Contents lists available at Aufklarung

Praxis: Jurnal Pengabdian Kepada Masyarakat
journal homepage:
http://pijarpemikiran.com/

ANCAMAN DAN PENCEGAHAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA KEPADA SISWA SISWI SMK PUSPITA BANGSA

Aa Kurniawan[1], Nurfiqih[2]

[1,2] Teknik informatika, Ilmu Komputer, Universitas Pamulang
Dosen02361@unpam.ac.id[1], dosen02371@unpam.ac.id[2]

Kata kunci:
Cyber security, phishing,

Abstrak

Di era modern seperti sekarang ini, orang-orang tidak bisa lepas dari yang Namanya internet dan *gadget*. Fenomenanya, pada saat ini hampir setiap orang memiliki akun jejaring sosial lebih dari satu. Selain itu, sosial media digunakan juga untuk lahan berbisnis misalnya *online shop* di saat maraknya pengguna sosial media di seluruh dunia, saat itu juga penjahat-penjahat dunia siber mulai melancarkan aksinya untuk mencari keuntungan dari pengguna sosial media. Salah satunya dengan Teknik *phishing*. *Phishing* merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang dibutuhkan oleh sang penjebak, diharapkan dengan adanya edukasi mengenai ancaman dan pencegahan *phishing* di jejaring sosial sehingga orang-orang mengetahui hal-hal yang mencurigakan pada akun jejaring sosial maupun situs web yang lain. Serta melakukan pencegahan terhadap serangan siber ini.

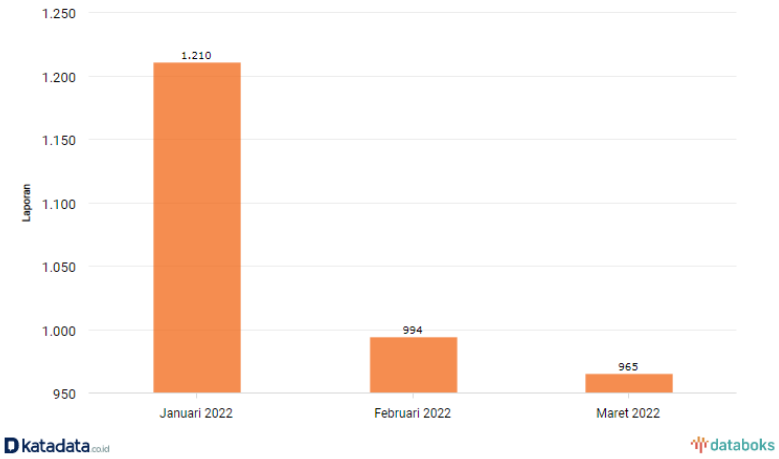
Pendahuluan

Di era modern sekarang, orang-orang tidak bisa lepas dari yang namanya internet dan *gadget*. Di tambah, saat ini orang-orang berlomba memperbanyak akun jejaring sosial mereka untuk mencari kepopuleran seperti Facebook, Twitter, Instagram, Snapchat, dan masih banyak lagi. Untuk mendapat berita ter-*update*orang-orang juga bisa menjumpai berbagai macam artikel baik dalam maupun luar negeri melalui sebuah laman *web* ataupun di jejaring sosial juga. Pastinya orang-orang membuka *web browser* dulu agar bisa pergi ke berbagai jejaring sosial semacam itu. Setiap orang pasti memiliki akun jejaring sosial lebih dari satu. Selain itu, sosial media juga digunakan untuk lahan berbisnis misalnya *online shop*. Kegiatan ini sangat mudah dan menguntungkan karena tidak membutuhkan modal dan hanya tinggal memposting barang jualan. Untuk pembayarannya bisa lewat rekening, *COD*, *market*, dll.

Di saat maraknya pengguna sosial media di seluruh dunia, saat itu juga penjahat-penjahat dunia siber mulai melancarkan aksinya untuk mencari keuntungan dari pengguna sosial media. Salah satunya yaitu dengan *phishing*. *Phishing* merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. *Phishing* termasuk dalam kejahatan siber, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan cari paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang *hacker*.

Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan. Hingga kini, banyak sekali akun sosial media yang sudah terjebak dalam *phishing*. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh *fake link* pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan. Dengan hal tersebut penyerang dapat mengambil informasi pengguna dan menggunakannya untuk mencari keuntungan misalnya untuk mengambil uang dari rekening pengguna atau menggunakan rekening untuk pembayaran *online*. Untuk pengantisipasian serangan *phishing* semacam itu yang paling sederhana yaitu untuk tidak meng-klik jika ada *link* yang masuk melalui akun sosial media maupun *email* yang di gunakan untuk akun sosial media. Karena *link* yang tidak di kenal patut di curigai sebagai serangan *phishing* yang menjebak akun sosial media untuk menyebar luaskan hal-hal yang tidak baik pada pengguna sosial media yang lain.

Sebenarnya tujuan di buatnya jurnal ini yang pertama yaitu agar orang-orang mulai mengubah pemikirannya terlebih dahulu terhadap serangan *phishing*. Kemudian orang-orang harus mengetahui hal-hal yang mencurigakan pada akun jejaring sosial maupun situs *web* yang lain. Bila benar ada serangan *phishing*, maka mereka harus meninggalkan laman palsu itu sesegera mungkin. Jangan hanya pergi begitu saja, kita juga harus mencari jalan keluar untuk menyelamatkan akun kita. Tentu kita harus mencari anti*phishing* untuk mencegahnya. Karena sekali kita terkena serangan, maka ancaman *phishing* juga akan menyerang pengguna yang lain. Dan serangan akan terus menyebar dan menyebar ke seluruh penjuru dunia. Bila dalam jejaring sosial pengguna yang terserang tidak tau apa-apa, di pihak lain akan marah-marah karena pengguna yang terserang tadi akan terus mengirim pesan spam pada seluruh akun yang berteman dengannya. Tidak tau sampai kapan serangan *phishing* akan di lancarkan sebagai kejahatan siber. Karena para *hacker-hacker* itu terus memunculkan ide-ide baru untuk merusak kegiatan di internet.Dan sayangnya di setiap tahunnya kasus seperti ini semakin bertambah banyak dan korban yang terjaring juga tidak bisa hanya di hitung dengan jari.



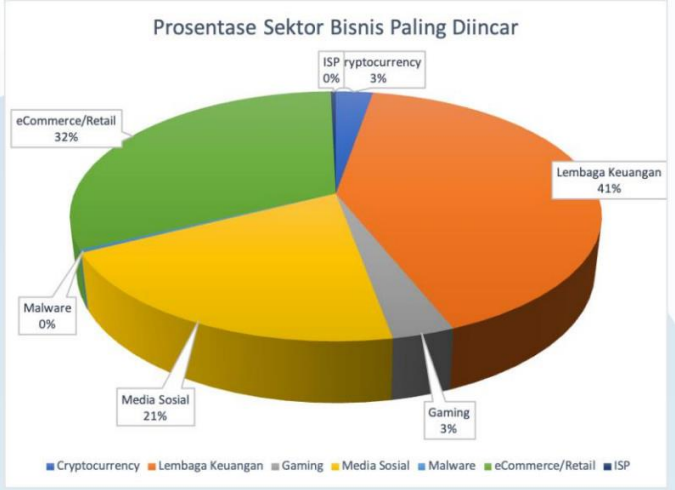
gambar 1 laporan kejahatan phishing tahun 2022

Indonesia Anti-Phishing Data Exchange (IDADX) mencatat, terdapat 3.180 laporan *phishing* di Indonesia selama kuartal I 2022. Jumlah itu berkurang dibandingkan pada kuartal IV 2021 yang sebanyak 5.325 laporan. Jika dibandingkan dengan periode yang sama di tahun lalu, jumlah laporan *phishing* pada tiga bulan pertama tahun ini mengalami peningkatan, di mana pada kuartal I 2021 IDADX hanya menerima 536 laporan *phishing*. Pada kuartal pertama tahun ini, kasus *phishing* paling banyak terjadi pada bulan Januari dengan total 1.210 laporan. Kemudian, kasusnya menurun pada Februari dan Maret menjadi 994 laporan dan 965 laporan. IDADX juga melaporkan jumlah oraganisasi yang diincar serangan *phishing* sebanyak 58 kasus dan ada 125 nama domain sepanjang Januari-Maret 2022. Adapun, IDADX mencatat nama organisasi/*brand* yang menjadi target

serangan *phishing* pada kuartal I 2022, di antaranya Internal Revenue Service (IRS), Microsoft, Crypto, Paypal, dan Amazon.

Mereka mencari uang dengan cara yang mudah. Namun tak selamanya mereka melakukan itu karena uang. Biasanya mereka hanya ingin bersenang-senang atau ingin mengintip kegiatan sang pemilik akun. Jika beruntung, mereka juga bisa mendapat uang sekaligus melihat-lihat isi akun pengguna yang mereka serang untuk bersenang-senang. Bila hanya orang biasa yang mereka serang mungkin masalah tidak akan terlalu besar. Bagaimana jika yang mereka serang adalah orang yang penting atau pun orang yang berpengaruh di dunia ini.Kasus itu pasti sudah sering terjadi. Orang-orang yang memiliki kuasa tertinggi beberapa juga melakukan kejahatan tetapi ia hanya menjadi bagian penyuruh untuk sang hacker. Selanjutnya hacker-hacker itu yang melaksanakan perintah untuk menyerang. Hal-hal itu sudah wajar terjadi apalagi saat masa-masa kampanye berpolitik ataupun contohnya pada saat dua perusahaan yang awalnya menjalin hubungan yang baik tiba-tiba salah satu perusahaan merasa kecewa karena saat pembagian hasil tidak memenuhi sepakat yang tercantum sebelumnya.

Indonesia Anti-Phishing Data Exchange (IDADX) mencatat, 5.579 laporan phising di Indonesia selama kuartal II (Q2) 2022. Jumlah ini naik sebanyak 1.637 laporan dibanding periode yang sama di kuartal I (Q1).



gambar 2 prosentase sektor bisnis yang paling diincar kejahatan phishing

Jika dilihat dari grafik diatas sector Media Sosial di Q2 sebesar 21% terbanyak ketiga disbanding sector lain, ini berarti media sosial perlu diperhatikan apalagi sebagian besar para remaja yang mudah sekali terkena phising.

Maka muncul lah ide-ide berbuat kecurangan. Mereka akan memanfaatkan *hacker* sebagai sarana penghancur sang lawan. Mereka menyuruh sang hacker untuk diam-diam mencuri data keuangan perusahaan musuh dan kemudian memanipulasi data tersebut sebaik mungkin. Lalu pada akhirnya semua uang hasil kerja sama mereka menjadi milik perusahaan yang menyewa hacker tadi semua. Pastinya si *hacker* tadi mendapat keuntungan beberapa persen. Untuk itulah masih ada banyak orang baik di dunia ini yang mau menciptakan alat pendeteksi atau aplikasi untuk mencegahnya. Para peneliti maupun pembuat aplikasi itu biasanya merupakan orang-orang yang pernah mengalami serangan *phishing*. Mereka tidak terima dan kemudian memutuskan untuk membalaskan dendamnya dengan sebuah aplikasi anti *phishing*.

Maka dari itu orang-orang harus memanfaatkannya sebaik mungkin agar mengurangi resiko terkena serangan *phishing*. Bila enggan melakukan sesuatu yang menurutnya terlalu merepotkan, mereka juga bisa menjaga akunnya sebaik mungkin dengan pengamanan yang tepat. Hanya dengan cara itu akun tidak akan di serang dan pengguna bisa nyaman bersosialisasi di dunia maya tanpa hambatan Tujuan dari pengabdian pada masyarakat ini

adalah memberikan pengenalan dasar pencegahan dari serangan phising di sosial media serta mengetahui respons siswa-siswi mengenai edukasi ancaman phising di sosial media.

METODE

Sasaran pada pengabdian masyarakat ini adalah siswa siswi SMK Puspita Bangsa, tempat pelaksanaan dilakukan kepada siswa siswi di SMK Puspita Bangsa ruang kelas pada jam 10:00

Metode yang digunakan dalam kegiatan pengabdian kepada masyarakat ini adalah dengan presentasi materi, tanya jawab, diskusi dan implementasi materi langsung tatap muka / offline kepada para peserta yang hadir, menggunakan media powerpoint untuk menampilkan slide materi sehigga dapat dilihat dan dimengerti oleh peserta. Setelah pemaparan materi peserta diberi kesempatan untuk bertanya sehingga apa yang dijelaskan oleh Tim Pengabdian dapat dipahami dengan baik.

Pada program PKM ini, kolaborasi yang terjadi hanya antara Universitas Pamulang yang diwakili tim PKM dengan pihak sekolah tanpa adanya pihak ketiga. Apabila program ini berjalan dengan baik, tim PKM dapat mencari pihak ketiga sebagai sponsor pelaksanaan PKM yang selanjutnya.

Tahapan atau langkah-langkah melaksanakan solusi yang ditawarkan untuk mengatasi permasalahan adalah sebagai berikut:

1. Ketua mengadakan kerjasama dengan pihak kepala sekolah SMK Puspita Bangsa untuk mengadakan acara penyuluhan mengenai Ancaman dan Pencegahan Phising Terhadap Pengguna Sosial Media sosial Kepada Siswa Siswi SMK Puspita Bangsa
2. Tim penyusun mempersiapkan sarana dan prasarana yang dibutuhkan untuk kegiatan penyuluhan.
3. Pada saat penyuluhan, narasumber memberikan materi berupa pengetahuan tentang Ancaman dan Pencegahan Phising Terhadap Pengguna Sosial Media kepada siswa siswi SMK Puspita Bangsa
4. Narasumber menjelaskan mengenai Ancaman dan pencegahan phising

Pelaksanaan penyuluhan program PKM ini sendiri direncanakan dapat dilihat minimal 20 orang. Dan nanti setelah acara, tim PKM akan melakukan evaluasi untuk memastikan program ini berjalan dengan baik. Namun apabila luarannya tidak sesuai dengan harapan, tim PKM akan melakukan evaluasi dan perbaikan di setiap pertemuannya serta mencoba semaksimal mungkin membantu supaya semuanya dapat berjalan dengan baik.

HASIL

Siswa-siswi SMK Puspita Bangsa setelah mengikuti pengabdian mengenai Ancaman dan Pencegahan Phising Terhadap Pengguna Sosial Media sosial Kepada Siswa Siswi SMK Puspita Bangsa dapat mengetahui penggunaan Ancaman dan pencegahan phising di media sosial.

Gambar 3 kegiatan saat pkm berlangsung

Gambar 4 dokumentasi saat kegiatan selesai dilaksanakan

PEMBAHASAN

Maka dari itu orang-orang harus memanfaatkannya sebaik mungkin agar mengurangi resiko terkena serangan *phishing*. Bila enggan melakukan sesuatu yang menurutnya terlalu merepotkan, mereka juga bisa menjaga akunnya sebaik mungkin dengan pengamanan yang tepat. Hanya dengan cara itu akun tidak akan di serang dan pengguna bisa nyaman bersosialisasi di dunia maya tanpa hambatan

SIMPULAN

Berdasarkan hasil pelaksanaan kegiatan yang telah dilakukan, dapat ditarik beberapa simpulan sebagai berikut:

1. Pengetahuan mengenai Ancaman dan Pencegahan Phising Terhadap Pengguna Sosial Media sosial Kepada Siswa Siswi SMK Puspita Bangsa
2. Kegiatan setelah mengikuti seminar ini diharapkan Siswa SMK Puspita Bangsa dapat mengetahui ancaman dan pencegahan phising di media sosial.

DAFTAR PUSTAKA

Fatimah, Nur.(2017).”*Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime*”. Journal of Education and Information Comunication Technology (JoEICT).Vol 1 No 1 2017.

Hakimi, Rifqy.(2016).”*Studi Isu Keamanan Jaringan Pada Facebook*”. Jurnal Pustakawan Indonesia Volume 11 No. 2.

Rachmawati, Dian(2014).”Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber”.Jurnal Ilmiah Saintikom.Vol 13 No 3.

I. Radiansyah and Y. Priyadi, “Analisis Ancaman Phishing Dalam Layanan Online Banking,” vol. 7, no. 1, 2016.

M. R. Akhyari and A. R. Pratama, “Kesadaran akan Ancaman Serangan Berbasis Backdoor di Kalangan Pengguna Smartphone Android,” Automata, vol. 2, no. 1, 2021, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/viewFile/17317/10906.

M. S. Alif and A. R. Pratama, “Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia,” Automata, vol. 2, no. 1, 2021, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/17279.

N. P. Singh, “Online Frauds in Banks with Phishing Journal of Internet Banking and Commerce,” no. August 2007, 2017.

Ni’matul Rohmah,Nuliya.(2020).”Media Sosial Sebagai Media Alternatif Manfaat dan Pemuas Kebutuhan Informasi Masa Pandemik Global Covid 19 (Kajian Analisis Teori Uses And Gratification)”. Jurnal Komunikasi dan Penyiaran Islam p-ISSN 2598-8883 | Vol. 4, No 1, September 2020, pp. 1-16

Riswanda,M, Imam Ghozali.(2020).”Tips & Trick Android Root:Cara Cepat dan Mudah Belajar Tips & Trick Android”.Jakad Media Publishing.