Volume 6 Issue 2 (2023) Pages 250 - 256
SEIKO : Journal of Management & Business
ISSN : 2598-831X (Print) and ISSN : 2598-8301 (Online)

Edukasi mengenai Mobile Hacking: Pengenalan dan Mitigasi

Yan Puspitarani[1], Fitrah Rumaisa[2], Sriyani Violina[3], Feri Sulianta[4], Ai Rosita[5]
[1,2,3,4,5] *Program Studi Teknik Informatika, Universitas Widyatama*

Abstrak

Data merupakan hal yang berharga dan bersifat pribadi bagi perseorangan maupun perusahaan. Akan tetapi, pencurian data seringkali dilakukan terhadap sistem keamanan data yang memiliki celah. Hacking ini sudah marak dilakukan oleh kalangan muda. Jika tidak diarahkan dengan baik, besar kemungkinan banyak generasi muda yang menjadi pelaku cyber crime. Selain itu, untuk melakukan investigasi terhadap cyber crime, diperlukan juga digital forensic terhadap perangkat. Oleh karena itu, kegiatan pengabdian ini, akan memberikan edukasi kepada para anak SMA sebagai generasi muda dengan harapan agar para generasi muda tidak menjadi korban atau pelaku.

Kata Kunci: *hacking; forensic; cyber crime.*

Abstract

Data is valuable and personal for individuals and companies. However, data theft is often carried out against data security systems that have loopholes. Hacking is already rife done by young people. If it is not directed properly, it is very likely that many young people will become cybercriminals. In addition, to carry out investigations into cyber crime, digital forensics is also needed for devices. Therefore, this service activity will provide education to high school students as the younger generation with the hope that the younger generation will not become victims or perpetrators.

Keywords: *hacking; forensic; cyber crime.*

✉ Corresponding author : Yan Puspitarani
Email Address : yan.puspitarani@widyatama.ac.id

PENDAHULUAN

Saat ini pengguna internet mencapai sekitar 4 milyar di seluruh dunia (Setiawan, 2016). Penggunaan internet meliputi segala aspek kehidupan termasuk diantaranya adalah pembelajaran, komunikasi dan hiburan. Tingginya tingkat keaktifan dan penggunaan Internet di Indonesia memberikan dampak baik positif maupun negative. Berdasarkan hasil survey yang dilakukan Markplus Insight, jumlah pengguna internet Indonesia didominasi oleh generasi muda berusia 15-30 tahun.

Pada tahun 2021 tercatat 90,54 persen rumah tangga di Indonesia telah memiliki/menguasai minimal satu nomor telepon Seluler. Angka ini meningkat jika dibandingkan dengan kondisi tahun 2018 yang mencapai 88,46 persen. Tingginya angka kepemilikan ponsel di Indonesia memiliki dampak baik positif maupun negatif. Dampak positifnya adalah tingkat akses informasi yang cukup tinggi, sedangkan dampak negatif

yang harus diwaspadai adalah kejahatan siber terhadap ponsel ("Statistik Telekomunikasi Indonesia," 2022).

Mengutip data dari National Cyber Security Index (NCSI) Indonesia berada di peringkat ke-6 Asia Tenggara dalam hal indeks keamanan siber. Sedangkan secara global, Indonesia menduduki peringkat ke-83 dari 160 negara. Indikator penilaian NCSI adalah 1) aturan hukum negara terkait cyber security; 2) Keberadaan lembaga pemerintah di bidang keamanan siber; 3) kerja sama pemerintah terkait keamanan siber; 4) bukti-bukti publik seperti situs resmi pemerintah atau program lain yang terkait (Dihni, 2022).

Kejahatan siber atau kerap dikenal dengan cyber crime merupakan tindak perilaku kejahatan berbasis komputer dan jaringan internet. Pelaku dari kejahatan siber biasanya akan meretas sistem untuk memperoleh data korban yang bersifat privasi. Terdapat berbagai jenis tindak kejahatan siber. Berikut empat jenis tindak kejahatan siber, penipuan, Phising, Peretasan, Cyber Stalking dan Cyber Bullying (Pertiwi, 2021).

Data merupakan hal yang berharga dan bersifat pribadi bagi perseorangan maupun perusahaan. Akan tetapi, pencurian data seringkali dilakukan terhadap sistem keamanan data yang memiliki celah. Hacking ini sudah marak dilakukan oleh kalangan muda. Jika tidak diarahkan dengan baik, besar kemungkinan banyak generasi muda yang menjadi pelaku cyber crime. Selain itu, untuk melakukan investigasi terhadap cyber crime, diperlukan juga digital forensic terhadap perangkat. Oleh karena itu, kegiatan pengabdian ini, akan memberikan edukasi kepada para anak SMA sebagai generasi muda dengan harapan agar para generasi muda tidak menjadi korban atau pelaku.

Pada pengabdian masyarakat ini akan dibahas terutama adalah peretasan ponsel. Peretasan ponsel dapat membahayakan identitas dan privasi tanpa kita sadari. Peretas (hacker) terus mengembangkan dan meningkatkan metode peretasan, membuat mereka semakin sulit dikenali. Rata-rata pengguna ponsel mungkin tidak memahami & tidak aware terhadap sejumlah serangan siber. Untungnya, kita dapat melindungi diri sendiri dengan tetap mengikuti perkembangan peretasan terbaru, dan melakukan tindakan pencegahan (prevention) untuk mengurangi resiko serangan.

Mobile Hacking / Phone Hacking melibatkan metode & teknik (peretasan) apapun dimana seseorang (hacker) memaksa (untuk mendapatkan) akses ke ponsel atau komunikasinya. Ini dapat meliputi dari pelanggaran keamanan tingkat lanjut (advanced) yang parah, atau hanya sekadar mendengarkan (menyadap) koneksi internet yang tidak aman (unsecure channel). Ini juga dapat melibatkan pencurian fisik ponsel dan meretasnya secara paksa melalui metode seperti brute force.

Pada pengabdian masyarakat ini, akan dibahas mengenai bagaimana cara kerja mobile hacking dengan tujuan untuk mencegah dan menjaga keamanan data.

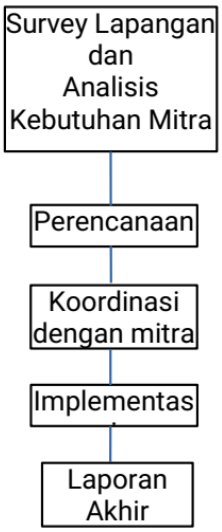
METODOLOGI

Survey lapangan, dilakukan dengan tujuan untuk mengumpulkan dan analisis kebutuhan serta mendiskusikan solusi yang akan dijalankan. Setelah dilakukan pengumpulan dan analisis kebutuhan, tim menyusun perencanaan sesuai hasil koordinasi tersebut. Tim kembali melakukan koordinasi dengan mitra untuk melakukan kesepakatan waktu pelaksanaan.

Tahap implementasi adalah pelaksanaan edukasi dalam format webinar dengan topik "Mobile Hacking: pengenalan dan mitigasi".

Tahap akhir adalah evaluasi kegiatan dan penyusunan laporan akhir sebagai dasar pertanggung jawaban kegiatan yang telah dilakukan oleh tim pelaksana. Luaran PKM yang ditargetkan adalah berupa artikel ilmiah yang diterbitkan di jurnal pengabdian masyarakat.

Metode pelaksanaan yang diimplementasikan dalam program pengabdian masyarakat ini dapat dilihat pada gambar 1.



Gambar 1. Metode Pelaksanaan Program

HASIL DAN PEMBAHASAN

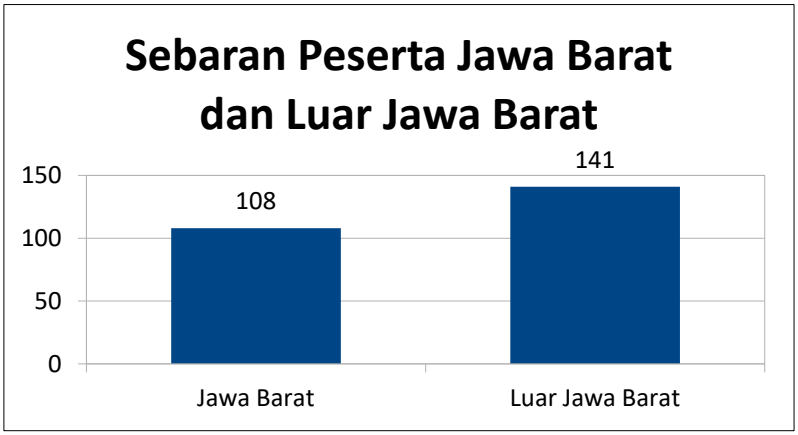
Hasil dari survey dan analisis kebutuhan mitra adalah perlunya edukasi kepada masyarakat khususnya siswa SMA tentang ancaman terhadap pengguna ponsel beserta migitasi untuk mencegah para generasi muda menjadi objek dan pelaku. Siswa perlu dikenalkan terhadap berbagai kemungkinan kejahatan cyber untuk mengurangi risiko menjadi objek dari kejahatan tersebut.

Setelah menganalisis kebutuhan dilakukan perencanaan proses edukasi dengan topik sesuai kebutuhan mitra. Hasil dari perencanaan adalah kegiatan akan dilaksanakan berupa edukasi dengan format webinar berisikan materi terkait keamanan penggunaan mobile device. Pada tahap perencanaan juga didiskusikan perlunya memperluas audiens yang tadinya terbatas pada mitra bisa dikembangkan ke masyarakat umum mengingat pentingnya topik yang akan dibahas. Hal ini tentu dikoordinasikan terlebih dulu bersama mitra dengan catatan peserta dari mitra menjadi prioritas utama kegiatan ini.

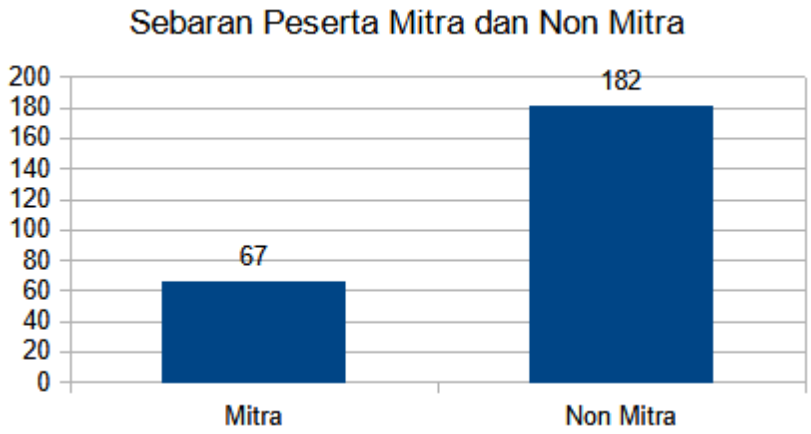
Tim kemudian kembali menemui mitra untuk melakukan koordinasi mengenai waktu pelaksanaan dan sosialisasi kepada siswa mengenai kegiatan tersebut.

Gambar 2. Koordinasi dan Sosialisasi Program

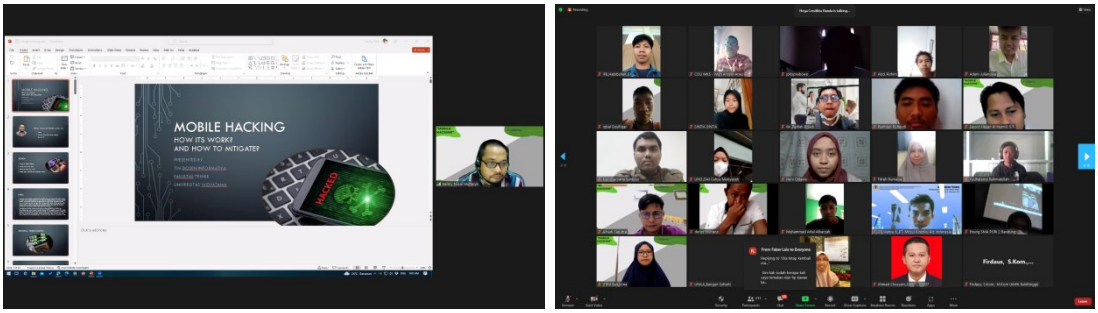
Kegiatan edukasi melalui webinar dengan topik "mobile hacking" diikuti oleh 249 orang, dengan sebaran peserta sepertipada gambar 3 dan gambar 4 berikut.



Gambar 3. Sebaran Peserta Mitra dan Luar Mitra



Gambar 4. Sebaran Peserta Jawa Barat dan Luar Jawa Barat



Gambar 5. Kegiatan Webinar

Sebagian besar peserta antusias dengan materi yang disajikan. Banyak peserta yang tertarik untuk mengajukan pertanyaan maupun komentar terhadap materi yang disajikan, Materi dan pertanyaan yang diajukan peserta dapat dilihat di tabel 1 dan tabel 2.

Tabel 1. Materi Edukasi

No	Materi
1.	Definisi dan Pengenalan Mobile Hacking
2.	Metode dan Teknik Mobile Hacking
3.	Ciri-ciri ponsel yang sudah dikuasai hacker
4.	Bagaimana melindungi data dan Privasi
5.	Apa yang harus dilakukan jika ponsel diretas
6.	Mitigasi agar terhindar dari serangan

Tabel 2. Pertanyaan Peserta

No	Pertanyaan
1.	Ciri-ciri HP kita sudah disadap
2.	Untuk SIM card swapping, apakah mungkin SIM Card kita di-clone oleh hacker secara remote?ai.
3.	Adakah demo RAT? Adakah RAT yg sering digunakan oleh mahasiswa?(remote admin tool)
4.	Bisa dijelaskan lebih terperinci cara menghapus data kita dari jauhd
5.	Apakah terdapat sebuah aplikasi atau website yang ampuh untuk mendeteksi suatu virus yang ada di handphone maupun perangkat lainnya. Serta bagaimana cara menghapus virus yang adag jarang
6.	Sebagai hacker selain memahami IT, ilmu apa lagi yang harus dipahami sebagai pemula
7.	Bagaimana cara mengetahui kabel yang ada O.MG nya
8.	Untuk testing guide mobile apakah ada standar khusus nya seperti owasp atau yang lainnya

No	Pertanyaan
9.	Bagaimana cara kita menemukan malware yang berada di hp kita? apakah menggunakan aplikasi tambahan?
10.	Bagaimana cara melakukan mitigasi agar terhindar dari serangan social engineering dan phising attack
11.	Bagaimana kira mengetahui siapa yang meretas tersebut?

Keaktifan dan banyaknya respon berupa komentar dan pertanyaan menunjukkan ketertarikan dari peserta untuk lebih memahami materi yang diberikan.

Diskusi

Teknologi perangkat mobile telah membawa semua akun & data pribadi kita ke dalam satu lokasi/lingkungan yang nyaman & mudah diakses. Hal itu menjadikan ponsel kita sebuah target sempurna bagi peretas. Mulai dari perbankan, email, marketplace, & media sosial ditautkan ke ponsel. Artinya, begitu peretas mendapatkan akses ke ponsel, maka semua aplikasi kita menjadi gerbang untuk pencurian data di dunia maya (cyber crime).

Kewaspadaan diperlukan untuk menjaga keamanan data terutama di perangkat mobil. Saat peretas masuk ke ponsel, mereka akan mencoba mencuri akses ke akun yang berharga (email, banking, social media, dll). Periksa kembali media social, email untuk permintaan reset password, lokasi login yang tidak biasa, atau verifikasi pendaftaran akun baru.

SIMPULAN

Dari rangkaian kegiatan edukasi dengan tema "Mobile Hacking: How it work and how to mitigate" berjalan dengan lancar, dan mendapatkan apresiasi positif baik dari pihak universitas, sekolah, maupun peserta lainnya. Mulai dari dari proses perijinan sampai dengan pelaksanaan, kegiatan ini didukung penuh oleh semua pihak yang terkait.

Keaktifan dan banyaknya respon berupa komentar dan pertanyaan menunjukkan ketertarikan dari peserta untuk lebih memahami materi yang diberikan sehingga diharapkan di masa yang akan datang akan ada pelatihan-pelatihan lanjutan baik tema yang sama/sejenis maupun topik-topik lain.

Referensi :

Dihni, V. A. (2022). *Indeks Keamanan Siber Negara-negara Asia Tenggara*. https://databoks.katadata.co.id/datapublish/2022/03/07/keamanan-siber-indonesia-peringkat-ke-6-di-asia-tenggara

Pertiwi, R. (2021). *Kenali 4 jenis kejahatan Siber*. https://kominfo.kotabogor.go.id/index.php/post/single/740

Setiawan, Y. (2016). *Mengenalkan teknologi Internet of Things kepada siswa/i SMK: Peluncuran Lomba SMK Inclusive Innovation Challenge 2016*. http://smk.kemdikbud.go.id/konten/1617/mengenalkan-teknologi-internet-of-things-kepada-siswai-smk-peluncuran-lomba-smk-inclusive-innovation-challenge-2016

Statistik Telekomunikasi Indonesia. (2022). In *Badan Pusat Statistik*. https://www.bps.go.id/publication/2023/08/31/131385d0253c6aae7c7a59fa/statistik-telekomunikasi-indonesia-2022.html