SIMULASI PANCINGAN DATA SPESIFIK
DI PEJABAT SETIAUSAHA KERAJAAN NEGERI SEMBILAN

SHARULFAIZAL TAHAR

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEH IJAZAH SARJANA KESELAMATAN
SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2023

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

23 Mac 2023

SHARULFAIZAL TAHAR

P114359

PENGHARGAAN

Syukur terhadap Ilahi kerana dengan limpah kurnia dan izinNya dapat saya melengkapkan kajian ini. Terima kasih kepada penyelia projek, Prof. Madya Dr. Masnizah Mohd di atas segala bimbingan dan tunjuk ajar sepanjang pelaksanaan sehingga lengkapnya kajian ini dengan sempurna.

Ucapan terima kasih juga dirakamkan kepada Jabatan Perkhidmatan Awam (JPA) yang telah memberi peluang dan tajaan kepada saya untuk melanjutkan pelajaran ke peringkat Sarjana dan kepada Pejabat Setiausaha Kerajaan Negeri Sembilan (PSUKNS) serta Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) di atas kebenaran, sokongan dan kerjasama dalam pelaksanaan kajian ini.

Saya juga merakamkan ucapan terima kasih kepada isteri, anak, kedua ibu bapa serta setiap ahli keluarga saya di atas segala doa dan dorongan semangat yang telah diberikan untuk saya meneruskan pengajian saya ini. Tidak lupa kepada rakan-rakan dalam perkhidmatan dan sahabat SDAR926 yang banyak membantu dalam menjayakan kajian ini, terima kasih!

ABSTRAK

Perkembangan industri teknologi maklumat telah menjadikan data atau maklumat sebagai satu komoditi berharga yang baharu. Ini secara langsung telah menyebabkan pengurusan maklumat sulit dalam sektor kerajaan menghadapi pelbagai bentuk ancaman siber, khususnya ancaman pancingan data. Situasi ini telah meningkatkan cabaran dalam usaha untuk memelihara kerahsiaan, integriti serta kebolehcapaian kepada sesuatu maklumat tanpa menjejaskan mutu perkhidmatan organisasi. Pemusatan perkhidmatan sistem e-mel agensi kerajaan di bawah sistem MyGOVUC yang dikawalselia Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) adalah satu langkah penambahbaikan yang bertujuan untuk meningkatkan tahap keselamatan teknologi maklumat sektor kerajaan dengan menggunakan teknologi perlindungan yang terkini terhadap ancaman pancingan data. Rekod MAMPU menunjukkan untuk tempoh 9 bulan sahaja iaitu bermula Mac sehingga November 2022, sebanyak 850,203 e-mel pancingan data telah dikesan dan berjaya disekat. Jumlah serangan pancingan data yang tinggi ini menimbulkan kegusaran sekiranya ia berjaya melepasi tapisan teknologi yang digunapakai, keselamatan maklumat kerajaan seterusnya hanya bergantung kepada kemahiran dan pengetahuan pengguna akhir, yang mana tahap kerentanannya masih belum pernah diuji. Kajian ini telah menjadikan Pejabat Setiausaha Kerajaan Negeri Sembilan (PSUKNS) sebagai domain untuk mendapatkan gambaran sebenar tahap kerentanan kakitangan sebuah organisasi kerajaan yang bertanggungjawab menguruskan maklumat terperingkat (sulit), terhadap ancaman pancingan data. Instrumen pengujian berbentuk simulasi telah dijalankan dengan melibatkan kakitangan daripada gred 19 sehingga 52 yang terlibat secara langsung dengan pengurusan maklumat terperingkat sebagai sampel sasaran. Seterusnya, satu soal selidik diedarkan kepada keseluruhan populasi kajian bagi mengenalpasti punca yang mempengaruhi respon populasi terhadap simulasi yang telah dijalankan serta persepsi kakitangan terhadap kepentingan untuk melaporkan sesuatu insiden keselamatan siber. Hasil simulasi mendapati sebanyak 19% daripada 278 personel telah terpedaya dengan e-mel pancingan data yang dibangunkan. Hasil simulasi dan soal selidik juga mendapati kekerapan kakitangan untuk melaporkan sesuatu insiden keselamatan siber masih rendah, walaupun mereka mempunyai pengetahuan tentang keperluan untuk melaporkan insiden berkenaan. Hasil utama kajian ini adalah satu prosedur simulasi pancingan data umum yang boleh digunapakai oleh pelbagai agensi di bawah sektor kerajaan yang menguruskan maklumat kritikal kerajaan. Manakala bagi populasi kajian pula, dapatan kajian ini boleh dijadikan sebagai penanda aras terhadap tahap kerentanan kakitangan organisasi terhadap pancingan data spesifik.

PHISHING SIMULATION IN NEGERI SEMBILAN STATE SECRETARY'S OFFICE

ABSTRACT

The evolution of the information technology industry has made data as an emerging valuable commodity. This has caused managing of classified information in the government sector, to face various cyber challenges and threats. This situation has increased the challenge in their effort to guard the confidentiality, integrity and accessibility of information without compromising the quality of the organization's services. The centralization of the government e-mail system known as MyGOVUC, regulated by Malaysian Administration Modernization and Management Planning Unit (MAMPU), is an enhancement that aims to increase the level of government sector information technology security. The system is focused on applying the latest protection technology against the threat of data phishing. MAMPU records show that for a period of only 9 months, from March to November 2022, a total of 850,203 phishing emails have been detected and successfully blocked. The high number of attempted phishing attacks is worrying, if they succeeded in penetrating the anti-phishing technology. The only security defense left is to rely on the skills and knowledge of the end users, whose level of vulnerability has yet to be tested. In this study, Negeri Sembilan State Secretary's Office (PSUKNS) has been chosen as the domain to get the level of vulnerability among employees of a government organization that often handles classified information, against phishing threats. A simulation-based testing instrument was conducted involving a target sample consisting of staffs from grade 19 to 52, who are directly involved with the management of classified information. A questionnaire had been distributed to the entire study population to identify the causes that influenced the population's response to the simulation as well as the staff's perception of the importance of reporting a cyber security incident. The results of the simulation were that 19% of the 278 personnel had fallen for the phishing e-mail. The simulation and questionnaire results also show that the frequency of the staff reporting a cyber security incident is still low, even though they have knowledge of the need to report such incident. The main result of this study is a general phishing simulation procedure that can be used by various agencies under the government sector that manage critical government information. As for the study population, the findings of this study can be used as a benchmark for the level of the workforce's vulnerability towards specific data phishing.

KANDUNGAN

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN

AI	Kecerdasan Buatan
BSOD	Skrin Biru Mati
IP	Protokol Internet
MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
ML	Pembelajaran Mesin
PPT	People-Process-Technology
PSUKNS	Pejabat Setiausaha Kerajaan Negeri Sembilan
UPTM	Unit Pengurusan Teknologi Maklumat
VM	Mesin Maya
VPN	Rangkaian Peribadi Maya

BAB I

PENDAHULUAN

1.1 PENGENALAN

Evolusi dalam sektor teknologi maklumat dewasa ini semakin bertambah pesat ekoran peningkatan dalam permintaan terhadap penggunaannya oleh pelbagai sektor, termasuk sektor kerajaan yang telah menyaksikan adaptasi teknologi untuk menyokong dan mempertingkatkan mutu penyampaian perkhidmatan yang ditawarkan. Penggunaan e-mel khususnya, dilihat semakin popular digunakan dalam sektor kerajaan bagi menggantikan pengiriman dokumen secara konvensional. Namun, pengadaptasian teknologi ini juga secara langsung dilihat telah meningkatkan tahap ancaman siber kepada organisasi kerajaan.

Mel elektronik atau e-mel adalah salah satu perkhidmatan yang paling banyak digunakan untuk pertukaran maklumat. Ia kerap digunakan untuk sebagai medium komunikasi kerana ia dapat menjimatkan tempoh masa, cekap dan ia mempunyai tahap kebolehgunaan yang lebih baik berbanding medium komunikasi lain. Laporan Statistik E-mel 2021-2025 yang dikeluarkan oleh The Radicati Group (2021) merekodkan jumlah e-mel yang dihantar dan diterima di seluruh dunia dalam sehari adalah sebanyak 319.6 bilion dan jumlah ini diramalkan akan meningkatkan kepada melebihi 376 bilion sehari pada akhir tahun 2025. Ini menunjukkan bahawa pengguna biasa menerima lebih kurang 40 sehingga 50 e-mel sehari manakala entiti perniagaan boleh menerima ratusan e-mel dalam sehari. Dengan jumlah e-mel yang banyak, masalah berkaitan *spam* dan serangan pancingan data turut meningkat. E-mel *spam* terbahagi kepada beberapa jenis yang berbeza dan setiap jenis tersebut mempunyai karektornya tersendiri. Jenis yang

paling biasa ialah e-mel *spam*/ sampah (*junk*) yang diterima dalam peti mel tetapi tidak mempunyai apa-apa kaitan dengan aktiviti atau pekerjaan si penerima. Contohnya e-mel yang mengandungi iklan berkaitan pinjaman wang. Satu lagi jenis e-mel *spam* yang biasa adalah e-mel penipuan (*scam*) dengan penipuan yang paling popular dipanggil e-mel pancingan data. E-mel jenis ini berbeza dengan e-mel *spam*/ sampah. E-mel pancingan data lebih cenderung untuk mempunyai perisian hasad (*malware*) dan kebiasaannya e-mel jenis ini boleh menyebabkan kehilangan data sensitif (Fadhil Naswir, Zakaria & Saad 2020).

Serangan pancingan data adalah cubaan untuk mendapatkan maklumat rahsia milik seseorang individu atau pun sesebuah organisasi. Ia melibatkan tindakan penyamaran sebagai halaman web yang dipercayai untuk menarik pengguna mendedahkan data sensitif mereka seperti nama pengguna, kata laluan dan maklumat kad kredit. Pancingan data adalah satu mekanisma yang ringkas tetapi kompleks. Hanya dengan sedikit maklumat mengenai mangsa, penjenayah boleh menghasilkan satu e-mel atau laman web yang kelihatan seakan-akan betul dan menyakinkan (Shabudin et al. 2020). Kebanyakan serangan pancingan data bermula dengan menghantar e-mel palsu yang mengaku daripada organisasi yang dipercayai dan sering dibuat untuk kelihatan serupa dengan yang sah sehingga menyebabkan ia sukar untuk dibezakan oleh pengguna (Hanis Binti Tuan Kob et al., 2020). *Spear phishing* atau pancingan data spesifik pula menumpukan sasarannya kepada sesebuah kumpulan yang mempunyai persamaan tertentu, sebagai contoh, sekumpulan individu dalam sesebuah organisasi (Nazreen & Munawara Banu n.d., 2013).

Bagi agensi-agensi di bawah Kerajaan Malaysia, sistem e-mel rasmi yang digunakan adalah salah satu fungsi dibawah Perkhidmatan Komunikasi Bersepadu Kerajaan yang juga dikenali sebagai MyGOVUC. Perkhidmatan ini diuruskan secara berpusat di MAMPU. Selain daripada perkhidmatan e-mel, ia juga turut menawarkan kemudahan *instant messaging*, persidangan audio, persidangan video, pengarkiban e-mel, penghantaran e-mel bersaiz besar, perkongsian dokumen dan perkhidmatan penghantaran notifikasi sistem. Pemusatan perkhidmatan ini di MAMPU adalah bagi memastikan perlindungan kepada data serta maklumat kerajaan dengan menggunakan

polisi serta perisian perlindungan yang seragam dan terkini. Berdasarkan rekod pada tahun 2018, sebanyak 213 agensi Kerajaan Pusat dengan seramai 310,957 orang kakitangan awam telah didaftarkan sebagai pengguna sistem MyGOVUC (MAMPU, 2018). Jumlah ini telah meningkat kepada 386,335 akaun setakat November 2022 (MAMPU, 2022), ekoran pengadaptasian sistem tersebut oleh beberapa Kerajaan Negeri termasuk Kerajaan Negeri Sembilan.

Kajian ini memberikan fokus kepada pancingan data spesifik dalam sektor kerajaan, dengan memberi penekanan kepada pengguna akhir yang menggunakan sistem e-mel kerajaan. Selaku penjawat awam yang bertanggungjawab untuk menguruskan maklumat sulit kerajaan, mereka perlu sentiasa peka tentang keperluan keselamatan sesuatu maklumat sulit. Justeru keupayaan mereka untuk melindungi kerahsiaan, integriti dan kebolehcapaian maklumat sulit daripada ancaman pancingan data adalah sangat penting. Kegagalan untuk melindungi maklumat sulit khususnya milik kerajaan, boleh mengakibatkan kerugian yang besar kepada kerajaan dan boleh mengugat keamanan serta kesejahteraan negara.

1.2 PENYATAAN MASALAH

Keselamatan sesebuah sistem adalah bergantung kepada pengguna akhir sistem tersebut dan ia juga bergantung pada pematuhan mereka terhadap polisi atau dasar keselamatan siber yang berkaitan sistem berkenaan (Desolda et al. 2022). Walaupun sesebuah sistem e-mel boleh dilengkapi dengan perisian perlindungan keselamatan yang berteknologi tinggi, pengguna akhir masih terdedah dan boleh menjadi mangsa pancingan data. Ini kerana pancingan data adalah salah satu cabang dalam kejuruteraan sosial yang meletakkan manusia sebagai sasaran dan terdapat pelbagai kaedah serangan pancingan data yang boleh dilakukan oleh penjenayah untuk memperdaya mangsa mereka (Shabudin et al. 2020; Yeoh et al. 2022). Pelbagai kaedah telah dilakukan untuk menghalang kegiatan pancingan data namun penjenayah sentiasa dapat mencari jalan untuk melakukan serangan ke atas sasaran mereka.

Laporan Trend Aktiviti Pancingan Data bagi Suku Kedua Tahun 2022 yang dikeluarkan oleh APWG, sebuah platfom dalam talian yang memantau dan menganalisa insiden serangan pancingan data global, telah merekodkan jumlah serangan yang paling buruk dalam tempoh suku kedua tahun 2022 iaitu sebanyak 1,097,811 kes. Bilangan serangan pancingan data yang dilaporkan kepada APWG pada suku kedua tahun 2022 ini adalah empat kali ganda lebih tinggi daripada rekod pada tahun 2020 dengan jumlah antara 68,000 ke 94,000 serangan pancingan data setiap bulan.

Terdapat beberapa kajian terdahulu yang telah menguji tahap kerentanan populasi kajian terhadap pancingan data dalam pelbagai sektor, seperti sektor pendidikan (Norhafizah Abu Bakar 2017), (Siti Zaleha Ahmad 2020), (Yeoh et al. 2022) dan (Alhaddad 2021), sektor makanan dan pertanian (Muhd Azi Pekeri 2021), sektor kewangan dan perbankan (Chatchalermpun & Daengsi 2021), serta sektor telekomunikasi (Ahmad Syukri Abdullah 2019) dan (Sharifah Raziah Mohd Aris 2020). Namun masih belum ada prosedur pengujian yang dijalankan ke atas organisasi kerajaan negeri yang menguruskan maklumat kritikal kerajan negeri.

Berdasarkan kepada laporan *Phishing Insight 2021* yang dikeluarkan oleh Sophos, masih banyak organisasi kerajaan yang tidak peka terhadap keperluan untuk melaksanakan program kesedaran keselamatan siber bagi menangani insiden pancingan data. Laporan tersebut mendapati Pihak Berkuasa Tempatan dan Kerajaan Pusat menduduki 2 tangga paling corot berbanding dengan organisasi daripada sektor lain dengan masing-masing mencatat 69% dan 83% dalam mengadakan program kesedaran untuk menangani pancingan data. Keadaan ini amat membimbangkan kerana sistem teknologi maklumat milik agensi kerajaan sentiasa menjadi tumpuan penjenayah siber.

Dengan bilangan pengguna akaun MyGOVUC yang semakin meningkat, MyGOVUC juga tidak terlepas daripada menjadi tumpuan penyerang pancingan data. Menurut rekod, hanya untuk tempoh 9 bulan bermula Mac sehingga November 2022 sahaja, sebanyak 850,203 e-mel pancingan data telah dikesan dan berjaya disekat (MAMPU 2022). Jumlah serangan pancingan data yang tinggi ini menimbulkan

kegusaran sekiranya ia berjaya melepasi tapisan teknologi yang digunapakai, keselamatan maklumat kerajaan seterusnya hanya bergantung kepada benteng terakhir iaitu kemahiran dan pengetahuan pengguna akhir, yang mana tahap kerentanannya masih belum pernah diuji.

Pejabat Setiausaha Kerajaan Negeri Sembilan (PSUKNS) merupakan tunjang kepada perkhidmatan awam bagi pentadbiran kerajaan di Negeri Sembilan. PSUKNS bertanggungjawab secara keseluruhan ke atas pembangunan dan kesejahteraan negeri. Sebagai organisasi teras dalam pembangunan Negeri Sembilan, PSUKNS turut menggunakan kemudahan teknologi maklumat untuk membantu dalam pelaksanaan perkhidmatannya. Hal berkaitan teknologi maklumat PSUKNS dikelola oleh Unit Pengurusan Teknologi Maklumat (UPTM) (Portal Rasmi Kerajaan Negeri Sembilan 2022). Dengan penggunaan teknologi maklumat, PSUKNS tidak terlepas daripada ancaman jenayah siber. Pengurusan maklumat-maklumat kritikal Kerajaan seperti hal pelaburan, pembangunan ekonomi negeri, maklumat sulit berkaitan Majlis Mesyuarat Kerajaan Negeri, data-data berkaitan istana negeri dan juga perihal pengurusan kewangan PSUKNS menjadikan ia sasaran yang menarik penjenayah siber.

Bagi melindungi PSUKNS daripada insiden siber seperti kebocoran maklumat, satu dasar keselamatan berkaitannya telah disediakan. Dasar Keselamatan ICT Pentadbiran Kerajaan Negeri Sembilan 3.0 yang diselaraskan dengan ISO/IEC 27001:2013 Pengurusan Sistem Keselamatan Maklumat telah dikemaskini pada 12 Februari 2019. Dasar Keselamatan ICT ini merangkumi semua perkara berkaitan keselamatan siber di organisasi berkenaan dan dijadikan panduan oleh setiap warga kerja. Namun demikian, walaupun dasar berkaitannya telah disediakan, ancaman jenayah siber tetap ada. Bagi memastikan amalan keselamatan siber yang baik dalam kalangan warga kerja PSUKNS, program-program kesedaran diadakan secara berterusan. Antara bentuk latihan dalam program kesedaran yang biasa dilakukan adalah melalui kaedah ceramah keselamatan yang kurang memberikan kesan berpanjangan kepada kakitangan, dan kursus pendek yang memerlukan komitmen masa daripada kakitangan. Latihan menggunakan kaedah simulasi yang mampu memberikan

kesan serta pengalaman sebenar kepada kakitangan tanpa memerlukan komitmen dari segi masa dan tenaga kakitangan, masih belum pernah dibuat.

Walaupun PSUKNS telah mempunyai polisi dan dasar keselamatan siber yang menyeluruh serta perancangan program-program kesedaran keselamatan yang berterusan, masih terdapat keperluan untuk melaksanakan simulasi umum pancingan data. Ini kerana kajian berbentuk simulasi ini belum pernah dilaksanakan dalam organisasi berkenaan. Pelaksanaannya akan dapat memberikan gambaran dan pengalaman sebenar sesuatu serangan pancingan data kepada warga kerja PSUKNS selain dapat mengukur tahap kesedaran keselamatan siber warga kerja PSUKNS terhadap pancingan data. Kebergantungan kakitangan PSUKNS kepada teknologi anti pancingan data semata-mata juga boleh mengurangkan kepekaan mereka terhadap bahaya ancaman pancingan data. Sekiranya teknologi yang diharapkan itu gagal berfungsi dengan baik, keselamatan maklumat sulit PSUKNS adalah bergantung sepenuhnya kepada kemahiran kakitangan selaku pengguna akhir, yang mana tahap kemahiran dan kesedaran keselamatan mereka terhadap pancingan data masih belum pernah diuji.

1.3 PERSOALAN KAJIAN

Berdasarkan kepada penyataan masalah di atas, terdapat beberapa persoalan kajian yang telah dikenalpasti iaitu:

1. Adakah prosedur simulasi umum pancingan data spesifik boleh digunakan dalam PSUKNS yang menguruskan maklumat kritikal kerajaan negeri?
2. Apakah faktor yang boleh mempengaruhi seseorang personel PSUKNS menjadi mangsa pancingan data?
3. Apakah tahap kerentanan PSUKNS terhadap serangan ancaman pancingan data?

1.4 OBJEKTIF KAJIAN

Objektif berikut telah dibina bagi mencapai matlamat kajian:

1. Menentusahkan kebolehgunaan prosedur simulasi umum pancingan data spesifik dalam organisasi yang menguruskan maklumat kritikal kerajaan negeri;
2. Merekabentuk simulasi pancingan data yang bersesuaian dengan organisasi yang menguruskan maklumat kritikal kerajaan negeri; dan
3. Mengenalpasti tahap kerentanan kakitangan PSUKNS terhadap ancaman pancingan data spesifik serta faktor yang mempengaruhi seseorang personel PSUKNS menjadi mangsa pancingan data.

1.5 SKOP KAJIAN

Skop kajian ini adalah untuk mengukur tahap kesedaran keselamatan penjawat awam dalam sektor kerajaan di Malaysia, khususnya yang menguruskan maklumat kritikal kerajaan seperti PSUKNS, terhadap ancaman pancingan data.

1.6 KEPENTINGAN KAJIAN

Pelaksanaan program kesedaran pancingan data berbentuk simulasi yang dibuat dalam persekitaran sebenar boleh memberi kesan yang lebih efektif kepada kakitangan. Mereka akan dapat merasai sendiri pengalaman kesan kealpaan mereka dan natijah sesuatu serangan pancingan data. Ini akan menjadikan mangsa lebih berhati-hati pada masa akan datang.

Dari perspektif organisasi, simulasi ini dapat membantu untuk mengenalpasti sekiranya terdapat kakitangan yang cenderung untuk menjadi mangsa pancingan data. Soal selidik yang dijalankan pula dapat membantu organisasi untuk mengenalpasti faktor-faktor yang mempengaruhi kecenderungan kakitangan terhadap ancaman pancingan data. Dapatan ini penting untuk dijadikan panduan kepada organisasi dalam usaha merekabentuk kaedah serta pengisian bagi latihan keselamatan siber selanjutnya.

Aktiviti simulasi ini diadakan secara tertib dan beretika mengikut peraturan dan polisi keselamatan PSUKNS sedia ada bagi mengelakkan masalah perundangan serta keadaan panik dan dalam masa yang sama melindungi data milik organisasi.

1.7 ORGANISASI TESIS

Tesis ini mengandungi lima bab utama. Bab I iaitu Pendahuluan memberikan pengenalan ringkas mengenai pancingan data secara umum serta mengenalpasti penyataan masalah, objektif serta skop kajian.

Bab II kajian ini pula mengandungi kajian literatur yang mengupas kajian-kajian terdahulu berkaitan pancingan data, manakala Bab III menerangkan Metodologi yang dilaksanakan untuk menjalankan kajian ini. Kajian ini melibatkan satu sesi simulasi pancingan data dan satu soal selidik sebagai instrumen, bagi mengenalpasti elemen yang mempengaruhi kecenderungan responden terhadap simulasi yang dijalankan.

Dapatan kajian daripada hasil simulasi dan soal selidik tersebut seterusnya dianalisa dan diterangkan dalam Bab IV. Kesimpulan kajian ini secara keseluruhannya dirumuskan dalam Bab V.

BAB II

KAJIAN LITERATUR

2.1 PENGENALAN

Pancingan data adalah satu bentuk penipuan dalam komunikasi digital, bertujuan untuk mendapatkan maklumat sensitif dengan menggunakan kaedah penyamaran sebagai seseorang yang boleh dipercayai. Ia adalah serangan siber yang mempunyai kadar kebolehjayaan yang tinggi, disebabkan pengguna tidak sedar akan kelemahan yang ada pada diri mereka selaku pengguna dan kurang memahami risiko ancaman pancingan data (Desolda et al. 2022). Cabaran utama untuk mencapai satu tahap keselamatan maklumat yang baik adalah untuk menangani elemen yang paling lemah iaitu manusia selaku pengguna akhir. Tindakan memanipulasi pengguna akhir bagi tujuan mendapatkan akses ke atas maklumat sensitif adalah dikenali sebagai kejuruteraan sosial (Steinmetz 2021)dan pancingan data adalah salah satu kaedah kejuruteraan sosial.

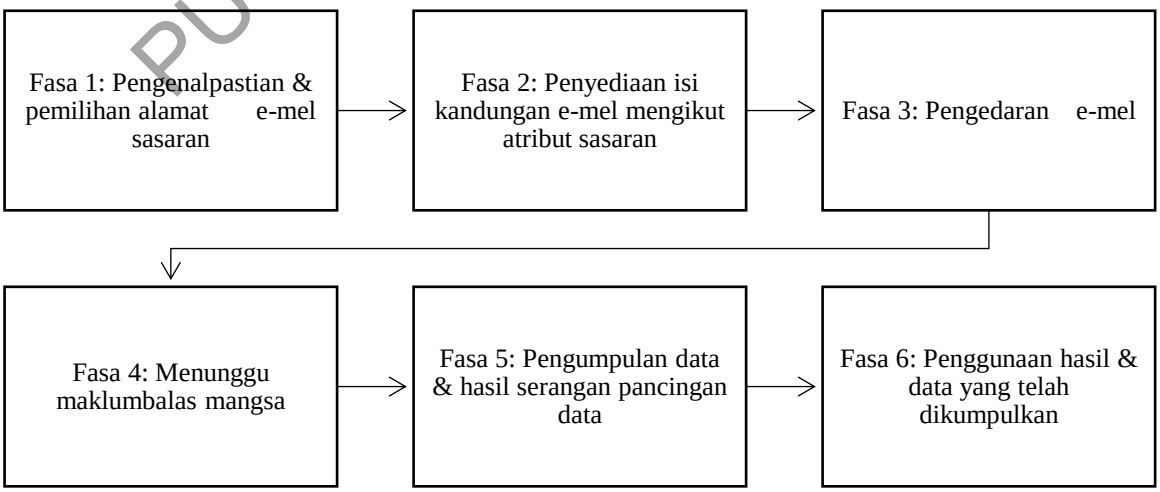
2.2 PANCINGAN DATA SPESIFIK

Pancingan data spesifik atau *spear phishing* adalah satu bentuk serangan yang biasanya menggunakan e-mel sebagai medium saluran untuk berkomunikasi dengan sasaran. Tujuannya adalah untuk memperolehi maklumat peribadi secara tidak sah melalui kaedah penyamaran sebagai seseorang yang berkepentingan dalam organisasi. Serangan ini mempunyai sentuhan peribadi dan ia mensasarkan individu tertentu yang mempunyai sesuatu autoriti yang diperlukan oleh penyerang(Atmojo et al. 2021). Pancingan data spesifik kini semakin berleluasa dan menjadi fokus utama kebanyakkan

organisasi. Dari sudut teknologi, ia murah dan mudah untuk dilaksanakan, justeru ia menjadi pilihan di kalangan penyerang.

Dalam sesuatu serangan pancingan data, penyerang akan menyamar sebagai satu entiti yang sah dan menggunakan saluran berbentuk e-mel untuk mendekati mangsa. Saluran e-mel kerap menjadi pilihan penyerang kerana maklumat mengenai alamat e-mel sasaran yang mudah diperolehi melalui kaedah *web crawling*, iaitu aktiviti mengumpulkan alamat e-mel sasaran daripada laman web. Penyerang seterusnya akan mengedarkan e-mel palsu yang mengandungi pautan tertentu kepada sasaran sebagai umpan. Bergantung kepada atribut sasaran, pautan tersebut akan mengandungi samada 1) pautan kepada satu laman web palsu yang dibangunkan untuk memperdaya mangsa supaya memasukkan maklumat peribadi mereka; atau 2) perisian hasad yang akan dimuat turun dan dipasang pada peranti sasaran tanpa disedari, yang berupaya mengutip maklumat peribadi milik sasaran.

Sesuatu serangan pancingan data terbahagi kepada enam fasa iaitu: 1) pemilihan alamat e-mel sasaran, 2) penyediaan isi kandungan e-mel, 3) pengedaran e-mel kepada sasaran, 4) menunggu maklumbalas daripada sasaran, 5) pengumpulan data dan hasil pancingan data, 6) penggunaan hasil dan data yang telah dikumpulkan (Rastenis et al. 2020).



Rajah 2.1 Kitar hayat serangan pancingan data menggunakan e-mel (Rastenis et al. 2020).

Grant Ho et al. (2017) telah mengkategorikan dua fasa penting dalam memastikan keberjayaan sesuatu serangan pancingan data spesifik menggunakan e-mel. Fasa pertama ialah untuk memikat atau menarik perhatian mangsa. Ini dilakukan melalui kaedah penyamaran sebagai seseorang yang mempunyai autoriti dalam organisasi, bagi mengeksploitasi kepercayaan dan keyakinan sasaran. Secara teknikal, terdapat beberapa kaedah penyamaran yang boleh dilakukan iaitu: 1) *address spoofer* apabila penyerang memanipulasi alamat e-mel dalam *header "From"* e-mel bagi memperlihatkan e-mel tersebut datangnya dari individu yang sah, 2) *name spoofer* apabila penyerang memanipulasi nama pengirim e-mel dalam *header "From"* e-mel bagi memperlihatkan e-mel tersebut datangnya dari individu yang sah, 3) *previously unseen attacker* apabila penyerang memanipulasi nama dan alamat dalam *header "From"* dengan menyamar sebagai satu entiti baru dalam organisasi, dan 4) *lateral attacker* apabila penyerang menggunakan akaun e-mel yang sah tetapi telah dikompromi.

Setelah kepercayaan mangsa diperolehi dalam fasa pertama, fasa kedua adalah eksploitasi kepercayaan yang telah diberikan oleh mangsa. (Grant Ho et al. 2017) mengariskan tiga bentuk eksploitasi yang biasa berlaku iaitu: 1) file *attachment* atau URL yang mengandungi *malware,* 2) URL kepada laman web yang memerlukan mangsa memasukkan maklumat peribadi seperti kata nama dan kata laluan, dan 3) tindakan luar konteks, sebagai contoh; arahan kepada Eksekutif Kewangan untuk membuat pembayaran kepada pembekal yang tidak wujud.

Grant Ho et al. (2017) seterusnya menyatakan bahawa kaedah mitigasi terbaik bagi menangani serangan pancingan data ini adalah dengan memberi tumpuan kepada jurang yang terhasil dalam fasa tindakbalas mangsa terhadap serangan tersebut. Tindakbalas yang dimaksudkan adalah pelaporan daripada mangsa kepada pentadbir teknologi maklumat organisasi. Grant Ho menggambarkan laporan mangsa adalah sebagai satu sumber yang belum tercemar yang mampu menjadi indikator kepada risiko berkaitan e-mel yang mencurigakan, selain ia berkeupayaan untuk mengawal magnitud sesuatu serangan pancingan data spesifik.

Namun, untuk membolehkan mangsa melaporkan sebarang serangan pancingan data spesifik, mereka perlu mempunyai kemahiran dan kepekaan untuk mengenalpasti sesuatu e-mel yang mencurigakan. Latihan dan program kesedaran secara umum sahaja tidak cukup untuk menjadikan mereka kebal terhadap serangan yang sofisikated (Burda, Allodi & Zannone 2020). Justeru, terdapat beberapa bentuk latihan yang lebih berkesan boleh dipertimbangkan seperti kaedah simulasi umum pancingan data spesifik yang mampu memberikan gambaran dan pengalaman sebenar sesebuah serangan kepada pengguna akhir khususnya dan organisasi amnya.

Prosedur simulasi umum pancingan data adalah serupa dengan kaedah serangan pancingan data yang sebenar, namun ia perlu dilakukan secara beretika dalam persekitaran yang terkawal. Ia bertujuan untuk melatih dan mengukur tahap kerentanan pengguna akhir dalam domain kajian, justeru ia perlu mematuhi setiap peraturan yang berkuatkuasa.

2.3 KAJIAN BERKAITAN

Prosedur simulasi pancingan data spesifik bukanlah satu kaedah yang baru. Terdapat pelbagai organisasi dari pelbagai sektor yang telah menggunapakai kaedah ini bagi mengenalpasti golongan kakitangan mereka yang cenderung untuk menjadi mangsa kepada pancingan data. Dari perspektif komersial, terdapat pelbagai produk di pasaran yang boleh diperolehi bagi melaksanakan simulasi pancingan data. Sebagai contoh, Phish Insight (Trend Micro, 2023) dan CanIPhish (Can I Phish Pty Ltd., 2023). Manakala dari pespektif akademia pula, terdapat beberapa kajian yang telah mengadaptasi prosedur umum simulasi pancingan data spesifik untuk mengenalpasti tahap kerentanan pengguna akhir terhadap ancaman pancingan data selain untuk mengukur tahap keberjayaan sesebuah kempen pancingan data dalam pelbagai domain kajian. Kajian-kajian ini telah menghasilkan keputusan yang pelbagai, bergantung kepada objektif masing-masing.

2.3.1 SEKTOR PENDIDIKAN TINGGI

Di kalangan institusi pengajian tinggi dalam Malaysia, salah satu institusi pengajian tinggi yang pernah menjalankan simulasi pancingan data spesifik untuk warga kerjanya adalah Universiti Kebangsaan Malaysia. Norhafizah Abu Bakar (2017) telah menjadikan 553 responden terdiri daripada kakitangan di bawah lima fakulti terpilih dalam institusi berkenaan sebagai populasi kajian untuk menguji tahap kerentanan mereka terhadap ancaman pancingan data. Hasil simulasi telah mencatatkan sebanyak 209 responden terpedaya dengan pancingan data yang dibuat. Soal selidik yang dijalankan seterusnya telah mengenalpasti demografi responden yang dikategorikan kepada bidang S&T dan *non*-S&T. Bidang demografi ini telah dijadikan sebagai faktor yang mempengaruhi respon seseorang mangsa terhadap simulasi serangan pancingan data yang telah dijalankan.

Dari segi magnitud kajian, Siti Zaleha Ahmad (2020) telah melibatkan skala responden yang lebih besar dan menyeluruh pada institusi yang sama. Kajiannya telah melibatkan kesemua 67 buah pusat tanggungjawab di bawah naungan institusi berkenaan dan mengambil 10,000 orang sebagai populasi kajian namun hanya seramai 953 orang responden telah terpedaya dengan kandungan e-mel pancingan data yang dijalankan. Bilangan responden yang rendah berbanding populasi kajian yang tinggi adalah disebabkan simulasi terpaksa diberhentikan lebih awal kerana pasukan penguji simulasi telah menerima laporan aduan yang meningkat secara mendadak dan menyebabkan Prosedur Pengurusan Insiden mengikut piawaian ISO ISMS 27001:2013 terpaksa diaktifkan. Simulasi hanya dapat dijalankan untuk tempoh 2 jam 30 minit sahaja. Walaupun demikian, kajian ini masih dapat mengenalpasti dan menguji faktor berasaskan demografi yang mempengaruhi seseorang menjadi mangsa. Berbeza dengan Norhafizah Abu Bakar (2017), selain daripada untuk mengukur tahap kesedaran keselamatan seluruh populasi kajian, Siti Zaleha Ahmad (2020) juga telah menetapkan objektif untuk membangunkan model mitigasi tahap kesedaran keselamatan siber terhadap serangan pancingan data yang terdiri daripada tiga tahap berbeza dan memberikan fokus kepada mekanisme pendidikan terhadap manusia.

Simulasi pancingan data juga ada dilakukan oleh Yeoh et al. (2022) di salah satu institusi pendidikan tinggi di Australia. Simulasi tersebut telah diadakan sebanyak 6 sesi dalam tempoh 6 bulan iaitu 1 sesi simulasi serangan pancingan data setiap bulan ke atas 10,000 orang populasi kajian. Objektif kajian adalah untuk 1) mengurangkan bilangan responden yang memberi maklumbalas kepada e-mel pancingan data, 2) meningkatkan bilangan responden yang melaporkan kejadian serangan pancingan data dan 3) mengenalpasti kumpulan yang cenderung untuk terpedaya dengan serangan pancingan data. Setiap sesi simulasi tidak merekodkan sebarang maklumat peribadi responden, ini kerana rangka kerja simulator akan merekodkan perilaku penerima terhadap e-mel pancingan data yang diedarkan seperti membuka e-mel, menjawab e-mel, klik pada pautan dalam e-mel atau melaporkan insiden penerimaan e-mel tersebut. Responden yang terpedaya dengan pautan e-mel berkenaan akan dibawa ke satu laman web yang memaparkan video kesedaran tentang kesalahan mereka yang telah terpedaya dengan e-mel pancingan data. Video berkenaan dianggap sebagai sebahagian daripada program kesedaran keselamatan siber dalam kajian ini. Penggunaan pelbagai faktor dalam kajian ini seperti penggunaan topik, isi kandungan dan rekabentuk yang berbeza dalam setiap e-mel pancingan data pada setiap bulan telah membuahkan hasil yang bercampur-campur. Terdapat penurunan dalam bilangan responden yang memberi maklumbalas kepada e-mel pancingan data dan terdapat peningkatan bilangan responden yang melaporkan kejadian serangan pancingan data, bergantung kepada pelbagai faktor. Kajian ini juga secara langsung telah dapat mengenalpasti kumpulan yang cenderung untuk terpedaya dengan serangan pancingan data. Rumusan kajian ini mendapati bahawa pendidikan tentang ancaman pancingan data adalah penting dan perlu dilaksanakan kepada setiap individu dalam organisasi. Keberhasilan metodologi kajian ini juga telah merumuskan bahawa beberapa kitaran latihan atau sesi simulasi boleh memperkukuhkan kesedaran individu terhadap ancaman serangan pancingan data.

2.3.2 SEKTOR MAKANAN DAN PERTANIAN

Satu replikasi Norhafizah Abu Bakar (2017) telah dibuat oleh Muhd Azi Pekeri (2021) dengan populasi kajian yang berbeza iaitu Institut Penyelidikan dan Kemajuan

Pertanian Malaysia (MARDI). Melalui dua sesi simulasi pancingan data ke atas 160 responden, kajian ini telah menilai kesan penggunaan faktor sentimen dalam isi kandungan pancingan data yang diuji. Dapatan kedua-dua sesi simulasi itu menunjukkan bahawa sentimen positif mempunyai kadar kejayaan yang lebih tinggi dan efektif berbanding sentimen negatif. Kajian ini memberikan gambaran bahawa mangsa pancingan data lebih cenderung untuk terpedaya dan mempercayai sumber yang memberikan kandungan yang mengembirakan berbanding kandungan yang berbaur ugutan. Kajian ini juga telah dapat mengenalpasti faktor berasaskan demografi yang mempengaruhi seseorang menjadi mangsa berdasarkan gred jawatan dan lingkungan umur.

2.3.3 SEKTOR TELEKOMUNIKASI

Ahmad Syukri Abdullah (2019) telah mengadaptasi prosedur Norhafizah Abu Bakar (2017) bagi mengkaji kebolehlaksanaan prosedur simulasi umum pancingan data ke atas organisasi di bawah sektor telekomunikasi. Sebanyak 39 responden terlibat dalam pengujian prosedur simulasi umum dan mendapati tiada satu pun responden yang terpedaya dengan e-mel pancingan data umum yang diedarkan. Satu prosedur simulasi spesifik seterusnya dijalankan melibatkan bilangan responden yang sama. Hasil mendapati 12 responden telah memberikan maklumbalas terhadap pancingan data spesifik. Kajian ini telah menambahbaik instrumen kajian berbanding Norhafizah Abu Bakar dengan melaksanakan sesi temu bual bersama Pakar Bidang Khusus bagi mendapatkan perspektif yang lebih holistik terhadap hasil simulasi dan soal selidik. Kajian ini mendapati bahawa sektor telekomunikasi mempunyai kerentanan yang lebih tinggi terhadap pancingan data umum berbanding dengan pancingan data spesifik.

2.3.4 SEKTOR KEWANGAN DAN PERBANKAN

Institusi dalam sektor kewangan juga adalah antara tumpuan ancaman pancingan data. (Chatchalermpun & Daengsi 2021) telah menjalankan satu simulasi pancingan data ke atas 20,300 orang pekerja dalam salah satu institusi kewangan Thailand. Simulasi tersebut telah diadakan sebanyak dua sesi, dengan satu sesi perkongsian maklumat

berkenaan ancaman pancingan data di antara kedua-dua sesi simulasi tersebut. Sesi simulasi pertama adalah tanda aras kepada tahap keselamatan institusi berkenaan, manakala sesi simulasi kedua adalah untuk mengukur tahap keselamatan institusi tersebut selepas diadakan sesi perkongsian maklumat kesedaran. Hasil simulasi pada sesi simulasi kedua menunjukkan pengurangan yang signifikan dan kajian ini merumuskan bahawa sesi perkongsian maklumat yang telah diadakan adalah berkesan untuk melindungi organisasi daripada ancaman pancingan data.

Berdasarkan kepada kajian-kajian terdahulu yang dibincangkan di atas, jadual perbandingan kajian kes berkaitan simulasi pancingan data adalah seperti di Jadual 2.1.

Jadual 2.1 Jadual perbandingan kajian kes berkaitan simulasi pancingan data.

Penulis	Sektor/ Organisasi	Tempoh Simulasi	Teknik	Bilangan Sampel	Bilangan Mangsa	Topik E-mel Pancingan Data
Norhafizah Abu Bakar (2017)	Pendidikan Tinggi/ UKM	3 hari	E-mel secara individu & laman web palsu	553 orang	209 orang	Bayaran Khas Tahun 2016 UKM
Siti Zaleha Ahmad (2020)	Pendidikan Tinggi/ UKM	2 jam 10 minit	E-mel secara berkumpulan & laman web palsu	10,000 orang	953 orang	Pengesahan Markah Akhir SPPU 2017
Yeoh et al. (2021)	Pendidikan Tinggi/ Universiti yang tidak dinamakan di Australia	6 bulan	E-mel secara individu & video kesedaran setiap bulan	10,000 orang	Berkurangan setiap bulan	Pelbagai
Muhd Azi Pekeri (2021)	Makanan & Pertanian/ MARDI	3 hari	E-mel secara individu & laman web palsu	160 orang	100 orang	Sesi I: Bantuan Kewangan
		3 hari			76 orang	Sesi II: Kegagalan Pengesahan Akaun
Ahmad Syukri Abdullah (2019)	Telekomunikasi/ Organisasi yang tidak dinamakan	5 hari	Secara berkumpulan	39 orang	Tiada	Sesi I: Kewangan
		19 hari	Secara individu	39 orang	12 orang	Sesi II: Keselamatan

bersambung..

..sambungan

Chatchalermpun & Daengsi (2021)	Perbankan & Kewangan/ Institusi kewangan yang tidak dinamakan di Thailand	5 bulan	E-mel secara berkumpulan Perkongsian maklumat E-mel secara berkumpulan	20,300 orang	Pengurangan mangsa yang membuka e-mel pancingan data	Sesi I: storan Gmail Sesi II: Shoppee

Merujuk kepada kajian-kajian kes yang telah dikupas di atas, didapati bahawa tahap insiden yang berlaku adalah bercampur-campur. Norhafizah Abu Bakar (2017), Siti Zaleha Ahmad (2020) dan Muhd Azi Pekeri (2021) telah menjalankan simulasi pancingan data ke atas institusi pendidikan tinggi dan institusi penyelidikan sebagai populasi kajian dalam tempoh yang singkat. Yeoh et al. (2022) dan Chatchalermpun & Daengsi (2021) pula telah menjalankan kajian pada populasi yang besar dengan tempoh yang lebih lama. Dapatan kajian serta hasil analisis demografi juga adalah berbeza, bergantung kepada pelbagai faktor dalam kajian.

Kajian-kajian di atas juga telah menggunakan pelbagai topik sebagai isi kandungan e-mel pancingan data sebagai faktor untuk mempengaruhi populasi kajian agar terpedaya. Muhd Azi Pekeri (2021) telah menggunakan dua topik e-mel untuk mengukur pengaruh sentimen isi kandungan e-mel pancingan data ke atas populasi kajiannya dan membezakan antara sentimen yang mengembirakan atau sentimen ugutan. Yeoh et al. (2022) turut menggunakan topik dan isi kandungan e-mel pancingan data yang pelbagai dalam 6 siri simulasi yang dijalankan. Isi kandungan yang dekat dengan persekitaran populasi kajiannya memberikan tahap insiden yang lebih tinggi berbanding isi kandungan yang tiada kena mengena dengan persekitaran populasi kajian. Pemilihan isi kandungan adalah penting dalam mempengaruhi mangsa dan untuk menentukan tahap insiden dalam kajian ini.

Dalam kajian lain, Jagatic et al. (2005) dan Abroshan et al. (2021) merumuskan bahawa kumpulan umur yang lebih muda antara 18 hingga 25 tahun dianggap lebih terdedah dan cenderung untuk terpedaya dengan serangan pancingan data. Ini kerana individu dalam golongan umur ini dikatakan lebih impulsif, jarang membuat

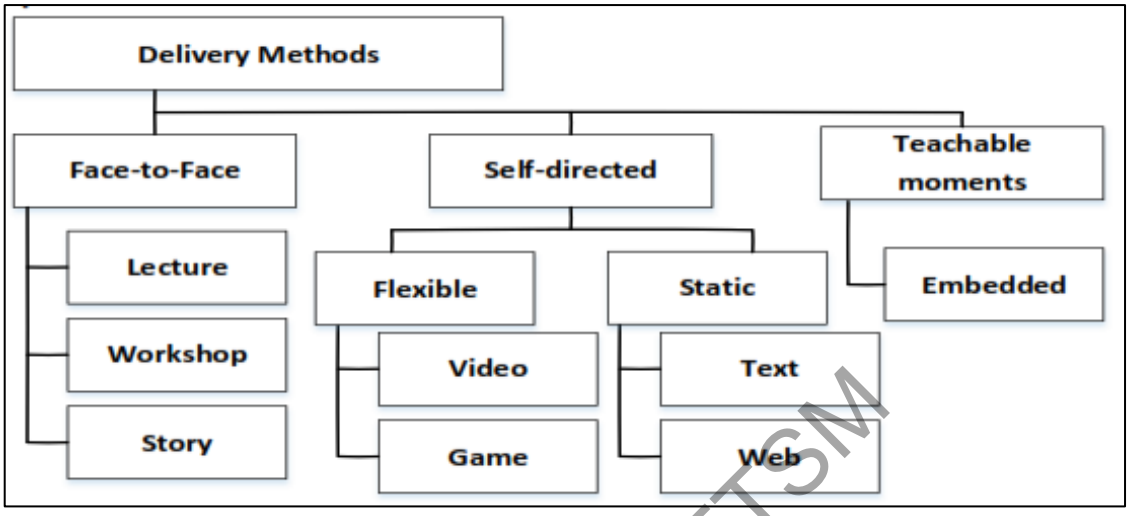
pertimbangan yang betul sebelum membuat keputusan. Golongan umur ini juga kurang pendedahan kepada latihan terhadap keselamatan siber menyebabkan mereka lebih mudah terdedah kepada serangan pancingan data. Rumusan ini berbeza dengan dapatan Hanis Binti Tuan Kob, Rahim & Azman (2020) yang mendapati tiada faktor tetap yang boleh menyebabkan seseorang untuk menjadi mangsa kepada serangan pancingan data. Hanis Binti Tuan Kob, Rahim & Azman (2020) juga mendapati faktor demografi tertentu seperti umur, jantina serta pengetahuan responden tentang teknologi maklumat tidak memberi kesan kepada keterdedahan ke atas serangan pancingan data. Namun demikian metodologi Hanis Binti Tuan Kob, Rahim & Azman (2020) dalam mendapatkan populasi kajian adalah lemah memandangkan magnitud dan kebolehgantungan data populasi kajian yang rendah. Muhd Azi Pekeri (2021) mendapati faktor demografi gred jawatan dari kumpulan pelaksana dan faktor kumpulan umur antara 31 tahun sehingga 45 tahun adalah kumpulan rentan yang berkecenderungan tinggi untuk terdedah dan memberi respon kepada serangan pancingan data. Berdasarkan kepada perbahasan ini, satu penyataan kajian dapat dibina seperti berikut:

Penyataan Kajian$_1$= Kajian menjangkakan akan terdapatnya elemen yang mempengaruhi insiden pancingan data di domain kajian.

2.3.5 SIMULASI SEBAGAI PENDIDIKAN KEPADA PENGGUNA AKHIR

Sebagai benteng terakhir dalam usaha mencegah pancingan data, kelemahan manusia perlu diberikan perhatian. Bagi tujuan ini, kognitif manusia perlu didedahkan dan dilatih dengan ilmu serta kemahiran yang berkaitan ancaman pancingan data. Justeru, program-program intervensi yang dapat meningkatkan kesedaran manusia perlu dilaksanakan secara berterusan. Terdapat pelbagai kaedah untuk menyampaikan ilmu serta latihan berkaitan keselamatan siber umumnya dan pancingan data khususnya. Kaedah ini bergantung kepada kemampuan organisasi dan juga keupayaan kakitangan yang terlibat untuk menerima kaedah berkenaan. Alhashmi et al. (2021) telah mengelaskan kaedah penyampaian program latihan yang bersesuaian kepada tiga kelas iaitu 1) secara bersemuka melalui syarahan, penganjuran bengkel dan juga penceritaan, 2) melalui hubungan langsung yang boleh dilakukan secara fleksibel seperti tayangan

video dan permainan, atau secara statik iaitu melalui penggunaan bahan bacaan atau laman web, dan 3) menggunakan pembelajaran berasaskan pengalaman seperti kaedah simulasi sewaktu dalam proses kerja harian.



Rajah 2.2 Klasifikasi kaedah penyampaian latihan kesedaran siber oleh Alhashmi et al. (2021).

Alhashmi et al. (2021) telah merumuskan bahawa kaedah pembelajaran berasaskan pengalaman akan dapat membantu dan memberi kesan yang lebih kepada kakitangan berbanding kaedah penyampaian yang lain. Ini seiring dengan Kumaraguru et al. (2010) yang telah menggariskan antara cabaran dalam memberikan latihan adalah kakitangan yang tidak mempunyai motivasi untuk menjalani latihan yang dirangka khusus berkaitan keselamatan siber. Kakitangan menganggap perkara latihan berkaitan keselamatan adalah tugasan sekunder dan mereka lebih mengutamakan tugasan hakiki. Ini menyebabkan latihan melalui kaedah bersemuka dan hubungan langsung sukar untuk dilaksanakan bagi mencapai objektif melatih iaitu untuk meningkatkan tahap keselamatan tanpa meningkatkan kecenderungan kakitangan untuk tersilap sewaktu membezakan ancaman. Rumusan ini juga selari dengan hasil soal selidik yang dijalankan oleh Norhafizah Abu Bakar (2021) yang menunjukkan 88.3% respondennya bersetuju bahawa simulasi serangan pancingan data spesifik ini meningkatkan kesedaran keselamatan siber mereka.

Berdasarkan kepada pernyataan ini, kaedah simulasi dilihat sebagai kaedah yang bersesuaian untuk mendidik kakitangan dalam sektor kerajaan kerana ia memberi kesan

dan pengalaman yang sebenar, tidak mengambil masa kakitangan dengan terlalu lama dan tidak memerlukan motivasi serta komitmen kakitangan secara langsung. Namun keberkesanannya ke atas sektor kerajaan yang menguruskan maklumat kritikal kerajaan negeri masih belum pernah diuji. Bagi PSUKNS, pada masa kajian ini dijalankan, latihan mengenai keselamatan siber yang biasa dilaksanakan adalah berbentuk kursus jangka pendek. Disebabkan kekangan logistik, latihan berbentuk kursus ini hanya mampu melibatkan bilangan kehadiran peserta dalam kumpulan yang kecil. Kehadiran calon juga adalah tertakluk kepada persetujuan Ketua Bahagian atau Ketua Unit masing-masing. Ini menyebabkan keberkesanan kursus adalah terhad dan liputan latihan juga adalah tidak menyeluruh.

2.4 RUMUSAN

Pancingan data adalah satu bentuk penipuan dalam talian yang semakin berleluasa. Ia telah menyebabkan kerugian yang besar setiap tahun. Berasaskan kepada kejuruteraan sosial, ia fokus untuk memanipulasi kelemahan manusia sebagai pengguna akhir. Program kesedaran dan latihan perlu dijalankan secara berterusan bagi memerangi ancaman pancingan data. Namun demikian, pelaksanaan program kesedaran ini menghadapi cabaran kerana kakitangan dalam sesebuah organisasi sentiasa menganggap isu keselamatan siber ini sebagai perkara yang tidak penting. Justeru, pendekatan latihan melalui kaedah simulasi dijangka akan dapat memberikan kesan dalam meningkatkan daya tahan kakitangan terhadap ancaman data, tanpa memerlukan komitmen yang tinggi daripada mereka. Kajian-kajian lepas yang mengadaptasi kaedah simulasi dalam pancingan data menunjukkan terdapat kesan langsung yang signifikan kepada domain kajian.

BAB III

METODOLOGI

3.1 PENGENALAN

Bab III ini menerangkan metodologi yang digunakan bagi memastikan pelaksanaan kajian yang lebih berstruktur.

Metodologi kajian ini melibatkan empat fasa iaitu 1) kajian teoritikal, 2) kajian emperikal, 3) kajian sebenar dan 4) penilaian dengan mengadaptasi rangka kerja Siti Zaleha Ahmad (2020). Ia turut mengadaptasi rangka kerja simulasi Norhafizah Abu Bakar (2017) dan menyesuaikannya kepada cara kerja organisasi kajian. Ringkasan aktiviti dalam setiap fasa beserta hasilnya adalah seperti Jadual 3.1.

Jadual 3.1 Ringkasan aktiviti dan hasil dalam Metodologi Kajian.

Fasa	Aktiviti	Hasil
1: Kajian Teoritikal	• Menjalankan kajian literasi dengan menyemak kajian-kajian terdahulu yang berkaitan. • Mengenalpasti instrumen dan merancang rangka kerja simulasi o Langkah I: Persediaan dan Kelulusan o Langkah II: Perancangan	• Mencapai objektif pertama kajian • Pernyataan masalah kajian • Objektif & Skop kajian • Kelulusan dasar daripada organisasi • Penubuhan pasukan penguji • Cadangan rangka kerja kajian dan simulasi.

bersambung..

..sambungan

2: Kajian Emperikal	• Melaksanakan kajian emperikal dengan membangunkan dan menguji instrumen simulasi dan soal selidik
	  o Penyesuaian dan penambahbaikan simulasi dan soal selidik
	• Merekabentuk poster bagi kempen kesedaran
	• Menentukan populasi dan sampel kajian
	  o Populasi: 368 kakitangan
	  o Sampel: 278 kakitangan bergred 19 sehingga 52 sahaja
		• Mencapai objektif kedua kajian.
		• Poster kempen kesedaran
		• Topik pancingan data
		• Laman web palsu simulasi
		• Platfom simulasi pancingan data
		• Set soal selidik

3: Kajian Sebenar	• Melaksanakan kempen kesedaran
	• Melaksanakan simulasi
	  o Implementasi Langkah III: Pelaksanaan
	• Melaksanakan soal selidik
	  o Implementasi Langkah IV: Pasca Simulasi
	• Pengumpulan data dan analisis simulasi
	  o Respon sampel melalui Gophish
	  o Demografi melalui semakan silang dengan portal rasmi organisasi
	• Pengumpulan data dan analisis soal selidik pasca simulasi
	  o Kempen kesedaran
	  o Aktiviti simulasi
	  o Persepsi pengguna
		• Implementasi simulasi pancingan data dan soal seldik
		• Mengenalpasti kelompok yang paling cenderung menjadi mangsa pancingan data serta faktor yang mempengaruhi

4: Penilaian	• Penulisan laporan
	  o Ringkasan penemuan
	  o Penilaian dapatan simulasi dan soal selidik
		• Mencapai objektif ketiga kajian

3.2 FASA 1: KAJIAN TEORITIKAL

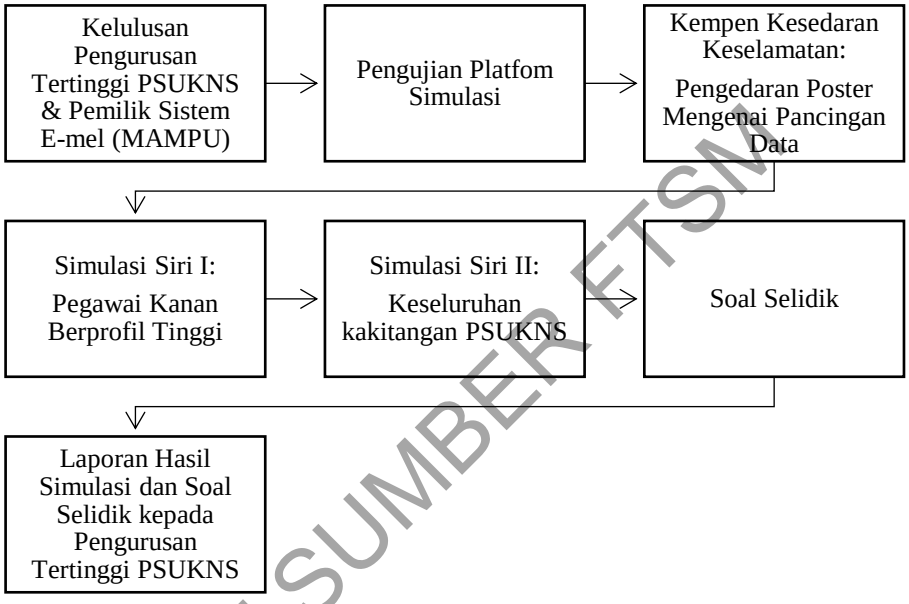
Kajian dimulakan dengan menjalankan sorotan susastera secara bersistematik ke atas kajian-kajian berkaitan terdahulu dan menyesuaikannya dengan keadaan semasa. Ini untuk mendapatkan pernyataan masalah, objektif serta skop kajian seperti yang telah dikupas dalam Bab I. Teknik penggunaan dan faktor penyumbang penggunaan kaedah kes dalam kajian-kajian terdahulu telah diringkaskan dan dikupas pula dalam Bab II. Keseluruhan aktiviti dalam Fasa 1: Kajian Teoritikal ini telah membantu dalam menyediakan rangka kerja bagi pelaksanaan kajian yang lebih teratur.

Melalui kajian teoritikal ini, dua instrumen penting telah dapat dikenalpasti bersesuaian untuk digunakan bagi mendapatkan data kajian iaitu simulasi dan soal selidik. Langkah-langkah pembangunan simulasi Norhafizah Abu Bakar (2017) telah dikenalpasti dan disesuaikan pelaksanaannya. Ia melibatkan empat langkah utama iaitu 1) Langkah I: Persediaan dan Kelulusan, 2) Langkah II: Perancangan, 3) Langkah III: Pelaksanaan dan 4) Langkah IV: Pasca Simulasi. Dua langkah pertama iaitu Langkah I dan II dilaksanakan dalam Fasa 1: Kajian Teoritikal, manakala Langkah III dan Langkah IV dijalankan dalam Fasa 3: Kajian Sebenar.

Setelah pernyataan masalah, objektif dan skop serta instrumen kajian dikenalpasti, kelulusan dasar daripada organisasi kajian perlu diperolehi bagi membolehkan kajian serta instrumen yang dirancang dapat dilaksanakan dengan teratur dan beretika. Kelulusan ini adalah penting kerana ia merupakan keputusan dasar yang menjadi punca kuasa kepada pelaksanaan kajian ini.

Kajian ini dilaksanakan dalam keadaan pasca Covid 19, justeru permohonan kelulusan daripada pengurusan tertinggi organisasi telah dilaksanakan melalui permohonan secara e-mel yang lengkap menerangkan tujuan, objektif serta skop kajian, cadangan tarikh kajian termasuk untuk aktiviti simulasi dan soal selidik, serta kebaikan kajian kepada organisasi.

Bersandarkan kepada kelulusan dasar berkenaan, satu pasukan penguji ditubuhkan dan perbincangan dengan pasukan penguji perlu diadakan bagi menyediakan rangka kerja simulasi selain mendapatkan input tentang keperluan teknikal simulasi dan pilihan topik-topik pancingan data yang bersesuaian. Ini kerana simulasi perlu dirangka dengan teliti supaya ia dapat dilaksanakan dengan tertib, beretika serta mematuhi peraturan yang berkuatkuasa. Ia juga perlu dirancang dengan kemas supaya tidak menganggu rutin operasi harian organisasi kajian.



Rajah 3.1 Rangka kerja simulasi pancingan data di PSUKNS.

Bagi membangunkan cadangan rangka kerja simulasi ini, dua langkah pembangunan instrumen simulasi telah dilaksanakan dalam Fasa 1 ini iaitu 1) Langkah I: Persediaan dan Kelulusan, dan 2) Langkah II: Perancangan.

3.2.1 Langkah I: Persediaan dan Kelulusan

Pasukan penguji yang ditubuhkan perlu terdiri daripada beberapa orang Pegawai Teknologi Maklumat khususnya yang bertanggungjawab ke atas infrastruktur sistem e-mel organisasi. Bilangan ahli pasukan penguji ini adalah kecil dan terhad serta perlu dirahsiakan bagi mengekalkan unsur kejutan dalam simulasi yang akan dilaksanakan.

Bagi tujuan kerahsiaan, Perjanjian Kerahsiaan Maklumat perlu dipersetujui dan ditandatangani oleh setiap ahli pasukan penguji.

Memandangkan perkhidmatan sistem e-mel yang digunakan oleh kebanyakan organisasi kerajaan kini telah dipusatkan dan dikawal selia oleh MAMPU, persetujuan dan kelulusan dari pihak berkenaan juga adalah diperlukan. Ini adalah penting kerana teknologi kecerdasan buatan (AI) yang digunakan pada sistem e-mel organisasi kerajaan pada masa ini telah mempunyai ciri-ciri keselamatan yang tinggi untuk mencegah serangan siber termasuk ancaman pancingan data. Persetujuan MAMPU untuk memasukkan e-mel pancingan data simulasi ke dalam *Whitelist* adalah sangat penting bagi memastikan e-mel tersebut masuk ke dalam *Inbox* dan bukan dalam folder *Spam*.

3.2.2 Langkah II: Perancangan

Setelah kelulusan daripada semua pihak diperolehi, perancangan untuk membangunkan instrumen simulasi perlu disediakan. Bagi tujuan ini, terdapat dua perkara penting yang perlu diberi perhatian iaitu 1) keperluan teknikal yang akan digunakan untuk menghantar e-mel yang seterusnya akan merekodkan respon sasaran dan 2) perincian e-mel pancingan data itu sendiri.

1. Keperluan teknikal

Memandangkan perkhidmatan sistem e-mel yang digunapakai oleh sektor kerajaan telah mempunyai ciri-ciri keselamatan yang tinggi menggunakan teknologi AI dan melibatkan penapisan yang ketat oleh pihak MAMPU, perhatian yang teliti perlu diberikan dalam menentukan a) platfom simulasi, b) pelayan e-mel pancingan data serta c) pelayan dan rangkaian yang digunakan untuk simulasi.

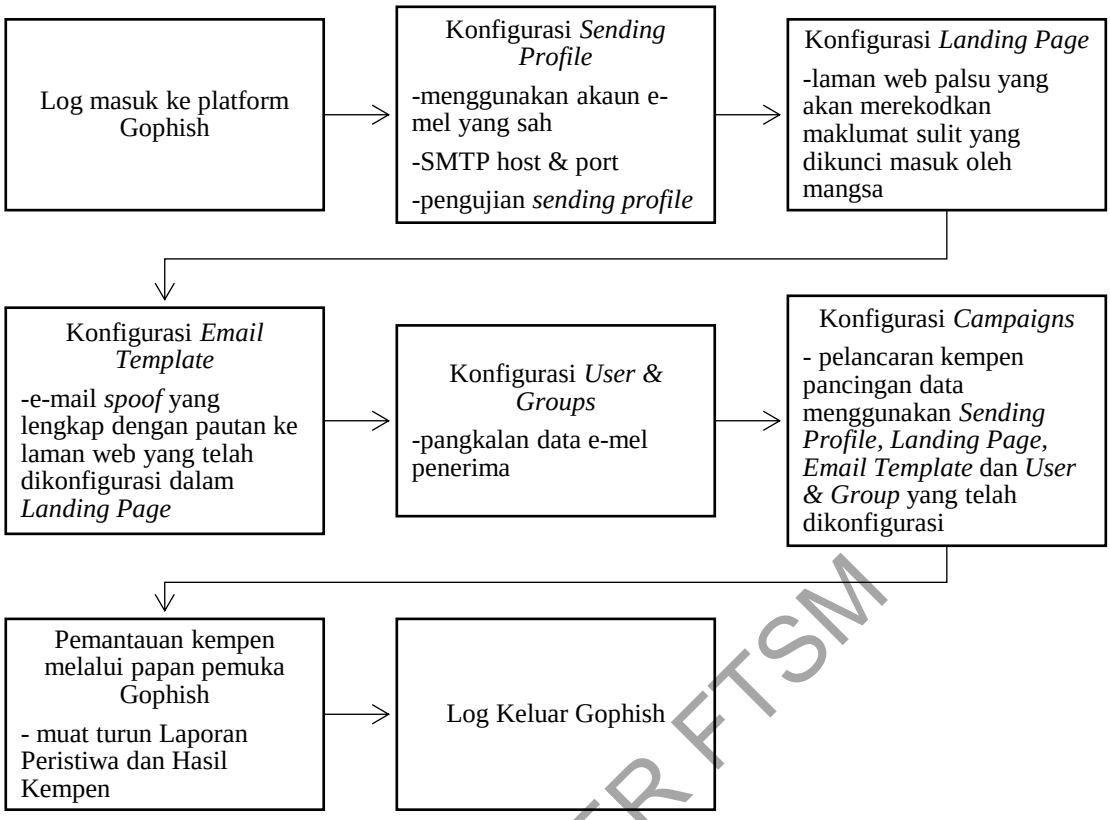
a. Platform simulasi: Gophish

Bagi memantau dan mendapatkan laporan yang terperinci mengenai pergerakan e-mel pancingan data yang dilancarkan, simulasi ini menggunakan platform simulasi Gophish. Gophish adalah satu perisian *open-source* yang boleh dimuat turun secara percuma dan mempunyai konfigurasi yang mudah. Mohd Azi Pekeri (2021) turut menggunakan platfom ini dalam kajiannya.

Selain daripada menyediakan kemudahan untuk memantau pergerakan e-mel dan respon penerima e-mel pancingan data melalui papan pemuka yang disediakan, kelebihan platform ini ialah ia menyediakan menu untuk konfigurasi kempen pancingan data dengan mudah. Ini termasuk konfigurasi pangkalan data e-mel sasaran, pembangunan laman web palsu dan penyediaan e-mel *spoof* yang lengkap dengan pautan ke laman web palsu.

Gophish turut menyediakan konfigurasi yang mudah untuk memilih maklumat sulit yang ingin direkodkan daripada laman web palsu pancingan data tersebut. Namun demikian, Gophish memerlukan satu akaun e-mel yang sah untuk mengedarkan e-mel *spoof*. Pemilihan akaun e-mel yang sah ini adalah sangat penting kerana kebanyakan pelayan e-mel komersial pada masa kajian ini dijalankan, tidak membenarkan pengiriman e-mel menggunakan platfom pihak ketiga seperti Gophish.

Platfom ini turut mempunyai kelebihan iaitu walaupun e-mel pancingan dihantar secara berkumpulan, mangsa hanya akan menerima e-mel tersebut secara individu. Ini memberi lebih keyakinan dan peluang keberjayaan yang lebih tinggi kerana e-mel yang dihantar memiliki elemen sentuhan peribadi.



Rajah 3.2 Proses kerja konfigurasi dan kempen pancingan data Gophish.

Laporan Peristiwa dan Laporan Hasil Kempen yang dijana oleh Gophish seterusnya membantu dalam mengenalpasti bentuk respon yang diterima. Laporan-laporan yang dihasilkan mengandungi maklumat 1) bilangan responden yang membuka e-mel, 2) bilangan responden yang klik pada pautan dan 3) bilangan responden yang mengunci masuk maklumat sulit ke laman web palsu. Manakala bilangan responden yang membuat laporan akan diperolehi daripada Pentadbir E-mel dan juga watak pengirim e-mel.

Bagi memastikan pelaksanaan simulasi ini dilaksanakan dengan beretika dan melindungi setiap data peribadi yang dikutip, konfigurasi *Landing Page* ditetapkan pada pilihan untuk mengutip alamat e-mel sahaja dan tidak merekod kata laluan yang dimasukkan oleh mangsa.

b. Pelayan e-mel pancingan data

Ahmad Syukri Abdullah (2019) telah mewujudkan satu akaun e-mel palsu bagi tujuan *spoofing* dan e-mel diedarkan serentak kepada setiap responden secara individu. Ia mudah dilakukan kerana kajiannya hanya melibatkan 39 responden. Bagi kajian yang melibatkan bilangan responden yang ramai, ia sukar dilakukan kerana limitasi pelayan e-mel komersial pada masa kajian ini dijalankan telah mengehadkan penghantaran e-mel kepada maksimum hanya 100 penerima sahaja dalam sehari.

Untuk mengelak daripada digagalkan oleh teknologi AI pada sistem e-mail MyGOVUC, dua akaun e-mel daripada dua pelayan e-mel yang berbeza telah digunakan bagi tujuan pengujian.

Jadual 3.2 Ketetapan pelayan e-mel bagi kedua-dua akaun e-mel.

	Akaun e-mel I	Akaun e-mel II
Akaun e-mel *Sending Profile*	albatros@heartsgourmet.com.my	no_reply@sigmasfera.com
Host pelayan e-mel	mail.heartsgourmet.com.my	mail.sigmasfera.com
Port	27	587

Kedua-dua akaun e-mel yang digunakan ini adalah akaun e-mel yang sah dan diwujudkan khas bagi tujuan simulasi. Kedua-dua akaun e-mel ini adalah daripada pelayan e-mel persendirian yang tidak mempunyai limitasi seperti pelayan e-mel komersial yang lain.

c. Pelayan dan rangkaian

Bagi memastikan kejayaan simulasi, pemilihan pelayan untuk Gophish dan rangkaian yang digunakan adalah penting dalam menjaga kerahsiaan maklumat yang dikutip oleh Gophish. Mengikut perancangan asal sewaktu perundingan dengan pasukan penguji, pasukan penguji telah bersetuju untuk menyediakan pelayan berbentuk mesin maya (VM) yang dihubungkan menggunakan rangkaian peribadi maya (VPN). Melalui

kaedah ini, Gophish dapat dimuat turun pada VM dan boleh dicapai menggunakan rangkaian VPN. Namun demikian, ketetapan ini tidak bersesuaian dengan mesin yang digunakan bagi tujuan simulasi ini kerana penggunaan VPN pada mesin penguji telah menyebabkan Skrin Biru Mati (BSOD). Justeru, pasukan penguji seterusnya bersetuju supaya simulasi ini dijalankan menggunakan pelayan persendirian serta rangkaian terbuka yang dipercayai. Bagi tujuan ini, Perjanjian Kerahsiaan turut ditandatangai oleh pengendali pelayan yang berkenaan.

2. Perincian E-Mel Pancingan Data

Serangan pancingan data spesifik dibina khusus untuk organisasi yang menjadi domain sasaran. Ia mempunyai perbezaan yang signifikan dengan pancingan data umum, memandangkan ia mempunyai sentuhan peribadi serta penggunaan gaya bahasa yang lebih menyakinkan bagi mengeksploitasi kognitif sasaran, dalam usaha memastikan kadar keberjayaan yang lebih tinggi (Burda, Allodi & Zannone 2020).

Secara amnya, setiap kakitangan kerajaan perlu patuh dan tertakluk kepada Akta Rahsia Rasmi 1972. Namun, dalam sesebuah organisasi kerajaan, kumpulan perkhidmatan yang bertanggungjawab secara langsung dalam pengurusan maklumat kritikal adalah terdiri daripada kumpulan Pengurusan & Profesional. Bergantung kepada jawatan, pegawai Pengurusan & Profesional akan dilantik sebagai Pegawai Pengelas di bawah Seksyen 2B Akta Rahsia Rasmi 1972 yang memberi tanggungjawab kepada pegawai tersebut untuk menilai sama ada sesuatu dokumen perlu diberi peringkat kerahsiaan mengikut tafsiran dalam Arahan Keselamatan, memberi tanda dokumen mengikut peringat dan mendaftarkan dokumen terperingkat dalam buku daftar berkaitan. Peranan ini memerlukan kepekaan pegawai Pengurusan & Profesional sewaktu menguruskan setiap dokumen milik organisasi. Justeru, kajian ini akan melibatkan kumpulan Pengurusan & Profesional sebagai sasaran tanpa mengenepikan kumpulan Pelaksana yang turut berurusan dengan dokumen atau maklumat terperingkat secara tidak langsung.

Komponen utama yang perlu diberi perhatian dalam memastikan kadar keberjayaan simulasi ini adalah a) pemilihan topik, b) kandungan e-mel dan c) petunjuk e-mel yang mencurigakan.

a. Pemilihan topik

Pada peringkat awal perancangan, simulasi telah dirancang untuk dijalankan sebanyak dua siri. Topik yang dipilih bagi kedua-dua siri simulasi adalah berkaitan dengan Persidangan Dewan Undangan Negeri yang akan berlangsung pada waktu berkenaan. Namun demikian, disebabkan beberapa keperluan teknikal yang masih belum tersedia menjelang tarikh persidangan, topik bagi kedua-dua siri telah ditukar dan disesuaikan mengikut keperluan.

Jadual 3.3 Topik yang dicadang untuk simulasi.

	Pancingan data Siri I	Pancingan data Siri II
Sasaran	15 orang pegawai kanan	386 orang pegawai dan kakitangan
Topik Asal	Mustahak: Pengemaskinian Maklumat Bagi Tujuan Pengedaran Dokumen Terperingkat Bagi Persidangan Dewangan Undangan Negeri	Penting: Pemberian Bonus Tahun 2023.
Topik Baru	Mustahak: Pengemaskinian Maklumat Bagi Tujuan Pengedaran Dokumen Mesyuarat Ketua-ketua Jabatan	Penting: Pemberian Bantuan Persekolahan Tahun 2023.

b. Kandungan e-mel

Kandungan e-mel yang digunakan mempunyai sentuhan peribadi serta penggunaan gaya bahasa yang menyakinkan bagi mengeksploitasi kognitif sasaran. Ia juga mempunyai sifat mendesak, segera dan penting untuk memperdaya populasi memberi respon tanpa berfikir panjang. Namun demikian, mengambilkira faktor demografi

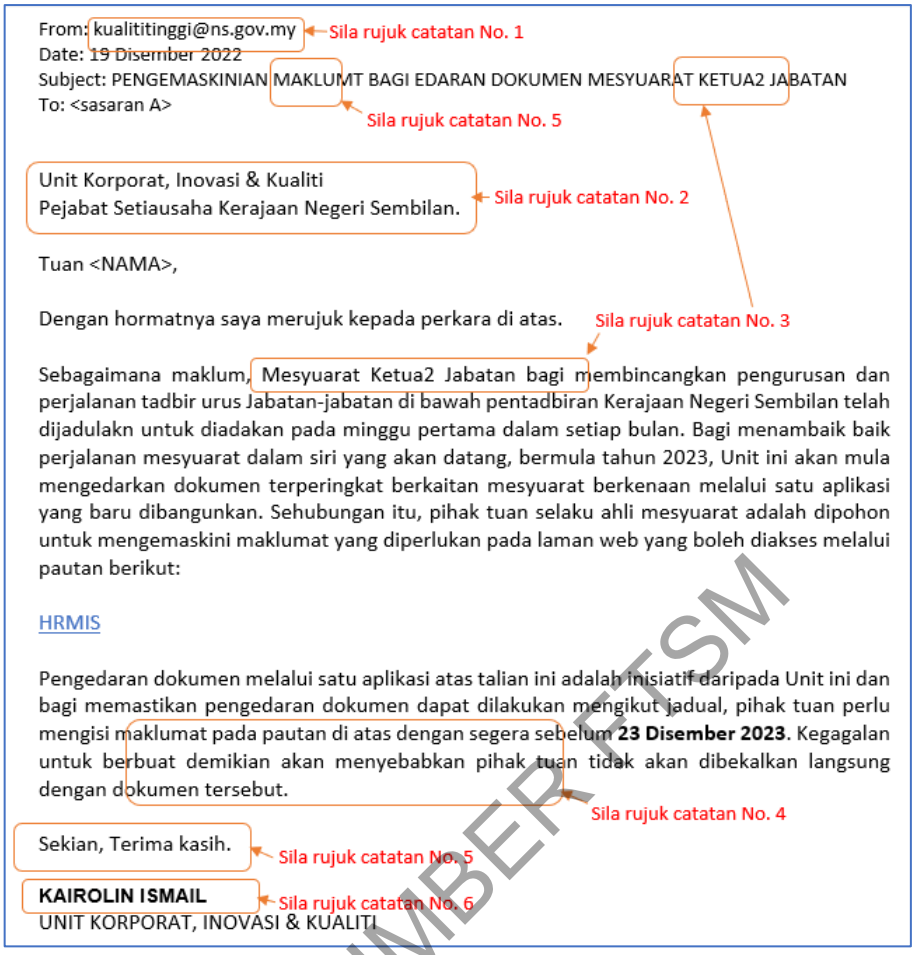
populasi yang diuji iaitu dua kumpulan perkhidmatan yang menguruskan maklumat kritikal kerajaan negeri, kedua-dua isi kandungan e-mel ini juga secara dasarnya adalah untuk menguji kepekaan responden memandangkan ia melibatkan satu program berimpak tinggi yang sekiranya benar-benar berlaku, program itu akan dihebahkan melalui pekeliling dalaman atau forum rasmi seperti mesyuarat dan portal rasmi organisasi.

c. Petunjuk e-mel yang mencurigakan

Terdapat beberapa petunjuk e-mel yang mencurigakan dimasukkan ke dalam e-mel pancingan data bagi simulasi ini bagi menguji kepekaan sasaran. Memandangkan kedua-dua e-mel pancingan data ini menggunakan watak yang wujud dalam organisasi, skrip asas bagi menjawab sebarang pertanyaan daripada populasi telah disediakan untuk rujukan kedua-dua personel tersebut dan juga Pentadbir E-mel.

Jadual 3.4 Catatan bagi penerangan kepada Petunjuk e-mel mencurigakan bagi Siri I.

No.	Catatan
1	Alamat e-mel yang mencurigakan.
2	Format e-mel rasmi tidak memerlukan alamat pengirim dimasukkan dalam permulaan e-mel.
3	Secara rasminya, nama mesyuarat yang dimaksudkan ialah Mesyuarat Ketua-ketua Jabatan, Pejabat Setiausaha Kerajaan Negeri Sembilan. Penggunaan kata ringkas bagi tujuan ini menjejaskan formaliti e-mel berkenaan.
4	Elemen desakan dan ugutan.
5	Kesilapan ejaan.
6	Nama sebenar Ketua Unit Korporat, Inovasi dan Kualiti adalah Khairolin Binti Ismail.
7	Kesalahan ejaan bagi e-mel ini adalah minimal dan tatabahasa yang digunakan adalah bersesuaian dengan penggunaan e-mel rasmi. Ini bagi menguji ketelitian dan kepekaan penerima yang merupakan pegawai kanan yang berurusan rapat dengan dokumen-dokumen terperingkat.

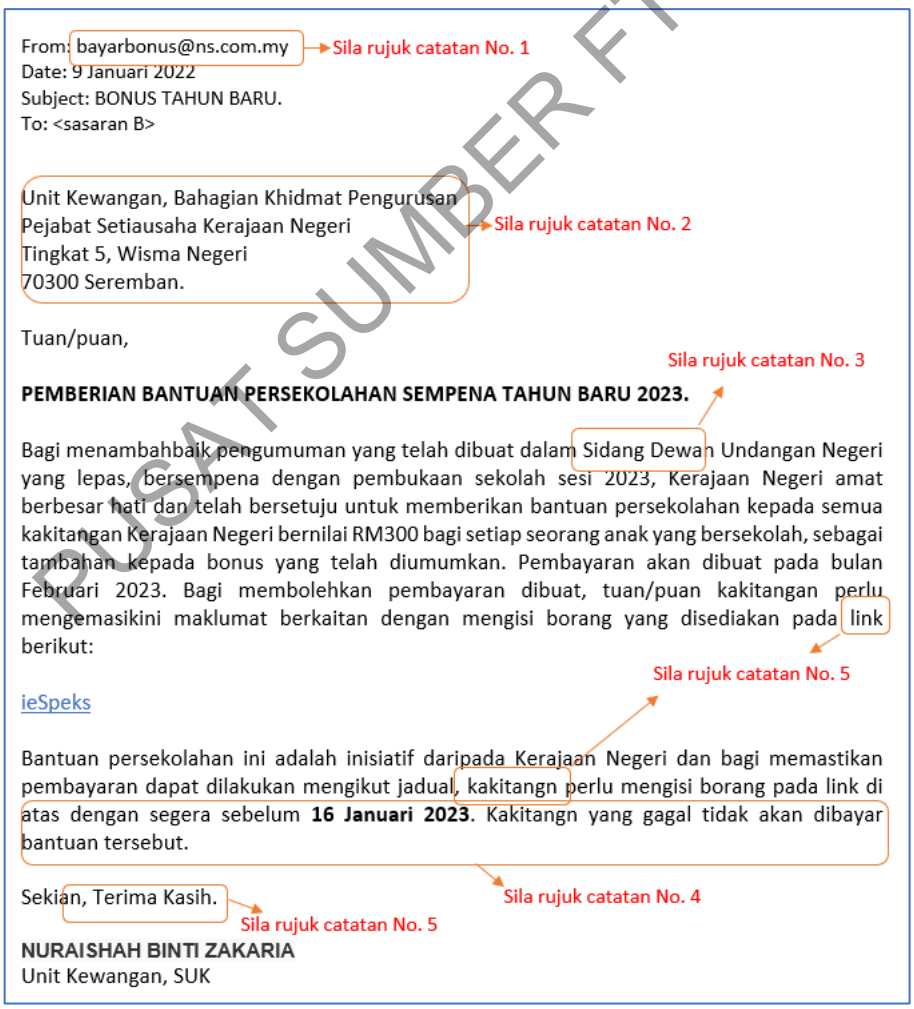


Rajah 3.3 Petunjuk e-mel yang mencurigakan bagi Siri I.

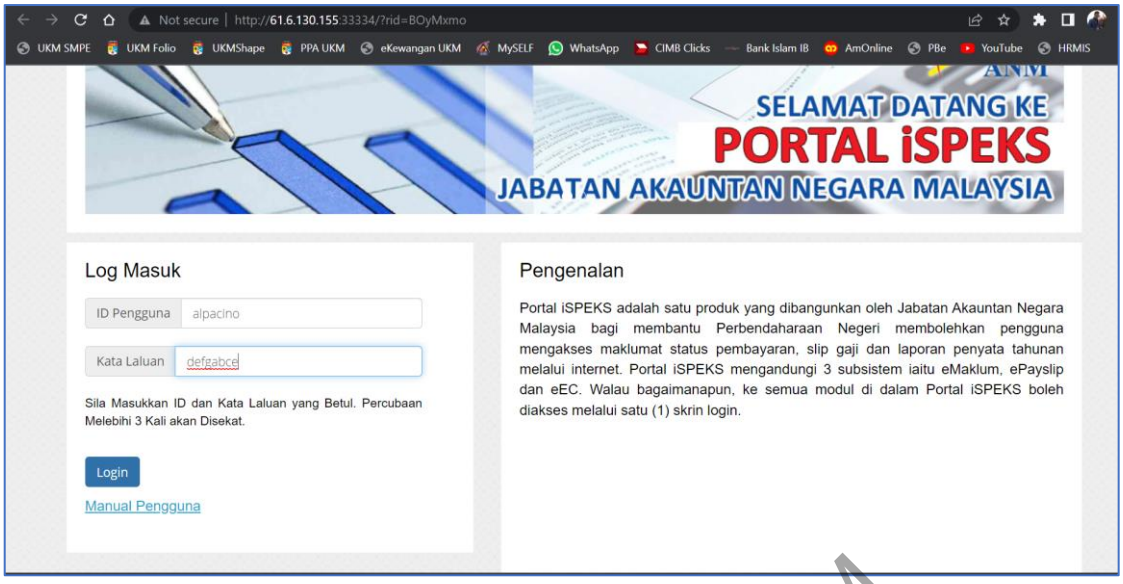
Rajah 3.4 Tangkap Layar Laman Web Palsu Untuk Simulasi Siri I.

Jadual 3.5 Catatan bagi penerangan kepada Petunjuk e-mel mencurigakan bagi Siri II.

No.	Catatan
1	Alamat e-mel yang mencurigakan.
2	Format e-mel rasmi tidak memerlukan alamat pengirim dimasukkan dalam permulaan e-mel. Pembayaran e-mel diuruskan oleh Pejabat Kewangan Negeri dan Perbendaharaan Negeri, bukannya Unit Kewangan, Pejabat SUKNS seperti didalam alamat. Poskod pada alamat juga adalah salah.
3	Secara rasminya, nama persidangan yang dimaksudkan ialah Persidangan Keempat (Belanjawan) Penggal Kelima, Dewan Undangan Negeri, Negeri Sembilan Yang ke-14. Penggunaan akronim atau singkatan bagi tujuan ini dianggap tidak rasmi dan menjejaskan formaliti e-mel berkenaan.
4	Elemen desakan dan ugutan.
5	Kesilapan ejaan/ penggunaan Bahasa Inggeris.



Rajah 3.5 Petunjuk e-mel yang mencurigakan bagi Siri II.



Rajah 3.6 Tangkap Layar Laman Web Palsu Untuk Simulasi Siri II.

SKRIP JAWAPAN

UNTUK ADUAN ATAU PERTANYAAN MENGENAI EMEL PANCINGAN DATA

Soalan: Salam puan, saya hendak buat pengesahan mengenai emel bertajuk "**xxx**". Adakah saya perlu memberi maklumbalas terhadap emel ini?

Jawapan: Wasalam, encik. Minta maaf, encik. Pihak saya tidak ada mengeluarkan sebarang emel berkaitan perkara tersebut. Buat masa ini, cara kerja adalah masih seperti asal, tiada sebarang pengemaskinian maklumat yang diperlukan.

Soalan: Sekiranya bukan pihak puan yang mengeluarkan emel ini, siapakah yang mengeluarkan emel ini?

Jawapan: Kemungkinan besar ini adalah emel pancingan data (*phishing email*). Jadi saya sarankan encik supaya tidak respon kepada emel tersebut dan panjangkan emel berkenaan kepada pihak UPTM untuk tindakan mereka selanjutnya. Alamat emelnya ialah helpdesk@ns.gov.my

Saya juga akan membuat aduan yang sama kepada pihak UPTM.

Soalan: Baiklah, saya akan/ tidak akan melaporkan insiden ini kepada pihak UPTM.

Jawapan: Baik, encik. Terima kasih.

Rajah 3.7 Skrip asas untuk rujukan watak dalam e-mel pancingan data dan Pentadbir E-mel.

3.3 FASA 2: KAJIAN EMPIRIKAL

Setelah rangka kerja simulasi dibangunkan dalam Fasa 1: Kajian Teoritikal, satu lagi instrumen iaitu soal selidik perlu dibangunkan untuk menyokong dapatan simulasi. Bagi membangunkan instrumen kedua kajian ini, soal selidik Norhafizah Abu Bakar (2017) yang hanya mempunyai 2 bahagian utama iaitu soal selidik dan persepsi pengguna, telah diadaptasi semula dengan beberapa penambahbaikan. Ini selaras dengan sebahagian objektif ketiga kajian ini iaitu untuk turut mengenalpasti faktor yang mempengaruhi seseorang personel PSUKNS menjadi mangsa pancingan data. Soal selidik ini mempunyai 5 bahagian utama iaitu 1) Bahagian A mengenai Kempen Kesedaran Keselamatan terhadap Ancaman Pancingan Data, 2) Bahagian B berkaitan Simulasi Pancingan Data Spesifik, 3) Bahagian C berkenaan Persepsi Pengguna Terhadap Simulasi Pancingan Data, 4) Bahagian D berkenaan Persepsi Pengguna Terhadap Pelaporan Insiden Keselamatan Siber kepada UPTM, dan 5) Bahagian E untuk mengenalpasti kumpulan perkhidmatan responden. Borang soal selidik disediakan dalam bentuk Google Form dan diedarkan kepada populasi kajian melalui Pentadbir E-mel selepas simulasi tamat. Borang soal selidik yang diedarkan adalah seperti di **Lampiran B**.

Bahagian A soal selidik adalah untuk mengenalpasti keberkesanan poster-poster yang telah diedarkan sebelum simulasi dijalankan. Soalan dalam bahagian ini juga akan digunakan sebagai panduan dalam menentukan medium yang bersesuaian untuk dicadangkan dalam pembentangan keputusan kajian kepada Pengurusan Tertinggi pada akhir kajian. Turutan soalan yang perlu dijawab dalam bahagian ini adalah bergantung kepada jawapan responden pada soalan pertama yang bertujuan untuk mendapatkan kepastian samada responden ada menerima poster-poster kesedaran atau tidak. Sekiranya responden ada menerima poster-poster tersebut, responden akan diajukan soalan berkaitan keberkesanan poster-poster berkenaan. Manakala sekiranya responden tidak menerima poster-poster tersebut, responden akan diajukan soalan berkaitan punca yang menjadi kebarangkalian mereka tidak menerima e-mel yang mengandungi poster-poster tersebut.

Bahagian B dalam soal selidik ini adalah untuk mengenalpasti faktor yang mempengaruhi responden sewaktu mereka menerima dengan e-mel pancingan data dalam simulasi, iaitu e-mel pancingan data. Kandungan soalan dalam bahagian ini bertujuan untuk mengenalpasti punca yang mempengaruhi respon sewaktu menerima e-mel pancingan data dengan mengambilkira petunjuk-petunjuk e-mel yang mencurigakan, seperti 1) pengirim e-mel yang meragukan, 2) kebimbangan untuk tidak menerima baucer percuma yang ditawarkan, 3) kandungan e-mel, 4) URL yang mencurigakan dan 5) samada semakan dibuat sebelum memberikan maklumbalas terhadap e-mel tersebut. Bahagian B ini turut mengenalpasti tindakan yang dilaksanakan oleh responden setelah mengenalpasti e-mel yang diterima adalah palsu.

Bahagian C soal selidik pula adalah untuk mendapatkan maklumbalas responden tentang keberkesanan simulasi yang telah dijalankan, manakala Bahagian D adalah untuk mengukur pengetahuan populasi terhadap garis panduan berkaitan keselamatan siber dalam organisasi dan mengukur kesedaran mereka tentang tindakan yang perlu diambil sekiranya menerima e-mel pancingan data.

Bahagian E adalah untuk mengenalpasti kumpulan responden yang memberikan maklumbalas dalam soal selidik. Ia cuma mengandungi soalan yang memerlukan responden memilih kumpulan perkhidmatan mereka sahaja.

Setelah rangka kerja simulasi dan soal selidik disediakan, simulasi perlu diuji terlebih dahulu sebelum dibentangkan kepada Pengurusan Tertinggi selaku pemegang taruh domain kajian. Pengujian ini bagi memastikan simulasi berjalan lancar, tidak terhalang oleh teknologi AI yang ada dan e-mel pancingan data dapat diterima oleh sasaran. Sesi pengujian ini, melibatkan bantuan daripada MAMPU dan mensasarkan empat akaun e-mel dalam domain kajian yang terdiri daripada akaun milik ahli pasukan penguji. Penglibatan MAMPU adalah perlu untuk memastikan e-mail pancingan data yang diedarkan dapat dimasukkan ke dalam senarai *whitelist*. Penglibatan pasukan penguji pula adalah untuk melaporkan ciri-ciri e-mail pancingan data yang diterima, selain dari menguji pautan ke laman web palsu yang disediakan dan menguji samada maklumat sulit yang dimasukkan dapat dikutip oleh Gophish atau tidak.

Pengujian rangka kerja simulasi telah diadakan sebanyak dua kali pada 24 November 2022. Pengujian pertama telah diadakan pada jam 10 pagi tetapi gagal melepasi ciri-ciri keselamatan AI yang ada pada sistem e-mel MAMPU. Pengujian Kedua telah diadakan pada jam 2 petang hari yang sama dan telah membuahkan hasil yang diharapkan. Satu protokol internet (IP) yang baru dan belum pernah digunakan untuk sebarang tujuan pancingan data telah digunakan dalam Pengujian Kedua ini. Konfigurasi *Listening URL* yang berfungsi untuk merekodkan input daripada mangsa juga telah diperkemaskan dengan menggunakan aplikasi *Tinyurl.* Konfigurasi dan laporan hasil pengujian bagi kedua-dua sesi adalah seperti di **Lampiran C**.

Setelah pengujian simulasi berjaya, satu sesi pembentangan dan demonstrasi kepada Pengurusan Tertinggi perlu diadakan. Ini bagi mendapatkan pandangan terhadap kesesuaian topik yang dipilih memandangkan sasaran yang bakal menjadi mangsa adalah turut terdiri daripada pegawai-pegawai kanan. Ia juga bertujuan bagi menyakinkan Pengurusan Tertinggi mengenai etika pelaksanaan dan pematuhan peraturan yang berkuatkuasa.

Sewaktu sesi demonstrasi, Pengurusan Tertinggi telah mencadangkan beberapa pindaan termasuk perubahan kepada topik yang kurang sensitif, simulasi dijalankan sebanyak satu siri sahaja dan hanya mensasarkan kepada kakitangan bergred 19 sehingga 52 sahaja. Justeru telah wujud persampelan bagi tujuan simulasi ini iaitu seramai 278 orang sahaja daripada keseluruhan populasi kajian berjumlah 368 orang. Manakala topik baru yang dipersetujui adalah “Program Program Khas Untuk Ahli Kelab - Baucer Online Percuma!” yang menggunakan watak Pengerusi Kelab Sukan & Rekreasi PSUKNS, dengan menggunakan laman web palsu baharu yang tidak ada kena mengena dengan laman web mana-mana agensi kerajaan.

Secara ringkas, aktiviti yang dilakukan dalam Fasa 2: Kajian Emperikal ini adalah seperti di Jadual 3.6.

Jadual 3.6 Aktiviti dalam Fasa 2: Kajian Emperikal.

Aktiviti	Tarikh Tindakan	Catatan
Pengujian Domain NS 1	24 November 2022, 10 pagi sehingga 11 pagi	• Hasil pengujian mendapati e-mel berjaya masuk ke dalam Inbox, tetapi Google AI berjaya mengesan kebarangkalian e-mel tersebut adalah e-mel pancingan data • Pautan dalam e-mel juga aktif, tetapi Google AI telah memaparkan kebarangkalian laman web pada pautan tersebut sebagai laman web pancingan data.
Pengujian Domain NS 2	24 November 2022, 2 petang sehingga 5.30 petang	• Setelah menggunakan IP yang baru dan belum pernah digunakan, e-mel berjaya masuk ke dalam Inbox. Google AI tidak memaparkan sebarang amaran. • Pautan dalam e-mel juga aktif, dan Google AI tidak mengesan sebarang kandung mencurigakan pada laman web yang dibawa oleh pautan. • Maklumat sulit boleh dikunci masuk dan Gophish berjaya mengutip setiap maklumat yang dimasukkan.
Pembentangan dan demonstrasi kepada Pengurusan Tertinggi	15 Disember 2022, 2.00 petang	• Pengurusan Tertinggi bersetuju simulasi dijalankan dalam satu siri sahaja, menggunakan topik lain yang kurang sensitif, melibatkan hanya kakitangan bergred 19 sehingga 52 sahaja dan tidak menggunakan mana-mana laman web kerajaan.

Secara teknikal, pelaksanaan Fasa 2: Kajian Emperikal ini telah membantu menghasilkan satu topik pancingan data yang dipersetujui oleh semua pihak, laman web palsu yang bersesuaian dengan topik simulasi, platfom simulasi pancingan data dan satu set soal selidik. Setelah setiap pindaan yang dicadangkan dalam sesi demonstrasi

diselesaikan, rangka kerja simulasi yang dibangunkan dalam fasa ini adalah sedia untuk dilaksanakan dalam Fasa 3: Kajian Sebenar.

3.4 FASA 3: KAJIAN SEBENAR

Bagi mencapai objektif kajian yang pertama dan kedua, rangka kerja simulasi yang telah diuji dalam Fasa 2: Kajian Emperikal perlu dilaksanakan ke atas sampel kajian. Langkah-langkah pembangunan simulasi Norhafizah Abu Bakar (2017) yang seterusnya iaitu 1) Langkah III: Pelaksanaan dan 2) Langkah IV: Pasca Simulasi adalah aktiviti penting dalam fasa ini.

Sebelum simulasi dilaksanakan, populasi kajian telah didedahkan dengan pengetahuan tentang ancaman pancingan data terlebih dahulu. Sebanyak empat poster telah diedarkan oleh Pentadbir E-mel kepada seluruh kakitangan mengikut jadual yang dipersetujui.

Jadual 3.7 Poster-poster kesedaran tentang e-mel pancingan data.

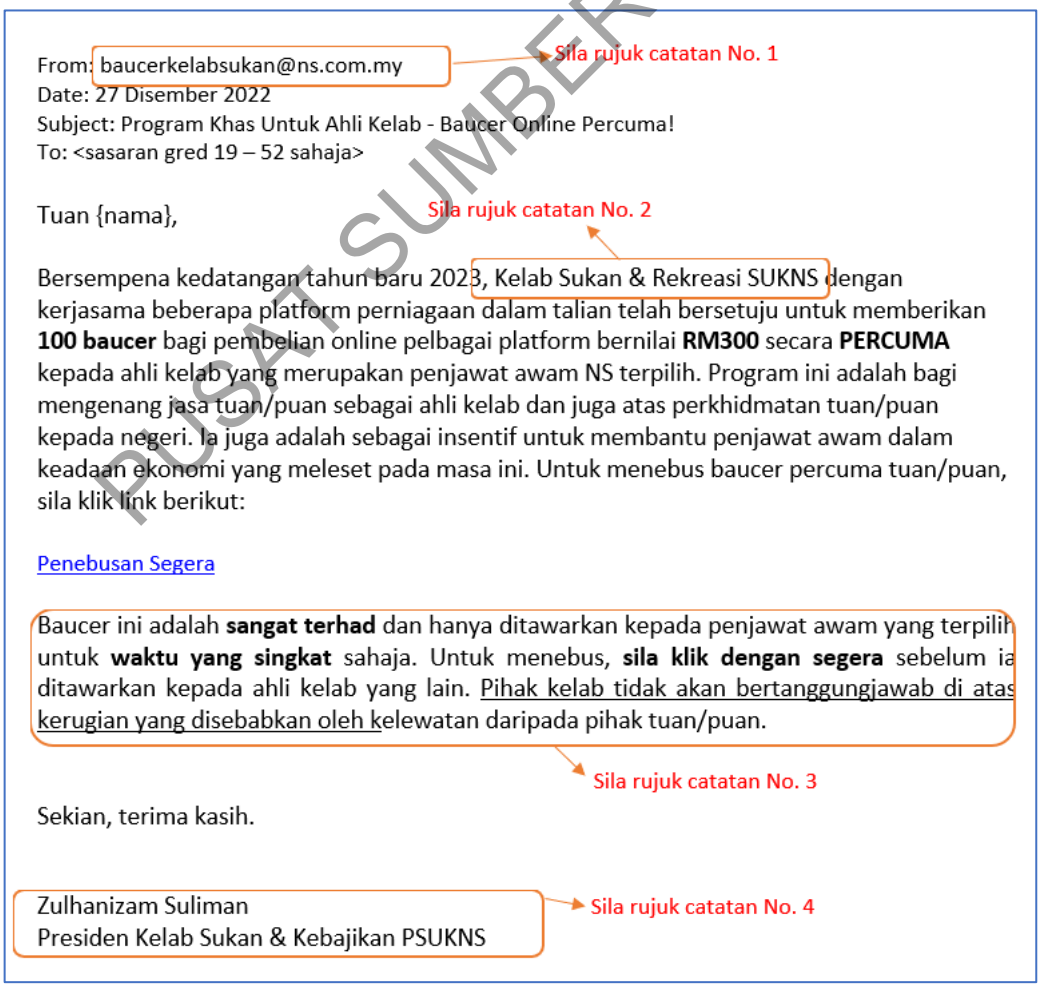
Tajuk Poster	Penerangan	Tarikh Edaran
Phishing Email	Penerangan ringkas secara info grafik tentang e-mel pancingan data.	14 November 2022
Bagaimana Untuk Mengenalpasti E-mel Pancingan Data?	Penerangan info grafik yang boleh membantu untuk mengenal ciri-ciri e-mel pancingan data.	15 November 2022
Bahaya Pancingan Data	Info grafik tentang kesan pancingan data	16 November 2022
Sekiranya Anda Menerima E-mel Pancingan Data	Info grafik yang menerangkan langkah-langkah yang boleh diambil sekiranya menerima e-mel pancingan data.	17 November 2022

3.4.1 Langkah III: Pelaksanaan

Selaras dengan arahan Pengurusan Tertinggi selaku pemegang taruh sewaktu sesi demonstrasi, topik baru yang dipersetujui adalah “Program Khas Kepada Ahli Kelab Kelab Sukan & Rekreasi – Pemberian Baucer Percuma”. Petunjuk e-mel yang meragukan bagi topik baru dalam simulasi sebenar ini adalah seperti di Rajah 3.7 dan Jadual 3.8.

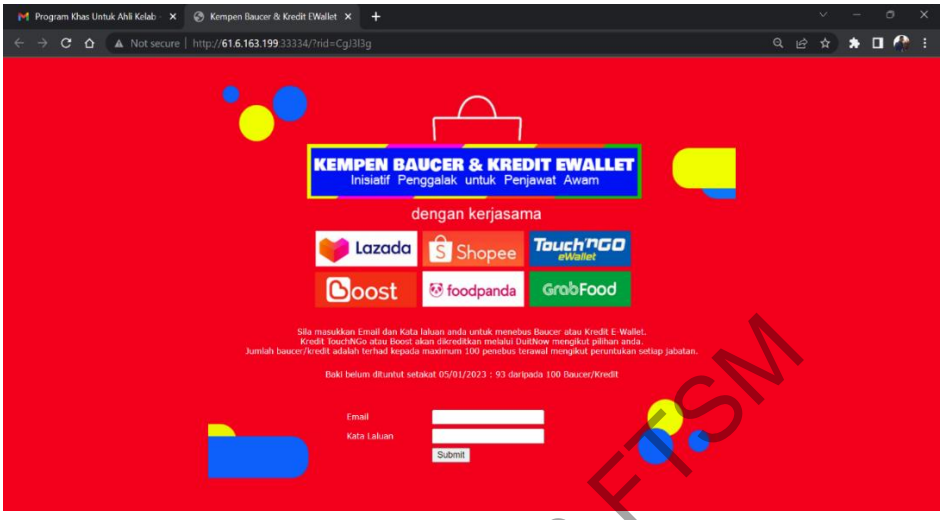
Jadual 3.8 Catatan bagi petunjuk e-mel mencurigakan dalam simulasi sebenar.

No.	Catatan
1	Alamat e-mel yang mencurigakan.
2	Nama kelab yang salah.
3	Elemen paksaan.
4	Ejaan nama watak pengirim dan jawatan yang salah.
5	Penggunaan bahasa dan ayat yang kurang formal serta terdapat kesalahan ejaan.



Rajah 3.8 Petunjuk e-mel yang mencurigakan dalam simulasi sebenar.

Beberapa petunjuk laman web yang mencurigakan juga boleh dikenalpasti dalam laman web palsu yang dibangunkan seperti 1) URL yang mencurigakan dan 2) elemen desakan bagi memujuk mangsa mengunci masuk alamat e-mel dengan segera tanpa berfikir panjang.



Rajah 3.9 Tangkap layar laman web palsu.

Prosedur simulasi ini juga dijalankan bertujuan sebagai pembelajaran melalui pengalaman (*teachable moment*) kepada kakitangan dalam organisasi. Bagi kakitangan yang terpedaya dengan e-mel pancingan data dari simulasi ini, satu notifikasi berbentuk nasihat dan amaran akan dipaparkan selepas mereka menekan butang “Submit” pada laman web palsu. Pemaparan laman web pendidikan berbentuk notifikasi ini mungkin akan menjejaskan keberkesanan simulasi, namun ia adalah penting dan amat diperlukan untuk mengawal keadaan panik yang mungkin berlaku sekiranya kakitangan menganggap tawaran yang dinyatakan dalam e-mel pancingan adalah sah dan kemudian menuntutnya daripada watak pengirim e-mel atau menuntut kerugian lain daripada pengurusan PSUKNS.

Rajah 3.10 Notifikasi kepada penguna yang terpedaya dengan pancingan data.

Memandangkan e-mel pancingan data yang dilancarkan menggunakan watak yang wujud dalam organisasi, skrip jawapan disediakan sebagai panduan kepada personel yang berkenaan bagi menjawab sebarang pertanyaan daripada kakitangan.

SKRIP JAWAPAN

UNTUK ADUAN ATAU PERTANYAAN MENGENAI EMEL PANCINGAN DATA SPESIFIK

BAUCER PEMBELIAN ONLINE PERCUMA UNTUK PENJAWAT AWAM NS

Soalan: Salam encik, saya hendak buat pengesahan mengenai emel bertajuk "**BAUCER PEMBELIAN ONLINE PERCUMA UNTUK PENJAWAT AWAM NS**". Adakah saya perlu memberi maklumbalas terhadap emel ini?

Jawapan: Wasalam, encik. Minta maaf, encik. Pihak saya tidak ada mengeluarkan sebarang emel berkaitan perkara tersebut. Buat masa ini, tiada sebarang program sedemikian yang dirancang.

Soalan: Sekiranya bukan pihak encik yang mengeluarkan emel ini, siapakah yang mengeluarkan emel ini?

Jawapan: Kemungkinan besar ini adalah emel pancingan data (*phishing email*). Jadi saya sarankan encik supaya kekal tenang serta tidak memberikan sebarang respon kepada emel tersebut dan panjangkan emel berkenaan kepada pihak UPTM untuk tindakan mereka selanjutnya. Alamat emelnya ialah helpdesk@ns.gov.my

Saya juga akan membuat aduan yang sama kepada pihak UPTM.

Soalan: Baiklah, saya akan/ tidak akan melaporkan insiden ini kepada pihak UPTM.

Jawapan: Baik, encik. Terima kasih kerana memaklumkan perkara ini kepada pihak kami.

Rajah 3.11 Skrip asas untuk rujukan watak dalam e-mel pancingan data.

SKRIP JAWAPAN HELPDESK

UNTUK ADUAN ATAU PERTANYAAN MENGENAI EMEL PANCINGAN DATA

Soalan:	Salam encik, saya hendak buat pertanyaan mengenai emel bertajuk "**Program Khas Untuk Ahli Kelab - Baucer Online Percuma!**". Saya mengesyaki ini adalah emel *phishing*. Adakah saya perlu memberi maklumbalas terhadap emel ini?
Jawapan:	Wasalam, encik. Terima kasih kerana menghubungi kami untuk pengesahan. Bagi tujuan semakan, mohon kerjasama encik untuk memanjangkan emel yang encik ragui tersebut untuk tindakan kami selanjutnya. Alamat emelnya ialah helpdesk@ns.gov.my Kami juga menyarankan agar encik tidak memberikan sebarang respon kepada emel tersebut.
Soalan:	Baiklah, saya akan/ tidak akan meneruskan laporan insiden ini kepada pihak tuan secara emel.
Jawapan:	Baik, encik. Terima kasih di atas kerjasama dan keprihatinan encik berhubung perkara ini.

Rajah 3.12 Skrip asas untuk rujukan Pentadbir E-mel.

Templat emel maklumbalas untuk setiap aduan berkaitan emel pancingan data yang dikemukakan oleh pengadu.

Tuan/puan,

Pihak UPTM mengucapkan terima kasih di atas laporan berkaitan emel pancingan data yang telah pihak tuan/puan kemukakan. Setelah semakan dibuat, pihak UPTM mengesahkan bahawa emel pancingan data tersebut adalah emel daripada projek simulasi pancingan data yang sedang dijalankan oleh UPTM. Simulasi ini adalah untuk mengukur tahap sensitiviti kakitangan terhadap ancaman emel pancingan data dan ia tidak mengandungi lain-lain tujuan komersial. Pihak UPTM merakamkan setinggi ucapan tahniah di atas kepekaan pihak tuan/puan dengan melaporkan ancaman ini kepada pihak UPTM.

Memandangkan simulasi ini masih berlangsung, kerjasama pihak tuan/puan adalah dipohon untuk tidak menghebahkan kandungan emel ini kepada rakan sekerja yang lain.

Sekali lagi pihak UPTM mengucapkan terima kasih di atas maklumbalas pihak tuan/puan berhubung perkara ini dan berharap agar tuan/puan terus cakna dan peka tentang keperluan untuk melindungi maklumat peribadi serta maklumat Kerajaan Negeri secara dalam talian.

Sekian, terima kasih.

UPTM, SUKNS.

Rajah 3.13 Template e-mel jawapan kepada pengadu secara individu.

Konfigurasi pelaksanaan simulasi adalah seperti di Jadual 3.9 manakala ringkasan pelaksanaan simulasi dalam Langkah III ini adalah seperti di Jadual 3.10.

Jadual 3.9 Konfigurasi pelaksanaan simulasi.

Perkara	Penerangan
Tarikh Mula	27 Disember 2022 (Selasa)
Masa Mula	10 pagi
Tarikh Tamat	3 Januari 2023 (Selasa)
Masa Tamat	6 petang
Penerima E-mel	278 akaun e-mel dibawah domain ns.gov.my yang terdiri daripada kakitangan bergred 19 sehingga gred 52
IP Server Gophish	61.6.163.199
Listening URL Gophish	https://tinyurl.com/suknsvoucher (61.6.163.199:33334)
	Sending Profile
• **Akaun E-mel**	albatros@heartsgourmet.com.my
• **SMTP *Host***	mail.heartsgourmet.com.my
• **SMTP *Port***	27
	Spoof Email
• ***Envelope Sender***	Kelab Sukan SUKNS< baucerkelabsukan@ns.com.my >
• **Tajuk E-mel**	Program Khas Untuk Ahli Kelab - Baucer Online Percuma!
• **Isi Kandungan E-mel**	{{.LastName}} {{.FirstName}}, Bersempena kedatangan tahun baru 2023, Kelab Sukan & Rekreasi SUKNS dengan kerjasama beberapa platform perniagaan dalam talian telah bersetuju untuk memberikan **100 baucer** bagi pembelian online pelbagai platform bernilai **RM300** secara **PERCUMA** kepada ahli kelab yang merupakan penjawat awam NS terpilih. Program ini adalah bagi mengenang jasa tuan/puan sebagai ahli kelab dan juga atas perkhidmatan tuan/puan kepada negeri. Ia juga adalah sebagai insentif untuk membantu penjawat awam dalam keadaan ekonomi yang meleset pada masa ini. Untuk menebus baucer percuma tuan/puan, sila klik link berikut: Penebusan Segera Baucer ini adalah **sangat terhad** dan hanya ditawarkan kepada penjawat awam yang terpilih untuk **waktu yang singkat** sahaja. Untuk menebus, **sila klik dengan segera** sebelum ia ditawarkan kepada ahli kelab yang lain. Pihak kelab tidak akan bertanggungjawab di atas kerugian yang disebabkan oleh kelewatan daripada pihak tuan/puan. Sekian, terima kasih. **Zulhanizam Suliman** Presiden Kelab Sukan & Kebajikan PSUKNS

Simulasi dimulakan pada 27 Disember 2023 iaitu selepas 6 minggu poster kesedaran diedarkan. Ini disebabkan kelewatan tarikh sesi demonstrasi yang diberikan oleh PSUKNS. Namun demikian, selang masa ini juga adalah bersesuaian memandangkan simulasi telah dilaksanakan pada waktu kakitangan tidak memberikan perhatian terhadap ancaman pancingan data.

Jadual 3.10 Ringkasan aktiviti dalam Langkah III: Pelaksanaan.

Aktiviti	Tarikh Tindakan	Catatan
Simulasi Pancingan Data	27 Disember 2022 10 pagi	• E-mel pancingan data telah dilancarkan melalui platform Gophish pada jam 10 pagi. • MAMPU telah melepaskan e-mel tersebut kepada sasaran pada jam 12 tengahari. • Pentadbir E-mel telah mengedarkan pemakluman mengenai e-mel pancingan data kepada warga PSUKNS pada jam 1.50 tengahari, ekoran beberapa aduan yang diterima. • Data dikutip sehingga 3 Januari 2023.

3.4.2 Langkah IV: Pasca Simulasi

Setelah simulasi ditamatkan, data yang dikutip oleh Gophish serta data yang dikumpulkan oleh watak pengirim e-mel dan Pentadbir E-mel perlu digabungkan dengan menggunakan metrik atau jadual respon yang telah dikenalpasti bagi mendapatkan corak respon yang lebih berstruktur. Metrik data mengandungi bilangan responden yang 1) membuka e-mel, 2) klik pautan dalam e-mel, 3) mengunci masuk maklumat peribadi dalam laman web palsu, dan 4) membuat laporan kepada watak pengirim e-mel atau Pentadbir E-mel.

Maklumat demografik yang diperlukan iaitu kumpulan perkhidmatan, boleh diperolehi daripada semakan silang antara maklumat yang dikutip oleh Gophish dengan maklumat yang ada dalam portal rasmi www.ns.gov.my. Bagi menyokong dan mengenalpasti faktor yang mempengaruhi kecenderungan responden, soal selidik adalah diperlukan.

Set soal selidik diedarkan kepada keseluruhan populasi kajian, walaupun simulasi hanya melibatkan sampel kajian. Ini memandangkan soalan dalam set berkenaan turut memerlukan input daripada populasi kajian yang tidak terlibat dengan simulasi secara langsung. Soalan yang dimaksudkan adalah mengenai 1) poster kempen kesedaran yang telah diedarkan dan 2) persepsi pengguna terhadap keperluan untuk melaporkan kejadian serangan siber kepada pihak teknikal organisasi.

Ringkasan aktiviti di Langkah IV ini adalah seperti di Jadual 3.11.

Jadual 3.11 Ringkasan aktiviti di Langkah IV: Pasca Simulasi.

Bil.	Aktiviti	Tindakan
1.	Semakan silang maklumat Laporan Hasil Kempen Gophish dengan maklumat daripada laman web direktori kakitangan PSUKNS. Gophish: e-mel responden Web: gred/ kumpulan perkhidmatan, unit, jawatan	Penguji
2.	Pengedaran soal selidik pasca simulasi berkaitan tindakan responden semasa mendapat e-mel pancingan data	Penguji
3.	Pengumpulan data dan analisis data	Penguji

3.5 FASA 4: PENILAIAN

Setiap data daripada simulasi dan soal selidik akan digabungkan serta dianalisa bagi mendapatkan kesimpulan yang jelas bagi menjawab persoalan ketiga kajian ini. Ia dikupas dengan terperinci dalam Bab IV bagi mendapatkan gambaran sebenar serta satu pernyataan yang jelas berkenaan tahap kerentanan responden terhadap ancaman pancingan data.

Dapatan kedua-dua instrumen juga akan dijadikan panduan kepada organisasi populasi kajian dalam menentukan bentuk penambahbaikan yang diperlukan.

Jadual 3.12 Ringkasan aktiviti dalam Fasa 4: Penilaian.

Bil.	Aktiviti	Tindakan
1.	Penilaian analisis dan dokumentasi keputusan	Penguji
2.	Pembentangan hasil keputusan kepada Pengurusan Tertinggi PSUKNS dan mencadangkan program kesedaran keselamatan yang bersesuaian	Penguji
3.	Pengedaran keputusan simulasi kepada seluruh kakitangan PSUKNS	PSUKNS
4.	Pertimbangan kesesuaian untuk pengulangan ujian	PSUKNS

3.6 RUMUSAN

Metodologi kajian yang dihuraikan dalam Bab III ini menerangkan kaedah yang dijalankan untuk menjawab persoalan kajian dalam Bab I. Ia telah mengadaptasi kajian terdahulu dalam membangunkan instrumen untuk mengumpul data premier kajian. Terdapat dua insrumen yang telah digunakan dengan setiap satunya memberi fokus kepada faktor utama iaitu kumpulan perkhidmatan yang menguruskan sesuatu maklumat dalam organisasi. Bab III ini telah menghuraikan kaedah yang telah digunakan untuk merekabentuk prosedur simulasi pancingan data yang sesuai dengan organisasi yang menguruskan maklumat kritikal kerajaan negeri sebagai instrumen pertama kajian. Selanjutnya, faktor-faktor yang mempengaruhi kecenderungan responden dalam simulasi pula dikenalpasti melalui instrumen kedua iaitu soal selidik yang telah dibangunkan dan dijalankan selepas tamat simulasi.

BAB IV

ANALISIS

4.1 PENGENALAN

Analisis terhadap data-data yang telah dikutip oleh kedua-dua instrumen perlu dilaksanakan bagi mendapatkan gambaran, keputusan dan tindak balas populasi terhadap persoalan dan objektif kajian. Dengan mengadaptasi Norhafizah Abu Bakar (2017), data statistik yang dikumpulkan oleh kedua-dua instrumen dianalisa secara deskriptif bagi menjawab persoalan kajian untuk mengenalpasti tahap kerentanan populasi kajian terhadap serangan ancaman pancingan data.

4.2 ANALISIS SIMULASI

Simulasi yang dijalankan dalam kajian ini memberi fokus kepada kumpulan perkhidmatan sebagai sasaran dan pemilihan topik e-mel pancingan data. Simulasi telah mengambil 278 kakitangan daripada kumpulan Pengurusan & Profesional dan juga kumpulan Pelaksana sebagai sampel kajian. Topik yang lebih umum telah digunakan iaitu pemberian baucer percuma kepada kakitangan yang merupakan ahli kelab sukan organisasi. Demografi sampel mengikut kumpulan perjawatan dan jantina adalah seperti di Jadual 4.1.

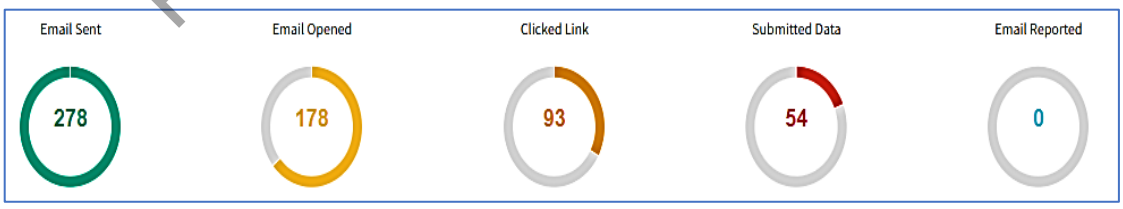
Jadual 4.1 Demografi sampel kajian.

Kumpulan Perkhidmatan	Bilangan
P&P	65
Pelaksana	213
JUMLAH	**278**

E-mel pancingan data bertajuk “Program Khas Untuk Ahli Kelab - Baucer Online Percuma!” telah diedarkan pada jam 10 pagi, 27 Disember 2022. E-mel berkenaan telah dilepaskan oleh pihak MAMPU pada jam 12 tengahari dan diterima masuk dalam *Inbox* e-mel 278 sampel kajian. Pentadbir E-mel telah menerima 2 aduan berkaitan e-mel pancingan data tersebut dan telah mengedarkan e-mel pemakluman mengenai ancaman pancingan data ini kepada keseluruhan warga PSUKNS pada jam 1.50 tengahari. Namun demikian, terdapat sedikit kekeliruan apabila Pentadbir E-mel telah menggunakan templat e-mel yang disediakan untuk menjawab aduan individu mengenai pancingan data, sebagai e-mel pemakluman tersebut.

Berdasarkan kepada papan pemuka Gophish, bilangan responden mengikut kategori tindakbalas sepanjang simulasi adalah seperti Rajah 4.1 yang menunjukkan sebanyak 278 e-mel telah berjaya diedarkan. Seramai 178 orang kakitangan telah membuka e-mel dan seramai 93 orang kakitangan yang klik pada pautan. Seramai 54 orang kakitangan telah terpedaya dan memasukkan alamat e-mel beserta kata laluan mereka dalam laman web palsu yang disediakan.

Papan pemuka Gophish tidak merekodkan e-mel pancingan data yang dilaporkan, kerana bagi kategori aduan atau laporan, data yang dikutip adalah secara manual daripada watak pengirim e-mel dan Pentadbir E-mel.



Rajah 4.1 Hasil keseluruhan simulasi pancingan data di PSUKNS.

Gophish turut merekodkan bilangan klik atau tindakbalas setiap responden sepanjang simulasi berlangsung. Justeru analisis simulasi ini turut mengambilkira bilangan klik yang telah direkodkan selain bilangan pegawai atau kakitangan.

Jadual 4.2 Jadual hasil bilangan klik mengikut kategori sepanjang simulasi pancingan data di PSUKNS.

Email Sent	*Email Opened*	*Clicked Link*	*Submitted Data*	*Email Reported*
278	212	167	61	0

Perbezaan antara hasil papan pemuka Gophish pada Rajah 4.1 dengan jadual hasil bilangan klik pada Jadual 4.2 ini menunjukkan bahawa terdapat pegawai dan kakitangan yang memberikan respon melebihi sekali bagi setiap kategori.

Memandangkan Pentadbir E-mel PSUKNS telah menerima dua aduan mengenai e-mel pancingan data ini, satu pemakluman mengenainya telah diedarkan kepada seluruh warga PSUKNS pada jam 1.50 tengahari. Jadual metrik yang membezakan waktu maklumbalas direkodkan, beserta bilangan laporan atau aduan yang diterima oleh Pentadbir E-mel dan watak pengirim e-mel secara manual sepanjang tempoh simulasi dijalankan. adalah seperti Jadual 4.3.

Jadual 4.3 Metrik maklumbalas yang diambil daripada Gophish untuk simulasi pancingan data.

Respon (klik) / Tarikh/ Masa	Buka E-Mel	Klik Pautan	Kunci masuk maklumat	Laporan kepada Pentadbir/ watak pengirim E-mel
27 Disember 2022, jam 12 tengahari sehingga 27 Disember 2022, jam 1.50 tengahari	66	65	20	22 (20 kepada watak pengirim, 2 kepada Pentadbir E-mel)
27 Disember 2022, jam 1.50 tengahari sehingga 3 Januari 2023, jam 6 petang	146	102	41	1 (kepada Pentadbir E-mel)

Jadual 4.3 juga menunjukkan bahawa walaupun terdapat e-mel pemakluman mengenai ancaman e-mel pancingan data ini diedarkan, ia tidak memberikan kesan terhadap simulasi. Ini kerana terdapat 41 insiden kakitangan memasukkan maklumat peribadi mereka selepas e-mel pemakluman diedarkan.