGM.

Penguji dalam gambar 4.6 melakukan pengujian masuk ke akun target yang mengorder jasa joki untuk *game* mobile legends, disini target menuliskan akses *login* mobile legendnya melalui akun media sosial facebook. Pada gambar 4.7 penguji berhasil mengakses akun media sosial target, setelah behrasil masuk penguji melakukan *login* ke akun *game* mobile legend milik target dan berhasil masuk juga seperti pada gambar 4.8.



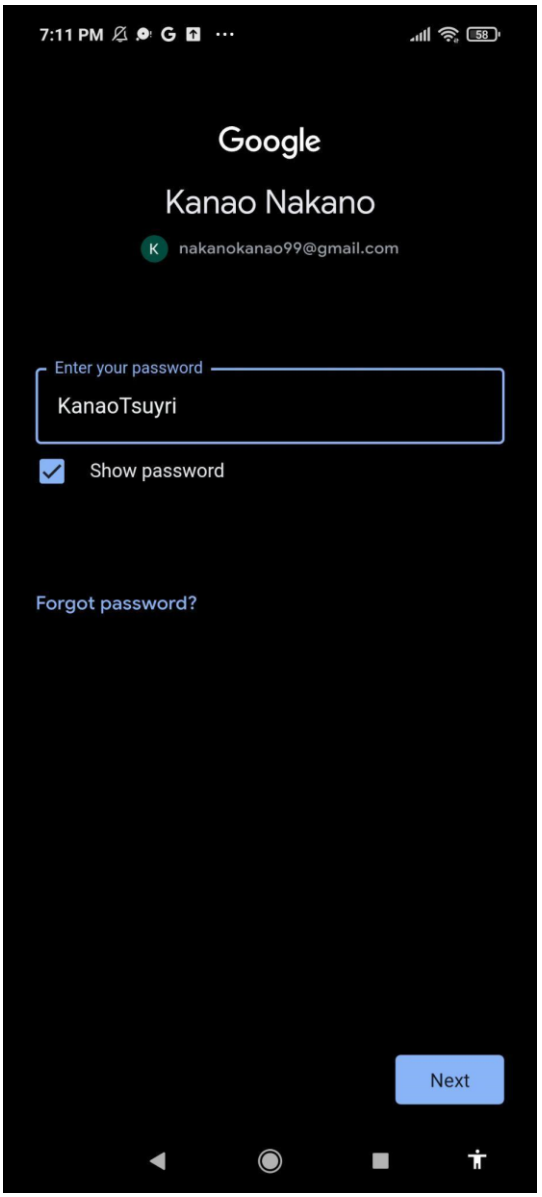
Gambar 4.6 Login ke akun media sosial target

Gambar 4.7 Berhasil *login* ke akun target.

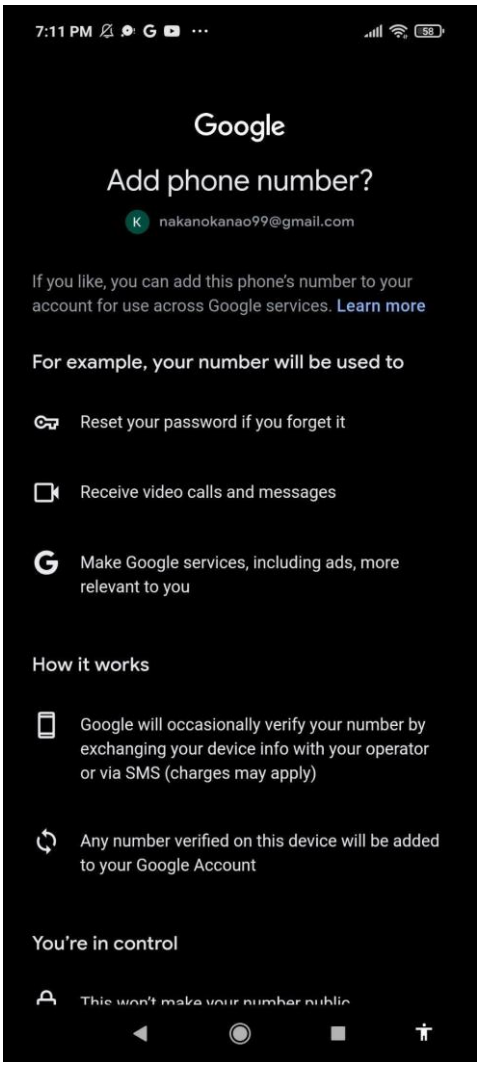


Gambar 4.8 Berhasil *login* ke akun *game* target.

Pengujian yang kedua dilakukan kembali kepada target yang memesan jasa joki *game* PUBG Mobile dengan akses *login* yang berbeda yaitu lewat email secara langsung. Pada gambar 4.9 penguji melakukan *login* sesuai dengan data yang telah di input lewat google form dan berhasil masuk pada gambar 4.10.

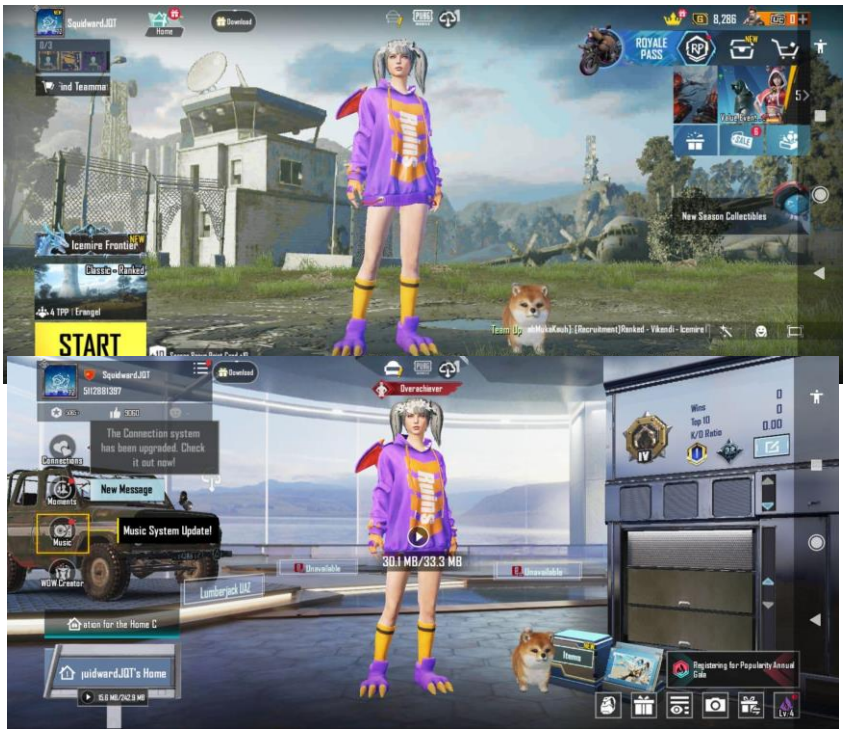


Gambar 4.9 Login ke akun Email target



Gambar 4.10 Berhasil *login* ke akun email target

Setelah berhasil mengakses akun email, penguji melakukan *login* ke dalam *game* PUBG Mobile menggunakan opsi *login* lewat google play dan berhasil masuk ke akun target pada gambar 4.11.



Gambar 4.11 Berhasil *login* ke akun *game* target.

4.2 Pengujian Impersonation

Pengujian kedua yang dilakukan penguji menggunakan *social engineering* dengan pendekatan teknik social berupa *pretexting* yang menargetkan *player* PUBG Mobile dan Mobile Legends, tahapan pengujiannya adalah :

penguji pertama-tama akan kembali memakai akun instagram Nubba.Corp dan membuat post dengan tujuan mencari worker/*player* untuk melakukan joki pada *game* PUBG Mobile dan Mobile Legends seperti pada gambar 4.12.

penguji lalu akan kembali membuat google form yang harus diisi oleh target untuk mendaftar sebagai worker sekaligus untuk memberikan informasi pribadi berupa alamat email (bisa untuk akun media sosial seperti facebook, twitter ataupun tiktok) dan password dari alamat email tersebut untuk di *login* oleh penjoki(peneliti). Sample yang terkumpul akan masuk ke dalam google sheets untuk diuji oleh penguji seperti pada gambar.

Setelah google form selesai dibuat, penguji juga akan melakukan scouting/stalking kepada beberapa target/*player* di discord, whatsapp, instagram, tiktok dan in-*game* untuk memperluas opsi sample data yang di dapat.

Gambar 4.12 Post Mencari Worker.

Nama & No Whatsapp	Worker Game :	User ID & Nickname	Login Game Via	Usia	Pendidikan Terakhir
Adr 081316401	Mobile Legends	Buzz - 21938540(2039)	Email - Jul	19–24	SMA
Akb 39940	Mobile Legends	RoCCinate - 21938450(1920)	Facebook at66	19–24	SMA
raul 3	Mobile Legends	[AFK] - Reaper 0 21838499(0293)	Email - ysu	19–24	S1
Ang 778	Mobile Legends	Shiki 两儀 23828326 (2039)	Facebook 95	19–24	S1
fath 31	Mobile Legends	Chans7Z - 23741993(1290)	Twitter - M 3	19–24	SMA
ama	Mobile Legends	MGWxMRCL - 21030150(2391)	Email - and ngguh	19–24	SMA
has	Mobile Legends	ELCRUZ - 08123744(9012)	Facebook 9876	19–24	S1
fred	Mobile Legends	Keciiiii 22903147(9912)	Email - Hu	19–24	S1
abd	Mobile Legends	PUFF2C 23881039(1203)	Twitter - sy 1	19–24	SMP
ima	Mobile Legends	ChoppeRR - 20183347(0012)	Email - nov ant11	19–24	S1
Ray 201	Mobile Legends	Rayhan Del Rey - 22934012(1056)	Email - aiic 991	19–24	S1

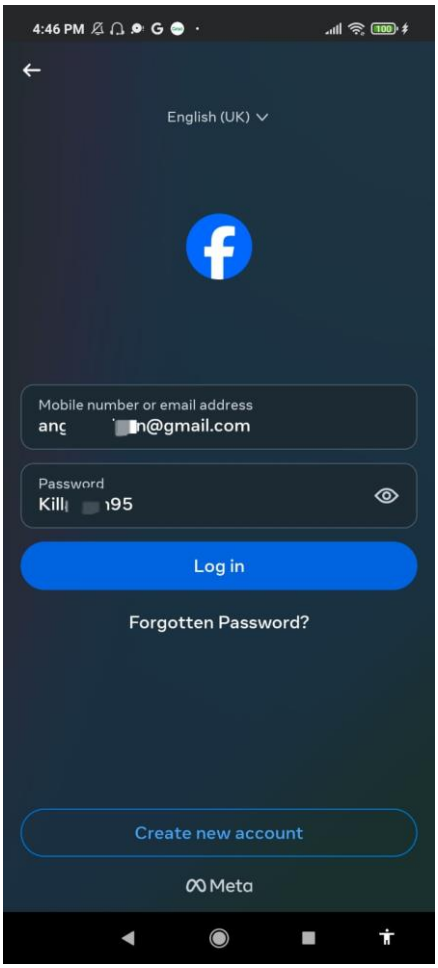
Gambar 4.13 Sample Google Form Worker

Setelah persiapan selesai, pengujian melakukan pengujian. Pertama- tama penguji akanmelakukan post mencari worker dan mengupload story di instagram

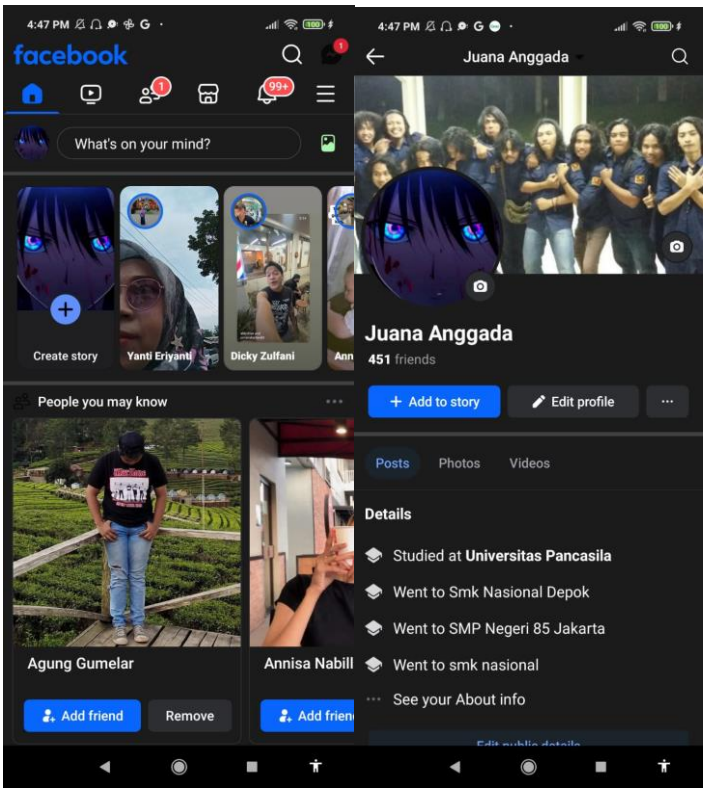
seperti pada gambar 4.12 tadi. Setelah itu penguji mengirimkan dm ke beberapa target potensial yang tertarik untuk menjadi penjoki di *game* PUBG Mobile dan Mobile Legends.

Penyerangan ini dilakukan dalam rentang waktu 24 jam, dimana setelah 24 jam terkumpul sebanyak 42 sample data dari google form jokinya. Dari data yang telah terkumpul penguji lalu melanjutkan ke tahap untuk masuk ke akun target yang telah mengisi form dan memberi email serta password mereka. Penguji akan melakukan *login* ke akun media sosial target terlebih dahulu lalu dilanjutkan dengan *login* ke akun *game* target, dilakukan dengan *game* Mobile Legends terlebih dahulu lalu dilanjutkan ke *game* PUBGM.

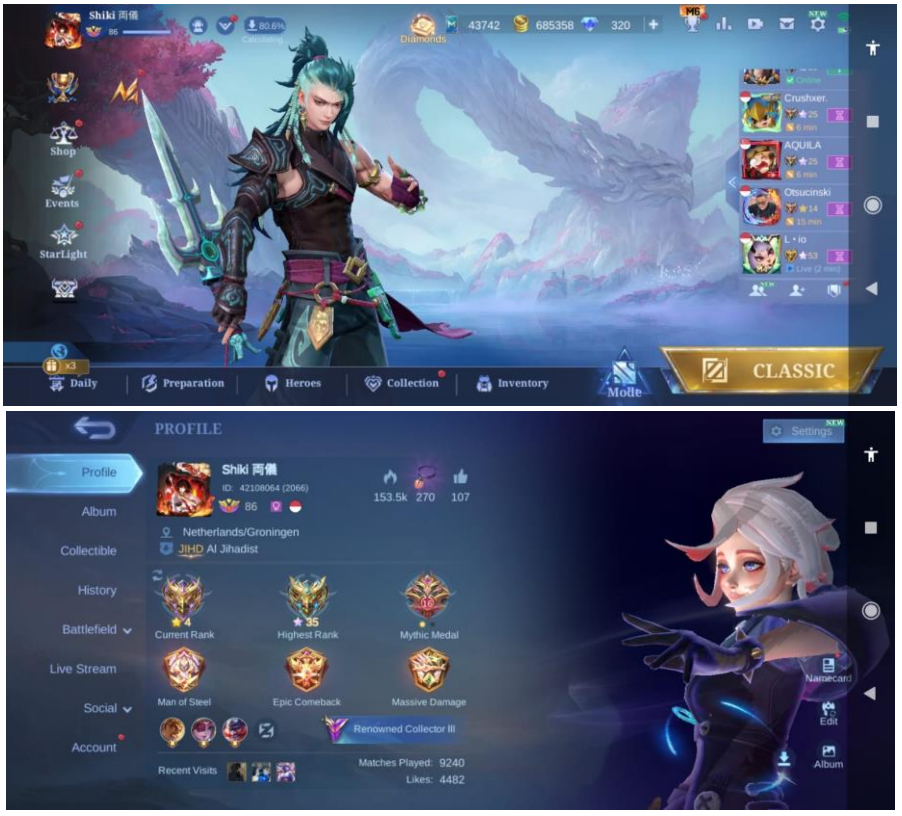
Penguji dalam gambar 4.14 melakukan pengujian masuk ke akun target yang mendaftar menjadi worker untuk *game* mobile legends, disini target menuliskan akses *login* mobile legendnya melalui akun media sosial facebook. Pada gambar 4.15 penguji berhasil mengakses akun media sosial target, setelah berhasil masuk penguji melakukan *login* ke akun *game* mobile legend milik target dan berhasil masuk juga seperti pada gambar 4.16



Gambar 4.14 Melakukan Login ke Akun Target



Gambar 4.15 Berhasil Masuk ke Akun Media Sosial Target

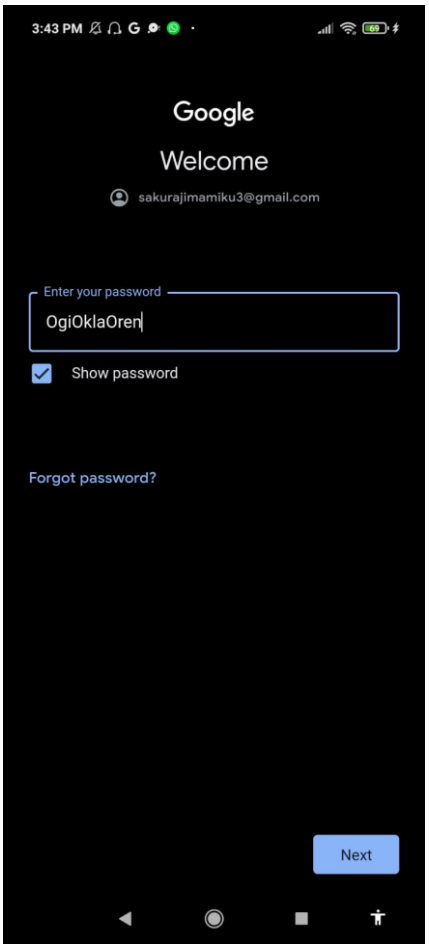


Gambar 4.16 Berhasil Masuk ke Akun Game Target

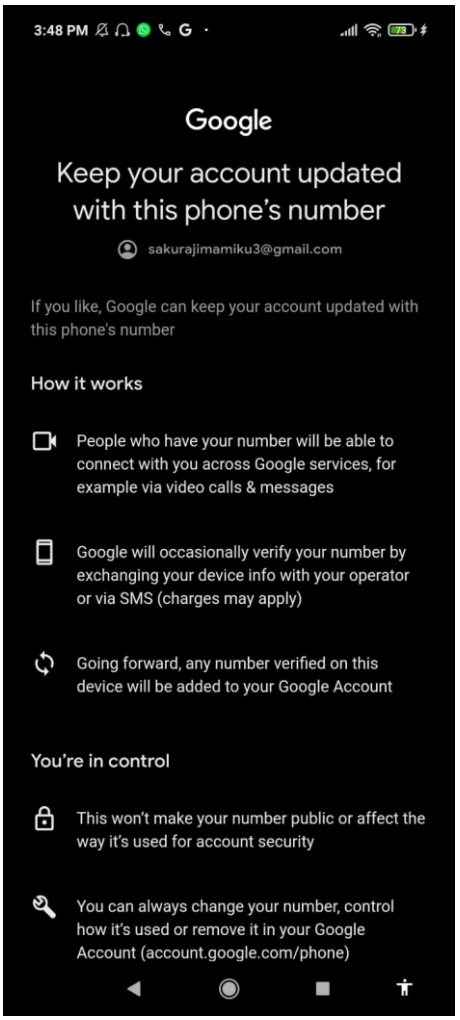
Setelah selesai melakukan pengujian di akun Mobile Legends, penguji hendak mencoba melakukan *login* ke *game* PUBG Mobile ke target berikutnya tapi mengalami misclick sehingga menyebabkan penguji melakukan *login* dengan akun facebook milik target pada gambar 4.15. Ternyata target juga memiliki akun PUBG Mobile yang tertaut dengan facebook miliknya pada gambar 4.17, ini membuat penguji mendapat 3 akun (media sosial facebook, akun Mobile Legends dan akun PUBG Mobile) dalam pengujian.

Gambar 4.17 Masuk ke Akun Target Sebelumnya Secara Tidak Sengaja

penguji melanjutkan kembali pengujian untuk target kedua yang mendaftar sebagai worker *game* PUBG Mobile dengan akses *login* yang berbeda yaitu lewat google play dan mengharuskan penguji melakukan *login* email secara langsung. Pada gambar 4.18 penguji melakukan *login* sesuai dengan data yang telah di input lewat google form dan berhasil masuk pada gambar 4.19

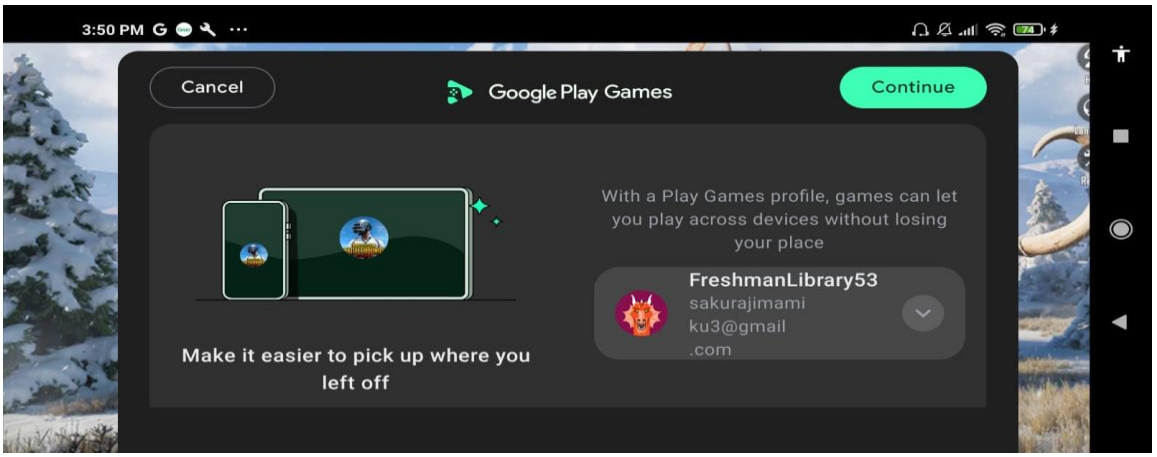


Gambar 4.18 Login ke akun Email target



Gambar 4.19 Berhasil *login* ke akun media sosial target

Setelah berhasil mengakses akun email, penguji melakukan *login* ke dalam *game* PUBG Mobile menggunakan opsi *login* lewat google play pada gambar 4.20 dan berhasil masuk ke akun target pada gambar 4.21.



Gambar 4.20 Login dengan google play

Gambar 4.21 Berhasil *login* ke akun *game* target.

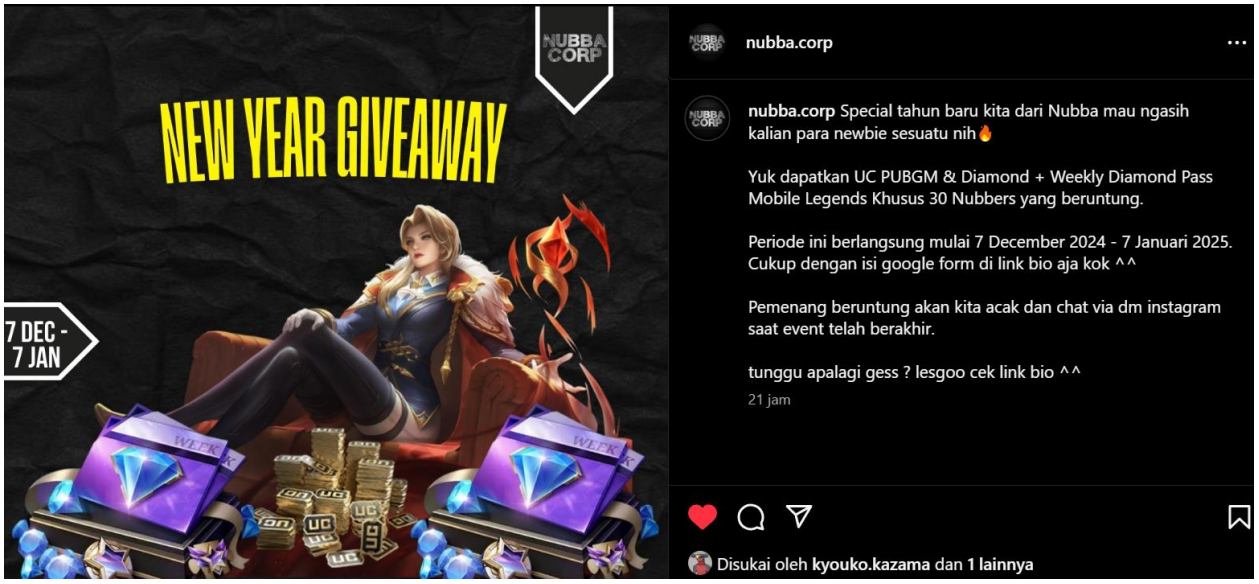
4.3 Pengujian Phishing

Pengujian ketiga yang dilakukan penguji menggunakan *social engineering* dengan pendekatan teknik social berupa *phishing* yang menargetkan *player* PUBG Mobile dan Mobile Legends, tahapan pengujiannya adalah :

penguji pertama-tama akan kembali memakai akun instagram Nubba.Corp dan membuat post dengan tujuan mengadakan giveaway berupa UC PUBG Mobile serta Diamonds & Weekly Pass Mobile Legends seperti pada gambar 4.22.

penguji lalu akan kembali membuat google form yang harus diisi oleh target untuk mengikuti giveaway dan memberikan informasi pribadi berupa alamat email (bisa untuk akun media sosial seperti facebook, twitter ataupun tiktok) dan password dari alamat email tersebut untuk di *login* oleh peneliti. Sample yang terkumpul akan masuk ke dalam google sheets untuk diuji oleh penguji seperti pada gambar 4.23.

Setelah google form selesai dibuat, penguji akan membagikan *post*ingan giveaway ini ke beberapa media sosial lain untuk kembali memperbanyak sample data yang dapat dikumpulkan.



Gambar 4.22 Post giveaway

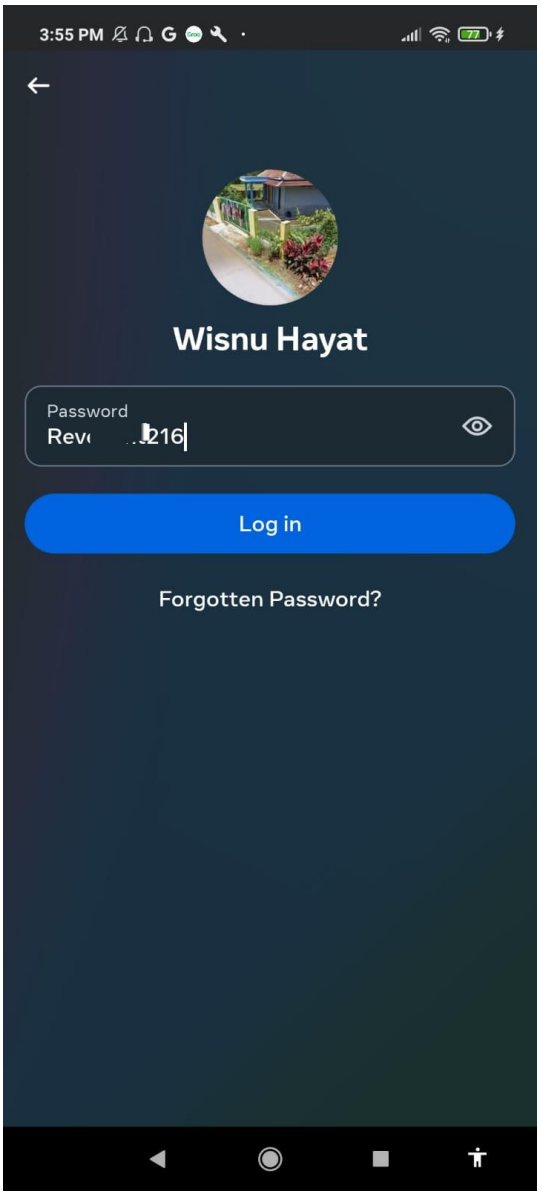
Nama & No Whatsapp	Usia	Give Away Game Apa	User ID & Nickname	Login Game Via
Wisnu Hayat - 0877224457	25–34	Mobile Legends	[illegible] 81423504 (2154)	faceb [illegible] t216
S [illegible]	34	Mobile Legends	MysticHunter & 47583920 (2031)	email
L [illegible]	5678-9	19–24	Mobile Legends	bayangan Wolf - 76491823 (1953)	Faceb [illegible] - indafirmansyah
E [illegible]	39	19–24	Mobile Legends	urfavdemon 38475196 (2947)	Gmail [illegible] hanif21
N [illegible]	234	19–24	Mobile Legends	hayabusasanzo, 85726349 (1820)	Faceb [illegible] rsyf98
E [illegible]	345	19–24	Mobile Legends	NightFury - 47281935 (2067)	Gmail [illegible] achan97
O [illegible]	0	19–24	Mobile Legends	AKU SIAPA 94175268 (1324)	Faceb [illegible] n123
A [illegible]	01	19–24	Mobile Legends	Hog Riderrrrrrrr & 62748395 (1498)	Gmail [illegible] 021
A [illegible]		19–24	Mobile Legends	StormBreaker, 35892741 (1854)	Faceb [illegible] afiqdaniel30
L [illegible]	1	19–24	Mobile Legends	MUGIWARAAAA - 62917548 (2002)	Gmail [illegible] ahcavi

Gambar 4.23 Sample Google Form Giveaway

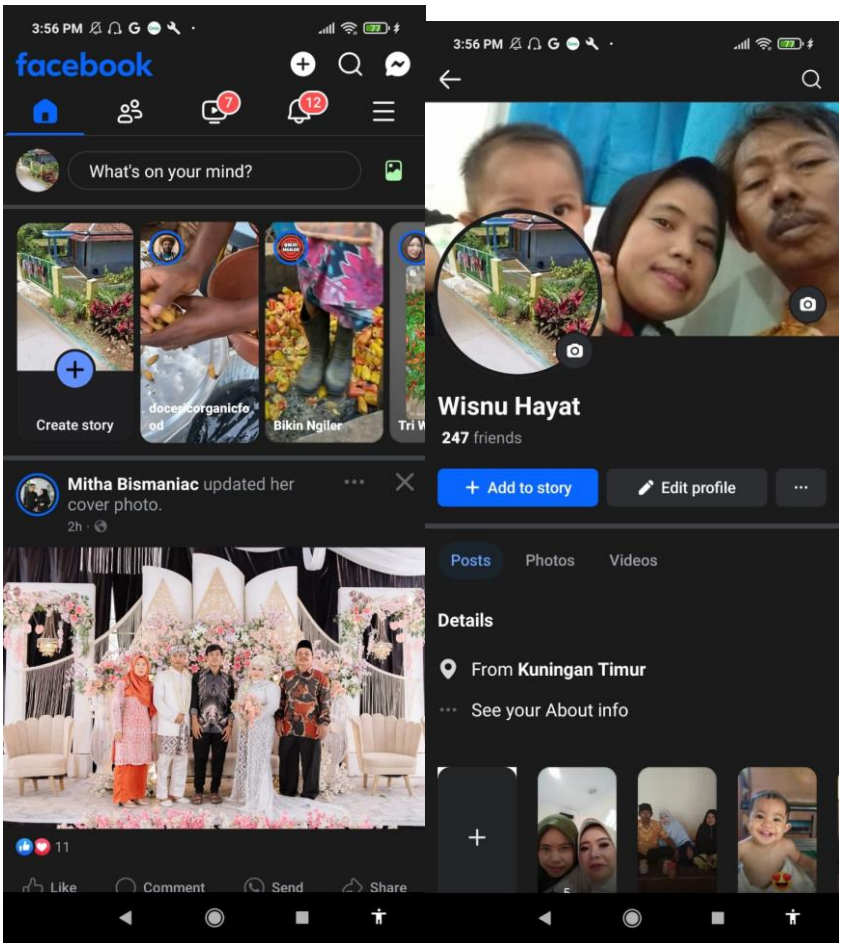
Setelah persiapan selesai, pengujiakan melakukan pengujian. Pertama- tama penguji akan melakukan *post* giveaway dan mengupload story di instagram seperti pada gambar 4.22.

Penyerangan ini dilakukan dalam rentang waktu 24 jam, dimana setelah 24 jam terkumpul sebanyak 41 sample data dari google form jokinya. Dari data yang telah terkumpul penguji lalu melanjutkan ke tahap untuk masuk ke akun target yang telah mengisi form dan memberi email serta password mereka. Penguji akan melakukan *login* ke akun media sosial target terlebih dahulu lalu dilanjutkan dengan *login* ke akun *game* target, dilakukan dengan *game* Mobile Legends terlebih dahulu lalu dilanjutkan ke *game* PUBGM.

Penguji dalam gambar 4.24 melakukan pengujian masuk ke akun target yang mendaftar giveaway untuk *game* mobile legends, disini target menuliskan akses *login* mobile legendnya melalui akun media sosial facebook tetapi tidak menyebutkan alamat emailnya dan hanya memberikan username serta nomor teleponnya. Pada gambar 4.25 penguji berhasil mengakses akun media sosial target.

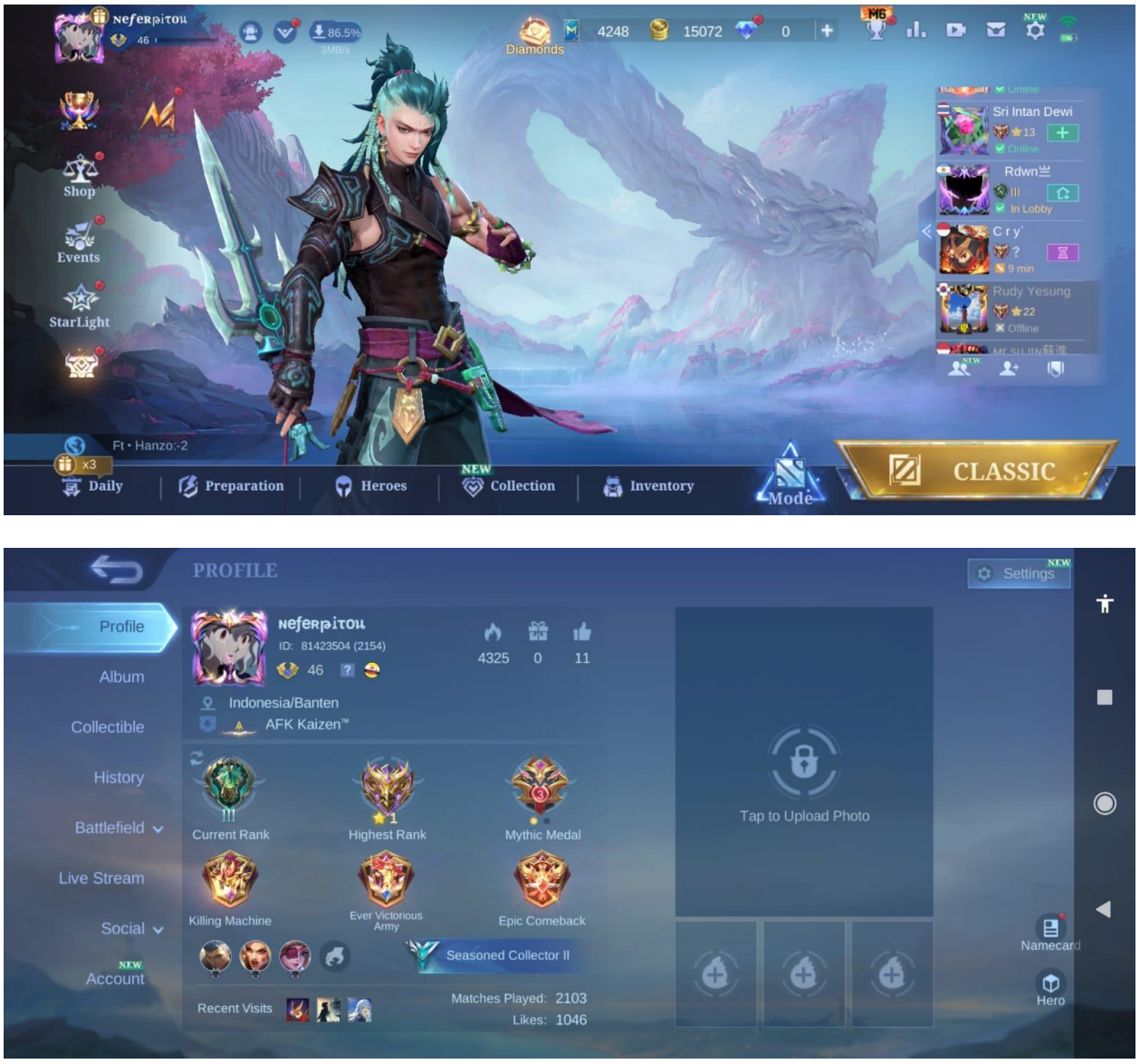


Gambar 4.24 Login ke akun media sosial target



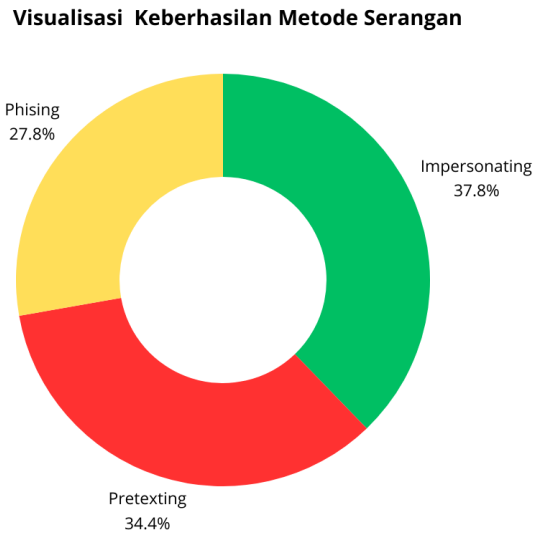
Gambar 4.25 Berhasil masuk ke akun media sosial target.

Disini penguji sudah melakukan cross check ke profile dan memang akun target ini tidak memiliki ataupun menautkan alamat email ke akun facebooknya dan menggunakan nomor telepon sebagai opsi *login*nya. , setelah berhasil masuk penguji melakukan *login* ke akun *game* mobile legend milik target dan berhasil masuk juga seperti pada gambar 4.26



Gambar 4.26 berhasil masuk ke akun *game* target

4.4 Visualisasi dan Analisis Keberhasilan Metode Serangan



Gambar 4.27 grafik tingkat keberhasilan metode serangan

Berdasarkan gambar graphic 4.27 dari 3 serangan yang telah dilakukan dengan total 124 responden, metode *impersonation* mendapatkan 42 responden dengan 33 akun berhasil dimasuki oleh penguji, kemudian metode *pretexting* mendapatkan 41 responden dengan 31 akun berhasil dimasuki oleh penguji kembali, dan terakhir metode *phising* mendapatkan 41 responden dan sebanyak 24 akun berhasil dimasuki oleh penguji, dengan demikian total sebanyak 88 responden akunnya seperti email pribadi, akun media sosial dan juga akun *game* milik target berhasil penguji masukki. Penguji memberikan analisa kenapa sangat mudah untuk melakukan *social engineering* kepada *player* di dalam *game online* bahkan dengan cara yang cukup sederhana:

1. Pressure Lingkungan Sosial & Kompetisi
    a. Banyak *player* merasa terdorong untuk menjaga atau meningkatkan peringkat mereka dalam permainan, terutama jika mereka aktif di komunitas *game*. *player* yang mempunyai peringkat yang tinggi akan mendapatkan pengakuan dan prestise, prestasi tinggi dalam *game* sering kali memberikan rasa bangga dan meningkatkan status di mata teman-teman mereka ataupun komunitas *online*yang tergabung oleh mereka.

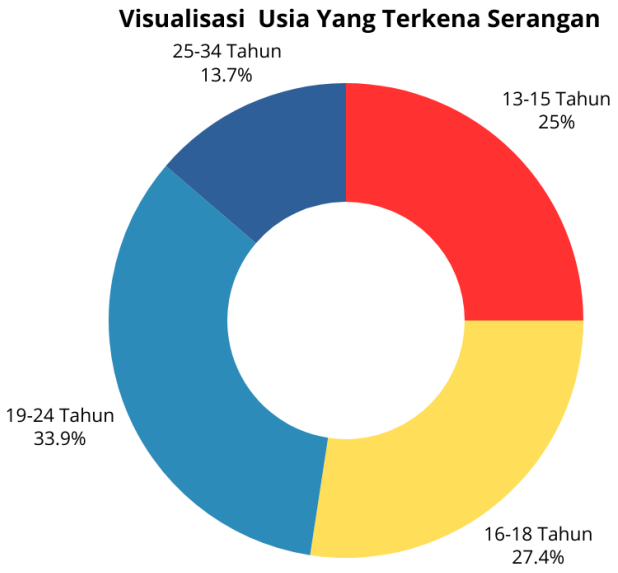
2. Keterbatasan Waktu
    a. Banyak *player*, terutama yang berada dalam ukuran usia produktif, memiliki kesibukan seperti kuliah atau pekerjaan, sehingga waktu bermain menjadi terbatas. Ditambah lagi, *game* seperti PUBGM dan Mobile Legends memiliki durasi permainan yang cukup lama. Menggunakan jasa joki dianggap sebagai cara cepat untuk mencapai target dalam *game* tanpa harus meluangkan banyak waktu bermain.
3. Minimnya Kesadaran terhadap Risiko
    a. Tidak semua *player* memahami risiko menggunakan jasa joki, mengikuti giveaway atau beberapa metode serangan yang meminta data pribadi akun mereka, ditambah kemungkinan akun terkena banned, pencurian data pribadi, atau dampak buruk lainnya. Banyak *player* merasa bahwa penyedia jasa joki dapat dipercaya atau menganggap risiko yang ada sangat kecil, atau mereka tergiur dengan giveaway dengan hadiah yang lumayan banyak tanpa memeriksa apakah tempat mereka mengikuti giveaway mencurigakan.
4. Pengaruh Teknik *Social Engineering*
    a. Penyedia jasa joki sering kali berpura-pura bekerja sama dengan *player* profesional untuk membangun kepercayaan calon pelanggan ataupun membuat store yang menyerupai atau terafiliasi dengan store-store yang sudah terkenal. Janji-janji seperti “dijamin aman” atau “berpengalaman dengan banyak testimoni” seringkali mempengaruhi keputusan *player*. Beberapa penyedia jasa memanfaatkan tautan palsu untuk menarik korban dan mencuri informasi akun mereka. Ditambah dengan faktor bahwa banyak store joki sekarang banyak membuat konten untuk tiktok/instagram mereka yang memungkinkan metode *impersonation* digunakan dengan mencuri identitas ataupun konten-konten yang di upload.
5. Budaya Instant & FOMO
    a. Generasi muda cenderung lebih terbiasa dengan hasil yang instan, sehingga penggunaan jasa joki untuk meningkatkan peringkat/rank mereka serta mendapatkan giveaway secara cuma-cuma tanpa

mengeluarkan uang mereka sendiri untuk membeli aksesoris in-*game* dianggap sebagai solusi yang cocok untuk kebutuhan tersebut. Selain itu faktor psikologis seperti rasa putus asa setelah mengalami kekalahan terus-menerus atau kesulitan naik peringkat ditambah FOMO (Fear Of Missing Out) karena peringkat dan aksesoris in-*game* mereka tidak sebagus *player* lain dapat mendorong *player* untuk mencari bantuan eksternal sehingga akhirnya menggunakan jasa joki dan mengikuti giveaway. *player* tidak ingin kehilangan peluang mengikuti event atau mendapatkan achievement/rank musiman yang hanya tersedia dalam waktu tertentu.

6. Kurangnya Edukasi tentang Bahaya *Social Engineering*
    a. Banyak *player* belum memahami ancaman yang mungkin mereka hadapi, seperti manipulasi psikologis oleh pelaku melalui teknik-teknik seperti *pretexting, impersonation,* atau *phishing*.
    b. Berdasarkan hasil pengujian terhadap 124 responden dengan tiga metode serangan *social engineering* (*impersonation, pretexting,* dan *phishing*), sebanyak 88 akun berhasil ditembus oleh penguji. Namun, terdapat 36 akun yang tidak berhasil ditembus. Faktor-faktor yang memengaruhi ketidakberhasilan ini dapat dianalisis sebagai berikut :
7. Pengaktifan Verifikasi Dua Langkah (2FA)
    a. Salah satu faktor utama yang menyebabkan kegagalan dalam menembus akun adalah penggunaan verifikasi dua langkah (2FA) pada akun *game,* media sosial, dan email. Dengan fitur ini, *player* harus memasukkan kode verifikasi tambahan yang dikirimkan ke perangkat atau nomor telepon yang terdaftar, selain kata sandi yang sudah ada. Hal ini secara signifikan mengurangi kemungkinan pengambilalihan akun, meskipun penguji berhasil mendapatkan data *login* pengguna. Pengguna yang mengaktifkan 2FA akan menerima notifikasi atau kode yang hanya berlaku dalam waktu singkat, membuatnya jauh lebih sulit bagi pelaku untuk mendapatkan akses tanpa izin.

8. Penggunaan Verifikasi Perangkat
    a. Beberapa akun menggunakan verifikasi perangkat, yang memerlukan otentikasi tambahan ketika *login* dari perangkat baru. Misalnya, jika seorang pengguna mencoba mengakses akun mereka dari perangkat yang tidak dikenal, sistem akan meminta kode verifikasi yang dikirimkan ke nomor telepon pengguna atau melalui aplikasi otentikasi. Ini menjadi penghalang besar bagi penguji, yang tidak memiliki akses ke perangkat yang sebelumnya digunakan oleh pemilik akun, sehingga mereka gagal untuk dapat masuk meskipun sudah mendapatkan data *login*.

4.5 Visualisasi dan Analisis Usia Yang Terkena Serangan



Gambar 4.28 Grafik usia yang terkena serangan

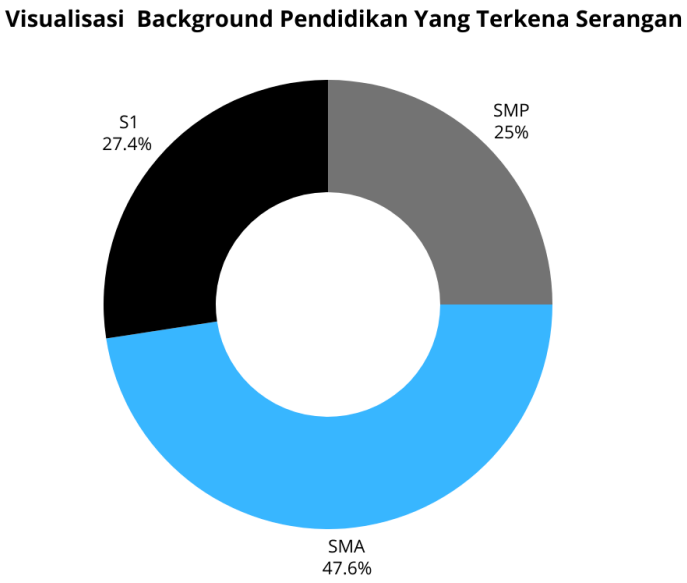
Berdasarkan data yang divisualisasikan dalam gambar 4.28 dari total 3 form yang dibuat dengan total 124 responden penguji memiliki beberapa analisa berdasarkan distribusi usia pengguna yang terkena serangan pada *game online* PUBGM & Mobile Legends sebagai berikut:

1. Usia 19-24 Tahun (33,9%)

a. Usia ini merupakan yang paling sering terkena serangan. Hal ini dapat dikaitkan dengan tingginya intensitas mereka dalam bermain *game online* serta motivasi untuk mencapai peringkat atau level tertentu tapi terhalang dengan keterbatasan waktu dan tekanan sosial menjadi faktor pendorong mereka menggunakan jasa yang berisiko.

2. Usia 16-18 Tahun (27,4%)
    a. Usia ini menjadi kelompok kedua terbesar yang terkena serangan. *player* di usia ini cenderung memiliki waktu bermain lebih banyak, tetapi kurang memiliki pemahaman atau kewaspadaan terhadap risiko serangan *social engineering*.
3. Usia 13-15 Tahun (25%)
    a. Meskipun lebih muda, *player* dalam rentang usia ini juga cukup rentan terhadap serangan. kurang memiliki pemahaman atau kewaspadaan terhadap risiko serangan *social engineering* ditambah faktor psikologis seperti masih labil juga berpengaruh kenapa usia ini masih mudah termanipulasi oleh serangan *social engineering*.
4. Usia 25-34 Tahun (13,7%)
    a. Kelompok usia ini lebih sedikit terkena serangan dibandingkan yang lain. Hal ini mungkin disebabkan oleh pengalaman yang lebih matang dalam mengenali ancaman *online* dan prioritas lain di luar *game*.

4.6 Visualisasi dan Analisis Pendidikan Yang Terkena Serangan



Gambar 4.29 Grafik background pendidikan yang terkena serangan

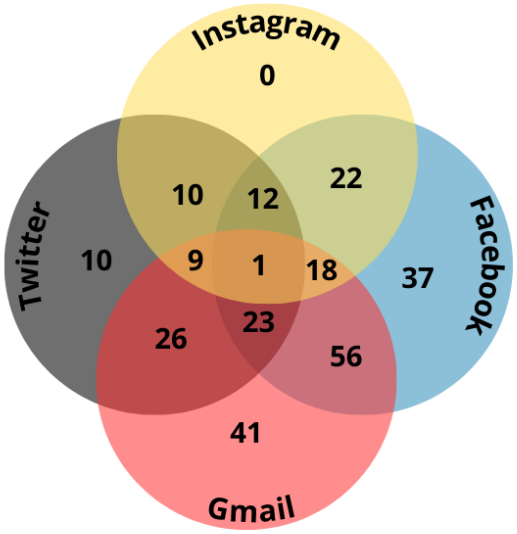
Berdasarkan data yang divisualisasikan dalam gambar 4.29 dari total 3 form yang dibuat dengan total 124 responden penguji memberikan analisis berdasarkan latar belakang pendidikan yang rentan terhadap serangan :

1. Pendidikan SMA (47,6%)
    a. Mayoritas pengguna yang menjadi target serangan berasal dari latar belakang pendidikan SMA. Hal ini dapat dikaitkan dengan tingginya jumlah *player game online* di kalangan pelajar SMA yang memiliki lebih banyak waktu luang untuk bermain dan bersosialisasi secara daring. Kurangnya kesadaran dan pengalaman tentang keamanan siber membuat mereka menjadi target empuk.
2. Pendidikan S1 (27,4%)
    a. Pengguna dengan latar belakang pendidikan perguruan tinggi juga menunjukkan tingkat kerentanan yang cukup signifikan. Hal ini dapat terjadi karena *player* di tingkat ini cenderung lebih sering terlibat dalam aktivitas kompetitif, seperti turnamen atau pembelian aset digital dalam *game*, sehingga mereka lebih rentan terhadap upaya manipulasi seperti *phishing* dan *social engineering*.
3. Pendidikan SMP (25%)

a. Kelompok ini menjadi yang paling kecil dalam data, tetapi tetap cukup signifikan. Faktor utama kerentanan pada kelompok ini adalah kurangnya pengetahuan mengenai ancaman keamanan digital dan ketidaksadaran terhadap dampak negatif dari interaksi daring yang berisiko.

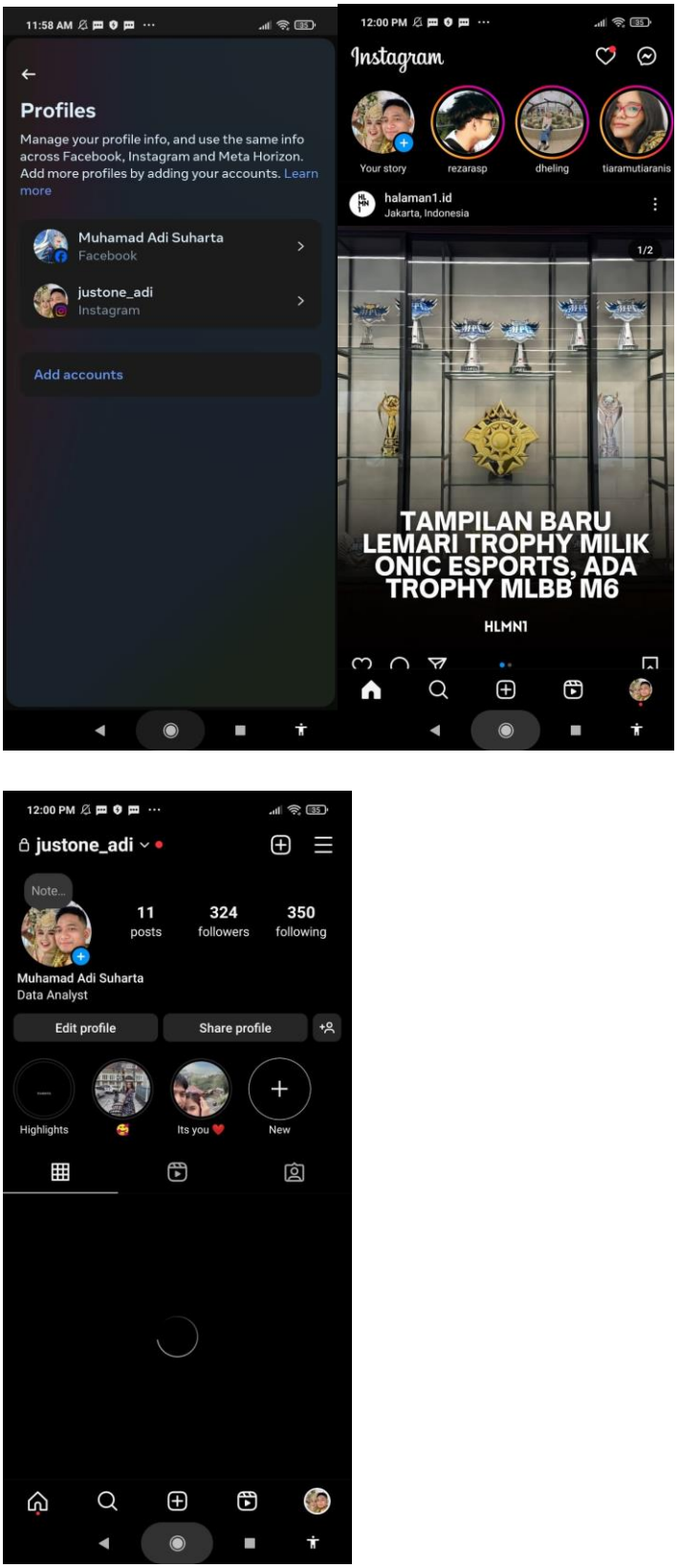
Berdasarkan analisis diatas, penguji dapat mengatakan bahwa apapun pendidikan dan berapapun usianya semuanya masih sering dan rentan terkena serangan *social engineering*. Ini disebabkan oleh masih sedikitnya kesadaran kita terhadap serangan *social engineering* serta jenis-jenis dan metode serangan yang kerap dipakai.

4.7 Visualisasi dan Analisis Akun Yang di Masukki di Luar Gmail & Game.



Gambar 4.30 Grafik login akun

Berdasarkan data yang divisualisasikan dalam gambar 4.30 dari total 3 form yang dibuat dengan total 88 akun yang berhasil dimasukki, beberapa akun diantaranya saling terhubung dengan gmail ataupun akun media sosial lain yang tidak diberikan saat mengisi google form sehingga penguji bisa mengaksesnya.



Gambar 4.31 Akun yang terhubung dengan data yang sama.

Penguji memiliki beberapa analisa berdasarkan visualisasi sebagai berikut:

1. Penggunaan Kredensial yang Sama di Berbagai Platform

   Banyak pengguna menggunakan alamat Gmail dan kata sandi yang sama untuk berbagai platform media sosial dan aplikasi. Hal ini disebabkan oleh:

   a. Kemudahan Akses: Dengan hanya mengingat satu kombinasi alamat email dan kata sandi, pengguna merasa lebih praktis dan tidak perlu mengingat banyak informasi login.
   b. Rendahnya Pemahaman Keamanan: Banyak pengguna tidak sepenuhnya menyadari risiko besar yang muncul jika kredensial ini diretas, terutama jika data tersebut digunakan untuk mengakses akun lainnya.

   Kondisi ini menjadi peluang besar bagi pelaku kejahatan melalui teknik credential stuffing, yaitu memanfaatkan kredensial hasil kebocoran data untuk mencoba masuk ke berbagai platform lain. Jika pengguna menggunakan kata sandi yang sama di berbagai akun, kemungkinan keberhasilan pelaku dalam mencuri akses menjadi sangat tinggi.

2. Persepsi Keamanan yang Keliru
   a. Anggapan Gmail adalah Layanan Aman: Gmail dikenal luas memiliki sistem keamanan yang baik, sehingga pengguna sering kali merasa kredensial mereka aman digunakan di berbagai platform tanpa mempertimbangkan risikonya.
   b. Kurangnya Pemahaman Risiko Social Engineering: Mayoritas pengguna tidak menyadari bahwa pelaku kejahatan dapat dengan mudah memanfaatkan manipulasi psikologis, seperti serangan phishing atau menyamar sebagai pihak terpercaya, untuk mencuri informasi sensitif mereka.
3. Keterhubungan Akun Melalui Gmail

   Sebagai layanan utama untuk mendaftar dan memverifikasi akun pada berbagai platform, Gmail sering kali menjadi pintu masuk ke akun lainnya. Ketika pelaku berhasil mendapatkan akses ke akun Gmail korban, mereka dapat:

a. Mereset Kata Sandi:

   Mengubah kredensial di akun-akun lain yang terhubung ke email tersebut.

b. Mengakses Akun Terhubung:

   Masuk ke platform lain melalui email verifikasi tanpa hambatan.

   Keadaan ini menciptakan efek domino, di mana satu pelanggaran akun dapat berujung pada akses ke banyak akun lain yang dimiliki korban.sistem keamanan yang baik, sehingga pengguna sering kali merasa kredensial mereka aman digunakan di berbagai platform tanpa mempertimbangkan risikonya.

4. Minimnya Penggunaan Autentikasi Dua Faktor (2FA)

Sebagian besar pengguna tidak mengaktifkan fitur autentikasi dua faktor (2FA), yang sebenarnya dapat memberikan perlindungan tambahan. Dengan tidak adanya 2FA, akses ke akun hanya bergantung pada kombinasi nama pengguna dan kata sandi. Jika kredensial tersebut bocor, pelaku dapat langsung mendapatkan akses tanpa hambatan tambahan.