

PENINGKATAN KEWASPADAAN TERHADAP KEJAHATAN SIBER PADA APLIKASI WHATSAPP DI KALURAHAN BANGUNJIWO

Dedy Hariyadi^{1*}, Alfirna Rizqi Lahitani², Irmma Dwijayanti³, dan Kartikadyota Kusumaningtyas⁴

Ringkasan

Potensi serangan siber yang semakin kompleks telah meningkatkan kejahatan di ruang digital, terutama melalui akses awal (initial access) ke perangkat pengguna, dengan aplikasi WhatsApp menjadi salah satu sarana baru bagi penjahat siber untuk melakukan penipuan online dan pencurian data. Untuk mengatasi hal ini, Universitas Jenderal Achmad Yani Yogyakarta bersama Desa Mitra di Kalurahan Bangunjiwo, Kabupaten Bantul, Daerah Istimewa Yogyakarta, melaksanakan kegiatan Pengabdian kepada Masyarakat yang bertujuan meningkatkan kesadaran dan melatih warga tentang langkah-langkah keamanan dasar, seperti Multi Factor Authentication (MFA) dan Two-step Verification. Program ini dilaksanakan melalui beberapa tahapan, termasuk koordinasi, observasi, sosialisasi, evaluasi, dan pelaporan, yang berhasil meningkatkan pengetahuan warga tentang ancaman siber dan penerapan langkah keamanan dengan persentase di atas 20%, tetapi juga menumbuhkan pendekatan proaktif terhadap keamanan siber, sekaligus menekankan pentingnya pendidikan dan dukungan berkelanjutan untuk memperkuat ketahanan masyarakat dalam menghadapi kejahatan siber, sehingga diharapkan dapat berkontribusi pada terciptanya ruang siber yang lebih aman bagi semua.

Kalurahan Bangunjiwo, Kabupaten Bantul, Daerah Istimewa Yogyakarta

Keywords

Whatsapp, Security Awareness, Kejahatan Siber, Multi Factor Authentication, Two-step Verification

Submitted: 09/10/24 — **Accepted:** 18/03/25 — **Published:** 27/10/25

^{1*} Universitas Jenderal Achmad Yani Yogyakarta, Indonesia — email: dedy@unjaya.ac.id

² Universitas Jenderal Achmad Yani Yogyakarta, Indonesia — email: alfirnarizqi@gmail.com

³ Universitas Jenderal Achmad Yani Yogyakarta, Indonesia — email: irmmadwijayanti@gmail.com

⁴ Universitas Jenderal Achmad Yani Yogyakarta, Indonesia — email: kartikadyota@gmail.com

⁵ Universitas Jenderal Achmad Yani Yogyakarta, Indonesia — email: grita1202@gmail.com

* corespondent author

1. Pendahuluan

WhatsApp telah menjadi salah satu platform instant messaging yang paling banyak digunakan di Indonesia untuk berbagi informasi [[1]]. Penggunaan meluas di berbagai sektor baik komersial atau non-komersial. Persentase penggunaan aplikasi WhatsApp di Indonesia mencapai lebih dari 80% sebagai media atau alat komunikasi utama [[2]]. Namun, meningkatnya penggunaan WhatsApp memiliki dampak negatif seperti meningkatnya kejahatan digital di ruang siber [[3]].

Kejahatan siber, termasuk penipuan online, pencurian identitas, dan penyebaran *malware*, semakin marak dengan memanfaatkan kemudahan dan kecepatan komunikasi yang ditawarkan oleh aplikasi WhatsApp [[4]]. Penjahat siber sering kali menggunakan teknik rekayasa sosial untuk menipu pengguna agar memberikan informasi pribadi atau melakukan transfer dana. Meskipun terdapat upaya dari pihak berwenang dan penyedia layanan untuk meningkatkan keamanan, kesadaran pengguna terhadap ancaman ini masih perlu ditingkatkan agar dapat melindungi diri dari risiko kejahatan digital yang terus berkembang [[5]].

Kalurahan Bangunjiwo, Kabupaten Bantul, Daerah Istimewa Yogyakarta sebagai wilayah di pemerintah desa memiliki berbagai potensi seperti desa wisata dan pertanian. Saat ini kejahatan siber tidak hanya mengincar sektor komersial tetapi juga masyarakat berbagai kategori. Metode yang digunakan untuk melancarkan tindak kejahatan para penjahat siber menyebarkan informasi secara acak baik melalui telepon atau pesan singkat, seperti *phishing*. Kegiatan Pengabdian kepada Masyarakat dilaksanakan di Padukuhan Ngentak, Kalurahan Bangunjiwo dengan tema kewaspadaan ancaman serangan siber atau penipuan online.

Phishing adalah teknik penipuan yang digunakan oleh pelaku kejahatan siber untuk mendapatkan informasi sensitif, seperti nama pengguna, kata sandi, nomor kartu kredit, atau data pribadi lainnya, dengan menyamar sebagai entitas terpercaya. Adapun kategori kejahatan siber berupa *phishing* diantaranya adalah email *phishing*, web *phishing*, *smishing*, *whaling phishing*, *voice phishing*, dan sebagainya [[6]].

Security awareness adalah pemahaman dan kesadaran individu atau kelompok tentang risiko keamanan informasi, serta tindakan-tindakan yang dapat diambil untuk mencegah terjadinya insiden keamanan. Tujuan dari *security awareness* diantaranya mencegah kejahatan siber, melindungi data pribadi, menguatkan ketahanan nasional dari ancaman serangan siber [[7]]. Maka dari itu pengabdian kepada masyarakat ini diselenggarakan pada kegiatan kemasyarakatan di wilayah Kalurahan Bangunjiwo, Kabupaten Bantul, Daerah Istimewa Yogyakarta.

2. Metode Penerapan

Perusahaan sistem pertahanan Amerika Serikat, Lockheed Martin melakukan pemetaan pola kejahatan yang dilakukan oleh penjahat siber yang disebut *Cyber Kill Chain*. Pada *Cyber Kill Chain* terdapat tahapan yang dilakukan oleh penjahat siber diantaranya *reconnaissance*, *weaponization*, *delivery*, *exploitation*, *installation*, *command & control*, dan *actions on objectives*. *Cyber Threat Model* yang direkomendasikan oleh Lockheed Martin untuk mencegah serangan siber pada sisi pengguna yaitu melakukan pencegahan pada tahapan *Delivery*. Tahapan *Delivery* adalah langkah yang dilakukan oleh penjahat siber melancarkan aksinya melalui berbagai media komunikasi menggunakan *phishing*, *malware*, *exploit* dan sebagainya [[8]].

Serangan siber dapat dicegah dari sisi pengguna dengan dilakukan kampanye *security awareness*. Gambar 1 merupakan tahapan kegiatan kampanye *security awareness* dengan penjabaran sebagai berikut:

1. Koordinasi merupakan bagian tahapan analisis situasi dengan desa mitra, Kalurahan Banunjiwa dengan melakukan koordinasi kegiatan Pengabdian kepada Masyarakat.
2. Observasi tahapan analisis situasi selanjutnya dengan melakukan identifikasi permasalahan, kondisi, dan potensi Kalurahan Bangunjiwo.
3. Sosialisasi merupakan kegiatan utama dalam kampanye *security awareness* dengan memaparkan potensi perkembangan teknologi beserta dampak negatifnya. Termasuk memberikan pendampingan untuk mengamankan perangkat gawai dan aplikasi Whatsapp untuk mencegah serangan siber.
4. Evaluasi merupakan tahapan melakukan pengukuran terhadap pemahaman penanganan aplikasi Whatsapp melalui pre test dan post test.
5. Pelaporan, hasil kegiatan Pengabdian kepada Masyarakat dilaporkan dalam bentuk kajian dan masukan penelitian yang akan datang tentang kampanye *security awareness*.



Gambar 1. Tahapan Pengabdian kepada Masyarakat

3. Hasil dan Ketercapaian Sasaran

3.1 Koordinasi

Sebelum pelaksanaan kegiatan Pengabdian kepada Masyarakat, Ketua Tim Pelaksana melakukan koordinasi intensif dengan Pemerintah Kalurahan Bangunjiwo. Tim membahas rencana kegiatan, target peserta dan metode pendekatan untuk memastikan efektivitas program. Bapak Praja, S.T., M.Si., selaku Lurah Kalurahan Bangunjiwo, menyambut baik inisiatif ini dan memberikan masukan berharga terkait kondisi masyarakat serta potensi tantangan yang mungkin dihadapi. Melalui koordinasi ini, terjalin kolaborasi yang kuat antara pihak universitas dan pemerintah desa sebagai fondasi penting bagi keberhasilan pelaksanaan kegiatan. Gambar 2 dokumentasi koordinasi Ketua Tim Pelaksana dengan Lurah Kalurahan Bangunjiwo.



Gambar 2. Koordinasi Dengan Lurah Kalurahan Bangunjiwo

3.2 Observasi

Pada tahap observasi, tim pengabdian masyarakat melakukan *Focus Group Discussion* (FGD) dengan perwakilan Dukuh di Kalurahan Bangunjiwo untuk memahami lebih dalam kondisi dan kebutuhan masyarakat terkait keamanan siber, seperti Gambar 3. Kegiatan FGD ini melibatkan perwakilan dari setiap Padukuhan yang memiliki pemahaman beragam tentang penggunaan teknologi digital. Dalam diskusi tersebut, terungkap bahwa sebagian besar masyarakat telah menggunakan aplikasi seperti WhatsApp dalam kehidupan sehari-hari, namun masih minim pemahaman tentang ancaman serangan siber seperti penipuan online dan pencurian data. Selain itu, peserta FGD juga menyampaikan kendala yang sering dihadapi, seperti kurangnya pengetahuan tentang langkah-langkah keamanan dasar dan ketidaktahuan cara melindungi informasi pribadi. Hasil observasi ini menjadi dasar dalam merancang materi sosialisasi dan pelatihan yang disesuaikan dengan kebutuhan serta tingkat pemahaman masyarakat, sehingga program pengabdian dapat memberikan dampak yang lebih efektif dan tepat sasaran.



Gambar 3. FGD Dengan Perwakilan Dukuh Kalurahan Bangunjiwo

3.3 Kegiatan Sosialisasi

Kegiatan sosialisasi di Padukuhan Ngentak, Kalurahan Bangunjiwo, juga dilengkapi dengan survei sederhana untuk mengukur tingkat pemahaman dan praktik pengamanan pada aplikasi WhatsApp yang digunakan oleh warga. Survei ini dilakukan secara interaktif dengan menggunakan kuesioner singkat yang dibagikan kepada peserta sebelum dan setelah sesi sosialisasi. Pertanyaan dalam survei mencakup topik seperti penggunaan fitur keamanan WhatsApp (contoh: *Two-Step Verification*), kesadaran tentang ancaman siber, serta pengalaman warga terkait penipuan atau upaya peretasan melalui aplikasi tersebut.

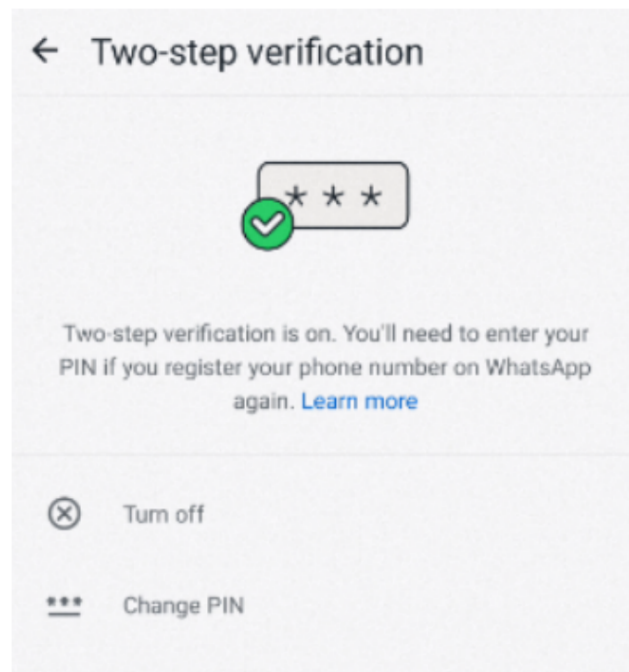
Setelah sesi sosialisasi, survei kembali dilakukan untuk mengevaluasi peningkatan pemahaman dan kesadaran warga tentang pentingnya mengamankan akun WhatsApp. Tim pengabdian menjelaskan hasil survei secara transparan kepada peserta dan memberikan rekomendasi praktis berdasarkan temuan tersebut. Misalnya, jika survei menunjukkan bahwa sebagian besar warga belum mengaktifkan *Two-step Verification*, tim akan memberikan panduan langkah demi langkah untuk mengaktifkan fitur tersebut. Survei ini tidak hanya menjadi alat evaluasi, tetapi juga sarana edukasi tambahan yang membantu warga memahami pentingnya langkah-langkah keamanan sederhana namun krusial. Dengan demikian, kegiatan sosialisasi tidak hanya bersifat informatif, tetapi juga partisipatif dan berbasis data, sehingga diharapkan dapat memberikan dampak yang lebih berkelanjutan bagi masyarakat. Adapun dokumentasi penyelenggaraan sosialisasi seperti pada Gambar 4.



Gambar 4. Kegiatan Pengabdian kepada Masyarakat

3.4 Sosialisasi Keamanan WhatsApp

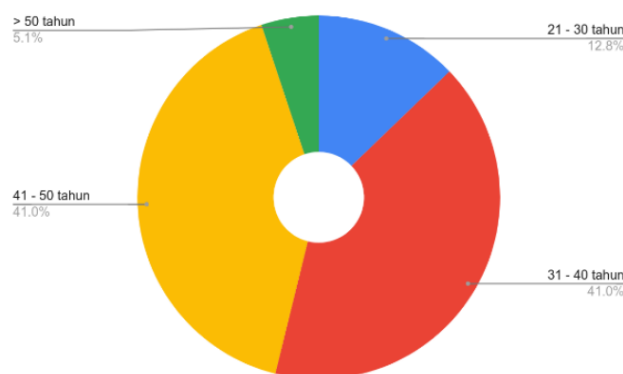
WhatsApp menawarkan berbagai fitur yang memudahkan pengguna, termasuk WhatsApp Web untuk komputer, aplikasi ini memiliki celah keamanan yang dapat mengancam privasi pengguna. Salah satu risiko utama adalah penyadapan percakapan yang melibatkan perangkat ponsel cerdas dan komputer [[9]]. Untuk meningkatkan keamanan layanan pesan instan seperti aplikasi WhatsApp, penggunaan *Multi Factor Authentication* (MFA) menjadi semakin penting. MFA menggabungkan dua atau lebih jenis autentikasi untuk memberikan cara yang lebih aman dalam memverifikasi identitas pengguna [[10]]. Implementasi MFA dapat meningkatkan tingkat keamanan sistem dalam hal ini aplikasi Whatsapp, mengurangi risiko pihak tidak bertanggung jawab mengakses aplikasi, dan meningkatkan tingkat perlindungan informasi sensitif pada perangkat [[11]]. Implementasi MFA pada aplikasi Whatsapp dengan mengaktifkan *Two-step Verification*, yaitu mengaktifkan terlebih dahulu *Personal Identification Number* (PIN) sebanyak 6 angka. Pengguna aplikasi Whatsapp yang sudah menerapkan MFA akan memiliki tampilan seperti pada Gambar 5.



Gambar 5. Two-step Verification

3.5 Evaluasi Security Awareness

Kegiatan Pengabdian kepada Masyarakat di Kalurahan Bangunjiwo, Kabupaten Bantul dalam bentuk sosialisasi atau kampanye security awareness dihadiri oleh 39 warga dengan rentang usia yang beragam. Berdasarkan hasil survei yang dilakukan rentang umur warga yang hadir dalam kegiatan ini didominasi warga berusia 31 - 50 tahun. Gambar 6 menunjukkan persentase rentang umum peserta kegiatan, adapun pembagian rentang umurnya adalah 21 - 30, 31 - 40, 41 - 50, dan lebih dari 50 tahun.



Gambar 6. Persentase Peserta Kampanye *Security Awareness*

Hasil survei merupakan instrumen melakukan evaluasi kegiatan dalam pemahaman terkait keamanan pada aplikasi Whatsapp dengan mengaktifkan *Two-step Verification* dan potensi tindak kejahatan siber. Berdasarkan hasil survei terdapat 4 warga yang tidak mengisi survei baik pre-test maupun post-test. Pre-test sebagai instrumen untuk mengetahui pengetahuan awal warga terkait keamanan siber pada ponsel cerdas. Sedangkan post-test sebagai instrumen untuk mengetahui pemahaman warga setelah diberikan materi tentang keamanan siber pada ponsel cerdas.

Instrumen dari survei yang utama adalah pengetahuan terkait potensi kejahatan siber pada ponsel cerdas dan teknik pengamanan aplikasi Whatsapp dengan mengaktifkan Two-step Verification. Berdasarkan Tabel 1 menunjukan warga menunjukan adanya peningkatan pengetahuan tentang kejahatan siber pada ponsel cerdas dan teknik pengamanan aplikasi Whatsapp. Pengetahuan warga Kalurahan Bangunjiwo, Kabupaten Bantul terkait kejahatan digital melalui aplikasi Whatsapp setelah mengikuti kegiatan menunjukan peningkatan sebesar 20,26 % sedangkan warga yang mengaktifkan OTP mengalami peningkatan sebesar 23,08%.

Tabel 1. Hasil Evaluasi

Pertanyaan	Pre-Test	Post-Test	Peningkatan
Apakah anda mengetahui adanya kejahatan melalui aplikasi Whatsapp?	30	34	20,26%
Apakah anda mengaktifkan PIN pada aplikasi Whatsapp?	5	14	23,08%

4. Kesimpulan

Kegiatan kampanye security awareness untuk warga sangat diperlukan hal ini disebabkan ancaman serangan siber yang semakin kompleks. Sasaran serangan siber tidak hanya perangkat digital tetapi initial access-nya justru dari pengguna perangkat digital, contohnya kurang waspada terkait informasi yang diterima berupa tautan phishing. Maka berdasarkan hasil survei masih perlu dilakukan pendampingan lebih lanjut untuk meningkatkan kewaspadaan dan ketahanan nasional pada sektor non-komersial.

Hasil dari kegiatan ini dapat digunakan untuk mendapatkan wawasan atau ide untuk penelitian lanjut. Hal ini dilihat dari potensi serangan siber dengan initial access-nya bersumber dari pengguna perangkat digital. Hanya terdapat 5 warga pengguna aplikasi Whatsapp yang sudah mengaktifkan PIN. Sehingga perlu dilakukan penguatan sumber daya manusia bidang keamanan siber pada sektor non-komersial.

Ucapan Terimakasih

Terimakasih disampaikan kepada pimpinan Kalurahan Bangunjiwo, Kabupaten Bantul, Daerah Istimewa Yogyakarta yang telah menjadi mitra Universitas Jenderal Achmad Yani Yogyakarta. Kegiatan Pengabdian kepada Masyarakat merupakan upaya melakukan transfer knowledge antar lembaga.

Sumber Dana

Universitas Jenderal Achmad Yani Yogyakarta. Surat Tugas Nomor ST/255/LPPMUNJAYA/VI/2024.

Pustaka

- [1] D. Susanti dan M. Suyudi, "WhatsApp Usage Training in Marketing Home-Based Products for Benzo Amanah Cooperative Members Bandung Indonesia," *IJRCS*, vol. 1, no. 3, hlm. 29–34, Okt 2020, doi: 10.46336/ijrcs.v1i3.106.
- [2] D. Andamisari, "Penggunaan Status Whatsapp Sebagai Digital Marketing Warga Kecamatan Medan Satria Bekasi Di Era New Normal," *lugas*, vol. 5, no. 1, hlm. 66–72, Jun 2021, doi: 10.31334/lugas.v5i1.1559.
- [3] D. T. Harsono, "Kewaspadaan Nasional Terhadap Ancaman siber dalam Rangka Penguatan Pertahanan Negara di Ibu Kota Nusantara," *Lembaga Ketahanan Nasional Republik Indonesia*, Jul 2023.
- [4] D. Hariyadi, A. Akbarul, Kharisma, dan A. Priadana, "Laron v2: Pengembangan Aplikasi Forensik Logikal untuk Mengakuisisi Percakapan Whatsapp di Android," *Smartics*, vol. 7, no. 1, hlm. 7–13, 2021.

- [5] A. M. Elmisery dan M. Sertovic, "Modular Platform for Detecting and Classifying Phishing Websites Using Cyber Threat Intelligence," *Electron. Commun. EASST*, vol. 80, hlm. 1–4, 2021, doi: 10.14279/tuj.eceasst.80.1178.
- [6] Z. Alkhalil, C. Hewage, L. Nawaf, dan I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, hlm. 563060, Mar 2021, doi: 10.3389/fcomp.2021.563060.
- [7] S. Chaudhary, V. Gkioulos, dan S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity*, vol. 8, no. 1, hlm. tyac006, Jan 2022, doi: 10.1093/cybsec/tyac006.
- [8] Lockheed Martin Corporation, "Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform," Lockheed Martin Corporation, 2015.
- [9] N. Anwar, Supriyanto Supriyanto, dan The Society of Digital Information and Wireless Communication, "Forensic Authentication of WhatsApp Messenger Using the Information Retrieval Approach," *IJCSDf*, vol. 8, no. 3, hlm. 206–212, 2019, doi: 10.17781/P002609.
- [10] A. Bissada dan A. Olmsted, "Mobile Multi-Factor Authentication," dalam 2017 12th International Conference for Internet Technology and Secured Transactions, *ICITST 2017*, 2018, hlm. 210–211. doi: 10.23919/ICITST.2017.8356383.
- [11] U. Rauf, M. Shehab, N. Qamar, dan S. Sameen, "Formal approach to thwart against insider attacks: A bioinspired auto-resilient policy regulation framework," *Future Gener Comput Syst*, vol. 117, hlm. 412–425, 2021, doi: 10.1016/j.future.2020.11.009.