

ANALISIS KESADARAN MAHASISWA YOGYAKARTA TENTANG *PHISHING* PADA *ONLINE BANKING*

Lukman Wijaya¹, Erna Kumalasari Nurnawati²

^{1,2}Program Studi Informatika, Institut Sains & Teknologi AKPRIND, Yogyakarta
Kompleks, Jl. Kalisahak Jl. Balapan No.28, Klitren, Gondokusuman, Yogyakarta,
Indonesia

e-mail: wijayalukman51@gmail.com, ernakumala@akprind.ac.id

Intisari

Phishing merupakan wujud serbuan semantik serta terkadang disebut dengan pencurian bukti diri online, yang bertujuan guna mencuri data sensitif semacam nama pengguna, kata sandi, serta perinci perbankan online dari korbannya. Didalam penelitian ini mencoba mengukur tingkat kesadaran mahasiswa yang ada di Yogyakarta tentang kejahatan *phishing* pada *online banking* dengan cara menggunkan metode deskriptif kuantitatif yang di dalamnya menggunakan *google forms* dan wawancara untuk pengambilan data dari mahasiswa yang ada di Yogyakarta dengan 11 pertanyaan baik menggunakan *google forms* maupun wawancara. Dengan hasil dari penelitian ini 77% dari total 40 partisipan *google forms* mengatakan tahu atau sangat mengetahui dan 7 dari 10 Partisipan wawancara mengatakan mengerti. Jadi dapat di ambil kesimpulan bawah sebagian besar mahasiswa yang ada yang ada di Yogyakarta telah mengetahui dan mengerti tentang hal-lah apa saja yang dapat dilakukan untuk dapat terhindar dari *phishing* dalam oline banking. Namun demikian, perlu ditingkatkan tingkat awareness mahasiswa terhadap keamanan akun yang dimiliki.

Kata kunci— *Phishing, online banking, keamanan, mahasiswa*

Abstract

Phishing is a form of semantic attack and is sometimes called with online identity theft, which aims to steal sensitive data such as usernames, passwords, and online banking details from its victims. In this study, we tried to measure the level of awareness of students in Yogyakarta about phishing crimes in online banking by using a quantitative descriptive method in which Google forms and

interviews were used to collect data from students in Yogyakarta with 11 questions using both Google forms and interviews. With the results of this study, 77% of the total 40 Google Forms participants said they knew or really knew and 7 out of 10 interview participants said they understood. So it can be concluded that most students in Yogyakarta already know and understand what things can be done to avoid phishing in online banking. However, it is necessary to increase the level of student awareness of the security of their accounts.

Keywords - *Phishing, online banking, security, students*

PENDAHULUAN

Perkembangan Internet sudah semakin pesat dimana pengguna dapat mengelola keuangan serta pengeluaran individu mereka dari rumah saja dengan menggunakan komputer pribadi atau *smartphone*. Dengan menggunakan aplikasi perbankan kita bisa melihat dan dapat mengatur banyak hal seperti tagihan yang harus dibayar, belanja, dan liburan, dapat dilakukan hanya dengan memasukkan data akun serta mengklik tombol pada *e-commerce online*. Perbankan *online* sudah membuat hidup lebih praktis untuk pengguna perbankan online, namun banyak peluang yang dimanfaatkan nya sebagai tempat mendapatkan keuntungan pribadi seperti penipuan[1]. Penipu kerap menyamar selaku orang yang secara intuitif dipercaya oleh korban guna mengelabui calon korban supaya memberikan uang atau benda berharga kepunyaan mereka. Seseorang penipu berseragam polisi, misalnya, tidak akan membuat si calon korban curiga dan si calon korban akan tidak curiga sama sekali. Demikian pula, *phishing* merupakan wujud pencurian data diri online yang bertujuan buat mencuri data sensitif dari pengguna semacam kata sandi perbankan online[2].

Phishing merupakan wujud serbuan semantik serta terkadang disebut sebagai pencurian bukti diri online, yang bertujuan guna mencuri data sensitif semacam nama pengguna, kata sandi, serta perinci perbankan online dari korbannya. Dalam gempuran *phishing*, korban ditunjukkan lewat email phishing agar mengakses replika atau email palsu(pelaku dari phishing selalu , mengaku berasal dari bank si calon korbanya) dan dari web website yang legal[3]. Aspek

dari terbentuknya kejahatan ini bertujuan meraup keuntungan secara ilegal dengan metode memperoleh data seperti alamat email, username, password, no kredit, serta informasi berarti yang lain dari si korban[4]. Tidak hanya meluasnya pemakaian pesan email serta web website palsu buat menarik pengguna supaya membocorkan data individu mereka. kami mengamati kenaikan jumlah kode beresiko yang secara spesial menargetkan data akun pengguna. Sehabis dipasang di komputer pribadi atau handphone korban[5].

Suatu riset yang dilakukan oleh Button, dkk berupaya mencari ketahu kenapa banyak orang yang terjerat penipuan online. pelaku berupaya buat menipu korban dengan berpura-pura sebagai seorang yang berasal dari sesuatu organisasi yang formal[6]. *Phishing* umumnya terdiri dari penyerangan(ialah, menerima email penipuan) yang mengandalkan aspek watak manusia sebagai penentu keberhasilannya. Korban dimanipulasi agar membocorkan data pribadi-suatu wujud rekayasa sosial[7]. Dari informasi yang dikumpulkan oleh *state of finance app marketing apps flyer* pada tahun 2020 memberi tahu kalau dari total 4, 7 miliar instalasi aplikasi *fintech* di dunia sebesar 2, 7 miliar instalasi terjalin di Asia Pasifik serta Indonesia tercantum kedalam peringkat 3 menjadi negeri yang sangat banyak menginstal aplikasi *fintech*[8].

Layanan pembayaran(*payment service*) sebagai zona industri yang sangat ditargetkan pada kuartal kedua 2014, dengan 39, 80 persen dari serbuan sepanjang periode 3 bulan dari April hingga Juni 2014, sebaliknya jasa keuangan(financial) terus menjajaki dengan 20, 20%[9].

Oleh karna itu, alternatif apa yang dapat menanggulangi kasus *cyber crime* ini? Langkah-langkah apa saja yang dapat pemerintah lakukan untuk memecahkan masalah dan menanggulangi kejahatan *phishing*, supaya masiarakat tidak dapat terserang kejahatan ini lagi. Dengan alternatif atau jalan penyelesaian pada kasus *phishing* ini, diharapkan masiarakat kususny mahasiswa Yogyakarta dapat terhindar dari kejahatan phishing, sehingga seluruh mahasiswa kususny di Yogyakarta dapat terhindar dari kejahatan ini.

Analisis Kesadaran Mahasiswa Yogyakarta Tentang Phishing Pada Online Banking

(Lukman Wijaya, Erna Kumalasari Nurnawati)

Pemerintah atau pihak yang terkait seharusnya bergerak cepat untuk menanggulangi kasus ini, seperti pengadaan seminar atau kegiatan yang bersifat penyuluhan kepada mahasiswa tentang kejahatan ini. Yeng menjelaskan tentang pengetahuan dasar tentang apa itu *phishing*, baga mana cara kerjanya, dan bagaimana menghindari kejahatan *phishing*. Pemerinta juga perlu mengusut tuntas kejahatan ini dengan cara merekrut pihak-pihat yang berkompeten atau ahli dalam bidang ini agar dapat menanggulangnya lansung dari akarnya atau menangkap *phiser* dan mengadili secara hukum yang berlaku.

Penelitian ini bertujuan untuk melihat tingkat kesadaran mahasiswa yang ada di Yogyakarta tentang kejahatan *phishing* yang dapat terjadi pada *online banking*. Yang dapat terjadi akibat ketidak tahuanya tentang hal-hal apa saja yang harus di lakukan atau di hindari untuk dapat terhindar dari kejahatan *phishing*.

METODE PENELITIAN

Dalam penelitian ini menggunakan metode deskriptif kuantitatif dengan survei. Riset ini menarangkan sikap atau aktivitas pemakaian media baru oleh Gen Digital yang meliputi motivasi, Kelaziman ataupun sikap, serta keamanan akses media online. Studi deskriptif berupaya menggambarkan ciri ilustrasi terpaut fenomena, suasana, serta peristiwa[10]. " Metode deskriptif bertujuan guna membuat deskripsi secara sistematis, faktual serta akurat tentang fakta- fakta serta sifal- sifat populasi ataupun objek tertentu"[11]. Prosedur studi deskriptif kualitatif umumnya disajikan secara deskriptif juga berkarakter relatif, teoritis serta banyak memakai analisis teoritik[12]. Didalam metode ini menggunakan dua cara pengambilan data dengan menggunakan *Google Forms* dan wawancara.

A. *Google Forms*

Peneliti ini menggunakan *Google Forms* yang dibagikan ke 40 mahasiswa dari beberapa kampus yang ada di Yogyakarta, bertujuan untuk mendapatkan data dari mahasiswa yang berbetuk kuesioner, berisi 11 pertanyaan dan 4 level pilihan yaitu.

A. Tidak Tahu/Tidak Tahu Sama Sekali

B. Kurang Tahu/Kurang Mengtahui

C. Tahu/ Mengetahui

D. Sangat Tahu/Sangat Mengetahui

Pertanyaan-pertanyaan tersebut bertujuan untuk melihat atau mengukur seberapa sadarkah mahasiswa Yogyakarta tentang kejahatan phishing dalam online banking. Adapun tahap pengumpulan data menggunakan *Google Forms* dapat di lihat pada gambar 1.



Gambar 2 Tahapan Pengumpulan Data Menggunakan Diagram Alir

Dalam penelitian ini juga dilakukan wawancara kepada 10 mahasiswa dari beberapa kampus yang ada di yogyakarta dengan 11 pertanyaan dan 2 level pilihan yaitu.

A. Tidak Tahu/Tidak Tahu

B. Tahu/ Mengetahui

Analisis Kesadaran Mahasiswa Yogyakarta Tentang Phishing Pada Online Banking

(Lukman Wijaya, Erna Kumalasari Nurnawati)

Wawancara ini dilakukan bertujuan mengumpulkan data, untuk kepentingan penelitian. Untuk lokasi wawancara di lakukan di beberapa tempat salah satunya di Kampus IST AKPRIND YOGYAKARTA dan di beberapa tempat lainnya.

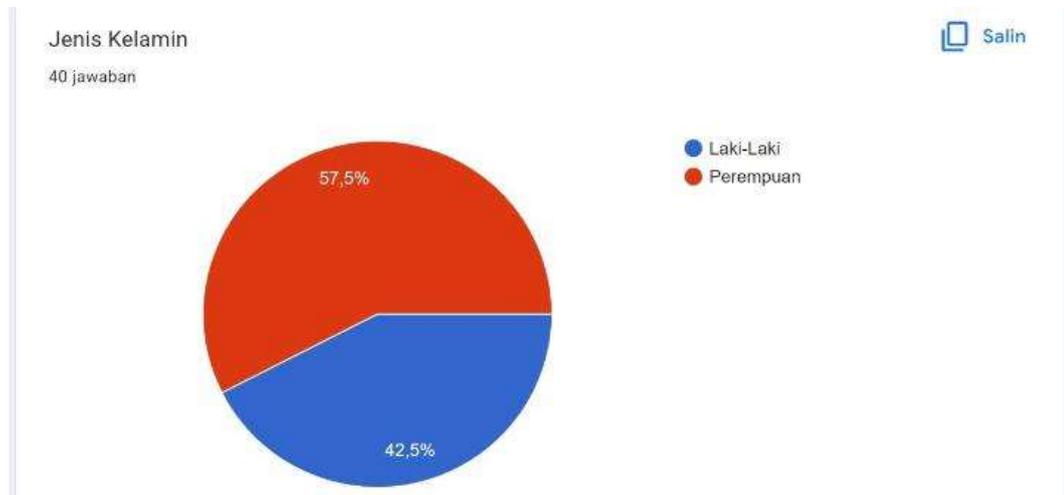
HASIL DAN PEMBAHASAN

Berdasarkan pengambilan data menggunakan *Google Forms*, dengan partisipan sebanyak 40 orang, yang masih bersetatus sebagai mahasiswa dari beberapa kampus yang ada di Yogyakarta, dengan beberapa keterangan seperti jenis kelamin, nama mahasiswa, dan setatus saat ini. Yang di tampilkan pada tabel 1. Didalam pengumpulan data penulis juga menggunakan wawancara yang di lakukan kepada 10 mahasiswa dari beberapa kampus yang ada di Yogyakarta untuk melihat seberapa sadarkah mahasiswa dalam menghindari kejahatan *phishing* yang dapat terjadi akibat ketidaktahuannya tentang hal-hal apa saja yang perlu di lakukan atau dihindari saat menggunakan internet atau media sosial.

TABEL 1. TABEL DEMOGRAFI NARASUMBER

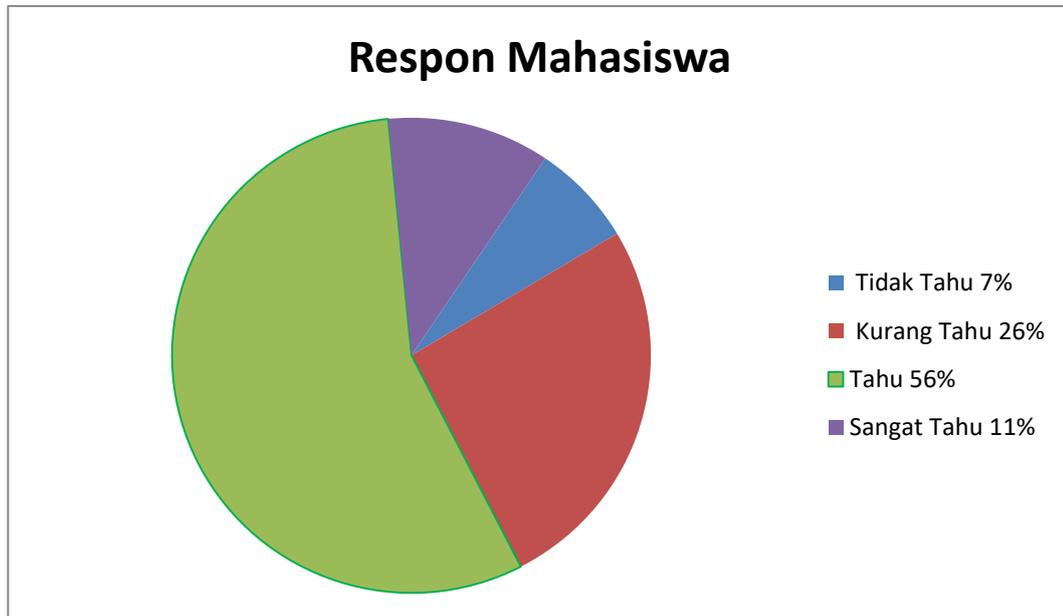
Varibel	Jumlah	Persentase%
Jenis Kelamin		
- Laki-Laki	17	42,5%
- Perempuan	23	57,5%
Respon Mahasiswa		
- Tidak Tahu	-	7%
- Kurang Tahu	-	26%
- Tahu	-	56%
- Sangat Tahu	-	11%
Setatus Saat Ini		
- Mahasiswa	40	100%

Berdasarkan jawaban dari reponden yang tertera pada tabel 1. Terlihat bahwa persentase dari tabel 1 di atas menunjukkan, 42,5% Laki-Laki dan 57,5% Perempuan dari total 40 partisipan mahasiswa mengatakan 7% tidak tahu, 26% kurang tahu, 56% tahu atau mengetahui, dan 11% sangat mengetahui. Dari sini dapat di artikan bahwa sebagian besar mahasiswa yang ada di Yogyakarta sudah mengerti atau mengetahui tentang hal-hal apa saja yang dapat dilakukan untuk menghindari kejahatan *cyber* kusunya *phishing* yang dapat di lihat pada tabel 1 menunjukkan bahwa 56% dari 40 partisipan telah mengetahui tentang hal-hal apa saja yang dapat dilakukan untuk menghindari kejahatan *phishing* ini. Walaupun hanya 11% dari total keseluruhan partisipan yang telah benar-benar mengerti atau sangat mengetahui tentang hal-hal apa saja yang dapat dilakukan untuk menghindari kejahatan *phishing*. Yang di tunjukan pada pada Gambar 2 Jenis Kelamin Responden dan Grefik 1 Respon Mahasiswa,yang ada di bawah.



Gambar 2 Jenis Kelamin Responden

Grefik 1 Respon Mahasiswa



Berdasarkan hasil yang di dapatkan dari wawancara secara langsung yang dilakukan kepada 10 mahasiswa dari beberapa kampus yang ada di Yogyakarta, dengan sistem pengambilan data, jika mengetahui atau mengerti mengatakan [Ya] dan jika tidak mengetahui atau tidak mengerti mengatakan [Tidak]. dapat di ambil kesimpulan bahwa 7 dari 10 partisipan dalam wawancara mengatakan [Ya] atau mengetahui dan mengerti tentang hal-lah apa saja yang dapat dilakukan untuk dapat terhindar dari *phishing* dalam *oline banking*.

KESIMPULAN

Berdasarkan hasil penelitian yang di lakukan dengan menggunakan metode deskriptif kuantitatif dan pengambilan data mengguakan *Google Forms* dan wawancara kepada mahasiswa dari beberapa kampus yang ada di yogyakarta dengan persentase *Google Forms* sebanyak 77% dari total 40 mahasiswa mengatakan tahu atau sangat menetahui, dan wawancara yang di lakukan kepada 10 mahasiswa, 7 diantaranya mengatakan mengerti. Jadi dapat di ambil kesimpulan bawah sebagian besar mahasiswa yang ada yang ada di Yogyakarta telah mengetahui dan mengerti tentang hal-lah apa saja yang dapat dilakukan untuk dapat terhindar dari *phishing* dalam *oline banking*.

SARAN

Diharapkan pemerintah atau pihak yang terkait dapat memberikan wawasan atau pengetahuan tentang kejahatan phishing yang dapat terjadi dalam online banking. Contohnya dengan melakukan seminar kepada mahasiswa agar dapat terhindar dari phishing dalam online banking.

DAFTAR PUSTAKA

- [1] Guy Larcom and Adam J. Elbirt, 'Gone Phishing', *IEEE Technology and Society Magazine*, 25.3 (2006), 52–55 <<https://doi.org/10.1109/MTAS.2006.1700023>>.
- [2] Engin Kirda and Christopher Kruegel, 'Protecting Users against Phishing Attacks with AntiPhish', *Proceedings - International Computer Software and Applications Conference*, 1 (2005), 517–24 <<https://doi.org/10.1109/COMPSAC.2005.126>>.
- [3] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Konstantin Beznosov, 'Phishing Threat Avoidance Behaviour: An Empirical Investigation', *Computers in Human Behavior*, 60 (2016), 185–97 <<https://doi.org/10.1016/j.chb.2016.02.065>>.
- [4] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Konstantin Beznosov, 'Phishing Threat Avoidance Behaviour: An Empirical Investigation', *Computers in Human Behavior*, 60 (2016), 185–97 <<https://doi.org/10.1016/j.chb.2016.02.065>>.
- [5] Jason Milletary, 'Technical Trends in Phishing Attacks', *Technical Trends in Phishing*, 2005, 1–17 <https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_503_15.pdf>.
- [6] Jason Milletary, 'Technical Trends in Phishing Attacks', *Technical Trends in Phishing*, 2005, 1–17 <https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_503_15.pdf>.
- [7] Alice Hutchings and Hennessey Hayes, 'Routine Activity Theory and Phishing Victimization', *Current Issues in Criminal Justice*, 20.3 (2009),

Analisis Kesadaran Mahasiswa Yogyakarta Tentang Phishing Pada Online Banking

(Lukman Wijaya, Erna Kumalasari Nurnawati)

20<<https://www.cl.cam.ac.uk/~ah793/papers/2009Routineactivitytheoryandphishingvictimisation.pdf>>.

- [8] Sahat Parulian, Devi Anassalifa Pratiwi, and Meiliya Cahya Yustina, 'Ancaman Dan Solusi Serangan Siber Di Indonesia', *Telnect*, 1.2 (2021), 85–92<<https://ejournal.upi.edu/index.php/TELNECT/article/view/40866>>.
- [9] Ikhsan Radiansyah, Candiwan Rusdjan, and Yudi Priyadi, 'Analisis Ancaman Phishing Dalam Layanan Online Banking', *Journal of Innovation in Business and Economics*, 7.1 (2016), 1 <<https://doi.org/10.22219/jibe.vol7.no1.1-14>>.
- [10] Zinggara Hidayat, Asep Saefuddin, and Sumartono Sumartono, 'Motivasi, Kebiasaan, Dan Keamanan Penggunaan Internet', *Jurnal ILMU KOMUNIKASI*, 13.2 (2017), 129–50 <<https://doi.org/10.24002/jik.v13i2.675>>.
- [11] Andri Sahata Sitanggang and others, 'Analisis Yang Mempengaruhi Penggunaan M-Banking Bagi Nasabah Bni', *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, Volume 7, 2527–6344 (2022) <<https://doi.org/10.30651/jms.v7i2.14216>>.
- [12] Akmal Ramadhan, Muhammad Alwi Alhafidh, and Muhamad Diki Firmansyah, 'Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS' *Kampret Journal*, 1.1 (2022), 11–15 <<https://doi.org/10.35335/kampret.v1i1.9>>.