ADAPTASI
JURNAL SOSIAL HUMANIORA DAN KEAGAMAAN

ADAPTASI

Jurnal Sosial Humaniora Dan Keagamaan

ISSN: 3032-386X e-ISSN: 3032-1697

PHISING: STUDI KASUS PERILAKU CYBER-DELINQUENCY PADA KALANGAN REMAJA DI KABUPATEN BATANG

Rayvaldo Maesha Revanza, Muhammad Khatami
Musyrifah Zidni Baroroh, Endon Nur Cahyati
Madrasah Aliyah Negeri Batang
Jalan May Jend Sutoyo, Karangasem Selatan, Batang, Jawa Tengah
nayangtaka371@gmail.com
endonnurcayati2023@gmail.com

Abstrak - Akses internet yang semakin mudah membuka peluang yang luas bagi remaja untuk berinteraksi dan memperoleh informasi. Kejahatan siber melalui *phising* menjadi ancaman serius bagi keamanan data pribadi. Penelitian ini bertujuan untuk mengetahui bagaimana perilaku *cyber-deliquency phising* pada kalangan remaja di Kabupaten Batang. Melalui metode kualitatif studi kasus dengan mendiskripsikan perilaku *phising* dengan teknik pengumpulan data melalui wawancara, observasi dan dokumentasi dengan informan yaitu Rakun, Marmut, Hamster, Tupai, Rubah, Berang-berang. Pengolahan dan analisis data menggunakan model interaktif Miles, Huberman, dan Saldana, yang terdiri dari pengumpulan data, kondensasi data, penyajian data, dan penarikan kesimpulan. Hasil penelitian menunjukkan perilaku Phising sebagai bentuk *cyber-delinquency* pada kalangan remaja melalui tiga aktivitas yaitu membuat *link* jebakan dengan media sosial, mulai dari Tiktok, Youtube, Facebook, hingga WhatsApp. Menyebarkan *link* jebakan melaui iming-iming *game* gratis, video porno, dan barang-barang gratis. Aktivitas pengambil alihan akun dangan menjual data-data korban dan memainkan akunnya. Alat dan media yang digunakan yaitu HP, laptop, komputer. Sedangkan motivasi dalam aktivitas Phising sesuai dengan Teori Herzberg bahwa motivasi aktivitas dipengaruhi oleh fakor ektrinsik dan instrinsik. prilaku *cyber-deliquency* merupakan hasil dari proses pemodelan, penguatan dan asosiasi diferensial sesuai Teori Belajar Sosial Albert Bandura. Sedangkan kebutuhan yang mendasari pada pada level Self-Actualization Needs, pada level ini remaja memenuhi potensi dan mencapai tujuan pribadinya. Implikasi dari penelitian menekankan pentingnya edukasi bagi masyarakat tentang pencurian data melalui metode *phising* yang sering terjadi di sosial media dan para pelakunya yaitu remaja. Penelitian ini menyarankan kepada pemerintah untuk menyebarluaskan edukasi tentang phising, khususnya remaja agar tidak terdoktrin oleh perilaku *phising*.

Kata kunci : Phishing, Cyber-delinquency, Keamanan siber, Perilaku online, Remaja

A. Pendahuluan

Masa remaja merupakan masa peralihan antara masa kanak-kanak dengan masa dewasa, yang ditandai dengan pertumbuhan dan perkambangan dalam hal fisik dan psikis. Remaja bukan lagi anak-anak dalam bentuk badan maupun cara berpikir, tetapi bukan pula orang dewasa yang telah mencapai kematangan (Daradjat, 1990: 23). Masa ini adalah masa

paling indah dan menyenangkan dalam kehidupan seseorang, hal tersebut dikarenakan seseorang bisa belajar dan mencoba banyak hal. Para remaja kerap kali mencoba sesuatu hal yang baru dan lebih menantang sekaligus masa pencarian jati diri.

Masa remaja dapat diketahui melalui beberapa ciri, di antaranya adalah peningkatan emosional yang terjadi sangat cepat, yang kemudian dikenal dengan masa strom dan masa stress. Peningkatan emosial yang terjadi merupakan akibat dari perubahan fisik, terutama perubahan hormon yang terjadi pada masa remaja. Pada masa ini, remaja dihadapkan dengan banyaknya tuntutan dan tekanan, seperti tuntutan untuk tidak berlaku seperti anak-anak, mereka harus lebih mandiri dan dapat bertanggung jawab atas diri mereka sendiri (Jahya, 2011: 235). Oleh karena hal tersebut, masa remaja juga merupakan suatu masa yang banyak menimbulkan masalah, seseorang seringkali tidak dapat mengendalikan emosinya sendiri saat menghadapi banyak masalah, baik di lingkungan rumah, sekolah, maupun di lingkungan sosial lainnya. Di sisi lain, sifat keingintahuan yang dimiliki remaja menyebabkan ia suka mencoba hal-hal baru, seperti hal yang sedang ramai di dunia maya. Sikap keingintahuan ini bila tidak diimbangi dengan landasan moral dan akhlak dapat menyebabkan anak berbuat tidak baik atau dapat membentuk perilakunya menjadi jahat. Tindakan remaja yang nakal ini dapat membuat banyak masalah, baik di lingkungan rumah, sekolah, bahkan di dunia maya. Kenakalan remaja mengacu pada berbagai perilaku yang tidak diterima norma atau melanggar hukum mulai dari masalah perilaku ringan misalnya minum minuman keras, perilaku antisosial, dan kriminal yang serius misalnya kekerasan dan pencurian (Hurlock, 2003: 211).

Data survey Asosiasi Jasa Pengguna Internet Indonesia (AJPII 2022)) tingkat penetrasi dan kontribusi pengguna internet 99,26% adalah pelajar dan mahasiswa, dengan konten media sosial menduduki posisi tertinggi yang diakses 89,15% dari konten lainnya. Perkembangan teknologi informasi yang semakin pesat ikut berpengaruh terhadap bentuk kenakalan remaja, dari yang semula kenakalan di dunia nyata menjadi kenakalan di dunia maya. Adanya ketergantungan internet menyebabkan remaja kecanduan dan ingin mencoba hal-hal yang tidak ia ketahui di jejaring internet dan menyalahgunakan untuk hal-hal negatif yang mencakup berbagai masalah perilaku, seperti pennindasan di dunia maya, penyalinan perangkat lunak secara ilegal, peretasan komputer, pencurian identitas seseorang, memposting, informasi palsu, dan lain-lain.

Pesatnya perkembangan teknologi internet juga diiringi dengan meluasnya penyalahgunaan informasi pribadi pengguna, sehingga menjadi masalah yang sangat

meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya yang bisa dikenal dengan *cybercrime*. Istilah lain dari *cybercrime* adalah *cyber-delinquency*. Perbedaan di antara keduanya adalah batasan usia pelaku. Apabila pelaku masuk kategori remaja maka di sebut sebagai *cyber- delinquency*. Sanjev Kumar dan Anupam Manhas (2021) menyebutkan bentuk-bentuk dari *cyber-delinquency* yang terdiri dari *cybercrime againts children, cyber-pornography, cyber- suicides, web hijacking, cyber-stalking, virus attacks, sofware piracy, phising, online gambling, cyber terrorism, cyber bullying, debit card and credit card frauds, impersonation and identity theft, online drug trafficking,* dan *hacking*.

Berdasarkan riset data dari POLRI, pada bulan April 2020 sampai Juli 2021, setidaknya ada 937 kasus kejahatan di dunia maya yang dilaporkan di Indonesia. Selain itu, terdapat kasus di e-MP Robinopsnal Bareskrim Polri menunjukkan 8.831 kasus kejahatan siber sejak 1 Januari hingga 22 Desember 2022. Kejahatan di dunia maya pada periode 2021 bila dibandingkan dengan periode 2022 jumlah kasus kejahatan meningkat hingga 14 kali. Dari kasus-kasus tersebut, terdapat pelaku kejahatan *cyber* yang merupakan kalangan remaja. Sebesar usia remaja yang paling banyak melakukan kejahatan di Indonesia, sebesar 65% pelakunya adalah remaja. Para pelaku ini menggunakan beberapa cara dalam melakukan kejahatannya antara lain penipuan *phising*, peretasan, *cyber stalking*, *cyber bullying*, dan lain sebagainya.

Berdasarkan sumber dari situs aag-it.com, kejahatan *cyber* yang paling umum adalah *phising*. Phishing adalah usaha *hacker* untuk mendapatkan informasi penting dan rahasia secara tidak sah dengan cara menggunakan email dan situs web palsu yang seperti *user id*, *password*, PIN, atau informasi rahasia yang lain dengan situs atau web, sedangkan situs *phising* merupakan sebuah situs yang di desain oleh pelaku dengan tampilan situs konten, URL domain, dan sejenisnya agar menyerupai situs aslinya untuk mengelabui korbannya (pengguna internet) dengan membuat korban seakan mengakses halaman situs aslinya. Berdasarkan latar belakang tersebut, maka peneliti memandang sangat penting melakukan penelitian berkaitan dengan perilaku Phising sebagai bentuk *cyber-delinquency* pada kalangan remaja di Kabupaten Batang.

B. Kajian Teori dan Tinjauan Pustaka

Phishing adalah bentuk rekayasa sosial dan penipuan di mana penyerang menipu orang untuk mengungkapkan informasi sensitif atau menginstal malware seperti *ransomware* (Jansson dan von Solms, 2011). Phising merupakan salah satu bentuk kejahatan elektronik berupa penipuan. Phising dimaksudkan untuk memperoleh informasi sensitif seperti

username, *password*, dan detil kartu kredit melalui menjerat dengan cara meniru sebagai sebuah entitas yang bisa dipercaya/*legitimate organization* dan sering kali berkomunikasi secara elektronik (Rachmawati, 2014: 211). Aktivitas Phising sering kali dilakukan dengan menggunakan media sosial yang terhubung secara online, seperti email, SMS, dan Website (Gulo dkk, 2020: 71).

Cyber Delinquency merupakan sebuah frasa yang terdiri dari kata *cyber* dan *delinquere*. Siber (*cyber*) adalah segala sesuatu yang berkaitan dengan sistem komputer dan informasi. Istilah *cyber* mencakup semua sistem komputasi, didalamnya termasuk penyimpanan data, perlindungan data, pengaksesan data, pemrosesan data, pentransmisian data, dan penghubungan data. Sedangkan *delinquere* sebagaimana penjelasan sebelumnya dapat diartikan sebagai kenakalan. Berdasarkan definisi tersebut *cyber delinquency* dapat diartikan sebagai kenakalan di dunia maya. Istilah lain dari *cyber delinquency* adalah *cyber crime* atau kejahatan di dunia maya. Perbedaan di antara keduanya adalah batasan usia pelaku. Apabila pelaku masuk kategori remaja maka di sebut sebagai *cyber delinquency*. Adapun faktor yang mempengaruhi *cyber delinquency* adalah depresi, kurang perhatian, penggunaan internet untuk komunikasi sosial, dan hubungan dengan guru (Yo, 2022).

Remaja adalah masa pertumbuhan dari kanak-kanak menuju dewasa yang berlangsung antara usia 11 tahun hingga usia 21 tahun. Pada masa ini seorang remaja berkembang, dimulai dari perkembangan organ-organ fisik dan berkembangnya kondisi individu yang mencakup aspek psikis dan sosial atau sebaliknya. Seorang remaja sudah tidak dapat lagi dikatakan sebagai kanak-kanak karena adanya pertumbuhan fisik, namun ia masih belum cukup matang secara pemikiran untuk dapat dikatakan dewasa. Berdasarkan definisi tersebut remaja dapat diartikan sebagai masa transisi/peralihan yang ditandai dengan adanya pertumbuhan dan perkembangan kepribadian individu yang mencakup kematangan mental, emosional, sosial dan fisik.

Motivasi berasal dari kata motif yang berarti kekuatan yang ada pada diri individu, yang mengakibatkan individu tersebut bertindak atau berbuat. Motif adalah daya penggerak dalam diri seseorang untuk melakukan aktivitas tertentu, untuk mencapai tujuan tertentu. Dari pengertian motif tersebut, motivasi dapat diartikan sebagai dorongan yang terdapat dalam diri seseorang untuk berusaha mengadakan perubahan tingkah laku yang lebih baik dalam memenuhi kebutuhannya (Uno, 2006). Apabila ditinjau dari sumbernya, maka motif terbagi menjadi dua, yaitu motif intrinsik dan motif ekstrinsik. Motif intrinsik adalah dorongan yang timbul tanpa membutuhkan rangsangan dari luar. Hal tersebut di karenakan

dorongan atau motif intrinsik memang sudah ada dalam diri seseorang sesuai dengan kebutuhannya. Sedangkan motif ekstrinsik adalah motif atau dorongan yang timbul karena adanya rangsangan dari pihak luar (Uno, 2006).

Menurut Abraham Maslow (1984: 39) dorongan dalam diri seseorang untuk melakukan suatu perbuatan dikarenakan adanya lima kebutuhan dasar manusia. Kelima kebutuhan dasar yang ada dalam diri seseorang kemudian dikenal dengan hirarki kebutuhan. Adapun kelima kebutuhan, yaitu *physiological needs* atau kebutuhan fisologi (sandang pangan), *safety needs* atau kebutuhan rasa aman (bebas bahaya), *love needs* atau kebutuhan akan kasih sayang, *esteem needs* atau kebutuhan akan harga diri, *self actualization* atau kebutuhan akan aktualisasi diri. Sedangkan menurut Herzberg, motivasi atau dorongan dalam diri seseorang untuk mencapai kepuasan dan menjauhkan diri dari ketidak puasan dipengaruhi oleh faktor *higiene* (faktor ekstrinsik) dan faktor *motivator* (intrinsik). Faktor *higiene* adalah dorongan dari dalam diri seseorang untuk keluar dari ketidak puasan. Faktor *higiene* merupakan faktor yang berasal dari luar diri seseorang (ekstrinsik), dapat berupa hubungan antar manusia, keuntungan timbal balik, kondisi lingkungan dan sebagainya. Sedangkan faktor *motivator* adalah dorongan dari dalam diri seseorang untuk mencapai kepuasan. Faktor *motivator* berasal dari dalam diri seseorang (intrinsik), seperti *achievement*, pengakuan, kemajuan tingkat kehidupan, dan lain sebagainya.

Penelitian yang dilakukan oleh Richwen Canady, Mandalan, dan DesfantioWuidjaja pada tahun 2022 dengan Tindakan Hacking dan Profesi Hacker: Persoalan Etis antara Utilitarianisme dan Deontologi yang dipublikasikan dalam jurnal *Praxis: Jurnal Filsafat Terapan*. Dengan menggunakan metode penelitian deskriptif kuantitatif melalui metode survei berbentuk kuesioner, hasil penelitian tersebut membuktikan teori utilitarianisme dan deontologi berlaku terhadap permasalahan *hacking* dan *hacker*. Penelitian tersebut memiliki persamaan dengan penelitian yang dilakukan, yakni Phising sebagai salah satu bentuk dari *grey hat hacker*. Letak perbedaanya ada pada metodologi yang digunakan, yakni metode kualitatif. Sehingga hasil penelitian ini diharapkan bisa memberikan gambaran secara mendalam tentang perilaku Phising sebagai bentuk *cyber-delinquency* di kalangan remaja

Penelitian yang dilakukan oleh Mohd. Yusuf DM., Addermie, dan Jasmine Lim tahun 2020 yang berjudul Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia yang telah dipublikasikan dalam *Jurnal Pendidikan dan Konseling*. Hasil dari penelitian tersebut menyatakan bahwa Cyber Crime merupakan kejahatan yang timbul karena dampak negatif pemanfaatan teknologi internet. Cyber Crime ini bukan hanya

kejahatan terhadap komputer tetapi juga kejahatan terhadap sistem jaringan komputer dan pengguna. Pelaku Cyber Crime saat ini melakukan kejahatan tersebut bukan hanya karna mempraktikkan keahlian yang dimiliki dengan metode *phising*. Motif pelaku Cyber Crime adalah karena faktor uang, dendam, politik, iseng, dan sebagainya. Cyber Crime dilakukan oleh orang-orang yang memiliki kemampuan tinggi terhadap komputer dan jaringannya. Penelitian tersebut memiliki persamaan objek dengan penelitian yang akan diteliti, yakni Phising. Perbedaannya adalah penelitian tersebut menitik beratkan pada aktivitas Phising sebagai Cyber Crime dan sistem hukum di Indonesia. Sedangkan penelitian yang akan dilakukan berusaha menggambarkan perilaku Phising yang dilakukan oleh remaja atau *cyber-delinquency* (kenakalan di dunia maya).

Penelitian yang dilakukan oleh Hasbi Ash Shaddiqi pada tahun 2016 dengan judul Subkultur Anak Muda Hacker di Dunia Maya. Hasil penelitian tersebut menyatakan bahwa aktivitas Hacking dilakukan karena adanya tantangan, rasa penasaran, mendongkrak identitas, jahil, dan membantu teman. Subkultur yang dibangun dalam komunitas Hacker Link adalah interaksi dan relasi antara para *hacker*, dan tidak diberikannya ruang untuk belajar *hacking* di lingkungan sekolah. interaksi yang dimaksud adalah interaksi baik bersifat positif, maupun yang bersifat negatif. Dari dua interaksi tersebut terdapat perbedaan pada tipologi dari unsur sub ordinal, intelektual organik, konformitas, integrasi budaya dan tingkat hegemoni. Penelitian tersebut memiliki persamaan objek dengan penelitian yang akan diteliti, yakni Hacking secara umum. Perbedaannya adalah penelitian yang akan dilakukan lebih fakus kepada Phising sebagai salah satu metode yang digunakan dalam aktivitas Hacking.

C. Metode Penelitian

Metode penelitian menggunakan penelitian kualitatif dengan pendekatan studi kasus. Penelitian kualitatif merupakan suatu paradigma penelitian untuk mendeskripsikan peristiwa, perilaku orang atau suatu keadaan pada tempat tertentu secara rinci dan mendalam dalam bentuk narasi berdasarkan kasus lapangan yang terjadi didalam masyarakat. Adapun kasus lapangan yang akan dilakukan penelitian adalah Phising sebagai bentuk *cyber-delinquency* pada kalangan remaja di Kabupaten Batang. Guna memperoleh data penelitian yang luas serta mendalam, maka upaya atau teknik pengumpulan data yang dilakukan adalah melalui wawancara, observasi dan dokumentasi.

Teknik wawancara dalam penelitian ini digunakan untuk memperoleh data tentang perilaku Phising. Wawancara ditujukan kepada informan sebagai pelaku Phising, hal ini

diharapkan untuk memperoleh data perilaku Phising sebagai bentuk *cyber-delinquency* pada kalangan remaja di Kabupaten Batang. Dalam melakukan wawancara, dibuat pedoman yang dijadikan acuan dan instrumen wawancara yang dilakukan bersifat terbuka, dan terstruktur dengan pedoman. Observasi adalah suatu teknik pengumpulan data di mana peneliti terlibat secara aktif dalam kegiatan yang diamati. Sehingga peneliti ikut serta dalam segala aktivitas Phising, mulai dari membuat *link* jebakan, menyebarkan *link* jebakan, sampai dengan aktivitas pengambil alihan akun. Hal tersebut diharapkan dapat memberikan gambaran secara menyeluruh berkaitan dengan perilaku Phising dan motivasi dalam aktivitas Phising. Metode dokumentasi yaitu mencari data mengenai hal-hal atau variabel yang berupa foto, dokumen, video, unggahan di media sosial dan sebagainya. Dokumentasi merupakan data sekunder yang menunjang metode wawancara dan observasi. Teknik dokumentasi digunakan untuk mengumpulkan data tentang aktivitas Phising. Informan penelitian terdiri dari 6 yang memenuhi syarat terdiri dari Rakun, Marmut, Hamster, Tupai, Rubah, Berang-berang.

Teknik analisis data yang akan digunakan dalam penelitian ini ialah teknik analisis deskriptif, yaitu metode penelitian yang berusaha menggambarkan dan menginterpretasikan objek sesuai dengan apa adanya. Dalam penelitian, peneliti mencoba untuk mendeskripsikan dan memaparkan hasil dari wawancara, dokumentasi maupun hasil pengamatan secara langsung yang berkaitan dengan perilaku Phising sebagai bentuk *cyber-delinquency* pada kalangan remaja di Kabupaten Batang. Sedangkan model analisis data yang akan digunakan adalah model interaktif Miles, Huberman, dan Saldana, yang terdiri dari pengumpulan data (*data collection*), kondensasi data (*data condensation*), penyajian data (*data display*), penarikan kesimpulan (*conclusions drawing*).

Pengumpulan data dilakukan degan menggunakan dua teknik pengumpul data, yakni wawancara dan dokumentasi. Teknik wawancara digunakan untuk memperoleh gambaran perilaku Phising sebagai bentuk *cyber-delinquency* di kalangan remaja. Sedangkan teknik dokumentasi digunakan untuk memperoleh data berkaitan dengan aktivitas Phising yang dilakukan oleh Group Facebook. Kondensasi data yakni proses pemilihan, memfokuskan, menyederhanakan, mengabstraksi, serta mentransformasikan data yang mendekati keseluruhan bagian dari catatan lapangan secara tertulis, transkrip wawancara, dan lain sebagainya. Kondensasi data dilakukan setelah peneliti mendapatkan data wawancara, observasi dan dokumentasi. Selanjutnya data hasil penelitian tersebut dipilah untuk mendapatkan fokus penelitian yang dibutuhkan. Adapun tahapan dalam kondensasi data

terdiri dari *selecting* (pemilihan data), *focussing* (pengerucutan data), *abstracting, simplifiying* dan *transforming.*

Penyajian data dilakukan untuk mempermudahkan peneliti memahami masalah untuk dapat melanjutkan ke tahap berikutnya. Setelah mengumpulkan data terkait perilaku Phissing di kalangan remaja, selanjutnya peneliti akan mengelompokkan hasil wawancara, observasi dan dokumentasi untuk disajikan dan dibahasa secara detail. Pada tahap penyajian data, peneliti menyajikan data yang diperoleh dari hasil wawancara, observasi dan dokumentasi melalui uraian singkat dari masing-masing informan secara terpisah berdasarkan masalah penelitian. Hal tersebut dilakukan untuk menyampaikan informasi yang diperoleh sebagai gambaran perilaku Phissing. Seluruh identitas informan ditampilkan dengan menggunakan inisial untuk kemudian dirubah menjadi kode untuk menjaga kerahasiaan identitas peserta didik.

Pada tahap penarikan kesimpulan, data yang diperoleh dari hasil wawancara, observasi dan dokumentasi untuk dianalisis dan ditarik suatu kesimpulan. Pengambilan kesimpulan merupakan suatu proses interpretasi data dari awal pengumpulan dengan disertai pembuatan pola dan uraian atau penjelasan. Setelah menyajikan data terkait perilaku Phissing di kalangan remaja, maka peneliti akan menarik kesimpulan tentang perilaku Phissing. Penarikan kesimpulan dalam tahap ini berdasarkan hasil informasi yang disampaiakan oleh para informan dan telah melalui berbagai tahapan analisis data.

D. Hasil Dan Pembahasan

1. Hasil Penelitian

Penggunaan internet di berbagai usia tanpa disertai literasi digital yang memadai membuka peluang terjadinya kejahatan siber. Remaja yang intens menggunakan internet tanpa pengawasan dan pemahaman yang cukup rentan menjadi korban atau pelaku kejahatan siber. Kurangnya literasi digital di tengah pesatnya perkembangan teknologi menjadi celah bagi pelaku kejahatan siber untuk melancarkan aksinya. Maraknya penggunaan internet di berbagai lapisan masyarakat tanpa diimbangi dengan kesadaran akan risiko keamanan siber dapat memicu berbagai bentuk kejahatan daring (Melanda, Surahman, & Yulianti, 2023).

Phising merupakan salah satu kejaharan siber, yang juga terjadi di kabupaten Batang. Perilaku *phising* terdiri dari berbagai macam aktivitas, melalui alat dan media yang beragam dan para pelaku termotivasi dari dalam dirinya dan di luar dirinya. Hasil penelitian perilaku *cyber-delinquency* pada kalangan remaja di Kabupaten Batang yang

diperoleh dari hasil wawancara, observasi dan dokumentasi bahwa, sumber informasi pembuatan *phising* diperoleh melalui media sosial seperti Youtube, Facebook dan Group jual beli. Selain itu sumber pembuatan *phising* juga informan peroleh dengan cara membeli di forum. Pembuatan *phising* melalui media sosial seperti yang terjadi pada informan Rubah, Rakun, Marmut dan Hamaster. Hal tersebut sebagaimana penuturan dari Rakun sebagai berikut: "Dari youtube terus grub grub wa jual beli akun biasane ada yang ngasih tutor ngephising". Hal tersebut juga didukung oleh pernyataan Marmut sebagai berikut: "Dari temen semua di grub facebook ada admin gtu aku tanya tanya phising terus dikasi carane kyak tadi".

Berbeda dari keempat informan tersebut, informan berang-berang dan tupai memperoleh dengan cara membeli. Berang-berang membeli dari teman dekatnya sedangkan tupai membuat *phising* dengan cara membeli forum jual beli Facebook sebagaimana penjelasannya sebagai berikut: "Saya cari-cari admin-admin JB yang tau tentang phising, terus saya beli website phisingnya."

Pembuatan *phising* bisa bervariatif berdasarkan alat dan media yang digunakan oleh para pelaku. Alat dan media yang digunakan untuk membuat *phising* dapat dibedakan menjadi tiga kategori, yakni pertama melalui *website chrome* dengan cara *copy codingan* dari *website* yang mau disamarkan, kedua membeli dari Group jual beli di Facebook, dan ketiga membuat melalui aplikasi *github*. Website bisa digunakan sebagai media pembuatan *phising*, hal ini biasa dilakukan oleh informan Rakun, Hamster, dan Marmut. Salah satu informan tersebut, yaitu Rakun berbicara sebagai berikut: "Mengcopy codingan dari website tertentu dan dimodifikasi semirip mungkin."Di sisi lain, adapun informan yang lebih memilih membeli website phising karena menurut informan tersebut lebih mudah membeli dan bisa meminta website yang seperti diinginkan. Berikut kutipan dari Tupai: "Kalau aku sendiri beli ke seller yang bisa buat phising di grub jual beli akun nanti aku terima jadi udah dibuatun website by request kukayak aku mintae website phising isinya bagi bagi diamond gratis, video porno, dll.".

Namun ada juga Informan yang membuat *phising* dengan alat-alat yang tersedia dari *github*. Berikut kutipan dari Rubah:

> "Caranya tu tinggal download ahmyt habis itu klik apk builder terus dicentang semua dari sms, file manager, telepon, pesan, dll setelah itu disana ada sebuah kolom berupa kolom IP, Port kita sendiri terus setelah IP, port kita isi kita klik buildrun aplikasinya kan sudah kedownload setelah didownload aplikasinya tu dikirim ke korban, kita jalankan dulu ipnya/aplikasinya menggunakan ahmyth yang bagian menu daftar. Disana ada sebuah kolom port yang kita isi sebelumnya, setelah itu kita klik listen si

> korban membuka aplikasi tersebut yang kita isi backdoor itu, terus korban itu mengizinkan aplikasi seperti telepon, file manager, dll. Setelah si korban mengizinkan semuanya maka IP server korban tersebut akan masuk kedalam aplikasi ke ahmyth, terus si pelaku bisa melihat semua informasi data yang ada server hp korban tersebut."

Para Pelaku *phising* juga selalu waspada saat mereka melakukan *phising*, hal ini demi menjaga identitas mereka tetap aman dan mencegah hal-hal yang tidak diinginkan. Oleh karena itu, para pelaku juga mempelajari cara menyembunyikan identitas mereka. Berikut kutipan singkat dari Hamster tentang cara menyembunyikan identitasnya: "pake file yang dimodifikasi". Adapun kutipan dari Rakun yakni: "saya menggunakan vpn dari negara lain sehingga alamat IP yang tercantum pada saat membagikan web phising. Jadinya saya tidak dapat terdeteksi dengan mudah."

Setelah pelaku selesai membuat *website* atau aplikasi *phising*, pelaku tersebut menyebarkan *link phisingnya* di berbagai media sosial, mulai dari Tiktok, Youtube, Facebook, dan WhatsApp. Tetapi dari sekian banyaknya media sosial, pelaku lebih menargetkan penyebaran *link phising* di Facebook, terutama di komunitas *game* karena rata-rata anggota grup tersebut berisi anak-anak/remaja yang tidak tahu tentang *phising* dan mudah ditipu. Informan Marmut menyatakan bahwa: "Aku biasa nebar di facebook grub komunitas game biar gampang cari korban dengan embel embel diamond gratis." Pernyataan tersebut didukung informan Tupai sebagai berikut: "Website phisinge we tak sebar nang tiktok yang followernya banyak yang biasa fyp akunne, terus grub facebook tentang game gane masalahnya targerku di player sultan game bocil bocil sultan game."

Saat pelaku menyebarkan *link phising*, pelaku tersebut biasa melampirkan iming-iming agar bisa menarik perhatian korban dan memanipulasi tautan agar terlihat seperti alamat institusi aslinya. Hal ini juga untuk membuat korban agar tergiur untuk memasuki *website* milik pelaku. Pelaku biasa menggunakan 3 tawaran agar korban mengklik *link* tersebut, yaitu *item game* gratis, video porno, dan barang-barang gratis. Hal ini dikarenakan iming-iming tersebut merupakan hal yang umum dan menggiurkan bagi orang-orang yang ingin ditargetkan oleh pelaku. Berikut iming-iming yang ditawarkan oleh informan Tupai: "website phising isinya bagi bagi diamond gratis, video porno, dll." Pernyataan tentang iming-iming tersebut juga didukung oleh Marmut dengan kutipannya:"website phising isinya bagi bagi diamond gratis, video porno, dll."

Target korban *phising* cenderung acak, hal ini dikarenakan pelaku hanya menyebarkannya di media sosial tanpa mengetahui siapa yang akan terpancing. Hal tersebut dinyatakan oleh Marmut melalui kutipan beriku:"Siapa aja yang kejebak

phising." Namun pelaku juga bisa menargetkan korbannya untuk balas dendam, dugaan diperkuat oleh Rakun dengan kutipannya yaitu: "saya ingin balas dendam untuk pelaku phising yang pernah menjebak saya waktu itu akun utama pribadi saya masuk ke link phising terus gabisa kembali lagi."

Phising tersebut saat korban sudah masuk ke *website phising* melalui *link* yang disebar oleh pelaku. Saat korban datang di *website phising*, korban akan diminta untuk mengisi formulir data yang diberikan di *website phising* tersebut. Saat korban sudah mengisi semua formulir data yang dibutuhkan maka secara tidak sadar, korban tersebut memberikan datanya kepada pelaku *phising*. Cara kerja *phising* tersebut juga dinyatakan oleh Marmut yakni: "Korbannya itu mengklik linknya terus mengisi forum data." Informan Rubah juga menjelaskan cara kerja phising tersebut, dengan kutipannya yakni: "korban membuka aplikasi tersebut yang kita isi backdoor itu, terus korban itu mengizinkan aplikasi seperti telepon, file manager, dll. Setelah si korban mengizinkan semuanya maka IP server korban tersebut akan masuk kedalam aplikasi ke ahmyth, terus si pelaku bisa melihat semua informasi data yang ada server hp korban tersebut."

Data yang didapatkan oleh pelaku tersebut dapat diambil alih dan dimanfaatkan untuk kepentingan pribadinya. Hal ini juga menyebabkan kerugian kepada sang korban karena datanya dapat diketahui oleh pelaku, pelaku tersebut cenderung menjual data-data korban dan memainkan akun *game* untuk dirinya sendiri. Informan Tupai menyatakan bahwa: "Aku koleksi buat main bentar terus akhire ya tak jual lumayan si" Tetapi ada juga informan yang justru menyimpannya dan membiarkan akun, hal ini dinyatakan oleh informan Rubah yaitu: "Kalo itu buat simpanan doang, gak saya jual. Soalnya kan tau bukan akun milik pribadi, akunnya orang."

Alat yang digunakan pelaku untuk membuat *phising* dibagi menjadi 3 kategori, yaitu HP, laptop, komputer. Ada 3 informan yang pernah menggunakan 3 alat tersebut, salah satunya yaitu Marmut yang menyatakan: "Alatnya opsional bisa HP, Laptop, PC."Adapun informan yang tidak bisa menggunakan ketiga alat tersebut, bisa jadi karena factor biaya atau kebiasaan. Seperti kutipan Rubah yaitu: "Saya biasanya menggunakan komputer." Dan kutipan dari Rakun yaitu: "Aku pake hp biasa waktu itu oppo jadul."

Spesifikasi dan Fitur-fitur yang disediakan dari alat juga dapat mempengaruhi efisiensi dalam pembuatan *phising*. Hal itu didukung oleh Rubah melalui kutipannya yaitu: "Bisa ngaruh tergantung spesifikasi device nya." Dan Hamster juga menyarankan: "Spek HP jangan kentang, nanti lag" Namun banyaknya fitur-fitur tersebut juga dapat

membuat bingung pelaku, hal ini disampaikan oleh informan Rakun yakni: "Lebih enak pake hp, karena kalo pake komputer itu pusing."

Setelah pelaku menyiapkan alat yang memadai, selanjutnya pelaku harus mempunyai media yang tersedia di alat itu. Media tersebut bisa melalui *website* atau aplikasi, tetapi pelaku juga bisa langsung membeli *website phising* dari seseorang. Seorang informan yaitu Tupai mengatakan: “Mending beli daripada bingung buat”. Dalam pembuatan *phising* melalui *website*, pelaku harus membeli media yang diperlukan. Berikut media yang dibeli berdasarkan informan Hamster yakni: "Medianya server, c-panel, WHM, file, dan domain.” Adapun Rubah yang membuat phising di aplikasi: "Saya biasa menggunakan windows, github, ahmyt."

Media juga berkembang dengan adanya AI yang semakin canggih, tetapi pelaku *phising* cenderung tidak menggunakan AI karena beberapa hal seperti kebingungan saat menggunakannya. Hal tersebut dikutip dari informan Marmut yakni: "Saya kebingungan saat menggunakannya." Dan Hamster yang mengatakan: "Saya tidak menggunakannya." Namun hanya Rubah yang menggunakan AI dengan cara berikut: "Bisa pake AI, kalo pake chatGPT kita ketik aja bagaimana cara membuat aplikasi rat di metasploit. Maka AI akan memberi jawaban cara membuatnya dan langkah-langkah."

Alasan kenapa pelaku tetap melakukan *phising* karena adanya motivasi yaitu ingin mendapatkan akun *game* yang bagus, dan mendapatkan uang sebagai penghasilan tambahan. Tetapi ada sedikit pelaku yang cuma untuk rasa penasaran dan pengetahuan. Hal tersebut diperkuat oleh kutipan Tupai yakni: "Ya cuman pengen aja ngambil akun game e orang apalagi sultan ada kepuasan tersendiri gitu klo dapet akun game banyak." Dan informan Hamster yang turut memperkuat pernyataan tersebut: "Biar dapet uanglah mayan." Tetapi ada juga pelaku yang melakukannya dengan motif yang sudah berubah, yaitu Rubah dengan kutipannya yakni: "Kalo menurut aku yang dulu, tujuannya itu buat ngehack akun. Terus yang sekarang ini coba membuat aplikasi backdoor yang bisa buat phising itu tujuannya buat pengetahuan doang sama belajar."

Pelaku cenderung senang saat mendapatkan akun dari hasil *phising*, pelaku kerap merasakan "penyegaran" secara batin saat melakukan *phising*. Hal ini dirasakan oleh informan Marmut, Rakun, Rubah, Tupai. Marmut memberikan kutipan yakni: "Serasa seger saat ada notifikasi masuk, yang menandakan ada akun masuk hasil phising.” Tetapi berbeda dari 4 informan tersebut, Hamster justru tidak merasakan adanya kesenangan

karena dia serius. Berikut adalah pernyataannya: "Gak ada, aku fokus cari akun buat dijual."

Pelaku bisa tertarik melakukan *phising* karena berbagai hal, bisa dari mengikuti temannya, penasaran untuk mendapatkan uang dan akun game. Hal tersebut dirasakan oleh Marmut, Rakun, Rubah, Berang-berang dan Tupai. Berikut adalah kutipan dari Marmut "Awal awalnya si penasaran kok di per jb an pada ngephising phising eh kok sampe sini malah bisa dijual dapet duit." Adapun informan yang mulai melakukan phising karena dia pernah menjadi korban, hal ini dinyatakan oleh Rakun yakni: "Awalnya saat saya kena tipu di website phising dan akun game saya hilang. Setelah kejadian itu saya ingin menjadi pelaku phising dan mendapatkan akun game."

Pelaku lebih memilih berkerjasama dengan orang lain, agar beban mereka menjadi lebih ringan. Pelaku bisa membagikan akun hasil phising atau membayar untuk orang yang berkerjasama. Hal ini juga bisa menambahkan semangat pelaku dalam pembuatan phsing dikarenakan adanya rekan kerja. Beberapa informan yang melakukan kerja sama saat melakukan phising yakni Rakun, Hamster, Tupai, Rubah dan Berang-berang. Rakun memberikan kutipan yakni: "Bekerja sma dengan memakai jasa tebar phising dengan memasang seseorang yang famous/terkenal untuk bekerjasama menyebarkan web phising saya di grub-grub media sosial sehingga target yakin untuk masuk web tersebut." Adapun informan yang melakukan kerjasama disaat-saat tertentu seperti Rubah yakni: "Kalo ngephising itu biasanya sendiri sih, tapi kalo uji coba ke temen hacker untuk kelinci percobaan berhasil atau tidak."

2. Pembahasan

Phishing adalah upaya yang dilakukan oleh peretas untuk memperoleh informasi penting dan rahasia secara ilegal dengan menggunakan email dan situs web palsu. Informasi yang dicari bisa berupa user ID, kata sandi, PIN, atau data rahasia lainnya. Situs phishing adalah situs yang dirancang oleh pelaku dengan tampilan, konten, dan URL yang menyerupai situs asli untuk menipu korban (pengguna internet) agar mereka percaya bahwa mereka sedang mengakses situs yang sah.

a. Aktivitas Phising Pada Kalangan Remaja di Kabupaten Batang

Pishing terdiri dari beberapa jenis, salah satunya yaitu web *phising*. Cara kerjanya menyebarkan *link* atau tautan, biasanya *phising* ini menyertai iming-iming agar bisa menarik perhatian korban untuk masuk ke *website* yang sudah dibuat pelaku *phising*. Iming-iming atau penawaran yang dimaksud bisa berupa pornografi, *item*

game gratis (contohnya diamond MLBB), dan bagi-bagi benda gratis (contohnya HP,uang). Saat korban masuk ke *website* pelaku *phising*, tampilan *website* akan dibuat semirip atau semeyakinkan mungkin. Pelaku akan meminta korban untuk memberikan informasi seperti data akun *game* dan data bank.

Cara kerja *phising* yaitu pelaku memilih calon korban pada media sosial yang ditargetkan lalu pelaku membuat sebuah postingan dan menyebarkan *link* tautan web *phising* yang berisikan iming-iming pornografi, *item diamond* gratis, atau yang *trend* sekarang agar korban tergiur masuk. Kemudian korban akan dimintakan untuk memasukkan data email dan *paswordnya* untuk *login* agar bisa mendapatkan apa yang di web tersebut. Otomatis data akun korban langsung masuk ke gmail pelaku dan pelaku bisa mengakses/mengambil akun tersebut. Dalam penelitian ini aktivitas *phising* terdiri dari tiga sebagaimana gambar berikut ini;

Gambar 1. Aktivitas Phising

Pelaku bisa belajar tentang *phising* dengan bertanya-tanya di media sosial dan browsing di internet. Pembuatannya juga perlu menyiapkan beberapa alat dan media. Phising bisa dibuat dengan *website* lalu mengedit dan *mengcopy codingan* dari *website* yang ingin disamarkan. Lalu pelaku bisa mengedit *website* tersebut agar *website* tidak *error* dan pelaku bisa mendapatkan data yang diinginkan. Pelaku juga harus menutupi identitasnya saat melakukan *phising* agar tidak mudah dilacak. Hal ini sesuai dengan penelitian Farid (2023) Terdapat indikasi tindakan peretasan sistem saat pelaksanaan penilaian tengah semester berbasis CBT pada semester genap tahun pelajaran 2022/2023. Peristiwa ini ditandai dengan perubahan tampilan aplikasi CBT dari warna putih menjadi hitam pada layar peserta.

Jadi disimpulkan bahwa pelaku *phishing* memiliki pemahaman yang cukup baik tentang teknik-teknik dasar *phishing*. Mereka memperoleh pengetahuan ini melalui berbagai sumber, seperti media sosial dan internet. Pelaku juga menunjukkan

kemampuan teknis dalam membuat dan mengelola situs web *phishing* dengan memodifikasi kode sumber dari situs web yang telah ada.

Pelaku menyebarkan *linknya* di media sosial dan masuk ke suatu komunitas tertentu untuk menyebarkan *link phisingnya*. Pelaku juga melampirkan iming-iming saat menyebarkan *phising* seperti video porno dan *item game online*, agar korban tertarik untuk klik *link* yang disediakan oleh pelaku. Pelaku menargetkan komunitas *game* agar pelaku mendapatkan akun *game* dari si korban dan pelaku juga bisa menggunakan *phishing* untuk balas dendam kepada seseorang.

Pelaku *phishing* umumnya memilih target secara spesifik, seperti komunitas *game*. Mereka menggunakan berbagai taktik untuk menarik perhatian korban, termasuk menawarkan iming-iming berupa konten dewasa atau *item game* langka. Selain itu, pelaku juga memanfaatkan media sosial dan komunitas online sebagai sarana untuk menyebarkan *link phishing*. Alkhalil.dkk (2021) *phishing, is that younger adults are more trusting when it comes to online communication, and are also more likely to click on unsolicited e-mails*, jadi remaja memiliki kecenderungan tinggdi untuk mengeklik email yang tidak diminta.

Cara kerja *phising* yaitu saat korban sudah klik *link* dan masuk ke *website* yang diberikan oleh pelaku. Setelah datang ke *website phising*, maka korban akan disuruh memasukkan data yang diinginkan oleh pelaku. Disaat korban sudah mengirim datanya, maka si pelaku akan menerima data korban dan dapat mengambil alih akun milik korban. Pelaku bebas menggunakan akun korban untuk memakai atau menjualnya. Hasil penelitian ini mendukung temuan Bhavsar dkk. (2018) yang menyatakan bahwa phishing merupakan bentuk penipuan sosial. penelitian ini menunjukkan bahwa pelaku phishing seringkali menyamar sebagai perusahaan, bank, atau layanan online populer untuk menipu korban.

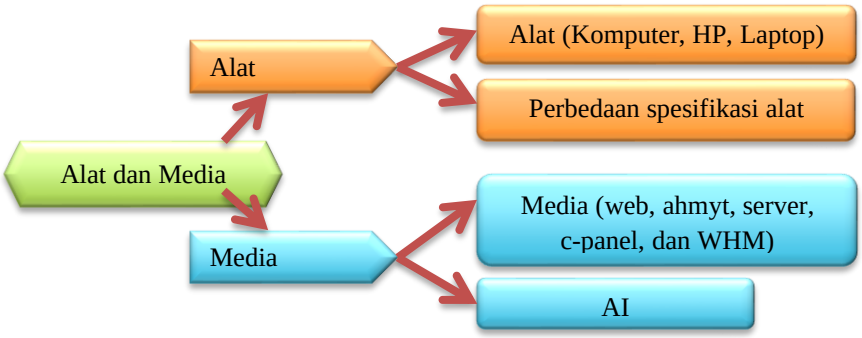
Alkhalil dkk (2021) menyampaikan mekanisme *phishing process flow and phases*, yaitu target *information gathering devising attack method (planing phase*). *Attacker exploits vulnerability and suitable medium (preparation phase*). *Attacker send treat, user respond, (attack phase). User valuable disclosed to attacker (valuable acquisition phase*) hal ini selaras dengan proses *phishing* di Kabupaten Batang yaitu target pengumpulan informasi melalui jaringan internet, kemudian melakukan penyerangan dengan memilih media sosial yang tepat yaitu Web, FB, Tiktok, dan lain-

lain, setelah mendapatkan balasan maka melakukan pengambilan akun untuk diretas agar mendapatkan keuntungan.

Mekanisme kerja *phishing* yang diidentifikasi dalam penelitian ini menunjukkan bahwa pelaku berhasil mengeksploitasi kerentanan pengguna internet. Dengan mengelabui korban untuk memasukkan data pribadi atau kredensial *login*, pelaku dapat mengakses akun korban dan menyalahgunakannya untuk berbagai tujuan, seperti pencurian identitas atau keuntungan finansial. Perilaku *Cyber-delinquency* tersebut menunjukkan bahwa manusia belajar melaui proses kognitif sosial. Albert Bandura (1977) dalam Teori Kepribadian Kognitif Sosial menyampaikan bahwa dilakukan melalui pengamatan dan imitasi. Dengan pembelajaran observasional, individu belajar dengan mengamati perilaku orang lain, terutama model yang dianggap penting atau relevan. Sedangkan proses kognitif dalam pembelajaran tidak hanya melibatkan imitasi sederhana, tetapi juga melibatkan proses kognitif seperti perhatian, retensi, reproduksi, dan motivasi. (Nabavi, R. T. :2012).

b. Alat dan Media Phising

Hampir semua perangkat bisa digunakan untuk membuat *phising*, tapi perangkat yang biasa digunakan oleh para remaja yaitu Handphone dan tidak banyak juga menggunakan komputer. Sedangkan media sosial yang biasa digunakan untuk menyebar web *phising* oleh pelaku yaitu Facebook, Instagram, Tiktok, Whatsapp. Dari sekian banyaknya media, media yang banyak memakan korban adalah Tiktok dan Facebook karena sosial media tersebut yang sedang tren/viral pada kalangan remaja khususnya.



Gambar 2. Alat dan Media Phising

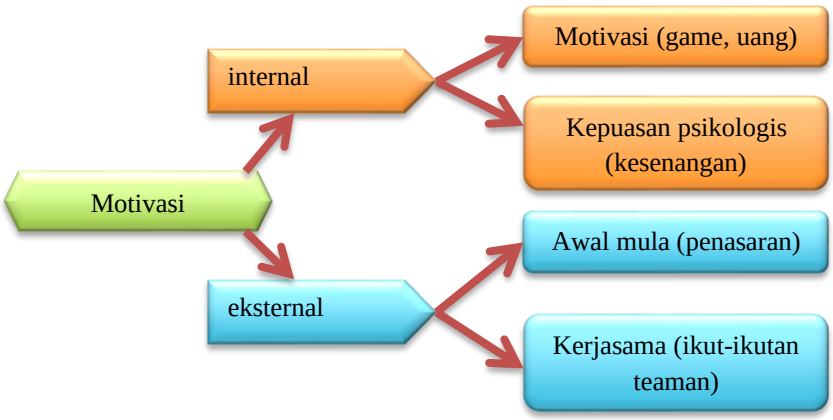
Pelaku dapat memilih alat untuk membuat *phising*, diantaranya HP, laptop, komputer. Tetapi hal ini dapat mempengaruhi efisiensi pelaku dalam membuatnya seperti, *error*, fitur terbatas, dan beberapa media yang tidak dapat digunakan di alat tertentu. Hasil penelitian Ansyafa dkk (2024) menunjukkan bahwa semua platform

media sosial yang diteliti tidak kebal terhadap serangan *phishing* dan *spoofing email*, mengkonfirmasi efektivitas teknik kloning situs web dalam mencuri informasi pribadi pengguna.

Pelaku bisa menggunakan *server, github*, WHM dan *c-panel* sebagai media dalam pembuatan *phising*. Dengan adanya AI, pelaku dapat menggunakan untuk meningkatkan efisiensi dalam *phising*. Hal ini berbeda dengan studi KeepnetLABS pada tahun 2018 mengkonfirmasi bahwa lebih dari 91% pelanggaran sistem disebabkan oleh serangan yang dimulai oleh email. Alkhalil. dkk. (2021).

c. Motivasi Phising

Berdasarkan penelitian ini, dapat diketahui bahwa motivasi pelaku *phising* untuk melakukan *phising* adalah untuk mendapatkan data akun *game* yang dituju/ditargetkan. Pelaku mendapatkan kepuasan tersendiri secara material maupun psikologis. Secara psikologis, mereka medapatkan kepuasan/kesenangan karena telah menipu dan mencuri data seseorang, serta sensasi "menyegarkan" saat ada notifikasi bahwa pelaku berhasil mendapatkan akun dari korban. Keuntungan yang didapatkan pelaku secara material adalah mereka bisa mendapatkan akun dari korban *phising*, baik akun game maupun akun bank. Akun-akun tersebut bisa dimanfaatkan dengan cara memakai akun game atau menjual akun game tersebut, serta mengambil uang dari akun bank.



Gambar 3. Motivasi perilaku Phising

Pelaku melakukan phising karena pelaku ada motivasi tertentu secara internal dan eksternal. Pelaku bisa mendapatkan uang, akun *game* untuk dimainkan, pengetahuan tentang *hacking*, dan kesenangan secara psikologis. Pelaku bisa melakukan *phising* secara efisien jika pelaku kerjasama dengan seseorang atau dibantu

temannya, hal ini juga bisa menjadi faktor dari asal mula kenapa pelaku mulai melakukan *phising*.

E. Kesimpulan dan Saran

Aktivitas *phishing* melibatkan serangkaian tindakan yang dirancang untuk menipu korban agar menyerahkan informasi pribadi mereka. Proses ini dapat dibagi menjadi beberapa tahap utama yaitu pertama membuat jebakan *link* melalui pemahaman yang cukup baik tentang teknik-teknik dasar *phishing* yang diperoleh dari berbagai sumber, seperti media sosial dan internet pelaku *phishing* memiliki. Kedua menyebarkan linknya di media sosial dan masuk ke suatu komunitas tertentu untuk menyebarkan *link phisingnya* dengan memilih target secara spesifik. Ketiga pengambilan akun dengan cara mengeksploitasi kerentanan pengguna internet, yaitu kalangan remaja.

Pelaku semakin tertarik untuk membuat *phising* dikarenakan adanya motivasi tertentu, mulai dari teman-temannya, menambah uang dengan menjual akun, mencoba akun *game* korban, menambah pengetahuan tentang *hacking*, hingga adanya kesenangan psikologi. Dengan adanya alat dan media yang tersedia, pelaku bisa membuat phising dengan bantuan dari teman-temannya atau pelaku bisa *browsing*. Terlebih lagi dengan perkembangan zaman ini, AI dapat pelaku agar lebih mudah dalam pembuatan *phising*.

Dengan memahami betapa bahayanya *phising*, maka kami selaku penulis ingin menyampaikan saran kepada pembaca. Pembaca disarankan jangan memasukin *website* sembarangan, karena *website* tersebut belum tentu *website* yang aman. Pembaca juga harus meningkatkan keamanan *cyber* yang diperlukan untuk menjaga data pribadi. Pihak pemerintah dapat menghimbau kepada masyarakat tentang *phising*, dan pihak sekolah juga dianjurkan untuk memberikan edukasi terhadap peserta didik tentang *phising*.

Daftar Pustaka

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

APJI. 2022. "*Profil Internet Indonesia*", https://apji.or.id, diakses pada 27 Agutus 2022 pukul 08.44.

Canady, R., Mandalan, Wuidjaja, D. 2022. *Tindakan Hacking dan Profesi Hacker: Persoalan Etis antara Utilitarianisme dan Deontologi*. Praxis: Jurnal Filsafat Terapan 1(1): 59-78. https://journal.forikami.com/index.php/praxis/article/view/45.

Creswell, J. W. 2012. *Research Design : Pendekatan Kualitatif, Kuantitatif, dan Mixed, Cetakan II*. Yogyakarta: Pustaka Pelajar.

Daradjat, Z. 2012. *Ilmu Pendidikan Islam*. Jakarta: Bumi Aksara.

Farid, I. (2024). Upaya Guru Akidah Akhlak dalam Mencegah Juvenile Cyber-Delinquency di Madrasah Aliyah Negeri Batang. *Tesis*. UIN KH. Abdurrahman Wahid Pekalongan

Feru Lantara. 2021. *Dosen Kriminolog UI: Kejahatan siber marak pada masa pandemic*. https://www.antaranews.com/berita/2297458/dosen-kriminolog-ui-kejahatan-siber-marak- pada-masa-pandemi.

Gulo, A.S., Lasmadi, S., Nawawi, K. 2021. *Cyber Crime dalam Bentuk Phising Berdasarkan Undang- Undang Informasi dan Transaksi Elektronik*. Pampas: Journal of Criminal Law 1 (2): 68-81. https://online-journal.unja.ac.id/Pampas.

Hurlock, E.B. 2003. *Psikologi Perkembangan*. Jakarta: Erlangga.

Jahja, Y. 2011. *Psikologi Perkembangan*. Jakarta: Prenadamedia Group.

Kementerian Komunikasi dan Informatika Republik Indonesia. 2022. "*Statistik Aduan*", https://kominfo.go.ig/statistik, diakses pada 11 Agustus 2022 pukul 15.51.

Kumar, S., Manhas A,. 2021. *Cyber Delinquencies. International Journal of Law Management and Humanities*.Vol. 4. No. 3. Hal 2536-2544.

Nabavi, R. T. (2012). Bandura's social learning theory & social cognitive learning theory. *Theory of Developmental Psychology*, *1*(1), 1-24.

Pusiknas Bareskrim Polri. 2022. *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat.* https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat.

Rachmawati, D. 2014. *Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber*. Jurnal Saintkom 13 (3): 211.

Santrock, J.W. 2002. *Adolescence Perkembangan Remaja*. Jakarta: Erlangga.

Shaddiqi, H.A. 2016. *Subkultur Anak Muda Hacker di Dunia Maya*. Surabaya: Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Airlangga.

Siagian, Sondang, P. 1995. *Teori Motivasi dan Aplikasinya.* Jakarta: PT. Rineka Cipta Jakarta.

Uno, H. B. 2006. *Teori Motivasi dan Pengukurannya Analisis di Bidang Pendidikan*. Jakarta: PT. Bumi Aksara.

Yo, J. A. 2022. *What shapes cyber delinquency in adolescents?: A holistic and comparative analysis of cyber and traditional offline delinquencies, Children and Youth Services Review.* Vol. 136.

Yusuf, M., Addermie, Lim, J. 2020. *Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia*. Jurnal Pendidikan dan Konseling 4 (5): 8018-8023. https://doi.org/10.31004/jpdk.v4i5.7977.